DIGITAL SECURITY &PRIVACY

FOR HUMAN RIGHTS DEFENDERS

FrontLine
INTERNATIONAL FOUNDATION
FOR THE PROTECTION
OF HUMAN RIGHTS DEFENDERS

DIGITAL SECURITY &PRIVACY

FOR HUMAN RIGHTS DEFENDERS

This book is dedicated to all human rights defenders, continuing their difficult and honest work, also on the Internet. Some of these people are in prison due to their activities on the Internet.
Mohammed Abbou is serving a 3,5 year prison term in Tunisia for publishing online an article that compared Tunisian prisons to Abu Ghraib.

FrontLine
INTERNATIONAL FOUNDATION
FOR THE PROTECTION
OF HUMAN RIGHTS DEFENDERS

DIGITAL SECURITY AND PRIVACY FOR HUMAN RIGHTS DEFENDERS

February 2007

by Dmitri Vitaliev

Front Line acknowledges financial support from Irish Aid which has made this project possible.
Responsibility for the contents of the manual rests solely with the author and Front Line.

ACKNOWLEDGEMENTS

Front Line and Dmitri Vitaliev would like to thank the following people and organisations for the invaluable help in researching and writing this book:

■ Reporters sans frontières	www.rsf.org
■ Privacy International	www.privacyinternational.org
■ The OpenNet Initiative	www.opennetinitiative.org
■ Wikipedia	www.wikipedia.org
■ Berkman Center for Internet & Society at Harvard Law School	http://cyber.law.harvard.edu
■ International Freedom of Expression eXchange (IFEX)	www.ifex.org
■ The Association for Progressive Communications	www.apc.org
■ Peace Brigades International	www.pbi.org
■ Electronic Frontier Foundation	www.eff.org
■ Cambridge Security Programme	www.cambridge-security.net
■ Privaterra	www.privaterra.org

Steven Murdoch
Ross Anderson
Elijah Zarwan
Julian Wolfson
Bert-Jaap Koops
Front Line Staff

...and numerous human rights defenders from countries around the world including Zimbabwe, Guatemala, China, Cuba, Tunisia, Saudi Arabia, Egypt, Yemen, Kyrgyzstan, Russia, Belarus, Mexico etc. for answering questions, providing testimonials and evidence that resulted in the idea behind this book and its contents.

graphic design and illustrations Assi Kootstra

FRONT LINE

The International Foundation for the Protection of Human Rights Defenders

Human Rights are guaranteed under international law but working to ensure that they are realised and taking up the cases of those who have had their rights violated can be a dangerous business in countries all around the world. Human Rights Defenders are often the only force standing between ordinary people and the unbridled power of the state. They are vital to the development of democratic processes and institutions, ending impunity and the promotion and protection of human rights.

Human Rights Defenders often face harassment, detention, torture, defamation, suspension from their employment, denial of freedom of movement and difficulty in obtaining legal recognition for their associations. In some countries they are killed or "disappeared."

Front Line was founded in Dublin in 2001 with the specific aim of protecting Human Rights Defenders, people who work, non-violently, for any or all of the rights enshrined in the Universal Declaration of Human Rights (UDHR). Front Line aims to address some of the needs identified by defenders themselves, including protection, networking, training and access to the thematic and country mechanisms of the UN and other regional bodies.

Front Line's main focus is on those human rights defenders at risk, either temporarily or permanently because of their work on behalf of their fellow citizens. Front Line runs a small grants program to provide for the security needs of defenders. Front Line mobilizes campaigning and lobbying on behalf of defenders at immediate risk. In emergency situations Front Line can facilitate temporary relocation.

Front Line conducts research and publishes reports on the situation of human rights defenders in specific countries. The organization also develops resource materials and training packages on behalf of human rights defenders as well as facilitating networking and exchange between defenders in different parts of the world. Front Line projects are generally undertaken in partnership with specific national human rights organizations.

Front Line promotes awareness of the Universal Declaration of Human Rights and is working to ensure that the principles and standards set out in the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognised Human Rights and Fundamental Freedoms (known as the Declaration on Human Rights Defenders) are known, respected and adhered to worldwide.

Front Line has Special Consultative Status with the Economic and Social Council of the United Nations.

To support this work Front Line relies entirely on the generosity of individual and organizational funding.

Front Line has been fortunate, since its launch in 2001, to have received funding from a variety of sources and gratefully receives donations on an individual basis.

Front Line has charitable status (CHY NO 14029), is independent and impartial.

CONTENTS

As we know, there are known knowns. There are things we know we know. We also know there are known unknowns. That is to say we know there are some things we do not know. But there are also unknown unknowns, the ones we don't know we don't know.

Donald Rumsfeld, US Secretary of Defence, December 2003

INTRODUCTION

Human rights defenders are increasingly using computers and the Internet in their work. Although access to technology is still a huge issue around the world, electronic means of storing and communicating information are getting more and more common in human rights organisations. In many ways, the Internet has improved the work and security of human rights defenders: it increased the effectiveness of their mission, facilitated their access to information and boosted communications with partner organisations. On the other hand, it has ushered in some previously unknown problems and vulnerabilities.

This book is not aimed at a computer wizard. Its purposes are educating ordinary computer users and providing them with solutions to problems of privacy and security in a modern digital environment.

———

We write documents, draw pictures and communicate with each other on a computer and via the Internet. Programs to carry out these functions have been made so simple that we do not have to know how exactly a computer operates – as long as it functions properly. We therefore utilise technology that we do not wholly understand, yet rely upon it heavily. As consumers of the digital era, we want a finished product, not the list of its components.

Whether we watch television that receives a satellite signal, cross the road on a green light or undergo surgery – we rely on computers.

But what do we do when things go wrong? When our computers break down and annihilate years of hard work? When our emails do not reach the addressees or when we cannot access a website? How do we react to a news story of a virus damaging computers around the world, or to an email purportedly from a friend, asking to open the attached file? Uninformed decisions lead to bad choices, and blind reliance on technology often results in costly mistakes.

———

The work of human rights defenders and organisations is intertwined with technology. It facilitates communications and allows us to store and process large amounts of information cheaply and within minimal space. Technology enables even a small and remote organisation to acquire a global voice. An electronic conversation that took place a couple of years before can be recalled within seconds, and a perpetrator of a human rights violation, say, will receive thousands of angry emails and faxes from around the world. In short, computers and the Internet have become essential and inseparable parts of human rights work.

The Problems

The abundance of digitally stored information and the ability to disseminate it around the world has created one of the biggest industries in human history –

the information industry. Worth billions of dollars, it generates huge profits for those who control and operate its underlying structure. The ability to manipulate, monitor and restrict electronic information has become a hobby, a job or a policy for many individuals, companies and government departments. The war on terrorism has provided them with a *carte blanche* to implement surveillance and censorship of the once open and free Internet. Justifications of such activities run deep and often erode some basic human rights and freedoms. Certain countries of the world have even introduced legislation justifying and encouraging such practices to further increase persecution and suffering of human rights defenders and to undermine their legitimate work thus reducing their ability to protect the rights of others.

As the new technology remains largely unknown, human rights defenders often choose to provide for their own electronic security. Dozens of defenders and independent journalists are currently in prison for trying to spread their work to the digital world without proper knowledge of how to do it safely.

It is important to say here that technology in general has not yet reached every corner of our planet. Millions of people have never seen a traffic light, let alone a computer. The enormous material gap between wealthy and poor nations also manifests itself in the world of electronic technology and is known as **digital divide**. The human rights defenders on the wrong side of this divide find their opportunities of reaching out to the global community greatly reduced.

This book is an introduction to the ever growing and complex world of electronic security. Not only will it raise your level of knowledge and awareness about computers and the Internet, it will also warn you of different risks you may face in the digital environment and will tell you how to deal with them.

The book is written for human rights defenders, and therefore it looks at the ways of preventing the erosion of universally guaranteed freedoms. Alongside elements of theory, it offers possible solutions to some problems of computer and Internet security.

Security as a process

This is not a book of answers. Imagine approaching a security expert for an advice on how to react to real-life threats and physical harassment. Before coming up with an answer, he is likely to ask you a number of questions as to the exact nature of risks and threats you are facing. It is the same with electronic security. I cannot possibly offer you an immediate solution for every problem of yours. If you ever spoke with security experts, you may have noticed that they seldom come up with direct answers. Because there is no such thing as a one and only right answer.

A security manual is not a list of possible problems and solutions to them. It is rather a descriptive process of introducing you to the many different components of computer and Internet operations (specifically for human rights defenders, in the given case). My goal is to improve your knowledge of the elements of electronic security and digital privacy. The book operates in facts, theories, methods and possible explanations of computer insecurities and solutions to them. Together, they should help you resolve and strengthen your own electronic security. Hopefully, the manual will also trigger enough interest in the above-mentioned topics to inspire you to carry out your own research and to continue learning.

A Guide to the Manual

This manual is divided into four parts which can be read in any order. The reader does not require any special expertise, although some basic knowledge of computer and Internet operations would come handy. The chapters, containing information of a more technical nature, are marked 'For Techies'.

The First Section is about understanding your security needs and vulnerabilities. It describes a non-technical approach to the digital environment. A method of mapping the threats, posed by a particular situation, is offered to help you decide on the strategies for implementing privacy and security solutions.

The Second Section lists various elements of computer and Internet security. It introduces the reader to computer operations and Internet infrastructure. Methods of securing data, bypassing Internet censorship and protecting yourself against malicious attacks are explained in detail.

The Third Section is a summary of worldwide legislation to restrict and monitor information flow and communications. It shows the downward trend, caused by the growth of restrictions to the rights to freedom of expression, privacy and communication, in many countries. Cases of human rights defenders currently in prison or persecuted because of their work through the Internet are presented as examples of the ways some governments enforce these pieces of legislation.

The Fourth Section drafts possible scenarios for human rights defenders and their organisations of dealing with problems of electronic insecurity and ensuring continuation of their work. The scenarios relate to the concepts presented throughout the book and solutions are based on realisable actions.

Following the case studies, you will find Appendices, aiming to provide you with detailed background on computers and the Internet, as well as in-depth explanations of certain security topics. At the end of the book, there is a Glossary explaining many of the more technical and unfamiliar words used in this manual.

This book can be used alongside the *NGO in a Box – Security Edition* project (http://security.ngoinabox.org) – a collection of software tools and manuals comprising the necessary resources to achieve better privacy and security on your computers and on the Internet. All software mentioned in this book can be found either in the *NGO in a Box – Security Edition* or will be included with its next release in the beginning of 2007. All the software can also be downloaded from the Internet.

Some of the concepts and technology, described and taught in this manual, have been made illegal in several countries of the world. Please pay careful attention to your local legislation and make an informed decision about possession and use of this book.

1.1 SECURITY AND INSECURITY

Computers and the Internet are all about information seeking, storage and exchange. Hence, the topic of security in the digital realm relates to the security of information. We need to operate in a climate where our information is not stolen, damaged, compromised or restricted. The Internet, in theory, provides everyone with an equal opportunity to access and disseminate information. Yet, as many incidents have shown, this is not always the case. Governments and corporations realise the importance and value of controlling information flows, and of being able to decide when to restrict them. The security of information is further complicated by malicious individuals creating computer viruses and hacking into computer systems, often with no other motive than causing damage.

—

Confusion is enhanced by the abundance of software, hardware and electronic devices designed to make the storage and exchange of information easier. An average computer today contains millions of lines of complex code and hundreds of components which could malfunction and damage the system at any time. Users have to immerse themselves in concepts and technology that seem to be far removed from the real world. The security of your computer falls first and foremost upon your shoulders and requires some comprehension of how its systems actually work.

—

The race to reap profits from the Internet has resulted in the appearance of numerous financial services and agencies. You can now book a flight, buy a book, transfer money, play poker, do shopping and advertise on the Internet. We have increased our capacity for getting more things done more quickly, yet we have also created a myriad of new information flows, and with them – new concepts of insecurity we do not yet know how to deal with. Marketing companies are building profiles of users on the Internet hoping to turn your browsing experience into a constant shopping trip. Personal information, collected by governments and social agencies, is then sold to data mining companies, whose aim is to accumulate as much detail as possible about your private life and habits. This information is then used in surveys, product development or national security updates. Our email accounts are cluttered with useless and unsolicited messages, causing a huge disruption to our work, the Internet connectivity and computer reliance.

—

It appears that chaos has come to rule our digital world. Nothing is certain and everything is possible. Most of us just want to get on with writing our document or sending an email, without considering the outcomes of insecurity. Unfortunately, this is not possible in the digital environment. To be a confident player in this new age of information highways and emerging technologies, you need to be fully aware of your potential and your weaknesses. You must have the knowledge and skills to survive and develop.

METHODS AND TRENDS OF SURVEILLANCE, CENSORSHIP AND ELECTRONIC ATTACK

1.1

The right to privacy is a contentious issue in the modern world. Does anyone have the right to access our private information? In the aftermath of the 9/11 attacks in the USA, most governments seem to think they should have full control of our communications and the ability to monitor and access our computers. Many countries have implemented legislation and introduced the technology that increased their power of surveillance to previously unseen levels. The **ECHELON** project, for instance, is a global surveillance system, able to record and process telephone, Internet and satellite communications.

In May 2001, the European Parliament's Temporary Committee on the Echelon Interception System (established in July 2000) issued a report concluding that "the existence of a global system for intercepting communications . . . is no longer in doubt." According to the committee, the Echelon system (reportedly run by the United States in cooperation with Britain, Canada, Australia and New Zealand) was set up at the beginning of the Cold War for intelligence gathering and has developed into a network of intercept stations around the world. Its primary purpose, according to the report, is to intercept private and commercial communications, not military intelligence.[1]

►**ECHELON** intercept station at Menwith Hill, England. *Source: www.greaterthings.com/Word-Number/Organizations/Echelon*

The right to freedom of expression and information has also been attacked and suppressed on the Internet. The ability to access information from any Internet connection point on Earth, regardless of where this information is stored, has resulted in many governments – not ready or willing to provide this type of freedom to their citizens – scrambling to restrict such free access. Huge resources have been poured into developing country-specific filtering systems to block the Internet information, deemed inappropriate or damaging to the local country's laws and 'national morale'.

In China, a system known as the "Great Firewall" routes all international connections through proxy servers at official gateways, where the Ministry for Public Security (MPS) officials identify individual users and content, define rights, and carefully monitor network traffic into and out of the country. At a 2001 security industry conference, the government of China announced an ambitious successor project known as "Golden Shield." Rather than relying solely on a national Intranet, separated from the global Internet by a massive firewall, China will now build surveillance intelligence into the network, allowing it to "see," "hear" and "think." Content-filtration will shift from the national level to millions of digital information and communications devices in public places and people's homes. The technology behind Golden Shield is incredibly complex and is based on research undertaken largely by Western technology firms, including Nortel Networks, Sun Microsystems, Cisco and others.[2]

1
European Parliament, Temporary Committee on the Echelon Interception System (2001) *Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON interception system)*, May 18, 2001. (2001/2098(INI)) (adopted July 11, 2001) Available at http://www.europarl.eu.int/tempcom/echelon/pdf/prechelon_en.pdf

2
Privacy International – Privacy and Human Rights Report 2004 – The Threats to Privacy

These filters undermine our ability to take advantage of the Internet and to cross geographical boundaries in our quest for learning and communication. They are also in breach of several articles in the Universal Declaration of Human Rights (UDHR) guaranteeing every person rights to privacy and free expression. Significantly, these systems were developed only after the growth and potential of the Internet as the global information exchange was noticed. They were not part of the original idea behind the development of the Internet.

—

Surveillance and monitoring techniques have passed from the hands of intelligence personnel to the hardware and software systems, operated by private companies and government agencies. Phone bugging and letter opening has been superseded by the technology that allows monitoring of everyone and everything at once. The popularity of the Internet and its integration into our daily life has made that possible. Previously, someone considered dangerous to national security was spied upon. Now, we are all under suspicion as a result of the surveillance and filtering systems our governments install on the Internet. The technology does not often differentiate between users as it waits for certain keywords to appear in our email and Internet searches, and when triggered, alerts surveillance teams or blocks our communications. In 1998, the Russian government passed a law stating that all Internet Service Providers (ISPs) must install a computer black box with a link back to the Russian Federal Security Services (FSB) to record all the Internet activity of their users.

—

I have witnessed such Internet-based filtering repeatedly. In the days following the attacks on the New York Trade Centre, while working for a global computer company, I had an urge to explore the obscure world of religious fundamentalism. After browsing through certain extremists websites, I was approached by two of the company's security guards who asked me why I was looking for that particular information. At first, I was dumbfounded – how did they find out? Then I asked the guards who gave them the right to question me. The next day, a company memo banned all staff from visiting websites that contradicted "the organisation's ethics and policy"'.

—

The debate about controlling the Internet and information flows for the purposes of countering terrorism is outside the boundaries of this manual. It has to be said, however, that such practices have reduced freedom of expression, association and privacy all over the world, in direct contravention of the UDHR. Governments have installed systems to monitor their citizens on the scale far beyond the measures to fight terrorism. Information on human rights, freedoms of the media, religion, sexual orientation, thought and political movements, to name just a few, has been made inaccessible to many.

> *... "The Uzbekistan government has reportedly ordered the country's internet service providers (ISPs) to block the website www.neweurasia.net, which hosts a network of weblogs covering Central Asia and the Caucasus. The government's decision to block all national access to www.neweurasia.net is believed to be the first censoring of a weblog in Central Asia..."*[3]

3
www.newseurasia.net
July 6th, 2006

... "The Socialist Republic of Vietnam regulates access to the Internet by its citizens extensively, through both technical and legal means. According to the study by the OpenNet Initiative (ONI), the Vietnamese state attempts to stop citizens from accessing political and religious material deemed to be subversive along various axes. The technical sophistication, breadth, and effectiveness of Vietnam's filtering are increasing with time, and are augmented by an ever-expanding set of legal regulations and prohibitions that govern on-line activity. Vietnam purports to prevent access to the Internet sites primarily to safeguard against obscene or sexually explicit content. However, the state's actual motives are far more pragmatic: while it does not block any of the pornographic, it filters a significant fraction - in some cases, the great majority - of sites with politically or religiously sensitive material that could undermine Vietnam's one-party system..."[4]

Encryption has become one of the last resorts of privacy on the Internet. It enables us to make our messages and communications unreadable to all but the intended party. A layer of **encryption** was even built into the Internet structure to allow for secure financial transactions (**SSL**). When this system began to be applied for securing other, non-financial, information, it was met with strong opposition in many countries. At first, the US government tried to ban all **SSL encryption** of the complexity higher than they could decrypt. In 2000, Britain, in her turn, introduced the Regulation of Investigatory Powers Act (RIP) which made no provisions for one's right to encrypt information, but stated that a user must surrender his passwords when asked to do so by the investigative forces or face 6-month imprisonment. In 1998, the government of Singapore passed the Computer Misuse Act that allowed the country's security services to intercept email messages, decrypt encoded messages and confiscate computers without a warrant in the course of investigations[5]. Some countries, like Turkmenistan have banned **encryption** altogether. A world-wide monitoring system, like **ECHELON** (or any other), will probably collect all encrypted emails for further inspection, simply because they were encrypted in the first place. Any attempt at privacy will therefore be seen as an intention to hide something.

SPECIFIC THREATS FACED BY HUMAN RIGHTS DEFENDERS

Human rights defenders often become targets of surveillance and censorship in their own country. Their right to freedom of expression is often monitored, censored and repressed. Often they are facing heavy penalties for continuing their work. The digital world has been both a blessing and a curse for them. On the one hand, the speed of communications has brought them closer to their colleagues from around the world, and the news of human rights violations spreads around within minutes. People are being mobilised via the Internet, and many social campaigns have moved online. The negative aspect of the widespread use of computers and the Internet lies in over reliance on complex technology and the increased threat from targeted electronic surveillance and attacks. At the same time, the defenders in poorer countries who do not have computers and/or access to the Internet have found themselves left out of global focus and reach – another example of the imbalance caused by the **digital divide**.

Over the years, HRDs have learnt to operate in their own environment and have developed mechanisms for their own protection and prevention of

4
http://www.opennet.net/studies/vietnam
Internet Filtering in Vietnam in 2005-2006: A Country Study

5
Reporters sans frontières – Annual Report 2006, Internet

attacks. They know their countries' legal systems, have networks of friends and take decisions based on everyday wisdom. Computers and Internet, however, constitute a whole new world to discover and understand. It is their lack of interest or capacity to learn about electronic security that has lead to numerous arrests, attacks and misunderstandings in the HR community. Electronic security and digital privacy should become not just an important area for comprehension and participation, but also a new battleground in the struggle for the worldwide adherence to the principles of the UDHR.

—

Emails do not arrive at their destination, Internet connection is intermittent, computers are confiscated and viruses damage years of work. These problems are commonplace and familiar. Another common phenomenon is the increasing attention of those in power to online publishing. The authorities are actively searching through Internet news sites, blogs and forums – with swift retribution in cases when "undesired" material originating from a HRD is discovered. Take the case of Mohamed Abbou, who is serving a 3,5 year prison term in Tunisia for publishing online an article that compared Tunisian prisons to Abu Ghraib6. In China, 50 journalists are in prison because of their Internet-related activities[7].

—

Human rights defenders need to secure their work by learning about the technology and concepts of the computer and Internet operations. This will make them more effective in protecting themselves and in promoting the rights of those they try to defend.

6
Front Line
http://www.frontlinedefenders.org/news/2081

7
Reporters sans frontières
www.rsf.org Februari 2007

1.2 SECURITY AWARENESS

ABSTRACT

1 Ask yourself, how easy is it for an intruder to gain access to your office and working space?
2 Be aware that using a computer in an Internet café is more insecurethan using a home computer.
3 The information stored on your computer should be protected by several layers of access: the security of the computer itself, the room the computer is in and the building where you work.
4 Know the precise physical location of your data files and any archived duplicates.
5 Do not use an empty password or reveal it to others.
6 Be extra vigilant when opening emails and disable the preview function in your email program.
7 Restrict immediate access to your computer when it is unattended.

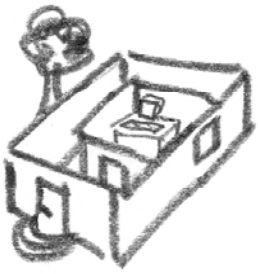
This chapter will discuss non-technical approaches to increasing the security of your information and communications. Being aware of your surroundings and thereby realising the potential threats you may be facing is the first step in your security plan. You should also understand your operational environment and have a level-headed approach to the likelihood of security incidents.

SECURING YOUR OPERATIONAL ENVIRONMENT

The majority of security incidents that affect the work and livelihood of HRDs are connected with physical violence and intrusion into their working environment. Whether you work from an office, carry around a laptop or only use Internet cafés, you should at all times be aware of your capabilities and limitations. Below is a list of questions you should be able to confidently answer. For each question, imagine the worst-case scenario and think how you would deal with it.

Office environment

- Is it easy for an outsider to access your office without permission?
- Can the windows be broken or the door forced?
- Do you have an alarm system, and do you trust the authorities that will respond to the intrusion?
- Do you have a 'waiting room' or reception area where a visitor can be queried before entering the main office?
- Do you have secure storage (e.g. safe) for confidential documents?
- Do you have a secure destruction method (e.g. file shredder) for confidential documents?
- What level of trust and access to your documents do any cleaning staff have?
- Do you dispose of your rubbish in a way that would make it impossible for an outsider to search or access it? In this regard, how do you dispose of confidential documents?



- Are you insured and do you have a strategy in the event of a natural disaster or theft?
- Are your office and staff visible from outside windows?
- How many copies of keys to your office are there and who has them?

Personal Workspace

- Can anyone else see your computer screen whilst you are working at your desk?
- Does anyone in the office know your password?
- Do you store confidential information in easily accessible places at your workspace?

- Do you restrict immediate access to your computer when you are away from your desk or office?
- Is your PC or laptop securely attached to your workspace, or can it be easily moved?

Public environment (e.g. Internet café)

- Does the café owner know your name and other personal details?
- Does the café owner monitor the Internet traffic of the customers?
- Are you confident that the computer you are using is free of viruses and spyware?

- Can people in the café see what you are reading or typing on the screen?
- When you are downloading files from the Internet, do they remain on the computer after you leave? How can you be sure?
- Is the Internet browsing history recorded on the computer?

All the above questions relate to a lack of security. You may note that thoroughness will be required should you wish to secure your working environment and your information. Some of these issues can be easily solved – like purchasing a metal cable to secure your laptop to your desk. Others will require co-operation of the entire staff - like greeting visitors upon entry and querying the purpose of their visit, as well as possible financial investment - like getting insurance or buying a safe. The majority of human rights organisations operate in an open, 'non-secretive' manner, yet they are often responsible for the confidentiality and security of their colleagues and those involved in the cases they deal with (witnesses, victims, claimants, etc.).

—

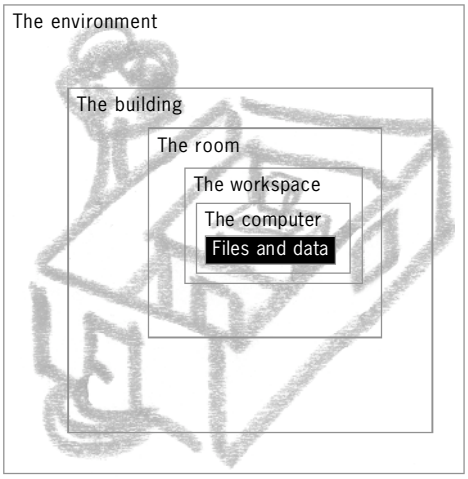
The ability to look at yourself from a different angle and evaluate your current security situation will go a long way towards forcing you to do something about the insecurities.

Assessing the threat to your safety and the safety of your computer must begin at the physical, real- world level. This is an area where you already have experience and expertise. Successful elimination of the risks, posed by the above questions, will provide a very important head start in the security of your digital environment.

Consider this diagram, which displays different layers of security around the information on your computer.

—

Security is all about layers to guarantee in-depth protection through the provision of barriers to access. You must build different layers of protection around important equipment and information. You need to protect access to:



- The building or premises where your equipment and/or files are located
- The room where your equipment and/or files are stored
- The workspace and physical location of your computer(s)
- Your files and data (including information on paper)

Perfect security is almost never attainable. As mere humans we all make mistakes, forget important information and bypass our own security strategies due to laziness or lack of time. We must employ some common sense when considering our security. It is not my intention to teach common sense to anyone, but I would like to present a list of questions that I would personally try to answer when ensuring that my work on and off a computer is done in the least compromising way to myself and to the security of my information. Later chapters will assist you in implementing some of the strategies below, so don't worry if some of my proposals seem too demanding at first.

QUESTIONS TO ASK YOURSELF

Where is my data?

First of all, always bear in mind where your most important documents are stored. This could be on the office computer or your laptop or on your USB memory card or even on a pile of floppy disks in the cupboard somewhere. It is critical that you have a copy of this data (a backup) as accidental loss or malicious damage would put you back several years. It is also a good idea not to have too many copies of files lying around, especially if they contain sensitive information. You have one backup copy on removable media, and another on a server in a different country (that you send via the Internet). You also bear in mind all locations of the copies, to make sure that they are not too numerous to control. If your office or home is cluttered with many disks in various locations, then you cannot ensure their safety.

Who knows my password?

Do not give out your password to anyone, even though you sometimes wish it were otherwise (critical situations, deadlines – I'm sure some of you have experienced this). Work pressure often demands that something be finished first and everything else will be sacrificed for this to happen. From a security perspective, this is a risky practice. Should your password be overheard by an intruder, written down and then lost, or fall victim of an accident, you may lose access to that email account or file forever.

Using a blank password is like leaving your house unlocked overnight in a rough neighbourhood. Maybe, no one will break in, or, maybe, they will and will steal everything. On the Internet, there are programs that automatically scan for 'open doors' and will find yours soon enough. Several years ago, Garry McKinnon – a British hacker managed to hack repeatedly into the

computer system of the US Government and the Department of Defence network by simply trying out blank or standard passwords (such as 'admin' or 'password'). Supposedly, he recovered information on Extra-Terrestrials and evidence of cover-ups. He was eventually caught and faces extradition from the UK to face court in the USA.[8]

I have many different passwords and no two are the same. Some of them are in my head (you must get used to creating and remembering good passwords), but most are stored in my password program. When I cannot recall a password or need one of great complexity, I ask the password program to create and store it for me. But I never write them down anywhere!

Whose computer is this?

Often I access my email and work on public computers in an Internet café or a library. I cannot make sure that each computer is free from viruses, spyware, Trojans or other malicious agents. Caution must be applied to the type of information I choose to open on this or that computer. This is not to say that I do not do any work on such a computer at all – I simply prioritise to ensure I work with the information that is not security sensitive and will not be a liability if corrupted or stolen. Remember that any file that I open or any text that I read on the Internet can easily be stored for later inspection or abuse if the computer I am on has been configured for that.

—

Some of you may not own a computer and have to use public computers all the time. Please, bear in mind the insecurity, described above, and take steps – wherever possible – to find out (and to check) what security precautions the computer owner has undertaken.

—

Every computer on the Internet has a unique identifier (more on this later). If the owner of the Internet café records your name and time of visit, then do not think your Internet browsing is anonymous. It could be linked directly to you.

Who is this?

Whenever I receive a strange email or an unidentified link, I always ask myself – who the sender of this information can be. If there are any doubts as to the legitimacy of a message, I do not click on it to find out if I was right, I delete the message immediately. Unfortunately, the world of computers has come so far that it is not even necessary to double-click on something to get infected with a virus. Modern day techniques can mean that the moment you open an email or a browser you may be infected with the newest brand of some destructive program or other.

This is why caution is your best friend. Our email boxes are bombarded with lots of useless information and, apart from being annoying and time-consuming, we normally do not see it as dangerous. In 2004, the Melissa virus reportedly caused the damage of up to 1.5bl USD around the world. It was actually a worm that was embedded into an email message. When the email was read, it automatically sent itself onwards to everyone in the recipient's address book. There was no other destructive malice involved. Yet this was enough to bring down large corporations for a long time and to make news headlines all over the planet. Disable the preview feature in your email program and if you want to read a new email from an unknown sender,

8 http://news.bbc.co.uk/2/hi/programmes/click_online/4977134.stm

make sure your virus cleaner and firewall are up-to-date. If you suspect the email is spam, delete it without opening.

Who can access your computer?

When you left your desk for the night or are stepping out for lunch, switch your computer off. Countless incidents can occur while your computer is operating and unattended. By switching the computer off, you are cutting its power supply and securing it from Internet attacks. Your **BIOS** or Windows security passwords are not effective if your computer is on. Some viruses lie dormant until the middle of the night, then activate your modem and dial a long distance number. It only takes a couple of minutes to boot most computers, so all you are sacrificing is a tiny bit of time while gaining a lot in security.

—

If you are using a public computer in an Internet café or library, try and reset it after you finished working (when using Windows, do this by pressing `Start > Shutdown > Restart` and wait for the computer to reload). This will clear a lot of the temporary data from your session.

Do you know your environment?

The knowledge of your surroundings is crucial to your security. You should be aware of the risks and dangers that each scenario presents, and of your resources for dealing with them. Working towards electronic security should include knowledge of relevant local legislation, office workspace security, a trusted circle of friends and colleagues, technical knowledge and awareness of your own and your computer's vulnerabilities and capacities. To prepare a better policy on security for yourself or your organisation, you need to build a threat model.

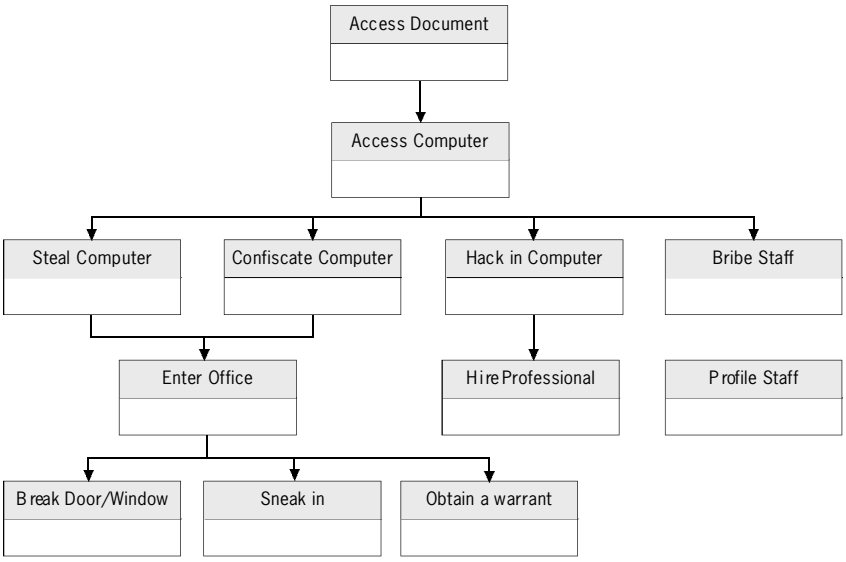
1.3 THREAT ASSESSMENT & THE SECURITY CIRCLE

ABSTRACT

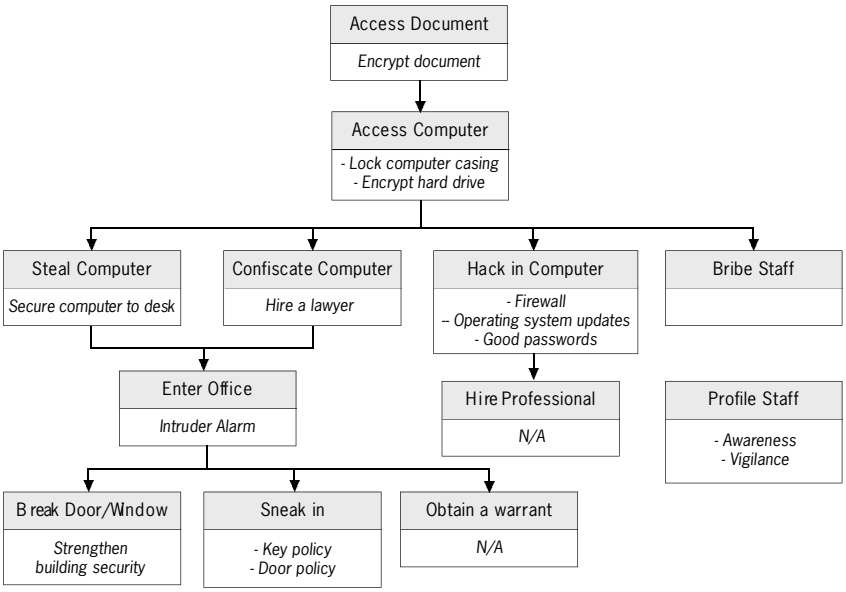
1 Write a list of possible threats to the security of your information.
2 Try to foresee and take necessary measures to prevent security threats from being realised.
3 React to incidents swiftly and investigate the causes.
4 When reacting to a security incident, assume the worst possible scenario and take relevant measures.
5 Approach security from an all-round perspective. Eliminate the weak links in your strategy and do not compromise the people who you work or communicate with by being careless about security
6 Lay out your findings in a diagram. This will allow you and your colleagues to grasp the big picture more quickly.
7 Concentrate on the weakest point in your security strategy

To decide what security precautions to take, you need to have a fair idea of the threats you face. These include threats to the security of self, staff, reputation, information and financial stability. All these factors can be compromised in one way or another by electronic insecurity. Since everyone's situation is different, I will only provide a few broad examples to highlight the general idea of modelling the threat.

The diagram is written from top to bottom. At the top level, we describe what it is we want to protect. The threat is the ability to compromise this. As you go down one level, you are listing the different insecurities that can occur – the threats to the protection of the upper level. The first example models the threat of someone accessing a document on your computer.

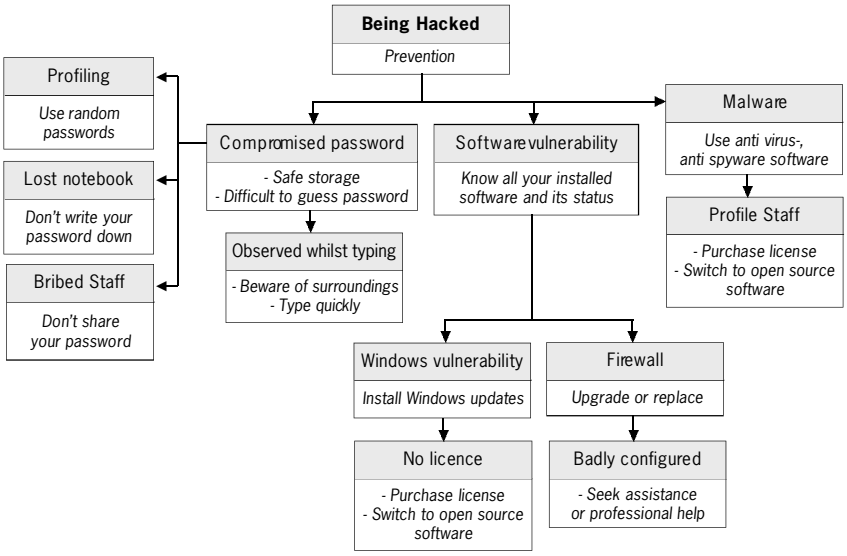


At the top level, write the threat that you want to prevent. In this case, to access the document, one will need to have access to the computer first. Access to the computer can be obtained by theft, confiscation, hacking orbribing one of your colleagues, and so on. You can choose how many levels down you want to take the model, depending on what is useful.

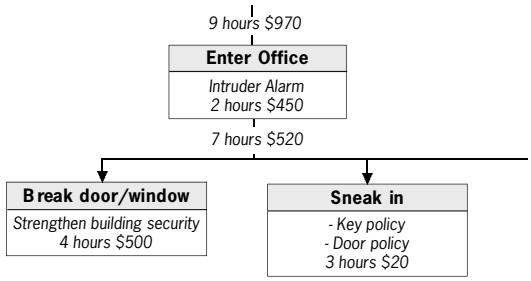


Now, working from down up, fill in the empty parts of the threat boxes with something that will remove or reduce the particular threat. Some of the threats you may not be able to change (like the police obtaining a warrant to enter your premises) but the majority of them you can influence. Work upwards until you have reached the top again.

At this point, you can make a decision as to which of the threats you are willing and capable of defending yourself against. Perhaps you can develop and introduce certain policies and safeguards within your organisation to further reduce the level of threat. You can study methods in this manual on how to protect yourself from hacking and spend some money on securing the entrance points to your office.



You can continue to develop your model by adding a cost or a time dependency limit to each box in the tree. Upper boxes will have the totals of all boxes beneath them. Such methods can help you with deciding budgets or resources to allocate for preventing a possible threat from occurring.



You can also evaluate individual threats from the diagram above. For example, to assess the threat of your computer being hacked (an outsider gaining electronic access to your computer) use the diagram below.
At first, it is perhaps difficult to realise all the threats you may be facing, especially in the digital domain. The knowledge will come with further research into the specific areas of electronic security. After studying this manual, your understanding of some technology-related threats should increase. It will then be advisable to detect the sensitive areas of your work and assess the threats you face. Although this may seem like mapping out rational decisions one would take anyway, the process can help you realise and deal with numerous factors that contribute to your insecurity, and prevent accidental mistakes.

Prevention

As opposed to threats encountered in the physical world, digital threats are sometimes difficult to notice and hence to prevent. The tendency is to be reactive rather than proactive with electronic attacks: the latter, more often than not, proves ineffective. A firewall must be installed before you are hacked, a virus cleaner must be updated before you lose documents due to a new virus infection. To deal properly with the possibility of a digital attack, one has to be extremely vigilant and paranoid. The threat model needs to be assumed at the very beginning. The worst case scenario must be understood and dealt with before it happens. The speed of computer and Internet operations means that security barriers are bypassed in a split second. Microsoft is of the opinion that 70% of Windows users do not have any anti-virus or anti-spyware software installed[9]. The reason for this is not the cost – there are several free anti-virus, spyware and firewall tools (also available on the *NGO in a Box* CD) – but complacency[10]. Don't wait until tomorrow to update your operating system, don't wait until you get a virus warning to update your anti-virus software, don't wait until your computer is confiscated or damaged before running the necessary tools to delete or backup your data. Be proactive!

Reaction

If your computer, password or network security has been compromised, you must assume the worst and take the necessary measures. If a virus has been found on your computer, disconnect it from the Internet. Run a full scan of your entire system and quarantine any virus that has been found.

9
BBC Online - http://news.bbc.co.uk/1/hi/technology/4694224.stm

10
See 'Malicious software and Spam' chapter for the difference between viruses and spyware

11
The event viewer can be launched by going to `'Start' > Settings > Control Panel > Administrator functions > Event Viewer`. This option is only available to users of Windows NT, 2000, XP. Look out for fault signals indicated by a red exclamation or yellow warning sign.

12
Available with the *Secure NGO in a Box* or http://www.markusjansson.net/

When you no longer get any warning messages, re-connect to the Internet and update your anti-virus definitions and Windows operating system files and do a search for the virus name to see what is known about it on the Internet. You could find information about the damage the virus causes and how to eradicate it properly from your system. Here's a guide to some common examples of computer malfunctions and suggested reactions to them. The methods used are taken from topics discussed throughout this manual and the tools - from the *NGO in a Box – Security Edition* project.

Incident	**Primary reaction**	**Method** (using this manual & NGO in a Box Security Edition)	**Follow up**
Virus attack	- disconnect from the Internet & run full system scan - update all virus definitions and operating system - run full system scan again	- run 'boot scan' on Avast anti-virus or full scan with AntiVir - update Avast (or AntiVir) - run another boot scan with Avast or full scan with AntiVir	- research virus on the Internet - retrace to the moment of infection - scan all backup and removable devices - recover virus-affected settings
Spyware attack	- disconnect from the Internet & run full system scan - update anti-spyware definitions	- run full system scan with Spybot - update Spybot - immunise computer against new spyware definitions	- research spyware on Internet - change all system and Internet passwords - change to using Firefox or Opera browser (if using Internet Explorer before)
Document corruption	- recover document from backup - search the temporary folders for recently modified documents (see 'Windows security' chapter)	- browse through your previously made 'Freebyte' or 'Abakt' archive - see chapter on 'Windows Security ' for tips on searching your computer - use 'Handy Recovery' program to analyse the computer	- find the cause of computer, document crash - update computer settings - update backup and backup procedure
Slow computer operation	- verify you have enough space on hard drive - uninstall unnecessary or recently installed programs - In Windows (NT,2000, Me, XP), check the 'event viewer' to see list of symptoms[11] - Check for viruses, spyware	- use 'BCWipe' to delete temporary files on computer - use 'Registry FirstAid' to scan and clean the Windows registry	- Disable Windows services (see Johansson's guide[12]) - Purchase more RAM - Call in a technician
Your access to a website is blocked	- Find out if others can access the website, ask friends from a different country	- see appendix B 'Internet explained' & 'Circumvention of Internet censorship and filtering' chapter - install 'Mozilla Firefox' and 'switchproxy' - install 'Tor' or run 'Torpark'	- use a proxy server or anonymity network - use a translation website that can fetch the website content
Your website is blocked	- Call the Internet provider to query the blockage - Move your website to a different host or domain name	- see appendix B 'Internet explained' & 'Circumvention of Internet censorship and filtering' chapter - use 'Httrack' (OpenCD) or 'SmartFTP' to mirror your website on a different server	- inform network of contacts about site block - Host website on several computers by mirroring. Ask friends and contacts to mirror your website - Query the reasons for blocking your website and develop strategy of appeal or compliance

Incident	Primary reaction	**Method** (using this manual & NGO in a Box Security Edition)	Follow up
Email does not arrive to recipient	- send email from a different account to recipient (also webmail) - do a trace route to recipient's domain. (see 'Internet Explained' appendix) - verify the email address is correct	- see appendix B 'Internet explained' - see **Encryption** on Internet section in 'Cryptology' chapter - use 'Soft Perfect Network Scanner' - use 'Hushmail'	- clean your computer of malware and install, update firewall. - begin using different email accounts (that offer higher security) - communicate over a different medium (online chat, website forum, telephone
Warning of a raid	- do a threat assessment - protect sensitive information - wipe sensitive information - make backup of information	- Review security policies - use 'Eraser' to wipe data - use 'Truecrypt' and 'Freebyte' to backup data to a secure location - use 'DeepBurner' to backup to CD or DVD disks	- introduce security policy in office - strengthen office security - ensure a safe backup off-site - develop system for quickly destroying data on computer
Receiving unwanted email (e.g. SPAM)	- install spam filter or switch to using Thunderbird with built-in filter - block email addresses - run virus and spyware scan	- use 'Mozilla Thunderbird' and read NGO in a Box SE chapter on setting the junk mail filter - use 'Avast' or 'AntiVir' and 'Spybot'	- change email address - develop a vigilant policy on publishing information with your email address - register additional email addresses that you use to sign up to services on the Internet

Note: All tools and methods listed in the table below can be implemented with the *NGO in a Box – Security Edition* tool kit, that can be ordered from Front Line or found at http://security.ngoinabox.org

Description of the 'security circle' – all round security

Your security is only as strong as its weakest point. There is not much sense in buying a strong metal door for your office, if you have no idea of how many copies of keys there exist to it. Your court case defending a victim of a human rights violation may not be successful, if your facts are not correct. You must always evaluate the entire scope of your security situation and be ready to notice and deal with all weak points, as it is often those that undermine the whole security process. This also applies to electronic security. Spending money on an expensive firewall will not prevent your computer from physical damage or theft. Implementing an encrypted mail system will not have much effect on your project's communication strategy, if other members of the project do not implement the same. We must approach our security from the perspective of a closed circle. All elements must support each other and weak links must be treated with the utmost care[13]. Let's have a look at the process of establishing a secure office.

—

You can probably imagine how a lapse in one area of this circle can lead to a collapse of the entire system. It can of course be slightly more complicated: the alarm system and safe will have a secret combination to open or disarm them. Whoever knows this combination will be able to compromise this system. The 'trustworthy staff' component can, unfortunately, also be a misnomer at times. A little security is still better then no security at all. Do not be daunted by the difficult scenarios described in this chapter. Be a little

13
There is another approach to a security system and that is defence in depth. While security is commonly only as strong as the weakest link, where possible it should be designed with independent, redundant protections so that one may fail without the entire chain failing. Example: if your computer is infected by a virus, you will be able to restore the lost files from a backup.

paranoid and take extra care in your computer operations. Learn more about the technology you are using and the relevant legislation in your country. It is better to have a long password that a short one, to use **encryption** than not to use it. But do not rely too much on electronic security without becoming aware of all the complexities first.

2.1 WINDOWS SECURITY

ABSTRACT

1 Regularly update your operating system
2 Know the locations of different files and documents on your computer
3 Use a BIOS password to protect the computer at start up
4 Use a lock screen function or password-protected screen saver to prevent immediate access to your computer
5 Do not use an empty password or reveal your password to others
6 Be careful when installing new software or buying a computer with pre-installed software. Use only the software that is necessary for your function and delete everything else.

We have discussed the security of your working environment and the importance of awareness of your computer operations. This chapter introduces a more technical aspect. The stability of your computer's operating system is integral to its operation. Different software and hardware could have a negative impact on its functionality and security, if you do not possess the ability to monitor and control it. Your operating system gives you the opportunity to increase (or decrease) the security of your computer by adjusting various settings. It is like your computer headquarters. Whilst security does not depend solely on the operating system, it is important to know the vulnerabilities and the critical administration points of your operating system.

—

The Windows operating system (OS) is well-known for its many security vulnerabilities, but if you do not change to a different OS (e.g. a distribution of Linux), you should at least be aware of the best methodology for securing what you have. This section is divided into different categories and sorted by versions of the Windows OS. It is worth noting that specific versions of Windows, like XP Professional have numerous security features, yet they are not switched on by default. You have to activate them yourself.

UPDATES

Windows updates are additions to the OS which were not included in the initial release. They are usually upgrades and patches to resolve discovered vulnerabilities. The large releases are called service packs. Microsoft has stopped releasing these updates for Windows 95, 98 and NT. You can find and download all the updates from the previous years, but you will not receive the continuous support. The Security updates and fixes for Windows 2000 and XP will run through to June 2010.
(see http://support.microsoft.com/lifecycle/).

—

If you do not have Internet access, you are less vulnerable to many of the electronic attacks. It is still advisable that you find upgrades for your OS on disk or CD. You can always write or email to Microsoft and request the latest service pack (bear in mind that you will need to include licence details of your original product).

If you are connected to the Internet, you can visit http://update.microsoft.com and follow the process on the website to discover your current Windows version and updates, and to install all the necessary ones. If you are running Windows XP on your computer, then the website will first check that your Windows software licence is valid. Even if your Internet connection is slow and expensive, I would strongly advise you to install these updates. If Internet connectivity is an issue, I suggest you install just the 'Critical Updates'.

—

You can also obtain all updates for any operating system by going to the Microsoft Catalogue website[14] and downloading the required files. This is a useful option to share Windows updates amongst many computers, without having to connect everyone to the Internet. The Microsoft Catalogue has updates for all versions of its operating system and does not check the licence validity of your product.

—

Users of Windows ME, 2000 & XP, who have a constant connection to the Internet, can specify Windows to periodically check for updates and install them upon their release. Go to the **Control Panel** and select (in 2000 - `Automatic Updates`, in XP – `Security Centre`). Choose the options that will automatically download and install the updates.

FILE ALLOCATIONS

This section describes some of the locations used by Windows to store specific user and temporary files on your computer. These are important for deciding what files to delete, detecting system intrusion and keeping a well-organised and secure file system.

User Documents

These files relate to the `My Documents` folder where many users store their personal files. Also this category collects information that is unique to your Windows profile. Since Windows gives you the opportunity of a number of users for the same computer, it keeps all the files particular to a user's session in one location. This includes your Internet browsing history and favourites, cookies, desktop files and your specific program settings (e.g. all your emails from Outlook)

Windows 95, 98, ME

The default (first) users will have their personal files stored in the following locations:

Documents `C:\My Documents`
Desktop files – `C:\Windows\Desktop`
Program specific settings – `C:\Windows\Application Data`
Internet favourites – `C:\Windows\Favourites`
Internet history – `C:\Windows\History`

All additional users (you can add them from `Control Panel > User Accounts`) will have their personal files located at `C:\Windows\Profiles\User`

There is not much security built into this system, as any user can have full access to all files of others.

14
http://v4.windowsupdate.microsoft.com/catalog/
Windows 95 users should go to http://www.microsoft.com/windows95/

Windows NT, 2000, XP
Windows has a dedicated user profile folder structure. User files and settings can be found in

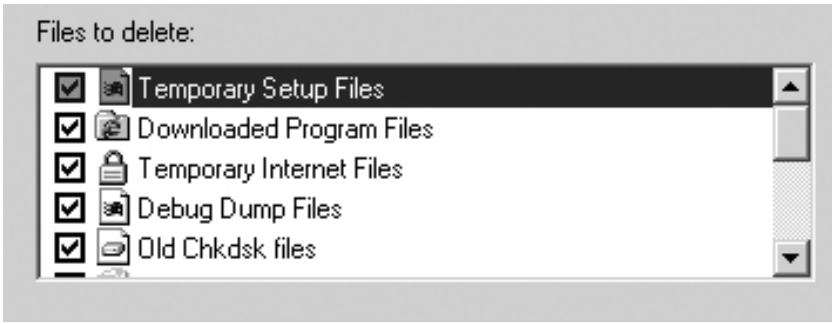
```
C:\Documents and Settings\User
```

Depending on the permissions granted to the user, they normally cannot see other users' files. There is an exception for an Administrator account, which should have access to all files on a computer. You should not be using an Administrator account or an account with administrator's permissions.

Temporary files

These are files collected by a computer as you go on about your work. They include unfinished or unsaved documents, Internet pictures and graphics (also known as cache) and a myriad of other files, which reveal your past activities on the computer. You should delete the contents of these folders periodically. To do this, go to:

```
Start > Programs > Accessories > System Tools > Disk Clean Up
```



► Microsoft Windows – cleaning temporary files

Select which temporary files you want to delete. For a secure, unrecoverable deletion of temporary files, use the BCwipe software utility (see *NGO in a Box – Security Edition*). It is also useful to delete these temporary files as they take up a lot of space on your computer.
For a thorough clean-up of temporary files with more options, use software like BCWipe and CCleaner.[15]

Lock Screens

Every Windows computer gives you an option to password-protect immediate access once the computer has powered on. This could either be a lock screen, or a password-protected screen saver.

►Lock Screen – **Windows NT, 2000**

Make sure that your user account is password-enabled.

```
Press the CRTL + ALT + DEL key simultaneously
Press: Enter
```

►Lock Screen – **Windows XP**

Option 1 Press the `Windows key` (if you have one) + `L` 

Option 2 You must switch to the 'Classic' Windows theme to activate the lock screen function.

15
These tools can be found in the *NGO in a Box – Security edition*, and on the website http://security.ngoinabox.org

Select: Start > Settings > Control Panel
Double click: User Accounts
Click: Change the way users log on or off
Untick: Use the Welcome Screen

Now you can use the Ctrl + Alt + Del key combination.

Option 3 Right-click on an empty space on your Desktop
Select: New > Short cut
Type: rundll32.exe user32.dll, LockWorkStation
Press: Next
Type: a name for the new icon (example: Lock Computer)
Press: OK

This will create an icon on your desktop. Double-click it to lock your computer screen. You will need to enter your password to unlock it.

Windows 95, 98, ME
Unfortunately, there is no separate lock-screen function in these Windows versions, so you will need to create a password-protected screen saver and put an icon or a time limit to activate it.

Screen Saver – (all Windows versions)

On your Desktop, right-click the mouse button and choose Properties from the menu that appears. Go to the SCREEN SAVER tab and select a screen saver. Tick the Password Protect box and enter the desired password. Set the time limit to 5 minutes. Now make a shortcut to activate the screen saver upon request. Then you won't have to wait for 5 minutes before it is launched.

Go to: Start > Search (for files & folders)
Type: *.scr
Press: Enter

The results will show up all the screensavers on your computer. Choose any screensaver and right-click on them.

Select: Send to -> Desktop (Create ShortCut)

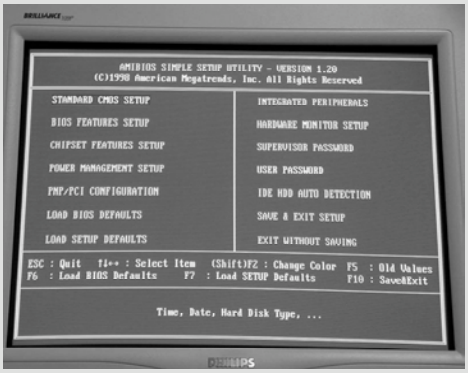
Now you can activate the screen saver by clicking on the shortcut on your desktop screen. However, we can make it even simpler:

Right-click on the shortcut and select Properties
Click in the textbox called short cut key and press Ctrl Alt S

Press: OK Now your screen saver will launch every time you press that key combination.

This is not an advanced security measure, yet it is still better then just leaving your computer open.

BIOS



Every computer has a **BIOS** – Basic Input/Output System. Its purpose is to give your computer initial instructions to begin with. **BIOS** is a set of essential software routines that execute when you switch on the computer's power. They test the hardware devices, start the hard drive and operating system. The **BIOS** instructions are stored in a place called ROM – Read Only Memory, and are usually invisible to the user. However, most computers give you the option to inspect and configure the **BIOS** settings. These include password protection.

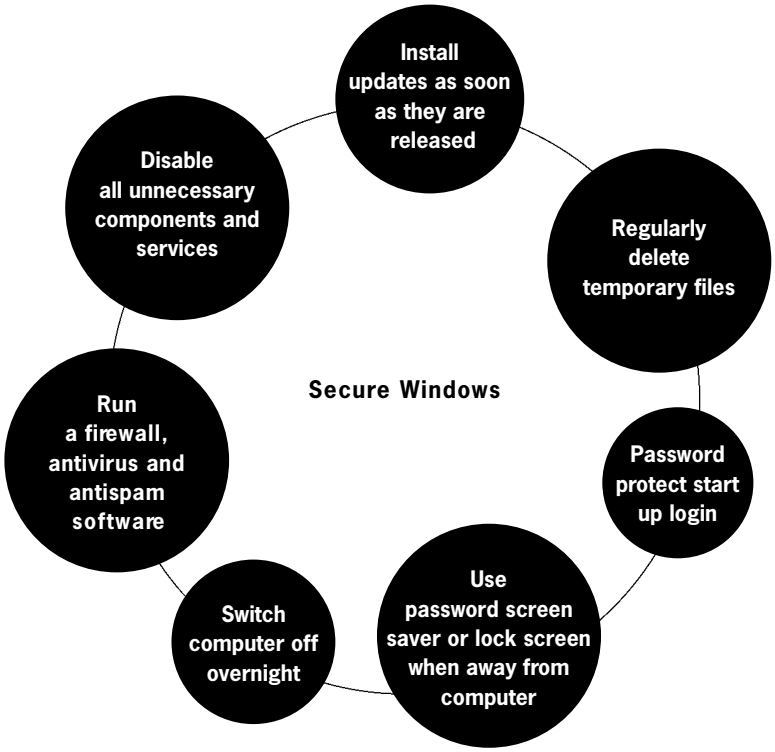
—

To enter the computer's **BIOS**, you are usually requested to press a certain key on your keyboard at the initial power-on screen. This is often the F1 or F2 or F10 or F12 key, depending on the type of **BIOS** you have. Sometimes, this can also be the ESC or DEL key. Some computers skip through this screen very quickly and you may have to press the 'Pause' button on your keyboard to read it properly. We will only discuss the password settings here. Do not change other standard **BIOS** settings, if you do not know their purpose. Not all **BIOS** are the same, but you will find either two or all of these passwords in yours.

—

Power On password – This will protect the **BIOS** from starting without a valid password. No devices will be loaded, and your computer will not start.
Hard-drive password – This will protect the **BIOS** from initiating and launching your computer's hard drive. This is a useful option for your laptop that is often left in 'standby' mode.
Supervisor password (**BIOS** password) – This is the main password that can overwrite the previous two passwords. You do not need to set it, but if you forget or want to change either the power-on or hard-disk password, you will need the supervisor password.

Setting these passwords will prevent immediate access to your computer, if it is switched off. It is a quick deterrent for a less ambitious intruder. The security is far from foolproof as there are several ways to bypass the **BIOS** password. Almost all of them include physically opening your computer. When you have done this, you can reset the **BIOS** or simply take out the hard drive and put it into a different computer that does not have **BIOS** password protection. Hence, if you have a lock on your well-built and strong computer case, you are again increasing the security of access to your information. If you forget your **BIOS** password, you will have to resort to the methods described above to reset it.



SOFTWARE INSTALLATION

Most computers come pre-installed with software. At least, that is what you should normally request. Bear in mind that this may not be the best security option. If you have unlimited or cheap access to the Internet, all you will need is your Windows CD. You can find all other necessary software on the Internet and all of it free[16]. When I buy a new computer, the first thing I do is format it, i.e. delete everything on it, including the operating system itself. It allows to start 'afresh' and build my system from scratch. Pre-installed software usually has many trial versions of virus cleaners, graphics packages and what nots. Sometimes, it will have lots of pre-installed spyware. By starting from scratch, I can gain full knowledge of all of my Windows' security settings, installed software and hardware. If you implement the security settings for Windows included in the Secure NGO in a Box, update it from the Internet, install a virus cleaner and a firewall, you will be a lot more secure when connecting to the Internet for the first time[17].

When installing new software, imagine yourself eating. You could poison yourself, if you consume the wrong food or a products that is past its use-by date. With software, you could poison your computer that sometimes will not recover. Investigate the software publishers and make a decision about their status and trustworthiness. Like keeping a healthy diet by staying away from junk food, do not install unnecessary software that may decorate your computer monitor or make filling in Internet forms easier. It is usually this very software that carries many of the bugs we describe in this Manual. Do not think that a computer can handle every piece of software you choose to install. If all you need a computer for is checking email and writing documents, all you will require are OpenOffice and Mozilla Thunderbird. Don't install anything else. It's that simple.

16
You could also order a free copy from the *NGO in a Box* range of CDs (including Security, Base, Audio/Visual) – see www.tacticaltech.org for more details

17
See the Markus Johansson Guide on installing Windows 2000/XP on the *Secure NGO in a Box* project CD

2.2 PASSWORD PROTECTION

ABSTRACT

1 Don't rely on Windows passwords to protect your information. They are easily broken.
2 Create passwords which are 8 characters or longer (in a few years' time, we will be recommending 9!) You can also use a short sentence as your password.
3 It is better to write down you passwords and keep them safe, than to have a short, easy to guess password[18].
4 Use numbers, small letters, capitals and symbols in your password.
5 Never use the same password twice
6 Do not use passwords which can be directly related or linked to your personal life or interests.
7 Do not share or tell anyone your important passwords.
8 Change your passwords every 3-6 months.
9 Remember that there are many programs available free on the Internet, which will identify your Windows password, wireless network encryption and just about any other type of computer password you may have.

Having good passwords is an essential part of using computers. They act as a security barrier providing authentication to the required service, be it an email account, network login or online banking. A password is like a key to a door. You may have several different keys for your home, your office, your car and your safe. None of the locks are the same, and you have a collection of different keys to open them. This makes breaking in more difficult. Even if the thief manages to find one corresponding key, they will not be able to open all other doors. Our door locks are getting more sophisticated and expensive. They are made of many different components with the sole purpose of preventing break-ins. The same should apply to your passwords. They are a door lock to your information banks. The advent of computers has seen passwords protecting the information that is often of a greater value than whatever is stored in your cupboard or safe. Therefore, in a technical sense, your passwords should be as strong as the most expensive safe to protect the information they guard.

—

In the world of digital security, a good password is the most essential and important element of any system. History has shown that breaking passwords is the most common method for hackers and intruders to attack your information systems.

CRACKING PASSWORDS

How do passwords get compromised? There are several methods of doing this. One is to observe someone typing their password from a distance. Another - to install a spyware program that would record all the keystrokes typed into the computer and transmit them to the attacker. Both of these

18
See the article from the Bruce Schneier's blog http://www.schneier.com/blog/archives/2005/06/write_down_your.html. Bruce is also the programmer of the PasswordSafe program (http://passwordsafe.sourceforge.net), an excellent utility that allows you to store passwords securely. It is mentioned later on in this chapter

can be prevented by vigilant behaviour. Make sure you notice your surroundings and always run frequently updated anti-spyware and anti-virus software.

Profiling

Profiling involves making an educated guess by collecting personal information and facts about the person who owns the password. In many cases, our passwords reflect something which is easy for us to remember - year of birth, name of a family member or a friend, town of birth, favourite football team, etc. The profilers take notice of these and other similar facts. If they have access to your office, they may also spot the books on your bookshelf. The naming system for your passwords is excusable (at least, until you finish reading this chapter!) since the ability to remember many different passwords that have no association with you and are difficult to memorise is limited. However, guessing a password by possessing personal information about the user is still the most common method of compromising a system that continues to be extremely successful for motivated hackers.

—

Many password systems on the Internet give you the option of recovering your password, provided you answer a previously set 'secret question'. For some unexplained reason, these secret questions (which you set when creating an account) invariably have something to do with the name of your pet, your first school or your mother's maiden name. This makes the profiler's job extremely easy. They will not even have to work out what your password is, but will simply answer the secret question and receive your password in an email. If you are ever asked to set up a recovery mechanism in the form of answering a simple question about your personal life, do not use it. If it is a requirement for completing the registration process, just write something unintelligible. Don't rely on the secret question recovery process to remember a password you have forgotten.

► Personal passwords are easily guessed

Social Engineering

Many people have been tricked into revealing their passwords through cleverly created scenarios and questions. It can happen in a phone call (supposedly) from your ISP saying that they are upgrading their servers and in order to make sure you do not lose any email in the process, they require your password. Someone could pose as a colleague from another branch of your NGO and request the password to access the shared email account, as the person who knows it is currently ill and they need to send something urgently. This is known as social engineering. There have been numerous cases of employees revealing potentially damaging information simply because they were tricked into it. It remains an effective method for hackers to try to gain access to a system.
No one should never reveal any computer related information (especially passwords and access codes) on the phone or to someone whose identity they cannot verify[19].

19
Good advice from Steven Murdoch, a researcher in the Security Group of the University of Cambridge: is to verify the person's name and affiliation, then look up their phone number in a trustworthy directory and call them back

Brute Force

Brute force is the practice of guessing a password by using all sorts of possible combinations. This could involve taking an electronic version of a dictionary and trying every word in it. It may seem a lengthy task for a human, but for a computer it takes only seconds. If your password is a properly spelt word from a dictionary, it can be compromised within minutes by a brute force attack.

Perhaps you have used the opening lines from one of a 1000 most famous songs or poems as your password? The digital world is ever expanding and growing as the the whole of world literature and thought is being transferred onto it. There exist electronic compilations of the works of literature, and these can also be used to break your password. You should think twice before using a natural language password – a intelligible or a famous phrase, a combination of words or a complete sentence.

—

Some password systems are protected against brute force attacks. Take a bank machine or a mobile phone as an example. Even though your password is usually a simple combination of four digits, the system will shut down (take your card, lock your phone) after three incorrect guesses.

CREATING PASSWORDS

Mnemonics

There exist various methods for creating passwords which are difficult to break and easy for us to remember. A popular one is mnemonics (a method or system for improving the memory, such as a rhyme or acronym[20]). Lets take a common phrase:

To be or not to be? That is the question (Hamlet, Shakespeare)

We can convert this to 2Bon2B?TitQ

In this example, we have substituted words with similar-sounding numbers and acronyms, with nouns and verbs capitalised and prefixes appearing in small-case letters. Or, for instance:

I had a dream, where all men were born equal (Martin Luther King)
1haDwaMwB=

This appears to be a relatively random password and not so difficult for you to remember as you know the trick of how it was made up. Other tips include substituting numbers for similar-looking letters, abbreviating words that resemble numbers and using emoticons.

I, i, l, t = 1 o,O = 0 s, S = 5,2 four, for, fore = 4 two, to, too = 2

Are you happy today? = rU:-)2d?

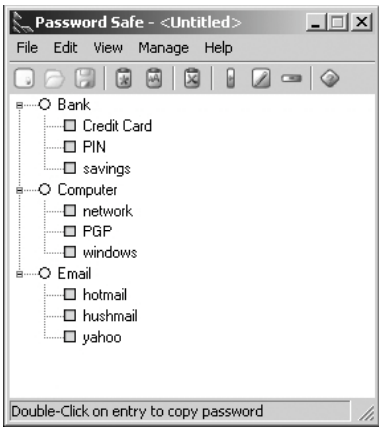
These are but basic examples, and you can always create your own method of coding numbers and words. It is advisable that you do so.

Note: Please do not use the examples shown above as your password!

20 *WordNet* by David Slomin and Randee Tengi

Using software

The next step towards improving your password complexity, is to use a password generation program[21]. This will create a random password and will store it securely. With the password generation program, you will be able to use extremely complicated passwords and will never have to remember them! It is the ideal solution. The password programs are generally very small and can be carried around on a floppy disc or a USB memory stick.

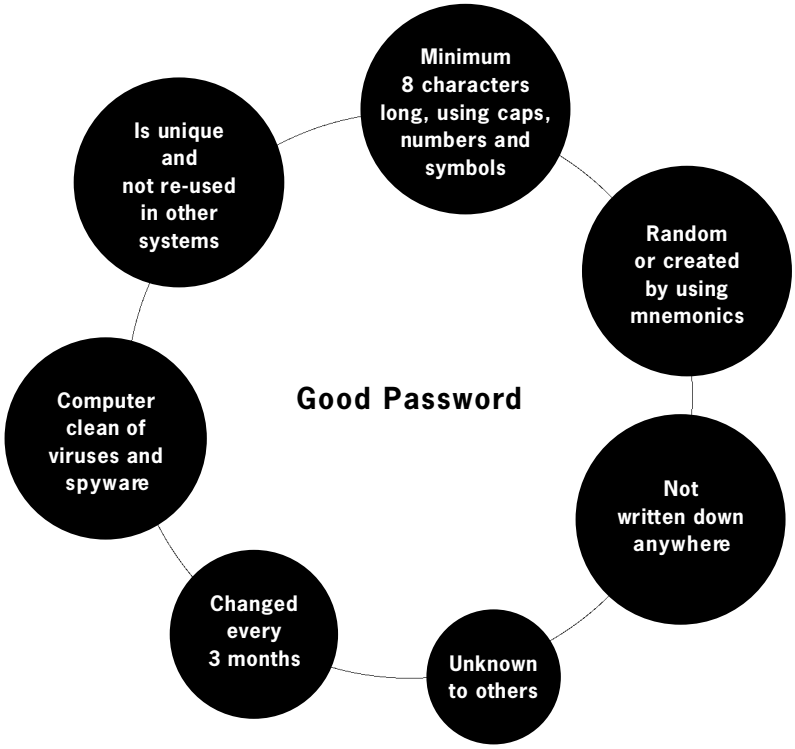


► A screenshot from the PasswordSafe program

You can group your passwords into categories and copy them from the program to the screen by using the clipboard. The passwords are stored encrypted in the program and have to be unlocked by you. Hence, the only password you will need to remember is the one to access the program itself.

It will take you a little while to begin creating and storing all passwords in such a program, but the benefits of security hugely outweigh the little of inconvenience of doing so.

Your password is often the first and most important guarantee of the security of your information. It is like a door to the house where you live. Using a bad password or no password at all, is like leaving the door open all night. Maybe, no one will walk in, or, maybe, someone will and steal all your belongings. Pay great attention to how you create your passwords and where you keep them.

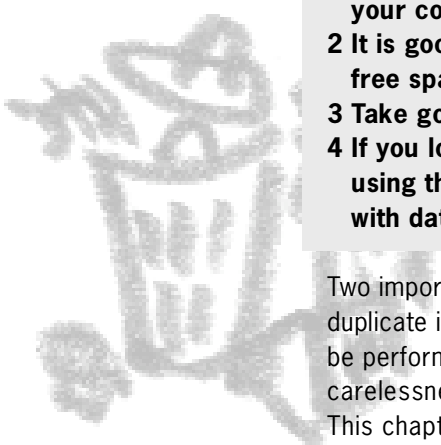


21 See programs PasswordSafe (http://passwordsafe.scoureforge.net) and Keypass (http://keypass.scourceforge.net), also available on *the NGO in a Box – Security Edition* CD.

2.3 INFORMATION BACKUP, DESTRUCTION AND RECOVERY

ABSTRACT

1 A backup strategy should include: the files to be archived, the frequency of updating the archive, location and storage of the archive.
Simply deleting data from your computer is not sufficient to make it unrecoverable. Sensitive information needs to be wiped from your computer.
2 It is good practice to wipe temporary files, Internet cache and free space on your computer.
3 Take good care of your computer's physical environment
4 If you lose a document, do a thorough search of your computer using the Windows search function and analyse your hard disk with data recovery software.



Two important issues to consider when working with information are how to duplicate it and how to destroy it. Computers allow these two processes to be performed quickly and efficiently, and it is, once again, human error and carelessness that are the commonest causes of malfunction of systems. This chapter will explore the theory behind replicating your computer-held information, restoring lost data and erasing unnecessary or sensitive information without the possibility of recovery. It will also describe good practice in this area.

INFORMATION BACKUP

Important documents are usually duplicated. *The American Declaration of Independence* was originally produced in 251 copes. People make photocopies of their passports, tax returns and driving licences. Manuscripts are copied before being sent to the publisher. These are all precautions against the loss of documents and information in them. Computers make duplication a very easy and rapid procedure. Numerous programs will create an identical copy of the original information base and store it in the location of your preference. Gone are the days when the loss of your little address book resulted in painstaking search for the forgotten phone numbers, and that, as you will see, is both a blessing and a curse.

—

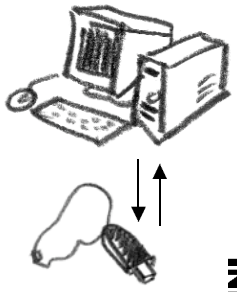
The need to create a backup copy of your computer files is often superseded by the belief that 'nothing will go wrong'. We rely on ourselves and our computers not to forget, lose or damage the information.

—

Information loss occurs on a micro and macro levels. You can lose just one document through a program malfunction or a virus. You can also lose the entire contents of your computer through a hardware malfunction or a malicious damage. Always have a backup strategy for all scenarios.

Backup strategies

Consider the type, quantity and frequency of backup for your information. You may wish to carry around a USB memory stick with a copy of all your documents. If your computer has a CD-writer, you can backup a lot of documents, photos and audio files on a weekly basis and keep a copy at a separate location. If you have a server computer in your office, it requires a periodic backup not only of the documents users store on it, but also of the software and system settings.



Frequent access files

This file type refers to the working documents you need to have access to at all times. These files are constantly updated and you need to have the latest version available.

—

The most applicable device here would be a USB memory stick. It is small, has no moving parts (therefore less prone to damage than a floppy disk) and usually provides sufficient storage space for many documents. You should be able to synchronise the content of a folder on your home/office computer to the USB memory stick[22].

► Backup frequency: daily.

Non-frequent access files

This is a collection of your entire document archive, built up over time. Files are infrequently created and updated. It may not be necessary to keep the latest versions of every file, but a backup is still essential.

—

The most efficient device to use as a backup medium in this scenario would be a re-writeable CD-ROM drive (CD-RW). It will allow for up to 800MB of storage space and you can overwrite the previous archive with the current one, only having to look after one or two CDs at a time[23].

► Backup frequency: weekly.

SYSTEM FOR TECHIES

To prevent a long process of restoration in the event of a computer crash or malfunction, you should periodically make a copy (image) of your entire computer. This is an advanced option, probably suited for your systems administrator or someone who looks after your computer. A system backup includes all the installed programs (and their licences), system registry, **device drivers**, etc. It could take days, sometimes even weeks, and cost a lot of money to restore your computer.

—

One way to perform this backup would be with a tape drive. These are quite expensive and usually do not come as standard with your computer purchase. The other option is to buy a removable hard drive and perform the backup onto it. A full system backup usually requires specialised software, known as disk imaging. It can be also done by using the Windows built-in backup functionality that you can access by going to Start > Programs > Accessories > System Tools > Backup. In case of fire or other

22
Use a program like Allwaysync (http://www.allwaysync.com) to perform synchronisation

23
Use a combination of the archiving program Freebyte (http://www.freebyte.com) and a CD burning program DeepBurner Pro (http://www.deepburner.com). Both can be found on the *NGO in a Box – Security Edition* CD

disaster, it is essential to keep a copy of the system backup away from the computer premises.

►Backup frequency: monthly.

For the sake of security, do not create too many backup copies. If you cannot overwrite a CD on a weekly basis, make sure you properly destroy the outdated versions. This way, your backup files would be harder for an attacker to find, and you won't get confused as to which CD contains the latest copy of your documents.

INFORMATION DESTRUCTION

It is virtually impossible to completely erase all information stored on your computer without resorting to cutting, burning or breaking into tiny pieces the data- carrying device. Whilst you may think that Windows has emptied your 'Recycle Bin', this is not true. We must take necessary precautions to make sure that the data no longer wanted on our machines is properly deleted.

Between 2000 and 2002, researchers Simson Garfinkel and Abhi Shelat of MIT purchased a large number of second-hand hard disks from various dealers through the online auction house eBay and examined these for any residual information they contained. They found an alarming quantity of data, for example:
- internal company memos relating to personnel
- lots of credit card numbers
- medical information
- e-mails
and many-many more.[24]

Data recovery is a growing industry, and many firms and government agencies have become incredibly advanced at salvaging lost and damaged data. Another element of our information security is the need for human rights organisations not only to keep sensitive information safe, but to destroy it properly as well. This section will examine the process of permanently deleting unwanted information from your computer.

Data deletion

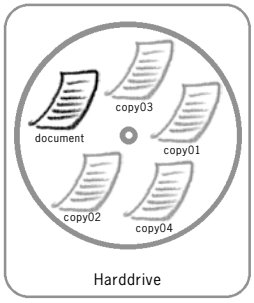
There is no computer function that can delete information. Strictly speaking, computers can only write new information to the hard drive. When you choose to delete a file in Windows, you are simply telling the computer that this space is now available to be overwritten with new data (we will call it unallocated space). Windows removes the file icon and the name reference from your screen, thereby making you believe the file is no longer there. It does not remove the actual data from the hard drive. You can compare this to removing the label from a filing cabinet, but leaving the files still in the drawer. Until you have overwritten the exact physical space on the hard drive with new data, the information is still there and is easily visible with the help of simple software.

—

Let's imagine that you are writing a large report. It takes you a week of work, several hours each day. Every time you press 'save' before shutting

24
Remembrance of Data Passed: A Study of Disk Sanitization Practices, Published in IEEE Security & Privacy, vol. 1, no. 1, 2003 By Simson L. Garfinkel and Abhi Shelat, Massachusetts Institute of Technology

down your computer and leaving for the day, Windows creates a different copy of this document and stores it on the hard drive. After a week of editing, you will have several versions at different stages of completion on your hard drive. Windows does not look for the exact physical location of the original file and overwrite it every time. It simply puts the latest version in unallocated space on your hard drive. This can, of course, lead to problems when you need to erase all traces of this document from your computer.



►Multiple copies of your document are created every time you edit it

Removable Devices

It is not only hard drives that store our digital information. Floppy disks, CDs and USB memory sticks are used frequently for file storage and movement between different computers. These are also susceptible to holding on to information that we have previously deleted. CDs have been known to contain recoverable information even after they were cut into pieces.

—

It seems that, apart from burning the device to ashes, the data can still be recovered. Some system administrators are given the task of destroying old company's hard drivers with a hammer. Others tried to erase the contents of CDs by putting them in a microwave for several seconds. There are, however, certain tools that can prevent the majority of intruders from retrieving our deleted information, without resorting to heavy machinery and kitchen appliances. These, mind you, do not make the recovery process totally impossible, yet in most cases they will make the task prohibitively expensive.

FOR TECHIES

Another Windows feature that - unbeknownst to you - stores your personal documents is the swap file (also known as paging file). Windows uses the swap file for the ease of operation. At its simplest, it is a part of the hard drive Windows assigns to itself to handle all your current operations. When you switch the computer off, the swap file retains all the information previously on it. Even if you are using **encryption** software, your files will not be stored encrypted in the swap file. It is advisable to disable this feature (you should have at least 256MB of RAM in your computer to replace the swap file's functionality) or to use a wiping tool to securely delete information on the swap file before shutting down the computer[25]. To disable the swap file on Windows 2000 and XP:

Select: `Start > Settings > Control Panel > System`
Click: `Advanced tab`
Click: `Performance`
Click: `Virtual memory (advanced > virtual memory for XP)`
De-select: `the swap file option or set it to '0'.`

If your computer is a laptop, disable the hibernation feature. It may take you 30 seconds but will greatly decrease the risks of access to information on your laptop.

Select: `Start > Settings > Control Panel > Power Options`
Click: `Hibernation tab`
De-select: `Enable Hibernate`

25
See wiping tools Eraser (http://www.heidi.ie/eraser) or BCWipe (http://www.jetico.com/bcwipe.htm) that can also be found on *the NGO in a Box – Security Edition* CD

Wiping

The non-violent solution to destroying old data on our hard drives is overwriting it with other random data. This method is known as wiping. You can wipe a single file (and all its previous instances) or you can wipe the 'empty' space on your hard drive. The latter action will find all presently unallocated space (or space not used by current files) and overwrite it with random data. Experts agree that at least one random pass is necessary to prevent recovery of your information. You must be aware that it is not only your documents that should be wiped, but also other files used by Windows and collected whilst you use the computer and browse the Internet. This should include your Windows swap file (if you haven't disabled it yet). Make sure to wipe the following file types from your computer (some wiping software will do this automatically for you – see footnote on previous page):

Temporary Windows files	Favourites
Temporary Internet files	Swap file
Internet log files	Temp files
Cookies	Recent documents
History	

Wiping guidelines

If you decided to erase all traces of previous and temporary files from your computer, you can perform the following steps, using one of the wiping software programs provided in the *NGO in a Box – Security Edition* project, or by sourcing it yourself.

- Make sure you have a backup of all your user documents, licence files and Windows registry.
- Close down all unnecessary programs and disconnect from the Internet.
- Wipe the temporary folders of all content
- Delete all unnecessary user files and empty the 'Recycle Bin'
- Wipe all the free space on your computer (could be done overnight)
- Get into the habit of wiping all the temporary files (and swap file) before shutting down your computer.
- Perform a free space wipe on your USB memory card or floppy disks.

Wiping software such as BCWipe and Eraser can integrate with Windows and allow you to wipe files or the 'Recycle Bin' with two simple mouse clicks. They can also wipe temporary files and free space on your computer or USB memory stick.

INFORMATION RECOVERY

Files that have not been wiped can be recovered. Some tools at our disposal can perform searches of our hard drive or other media device for lost, damaged or corrupted files. In the worst case, there are many organisations that have sophisticated techniques for recovering lost data. Simply search the Internet using the keywords 'Data Recovery'.

Prevention

Keeping your system from crashing and losing your documents will require a careful approach to its environment and stability. First of all, consider

physical damage. Do not drink or eat, or perform any number of other functions that could potentially cause physical damage around your computer space. Due to the complex nature of electric circuity, computers do not react well to water or magnets. Keep your computer away from the ground, lest heavy footsteps or jumping should shake it. Secure your computer from electricity surges either with stabilisers or with fused sockets. You may consider purchasing an alternate battery supply (UPS). It is best to ask an expert in a computer shop for a more detailed description of the above items and how they can prevent your computer from being damaged.

—

On the software side, apart from maintaining a backup procedure, make sure your operating system is properly installed and updated. The same applies to your virus cleaner and firewall. Keep in mind that every time you install a new piece of software you stand a slight risk of destabilising your system. Some software programs conflict with each other and could make your system unstable.

Recovery

As a first step, you should carefully search your computer for the missing/lost file. It may not be deleted, but simply misplaced by you or by a program error. You can use the Windows search function to search the entire hard drive(s) for the file name. Perform a search on all recently modified files (e.g. files modified in the last day). Sometimes, a program crash causes the file name to become corrupted and unrecognisable. The 'modified date' stamp (and size of file) could be your hint to recovering it.[26]

—

The Windows search function can be launched from

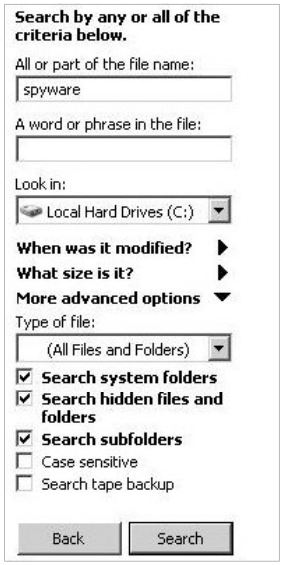
`Start Menu > Search > Files & Folders`

—

Next, you should set the criteria for the search including file name, size of document, date modified, etc. If your original document cannot be found by its name, you could look into automatically created 'temp' files, judging by the date the file was last accessed and its size.

—

Some software can recover lost files[27] by taking advantage of the inability of computers to delete data (as mentioned above). The recovery program performs an exhaustive search through all the hard drive sectors, looking for files and parts of files that are salvageable. If you cannot recover the necessary data with this technique, you may wish to consider paying for a professional service. These services have considerable skill in salvaging lost information, but they are expensive. Yet, most people only realise the value of their information once it has been lost.



► Microsoft Windows search screen

26
Also see Graham Mayor's guide on *What to do when Word crashes* http://www.gmayor.com/what_to_do_when_word_crashes.htm

27
Handy Recovery http://www.handyrecovery.com/ also available on the *NGO in a Box – Security Edition* CD; also see http://www.officerecovery.com/freeundelete/

2.4 CRYPTOLOGY

ABSTRACT

1 Encryption is the process of making your information inaccessible to all but the intended party. You can encrypt a message, an email or your entire computer
2 To communicate using encryption, we use the public key system. Our encryption method consists of a public and a private key. We share the public key with those who wish to communicate with us. They then encrypt a message to us using our public key.
3 The security of this system relies on the validity of the public key you are encrypting to, a virus and spyware free computer, and a good password, protecting your private key.
4 We can prevent unauthorised tampering with our email en-route to its destination by using digital signatures.
5 The level of security offered by encryption has led to its practice or theory (teaching) being outlawed in several countries.

HISTORY

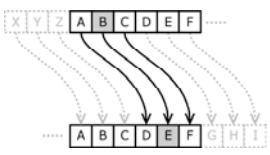
Cryptology is concerned with linguistic and mathematical techniques for securing information. The messages are coded to become unreadable to everyone but the intended recipient. Its long and colourful history goes back to around 5th century BC when the Spartans created the earliest known method of **encryption** using two identical wooden staffs and a piece of parchment. The parchment would be wrapped around the stick and the message written lengthwise. Unwrapped, the letters did not appear in any comprehensible order. The parchment was sent to the recipient, who had an identical staff to read the message on. Another early user of **cryptology** was Julius Caesar, the Roman emperor. His method of securing messages was to put two sets of the alphabet side by side and shift one of them by a specific number of places. He was known to use a 3-place shift when coding messages of military importance. Both of these methods remain in use today, and the latter is called the Caesar cipher. But the use of parchment and letter-shifting became obsolete in the complex world of computational mathematics in which our ever more powerful computers operate. Other methods to secure information from outsiders include linguistic **cryptology** (e.g. hieroglyphics) and steganography, which is the process of hiding the existence of the message itself.

Scytale
Source: Wikipedia.org
http://en.wikipedia.org/wiki/Cryptology

—

The message written on the parchment along the length of the stick (scytale). The scytale uses what is now known as a transpositional cipher, whereby you rearrange the order of letters in a message.

—



The Caesar cipher uses a method of substitution – where you are replacing a letter with one of a fixed position further down the alphabet.
The practice of breaking a cryptographic message is called cryptanalysis. It aims to find a weakness or insecurity in the method of cryptography. One famous example from 20th century was the Polish and British cryptanalyst's' breaking of the Nazi "Enigma" code. Churchill was of the opinion that it was

a turning point in WWII as the Enigma-code-encrypted communications were used by the Germans to navigate and direct their feared U-boats.
The security, provided by cryptography alone, should not be overestimated. Its fallibility is usually a result of human error or a bug in the overall security procedure. The use of cryptography has also been restricted by legislation. Civil society in the US fought for a long time to prevent the outlawing of public access to **cryptology**. Many countries that wish to access and control the flow of Internet communications have either restricted or banned the civilian use of cryptography altogether.

ENCRYPTION

Encryption (and its opposite – decryption) is a popular study in the field of **cryptology**. **Encryption** works by applying a large mathematical pattern to a set of data and coding it so that it appears incomprehensible to anyone who does not have the decryption method, otherwise known as the key.

Hard disk encryption

You can use **encryption** to protect your entire hard drive. You will in essence code every bit of information on it, so that only you, having entered a password, can access this data. All the sectors on your hard drive (the area where information is stored) will be encrypted. You still retain the free space on your hard drive to add additional files or programs, but as soon as you copy them to your computer, they are automatically encrypted. Whenever you extract the data from your computer (for example, to send an email attachment) they are automatically decrypted. If your computer is switched off and the attacker wishes to bypass its **BIOS** security (which you may have set after reading the Windows chapter) by physically removing the hard drive, the information on it will remain inaccessible as it will be encrypted[28].

—

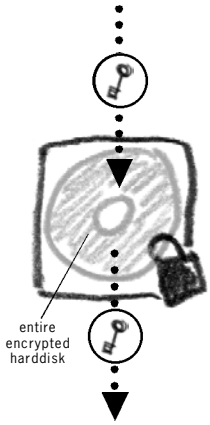
You can also create an encrypted partition. A partition is the computer's method to virtually dividing one hard disk into two or more (by "virtually" I mean that your computer will now see your hard disk as two separate ones). Physically there will only be one hard disk, but the computer will function as if there were several. If your computer has one disk (C:) with 5GB of free space, you can create another partition (D:) and allocate 1GB of space to it. This partition will be encrypted, and you can store your documents on it. The main C: partition will remain 'open' and will store your software and other files that are not sensitive. This is an excellent option for stable and secure operation of your computer[29].

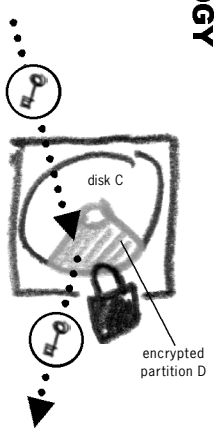
—

You can set your email program (e.g. Thunderbird) to store all files on the encrypted partition. Only you, or the bearer of your password, will be able to access the email on this partition.

—

You can also encrypt your entire USB memory card or other removable devices. This is very useful if you are constantly travelling and have all your documents on the memory card. Some software (True Crypt, CompuSec) can encrypt your USB card, so that you will not need the program to be installed on every computer you wish to use with the memory card.





28
An example of software that could encrypt your entire hard drive is CompuSec (http://www.ce-infosys.com) also available on the *NGO in a Box Security Edition* CD

29
An example of software that could create and encrypt a partition on your hard drive is TrueCrypt (http://www.truecrypt.org) also available on the *NGO in a Box Security Edition* CD

Public Key Encryption

Traditional methods of encrypting the information you wanted to share with another person required you to give them the password to decrypt it. This was not a very secure method, as it was possible to compromise your password in the process. To get around this problem, mathematicians developed public key **encryption** (PKE). It is the most common method of encrypting communications (e.g. Email) today.

—

When using PKE, your key will be made up of two parts: a public and a private key. Together they will make up your key pair. The keys are intertwined and what you encrypt with one, you can decrypt with the other. This is an integral part of PKE and a basis for its security and fallibility.

—

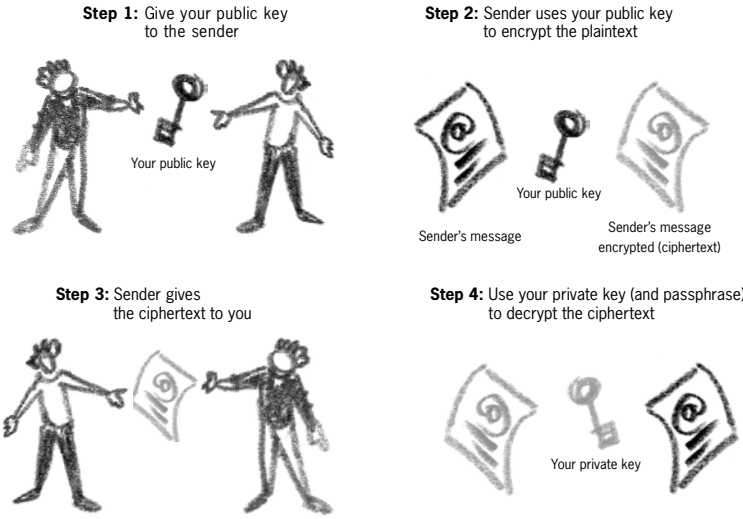
You share your public key with anyone you want to communicate with. You can also upload your public key to a key server on the Internet. The private key is kept secret on your computer or floppy disk and additionally protected with a password that only you should know. Do not share your private key with anyone. If you think that your password has become compromised (stolen) then you will need to revoke your key pair and recreate them from scratch.

Encrypting and decrypting a message[30]

In the PKE system, messages are encrypted for sending to us using our public key, and we decrypt them using our private key. People obtain your public key when they wish to send you an encrypted message by asking you for it or finding one you left previously on an Internet key server.

—

Example: You have a message that you wish to send to me encrypted. First, I must give you a copy of my public key. You use this public key to encrypt the message and send it back by email or other means. Only I will be able to decrypt this message since only I have the missing link – my private key.



Note that by "plaintext" we refer to the original message and "cipher text" refers to the message once it has been encrypted.

30
Suggested software with which you could perform PKE is GPG4Win (http://www.gpg4win.org) or by installing the GnuPG and GPGshell software from the *NGO in a Box – Security Edition* CD. It may help you replicate some of the examples in this chapter.

This facilitates communication of encrypted messages without having to share a password and dramatically increases the security and practicality of your communications. PKE has been applied to email, Internet chat, web browsing and many other Internet services. Its security has caused controversy with many governments. The level of privacy offered by the successful application of this system has made many surveillance and intelligence agencies very worried.

Key Security

The reliability of the **encryption** depends on :

- the size of your key pair (usually 2048 bits long)
- the ability to validate the recipient's public key
- protecting your password that unlocks the private key

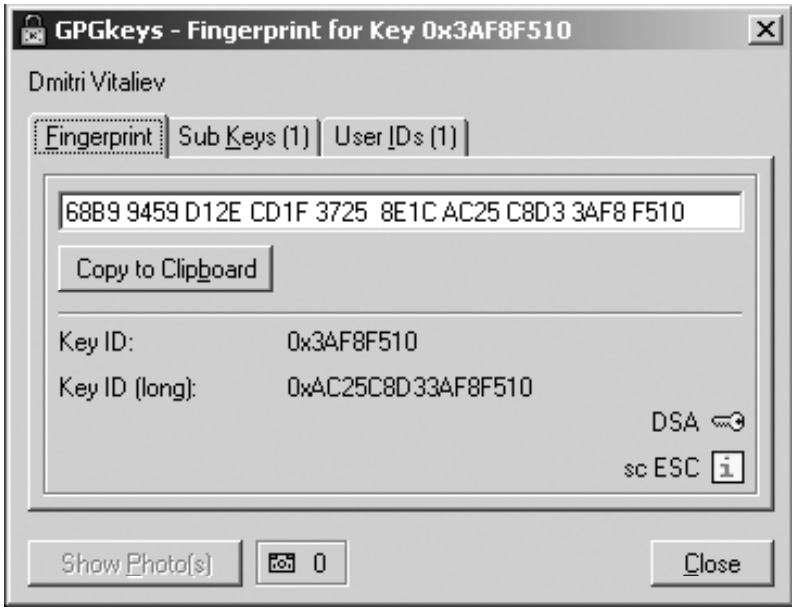
—

The PKE infrastructure relies on the valid identity of the public and private key. When you are encrypting a message to me using my public key, you want to be sure that this key belongs to me. Let's have a look at the properties of a key pair.

—

A key pair is identified by 5 distinct features:

- User ID: usually the email address of the key holder. Make sure it is spelt correctly.
- Key ID: a unique ID automatically generated by the **encryption** program.
- Fingerprint: (sometimes called MD5 and SHA1. See '**Encryption** on the Internet' chapter for more detail) this is a unique identifier that is generated from the public key.
- Date Created: the day on which the keypair was created.
- Date Expired: the day on which the keypair expires.



►Fingerprint as seen in the GPGshell program

Try and verify the above details before using someone's public key to communicate with them. Since public key **encryption** does not require you to

share a password with the message recipient, it is important that you can validate the true identity of the public key. Public keys are easy to create but the identifying features can also be falsified. That is why you should authenticate the person's public key before you use it (see 'Digital signatures' below). Once you have established that the public key belongs to them, you can 'sign' it. This will tell the program that you trust the key's validity and wish to use it.[31]

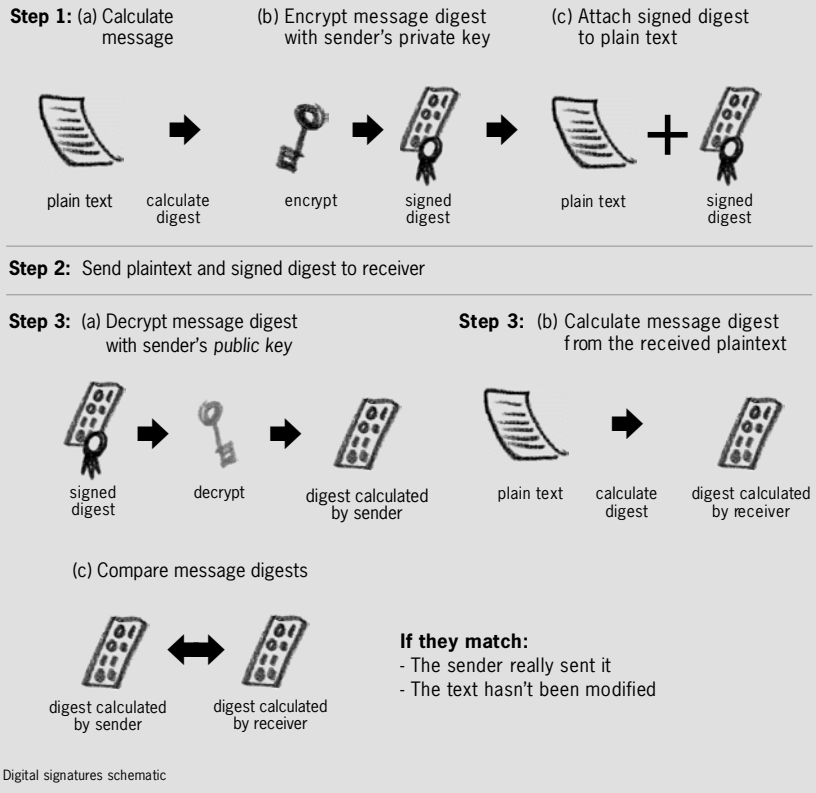
—

The key size is usually 2048 bits. This level of **encryption** is assumed to be far more complex than modern computers can break[32].

FOR TECHIES

Digital Signatures

We need the ability to verify the authenticity of our messages. This can be done by a digital signature, which also uses PKE to function. When you digitally sign a message, you include in it a unique mathematical calculation derived from its size, date and specific content. This digest is then encrypted with your private key so that the recipient can verify its validity. Once decrypted, the original digest in the signature is checked against the file received and confirms whether the file has been modified or not since it was signed. It is virtually impossible to change the content of your message without invalidating the signature.



▶ Digital signatures schematic

Some programs (e.g. GnuPG) that perform PKE can be integrated with an email program (e.g. GnuPG with Thunderbird using the Enigmail plug-in[33] or with MS Outlook using the G Data GnuPG plug-in[34]) making the whole operation simpler and faster to perform.

31
It will also add your signature to this key; should you send it to someone else, they will see your signature and know that you trust the validity of this key.

32
See this article http://www.keylength.com/en/3/ for a description of current and futurekey length necessities

33
Please refer to *the NGO in a Box – Security Edition*

34
http://www3.gdata.de/gpg/download.html

It is advisable to encrypt all your communications once you and your contacts have set up and began using PKI. This counteracts the possibility of arousing suspicion of a lone encrypted email, containing sensitive information.

To sum it all up, using **encryption** is really not so difficult with modern software at hand. The main points to remember:

- You need to create a keypair and keep your private key safe
- You encrypt your messages to the recipient's public key
- You should always verify the recipient's key by checking the fingerprint

ENCRYPTION INSECURITY

The biggest problem with using **encryption** is that it sometimes gives the user a false sense of security. Just because you are using **encryption** does not mean that your messages will remain 100% secure. It is, of course, an excellent method of raising your level of security, but it is not foolproof. The main problem with PKE security is the human factor: mistakes that we make by carelessness or ignorance. I will discuss three methods of breaking your **encryption** privacy.

- **Compromising your private key.** If the attacker manages to receive a copy of your private key by gaining access to your computer or otherwise, all they have to do is break the password protecting it. This can be done by brute force (using a password-cracking program that tries all common and random combinations) or by simply observing you type your password on the keyboard. Another method of stealing your password would be to install a keylogger program by gaining access to your computer with the help of an email attachment. A keylogger will record all the keys that you press on the keyboard and send this information to a designated Internet or email address. This way the attacker can receive the password you use to access your private key without requiring physical access to you or your computer.[35]

The solution here is to use updated anti-virus, and anti-spyware programs and a firewall. This will, hopefully, either detect the presence of the keylogger or prevent it from sending this information outside. Take care when typing the password and make sure that no one can see your keyboard or the computer screen. Most good **encryption** programs do not display the password on the screen. You have to write it 'blind'.

- **Key Recovery Systems.** Since **encryption** is now integrated into more devices and uses with every passing day, its highly secure framework has become a problem for many government and law enforcement agencies. For many years they have been trying to implement key recovery systems (key escrow) which would give the authorities access to your private key. Alternatively, governments have began passing laws stating that you must surrender a copy of your private key to them for storage. Some closed **encryption** programs, where the **encryption** method has not been publicly tested, actually provide a **backdoor** for security agencies. Although this practice has been made illegal in many countries, it can still be found in different versions of software and hardware. The solution here is to use open source products (like GnuPG), thoroughly analysed and tested by the Internet community.

35
In 1991, the FBI launched a technique named 'Magic Lantern'. Reportedly, it would attempt to install a Trojan Horse, attached to an email, on your computer. When activated, it would record all the keys a user typed and would send this information back to the headquarters. One justification for these actions was a response to the increased use of PKE. Since the FBI could not read an encrypted message, they tried to steal the user's private key password. This initiative was reportedly dropped after courts questioned its legality but we cannot be sure a variation has not been developed in the meantime.

- **Public key validity and deception**. As already mentioned in this chapter, the validity of the public key you are encrypting to is central to the all-round security of public key cryptography. The problem is that keys can be easily falsified. Carelessness on the user's part may lead to using an adversary's key under the assumption that it actually belongs to someone else. Pay close attention when receiving and importing public keys. The steps to verifying public key validity are explained above. Even though this may slow down the process of communication slightly, these steps should not be ignored.

There are also, of course, traditional methods of physical intimidation and force that could be used to make you reveal your password.

—

Choose **encryption** programs that have been publicly verified to have no back doors (such as PGP, GnuPG, TrueCrypt). Be aware of your local legislation and whether it allows you to use **encryption** and if yes, at what level of complexity (key size). You should also understand that the current legislation in your country may oblige you to reveal your password to the authorities. Try to find out if there are any legislative privacy safeguards which you can use to prevent this from happening.

—

There exist several other methods of breaking public key security. Your computer could have a compromised hardware that will leak your passwords and the content they protect to the intruder. There is nothing that can be done about this. The conclusion is not to rely fully on **encryption**. Use it to increase your security but do not operate under the impression that PKE is unbreakable. No one in the physical world is 100% secure and this is also true in the digital domain.

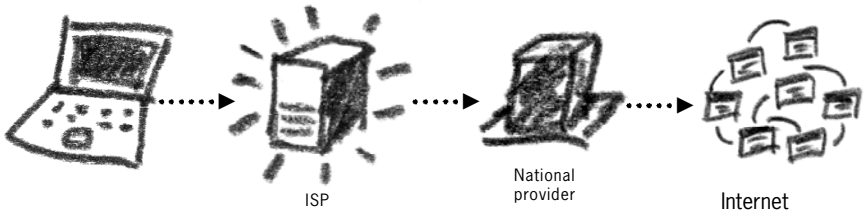
2.5 INTERNET SURVEILLANCE AND MONITORING

ABSTRACT

1 Monitoring your Internet and email activity is a simple task that is practised by businesses and governments all round the world.
2 Cookies record your Internet activity and are stored on your computer and the websites visited.
3 Email can be filtered by searching for specific words and phrases in your message.
4 Internet searches and requested webpages can be filtered by disallowing use of specific key words.
5 Access to certain websites can be blocked from within a country.
6 Access is usually blocked by the website's IP address or DNS name.

Surveillance and intelligence gathering have moved on – from monitoring phone calls and opening people's mail – to the Internet. Because of the Internet's open structure, today's surveillance can be carried out by governments, businesses, hackers and criminals. It is relatively simple to establish mechanisms that will record and monitor all of your Internet activity. All websites log information about their visitors (IP address and time of visit) as do the majority of email providers. Such surveillance has even become mandatory in many countries. In 2006, the EU passed the legislation requiring the ISPs to store the traffic data of all their subscribers for a maximum period of 2 years,[36] although some member states are not adhering to these rules and are storing the information for much longer periods. Let's have a look at how to monitor and censor your Internet activity on a local, national and global level.

MONITORING INTERNET BROWSING



► The ISP can monitor your Internet connection

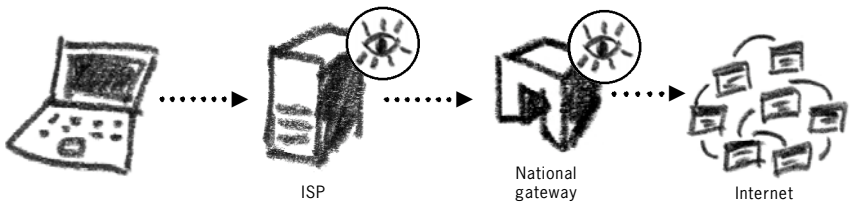
When you wish to eavesdrop on someone else's phone call, you need to get physical access to the telephone line or a contact at the phone exchange who would provide access to the line used by the conversing parties. Similarly, on the Internet it is possible to either intercept the line that connects you to the Internet or persuade the **ISP** to do the same. By doing this, all Internet activity originating from your computer can be recorded or even controlled by the surveillance mechanism.

36 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006

Whilst intercepting a phone or an Internet line may require specific skills and clandestine actions, influencing the **ISP** is a lot simpler. Many countries have only one **ISP** and it is usually under the control of their governments. Other countries, like Russia, have introduced laws that require all ISPs to install a computer specifically to monitor Internet activity. In Russia, this information is then fed directly to the Federal Security Service (FSB) databases[37].

—

All countries have access to an Internet gateway. This is like a door that can open or close to control the Internet access to and from the given country. All the Internet traffic will therefore pass through the national gateway, and one can assume that to have control over the country's gateway means being able to access to all country-related Internet traffic[38]. China has installed a system to monitor and filter all Internet traffic on its national gateway, known as the 'great firewall', and it restricts the Internet access for the entire population of China. Recently, the Chinese built an additional structure into this surveillance system. Known as Golden Shield, it can bring the filtering mechanisms into smaller regional networks, thereby distributing the workload from the national gateway to the local routers.



► Internet monitoring at the ISP and the national gateway

The above-mentioned tools for monitoring and censoring Internet traffic were not deemed sufficient in all the countries. The US, UK, Canada, Australia and New Zealand began to develop a global surveillance system that would encapsulate all major traffic points on the Internet. The events of September 11 in the United States led to huge investments to improve the system known as **ECHELON** which operates under the supervision of the National Security Agency (NSA). It is not known for how long **ECHELON** keeps the traffic data. It may seem that on a global level it is difficult to efficiently analyse and categorise all Internet and telephone communication, but the NSA claims a 90% success in doing that.[39]

Cookies

Records of our Internet activity are further stored on the websites we visit and on our personal computers. Many websites require installation of a cookie on our computer. A cookie is a small amount of data that stores specific user information about us. For instance, it could record our country of residence, so that we are presented with a relevant country page when visiting a particular website. This is often practised by airline websites. Other information could include the links we have followed to arrive at this or that website, or even personal data about us from our own computers. After browsing the internet for a month, you may have hundreds of different cookies on your computer. Accessing them can reveal information about your interests and affiliations. A cookie on your computer can act as a proof of your visiting a particular website. The largest Internet advertising service,

37
Privacy International – Privacy and Human Rights Report 2004 – *The Threats to Privacy*

38
In many countries satellite connections provide an alternative to using local ISPs. This makes surveillance a lot more difficult for the national government toimplement.

39
Echelon Watch
http://www.nsawatch.org

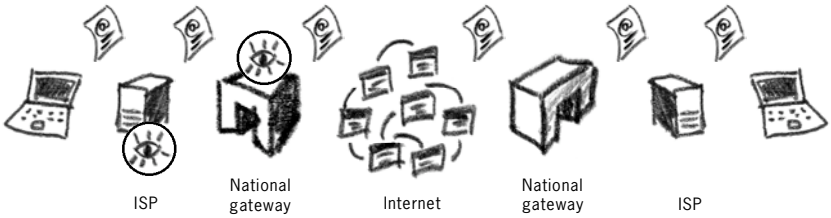
DoubleClick, has agreements with thousands of websites and maintains cookies on over 100 million users, each linking to hundreds of details of the user's browsing habits.[40]

—

It is possible to delete cookies from your computer. This can be done from your Internet browser or by finding and deleting them manually. It is also possible to tell your browser not to accept cookies at all. This may result in many websites refusing to open on your computer, but will provide you with maximum protection from cookie infiltration.

Monitoring Email

Email communication uses the same principles as general Internet browsing, except that each message of ours has a destination: another person who also connects to the Internet through his or her country's local provider.



►Monitoring email at the ISP and national gateway

Following this scheme, our email message can be intercepted at all major routing points on its way. If you live in a country with strong legal protection of privacy, its legislation won't apply when your email reaches the **ISP** of the recipient in a country with different privacy laws. Bear in mind that whilst your email is on its way from country A to country B, it could pass the routers of several other countries on its way.

—

Many ISPs and email providers keep a copy of all emails on their servers. Sometimes this is to our benefit, as we may want to access an email that was sent to us 3 years ago. However, it also allows an outside party to request/demand access to our email accounts. Yahoo! handed over to the Chinese government its user information on four Chinese dissidents resulting in their arrest and conviction.[41]

SPOOFING

It is relatively easy to 'spoof' an email address. Spoofing means that you fake the name and email address of the sender that can appear as a random address or the one of someone you know. For example, someone can use your email address and name to send a controversial article to a newspaper. The newspaper does not bother to verify whether it was actually you who had sent the article and simply publishes it. The outcome could be embarrassment, damaged reputation and even litigation. Email can also be intercepted and its contents altered while it is en route to its destination. It is almost impossible to tell a real email from a spoofed one, as all its identifying features can be faked. Digital signatures are the only way to make sure the message is not tampered with or faked[42].

40
Privacy International – Privacy and Human Rights Report 2004 – *The Threats to Privacy*

41
Human Rights Watch - *"Race to the Bottom" Corporate Complicity in Chinese Internet Censorship*, August 2006

42
see 'Cryptology' chapter and also 'Identity Theft and Profiling' chapter for an explanation of digital signatures and how to secure your digital identity

► Your message or identity can be spoofed by an adversary on the Internet

INTERNET & EMAIL FILTERING

Apart from monitoring our Internet activity and emails, government and intelligence bodies have the ability to scan the contents of our messages and to prevent us from accessing certain websites. At this point, surveillance becomes censorship in breach of Articles 12 & 19 of the Universal Declaration of Human Rights[43].

—

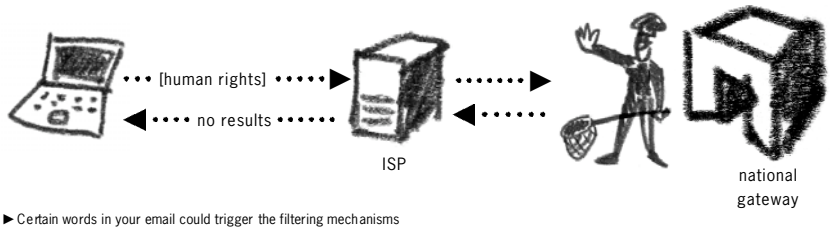
All information on the Internet, unless otherwise specified, travels in an open manner. When you send an email, the data in it goes to its destination unsecured. To compare this transmission to a telephone conversation, if you were you to pick up the phone at the **ISP**, you would hear the message content read out to you by all ISPs users currently sending emails and/or browsing webpages! Therefore all your email as well as exchanges from Internet forums or blogs can be easily intercepted and read. Internet filtering scans the contents of every web page, **blog** of forum that you visit. We have seen already how easy it is to collect all our email and Internet traffic, and one can only imagine the amount of information freely submitted to the surveillance agencies simply by not making our communications secure.

—

Certain countries are particularly sensitive to the information communicated by human rights organisations. Modern technology means that it is no longer necessary to sit in a dark room reading all email messages in or out of the country in search of undesirable or damaging information. This task is now performed by computers and is known as filtering.

Email Filtering

A program to scan the content of all email messages is installed at the **ISP** or a national gateway. It is instructed to look for the keywords 'human rights' or 'freedom of expression'. In reality, it could be programmed to search for



► Certain words in your email could trigger the filtering mechanisms

43
Article 12 – No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 19 – Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

thousands of specific words and phrases. Whenever an email containing the listed keyword is found, it is either blocked and not allowed to pass further on, or recorded for further investigation of the sender's and recipient's identity. Filtering can occur at any point of the message's routing on the Internet.

—

The **ECHELON** system uses the above filtering technology. Here's a list of some words that would trigger a response should they be found in your email by **ECHELON**.

—

Rewson, SAFE, Waihopai, INFOSEC, ASPIC, MI6, Information Security, SAI, Information Warfare, IW, IS, Privacy, Information Terrorism, Terrorism Defensive Information, Defense Information Warfare, Offensive Information, Offensive Information Warfare, The Artful Dodger, NAIA, SAPM, ASU, ASTS, National Information Infrastructure, InfoSec, SAO, Reno, Compsec, JICS, Computer Terrorism, Firewalls, Secure Internet Connections, RSP, ISS, JDF, Ermes, Passwords, NAAP, DefCon V, RSO, Hackers, **Encryption**, ASWS, CUN, CISU, CUSI, M.A.R.E., MARE, UFO, IFO, Pacini, Angela, Espionage, USDOJ, NSA, CIA, S/Key, **SSL**, FBI, Secert Service[44]

Internet Filtering

The same methodology is applied to Internet browsing. When you enter a search query into Google, it is passed through the **ISP** and a country gateway, before you get a reply. A filtering system could intercept your search for 'human rights' and return a null or wrong result. Below are images of a search result from 2004 on 'falundafa' (a banned spiritual movement in China) performed on Google.com from China.

It appears as if there is no information on this topic in Google, but the error message actually comes from the filtering software, not Google itself[45].

—

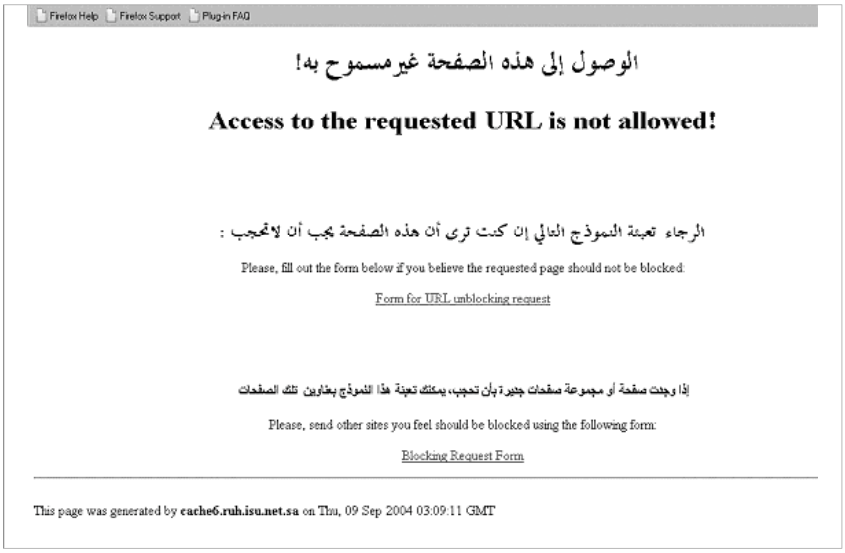
Internet filtering can also scan the content of websites you wish to access, and block your request, should the website contain any words the filter is programmed to look out for.

44
http://attrition.org/misc/keywords2.html – these tests were done by including words in email and recording the time difference in the hops taken to the destination.

45
This method of blocking has recently changed. Now, Google will display its own message stating that the search query you entered is not allowed by the local authorities.

INTERNET CENSORSHIP

Numerous countries have banned access to certain websites for their citizens. These websites present information on religious extremism, terrorism, paedophilia. Some countries also block websites that criticise or expose government policy, discuss issues of human rights or provide tools that could enable one to bypass these censorship blocks. Here is the result of a request from Saudi Arabia to access a banned website.

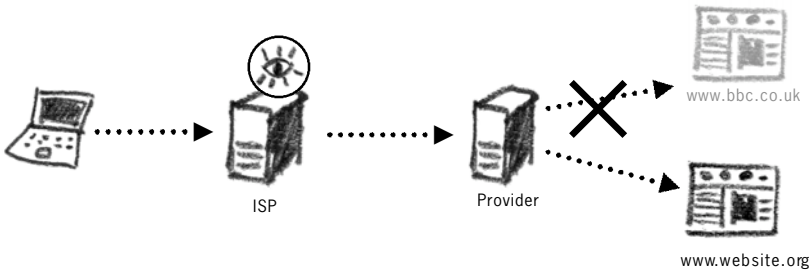


►A screenshot of a blocked website from inside Saudi Arabia

Governments tend to decide for themselves what content they wish to censor. The majority of governments that perform filtering use US and Israeli technology. Some of the more infamous products are SmartFilter and WebSense. These are bought (or pirated) by states who then set up the filtering based on the software's criteria, with additional modifications. Websites can be blocked and Internet searches restricted with the help of the three following methods:

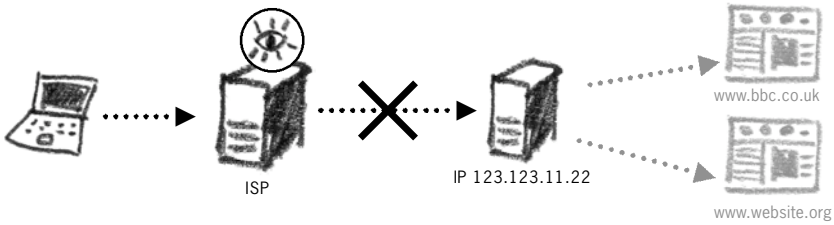
Blocking by DNS

This block on the filter ensures that all requests to www.bbc.co.uk will not be allowed to pass. The block is applied to the domain name of the website. Should the website be re-registered or mirrored under a different domain name, it will become accessible again.



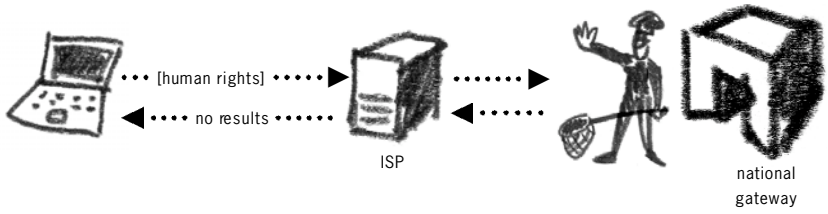
Blocking by IP

This method blocks the website's IP number from access. This is a much more effective block as a new DNS name for the website could still point to the same IP. However, a problem arises when blocking websites by IP. Sometimes these websites sit on large web servers that host several thousands of different websites. These web servers only have one IP. Blocking a website's IP address effectively blocks all other websites sitting on the same webserver.[46]



Blocking by keywords

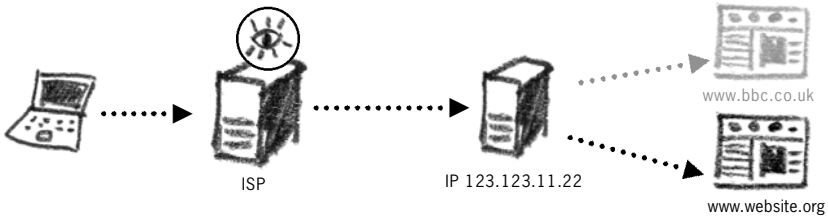
Any email or search query that contains words banned by the filter is not allowed to pass through. The same applies to any website that contains banned words.



These rules can be applied separately or together to create filtering and blocking capacity. Some countries rely on the pre-defined categories of the filtering software and add new websites to its configuration, whilst others employ huge teams of people to scan the Internet and catalogue what should appear in the filter. The Internet's open structure is being limited and reduced to allow only approved content to appear for the nationals of many countries. For an in-depth study into country-specific filtering methods and technology, go to the OpenNet Initiative – Country Studies website.[47]

DNS hijacking

This is a recent Internet practice that has been used in presidential campaigns (2004 US elections) as well as by countries that filter the Internet. When you enter an address of a website you wish to visit, you are automatically re-directed to another website. Some users may not even notice the difference.



46
"..more than 87% of active domain names share their IP addresses with one or more additional domains, while more than two thirds of domain names share their IPs with fifty or more domains.." /Ben Edelman, Web Sites Sharing IP Addresses: Prevalence and Significance, February 2003 http://cyber.law.harvard.edu/people/edelman/ip-sharing/

47
www.opennetinitaitve.net

On September 8th 2002, users in China were prevented from going to Google's web search page. Instead, they were re-directed to a number of China-based pages. The address in the URL said www.google.com[48]

►A screenshot of the Chinese Internet hijacking the www.google.com DNS

48
Empirical Analysis of Internet Filtering in China, Berkman Center for Internet & Society, Jonathan Zittrain and Benjamin Edelman, 2002

2.6 CIRCUMVENTION OF INTERNET CENSORSHIP AND FILTERING

ABSTRACT

1 Website blocks can be circumvented by using proxy servers. There are several types of proxy servers differing in their location, reliability and security features.
2 Keyword filtering can be overcome by using encrypted connections as well as proxy servers that operate over 'HTTPs'.
3 Anonymity networks allow us to browse the Internet without any restrictions or identifiable traces.
4 You must also know how to research and find new circumvention tools and proxy servers yourself

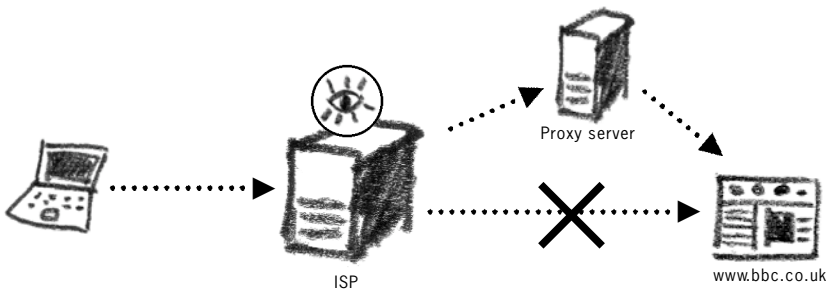
This chapter will show you different methods of bypassing Internet censorship and protecting yourself from keyword filtering. In other words, it will explain how to access blocked websites, how to conceal from surveillance agents whatever you are reading or sending on the Internet, and how to hide your presence from Internet monitoring. For non-technical readers, it is advisable to first review the previous chapter on 'Internet surveillance and monitoring' as well as the 'Internet explained' appendices, in order to understand this section in full.

—

Many tools and strategies to circumvent Internet restrictions are in existence today. This chapter will introduce you to only a few of them. With time, many well-known tools and websites could also get censored by surveillance agents in your country. To maintain your right to the freedom of the Internet, you will have to find new websites and tools that offer similar services. This can usually be achieved by extensive web searching and via communication with your peers. The purpose of this chapter is to make you aware of current services and strategies to use in the future.

PROXY SERVERS

It is relatively easy to block access to a website from a particular country, but it is also not that difficult to bypass these blocks. If you are not allowed to access bbc.co.uk, you can ask another computer (proxy) to fetch the



►Re-routing a censored connection through a proxy server

website for us. Thus you will effectively be accessing only the proxy and therefore won't be restricted by your country's filtering rules. There are thousands of such proxies, and their mission is to be the intermediary between a client's computer and a host website. Since there are many countries in the world which do not block access to websites on human rights, independent journalism, religion, etc., you can use the proxies set up in them to get access to information which is blocked in your country.

—

Proxy servers are divided into several categories. It is important to know the functions and security provided by the proxy server you select to use. Please remember that you cannot conceal the information you are sending and receiving from the proxy server itself.

CGI proxy

The simplest type of proxy server is CGI proxy. The coding for proxy server operations is built into a web page and you can use its services simply by browsing the Internet directly through it. Two famous CGI proxies are Anonymizer and The Cloak. Their popularity has led many countries that practise Internet filtering to block access to these sites as well. There are many other public CGI proxies that you can find my entering the keywords 'CGI proxy' or 'nph-proxy' into a search engine.

http://www.anonymizer.com
http://www.anonymouse.org
http://www.the-cloak.com
http://www.webwarper.net
http://www.proxify.com
http://www.peacefire.org[49]
http://www.stupidcensorship.com
http://www.mypr0xy.com[50]
http://www.webproxylist.net/sites_Results.php[51]

Remember that if the Internet connection is not encrypted (HTTP), it is still possible to read the data you are sending or receiving.

HTTP proxy

This is a standard proxy that will fetch a blocked website for you. It is possible for surveillance to see that you are connecting to a proxy server and the website you are trying to access through it.

49
Peacefire.org activists frequently change the address of their CGI proxies as they become blocked in some countries. You can sign up to their email list to receive addresses of newly set up CGI proxies.
Go to http://www.peacefire.org/circumventor/

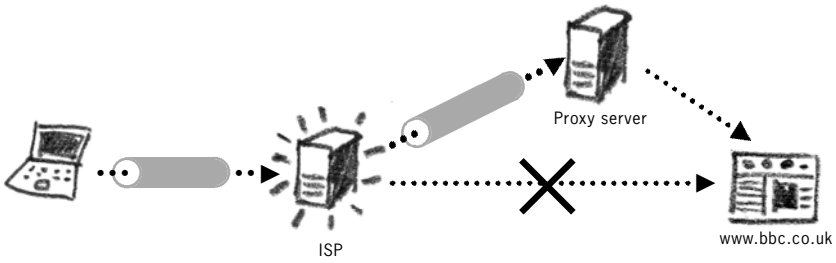
50
On this website, you can create your own address where the CGI proxy will appear.

51
This website has an automatically updated function that looks for current CGI proxies and a link to them. There are over 30 thousands working proxies at any one time.

Both the CGI and HTTP proxy servers can be further secured by having one or both of the following elements:

HTTPS (or SSL) proxy

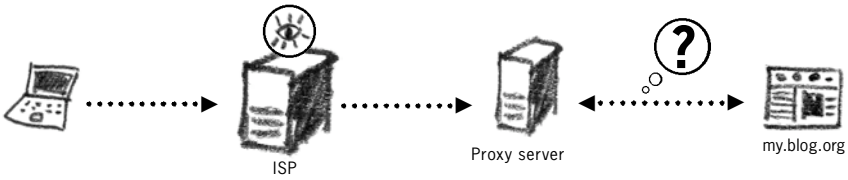
An encrypted tunnel is created between you and the proxy server and surveillance agencies cannot know the destination website, but only see that you are connecting to the proxy server itself. This is a more secure option when using a proxy, but you should be aware of Man-in-the-Middle attacks (see '**Encryption** on the Internet' chapter) and know that information you send and receive is not hidden from the proxy server provider.



►Encrypting your connection over **SSL** to the proxy server

Anonymous proxy

Your connection to the proxy server is not encrypted but the proxy is set up so that it hides your origin at the destination website and reveals only that the website is communicating with the proxy server itself.



►The visited website does not know the origin (the real IP address) of your computer

Here's a list of websites that collect current information about new proxy servers you could connect to. These lists contain a range of standard HTTP, secure and anonymous proxies.

http://www.samair.ru/proxy
http://www.antiproxy.com/
http://tools.rosinstrument.com/proxy/
http://www.hidemyip.net/
http://www.web.freerk.com/proxylist.htm
http://www.proxy4free.com
http://www.proxyblind.org/protect/free_proxy_server.php (password:letmein)
http://www.proxy-list.net/anonymous-proxy-lists.shtml[52]

IP address	*Port*
80.80.12.124	80
165.228.128.10	1080
194.170.187.5	8080

These websites will show you a range of different proxy servers. They will always consist of an IP address and port number. You will need to insert these details manually into your web browser.

52
This list was compiled in October 2006, and its accuracy as at time of reading cannot be guaranteed. You can search for the keywords 'proxy servers' in your search engine to find other websites should the listed ones not respond.

Internet Explorer

To insert a proxy server into your Internet Explorer web browser, on the menu bar:

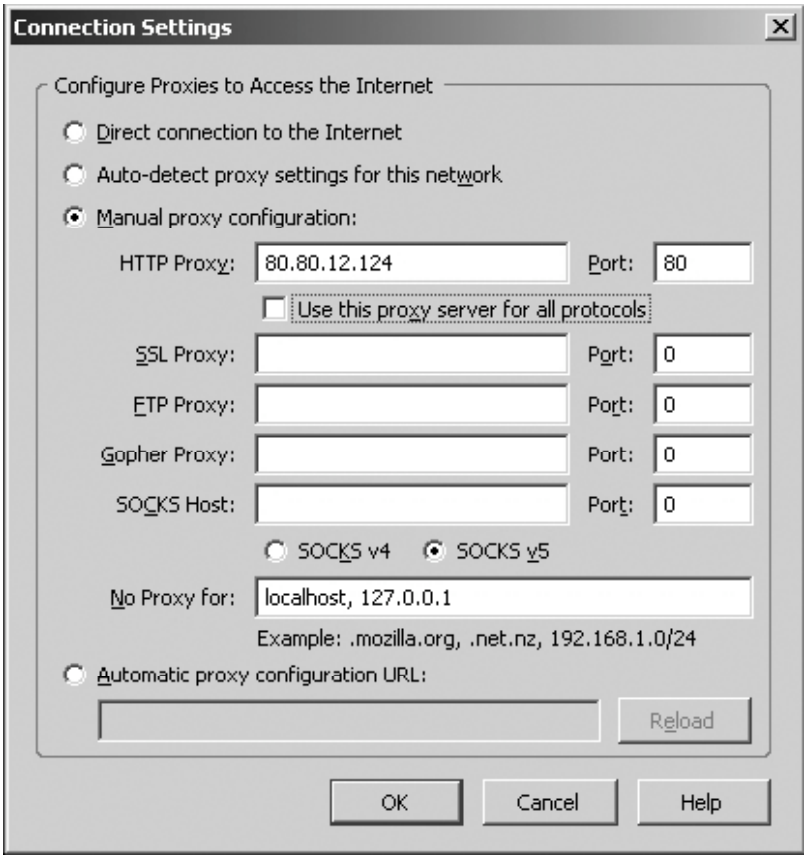
Select: `Tools > Options`
Click on: `'Connections' tab`
Click on: `'LAN settings' button`
Select: `'Manual proxy configuration' option`

Insert the proxy IP address and port number into the relevant windows of the 'HTTP' line.

Mozilla Firefox

To insert a proxy server into your Mozilla Firefox web browser, on the menu bar:

Select: `Tools > Options`
Click on: `'Connections' button`
Select: `'Manual proxy configuration' option`



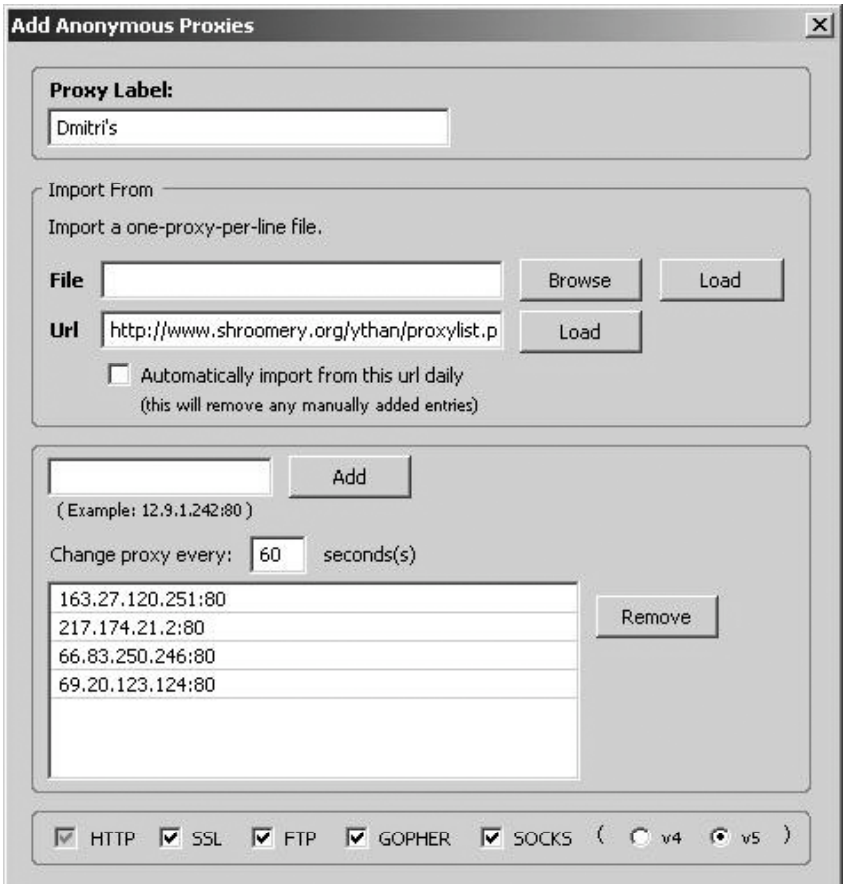
► Setting a proxy server in Mozilla Firefox

Insert the proxy IP address and port number into the relevant windows of the 'HTTP' line.

The Mozilla Firefox Internet browser has a useful little plug-in called 'switchproxy'. It will allow you to input a large range of different proxy servers and set a time for switching between them. This is a good option as you should not use one public proxy server for too long[53].

► The switchproxy toolbar in Mozilla Firefox

53
The switchproxy plug-in can be downloaded from http://mozdev.org/switchproxy or from the *NGO in a Box – Security Edition* CD (including a guide to using switchproxy). Make sure you have the Mozilla Firefox browser installed first.



► The switchproxy configuration screen

Private circumventors

These are proxy servers, set up by your friends or colleagues from the countries that do not filter the websites you wish to access. They are not well-known, and you will need either the IP address and port number, or in the case of a CGI proxy, the web page address and, possibly, login details as well. The main advantage of these circumventors is that they use trust networks – a private group of friends sharing their computer resources to help each other. Such networks provide for greater privacy as they are closed to the public and hence difficult to detect and to block.

—

Psiphon[54] is a recently developed private CGI proxy that aims to use trust relationships between people wishing to help their friends from the countries that censor the Internet. The server is easily installed on a computer running Microsoft Windows and generates login details for its clients. The details (IP address, user name and password) are passed among a closed circle of friends who then use the Psiphon computer's Internet connection as their proxy.

► Psiphon adds another search bar to your browser screen. You should type all your addresses in there now

► The Psiphon CGI proxy will fetch websites for you that may be blocked in your country

54
http://psiphon.civisec.org

Peacefire Circumventor[55] – allows you to create your own CGI proxy server for others to use. You will need a dedicated computer and an Internet connection to install and run this server. It is recommended that your server is installed in a country that does not implement Internet censorship. The connection details to your computer/proxy server are then passed to users living in the countries that do implement censorship.

Commercial circumventors

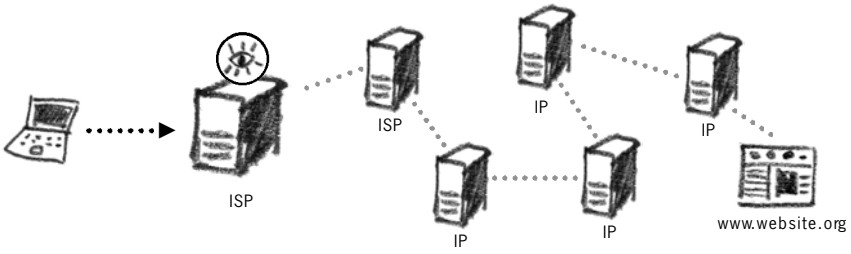
There are a number of fee-paying **circumvention** software programs and services available on the Internet. They provide good security and may not be blocked in your country as they are often used by businesses.

http://www.steganos.org
http://www.anonymizer.net/

ANONYMITY NETWORKS

Using proxy servers has its disadvantages. They are often difficult to find and do not always offer ideal security for your Internet browsing. However, there exist Internet tools that will perform all functions of a proxy server, including much higher levels of privacy and anonymity for you.

Imagine that you send a letter to a friend and package it in several different envelopes writing a different address on each one. The letter will circulate around these addresses in a secret order, and none of the addressees will know its origin or final destination, but only the previous address it came from and the next one it will be going to. Similar systems have been created on the Internet. A recent and stable addition to them is known as the TOR network.[56] It will anonymise your presence on the Internet and your browsing requests. Surveillance agents at your **ISP** or a country gateway will not know the final destination of your browsing query and the website you visit will not know where your request came from. Increasingly, the TOR network is being used as a **circumvention** tool, easily bypassing national firewalls and website filters.



► Anonymising your Internet presence on the TOR network

It relies on a number of servers (and on the volunteers to set them up) around the world and uses **encryption** between each of the points your message passes through. Therefore, the computers that your request goes through, will not be able to make sense of the data or decrypt it.

Recently, Torpark – a mobile version of TOR was released. It does not need to be installed on your computer and can be carried around on a USB memory stick. It also has an Internet browser, with TOR already pre-configured[57].

55
http://www.peacefire.org/circumventor/simple-circumventor-instructions.html

56
http://tor.eff.org

57
You can download a copy of TorPark from http://torpark.nfshost.com/ or find it on *the NGO in a Box – Security Edition* CD.

It should be noted that Torpark is not written by the developers of TOR and its code remains closed for inspection and scrutiny. Therefore, the security of Torpark has not yet been verified.
TOR is better than public proxy servers, but its strong anonymity becomes a disadvantage when using webmail or, say, publishing on Wikipedia.org. You will need to investigate first if your desired website will function with TOR. It also slows down your connection speed, especially if you are connecting over a dial-up telephone line. TOR developers are currently working on eliminating this hitch.

FOR TECHIES

Freenet[58] – is an anonymity network for document storage and publishing. All members of the network donate a small portion of their hard drive for storing information from other members. The files are encrypted and not accessible to the computer owner. This way you can store your documents, websites and messages on multiple computers, with secure and anonymous connections. The Freenet network has been especially popular in China and in the Middle East.

A WORD ON ANONYMOUS INTERNET PUBLISHING

Those who maintain (or contribute to) a **blog** or an Internet forum need to be aware that their anonymity will not be guaranteed merely by signing with a pseudonym. Every **blog** entry records the IP address of the computer it was sent from, and many ISPs record all traffic that has passed through them. Therefore, if you are publishing sensitive information on a website, you must take precautions not to be found out. By using anonymous proxy servers you can disguise your IP origin from a particular website; by using an **SSL** proxy you can hide the article you are uploading from the **ISP**. Another option is to use the Tor anonymity network (if your **blog** site will function with it).

—

One aspect of security that you cannot guarantee by using these servers is time stamping. If, for example, you were to publish a website about government activity in your country by using the Tor network, surveillance agents won't see that you were sending this information to a particular **blog**, but they may notice that whenever you enter an Internet café a new post appears on the site. This could probably be linked to you, especially if your Internet café owner writes down your name and the time of your visit. To overcome this difficulty, it would be advisable to ask friends from a different country to post the **blog** for you. You could use a secure webmail service (or **encryption**) to send the article to them and ask them to wait for a while before publishing it on your **blog**.

—

For an extensive guide to online publishing, see 'Guide for bloggers and cyber-dissidents' from the Reporters sans frontières web page.[59]

SUMMARY

The tools and techniques, described in this chapter, are useful to those living under the regimes that apply strong censorship and filtering to the Internet. With their help, you can get around some of the blocks to

59
You can download a copy of Freenet from http://freenetproject.org/

59
http://www.rsf.org/rubrique.php3?id_rubrique=542

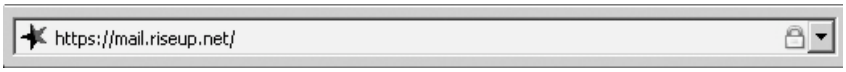
accessing websites and regain some privacy when publishing material online. Bear in mind that the countries practising Internet censorship and filtering are constantly on the lookout for new proxy servers and privacy tools with the intention of blocking access to them as well. In response, users from all over the world are setting up new proxies every day – a true cat and mouse game.

2.7 ENCRYPTION ON THE INTERNET

ABSTRACT

1 Information that you send or receive on the Internet travels in an open manner.
2 Some websites can help secure this information by creating an encrypted tunnel between themselves and your computer.
3 This tunnel is built automatically, authenticated by you and has distinguishing features.
4 There remains a possibility of intercepting and breaking the security of this system by what is known as a Man-in-the-Middle attack.
5 You must carefully validate the security certificates, presented by the website offering encrypted connections

Methods of **encryption** have been integrated into various Internet services. Some of them affect us all. When we log into our email accounts, make purchases online or transfer important information from one place to another, we want to enjoy a good deal of security from surveillance and information theft. An infrastructure that allows encrypted communication on the Internet is called the **Secure Sockets Layer** (**SSL**). You can see when



your Internet browser has entered **SSL** by two distinguishing features:

- The address for the website will begin with https:// (the 's' standing forsecure)
- A little padlock will appear in the bottom toolbar of your Internet browser

► Connecting over **SSL** to a website

This means that the website you are visiting and your Internet browser have agreed upon an encrypted communications channel. To find out more about the security of this method, we need to have a look at how it works.

SSL CERTIFICATES

The **SSL** system works on the Public Key Infrastructure (PKI) concept. All websites wishing to use **SSL encryption** must obtain an **SSL** certificate. Your Internet browser communicates with the **webserver** and encrypts all information sent between the two points. The strength of the **encryption** depends on the **SSL** certificate at the **webserver** end. The Internet standardat the moment is 128/256 bits, which is strong enough for nearly all instances.

Your Internet browser (we assume it is Internet Explorer & Mozilla Firefox) has a built-in list of trusted **SSL** Certification Authorities. If you browse to a website that presents you with an **SSL** certificate, your browser will automatically check whether it was issued by a trusted authority on your list and whether all its details are correct (i.e. they do not arouse suspicion). Each certificate contains at least the following:

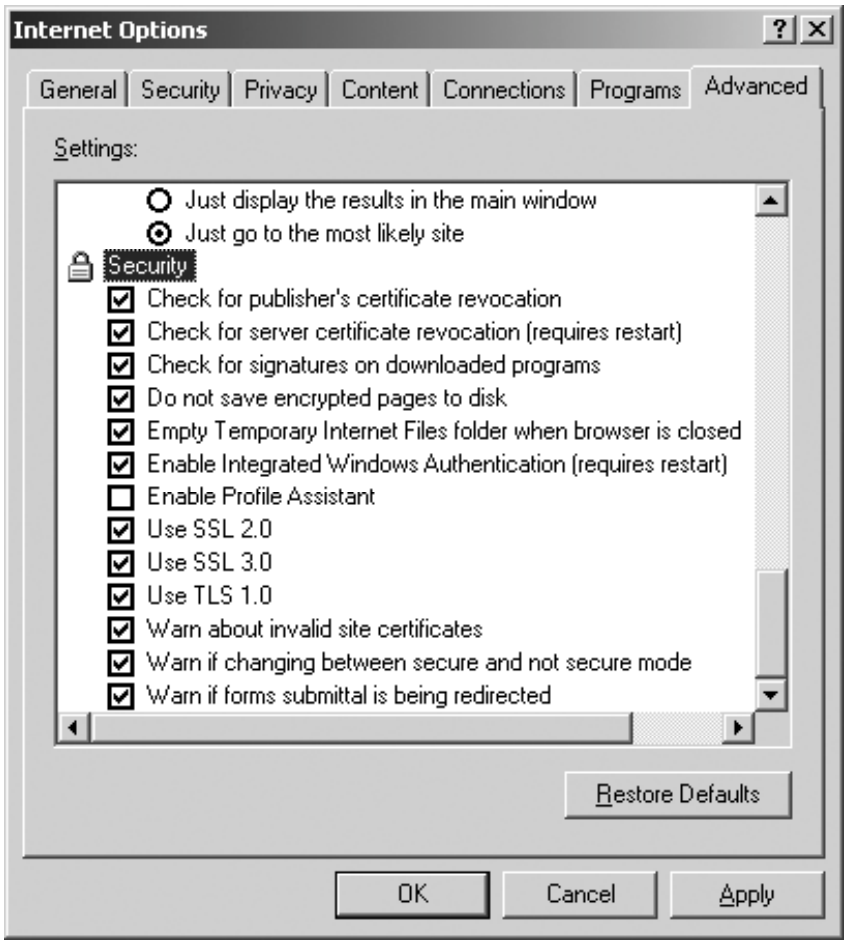
- Owner's public key Owner's name or alias
- Expiration date of the certificate
- Serial number of the certificate
- Name of the organization that issued the certificate
- Digital signature of the organization that issued the certificate

If the authority that issued the certificate is not on your list, or one of the certificate's details could be a cause for security concern, your browser will issue a warning and will allow you to examine the certificate.

Note: This does not happen automatically if you are using Internet Explorer, in which case you first need to set this option in the program.

Select: `Tools > Internet Options`
Click: `Advanced`

Scroll down the list to the 'Security' section until you find the entry 'Warn about invalid certificates' and make sure this box is ticked.



► Advanced Internet settings of Internet Explorer

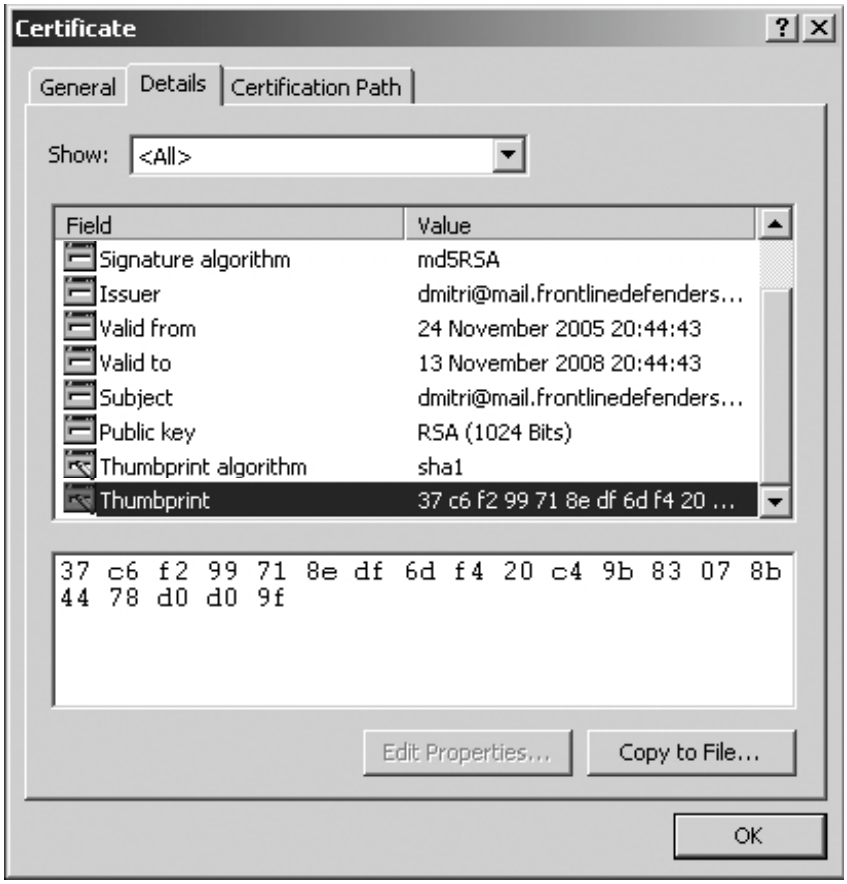
►Internet Explorer Certificate Warning

►Mozilla Firefox Certificate Warning

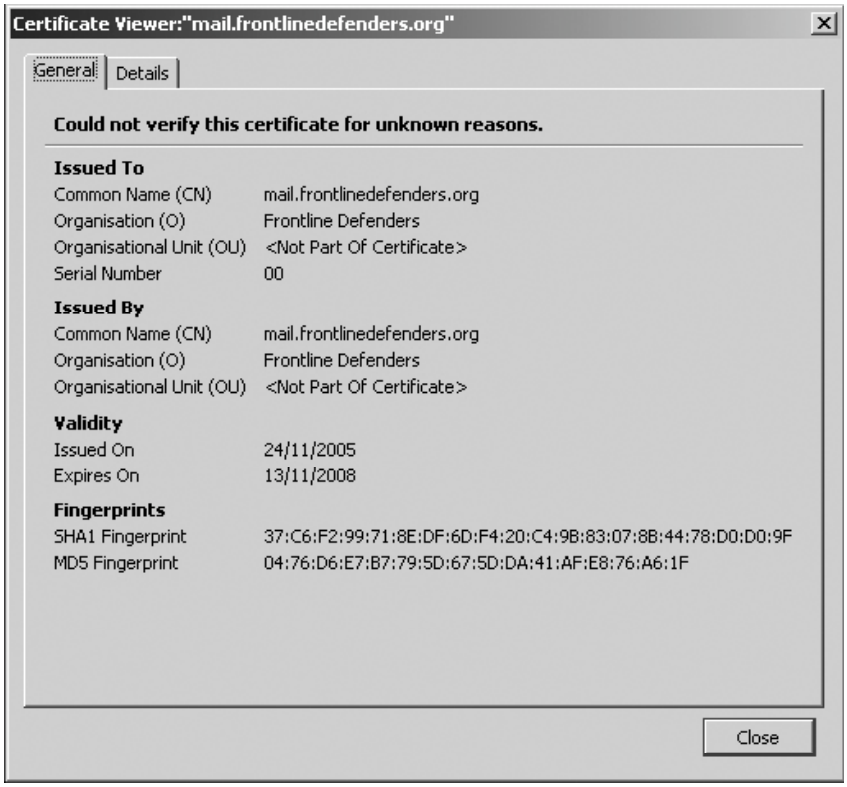
Both of these messages refer to the same problem, although they look different in their respective programs. In both cases you have the option of examining the certificate yourself and then deciding whether you wish to accept it or not. If you do not accept it, you will not have access to the website. If you do choose to accept it ('Accept this certificate permanently' in Mozilla Firefox), then the certificate and its issuing authority will be added to your trusted list and **you will not be asked for approval of this certificate again!**

—

If you need to inspect the certificate, you should be aware of the things to look out for. The main identification feature of the certificate is its fingerprint



► Internet Explorer Certificate Information



► Mozilla Firefox Certificate Information

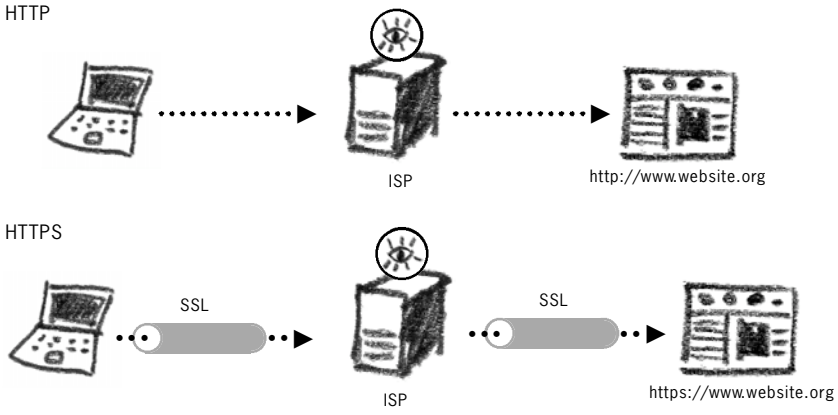
(sometimes called thumbprint or MD5). It is the verification of this fingerprint that can positively identify the certificate has really been created and issued by the owners of the website you are visiting. To validate its authenticity, you will need to contact the website owner and check the fingerprint with them manually (by phone, fax, Internet chat or in person). Although this may sound quite annoying, it is a necessity of good security, and the next section will explain the vulnerability you expose yourself to if you do not follow this procedure.

SECURE EMAIL

SSL connections have been built into email services on the Internet. This applies to webmail as well as to hosted email. Some webmail accounts offering such security measures free of charge are:

https://www.riseup.net
https://www.bluebottle.co.uk
https://www.fastmail.fm
https://www.safe-mail.net
https://gmail.com

These webmail services allow you to enter your email account and communicate with it on an encrypted connection. Even though this data can still be captured by any filtering or surveillance mechanism, it will be next to impossible to make sense of it or decrypt it. Notice how the address is deliberately written with 'https:' in the beginning.

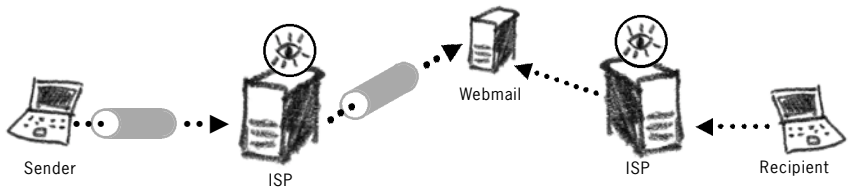


Essentially, this creates a much more private method for reading and writing email. Used with a good password (see Passwords chapter), it will pave the way to securing your Internet communications. Registering one of these email accounts does not differ at all from registering with Yahoo or Hotmail. The reason is that the majority of webmail providers do not offer **SSL** connections to their clients.

Security Circle

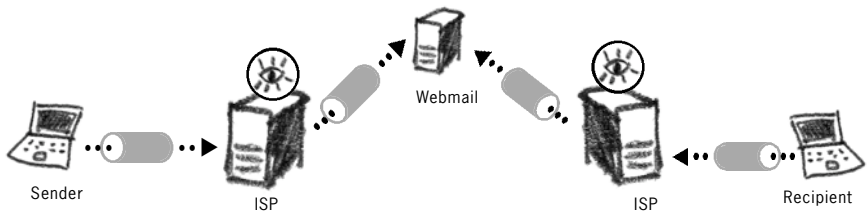
Please note that the recipients of your email may not be using similar security when connecting to their webmail account. As soon as your email hits the recipient's webmail it becomes prone to the security standards of

his/her server. If the recipient connects to his/her webmail using an open (non-encrypted channel), surveillance agents at the **ISP** or a national gateway will be able to scan and read your message in full.



► Encrypting one side of the communications channel

To maintain a higher level of privacy in email communications, both parties must use a secure connection to their webmail server, whatever it may be. If your ambition is simply to 'escape' the country where you are sending the email from, and the path taken by your email from the recipient's webmail server to the recipient's computer is irrelevant, you may, of course, not pay heed to the example below. Yet, to maintain a closed loop of communication always constitutes a good security practice.
The security of this approach can further be improved if both parties use the same **SSL** webmail service provider (RiseUP, Bluebottle). Email, travelling on the Internet between servers, is usually unencrypted and can easily be intercepted.



► All-round **SSL** encryption in email communications

There is a security consideration when both parties use the same **SSL** webmail service. It is the webmail server itself that stores and processes all your messages. Even though your connection to the server is encrypted, the email is accessible to those who maintain the server or hack into it. You may wish to research the security and reliability of your webmail provider as well as the country where it is located. This becomes an issue when you consider a country like the United States, where authorities can issue a subpoena to confiscate the server and all information on it. The above-mentioned webmail servers are situated in the following locations:

www.riseup.net – United States
www.bluebottle.com – United Kingdom
www.fastmail.fm – United States
www.safe-mail.net – Israel
www.gmail.com – multiple servers including United States, Australia, Mexico, South Korea and China

The ability to protect your information from the provider has been offered by a number of webmail services. The latter not only use a secure channel of access but also encrypt your data on the server. Your webmail account can only be accessed and opened by you. Email sent to the recipients, who

have an account with the same provider, can also be encrypted. Such webmail providers offer a higher level of communication security, but usually require a relatively fast internet connection, for every time you access your account, the website automatically installs temporary **encryption** software on your computer.[60] Services, allowing you to register free accounts, are :

www.hushmail.com
www.vaultletsoft.com
www.s-mail.com

MAN-IN-THE-MIDDLE FOR TECHIES

The biggest threat to the **SSL** Certificate model is what is known as a Man-in-the-Middle (MITM) attack. At its most basic, it is an interception of your Internet information stream – your communication with a web server. It can be used specifically to break the otherwise secure **SSL** model explained above. First of all, the adversary must get physical access to your Internet line. This can be done at the **ISP**, a national gateway or even a local network. The adversary then tricks you by presenting an alternative certificate (possibly similar to the above) when you try and access your secure webmail account. Only this certificate is not from the webmail provider, but belongs to the adversary. By accepting the certificate, you enter into a connection with your website **through** the adversary's server. As you input your information – login details, financial details, witness testimonies – the adversary receives it all without an effort.

—

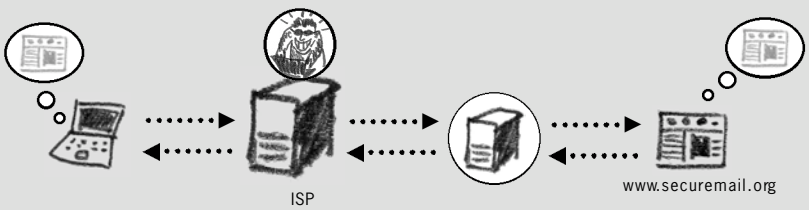
The problem is that it is very easy to get you accept a certificate you have yourself presented. People tend to click 'OK' without reading the messages. While on a security training course, I saw computer technicians compromise a highly sophisticated **encryption** system simply by not verifying the presented certificate before accepting it.

—

An adversary might be motivated to carry out a MITM attack when he cannot read your email and other Internet transactions because you are operating over 'HTTPs'. He can see you accessing your webmail server, but he cannot see the email you read and write.

—

When your Internet line has been intercepted and you accept the adversary's certificate, all your data transmissions during this (and, possibly, future) sessions will go via the adversary's server. This means all your login details, private email, etc. Another problem is that once you have been successfully attacked, it is very difficult to notice that your connection is being routed through another computer.



►Man-in-the-middle. Your communication channel is intercepted and relayed by an adversary. Both sides are under the impression that their communications continue as normal

60
Such webmail services usually require the presence of the Java VM (compiler) on your computer. See *NGO in a Box* for more details

Whenever your Internet browser asks you to verify the **SSL** Certificate, ask yourself two questions:

1 Is this the first time I am accessing this website from this computer?
2 Have I checked the validity of the certificate properly?

If the answer to question 1 is 'no', then you either did not save the certificate permanently or are facing a Man-in-the-Middle attack. As mentioned earlier, your browser will not ask for your acceptance of a certificate you have previously saved. If you are being asked a second time to accept a certificate to a website whose details should already be in your trusted list, it is probably not the same website.

Note: If you are in an Internet café, you may not be able to verify whether the fingerprint has already been accepted. It is advisable to write down your website's fingerprint the first time you access it from a secure location and then verify it every time you access it from other locations.

Answer question 2 by inspecting the certificate's fingerprint and contacting the website owners (best done by telephone or secure email) to verify it. This may take some time and could be frustrating. Unfortunately, such is the structure of the **SSL** Certificate system on the Internet and the only option we currently have.
There are not that many websites using **SSL** technology. They include some webmail providers, online shopping and other online finance services. You may only ever be accessing 2 or 3 such websites. Prepare yourself by writing or phoning the operators of these websites and recording their **SSL** fingerprints. Thus you will be certain of its authenticity when having to review and accept an **SSL** certificate from their service.

—

If the adversary manages to successfully trick you, he will receive all the information you've input into the website. If it is an email account he has managed to intercept, the adversary will get your login details, and then login to your real webmail himself - a common attack that has claimed many victims on the Internet. It is therefore very important that you understand the procedure of **SSL** certification and know how to protect yourself.

2.8 STEGANOGRAPHY

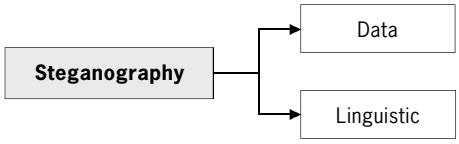
The science or art of hiding the very existence of a message is called steganography. Whereas **encryption** conceals your message by making it unreadable to the outsider, the aim of steganography is to hide the message being communicated. You may have heard of invisible ink or of writing a letter with lemon juice. Those are types of stenography. An early example of it is a secret message, sent from captivity by Herodotus circa 440 BC. He shaved the head of his favourite slave, tattooed the text on his scalp, and waited for the slave's hair to re-grow thus obscuring the message from guards. The same method was used by the German army as recently as in the early 20th century.

—

With the international legislation regulating complex **encryption** getting stricter, we are presented with the problem of upholding the right to the privacy of our information by legal means. Steganography does not try to present an outsider with the task of breaking a complex code, but instead aims to bypass his attention altogether. As there are no specific rules defining the exact nature of a steganographic message, it is very difficult to outlaw (for example, subliminal messages are a form of steganography). Some interesting recent developments in the field of linguistic steganography are discussed in this chapter.

—

There are two main methods of modern steganography. One is data steganography. It relates to hiding a message in an image, a photo, a sound file or 'within other data'. The other is linguistic steganography, i.e. using the language for sending a secret message – by symbols, ambiguous meanings, re-arrangement of letters and other forms of linguistic manipulation. Since linguistic steganography for computer systems is still purely theoretical, our discussion and examples will deal with more traditional message-hiding techniques.



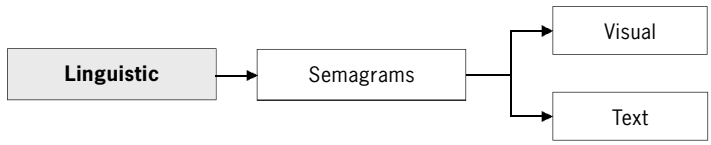
LINGUISTIC STEGANOGRAPHY

Linguistic steganography has been gaining attention in the last couple of years. In itself, it almost constitutes a throwback to computer-assisted hiding and coding techniques, for it relies on the skill in which people are still more proficient than computers – the use and comprehension of language. Comprehension of words, their transformation into meaningful information, detection of humour, symbolism and ambiguities are all still the privileges of the human mind that have no parallels in the computer world. This section will explain different methodologies of linguistic steganography that will allow you to bypass modern technology-based surveillance systems.

Our language is in itself a code that appears incomprehensible to anyone who has not learned it. Computers cannot learn languages, and voice recognition software simply operates by detecting different frequencies in our voices and relating them to pre-programmed equivalents of letters. No matter how hard we try teaching computers to understand the meaning of words, such artificial intelligence (AI) remains a distant reality at present. Another language application that lies beyond computers is symbol recognition, applied by humans when reading. Symbol recognition has been used as a method of security in many webmail registration services (Hotmail, Yahoo) when asking the user to manually input several letters shown to them on-screen. This system, called HIP – Human Interactive Proof, is designed to prevent automatic registration of email addresses by computer programs wishing to create email accounts for sending spam. Such programs cannot recognise letters in a picture. The AI-community knows of many other problems a computer cannot easily solve, simply because no one has yet discovered how to build an *intuition* into its circuits.[61]

Semagrams

Semagrams are used to hide information through the use of signs and symbols. A visual semagram could relate to an arranged code that is transmitted by waving your hand, placing an item in a specific location on your desk or altering the look of your website. These signs are difficult to detect and have the advantage of normality in an everyday world. Sometimes the effective use of visual semagrams may be your only method of communication with your friends and colleagues, and it is important to establish and pre-arrange some messages that may need to be relayed in times of danger.



Text semagrams are symbolic messages encoded through the medium of text. Capitalised letters, accentuation, peculiar handwriting, blank spaces in-between words can all be used as signals for a pre-defined purpose. Subliminal messages also fall into this category. They are sometimes useful when you wish to communicate a small bit of information. For instance, you could agree with your contacts to exchange seemingly innocuous daily weather reports by email. The phrase 'the sky is grey' may serve as an alert meaning you are in trouble and they should mobilise international help.

Open Codes

Open code steganography hides the message in a legitimate piece of text in the ways not immediately obvious to the observer. Computers and humans have different abilities when it comes to steganalysis, or detecting steganographic messages (see below under 'Detection' sub-heading). The following examples may not be applicable to the surveillance carried out by a human steganalyst. They use linguistic variations of the text to fool the common formulas used by electronic filters and surveillance systems. Please bear in mind that these can only be regarded as hints or suggestions to take advantage of the non-intelligent nature of computer systems. They

61
Source: *Classification of Steganography Techniques* (Adapted from Bauer 2002)

should not be used to communicate important information, but only to test the effectiveness of the filtering system. If you know that certain words in your email will result in its failure to reach the recipient and this information alone will not get you into trouble, you can try out some of the variations below.

Misspellings

Since electronic filters are programmed to react to certain words, it is impossible to be sure how many variations of the spelling of a word have been considered. It is possible to retain the meaning of the word with some incredibly advanced misspelling! A phrase like 'human rights' could be also conveyed as:

hoomaine roites umane reites huumon writes

and many more. Whereas this technique is not practical for longer messages, you can reserve it for certain words that you think may have been included in the filtering systems.[62]

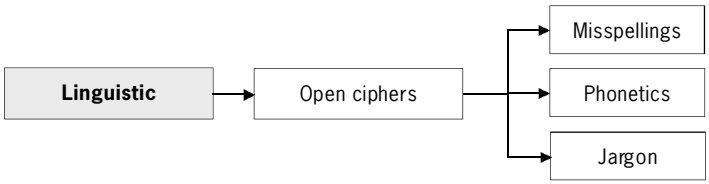
Phonetics

Most in-country filtering systems are aimed at specific keywords in the local language/s. Sometimes they may also include keywords of a popular second language used in the country or on websites (English, French). Again, one cannot be certain as to how exactly the filtering has been programmed, but for ease of understanding and variety, you can apply the phonetic spelling to your message. This could be particularly useful, if you are accustomed to using a script different from the one used in your country (e.g. Latin script for Arabic speakers or vice versa).

Houkok Al Insan حقوق الانسان

Jargon

Using jargon in your messages could render its content meaningless to an outside observer. Prearranged meanings or underground terminology can hide the real contents of the message. It is advisable to choose words in such a way that the carrier message remains legible and comprehensible, if not true. The possibilities of the use of jargon are limited only by the stock of the words known to the communicating parties.



Covered Ciphers

Covered ciphers employ a particular method or secret to hide text in an open carrier message. Sometimes these include simple techniques of embedding a message into the words of the carrier. Consider the example below, sent by the German Embassy in Washington DC to the headquarters in Berlin during World War One:

62
See the OpenNet Initiave filtering country reports for an idea of keywords used in filtering http://www.opennetinitiative.net/studies/

PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY.

APPARENTLY NEUTRAL'S PROTEST IS THOROUGHLY DISCOUNTED AND IGNORED. ISMAN HARD HIT. BLOCKADE ISSUE AFFECTS PRETEXT FOR EMBARGO ON BYPRODUCTS, EJECTING SUETS AND VEGETABLE OILS.

By reading the first character of every word in the first message, and the second character of every word in the following message, you can extract:

PERSHING SAILS FROM N.Y. JUNE 1

The advantage of this method is that the carrier message may also appear as some relevant piece of communication and may not arouse suspicion as to any hidden meanings within it.

—

Another form of a covered cipher is the use of an arranged formula to hide the text in the carrier message. Consider this output for the message 'Please help me' from the website www.spammimic.com

Dear Friend ; You made the right decision when you signed up for our mailing list . This is a one time mailing there is no need to request removal if you won't want any more . This mail is being sent in compliance with Senate bill 2116 ; Title 1 , Section 302 . This is not a get rich scheme ! Why work for somebody else when you can become rich inside 52 WEEKS . Have you ever noticed nobody is getting any younger and more people than ever are surfing the web . Well, now is your chance to capitalize on this ! We will help you SELL MORE and SELL MORE ! The best thing about our system is that it is absolutely risk free for you . But don't believe us ! Prof Simpson of South Carolina tried us and says "Now I'm rich, Rich, RICH" . We are a BBB member in good standing . Do not delay - order today ! Sign up a friend and you'll get a discount of 90% ! Thanks . Dear E-Commerce professional ; Especially for you - this breath-taking news ! If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail . This mail is being sent in compliance with Senate bill 2116 ; Title 4 , Section 302 ! This is not a get rich scheme . Why work for somebody else when you can become rich in 41 DAYS . Have you ever noticed people love convenience plus most everyone has a cellphone . Well, now is your chance to capitalize on this . We will help you deliver goods right to the customer's doorstep & turn your business into an E-BUSINESS . The best thing about our system is that it is absolutely risk free for you ! But don't believe us . Ms Anderson of Hawaii tried us and says "I was sceptical but it worked for me" ! We are licensed to operate in all states ! We BESEECH you - act now ! Sign up a friend and you get half off ! God Bless.

Note: to decode this message, simply copy and paste it into www.spammimic.com/decode.shtml

Here, a spam message is mimicked to relay a hidden one within its content. The spam text is derived from a formula of words that is interchangeable depending on your message. It ensures that the spam is still readable and appears 'authentic'.

—

You can create your own messages that would use a standard format of a typical spam message or other format and agree a specific method of embedding text within it.

Future

The future of linguistic steganography will involve developing software that creates comprehensible text, in which the real message is hidden, using lexicons, ambiguities and word substitution. However, the experts are not yet sure whether computers will be capable of creating meaningful text from scratch and of hiding our messages in it using language semantics and schematics.

DATA STEGANOGRAPHY

The advent of computers has allowed us to begin embedding messages into pictures or sound files. To the human eye, the picture itself remains unchanged, yet within it there could be up to a book's worth of information. I will quickly explain how this is achieved.[63]

Computers, as you may know, operate in binary. That means that every letter and instruction is eventually broken down into a code of '1's and '0's. Let's say that the binary for the letter 'A' is

11101101

Originally, computer architects designed this system in such a way that the very last '1' or '0' had no particular influence on the value of the designated character. If the last number in this message were '0' instead of '1', the computer would still know that this is an 'A'.

11101100

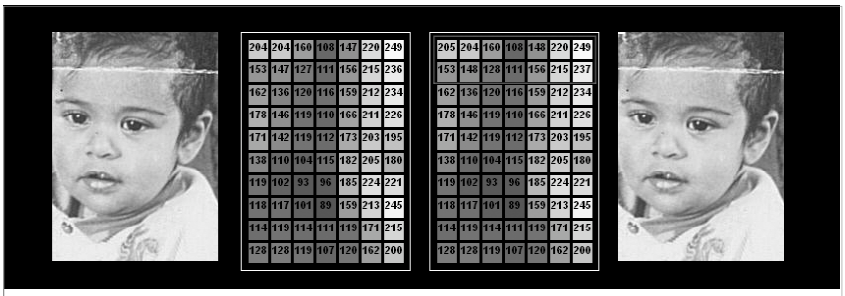
The last digit of all binary messages, which is neither meaningful nor necessary, is known as the Least Significant Bit (LSB). One method, used by data steganography software, is to break up the hidden message between the LSBs of the carrier in a pre-determined pattern. This does not change the original meaning of the message. This method implies that the *hidden message* cannot be bigger than the *carrier* and should really be much smaller.

Hiding in Images

Digital images (those that appear on your computer) are broken up into pixels - tiny dots with a specific colour that together make up the image you can see. For images, steganographers encode the message into the pixel LSB. This means that, to the human eye, the colour of the pixel (represented by binary code to the computer) does not change. The hidden

63
I will refer to the medium you hide your message in as the *carrier*, and to the message itself as the *hidden message*

message can be withdrawn from the picture provided you know: a) that there is a message in the image b) that you use the same steganographic program for decoding as the one used to hide the message.



The carrier image

A fragment from the photo, representing different values of individual pixels

The top two rows of the palette have the word 'OK' embedded into the LSBs

The resulting steganographic image

Source: The Code Book, Simon Singh

Note: Steganographic images are detectable. They do not appear any different to the human eye, but computers, programmed to look for them, can notice slight colour variations when modifying the LSB. It is for this reason that many security experts doubt the practicality of using steganography. If this proves to be the case, other methods, like **encryption**, can also be used. Some programs will not only code your message into an image, but will encrypt it, too. The steganalysts (those responsible for decoding steganographic messages) would still have to break the **encryption** in the message extracted from the image.

Hiding in Audio

Steganography can also be applied to audio files. Take, for example, the MP3 format. It is a method of compressing a natural audio file to a much smaller size. This is achieved by removing the audio frequency that the human ear cannot pick up: our ears can only hear sounds of a particular range of frequency. Natural audio, however, records a much larger frequency, and removing the excess sounds does not significantly change the quality of the audio (to our ears). This is how MP3 files are made. Audio steganography adds the message to the unused frequency in them, and – once again – the human ear is unable to detect the difference in the sound quality.

► Here's a frequency diagram of an audio transcript

► And here is the same piece of audio, with a message hidden within the frequency:

Source: Gary C. Kessler – *An Overview of Steganography for the Computer Forensics Examiner*

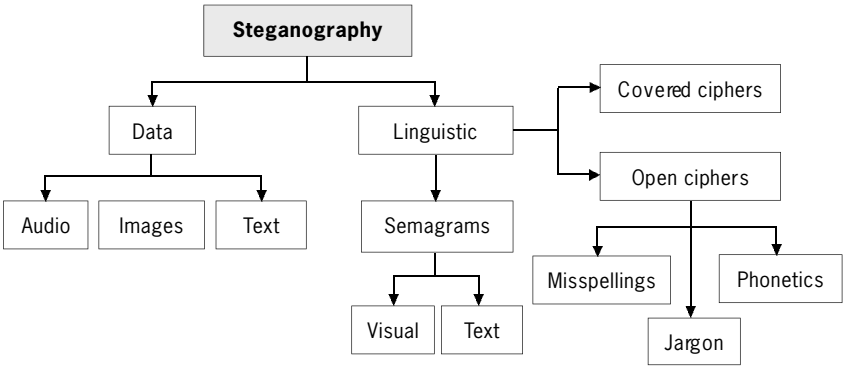
And whereas you may be able to detect the difference by looking at the diagram, it is much more difficult to hear.

Hiding in Text

The steganographic principles can also be applied to a normal text file. Sometimes, this is done by hiding the message in the blank spaces between words. The message is separated between the LSBs of the binary code for the empty space throughout the text. Once again, this method requires the text your are sending to be considerably longer than the message you are hiding within it. You can also hide messages in PDF documents and in a variety of other standards, depending on which program you wish to use.

Steganography software

There exist about a hundred different programs performing data, audio and text steganography. Each one uses it own particular method of arranging your message in the carrier file. Some of the better known are jphide and jpseek (http://linux01.gwdg.de/~alatham/stego.html), mp3stego (http://www.petitcolas.net/fabien/steganography/mp3stego/), as well as the commercial product Steganos Security suite (http://www.steganos.com). You can find many more at http://www.stegoarchive.com/.



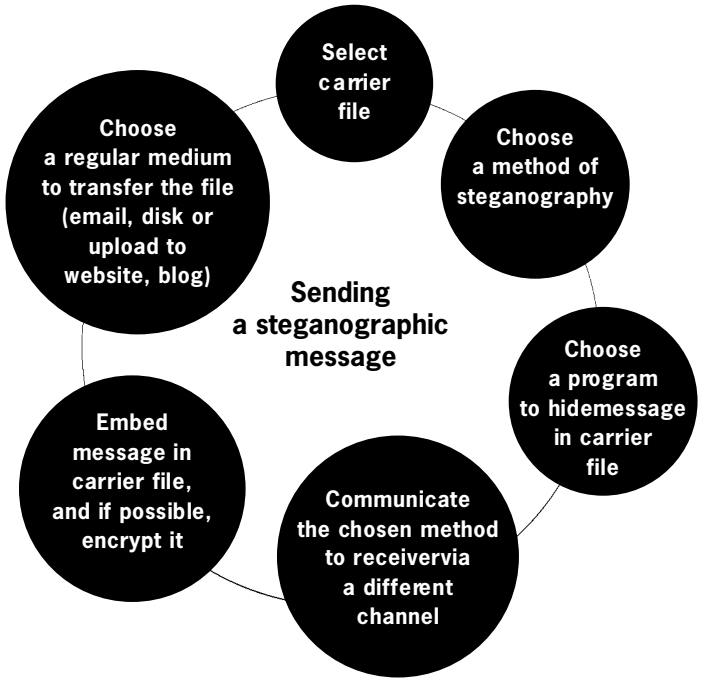
DETECTION

Steganalysis is the process of detecting steganography. Although it is technically easy for computers to detect steganographic content, they must first be configured to look for it. The advantage of using steganography stems from the 'needle in a haystack' principle. Every day millions of images, MP3 files and plain text documents are passed around on the Internet. They do not arouse suspicion and, unlike encrypted messages, are not normally captured for analysis. When sending around photos of your last holiday, you can code a steganographic message into one of the them. Sharing your music collection with a friend presents an opportunity to include a short message in one of the songs. You can imagine the impossibility of scanning huge loads of information transmitted on the Internet for all types of steganographic content.

In the aftermath of September 11, 2001, there appeared articles suggesting that al Qaeda terrorists employed steganography. In response to these reports, attempts were made to ascertain the presence of steganography images on the Internet. One well-known study searched more than three million JPEG images

from the eBay and USENET archives using stegdetect. Only one to two percent of the images were found to be suspicious, yet no hidden messages were recovered with stegbreak. Another study – also using stegdetect and stegbreak – examined several hundred thousand images from a random set of Websites and, obtained similar results.[64]

However, you should always assume that the eavesdropper (surveillance team) knows about the possibility of you hiding your messages. If you have never sent your contact a photo before, why do it now? Because there is a steganographic message in it? The 'needle in a haystack' principle only works if there is a 'haystack'. If you have always shared photos of your holiday or your favourite songs with your Internet contact, then the obscurity of your message increases when just another photo or song is sent. Don't use common or out-of-context images. Don't download images from the Internet and hide messages in them (the attacker could download the same image and compare the two digitally). In short, don't reveal your steganographic practices through an anomaly. Establish a pattern of communication, and use it sparingly for transmitting hidden messages. Do not rely on steganography alone to secure your communications. If the hidden message is revealed to the attacker, they should still be prevented from reading its content. Enhance the security of your message by encrypting it within your carrier file.



The purpose of steganography is to hide the existence of a message so as not to arouse suspicion. Good steganography will employ carrier methods and files that will blend with everyday Internet traffic. Extra security of hidden messages can be achieved by their **encryption**. You may employ one or several techniques described in this chapter, but always operate with the assumption that the attacker is aware of your chosen method and has access to the same programs.

64
Gary C. Kessler – *An Overview of Steganography for the Computer Forensics Examiner*

2.9 MALICIOUS SOFTWARE AND SPAM

ABSTRACT

1 There are many types of malware, transmitted from computer to computer in a multitude of different ways, causing untold damage to information.

2 Install and regularly update your anti-virus, anti-spyware software. Run a firewall and be extremely cautious when opening email or inserting media into your computer.

3 Spam is unsolicited junk email which today constitutes an enormous part of all Internet traffic and has become a huge problem for people and networks.

4 Be careful with distributing your email address and never reply to or even open spam messages.

Malware is a term used to describe software that damages your computer and compromises your security and the confidentiality of your information. It can be broken up into several categories, including viruses and spyware. Millions of computers around the world have been infected by a virus or spyware, causing huge problems in the industry. The Internet has become the most widely used medium for spreading malware, and we are always battling to protect ourselves from myriads of old and newly written malicious infections. The word 'spam' is used to describe undesired and unsolicited email messages, sent in bulk around the Internet and to our email accounts. This chapter will explain the differences between various types of malware, the history of famous infections and will provide assistance as well as a guide to how to protect against them.

VIRUSES

Similar to a human virus, computer viruses infect computers and other technical devices with the intent of changing their stability, operation or integrity. They are usually small pieces of software code that are executed on your computer following a specific action you take. They also have a tendency to re-create and multiply. You can receive a virus in an email, on a inserted floppy disk or other removable media, by browsing to specific websites and sometimes just by being connected to the Internet.

History

The first recognised instance of a spreadable computer virus was the Elk Cloner. It was written around 1982 by a 15-year-old high school student Rich Skrenta and was aimed at Apple II systems. Elk Cloner spread by infecting the Apple II's operating system and was transmitted on floppy disks. When the computer was booted from an infected floppy, a copy of the virus would automatically start. Whenever a new floppy disk was inserted into an infected computer, the virus copied itself to it, thereby allowing itself to spread. It did not cause specific harm to the computer, but was merely an annoyance. On every 50th booting, the virus would display a short 'poem':

```
Elk Cloner:  The program with a personality

  It will get on all your disks
    It will infiltrate your chips
      Yes it's Cloner!

  It will stick to you like glue
    It will modify ram too
      Send in the Cloner!
```
[65]

The first virus to infect a PC was called (c)Brain and was written by Basit and Amjad Farooq Alvi, two Pakistani software developers. They wanted to stop the piracy of the medical software they had written and claimed that the virus only existed to prevent breach of copyright.

—

Originally, viruses were spread by floppy disks inserted into various computer systems. The Internet has provided a new means of spreading viruses around with the greatest of ease. The first well-known case was the Morris Worm, written by Robert Tappan Morris in 1998. It was estimated to have infected around 6,000 computers worldwide[66] and caused between 10 and 100 million USD of damage. Morris received 3 years of probation and had to pay 10,000 USD in fines. The devastating effect the virus had on the Internet led to the creation of a new industry for countering similar attacks and resulted in the formation of CERT (Computer Emergency Response Team), a US federal-funded research institute and development centre (http://www.cert.org).

—

The month of August 2003 was the worst ever for damages from viruses - the result of a simultaneous attack from the Blaster and Sobig worms. Causing untold damage around the world, it severely crippled Internet speeds. The writer of the Blaster virus, 18 year-old Jeffrey Lee Parson from Minnesota, was eventually caught and jailed for 18 months. The MyDoom virus of 2004 accounted for 1 in 12 of every email sent on the Internet and was able to co-ordinate the biggest **denial of service attack**[67], involving more then 1 million computers from all over the globe.

MALWARE VARIATIONS

There are numerous types of malware, and each has a specific method of operation and distribution.

—

■ **A virus** is a piece of computer code that damages the software (and increasingly the hardware) of your PC, with possible effects of data loss or computer malfunction. Viruses must be executed (run or opened) by the user and can replicate themselves to infect other computers.
Infection: viruses come as email attachments, files loaded from floppy disks or other removable media. Files that could contain viruses usually (but not always) have the following extensions: .exe .com .bat .vbs .php .class .jbs .scr .pif
Solution: Use anti-virus software and update it frequently. Install a firewall and never open unknown attachments to email. Always perform a full scan of any removable media you insert into the computer. If your organisation has a computer network, it is advisable that you remove the computers,

65
Wikipedia
http://en.wikipedia.org/wiki/Elk_Cloner

66
Government Accountability Office – www.goa.gov

67
see Glossary

connected to the Internet, from it: upon infection, the important documents on your network will not be damaged then.

■ **A worm** – is similar to a virus but the former does not try to delete or corrupt information on your computer. Worms usually come embedded in an email message. They exploit security vulnerabilities in operating systems and spread themselves to other computers via the network or the Internet.
Infection: worms infect your computer as soon as you open the email message in which they are hiding. Your computer could also be sending and receiving worms by simply being connected to the Internet.
Solution: use anti-virus software and a firewall. Install all necessary operating system updates (see Windows chapter). Be extremely vigilant when opening email and disable the preview screen in your email program[68]. Do not open email from unknown, untrusted sources. In reality, it is quite difficult to prevent the spread of newly written worms.

■ **A macro virus (or a macro)** – takes advantage of the Microsoft Office products, which allow the user to create a small program within a document to automate a specific function (e.g. to perform a calculation in Excel). If you open a file that contains a macro virus, it will infect the program and all documents you open with this program later.
Infection: macros are hidden in MS Office documents, such as .doc .xls .ppt .mdb. They become operational when you open such a file.
Solution: You can disable macros in your MS Office applications. This option is presented to you every time you open a document that contains macros.

►A warning of a macro inside an Adobe PDF document

Always choose to 'Disable Macros' in your document. In your organisation, introduce a policy of saving all Word files in Rich Text Format (.rtf) and all Excel files as .csv. These file types do not carry macros.

■ **Trojans** (Trojan horses, backdoor Trojans) are programs posing as legitimate software but actually containing malicious code. They do not replicate themselves but can force your computer to download a virus.

68
If you can see the content of the email in your main program screen, you have the preview pane switched on. To disable it in Microsoft Outlook: go to the menu bar and de-select View > Preview Pane.
In Outlook Express: go to the menu bar View > Layout. In the Layout window de-select the option 'Show Preview Pane'.
In Mozilla Thunderbird go to the menu bar View > Layout and de-select 'Message Pane' or simply press F8.

Backdoor Trojans can give full access to your computer to an outsider. They could give an attacker access to all your programs and documents. Some Trojans record all your keystrokes and send this information to a pre-determined address. This is a common method of obtaining passwords.
Infection: Trojans pose as legitimate programs and become active when you execute them. Sometimes viruses install Trojans on your computer.
Solution: use anti-virus software and a firewall. Install all necessary operating system updates (see Windows chapter).

■ **Spyware** are malicious programs that track your movements on the computer and the Internet and send this information to an outsider. The main aims of spyware are to undermine the computer's security and to reveal information about its user for reasons of profit or gain.
Infection: Spyware can appear in emails and come embedded in programs you install. You can receive spyware by visiting web pages (especially relevant to Internet Explorer) or using file-sharing software. They can come in email attachments or get installed with a virus.
Solution: There exist numerous anti-spyware programs and some of them come automatically when you install a virus cleaner. It is advisable to have several spyware detection programs. Programs like Spybot will detect if the spyware is trying to dial an unauthorised number or make changes to the computer registry. Don't install unnecessary programs or those the reputation of which you cannot verify.

—

Viruses are known to be spreading to mobile phones and personal organisers. Technically, any electronic medium with a processing unit can be infected by a virus. Virus hoaxes have also gained notoriety because of their crippling effects on companies and users. They are usually spread by email and warn you of an impeding new virus attack. They may also try to persuade you to click a link in the email, which will 'help you to secure your computer system'. Albeit not terribly damaging, virus hoaxes slow down the Internet connection and fill email boxes with unnecessary email.

—

An organisational policy that pro-actively prevents downloading and executing of viruses is required. Some of it can be done at the program level, by setting specific settings to make your programs more robust against viruses and by obtaining and running anti-virus, anti-spyware and firewall software. All software, including fixes for Windows, must be actively sought and updated. This will increase your protection against newly written malware. The main approach to tackling malware is at the policy level.

You need to:
- keep a backup of your important documents on removable media
- block all malicious email attachments at your server or program level
- never open any email attachments that you are not expecting and those originating from unknown sources
- run a full scan of your system at least once a week
- do not download unnecessary programs onto your computer. MSN and Yahoo Chat programs are popular targets for spreading viruses. Try to refrain from using these programs and file-sharing software on your work computer.
- stay informed about the latest threats

If your computer is infected with a virus:

- Disconnect it from the Internet and from any networks immediately.
- Close all programs and run a full anti-virus scan. Some programs allow you to schedule a boot scan which will check your entire computer upon restart. This is useful as some viruses hide in files that Windows cannot check when it is running. Delete any viruses found and write down their names. Then run the scan again, until you have no more warnings.
- Connect to the Internet and obtain the latest information on the particular virus you have received. You can check www.symantec.com or www.sophos.com or www.f-secure.com for the latest information about viruses, the damage they can cause and methods of their detection, prevention and deletion. Update your Windows operating system with any necessary patches.
- If a virus is found on a computer that resides in a network, disconnect all computers from the Internet and then from the network. All users should stop working, and the steps listed above must be taken for every computer. This may sound like an exhausting process, but it is an absolute necessity.

The most important rule is to be aware and vigilant. Take the required precautions but do not let the existence of anti-virus or anti-spyware programs give you a false sense of security. As you might have guessed from the above, it is a never-ending battle. Viruses spread not because of their clever programming, but because of the carelessness and nonchalance of the user.

SPAM

Spam is the process of sending bulk and unsolicited emails. They normally take the form of advertising or nonsense messages that often fill up our email boxes. Spam is an activity aimed at increasing the profits of

companies, and increasingly of spam gangs. It is a lucrative method, for the costs of mass distribution are minimal - far cheaper then postal junk mail and other means of mass advertising. Spam now accounts for 50% of all Internet activity and is an enormous problem to individuals and to businesses. This section will tell you how to reduce the amount of spam in your email box.

—

Many on-line companies provide lists of their customers' email addresses to organisations specialising in sending unsolicited commercial email (spam). Other companies mine email addresses from messages posted on mailing lists, newsgroups, or domain name registration data. In a test by the US Federal Trade Commission, an email address, posted in a chat room, began receiving spam within eight minutes of submitting a post[69].

History

The term *spam* is derived from the British comedy series 'Monty Python'. One of the episodes, 'SPAM Sketch', is set in a café where everything on the menu includes SPAM luncheon meat. As the waiter recites the SPAM-filled menu, a chorus of Viking patrons drowns out all conversation with a "SPAM, SPAM, SPAM, SPAM" refrain thus 'SPAMming' all other noises. The obsession with SPAM goes back to food rationing in Britain during and after World War II. SPAM (a ham substitute made from processed meat) was one of the few foods that was not restricted and was widely available, so by the end of the rationing period the British had been rather fed up with 'luncheon meat'.[70]

—

The concept of spamming as an advertising technique was first introduced in 1994 by two New York immigration lawyers wishing to promote their services through mass emailing. They argued it was a viable and justified new method of marketing and labelled their critics as "anti-commercial radicals". Since then, the popularity of 'spamming' grew very quickly.

Preventing spam

There are several methods of reducing the amount of spam you receive, although you may never be able to get rid of it completely. If you are using a webmail account (like Hotmail or Yahoo), the provider should have automatic spam filtering software installed. Some email programs (like Mozilla Thunderbird) have a built-in spam filter that learns what email you would classify as spam, and stops similar emails from cluttering up your inbox. Be aware that spam keeps being downloaded, but is automatically moved to the Junk folder.

—

The main method of spam prevention is not to reply or to click on any links in the spam message. Even if you are upset by the amount of spam and wish to reply to the message with a complaint or a request to stop the spamming, you are simply confirming the existence of your email address and labelling yourself as someone who reads spam and reacts to it. Never purchase anything advertised in spam messages. Even if it is legitimate, you'll end up further funding the spammer market.

Do not list your email address on any websites or list servers. If this is not

69
Privacy International – Privacy and Human Rights Report 2004
Threats to Privacy

70
Wikipedia
http://en.wikipedia.org/wiki/Spam_%28electronic%29

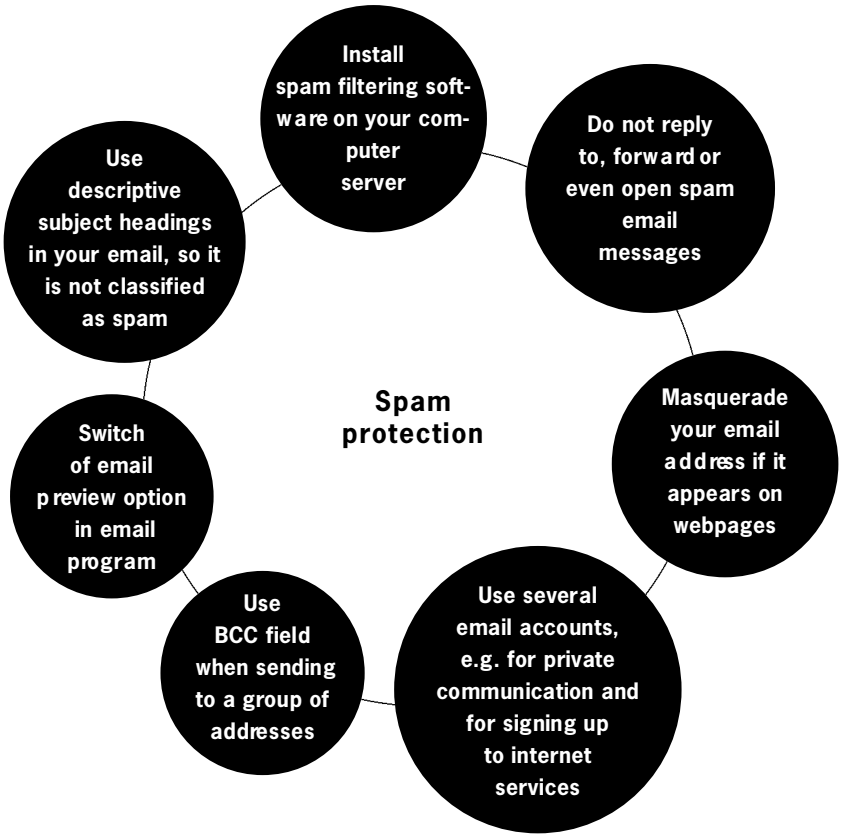
possible, disguise it by putting # or 'at' instead of using the normal @ symbol. This will prevent web-spiders from capturing your email addressing

`user#frontlinedefenders#org  user AT frontlinedenfeders DOT org`

If you are sending a large group email, insert the contacts into the '**Bcc**' field. This will hide the existence of the mass email and prevent spammers from using the list for their purposes. Also, switch off the email preview option in your email program. When an email is previewed, it may alert the spammers that your address exists and you have read the message.
Try to use several email addresses. One will be your private email which you will give out only to trusted contacts. You can use other addresses for registration and authentication when on the Internet. Thus you will be able to separate private email accounts from those that get spammed.

—

If your account is already facing massive spamming and the filters are simply not working any more, you have no other option but open a new email account and be more vigilant.



2.10 IDENTITY THEFT AND PROFILING

ABSTRACT

1 Your digital identity is a collection of computer and Internet records that either relate to you or could be used to identify you.
2 A digital profile can be used to make certain assumptions about your buying habits, character, political or social affiliations.
3 A digital profile can be faked, stolen or modified, and all systems that depend on this profile will function according to the new data.
4 Your presence on the Internet should be a well-thought-out balance of open and anonymous actions.

This chapter deals with preserving and securing your digital identity on the Internet. It explores some topics already covered in the Manual. You will need to study them first before proceeding with this section. Stealing of one's identity has become a common crime in the modern world. Carried out primarily for financial benefit, identity theft has resulted in untold financial and moral damage to the victims. It can also be committed out of malice or for political gain. The Internet presents an ideal location for thieves wishing to assume someone else's persona. The digital domain, where we are routinely recognised by our email address, password or chat account, is removed from the natural world of recognition by sight, voice and touch. If the digital information we supply is faked by an outsider, it is difficult to verify the true identity of the sender.

—

Profiling is one of the steps involved in discovering someone's identity and habits. A history of your Internet browsing and email communications can reveal important information about yourself to an attacker or a spam sender. Many companies, including Internet Service Providers (ISPs), search engine firms and web-based businesses. They also monitor users as the latter travel across the Internet and collect information on the sites they visit, the time and length of these visits, the search terms they enter, the purchases they make, or even on their "click-through" responses to banner ads. In the off-line world this would be comparable to having someone follow you through a shopping mall, scanning each page of every magazine you browse through, every pair of shoes that you look at and every menu entry you read at the restaurant. Combined with other information, such as demographic or "psychographic" data, these details add up to highly detailed profiles of individuals. Such profiles have become a major currency in electronic commerce where they are used by advertisers and marketers to identify users' preferences, interests, needs and possible future purchases. Most of these profiles are currently stored in an anonymous form, yet in the future they could be easily linked with names and addresses, gathered from other sources and making them personally identifiable.[71]

PROFILING

After the 9/11 attacks, the US Federal Aviation Administration tried to start profiling all passengers who had boarded a plane in the country. They

71
Privacy International – Privacy and Human Rights Report 2004
Threats to Privacy

collected lots of social, personal and financial data to single out potential terrorists. The people marked out by such profiling, were meant to undergo more extensive bag and body searches. Enormous amounts of money went into developing the system, and some laws were modified for its sake. The method, however, was flawed from the beginning, and would-be terrorists could easily beat it by simply finding in their ranks the people who were not singled out by the profiling by sending volunteers on flights and picking up those whose profiled background did not seem to alarm the authorities. Those could then be designated hijackers without the risk of extensive scrutiny when boarding the plane[72].

—

This is just one example of how governments try to use surveillance systems to control people through profiling. Their logic is that when a person's identity is known, certain assumptions may be made about his/her abilities, motivations and socio-political attitudes.

—

If previously profiling systems were mostly used in finance and insurance industries, now we can see them being increasingly applied to our personal lives, particularly in the states that do not wish to stick to the internationally recognised principles of human privacy.

—

Profiling in the interests of global or national security remains a controversial issue. Targeted profiling to identify a person or a group on the basis of certain assumptions would constitute a breach of the legitimate and universally accepted privacy right. And although digital profiling is not yet practised in the countries with under-developed digital infrastructure, it is important to know what the future holds for them.

—

Profiling is an emerging business for private companies. Cyber Trace[73] offers its clients the services of a partner's marital faithfulness check, with evidence to be used in a divorce court. They services invite their customers to look for incriminating information by watching their colleagues' online activities. The ability to collect and collate digital data is a powerful resource for conducting investigations, evaluations of a person or company and making accusations against them.

—

The American newspaper 'Chicago Tribune' was able to identify 2,653 CIA employees by simply searching through fee-paying data-mining websites[74].

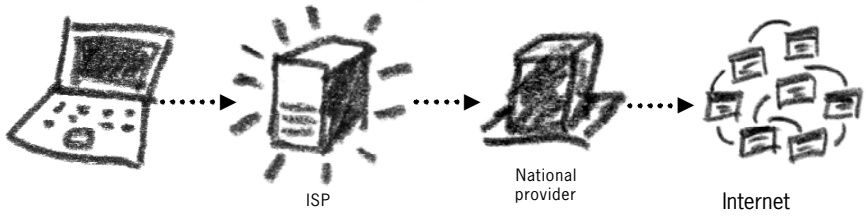
Digital Profile

Your presence on the Internet can be identified by several factors, some of which you can control and some cannot. These factors are integral to the way the Internet currently operates. Your computer is identified by an IP address. The Internet Protocol address is a unique number that is assigned by your server or **ISP** when you connect. It can either be static (always the same) or dynamic (assigned to you from a pool of addresses, see 'Appendix B – Internet explained' for more details). If you are connecting to the Internet through an **ISP**, your IP address will usually come from a range that has been purchased by the **ISP**. Therefore, your computer may at first be traceable back only to the **ISP** and then, depending on the time of connection, to you, too.

72
Carnival Booth: An Algorithm for Defeating the Computer-Assisted Passenger Screening System by Samidh Chakrabarti and Aaron Strauss

73
http://www.cyber-trace.info

74
http://news.bbc.co.uk/1/hi/world/americas/4799174.stm



► You can be identified on the Internet by many distinguishing factors

Whenever you browse to a website or send an email, your IP address and time of access are recorded by the website or email server that receives your request. This data is usually stored for a long time. In many countries laws have been passed to demand that it is collected and made available to the authorities whenever necessary. Since a government cannot always have access to every website in the world, the data is often collected and passed on by the **ISP** that connects you to the Internet. If you only connect to the Internet from one computer using the same **ISP**, it is possible to have a record of your entire Internet browsing history. This could include all news sites and articles you have read, all organisations whose websites you have visited, all email addresses you have written to, etc. To prevent Internet anonymity, some countries (e.g. Tunisia, Syria) have passed legislation forcing public computer centres (Internet cafés and libraries) to record all their customers' names and time of use. This way your browsing history can be traced back to you personally even if you use a public computer.

Cookies

Whereas cookies are primarily collected for marketing (and spam) purposes, they also create a distinct trace of your activity on the Internet which can be found at the website itself, at the **ISP** and on your computer. See 'Internet surveillance, filtering and censorship' chapter for more on cookies.

DIGITAL IDENTITY

You are identified on the Internet by the current IP address of your computer, as well as by the email address and the name associated with it. Together, these can be used to identify or monitor your activities, to create a profile that will describe your interests and circle of contacts, to be presented as evidence in court or to be falsified to assume your digital identity for a malicious purpose. The **ECHELON** system was created specifically for collecting and profiling as much information on the Internet users as possible. The majority of countries collect and store all the browsing and email data of their citizens.

—

A huge problem with the system of Internet authentication is that all the identifying features we have spoken about can be faked. In other words, an experienced user (or hacker) can falsify his IP address and email account to match yours. It is entirely possible for you to receive an email with an address that has the appearance of originating from your own computer and sent from your non-existent email account. By digging deeper into the coding of the message and using other information resources, we can uncover the real identity of the sender, but not many of us possess the necessary expertise in digital and Internet forensics. Only a few organi-

sations and lawyers are now ready to face up to the fact that an email addresses and IP do not constitute fool-proof methods of identification. The majority of countries do accept the validity of a digital identity derived from the above.

—

Take an Internet chat. When chatting, you assume that the other party is the owner of the account. This can be your friend or colleague. In contrast to telephone conversations, you do not have the advantage of recognising the other party's voice. Since Internet passwords can easily be stolen or compromised, an Internet chat becomes dangerous when your adversary could easily assume your friend's identity and thereby receive important information from you. It is quite difficult to electronically determine the interlocutor's true identity in an Internet chat. Here we must resort to using standard means of identification, by revealing pre-arranged or personal details, only known to the two parties, to each other. You could prepare a secret word or a phrase to be shared upon initiating a chat, or surprise the other party by asking a personal question, to which only the two of you know the answer. However, even this information can be compromised, especially if you do not use a secure chat client. The best solution for security and privacy in an Internet chat is not to reveal any sensitive or compromising information.

AUTHENTICITY

Digital signatures were created as an answer to the uncertainty of Internet-based authentication. They employ **encryption** to record the contents of your message and your identity, secured by a strong pass phrase. If the message is tampered with, the digital signature will become corrupt and the receiver will be made aware of the message's invalidity. When you have implemented a good system of public key **encryption**, your digital signatures will be of utmost value in authenticating your message to the recipient, or his/her message to you.[75]

—

Do not trust the authenticity of an email if you cannot verify the sender by other means. Amnesty International recognises this problem, and all its email communications carry a disclaimer at the bottom:

> *"..Internet communications are not secure and therefore Amnesty International Ltd does not accept legal responsibility for the contents of this message. If you are not the intended recipient you must not disclose or rely on the information in this e-mail.."*

If the email you are reading contains important information and cannot be verified by a digital signature, pick up the telephone or contact the sender by some other means to confirm the details in the email. This probably makes the whole email process irrelevant, but it also confirms one of the main messages of this book: do not over-rely on technology if privacy is a concern.

ANONYMITY

Our privacy, it seems, gets more and more undermined. Governments force their citizens to carry passports at all times. In the aftermaths of the recent terrorist attacks in the US and Europe, the countries that used to take the

75
see 'Cryptology' chapter for more details

issue of their citizens' personal IDs fairly lightly, are making legal provisions for reinstating their importance. The UK continues to debate the introduction of ID cards, with heaps of personal information, for all its citizens. Our movements around the world can be traced from airline tickets, bank records, car registration numbers, mobile phones and Internet email accounts.

—

Large corporations that provide Internet services are turning into data-mining warehouses. They hold records of our personal information shared when using their services. Increasingly, these corporations collude with governments giving the latter access to our personal data. One eye-opening example was the jailing of Shi Tao, a Chinese journalist, and LI Zhi, a former official, after Yahoo allowed the Chinese government access to their email accounts.[76] Currently there are 48 people in Chinese prisons convicted as a result of their criticism of the government on the Internet.

—

It seems that our right to privacy on the Internet can now only be achieved by anonymity. Since businesses and governments do collect information to profile us from it, we cannot rely on their goodwill not to use it illegally, i.e. in breach of our rights. And although some progress has been made towards developing anonymous Internet systems (these are described in the 'Internet Surveillance, Filtering and Censorship' chapter), we must keep coming up with our own methods of obscuring, and thereby securing, our digital presence.

—

Imagine the Internet with no anonymity whatsoever. Everybody's personal data is available for inspection and scrutiny. One cannot publish an anonymous **blog** or article for fear of reprisals from those who do not share the writer's point of view or do not want it to reach a wider audience. You cannot read a website, classified as 'subversive' or 'inappropriate' by your country's legislation. In such a censored world, every imaginable restriction of our privacy and freedom of expression can be easily implemented.

—

You can achieve relative anonymity by registering an obscure email address with a random account name. It is best that you do this from a public computer (for example, in an Internet café or a library). If you choose a widely used service, like Hotmail or Yahoo, you are sharing a user base with millions of others. An email address of 123random@hotmail.com will not immediately give away as much information about you as, say, dmitrivitaliev@hotmail.com If this account is registered under the name of 'Someone Random', the latter will appear in the 'From' field for the recipient. Do not include your name anywhere in the email message. Do not write details that could directly pinpoint your true identity. You must make arrangements with the party you wish to contact, so that they will know the email is from you. Even though these tricks do not offer the security of **SSL** or of message **encryption**, they make messages difficult to trace to a particular sender. Your email will only be identified by the IP address it originated from and the time of sending.

—

Do not reveal the identity of others through carelessness. If you are sending a group email, think whether it is essential that everyone sees the email addresses your message is going out to. Also, consider the possibility that

76 Reporters sans frontières Annual Report 2006, Internet

your adversary can obtain a copy of the message and realise the relationship among the recipients. In most cases, putting yourself into the 'To' field and the recipients into '**Bcc**' (Blind Carbon Copy) will protect group email addresses from each other and from any adversary monitoring your communications.

—

When you receive an email that you want to forward, only do so after considering whether the original sender wants to be known to the people you are forwarding the message to. In some cases, it is better to copy the contents of the email and compose a new message.

—

When browsing websites, pay attention to how your activity can be monitored. If you wish to dispel concern over your browsing to undesired websites (however those may be defined in your country), you should only look at them from public computers and preferably whilst using an anonymity network or anonymous proxy servers. If you do not want the websites you visit to collect identifiable information on you, apply similar methods and make relevant changes in your browser to deny the downloading and setting of cookies.[77] Do not relax in this approach by browsing to an illegal website from your unprotected office computer 'just for once'. Computers never relax, and the data once created do not just disappear.

Steps to preventing profiling

- Do you need to sign up for a particular service or newsletter?
- Some countries allow purchasing top-up credit for mobile phones. This is sometimes a better option for anonymity, as opposed to initiating a contract where all your details are listed and linked to the phone number.
- Try and profile yourself and your organisation. See how much potentially damaging information is openly available.
- Do a threat assessment with your colleagues to determine how much information is liable to be lost to successful profiling. Implement policies to defend your organisation against it.
- Do not reveal any personal or potentially sensitive information in a telephone conversation.

On Computers and Internet

- Do not create passwords which use information from your personal life
- Do not use real names in creating email and other online accounts
- Pay attention to which websites you visit and how you connect to them (e.g. through a proxy)
- Do not disclose any personal information in an insecure email or an Internet chat.
- Install a firewall and anti-virus/spyware software
- Try not to send group emails and when you do, use the **Bcc** field for all addresses.

77
see 'Internet Settings' chapter for more details

3.0 CHANGES TO LEGISLATION ON INTERNET PRIVACY AND FREEDOM OF EXPRESSION AFFECTING THE WORK AND SAFETY OF HUMAN RIGHTS DEFENDERS AROUND THE WORLD[78]

This section will deal specifically with current laws undermining the legitimate and important work carried out by human rights defenders – as applied to the digital world. We'll focus on direct and indirect effect of these laws on security and safety of HRDs.

The Internet has ushered in a new medium for global communication and learning. The majority of the world's governments are aware of its economic and social potential. And whereas most of them are keen to capitalize on the new global market, some are wary of the impact the Internet may have on stability and survival of the ruling regimes.

—

According to current estimates, around 750 million people on our planet use the Internet – fewer than the population of China or India, yet the number of users keeps growing exponentially. In many countries, the Internet infrastructure is improving, connection costs are going down, and new wireless technologies promise to bring the Internet into every home in the foreseeable future.

—

The Internet crosses administrative and geographic boundaries with the ease and speed never seen before. It provides a pioneering method of communication, in which one's voice can be heard simultaneously by all those connected. As opposed to traditional media, where information is sourced, rationed, edited and summarized – on the Internet people choose what they want. They are not fed political propaganda, celebrity news or sports round-ups unless they choose to be exposed to those. Users select what they want to read, who they want to communicate with and which truth is the real truth for them. Unsurprisingly, this has caused a major problem for the countries wishing to maintain political, social and religious freedoms of their citizens within their governments' grasp.

—

The Internet's open infrastructure serves to promote the Universal Declaration of Human Rights (UDHR), especially freedom of expression, assembly and association (article 19). In his Report to the U.N. Commission on Human Rights of January 29, 1999, Special Rapporteur on the protection and promotion of freedom of opinion and expression Abid

78
Facts and quotes in this chapter have been borrowed liberally, with permission, from the Privacy and Human Rights report 2004 published by 'Privacy International' www.privacyinternational.org; Facts and quotes in this chapter have been borrowed liberally, with permission, from the Reporters sans frontières website www.rsf.org

Hussein observed that "while perhaps unique in its reach and application, the Internet is, at base, merely another form of communication to which any restriction and regulation would violate the rights set out in the Universal Declaration of Human Rights and, in particular, article 19." He further argued that:

> *"As regards the impact of new information technology on the right to freedom of opinion and expression, the Special Rapporteur considers it of pre-eminent importance that they be considered in the light of the same international standards as other means of communication and that no measures be taken which would unduly restrict freedom of expression and information; in case of doubt, the decision should be in favour of free expression and flow of information. With regard to the Internet, the Special Rapporteur wishes to reiterate that on-line expression should be guided by international standards and be guaranteed the same protection as is awarded to other forms of expression."* [79]

The rise of Internet Communication Technologies (ICT) has also highlighted the issues of privacy. As we move more of our information and communications over to the digital world, we are confronted by governments and corporations wishing to collect, process, analyse and control this data. It includes the websites we visit, our emails, travel destinations, personal finances and medical history, memberships of political or social movements, religious associations and so on. Whereas this practice of privacy invasion is certainly not new, our over reliance on modern technology and its surveillance-friendly structure has made these threats to our privacy easier to implement. The UN itself has fallen prey to these problems. At the 2003 First World Summit on Information Technology (WSIS) in Geneva (the Second Summit was held in Tunisia in 2005) all participants were issued with identity cards, into which – unbeknownst to the delegates – a radio frequency identification chip was built in. The chip could be used to record the participant'smovements and contacts during the Summit.
The 9/11 bombings in 2001 had a negative effect on privacy laws causing the countries that had not yet implemented (or even discussed) the need to develop monitoring and surveillance technologies, do so.

> *''The immediate period after September 2001 was a time of fear, flux and uncertainty. The United Nations responded with Resolution 1368 calling on increased cooperation between countries to prevent and suppress terrorism. NATO invoked Article 5, claiming an attack on any NATO member country is an attack on all of NATO; legislatures responded accordingly. The Council of Europe condemned the attacks, called for solidarity, and also called for increased cooperation in criminal matters. Later the Council of Europe Parliamentary Assembly called on countries to ratify conventions combating terrorism, lift any reservations in these agreements, and extend the mandate of police working groups to include "terrorist messages and the decoding thereof."* [80]

In October 2001, the US House of Representatives ratified the Act to Provide Appropriate Tools Required to Intercept and Obstruct Terrorism ("the USA-Patriot Act"). It empowered the FBI to install the online surveillance system, known as CARNIVORE (later as DCS 1000), at all ISPs. In 2003, the US Congress removed the need for investigative teams to

79
Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression to the U.N. Commission on Human Rights, January 29, 1999, E/CN.4/1999/64.

80
Privacy International – Privacy and Human Rights Report 2004 – The Threats to Privacy

obtain warrants in procuring personal data about the Internet users and separate websites[81]. After that, General Ashcroft granted the FBI the authority to gather information on the Internet users outside official investigations and to initiate online surveillance on the basis of a priori suspicion. Originally passed as a temporary law, this Act was made permanent in the aftermath of the London bombings in July 2005.

—

In contradiction to its own Constitution, Australia quickly followed suit. According to the Preamble to the Australian Privacy Charter, "A free and democratic society requires respect for the autonomy of individuals, and limits on the power of both state and private organizations to intrude on that autonomy. ...Privacy is a key value which underpins human dignity and other key values such as freedom of association and freedom of speech... Privacy is a basic human right and the reasonable expectation of every person."

—

Despite the above and following the Bali attacks of 2003, the Australian Government introduced laws that required all ISPs to voluntarily collect and monitor the data passing through their servers, urge the users to disclose their **encryption** keys and take part in the US-led **ECHELON** global surveillance project. The government then granted its agencies powers to intercept and read email, SMS and voice-mail messages without a warrant (as proposed in the Telecommunications Interception Legislation Amendment Bill of 2002) on the grounds that such communications, allegedly, constituted "access to 'stored' data" rather than the information 'intercepted' in real-time.

—

Some governments regarded every terrorist incident as opportunity further to enhance their powers. In Russia, a number of new government powers were introduced with little debate in the wake of terrorist attacks. Those included harsher penalties and bans on media coverage of terrorist activities. After the July 2005 bombings in London, France and Italy began collecting DNA samples from immigrants.

Cuba listed "hacking" as an offence in its new anti-terrorism law; Colombia legitimised interception of private communications, related to terrorism, without judicial approval; India passed the Prevention Of Terrorism Act (POTA) which gives the police sweeping powers to intercept communications; Jordan amended its Penal Code to include Article 150 imprisonment for anyone who publishes "a story, speech or act in any way that offends national unity, stirs people to commit crimes, implants hatred among members of society, instigates sectarianism and racism, insults the dignity and personal freedoms of individuals, promotes fabricated rumours, incites others to riot, sit-in or organize public gatherings that violate the laws of the country."; The Netherlands agreed to a legislative proposal that enables a public prosecutor to request traffic data from providers of public telecommunications networks and services and passed a special decree to allow wiretapping of lawyers; Singapore amended the Computer Misuse Act to allow its authorities to launch pre-emptive actions against suspected hackers based on "credible information" linking the suspects to planned attacks on sensitive information networks.

—

Those are but a few sweeping measures to increase the governments' ". We did not mention the practices of intelligence agencies, operating outside the

81
In January 2005 it emerged that the FBI was no longer using Carnivore, and instead switched to an unspecified commercial softwareapplication

existing laws and involved in illegal wiretapping, intercepting email and stealing information from personal computers. In March 2006, it transpired that the Bush administration planted thousands of wiretaps on private phones without a permission from the Congress. The rationale behind this decision was that the president's powers and the need for security outweighed the necessity to operate within the existing law.

—

The issue of the power abuse, supported by legislative changes, is particularly topical in the countries without a fair judicial system and independent regulatory bodies. The majority of people realise the need to fight terrorism, but are nevertheless surrendering their personal freedoms and their rights to privacy and confidentiality without thinking of consequences.

—

To quote a general comment on the right to privacy by the United Nations Human Rights Committee, the body that is an authorised to interpret state duties under the International Covenant on Civil and Political Rights:

> *"As all persons live in society, the protection of privacy is necessarily relative. However, the competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant. [...] Even with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorized interference must be made only by the authority designated under the law, and on a case-by-case basis. [...] Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited."*[82]

Bangladesh, Zimbabwe[83], Pakistan, China, Vietnam and a number of other countries granted government agencies sweeping powers to access all Internet and email traffic at the latter's discretion. Multinational Internet corporations are ignoring international standards on privacy. They cooperate with governments by providing personal user information stored on their servers.

—

Negating the rights to privacy and freedom of expression became a general tendency in many parts of the globe. Technology is being used to monitor individuals – be they on the street or on the Internet. A peculiar reasoning behind this approach was summarised by one Indian policeman: "If people aren't doing anything wrong, why should they worry about privacy".

82
United Nations Human Rights Committee, General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17), 08/04/88, paras. 7 and 8.

83
Proposed in the INTERCEPTION OF COMMUNICATIONS BILL, 2006 published in the government Gazette on Friday 26th May, 2006

3.1 CENSORSHIP OF ONLINE CONTENT

ONLINE PUBLISHING

Human rights defenders have benefited from the Internet that enabled them to easily communicate with the global community. News of human rights violations are published online and can stimulate quick condemnation from outside a particular country or area. Regions, previously outside the reach of international media, can now have their voices heard. Governments, trying to silence dissenting voices in their countries, now face difficulties on the global level.

—

National media laws are not appropriate for Internet publications, as the latter are targeted at a global audience. If a country's law prohibits publication of any material that criticises the royal family, what can the authorities do, if the critical story appears on a website hosted in a different country? Can they still persecute the writer? Let's look at the Australian libel case *Dow Jones Media group v. Gutnick*.[84] Joseph Gutnick brought an action for defamation against the online magazine *Barrons*. The High Court of Australia confirmed the decision of the State of Victoria Supreme Court, which agreed to consider the case on grounds that the article could be also seen on the computers situated in the state. In other words, the place of publication was anywhere in the world where the article could be read, not just the particular geographic location where it was put online. The same ruling has been repeatedly applied to similar cases in Canada and France.

—

In order not to inhibit the right to freedom of expression on the Internet (provided it conforms to Article 19 of the UDHR), the above issue must be dealt with at an international level.

—

Another case, relating to censoring online content, began in 2000 and led to the *Yahoo! Inc. v. La Ligue Contre le Racisme et L'antisemitisme* proceedings in France and in the U.S. The issue was the publication of Nazi literature and memorabilia on Yahoo run websites, which were also accessible to users in France, where such activity is illegal. The French court insisted that Yahoo took measures to stop such content from being accessible in France. Technically, it was very difficult to implement, and Yahoo would have had to remove this content altogether, even though such websites are not deemed illegal in the United States – where the Yahoo servers are located. Eventually, courts in both countries ruled against Yahoo, in defiance of the First Amendment to the US Bill of Rights. This was a dangerous precedent that allowed one country's laws to be enforced in another, thus restricting the global nature of the Internet.

—

Many countries issued specific directives on the legality of publishing information online. For instance, in Iran the law "...prohibits and considers a crime to publish on the internet any material in conflict with or insulting the

84
(2002) 210 CLR 575

Islamic doctrine, revolution's values, the thoughts of Imam Khomeini, the Constitution, jeopardizing national solidarity, instilling cynicism in the public regarding the legitimacy or efficiency of the ruling body, propagating a good image of illegal groups, revealing state classified information, promoting vice, advertising smoking, accusing or insulting state officials..." [85]

—

In Burma, "Internet users are banned from posting contents related to politics that are 'detrimental' to the country's interests or the current policies and affairs of the government." [86]

In Zimbabwe, the Public Order and Security Act (POSA) is particularly vague classifying the publication of anything "likely to cause alarm or despondency" as a criminal offence.

In Egypt, the ever-extending Emergency Laws include a statement on publishing, "...calling by word of mouth or by writing or by any other means for the impediment of any provision of the constitution or laws; possession of written material that calls for or favours the previous actions; deliberate dissemination of news, statements, faulty or ill-motivated rumours or agitating news if the objective thereof is to disturb public order, induce fear in people, or causing harm to public interest or possession or development of publications that contain any of the previous crimes." [87] In 2002, Egyptian Internet users were warned of taboo issues (such as relations between Copts and Muslims, publicising terrorist ideas, human rights violations, criticising the president, his family and the army and promoting modern versions of Islam) and told that excessive openness was unwelcome.

Oppressive regimes have come down strongly on the human rights defenders attempting to criticise governments and officials.

Mohammad Reza Nasab Abdullahi

Iran - On February 23, 2005, following a closed-door trial held without his lawyer, Mohammad Reza Nasab Abdullahi was sentenced to six months in prison on appeal for insulting the SupremeLeader and spreading anti-government propaganda. He was imprisoned five days later. Abdullahi, a university student, human rights defender, editor of a student newspaper, and blogger in the central Iranian city of Kerman, served six months in an Iranian prison for posting an entry on his **blog**, Webnegar, ("Web writer")[88]. The offending post, titled "I Want to Know," was addressed to the Supreme Leader Ayatollah Khamenei and criticised the suppression of "civil and personal rights and liberties" by the government.

Arash Sigarchi

Iran – Because of his activities as a journalist and blogger, Arash Sigarchi has been in prison since 26 January 2006, four days after being given a three-year sentence for "insulting the Supreme Guide" and "propaganda against the regime."

He was previously arrested and imprisoned for two months in early 2005 and was sentenced to 14 years in prison by a revolutionary tribunal on the same charges in February 2005. After paying bail of 1 billion rials (95 000 euros), he was released on 17 March 2005.

85
'Access Denied' – A report on the status of Internet in Iran, Iran CSOs Training and Research Centre, 2005

86
Privacy International – Silenced 3/09/2003

87
www.eohr.org/PRESS/2003/3-9.HTM

88
Available at www.iranreform.persianblog.com

Prior to that, he was arrested on 27 August 2004 and held for several days for posting an article online, with photos, about a rally held in Tehran by the relatives of prisoners executed in 1989. Since then, he has been constantly harassed by the police.

The former editor of the daily Gylan Emroz, Sigarchi kept a political and cultural blog (www.sigarchi.com/blog) for three years in which he often criticised the regime. The authorities made it impossible to access the blog from within Iran.

Al-Mansuri

Libya – Al-Mansuri published his last article on January 10, 2005. It was a critique of a debate between two government officials, one of whom, Shukri Ghanim, was a reputed reformer, and the other, Ahmad Ibrahim – a reputed hardliner. Al-Mansuri expressed hope that al-Qaddafi would support the former. 15 On October 19, 2005, Akhbar Libya reported that a Tripoli court had sentenced al-Mansouri to one-and-a-half years in prison for illegal possession of a weapon.

Ibrahim Lutfy, Mohamed Zaki, Ahmad Didi and Fathimath Nisreen

Maldives – Ibrahim Lutfy was arrested (together with Mohamed Zaki, Ahmad Didi and Fathimath Nisreen, Lutfy's assistant) in January 2002 for producing *Sandhaanu*, a newsletter about human rights violations and corruption distributed by email. Accused of "defamation" and of "trying to overthrow the government," Lutfy, Zaki and Didi were condemned to life imprisonment on 7 July 2002. Nisreen, who was only 22 at the time of the trial, received a 5-year prison sentence. He was released in May 2005 after 3 years in prison.

Lutfy gave his police guard the slip on 24 May, while in nearby Sri Lanka for an eye operation. He was suffering from chronic conjunctivitis, aggravated by poor prison conditions (after many refusals, the authorities had finally given him permission to go to Sri Lanka for treatment). He spent several months in hiding in Sri Lanka with the help of a network of friends. Then the UNHCR helped him obtain refugee status in Switzerland, where he currently lives. The policeman, assigned to guard him while in Sri Lanka, was imprisoned.

Didi was hospitalised in Male in February 2004 and was then put under house arrest. He had serious heart problems which probably needed surgery. Zaki, whose health deteriorated seriously while in prison, was also put under house arrest. Both their sentences were reduced to 15 years in 2003.

Dr Nguyen Dan Que

Vietnam – Dr Nguyen Dan Que, 61, a freedom of expression activist, released in 1998 after nearly 20 years in prison, was re-arrested at his home in Saigon on 17 March 2003. Officials did not give the reason for his arrest, but it was thought to be linked with a statement he posted online criticising the lack of press freedom in Vietnam. He was responding to remarks by a foreign ministry spokesman claiming that freedom of information was guaranteed. Although he is suffering from high blood pressure

and a stomach ulcer, his family has not been allowed to visit him or give him the medication he needs, and he has not been brought to trial. On 22 September 2003, 12 Nobel Prize winners wrote to the Vietnamese communist party Secretary General Nong Duc Manh voicing concern about Que's health and asking that he be allowed proper medical treatment and family visits pending his release.

Nguyen Vu Binh

Vietnam – The former journalist was sentenced to seven years imprisonment on 31 December 2003 at the end of a trial lasting less than three hours. The people's court of Hanoi also sentenced him to three years house arrest once he reaches the end of his sentence. Sources close to the Vietnamese authorities said that the main charge reportedly relates to a letter sent by Nguyen on 19 July 2002 to the Human Rights Commission of the US Congress, in which he criticised the human rights situation in his country. He is apparently also charged with being in contact with "subversive dissidents" such as Le Chi Quang and Pham Hong Son, both of whom are also behind bars. He is further accused of having received 4.5 million dongs (about 230 euros) "from a reactionary organisation based abroad", taken part in an anti-corruption organisation and having called on the Vietnamese authorities in 2000 to set up a liberal democratic party. Vu Binh is also charged with posting messages of a "reactionary nature" on the Internet, in particular an essay headlined, "reflections on the Sino-Vietnamese borders agreements" in which he criticised the 1999 treaty between the two countries.

Zouhair Yahyaoui

Tunisia – Zouhair Yahyaoui, founder and editor of the news website *TUNeZINE*, was conditionally released on 18 November 2003 after serving more than half of his 28-month sentence. Arrested in a Tunis publinet (government initiated Internet café) on 4 June 2002, he used his site to spread the news about the fight for democracy and freedom in Tunisia. Under the pseudonym "Ettounsi" ("The Tunisian" in Arabic), he wrote many columns and essays and was the first to publish an open letter to President Ben Ali criticising the Tunisian judiciary's lack of integrity.

TUNeZINE was censored by the authorities right from the start. But its fans received a weekly list of "proxy" servers through which they could access it. On 10 July 2002, Yahyaoui was sentenced by an appeal court to 12 months in prison for "putting out false news" (article 306-3 of the criminal code) and another 16 months for "theft by the fraudulent use of a communications link" (article 84 of the communications code), meaning that he used an Internet connection at the publinet where he worked. He was jailed under very harsh conditions and staged two hunger-strikes in early 2003 to protest against his imprisonment. He was released more than a year later, in November 2003, and died of natural causes in March 2005 at the age of 36.

Mohammed Abbou

Tunisia – Mohammed Abbou is a prominent human rights lawyer who is currently serving three and a half years in prison for publishing statements on the Internet that called attention to human rights abuses in the Tunisian prison

system. The statements compared the torture and ill treatment suffered by Tunisian prisoners to that suffered by prisoners in Abu Ghraib. Mohammed is a member of the National Committee for Liberties in Tunisia, one of many national NGOs that the Tunisian government refuses to recognize, and a former Director of the Association of Young Lawyers. A vocal critic of corruption, he was one of the few lawyers in Tunisia willing to publicly comment and act on corruption allegations involving President Ben Ali?s family. He was imprisoned in April 2005, following a trial widely condemned as unfair and arbitrary by Tunisian and international NGOs and is incarcerated in El Kef prison, 170 km from his home and family in Tunis. From 11 March to 21 April 2006, in order to draw attention to the inhuman and degrading conditions in which he is being held and the harassment faced by family members whilst visiting him, Mohammed went on his second hunger strike since his imprisonment.

Samia Abbou, wife of Mohammed Abbou, was subjected to a brutal assault on 7 December 2006. She and three other leading Tunisian human rights defenders were attacked and beaten outside El Kef prison, near Tunis, by a group of about forty men in civilian clothing. National Freedom of Samia Abbou traveled to El Kef to visit her imprisoned husband with human rights defenders; Moncef Marzouki, former president of the National Committee for Liberties in Tunisia (CNLT) and the Tunisian League for Human Rights (LTDH) Salim Boukhdhir, a well known Journalist and Samir ben Amor, founding member of the International Association for the Support of Political Prisoner. According to reports, police stopped the car in which they were traveling on a number of occasions throughout the journey to El Kef and were present outside the prison at the time of the assault.

Habib Salih

Syria – On May 29, 2005, military intelligence officers arrested Habib Salih in Tartus, approximately 100 miles (130km) north of Damascus (he had only just been released from a previous incarceration - for participation in the civil society movement of the "Damascus Spring"). This time, he was arrested for posting on two Web sites a series of open letters addressed to the delegates attending the June 2005 Ba`ath Party Conference in which he detailed his prison experience. In the months since his release, he had also written critical articles for the Lebanese newspaper *an-Nahar* and the banned Web site http://www.elaph.com. The authorities quickly transferred him to the investigations office, where he risks torture. His trial is still pending.

Huang Qi

China – Huang is a human rights defender who set up the Tianwang website (www.6-4tianwang.com) in June 1999 to publicise information about missing people. Gradually, the site also began to feature comments and news articles on topics not normally covered by the state-controlled media. It published stories about human rights abuses, government corruption, and - just days before Huang was taken into custody - several pieces about the Tiananmen Square massacre. Huang was arrested on June 3, 2000 – the day before the 11th anniversary of the 1989 Tiananmen Square protests of

1989 – and charged under articles 103 and 105 of the criminal code. He was accused of posting on his website articles about the protests written by dissidents living abroad. In an interview with the BBC, Huang said he was ordered to sleep on the floor next to the toilet for the first year in jail. He denied the charge of subversion and insisted it did not apply to him.

Huang said: "If someone in China fights for democracy and freedom and is then accused of being a participant of the June 4th incident, a member of Falun Gong or a pro-democracy activist, I am definitely going to tell the Chinese regime that I am one of them and proud of it. There is no doubt that I am in pursuit of democracy and freedom." On June 4, 2005, Huang Qi was released from jail after completing his sentence. Reporters sans frontières awarded him the Cyber-Freedom Prize in 2004.

3.2 WEBSITE FILTERING

Countries around the world are adopting Internet filtering technology. It allows them to block websites or specific website content from the Internet users on their territory. It is, in essence, censorship applied through the Internet medium. Filtering occurs in almost every country connected to the Internet. It is usually done by categories, with Internet content divided into specific areas: religion, politics, pornography, paedophilia, human rights, etc. Some countries limit the categories to reflect the national laws, others block websites selectively and without any clear legal basis.

"There are two fundamental philosophies regarding access to information, which can be summed up as (1) Everything that is not explicitly permitted is forbidden; and (2) Everything that is not explicitly forbidden is permitted. These are generally referred to as whitelists and blacklists respectively. Because websites come and go so quickly on the Internet, maintaining lists of either type is a full-time job. Both types are used at the national level. Australia, for example, has a law requiring ISPs to block access to certain types of material deemed harmful to minors, including pornography involving children and animals, excessive violence, information about crime and drug use (a blacklist).[89] On the other hand, Burma, which initially banned Internet altogether, tried to create its own local version, called MyanmarNet. Recently, the government opened the country to the Internet, yet only 0.5% of the population have connectivity and swift measures were taken to purchase a filtering firewall from Fortinet to control what websites its citizens have access to.

—

The difficulty of maintaining these white and blacklists has often resulted in this task being passed into the hands of the ISPs and involved holding them liable should one of their users be able to access a website whose content is illegal in the user's country. This makes the task of small ISPs that have to scan several billion webpages to decide which ones to censor almost unrealistic. It also gives power of censorship to a commercial, unelected body that will allow no avenue for a debate of their decisions.

—

Another approach is to categorise Internet websites as part of mass media and thereby accept all the national freedoms or limitations that apply. Such legislation has been enacted in Armenia, Iran, Kazakhstan, Egypt and some other countries. This approach demonstrates misunderstanding of Internet technology. In contrast to traditional forms of media, such as television, newspapers and radio, where information is collated, edited and then presented for consumption, the Internet presents its entire collection at once and allows the user to decide what they want to read and contribute to. The Internet does not have an opinion nor can it be influenced by any.

—

States are foregoing international agreements on freedom of information and expression and deciding for themselves what content their citizens can and cannot view. This is usually done under the pretence of maintaining national

89
Privacy International – Silenced
3/09/2003

stability and preservation of culture, security and rule of law. These excuses have been widely used to stifle the websites devoted to the issues of freedom of expression, politics, independent media and human rights. There is a strong tendency to reverse the open structure of the Internet and to turn it into a collection of information, customised to suit particular governments.

—

On December 31, 2002, the Iranian government issued "Decree on the Constitution of the Committee in Charge of Determination of Unauthorized Websites" stating that, "In order to safeguard the Islamic and national culture, a committee comprising the representatives of the Ministry of Information, the Ministry of Culture and Islamic Guidance, the Islamic Republic of Iran's Broadcasting, the Cultural Revolution High Council, and Islamic Propagation Organization shall be set up by the Ministry of Information to determine and notify the Ministry of ICT of the criteria regarding unauthorized websites". Websites revealed to the Ministry of ICT by the committee are added to the list of those subject to censorship.

—

In Singapore, websites are controlled and licensed by the Singapore Broadcasting Authority (SBA) and must abide by the agency's strict guidelines as to "objectionable" content, ranging from pornography to "areas which may undermine public morals, political stability or religious harmony". [90]

—

Often though, government's intentions in blocking websites are not publicised, and lists of blocked websites are not publicly available. Therefore, Internet sites are being blocked not because they contravene specific regulations, but because the government considers access to them detrimental to the policy it promotes within the country. A classic example of this methodology is China, where all ISPs and other communication providers have simply agreed to "resist firmly the transmission of information that violates fine cultural traditions and moral codes of the Chinese nation." As a result, China has been able to deploy the world's most sophisticated filtering technology, employing thousands of people whose job is to constantly scan and update the white/blacklists of websites.

—

Generally, there is no public consensus on which websites the governments can censor and often no process of appeal against removing a block to a website. This results in people applying **circumvention** technologies in order to bypass their country's filtering regimes. The process usually involves requesting a computer that stands in a country where the Internet is not as strongly censored, to fetch the website and pass on the content. From a technical point of view, the user is only accessing that relaying computer and not the banned website. To quote the founder of the Electronic Frontier Foundation, John Gilmore, "The Internet perceives censorship as damage, and routes around it."

—

Internet filtering not only impedes the work of human rights defenders but can sometimes prevent news of human rights violations from reaching the local and global community. Governments can block access to a website hosted in their country, thereby crippling the capacity of the host organisation to transmit news and updates. Alternatively, they can prevent their citizens from accessing certain websites on the Internet, thereby restricting the HRDs access

90
Internet Censorship Report
The Canadian Committee
to Protect Journalists

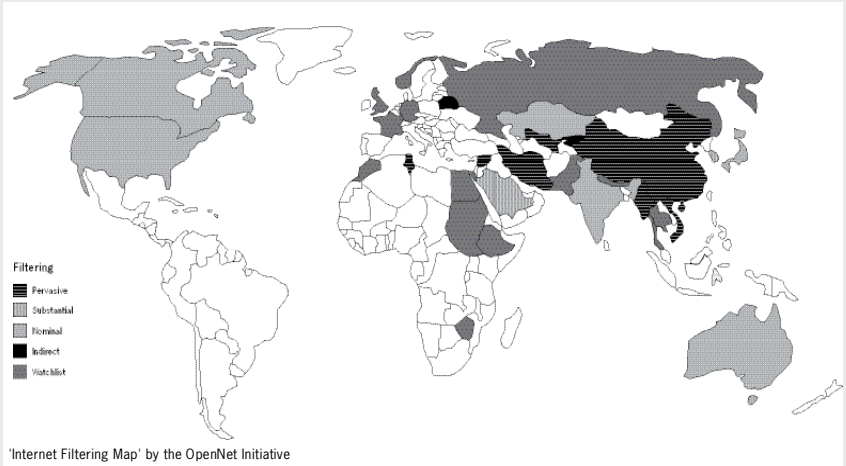
to communications, information and their ability to freely express opinion. Either of the above actions is in direct contravention of *Article 2* of the UN Declaration on Human Rights Defenders[91] adopted by the UN General Assembly and proclaiming that:

> 1. *Each State has a prime responsibility and duty to protect, promote and implement all human rights and fundamental freedoms, inter alia, by adopting such steps as may be necessary to create all conditions necessary in the social, economic, political and other fields, as well as the legal guarantees required to ensure that all persons under its jurisdiction, individually and in association with others, are able to enjoy all those rights and freedoms in practice.*
> 2. *Each State shall adopt such legislative, administrative and other steps as may be necessary to ensure that the rights and freedoms referred to in the present Declaration are effectively guaranteed.*

A quick word about the companies who develop and sell surveillance and filtering software and thereby help oppressive regimes develop their infrastructure. Defenders and human rights organizations have for years accused Cisco and other Western corporations of actively assisting China in developing censorship and surveillance systems. For example, Amnesty International, Human Rights Watch, and Reporters sans frontières have consistently highlighted the issues of corporate responsibility and Internet freedom raised by China's use of Western technologies. These groups allege that Western corporations have facilitated the construction of China's censorship and surveillance infrastructure, and that they may even be involved in the system's ongoing maintenance and operations.[92]

—

The majority of filtering software manufacturers also originate from the United States. These include companies like SecureComputing, Websense, Fortinet... Their software contains predefined categories of Internet content and allows the operator to add additional sites at their discretion. There is a need for international agreements and commitments that would forbid anyone to sell a product which will be used to restrict another person's rights. States that have shown systematic abuse of the UDHR should be denied access to filtering software developed in other countries.



'Internet Filtering Map' by the OpenNet Initiative

91
United Nations Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms

92
See, e.g., Amnesty International, *People's Republic of China: Controls tighten as Internet activism grows*, Jan. 28, 2004, at http://web.amnesty.org/library/Index/ENGASA170012004;
Human Rights Watch, *China Tightens Internet Controls*, Aug. 1, 2001, at http://www.hrw.org/press/2001/08/china-0801.htm;
Reporters Sans Frontieres, *Internet Under Surveillance: China*, June 22, 2004, at http://www.rsf.org/print.php3?id_article=10749;
Rights & Democracy (International Centre for Human Rights and Democratic Development), *Human Rights at Risk on the Cyber-battlefield: The Sale of Security & Surveillance Technology to China*, at http://www.dd-rd.ca//english/commdoc/publications/globalization/surveillancetechChina/briefingpaper.htm.

3.3 COMMUNICATIONS SURVEILLANCE

Surveillance of communications has been conducted for many years. It is generally accepted that police and intelligence services need the power to eavesdrop on others for the overall benefit and security. Many criminals have been caught because of wiretapping and retrieval of phone records. It is also assumed that these powers are not given lightly and a rigorous judicial or similar process takes place before such actions are authorised. People would stand up and shout if they found out that every telephone conversation they ever had was recorded and stored.

It is therefore both surprising and unfortunate that so many countries were able to quickly and quietly introduce the laws permitting surveillance of Internet communications. No doubt, the September 11 attacks caused enough concern in civil society to allow authorities additional power. The result was far beyond the freedoms granted to them in the epoch of telecommunications.

—

In 1996, Digicom, the largest provider of electronic services in Pakistan, asked its clients to sign agreements that imposed a number of restrictions on the use of the Internet. Under the terms of the agreements, users were prohibited from using data **encryption** and had to accept that their electronic communications could be monitored by government agencies. On top of that, users of Internet services had to provide Digicom with copies of their National Identity Cards (NIC), whereas foreign nationals had to submit copies of their passport. Those failing to do so would face disconnection of their services. [93]

—

As mentioned already, the Internet surveillance systems have been implemented at national levels for some time. Russia's FSB installed a black-box monitoring system at every **ISP** (the project is known as SORM2). In addition to that, they forced the ISPs to pay for the monitoring equipment. The United States introduced a similar system - CARNIVORE. China's 'Golden Shield' project was announced on 2001. Rather than relying solely on the national Intranet, separated from the global Internet by a massive firewall, China is preparing to build surveillance intelligence into the network, allowing it to "see," "hear" and "think."[94] A global surveillance system known as **ECHELON**[95] was jointly launched by the US, the UK, Australia, New Zealand and later Germany after the end of the Cold War.

—

Commercial companies are no less interested in collecting as much of our personal data as possible. In 2004, Google launched its free webmail service, called Gmail. It provided the unprecedented one gigabyte of storage space. The aim was for people to switch to Gmail where they would never run out of storage space. The privacy statement to be agreed upon registering, enables Google to access the contents of your email messages with the intention of providing relevant advertising on the sidebars. All users of Gmail had to agree to have their email monitored and its content analysed and acted upon. The

93
Internet Censorship Report - The Canadian Committee to Protect Journalists

94
G. Walton, China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China 9 (Rights and Democracy, 2001) available at http://serveur.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html

95
The use of Echelon to target diplomatic communications was highlighted as a result of disclosures made in 2003 by a British intelligence employee, former United Nations officials, and a former British Cabinet The use of Echelon to target diplomatic communications was highlighted as a result of disclosures made in 2003 by a British intelligence employee, former United Nations officials, and a former British Cabinet Minister concerning eavesdropping by the US NSA and the British GCHQ over UN Secretary General Kofi Annan's telephone communications and private conversations.

users were relying on Google not to disclose this information to third parties. Gmail's Terms of Use stated:

—

"Google may, in its sole discretion, modify or revise these terms and conditions and policies at any time, and you agree to be bound by such modifications or revisions. If you do not accept and abide by this Agreement, you may not use the Gmail service."

In effect, were Google to change their policy overnight (and theoretically they can), your entire email data and its analysis would become available to the highest bidder. We already know how willingly Yahoo! cooperated with the Chinese government by providing access to private email accounts, with several account holders being put behind bars as a result.

—

The surveillance methods that can bypass **encryption** have been used in the United States since 2001. These devices are called keyloggers and installed (often remotely) on personal computers without the users' notice or authorisation. A keylogger records all the keys a user types on their keyboard and sends this information to a designated address. Such surreptitious police decryption methods were highlighted in the case of *United States v. Scarfo*.[96], when the FBI manually installed a key logger device on the defendant's computer to capture his PGP **encryption** password. Once they discovered the password, the files were decrypted, and incriminatory evidence was found. In December 2001, the FBI confirmed the existence of a similar technique called 'Magic Lantern'.

—

Internet data is not only being monitored, it is also stored and often for a long time. In 2005, the European Union, under pressure from the Council of Europe, introduced legislation that obliges all member countries to retain Internet data for a minimum of two years[97] (although members can choose to hold it for longer periods). Article 8 of the European Convention on Human Rights guarantees the individual's right to respect for his private and family life. Article 8 specifies that public authorities may only interfere with this right in narrowly defined circumstances. In particular, any interference must be in accordance with the law and can only be conducted in the interests of national security and crime prevention.

—

The existing approach to systematic data retention therefore assumes that we are all guilty until proven innocent. In the meantime, our personal data becomes open to abuse by either public or private agents. Furthermore, indiscriminate surveillance and retention constitute a breach of a person's right to privacy.

—

Illegal by international standards, these practices nevertheless occur on a global scale. Many countries that do not have the resources to build nationwide surveillance and retention systems (like, for example, India and Tunisia), instruct the ISPs to do it instead. Some other countries simply do not have sufficient safeguards to prohibit unauthorised access and manipulation of the Internet data which then becomes susceptible to corruption and hacking. In other words, anyone could be brought to court and judged on the evidence,

96
180 F. Supp. 2d 572 (D.N.J. 2001).
See generally EPIC's Scarfo web page http://www.epic.org/crypto/scarfo.html

97
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2005-0512+0+DOC+XML+V0//EN&language=EN

fabricated to look as if it was contained in the emails written by the defendant several years earlier.

—

Indiscriminate surveillance and data retention constitute a threat to the right to privacy of individuals, particularly human rights defenders, already targeted by extra surveillance and monitoring on behalf of the state. The state's ability to monitor, record and store HRDs' communications leads to interruption of their work. This data can also be tampered with and corrupted to bring a HRD into disrepute or to impose criminal sanctions. Internet corporations, cooperating with repressive regimes, are therefore contributing to destabilisation of an individual's privacy.

—

Every country involved in mass surveillance of its citizens' Internet activity must establish an independent authoritative body to monitor the collection of such data as well as access to it. Strict laws to prevent the abuse of these systems must be in place to protect our privacy, identity and peace of mind.

3.4 CRYPTOLOGY AND CIRCUMVENTION

In the previous sections of this chapter we described practices of the Internet surveillance, monitoring and censorship affecting our basic human rights. It is therefore justifiable and even necessary for the users to possess the means of regaining such privacy. If the information is collected and stored regardless of its content or one's activity, one is entitled to taking action to make this data private and not susceptible to tampering. Likewise, if governments censor our right to seek and share information on the Internet, methods of circumventing such censorship are essential for maintaining a free and unhindered online community.

The 'International Survey of **Encryption** Policy' published by the *Electronic Privacy Information Centre* in 1999 began with the following statement: "Most countries in the world today have no controls on the use of cryptography. In the vast majority of countries, cryptography may be freely used, manufactured, and sold without restriction. This is true for both industrial and developing nations".

—

Only 5 years on, we saw drastic changes in the world's approach to **encryption**. Below is a diagram, compiled by Bert-Jaap Koops for his Crypto Law Survey.[98]

The importance of **encryption** in providing privacy of information and communication was quickly taken on board by many governments. Introduction of public key cryptography and several easy-to- use tools placed this incredibly complex technology within the grasp of all. Its effectiveness in neutralising the capabilities and capacities of government agencies to perform successful surveillance was soon realised. Since then, governments have been scrambling to restrict public use of **encryption** or to ban it altogether.

—

The strength of privacy provided by **encryption** has lead to its classification as a military grade weapon and inclusion into the Wassenaar Arrangement[99]. The United States initially demanded for a world wide key escrow system, i.e. for a copy of all **encryption** keys to be stored with the

98
http://rechten.uvt.nl/koops/cryptolaw/cls-sum.htm

99
The Wassenaar Arrangement is an agreement by a group of 33 industrialized countries to restrict the export of conventional weapons and "dual use" technology to certain other countries considered pariah states or, in some cases, those that are at war.

government so that they could decrypt messages at their discretion. A project known as the Clipper Initiative would have this key escrow built into **encryption** software. The project was rejected by the Congress and presently **encryption** in the US is only limited by export laws, prohibiting its sale or transfer to any of the seven countries labelled as 'terrorist states'. All cryptographic algorithms must be approved and licensed by the National Security Agency.

—

This trend has been followed by many countries. At first, governments feared loss of intelligence- gathering powers and restricted the use of cryptography unless they were able to decrypt it. Eventually, privacy advocates won the battle for not limiting the use of cryptography to secure personal information. Unfortunately, some countries continue to ban **encryption**, either outright or through persecution of its users. China, for instance, approves of the use of **encryption** products that are developed and licensed in China – presumably, including some form of key recovery. Turkmenistan does not have any laws banning **encryption** use, yet if surveillance notices that a person's Internet traffic is encrypted, they will demand to know what is being sent. Another approach, taken by India and the UK, is to allow **encryption**, yet to force the owner of the keys to submit their passwords or face imprisonment. Iran bans the use of **encryption** altogether – a hardly realisable ruling if we remember that the Internet has built-in **encryption** (**SSL**)[100]. Whenever you access an email account (Yahoo, for instance) or carry out any kind of financial activity, your Internet connection to the website becomes encrypted in the **Secure Sockets Layer** (**SSL**). Yahoo uses **SSL** to pass your login name and password secure to its server. You don't have another option. Hence, under the legislation as strict as Iran's, Yahoo email accounts as well as many other Internet services and functions should be made illegal. If a country wants to benefit from the Internet economically or culturally, **encryption** cannot be limited or outlawed.

—

Circumvention technologies allow the user to bypass website blocks when browsing the Internet and sending email. They strive to restore the human right to seek and exchange information in the countries where, in contradiction to international standards, free Internet browsing and free email exchanges are prohibited. **Circumvention** tools take advantage of the computers in uncensored countries and route communications through them. In real terms, if your country prohibited you to speak with me but not with a colleague of mine, you would convey the information to me by conversing with my colleague. Internet users in Iran and China, accustomed to the difficulties of the Internet-censoring regimes, became experts in sourcing out new methods of circumventing in-country blocks, but even those are outlawed and heavily punishable in many states.

—

Human rights defenders must possess the knowledge and the ability to secure their information and to bypass illegal censorship channels. States that have ratified the Convention on the Protection of Human Rights Defenders have an increased obligation to ensure that the legitimate work of HRDs is not restricted or punished. Civil society at large should guarantee that no legislation prohibits the use of these rights-restoring tools and techniques.

100
Unfortunately this classification has become a strategy used by many repressive governments around the world. Internet is effectively outlawed due to its **encryption** capabilities, yet enforcement of this law is selective and could be used to pressure human rights groups.

4.1 CASE STUDY 1 CREATING A SECURITY POLICY

When developing a security policy for yourself or your organisation, you must also develop a clear understanding of the risks to the security of your computers and information. The level of risk increases in direct proportion to threats and your vulnerability to them, as shown by this equation:

RISK = THREATS x VULNERABILITIES

Threats represent a possibility that someone will harm the security of your computers, information stored on them and online communications. Making a threat assessment means analysing the likelihood of a particular threat being put into action. Examples of threats:

- **A virus attack**
- **Confiscation of computer equipment**
- **A website block**

Vulnerability means the degree to which you are susceptible to loss, damage and suffering in the event of an attack (if a threat is realised) that varies with situation and time. Vulnerability is always relative, because all people and groups are vulnerable to some extent. Often, the main vulnerability in the realm of technology is lack of understanding or insufficient training. Another vulnerability comes from over-relying on technology that one does not fully comprehend.

- Vulnerability can be about location. For example, your computer screen and operations are easily observed when you operate from an Internet café. If you live in a country suffering droughts and electricity shortages, then your vulnerability will be lack of electricity (or electrical surges) and hence inoperable computers and the Internet.
- Vulnerabilities can also include lack of communication means, like not having access to a phone or to an Internet connection.
- Vulnerabilities may also be connected with team work and fear: a defender who receives a threat may feel fear, and his/her work will be affected by fear. If s/he has no proper way to deal with this fear (somebody to talk to, a good team of colleagues, etc.) chances are that s/he could make mistakes or poor decisions. This is a non-computer-related threat, but one which could be of great relevance to computer security because it increases an already existing threat.

Capacities are strengths and resources a group or a defender can access to achieve a reasonable degree of security. Examples of capacities could be training in computer- or security-related issues. Knowledge of the computer/Internet environment is an essential capacity for dealing with possible insecurities. Access to a trusted computer technician or a network of skilled people is a great resource.

- security policies within the organisation: efficient file storage, backup and online communications
- secure office entrance and strong locks on doors and windows
- copies of all hardware warranties and licences for software (alternatively, using only open source software)

Not knowing enough about your work environment and the technology you operate with is a vulnerability, while having this knowledge is a capacity. The risk, created by threats and vulnerabilities, can be reduced if defenders have enough capacities (the more capacities, the lesser the risk).

$$\textbf{Risk} = \frac{\text{threats x vulnerability}}{\text{capacities}}$$

DRAFTING A SECURITY PLAN

Components of the plan

A security plan is aimed at reducing your risk. It will therefore have at least three objectives, based on your risk assessment:

- Reducing the level of threat you are experiencing.
- Reducing your vulnerabilities.
- Enhancing your capacities.

It could be useful if your security plan also includes:

- Preventive plans or protocols to ensure routine work is done within security standards. For example, how to communicate by email on sensitive topics with a group of people
- Emergency plans for dealing with specific problems, for example, confiscation of office equipment.

Responsibilities and resources for implementing the plan

To ensure that the plan is implemented, security routines must be integrated into daily work activities:

- Include context assessment and security points routinely in your agendas.
- Register and analyse security incidents.
- Allocate responsibilities.
- Allocate resources, i.e. time and funds, for security.

Drafting the plan – how to begin

If you have done a risk assessment for a defender or an organisation, you might have a long list of vulnerabilities, several kinds of threats and a number of capacities. You can't realistically cover everything at the same time. So where to begin? It's very easy:

■ **Select a few threats.** Prioritise the threats you have listed, be it actual or potential ones, using one of these criteria: The most serious threat – loss of all computer data, for example; OR the most probable and serious threat: if organisations similar to yours have been attacked, that is a clear potential threat for you; OR the threat which corresponds most to your vulnerabilities – because you are more at risk of that specific threat.

■ **List the vulnerabilities you have which correspond to the threats you have listed.** These vulnerabilities should be addressed first, but remember that not all vulnerabilities correspond to all threats. For example, if you have no idea whether a backup of all your computer data exists, then this relates directly to the threat of losing your computer data irrecoverably.

■ **List the capacities you have which correspond to the threats you have listed.** You are now in a position to address the selected threats, vulnerabilities and capacities in your security plan, and can be reasonably sure that you will be able to reduce your risk from the right starting point.

CASE STUDY

Security Plan for 'Defending Minority Rights' NGO

The purpose of this plan is to ensure that the information held on our computers is not lost, stolen or damaged irrecoverably in any way.

Threats	Vulnerabilities	Capacities
Virus attack	- Staff open emails without caution - Nobody knows if virus scanner is on all machines or updated - no backup of information	- Just received a copy of 'NGO in a Box – Security Edition' from http://security.ngoinabox.org
Confidcation of computers	- Easy access to office - No backup - No funds to purchase new equipment - information is not protected	- good team of colleagues who know each other and co-operate very well - good contact with funders
Computers are damaged by weather or other external forces	- No Backup - No knowledge of how to protect network and electrical equipment	- good contact with funders - a relative of a staff member is a skilled plumber

Now we begin to work on decreasing our vulnerabilities and hence increasing our capacity for dealing with this and other threats that may arise in the future. Your solutions and resources may differ in each case. Notice that lack of information backup is a common vulnerability that would cause great harm should any of the threats be realised. Below is a list of actions you could take to decrease the vulnerabilities (all tools and explanations on how to perform these actions can be found in this manual and the *NGO in a Box – Security Edition*).

Virus attack

- Introduce strict policy on opening mail from unknown sources or replying to spam. In plain words, forbid anyone to do so. People who receive hundreds of viruses and spam should change their email address.
- Install a free anti-virus (Avast, AntiVir, AVG) on all computers and update the virus definitions from the Internet. Program files and guides can be found in the *NGO in a Box – Security Edition*. Make sure every computer in the office is operating with a fully functional anti-virus program.
- When your computer is clean of viruses, make a backup of all important user documents. Keep this on a separate media (CD, USB stick) and away from the office. If you do suffer a virus attack, at least you can recover your files.

Confiscation of computers

- To prevent theft you have to secure your offices and work premises. Strong doors and windows are essential, as is an intercom or other form of visitor identification system. Ideally, your office should have a reception desk, where visitors will be greeted before gaining access to the main room.
- Backup of all information should be made and kept securely in a different location.
- You should have access to emergency funds to purchase new equipment and to load the backup data onto it.
- If computers are confiscated, at least the documents on them should be protected from unauthorised access. Use **encryption** software to protect a part of the hard drive. Likewise, wipe all unnecessary data to prevent its restoration by the confiscators. (See Information Backup, Destruction and Recovery chapter)
- Be aware of who has keys to the office and how many copies are in existence. If your computers are not protected by **encryption** or you store sensitive data on paper and computers, then make sure that no one has unaccompanied access to your office, even the cleaning staff.

Computers are damaged by weather or other external forces

- Ideally, a plumber or an electrician should check your premises regularly to report on their stability, any water damage sustained and the amount of fire insulation. All loose electric cables should be discarded and faulty connections patched. This may be costly but it is necessary, as computers are extremely delicate and cannot survive water or heat damage.
- Backup of all information should be made and kept securely in a different location.
- You can purchase an Uninterrupted Power Supply (UPS) battery for your computers to prevent sudden shutdown in case of electricity loss. Power sockets or power boards should have surge protectors, so that they switch off in case of electric spikes. Regions that suffer loss of electricity for months at a time should consider a petrol-powered generator or other sources of energy.

It is difficult to introduce security policies without undermining some aspect of productivity in your office. Paying attention to security usually takes time and concentration. Carelessness, deadlines and insufficient manpower are the enemies of good security. It is therefore necessary that the rules are agreed upon and rationalised by all. Their implementation should apply to everyone and directors of the organisation must take the lead in setting an example. Good security also requires you to be pro-active and realise your threats and ways to handle them before they occur.

4.2 CASE STUDY 2 COMMUNICATION CHANNELS

OUTLINE

The global NGO 'Human Rights for All' (HQ) based in Europe has requested that one of its international branches (the Bureau) performs an investigation into cases of torture at the hands of the local government. The selected country 'N' has long become notorious for using torture against prisoners and especially human rights defenders. The Bureau is located in the capital of 'N' and employs a number of skilled people with many years experience of working in difficult situations. They can collate the necessary information for the report on torture but worry that the government will stop at nothing to prevent them from doing so. 'N' has a very tight policy on controlling information and making sure that the outside world knows as little as possible about its internal activities.

—

HQ decides to publish the report, based on the information they will receive from the Bureau, themselves. They need to establish a secure channel of communication with the Bureau and make sure that the project continues until completion, or for as long as possible. There is an understanding that security is a primary issue here and they have allocated a budget of 5,000 USD to the Bureau especially for this cause. The project needs to survive attempts by the local forces to compromise, restrict or destroy it completely. The Bureau is to undergo a review of its methods of collecting and communicating information as well as of building a security policy for all staff to implement.

—

It is decided that all staff undergo information security training by a local expert and do their own study and research in security issues on the Internet. Case studies, witness reports and other information on torture cases they may uncover will be stored on paper and in electronic format. Field reporters will communicate their findings by bringing back a collection of notes taken during the mission, and by making daily reports from an Internet café. In other words, all information will be duplicate in physical and electronic format.

—

The office comprises a rented apartment in the centre of the city. There are two computers and an Internet connection. The staff are well-acquainted with the neighbours and enjoy their support. The office had previously been broken into, although nothing of importance was taken.

THREATS

To get an understanding of what elements the Bureau will need to secure this project, they first decide to list all the threats they may face. The project work area is shared by HQ, the Bureau's office and the field workers. Each face their own particular threats and these must be dealt with separately. Likewise, the threats themselves are separated into those affecting office, information and communications security[101].

101
There is an additional element of staff security, but this is best described in the Peace Brigades' 'Protection Manual for Human Rights Defenders ' www.frontlinedefenders.org/manuals/

HQ

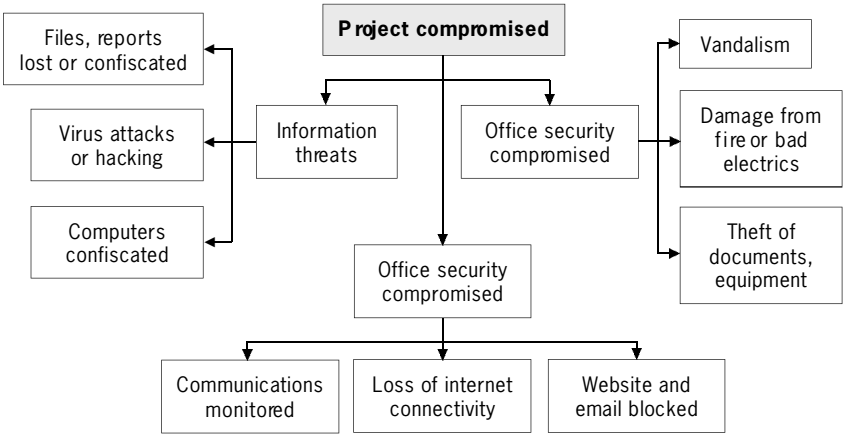
Office threats: minimal
Information threats: Reports could be lost due to virus damage or hacking
Communication threats: The communications link with the Bureau could be broken, or reports could be spoofed (falsified by malicious intrusions).

The Bureau

Office threats: Vandalism to equipment, theft, electricity faults, fire
Information threats: Computers are confiscated, data is corrupted by virus attacks or hackers
Communication threats: Office internet is disconnected, email does not send or arrive, HQ website and email address blocked, communications monitored

Field workers

Information threats: reports are lost or confiscated
Communication threats: field workers cannot access Internet café, the Bureau's or HQ's website become blocked from access within N.



SOLUTIONS

Communication

Communication between the different players in this project is essential to its survival. Therefore the participants devise several standards and methods of establishing and continuing this communication.

—

Three distinct channels of communicating with HQ are established. There is an **open channel**, where information is communicated in an insecure fashion – by telephone, post and regular email. It is important to have an open channel, so that the monitoring bodies can be satisfied of having ready access to the project communications. Information passed through the open channel is not sensitive and would include typical administrative and organisational data.

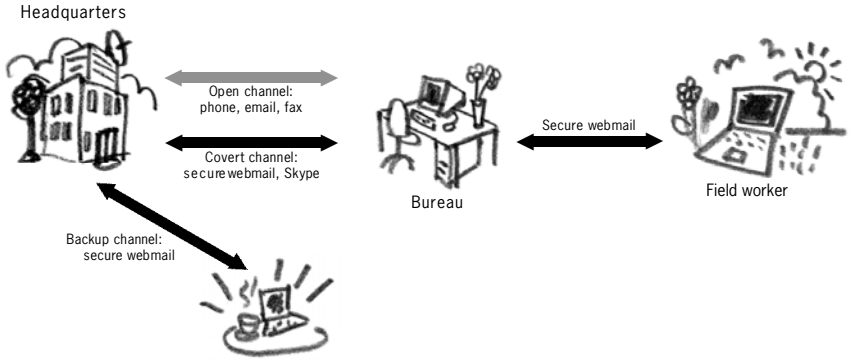
—

A **private channel** will provide for sensitive and secure communications. It will be used for exchanging information about cases, witness reports and organisational strategy. It is decided to use a secure webmail solution and Gaim with OTR plug-in for instant messaging[102]. No sensitive information will

102
You can download the latest version of Gaim from http://gaim.sourceforge.net/downloads.php and the OTR plug-in from http://www.cypherpunks.ca/otr/#downloads or find it on the *NGO in a Box – Security Edition* CD

be passed by telephone, fax or insecure email. The private channel will not be used regularly so as not to attract too much attention.

The above channels require a functioning Internet connection for communication. It is agreed that HQ will not suffer from Internet shortages and a **backup channel** is devised for the Bureau and their field workers, in case the Internet stops working or is disconnected. The backup channel will involve the Bureau workers using a nearby Internet café.



►A graphical schematic for the Bureau's communications system

Information

All data recorded and collected by the staff will be kept on paper and electronically. This will require necessary safety measures to ensure that the data is not lost, stolen or damaged. It will be very important to create and maintain a backup procedure that will outlive possible attacks. Likewise, the backup medium itself will need to be secure, as it creates an additional copy of sensitive documents.

—

To make sure that no field reports are lost before they are transmitted back to Bureau, a laptop will be purchased. Field workers will record information on paper and duplicate it to laptop. They will communicate this information to the Bureau from an Internet café on a daily basis (or as often as possible).

Office

Office security will include a rigorous policy for the staff, strengthening of entry points to the building and general upkeep to make sure that the chances for computer crashes are reduced. Physical documents will need to be kept in a safe, and wasted paper will need to be properly destroyed. It must be taken into account that computers and other office equipment could be damaged or confiscated, so a reserve fund is maintained to allow the organisation to purchase new equipment and resume work should this occur.

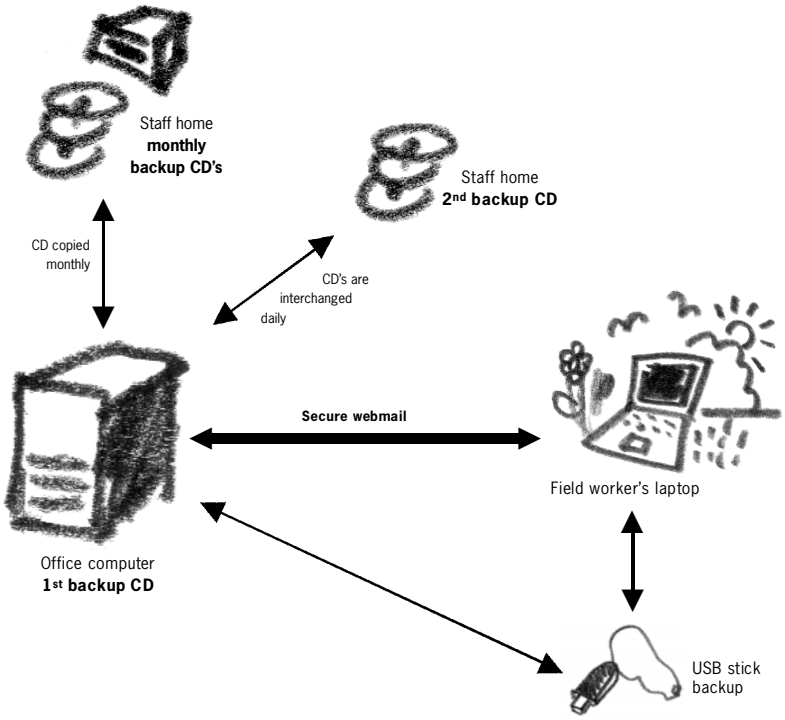
DETAILED RESPONSES TO THREATS

After developing a general idea of how to operate when dealing with possible disruptions to their work, the staff attempt to counteract all of the individual threats listed in the diagram. They undergo security training and perform their own research into electronic security on the Internet.

Information threats

- **Files, reports lost or confiscated:** To prevent the loss of data, regular backup is made of the information on computers and laptops. A re-writeable CD drive (CD-RW) is sourced for 200 USD and installed on one of

the computers. Information backup is implemented by using the DeepBurner and Freebyte programs available on the *NGO in a Box – Security Edition* CD. Every second day a backup is made of all the user documents, put on a CD and taken off-site. The person to maintain this backup rotates 2 CDs, one of which is always in the office and the other - at his/her house. At the end of every month, an additional backup is made and given to another person to keep at home. This way, should the computers in the office be damaged and the daily backup system be compromised (quite difficult to orchestrate), there will be a third tier of information backup from the previous month. Backup for field workers is done on a USB memory stick. The stick contains a copy of all recent documents, made by reporters since they last visited the office. If the laptop is lost or



► Multiple layers of data backupconfiscated, the documents can at least make it back to the office.

- **Virus attacks or hacking:** To prevent the loss of data through a virus attack or hacking, the Bureau installs the Avast4 anti-virus software on all computers and laptops. The software is free for non-profit organisations and updates automatically when the computer is connected to the Internet. They also install Spybot to counteract other malicious software and the ZoneAlarm firewall to prevent hackers from intruding into their computers. All software and explanations are found on the *NGO in a Box – Security Edition* CD. A strong policy on viruses is introduced, ensuring that nobody opens suspicious-looking email messages or uses an external diskette in a computer without scanning it with the anti-virus software first.

- **Computers confiscation:** If the computers are confiscated with official warrants or otherwise, the organisation must have the means to continue its operation. It will be necessary to purchase new computers, and money must be allowed in the budget for this. Even one computer will suffice if

the circumstances demand it. The staff source a computer retailer who will sell a new computer for 1000 USD. Needless to say, a backup of the files and documents will be required to bring the organisation back to its original state and allow the project to continue.

- **Theft of documents, equipment:** A strict key policy is introduced and only those in need of possessing office keys are given a copy. No additional copies can be made without general consensus. All computers are switched off at night and a safe for files is purchased at 300 USD. All CDs, diskettes and paper with sensitive information on it is kept in the safe. Measures are implemented to make sure that no unwanted persons could sneak into the office. The windows are within ground level and will be protected with metal bars. The door is also strengthened and a peep hole installed. A local company agrees to do both services for 500 USD.

- **Loss of Internet connectivity:** It is possible that the Internet is disabled from use for the Bureau. This could be the result of pressure on the **Internet Service Provider** or a malfunction of the network itself. To counteract, the staff decide to use an Internet café. Should the interruption to the office Internet connection prove long-term, 500 USD is set aside as emergency fund to for using the Internet café. A USB memory card will be used to transmit files between the office and the Internet café.

- **Communications monitored:** If the surveillance infrastructure of N is sufficiently advanced, they will be monitoring email that comes in and out of the country. The Bureau has a suspicion that their email is sensitive enough to warrant its monitoring and switch over to using a secure **SSL** webmail service. They register two accounts at https://www.riseup.net[103] and use one for communicating with HQ and one for the field workers. All information is passed to the headquarters daily via email. Since the connection to the webmail client is over **SSL** (HTTPs), it is encrypted. The Bureau staff research the possibility of Man-in-the-Middle attacks and are careful checking the certificates presented by the website.

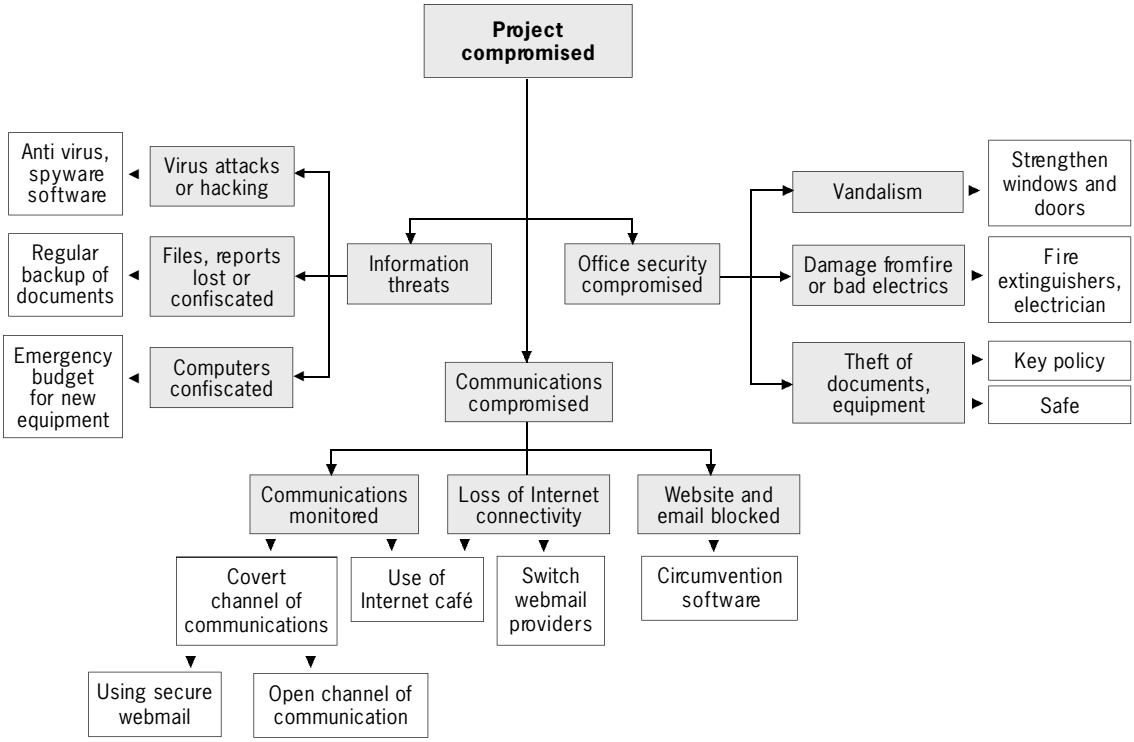
- **Website and email blocked:** If the government decides to block Internet access to the HQ website and to the RiseUP webmail, an alternative must be found. The Bureau employees can find other secure webmail providers or employ a number of **circumvention** methods to bypass these blocks. It is decided to purchase such software either through http://www.anonymizer.net or the 'Internet Anonym' package from http://www.steganos.com. These tools will give the office computer anonymous access to the HQ servers. Bureau staff research and find many similar organisations offering such access from a fixed computer as well as as from public ones they may need to use in an Internet café. Money for this has been allocated in the emergency budget and 200 USD has been put aside for it.

- **Computer technician:** A previously tried and tested consultant from a computer company will visit the office twice a month for general administration and will be on call for emergency situations. The fee will be 1,000 USD for 6 month.

103
Other possibilities for secure webmail include https://www.bluebottle.com and https://www.fastmail.fm

Budget

■ Bars on windows and door strengthening	500 USD
■ CD re-writer and 10CDs	200 USD
■ Safe	300 USD
■ 2 USB memory cards	100 USD
■ Laptop	1,000 USD
■ Computer Technician	1,000 USD
	Total 3,100 USD
Emergency money: 1000 for PC, 500 for Internet café, 200 for Circumventing Website blocks	1,700 USD
	Budget Total 4,800 USD



4.3 CASE STUDY 3 SECURING AND ARCHIVING DATA

OUTLINE

A human rights NGO, based in a developing country, is providing free legal assistance to victims of human rights violations. They have collected the cases and assisted the town's citizens for five years. Recently, they began to make a submission to the regional human rights court on a particularly complicated and sensitive case of police brutality to one of their clients. Last week, they received two threats from an unknown person – one was by telephone demanding they ceased their work immediately and another - worded by a local policeman. He said that the material they were collecting was considered dangerous to national security interests and could be confiscated at any time. The NGO lawyers are convinced that this is not true and is simply a method of intimidation. They are perfectly satisfied that the case falls within national laws and international agreements. The NGO wishes to pursue this case to the end and has applied to a funder for a small grant to help them increase the security of collected information.

—

The office is located in a well-protected building, with easy access to a busy street. The NGO has an established reputation within the local community and official circles. Their neighbours are always happy to assist and to keep an eye out for intruders. During its five-year operation, office security has not been compromised, the staff feel confident about their location and have established strict policies regarding the handling of office keys and client visits. Recent changes in the local government worry the NGO, as they fear that the police will be given permission to raid their office and confiscate case-related documents. They are prepared to challenge any such action in court but are concerned that the content of the confiscated material could compromise the security of many people. They decide to secure collected information against this possibility. It has also been decided to protect all case-related information collected since their establishment.

—

The office has one computer and the staff possess little technical skill. The computer has internet connection through a dial-up modem and the office purchases Internet cards with temporary connection details. This computer has long since ceased to function properly as it is plagued by viruses. The office cupboards are full of paper relating to cases the NGO has worked on in the past. The grant from the funder came to the sum of 1500USD.

Threats and Vulnerabilities

The NGO staff realise that the main threat they face is having their submission to the court compromised should the police confiscate their case material. This could possibly endanger their clients and witnesses. This threat can be realised by either:

1 confiscation of all documents with a warrant
2 illegal confiscation of documents by force

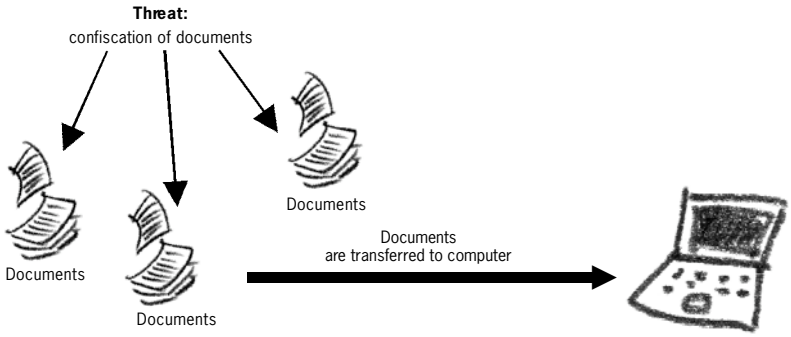
In either case, the outcome will be the same and the information must be protected against both eventualities. The NGO must not only protect this information but ensure that case details remain in their possession so that the work can continue. The NGO makes a list of their vulnerabilities to have a better understanding of what areas need the most attention.

- **notes of cases of violations that exist on paper only are not secure**
- **the computer is not functioning because of viruses**
- **pirated/unlicensed software may be used as an excuse for computer confiscation**
- **files stored on computers are not secure against hackers**
- **there's no backup system for documents in case they get confiscated or lost**

SOLUTIONS

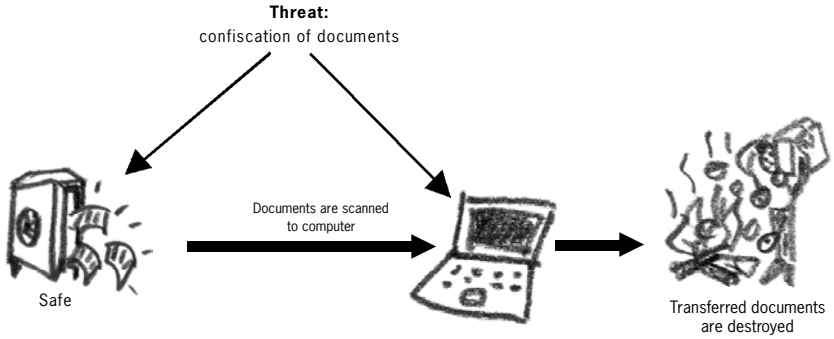
Access to information

It is decided to eliminate the risk, posed by the information that exists only on paper, by transferring it to the computer. The cases on paper will then be destroyed and all the data will be stored electronically, with the possibility of printing the required document upon request.



►Paper documents are scanned to a computer

The information, currently held on paper, must also be stored securely while it is being computerised. For this purpose, a safe will be purchased and all important documents will be kept in it prior to their computerisation, after which they will be destroyed (the staff decide that the safest method to do that will be by burning).



►Redundant paper documents are destroyed

Computers

The NGO staff decide that their current computer is too old and may not be able to handle the large amount of information that will be needed to store all the scanned documents. After searching around the Internet and speaking with their friends, they realise that it is possible to buy a removable hard drive with large storage capacity. It is essentially a hard disk that can be carried around and plugged into any computer.

—

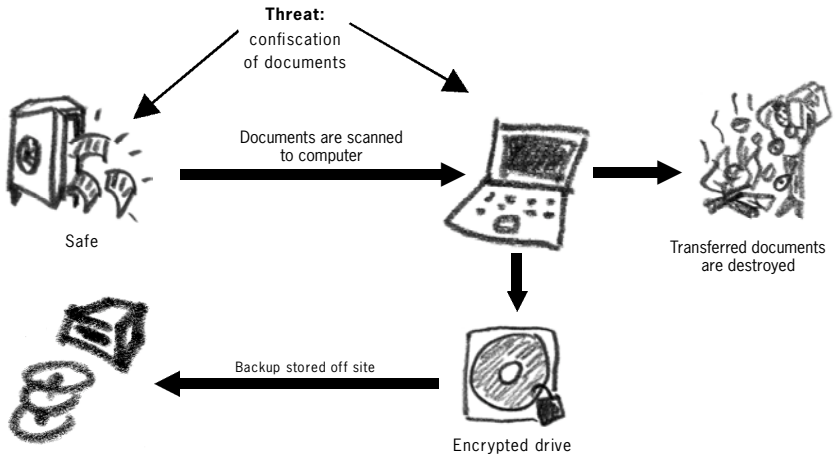
To protect the data stored on the computer, the staff are recommended to use **encryption**. Although no one is really sure how to encrypt, they obtain a copy of the *NGO in a Box – Security Edition*. It appears that the TrueCrypt program will be able to encrypt an entire hard drive so that no one will be able to access it without a password. They decide to encrypt the removable hard disk using TrueCrypt. If the removable hard drive is confiscated, the data on it stays encrypted.

—

Since all the information is centralised, it is essential that a backup system is created, in case the removable hard drive gets damaged or confiscated. The backup medium will be a DVD writer. At the end of each day, a DVD backup of the removable hard drive will be made and taken off site. Since the information on the hard drive is encrypted, it will remain encrypted on the DVDs.

—

Transferral of paper documents to electronic files is done by a scanner. It is estimated that one person operating a computer and scanner can digitise 100 pages per day. If so, the work can be completed within two weeks.



► Electronic documents are protected from loss with the creation of a backup mechanism

Software

The NGO decides to purchase a copy of Microsoft Windows XP Home edition. The justification for this purchase is to ensure that all proprietary software on their computer is properly licensed. Instead of using a pirated version of Microsoft Office, they obtain a copy of the TheOpenCD (comes in package with the *NGO in a Box – Security Edition*) and decide to use Open Office and the GIMP program for scanning files. All other necessary software: anti-virus, firewall, **encryption** and DVD-burning - is also in the Box and is entirely free and open-source. The NGO therefore cannot get into trouble for using illegally obtained software.

DETAILED RESPONSES TO THREATS

Hardware: A staff member is sent to the nearest city to purchase a scanner, a removable hard drive and a removable DVD writer. These are readily available at most computer shops. The items purchased are of reputable brand and on the expensive side. An A4 scanner is priced at 150 USD, the removable hard drive with 100 gigabyte capacity costs 250 USD, and a removable DVD re-writer – 250USD as well.

—

Software: A copy of Microsoft Windows XP Home edition is also found in the computer shop retailing at 96USD. The staff member asks whether the computer shop could provide a technician to install all the hardware and software. There is a technician available and he will do the job for 100USD. The *NGO in a Box – Security Edition* is ordered through the website http://orders.ngoinabox.org. The Box also contains the OpenCD.

—

The computer technician installs a fresh copy of Windows XP and erases all previous data. This is advisable to get rid of all the viruses and malfunctions that previously resided on the computer. He also attaches the DVD writer, the scanner and the removable hard drive. He then installs the following software:

Software	Purpose	Source
Open Office	Open Office Word processing, spreadsheets, presentations, database (fully compatible with Microsoft Office documents)	The OpenCD
GIMP	Image-editing and scanning	The OpenCD
Avast 4	Anti-Virus	Secure NGO in a Box
Spybot	Anti-Spyware	Secure NGO in a Box
Zone Alarm (internet computer)	**Firewall**	Secure NGO in a Box
TrueCrypt (data computer)	Disk **encryption**	Secure NGO in a Box
DeepBurner (data computer)	DVD writing software	Secure NGO in a Box

Encryption: The TrueCrypt program will encrypt the removable hard drive in such a way, that it could be easily copied onto a DVD at the end of each day. The staff create partitions on the removable hard drive, each sized at 4 gigabytes (which complements the amount of storage space on a DVD).

—

The encrypted partition is protected by a password, known only to the operational staff. The same password will be necessary to open this partition from the DVD. The password containing 12 characters and comprising both letters and numbers is chosen. It is not written down anywhere and is memorised by all those requiring access.

Backup: At the end of each day, the dismounted partition, now a file, is copied to the DVD. It is better to re-write the previous version of the file (for this, you will need to purchase a re-writeable DVD recorder and re-writeable DVD disks).

—

The backup DVD is kept off-site – at one of the employees' home. At the end of each week, a separate backup is made and kept at an undisclosed location. This is an additional backup measure, in case the removable hard drive and daily backups are confiscated.

Budget

■ A4 Scanner	150 USD
■ Removable hard drive	250 USD
■ Removable DVD re-writer	250 USD
■ 10 DVD re-writeable disks	50 USD
■ Microsoft Windows XP	96 USD
■ Computer services	100 USD
■ Safe	300 USD
Total:	**1,145 USD**

There is more money left in the budget, in case a new printer or additional DVD disks need to be purchased.

—

The advantage of this system is the increased security of all the documents collected by the NGO. After the initial period of digitising paper documents, there will be no data readily accessible to an outsider. The entire collection of documents will be easily transferable between computers. Even if all equipment is confiscated or damaged, the staff will only require the DVD disk with a backup and another computer with the TrueCrypt program installed. Of course, someone must know the password!

4.4 CASE STUDY 4 SECURE EMAIL AND BLOGGING

OUTLINE

An independent journalist reports on human rights violations in her country. She has a laptop on which she works from home and which she often takes with her on assignments. She writes mainly for foreign publications and uses a pseudonym, for it is dangerous to publish such information in her country, where the media are severely censored and the government is known to have sufficient expertise in tracking online journalists. She also runs a **blog** where all her articles are published, too.

—

She is finding it increasingly difficult to keep working. Her articles sent by email do not arrive at their destination, access to her **blog** site has been blocked and she is afraid of endangering the people whom she interviews and mentions in her reports. She fears that her email is being monitored. On one occasion, an editor wrote to her surprised by the content of her recent article. On re-reading it, she realises that the article has been altered by someone on the way from her email box to the newspaper.

THREATS

Before deciding what actions to take, she lists all the current threats she is facing:

- **cannot send articles by email**
- **cannot access her blog and update it**
- **her assumed identity could be compromised**
- **articles, stored on her laptop, are accessible to outsiders**
- **viruses or hackers could damage the articles on her laptop**

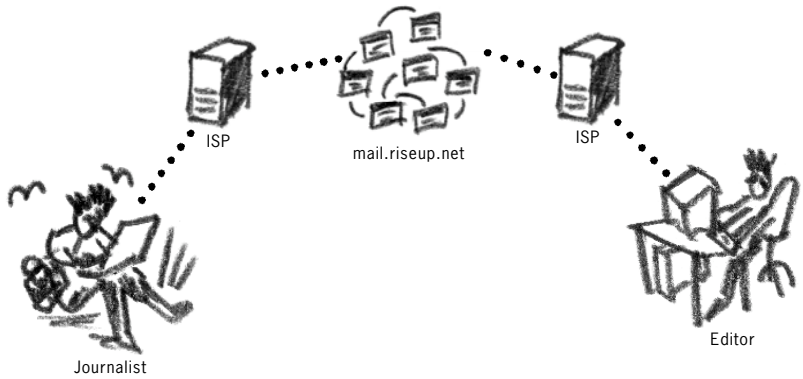
SOLUTIONS

Secure email

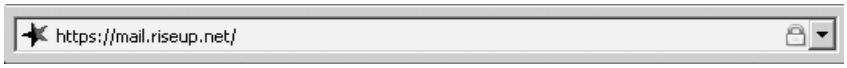
As the first priority, she decides to secure her email box, so that her messages could not be read or altered by an outsider. She writes to www.riseup.net and asks to create an account for her. This is a webmail email account that can only be accessed when she is on the Internet. The webmail operates over **SSL** and is therefore encrypted between her computer and the webmail server. She asks all her correspondents (recipients) to register a free account with www.riseup.net, too, so that her articles could reach them only via encrypted Internet tunnels. She decides to trust the people running www.riseup.net not to compromise or access her email.

—

This appears a simple and effective method for dealing the journalists' concerns. As long as the address bar in the Internet browser through which she accesses her email account begins with 'https:', she knows that her communications are secure.



► Secure communications over **SSL** Riseup.net email accounts

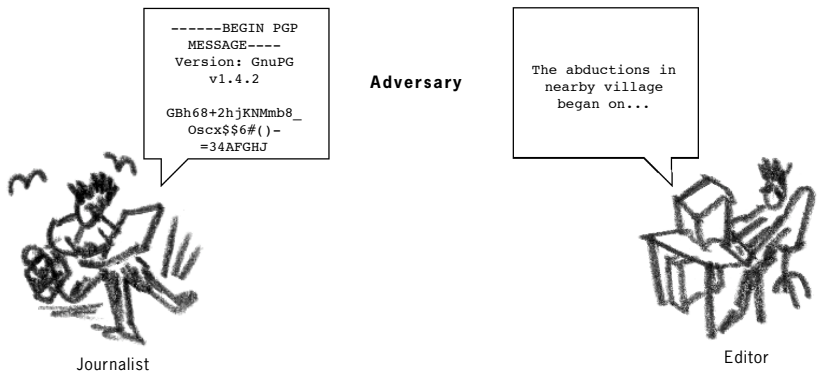


As a further precaution, she writes to www.riseup.net and asks them to send the fingerprint of their **SSL** certificate. They forward her to a page on their website where this fingerprint is shown. The precaution she is taking here is against a Man-in-the-Middle attack, whereby the adversary intercepts the communication line to www.riseup.net and attempts to fool the user into thinking they have arrived at the intended website. An **SSL** certificate is presented and, once the user accepts it, the connection is re-directed to the adversary's website. However, an inspection of the **SSL** certificate will show whether or not it is different from the original.[104]

MD5 Fingerprint	68:82:D8:DC:E1:BF:D0:ED:E0:2F:4C:CA:46:B5:D1:AC

Securing information

Even though she has managed to secure her email box, she would still like to make the articles she sends unreadable to anyone but the designated recipient. This is done in case she loses her email password or it gets compromised. It is also a good precaution against Man-in-the-Middle attacks. By using the GnuPG program, she can encrypt her articles to the public key of the editor. This means that all the parties, with whom she normally communicates securely, will have to install and use a public key **encryption** system (like GnuPG), and swap their public keys with each other[105].

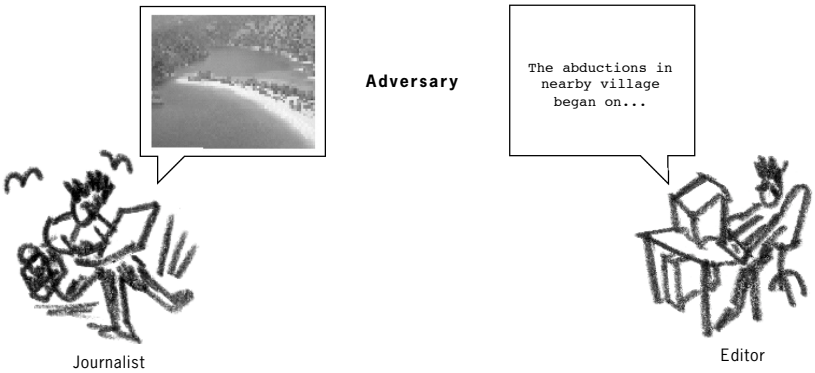


► Using **encryption** to secure sent messages

104
For more info see chapter '**Encryption** on the Internet'

105
For more info see chapter 'Cryptology'. To download the GnuPG program visit http://www.gnupg.orgor find it on the *NGO in a Box – Security Edition* CD

Sometimes, the use of **encryption** may alert the monitoring body. She does not know whether **encryption** is legal in her country and whether using it will just attract a lot more unwanted attention to her. She decides to employ an alternative method that will not immediately appear cryptic and hence suspicious. By using a steganography program, she can embed her article in a photo and upload it to an inconspicuous website. As long as there is a prior arrangement, whereby the editors know where and when to look for this picture/article, this method can bypass many surveillance systems. It should be implemented by maintaining a regular stream of similar activity (uploading photos to the Internet) and should not appear irregular in her normal pattern of activity.[106]



►Using **steganography** to hide the presence of a message in your communications

Anonymous email

Another way of countering email blocking and censorship is to use an array of popular free webmail services. Yahoo, Hotmail, Gmail and others have millions of registered users. It is possible to create a completely new account every time you wish to send an email. The registration details can be random and, if sent from a public space (e.g. an Internet café), the email would be very difficult to track.

—

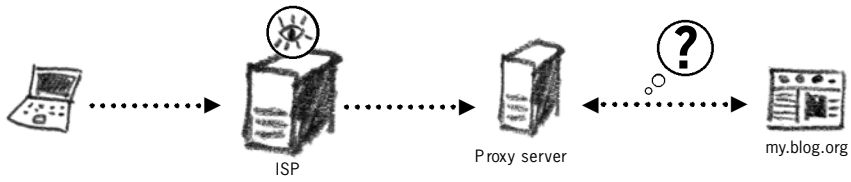
It is likely that secure email services (like www.riseup.net) may already be blocked or will become blocked after frequent use. Only a handful of countries block access to large free email systems, like Yahoo. However, these global providers have in the past cooperated with some governments (e.g. the Chinese government) in giving the latter access to their users' email accounts. Should our journalist decide to use a large webmail provider, her usage must be limited to accessing it from an Internet café or other public space, where her details are not recorded and the IP address, from which the email is sent, cannot be traced back to her. She can also create accounts using a pseudonym, pre-arranged with her editor.

Circumventing website blocks

To access her **blog** site, the journalist will require different methods of circumventing the Internet block inside her country. The choice of tools will depend on the government's blocking practice. For example, she could use a popular commercial product (e.g. 'Anonymizer') or search the Internet for publicly available anonymous proxy servers.[107]

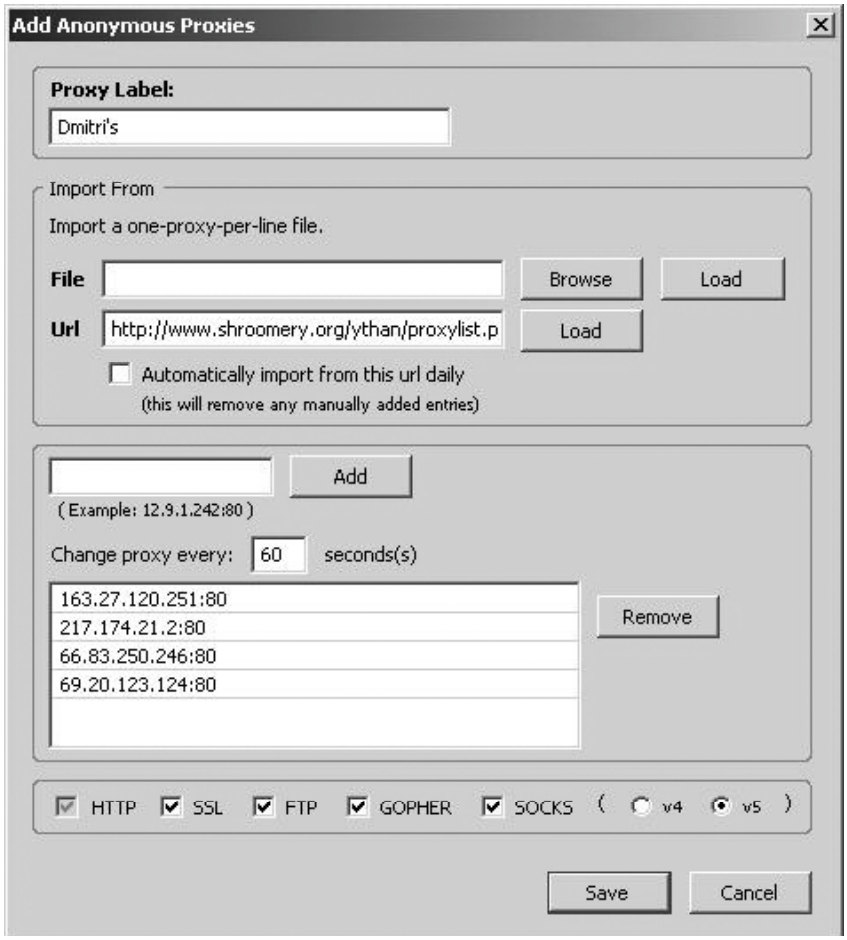
106
For more info see Chapter 'steganography'

107
For more info see Chapter 'internet surveillance, filtering and censorship'



► With an anonymous proxy, the destination website will not know where your computer is really located

On her laptop, she installs the Mozilla Firefox Internet browser and the switchproxy[108] extension. The extension allows her to get to a particular website that lists and updates anonymous proxy server IPs. She sets the program to alternate between the different servers every 300 seconds. Not all servers will function properly all the time.



► The switchproxy configuration screen

By installing the Tor program on a USB memory stick, she can operate without any blocking restrictions, but not all websites may function properly this way. Tor will anonymise her website requests and will penetrate the majority of national firewalls.

It is often easier and more practical to ask a friend from another country to upload your articles onto your **blog**. The articles can be transmitted by any of the above-listed secure or anonymous email methods.

108
see Circumvention of Internet censorship and filtering chapter

Protecting identity

At present, the journalist does not wish her identity to be linked with her pseudonym. She is very careful to not include her real name in the emails and articles she sends through the Internet. Nor does she use her **ISP** email account, as it is linked directly to her. She only uses her home Internet connection to access a secure webmail account or does it in conjunction with an anonymous proxy server, when updating her **blog**.

Some Internet cafés in her town have begun to record their users' names and times of access. She avoids these cafés, as Internet and email activity can traced back to the computer's IP and eventually to her.

When using a computer in an Internet café, she is very careful not to allow the browser to remember her passwords and browsing history. At the beginning of her session, she spends a couple of minutes configuring the Internet browser to be more secure and deletes all saved information from the computer at the end[109].

Securing laptop

All articles are written and stored on her laptop. She must secure herself against their loss, unauthorised entry and damage from viruses and spyware. She sets a **BIOS** password to prevent immediate access to her computer and installs a free anti-virus, anti-spyware and firewall program from the NGO in a Box - Security Edition CD. She updates her Windows software as soon as known fixes become available. Since her laptop has a CD writer, she buys some blank disks and creates a backup of her documents.

Passwords

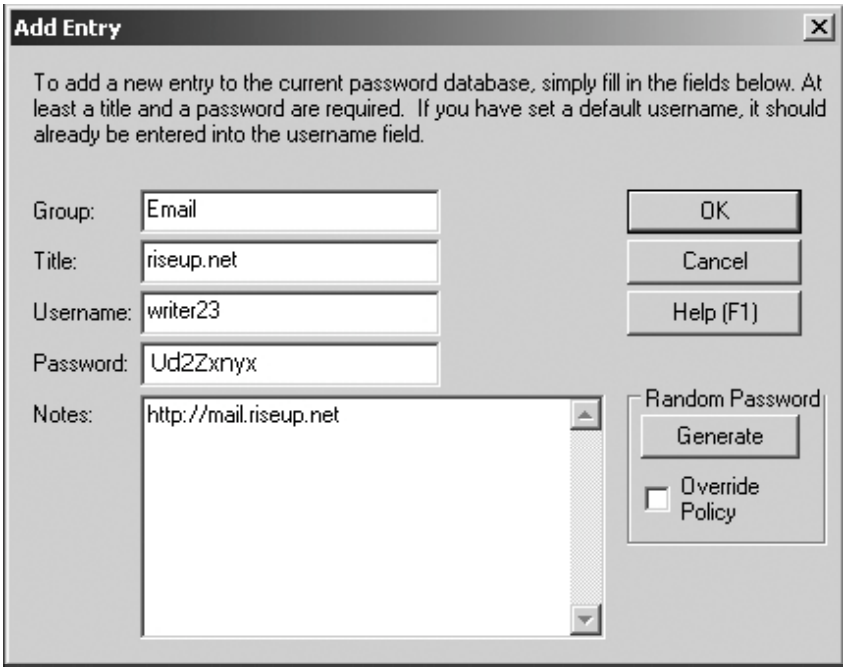
Her laptop, **BIOS**, email accounts, blogs etc. require a password each. These passwords are essential to her security, as even the most advanced system is often only as good as the password that protects it. Since it is impossible to memorise all the passwords, she uses the Password Safe program to store them for her. She has a copy of the program and the passwordfile on her laptop and USB memory sticks. To increase the securit yof her passwords, the Password Safe program creates them for her.

—

To sum up, she has a bag of different tricks and methods to use at her discretion. At first, they may appear laborious and time-consuming, but she knows that her security is paramount. Perhaps a secure laptop and email address will be enough for her to continue her work. As some methods of protection become obsolete or unavailable, she may choose different solutions. The Internet is a vast landscape, with many possibilities for both surveillance and anonymity.

► PasswordSafe

109
Please see chapter 'Internet Program Settings'



► Adding a new password entry

APPENDIX A
COMPUTERS EXPLAINED

A

Consider a future device for individual use, which is a sort of mechanized private file and library. It needs a name, and to coin one at random, "memex" will do. A memex is a device in which an individual stores all his books, records, and communications, and which is mechanized so that it may be consulted with exceeding speed and flexibility. It is an enlarged intimate supplement to his memory.

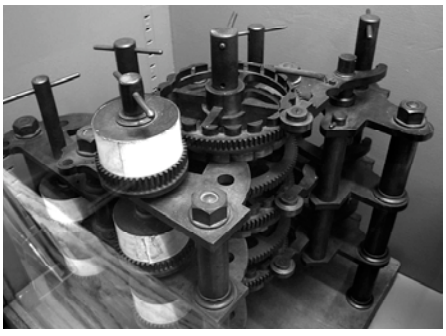
It consists of a desk, and while it can presumably be operated from a distance, it is primarily the piece of furniture at which he works. On the top are slanting translucent screens, on which material can be projected for convenient reading. There is a keyboard, and sets of buttons and levers. Otherwise it looks like an ordinary desk.

Vannevar Bush – Joint Research and Development Group, 1945

HISTORY

The theory and mathematics for creating computers were planted centuries ago. The binary system of arithmetic (using '1' and '0' to perform all arithmetic equations) was invented by Gottfried Wilhelm von Leibniz (1646 – 1716), who was also credited, alongside Isaac Newton, as an inventor of calculus. Charles Babbage is probably the most widely recognised father of early computing. He was the creator of the Difference and Analytical Engines. The latter used punch cards to read in and output numbers, so that a previous calculation could be kept and fed into the computer at a later stage. Babbage describes five logical components of the machine - the store, the mill, the control, the input and the output (in modern terms: hard drive, Central Processing Unit (CPU), software, keyboard/mouse and monitor).[110]

Charles Babbage (1791 – 1871)



1991 Reconstruction of the Difference Engine by the London Science Museum

George Scheutz first heard of Babbage's Difference Engine in 1833, and, with his son Edvard, attempted to build a smaller version of it. By 1853, they had constructed a device that could process 15-digit numbers and calculate fourth-order differences. Their machine won a gold medal at the Paris Exhibition of 1855, and later they sold it to the Dudley Observatory in Albany, NY, which used it to calculate the orbit of Mars. One of the first commercial users of mechanical computers was the US Census Bureau, which tabulated data for the 1890 census with the help of punch-card equipment, designed by Herman Hollerith. In 1911, Hollerith's company merged with a competitor to form a corporation that was to become International Business Machines (IBM) in 1924.

110 http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians


The IBM 5150, released in 1981

PRESENT DAY

The first modern personal computer was called 'Simon' and was built by a couple of students from the University of Columbia. Useless as a processing machine, it was an inspiration to other models. The earliest and the most popular commercially affordable PC was the IBM 5150, released in 1981.

—

No one knows exactly how many computers are in use today. According to a 2002 press release by the hi-tech consultancy firm Gartner Dataquest[111], "..one billion personal computers have been sold across the world". This number excludes personal organisers, mobile phones, video game consoles and myriads of other devices that have become part of our everyday life. Cars and traffic lights are now computer-operated, just like planes and weather reports. Computers generate and store music, check the spelling of our documents and prepare our food. What sounded like science fiction 60 years ago, has become common-place today.

—

Computers have grown increasingly smaller (while operating faster and storing more and more information). Average PCs can now perform a billion operations per second and hold as much data as any local library.

HOW COMPUTERS WORK

Below is a description (and diagrams) of the main components of a computer.

- **Power Unit** – Supplies and regulates electric current to the computer. Laptops also have a backup power source, stored in a battery.

- **CPU** – Central Processing Unit. Performs computer operations. This is a succession of numerous mathematical and logical operations carried out at a great speed. A CPU heats up to high temperatures and must be cooled by a fan.

- **Hard disk** – This is where all the data on your computer is stored. It is usually a rotating magnetic disk. A hard drive must have protective casing as it is sensitive to magnetic fields.

- **RAM** – Random Access Memory. This is a temporary storage unit for data that you are currently using. When you open a program (e.g. a word processor) the computer copies the program from the hard disk to the RAM. When you write a document, it is also stored in RAM. By opting to 'save' the document, you move it to the hard disk.

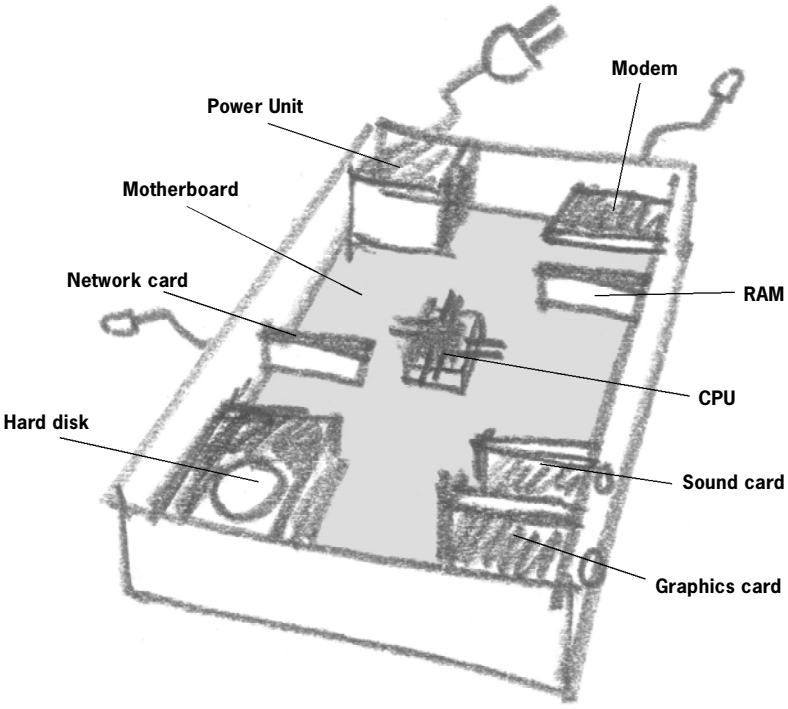
- **Motherboard** – A large integral part of the computer that allows all devices to communicate with each other.

- **Graphics card** – Responsible for the display of information on the monitor.

- **Sound card** – Responsible for the input and output of sound in the computer.

- **Network card** – Responsible for connecting to a network. You can connect to the Internet, provided the network you are on has Internet access.

111
Gartner states that "2005 saw the sale of 285 million PCs and notebooks around the world. The two billion mark should be reached by 2008" sources: http://news.bbc.co.uk/2/hi/science/nature/2077986.stm and http://www.dailytimes.com.pk/default.asp?page=2006%5C01%5C23%5Cstory_23-1-2006_pg6_1



- **Modem** – Connects your computer to an analogue phone line. Variations include ADSL and digital modems. These can be used to connect your computer to the Internet.

- **Monitor** – Displays information from the computer on a screen.

- **Keyboard and Mouse** – Allows you to input data into the computer.

Let's have a look at how some computer operations function:

1 You open a word-processing program and write a document.

CPU ► finds the program on the hard drive and copies it to the RAM ► the graphics card displays the program on the monitor ► you write a page and 'save' the document ► the document is copied from the RAM to the hard drive

2 You check your email and print an email

CPU ► finds the internet browsing program on the hard drive and copies it to the RAM ► the modem connects your computer to www.riseup.net ► you type in your password ► the email is displayed on the monitor ► email is copied to the RAM ► you choose to print ► Motherboard communicates with printer ► document is printed

Note: your email has been copied to your computer, even though you did not ask to save it. You now have a copy in the RAM. This is a standard way computers operate, and it must be taken into account when assessing computer security (also see the 'Windows Security' and 'Data Backup, Destruction and Recovery' chapters).

Computers are all about speed and capacity. Here's a rough guide to understanding how these are measured:

Let's assume that the character 'A' requires 1 byte of storage capacity.

```
8 bits = 1 byte (B)
1024 bytes = 1 kilobyte (kB)
1024 kilobytes = 1 megabyte (MB)
1024 megabytes = 1 gigabyte (GB)
1024 gigabytes = 1 terabyte (TB)
```

Note: the measuring unit of 1024 is because it is a factor of 2, necessary for a digital system.

Let's assume that one computer operation per second is called a *hertz*

```
1000 hertz = 1 kilohertz (kHz)
1000 kilohertz = 1 megahertz (MHz)
1000 megahertz = 1 gigahertz (GHz)
```

So, a computer with a speed described as 1.3GHz/s performs 1,300,000,000 operations per second.
Which is a lot faster than 'Simon'.

OPERATING SYSTEMS

All computers require instructions in order to function. The main source of these instructions, and the bridge that connects all computer parts, programs and us – the users – is an operating system (OS). You are probably aware of Windows, which is the most popular operating system and is produced by Microsoft. Its popularity is the result of easy-to-understand graphical interfaces, successful contracts with computer manufacturers and aggressive marketing strategies.

—

Numerous versions of Windows have been produced. When you buy a new computer, it is likely to have Windows already installed on it. The Windows OS is not free, and you must have a valid licence. This is not the case with all computers: many have an illegal 'pirated' version of Windows. Many computer enthusiasts and technicians despise Windows for its marketing strategies, flawed programming and monopoly of the market. Some of them try to discover vulnerabilities in the operating system and either alert Microsoft to create a fix or write viruses, taking advantage of these flaws and corrupting the data on the computers that become infected.

—

*There are many alternatives to the Windows OS. For instance, the Apple com*puter runs its own OS. There is also Linux, which is a free operating system that became very popular due to its distribution on the Internet. Linux was written by many different people who are not employed by any company. A product of mass voluntary participation, it is released for free. Many different versions (including language distributions) of Linux have come onto the market, and the majority of them are free.

SOFTWARE – PROPRIETARY VS FOSS

A

A piece of software is regarded as the intellectual property of its creator (like a book or a film script). A licence to use it is sold along with the computer code. The practice of pirating software. i.e. breaking the licence code or simply running software without a valid licence, is wide-spread around the world. Many governments have passed legislation that protects software under the law on intellectual property. Harsh penalties are handed out to individuals and organisations caught using pirated software.

—

Not all programs carry the licensing restrictions mentioned above. Just as you can volunteer your time and skills for a particular non-profit or charitable purpose, some programmers create and then distribute their software for free. This software is often written using open source. This means that the programming code is open for inspection, modification and improvement. Volunteers translate this software into their own languages and release it for free distribution. This type of software is described as FOSS – Free and Open Source Software. You can find almost any kind of it on the market.

—

A fully licensed Microsoft Office suite will costs you between 200-500USD[112] per copy, whereas the OpenOffice (available on the OpenCD) is distributed for free. Both of them are very similar in their operations and functionality: they create the same document types. Issues of inter-operability between a '95 and earlier versions of Microsoft Office and Open Office have been raised. The solution is to switch your office and the colleagues you communicate with over to one product entirely. This may not be an easy task, but if you are concerned for the legality of your software, you should consider getting away from Microsoft products, or else purchase their licences.

—

FOSS will release you from the legal problems of proprietary software piracy. Although FOSS may not be as user-friendly (in terms of installation, intuitive guidance and graphics) in helping you with the program or offering the same support as paid-for software, it has a large community of users, who have set up numerous forums to answer your common questions and will address any new queries you may submit. In essence, you will find a more responsive and detailed support network in the open-source community than the one offered by the costly and constantly 'on-hold' technical support number for the latest version of Microsoft Windows.[113]

112
Different prices found by searching the Internet in September 2006

113
For more info see the Free Software Foundation http://www.fsf.organd the Open Source Initiative http://www.opensource.org/

APPENDIX B
INTERNET EXPLAINED

HISTORY

The idea of interconnecting computers in different geographic locations emerged after WWII. While computers were still in their infancy, the concept existed only in the minds of futurologists and philosophers. The Soviet launch of the 'Sputnik' satellite prompted the US government to invest heavily in technology research and development. The Advanced Research Project Agency (ARPA) was established in the late sixties, and by 1969 four computers had been connected to the ARPANET. In 1972, Robert Kahn held a successful demonstration of the ARPANET to the International Computer Communications Conference and introduced a new application for it – email. The ARPANET network was the grandfather of the Internet as we know and use it today.

—


Illustration 49: Robert Kahn

In 1977 the ARPANET connected 111 computers, and by 1985 the network had reached Europe and Australia. The Internet was becoming global and de-militarised. 1983 saw the introduction of TCP/IP version 4 – a protocol with which any computer in the world, irrespective of its make or model, could communicate with any other on the same network. This technical breakthrough is regarded as the birth of the Internet. Robert Kahn developed the Transmission Control Protocol/Internet Protocol with four basic principles:

- **Network connectivity**. Any network could connect to another network.
- **Distribution**. There would be no central network administration or control.
- **Error recovery**. Lost packets would be retransmitted.
- **Black box design**. No internal changes would have to be made to a network to connect it to other networks.

TCP/IPv4 is still the common protocol of the Internet today. Its very structure has so far ensured that no particular person or company runs the Internet, and that all who connect to the Internet are given unrestricted access to its content (we have discussed Internet censorship and filtering earlier).

THE WORLD WIDE WEB

The most popular way of using the Internet today is through the World Wide Web (WWW). The Internet itself is the physical connection of computers with computer networks, whereas the WWW is one specific platform for these computers to communicate upon. The concept and technology of the WWW were developed by Tim Berners Lee and Robert Cailliau at the nuclear physics laboratory *Conseil Européen pour la Recherche Nucleaire (CERN)* and made public in 1991. The WWW's main features were:

- **links** – (hyperlinks) that connected one webpage to another
- **communication** – HTTP (hypertext transfer protocol) - an electronic language spoken by computers on the Internet.

- **webpages** – HTML (hypertext markup language) used to design webpages and interact with others by means of links.
- **addresses** – URL (universal resource locator) - an addressing system for referencing web pages and other information on the Internet.

Together they constitute the building blocks of the Internet we use today. Basically, every webpage has an address, is written in HTML and has links to other webpages on it. The communication between websites is performed by TCP/IP.

INTERNET TODAY

According to the Internet Statistics Survey, there were over 1 billion Internet users in January 2006. This is an incredible figure, considering that no one heard of the Internet in 1990. It has become a primary method of information storage and exchange for many people. In its essence, it encourages participation and global community awareness. In the beginning, most people assumed that the Internet would not be popular, for too much investment was needed to make it a useful source of information, similar to a library. The breakthrough came when it became clear that anyone could construct web pages and contribute to them. Amazon.com was flooded with book reviews, while enthusiasts of different sports or hobbies would start their own websites, inviting like-minded people from anywhere in the world to join them in discussions, thus creating a virtual community. People embraced the technology and the possibilities offered by the Internet. eBay was originally dismissed as unworkable, for it allowed two people, who had never met, to trade goods, without a guarantee that the goods or the money would materialise. Now, over 50 millions auctions are taking place on the eBay website each year, and over half a million people earn their living by trading on it.

—

A significant recent example of the power of the Internet is Wikipedia.org - an online encyclopaedia, with articles written and edited by the Internet community. Within 5 years since its foundation, Wikipedia.org had over one and a half million articles in English and at least one hundred thousand in ten more languages. Its popularity lead to an independent evaluation of the accuracy of its information as compared to Encyclopaedia Britannica. The results showed that the two encyclopaedias were just about as accurate as each other.[114]

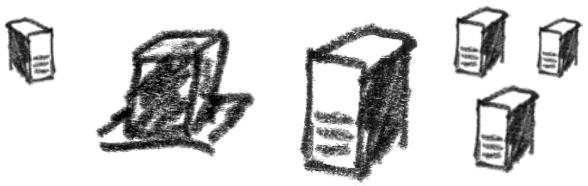
BASIC INFRASTRUCTURE

The Internet is the ultimate distributed network. This means that it has no central base or server. Yet, it does apply standards to the way it operates (called protocols) and to the organisations that develop these standards. Today's Internet has 3 main layers to its operation. First, there is the telecommunications infrastructure. A collection of telephone cables, optic fibre, microwaves and satellites - all working together to ensure that Internet traffic reaches the world's every corner. The second layer are technical standards and services. It is composed of different protocols, directing the traffic around the infrastructure and allowing us to view webpages and send email. It is on this layer that we connect to the Internet. The last layer: content and applications - is where all the web pages and Internet services operate. One of the Internet's main strengths is that each of these layers operates independently[115].

114
http://news.bbc.co.uk/2/hi/technology/4530930.stm

115
Internet Governance – The infrastructure and standardsation basket

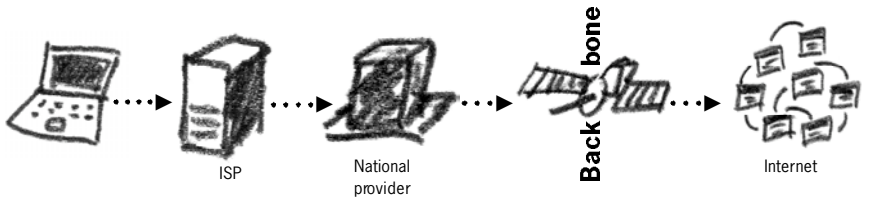
Content and application standards



Technical standards (TCP, IP, DNS etc.)

Telecommunication infrastructure

Let's look at how the Internet functions from the end user's point of view. First, we need to be connected to the Internet. This can be done by creating an account with an **Internet Service Provider** (**ISP**), which in turn, purchases its own access from a national provider. National providers receive their connection from one of the multinational companies that maintain the Internet's backbone. The backbone is a high-powered and high-bandwidth structure, with global connections via underwater cables and satellites, that enables communications between countries and continents. Also known as Tier1, it is run by companies such as MCI, AT&T, Cable Wireless, and France Telecom.



When you get connected to the Internet, your computer is assigned an IP address. Like a postal address, it uniquely identifies this computer on the Internet. Depending on your **Internet Service Provider**, you may be assigned different IP addresses at different connection times. All web sites and web servers have an IP address.

www.frontlinedefenders.org is actually 217.67.142.198

However, when we want to visit a website, we don't request to see 217.67.142.198 but type in www.frontlinedefenders.org instead. There exists a method to translate the IP numbers into common languages names. It is called the Domain Name System (DNS), and there are dedicated computers on the Internet whose function is to perform these translations.

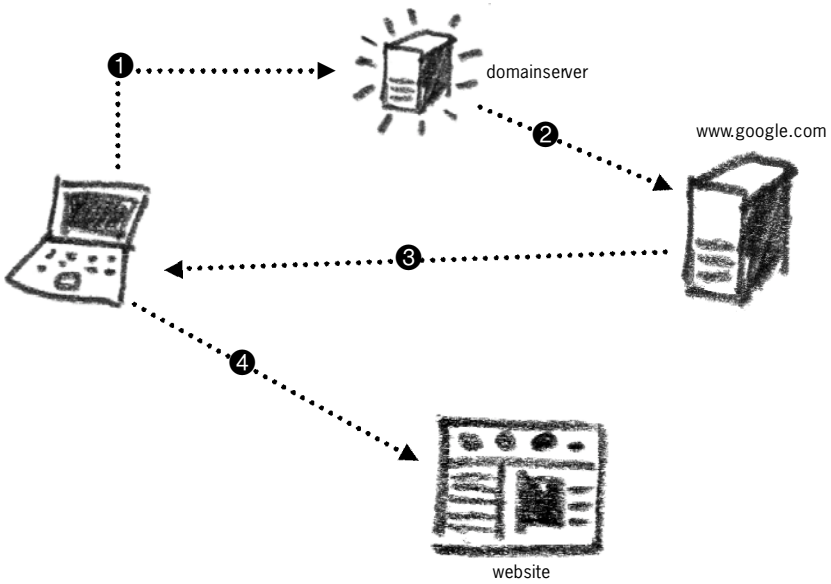
Therefore, we don't have to burden ourselves with memorising complex number combinations, but only have to remember linguistic descriptions of the website name.

—

DNS relies on root servers. These are, in plain words, several chosen computers that maintain a list of the most important website names and their relevant identifiers (.COM .ORG .NET .GOV, etc.). Some of these computers are privately owned and some are operated by the US government agencies. The majority of these servers are currently located on the East Coast of the USA. The DNS structure is administered by the Internet Corporation for Assigned Names and Numbers, operating under the jurisdiction of the US Department of Commerce. In effect, some of the major players (those who own and manage the root servers), like Verisign (a private US company), have the power of veto in this ruling body – the fact that has become a contentious issue for those fearing that the US exerts too much control over the Internet.

—

To see a web page from your computer, you must request it by typing its website name into the URL. The Internet then finds the website IP by querying the DNS. Eventually, a path from your computer to the destination website must be found. This path could travel through countries, oceans and space; it could be thousands of miles long and could pass through numerous computers. How does it know which way to go, when there exist hundreds of millions of different websites? The task of directing your message to the website (and back) is performed by routers, and the process is known as routing. These routers can be manipulated to record or re-direct their packets or to block access to certain websites.



► Example of how your message travels on the Internet when finding a webpage through Google

1. You type in www.google.com The computer looks to the DNS server to find Google's IP
2. The DNS server forwards you to www.google.com
3. You type in your search query and are given the results by Google
4. You are directed to the result page (note: it is possible that your computer will find the IP of this webpage via the DNS server again)

Every computer or router, which you go through to get to your destination, is called a hop. The number of hops is the number of computers/routers your message comes in contact with along its way. Below, is the path my computer makes on the Internet to get to www.google.com. You can see that my request will pass through at least 13 computers (hops) to get to its destination.

```
traceroute to www.l.google.com (66.249.93.99), 64 hops max, 40 byte packets
 1 217.67.143.157 (217.67.143.157)  74.53 ms  30.910 ms  49.643 ms
 2 217.67.140.61 (217.67.140.61)  29.780 ms  28.60 ms  29.628 ms
 3 217.67.131.10 (217.67.131.10)  49.987 ms  29.872 ms  29.615 ms
 4 217.67.131.6 (217.67.131.6)  40.267 ms  34.815 ms  40.219 ms
 5 85.91.0.61 (85.91.0.61)  41.237 ms  39.192 ms  38.831 ms
 6 208.50.25.109 (208.50.25.109)  31.452 ms  115.234 ms  37.396 ms
 7 so0-0-0-2488M.ar3.LON2.gblx.net (67.17.71.25)  89.496 ms  44.303 ms
   46.455 ms
 8 ldn-b1-pos2-0.telia.net (213.248.100.1)  47.497 ms  44.190 ms  45.240 ms
 9 google-104716-ldn-b1.c.telia.net (213.248.74.194)  52.678 ms  89.984 ms
   61.543 ms
10 72.14.238.246 (72.14.238.246)  69.863 ms 72.14.238.242 (72.14.238.242)
   59.778 ms 72.14.238.246 (72.14.238.246)  75.364 ms
11 216.239.43.91 (216.239.43.91)  65.671 ms  61.264 ms  53.603 ms
12 72.14.232.141 (72.14.232.141)  55.727 ms  54.204 ms 216.239.43.88
   (216.239.43.88)  54.456 ms
13 64.233.175.246 (64.233.175.246)  72.265 ms  53.48 ms  55.586 ms
14 66.249.93.99 (66.249.93.99)  54.490 ms  113.495 ms 66.249.94.46
   (66.249.94.46)  57.798 ms
trace complete
```

If you have used the Internet before, you know that, despite its seemingly complex structure, it is very easy to operate. This simplicity is the result of its stable architecture, as explained above. It allows us to quickly locate what we need in the ocean of electronic information. DNS servers and routers are responsible for coordinating this process. If someone can control or influence their operation, our use of the Internet will be damaged or restricted.

EMAIL

Electronic email is composing electronic messages and sending them around the Internet. Anyone can register an email account on the Internet, or receive one from their **ISP**, and these hosts will become our email providers. Every email account has a unique address (dmitri@email.com) where the user name is separated from the provider's address by a '@'.
Email is sent around the Internet following the same principles of DNS and routing. First, the email provider is found by its domain name (e.g. email.com), then the provider is queried for the existence of a particular user account (e.g. dmitri). If the information is correct, the email is delivered. If not, the email is returned (or bounced) to us with an error message.

Every email message you send or receive contains the following information:

- the name registered for the email account (e.g. dmitri vitaliev)
- the email address
- The IP number of the originating computer or email provider
- The route taken by the email to get to its destination
- The date the email was sent and received

This information is stored in email message headers and usually looks like this:

```
Received: from hotmail.com (bay17-f12.bay17.hotmail.com [64.4.43.62])
by mail2.frontlinedefenders.org (Postfix) with ESMTP id 5AB164F
for <dmitri@frontlinedefenders.org>; Thu, 20 Jan 2005 14:44:06 +0000 (GMT)
Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC;
         Thu, 20 Jan 2005 06:44:04 -0800
Received: from 217.67.142.198 by by17fd.bay17.hotmail.msn.com with HTTP;
        Thu, 20 Jan 2005 14:43:58 GMT
Message-ID: <BAY17-F12DBF0F22EC08A06194JKDB9810@phx.gbl>
From: "Dmitri Vitaliev" <dmitri@hotmail.com>
To: dmitri@frontlinedefenders.org
Date: Thu, 20 Jan 2005 15:43:58 +0100
Content-Type: text/plain; format=flowed
X-Originating-IP: [217.67.142.198]
X-Originating-Email: [dmitri@hotmail.com]
X-Sender: dmitrv@hotmail.com
```

This example shows a message header for the email sent from dmitri@hotmail.com to dmitri@frontlinedefenders.org. You can see the IP of the Hotmail servers (64.4.43.62) and the IP of the computer the email was sent from (217.67.142.198).
All our email and Internet traffic are identified and recorded by the destination/origin IP and the time sent/received. This information is used to authenticate our message and its delivery. At times, it is also used to monitor and restrict our activities on the Internet. The crucial Internet infrastructure, described above, is rather lucrative for surveillance and censorship, simply because security was not on the minds of the original Internet developers.

WEBSITES

A website is a collection of pages written in HTML (and other Internet adaptable languages). A website must reside on a **webserver**, also referred to as a **host** The host provides an IP address for the website, and you must also register a unique DNS name for it, e.g. www.mywebsite.com. One website could share its IP address with many others residing on the same host, yet they will all have unique DNS names.

—

For stability and security, some websites are mirrored by being copied to different hosts, often in different countries. If your primary website breaks down or is blocked from access, the mirror takes over.

VoIP

Voice over IP is a technical name for "Internet based telecommunications". Instead of using the telephone exchange network, you can have a voice conversation over the Internet. It is an increasingly popular method of communication, because after the initial set-up costs, you are not paying long-distance charges: geographic location is irrelevant to the Internet. Skype is probably the best known program (with around 100 million subscribers) using this technology at the moment[116]. VoIP has become a major competitor to traditional telecom companies and has faced stiff opposition in the countries trying to maintain the monopoly of telecommunications.

Blogging

This is perhaps the most influential recent feature on the Internet. An online diary or an opinion column in its essence, it can be created by anyone on any of the Internet's multiple free **blog** hosts. You do not need to set up a **webserver**, nor do you bear any costs. Sometimes, the webpage structure is already custom-built, and all you have to do is fill it up with your content. Blogging provides an opportunity to voice your opinion on any subject of your choice.

—

In stark contrast to traditional media that expects consumers to simply digest the information presented to them, online publishing is the closest available proximity to a global voice. It is a collection of every article, opinion and **blog** (currently there are around 50 million blogs) on every existing subject. It carries totally unedited information that only expresses the opinion of its publisher.

—

'Citizen journalism' is a term, applied to those who report on news, events and changes in their countries through a **blog**. Often, it is the only source of 'real' news from a country. 'Citizen journalism' has become a powerful weapon in the struggle for freedom of expression, and therefore it is heavily monitored and stifled by oppressive regimes.

116
You can download Skype from http://www.skype.com or see *the NGO in a Box – Security Edition* CD. There have been many debates as to the security of Skype communications. Even though Skype uses **encryption** to secure instant chats and file transfers, their program code is closed and the security cannot be verified by external experts. See the paper written by Simon Garfinkel on Skype security http://www.tacticaltech.org/files/tacticaltech/Skype_Security.pdf

APPENDIX C
INTERNET PROGRAM SETTINGS

This chapter will review the security settings of today's two most popular Internet browsers. To prevent the installation of malware on your computer, to erase temporary files – the result of your browsing activity - and to offer you the best possible protection against other Internet insecurities, it is important to make sure that your Internet browsing program is configured correctly .

The are several precautions you should take when using any Internet-browsing program. The main point is never to visit a website 'just for the sake of it'. The Internet, like a dark alley in a strange neighbourhood, has become an insecure place to browse. If you are on your work computer, only go to the sites you absolutely have to visit.

—

Do not install any programs that make it easier for you to fill out web forms and to save your passwords or offer other seemingly useful features. Most of these programs come with a bunch of spyware, advertising and other malicious code in hand. Never ask your browser to remember a password for you – use a password program (*NGO in a Box – Security Edition*). In short, do not try to make your web browsing easier by installing additional software.

INTERNET EXPLORER

Internet Explorer (IE) has a reputation of being the least secure out of all Internet browsing programs. If you are using Microsoft Windows, you have Internet Explorer already installed. It is very difficult and often impossible to uninstall this program from your computer. Your can either strengthen the security of IE or install a parallel browsing program.

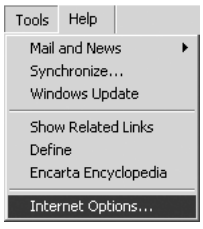
—

Always make sure you are using the latest version of IE and have installed all the necessary updates provided by Microsoft. On the menu bar select:

```
Tools > Windows Update
```

Let Windows check your computer and present a list of necessary updates. Alternatively, you can go to www.microsoft.com/windows/ie/ie6/downloads and choose to download IE6 in the desired language manually.

Basic Security Settings

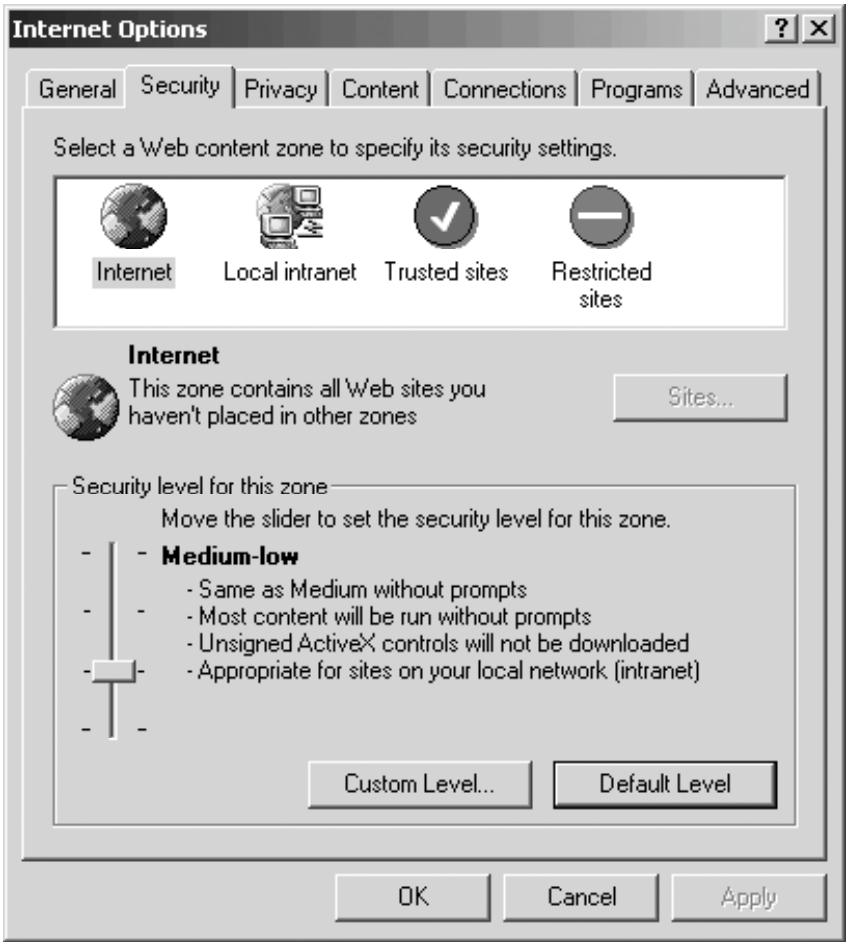


IE can be a reliable and secure browser, if you specify to it which websites you trust and which you do not. By default we should ask it to NOT trust any websites unless we allow it to do so.

```
Tools > Internet Options
```

Go to "Security" tab and move the security level bar on this "Internet zone" to "High". If you can't see the security level bar, click "Default level" and

move it to "High". This will protect you from many dangers, like, for example, harmful Active-X content



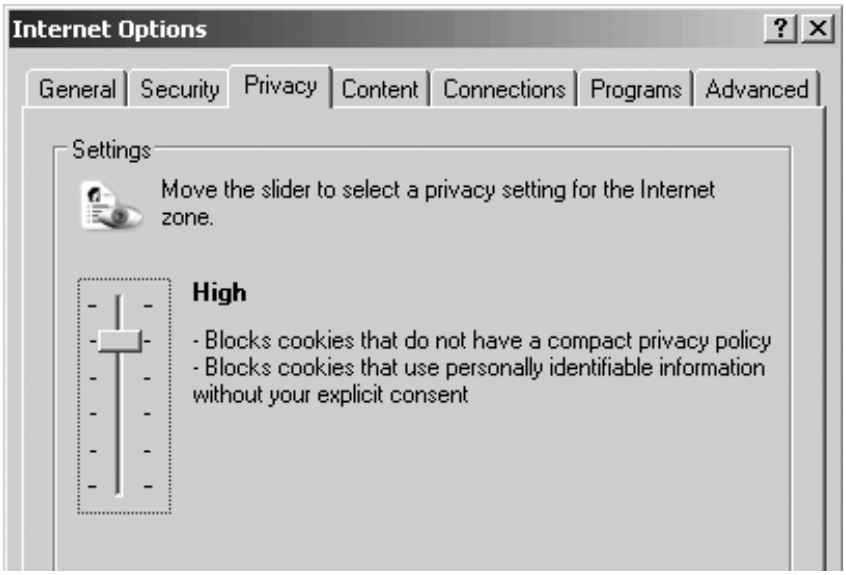
► Internet Explorer options

Click "Trusted Sites" and move the security level bar to "medium low". If you can't see the security level bar, click "Default level" and move it to "Medium low". You must add sites you absolutely trust to your "Trusted Sites" by pressing the "Sites" button. Add pages like *.microsoft.com, *.bbc.co.uk, *.frontlinedefenders.org, any webmail you use and other websites you regularly visit and trust. Press "Add". Now, all the pages belonging to Microsoft (like http://windowsupdate.microsoft.com, for example) are considered trusted. The * denotes that all web pages within this domain are treated as such. Also, remember to disable "Require server verification (https) for all sites in this zone"! The sites you add will be able to function to their full capacity and will not be restricted by any security limitations, so that cookies, JavaScript, Active-X, etc. will work in these pages. Press OK to go back to the rest of the settings.

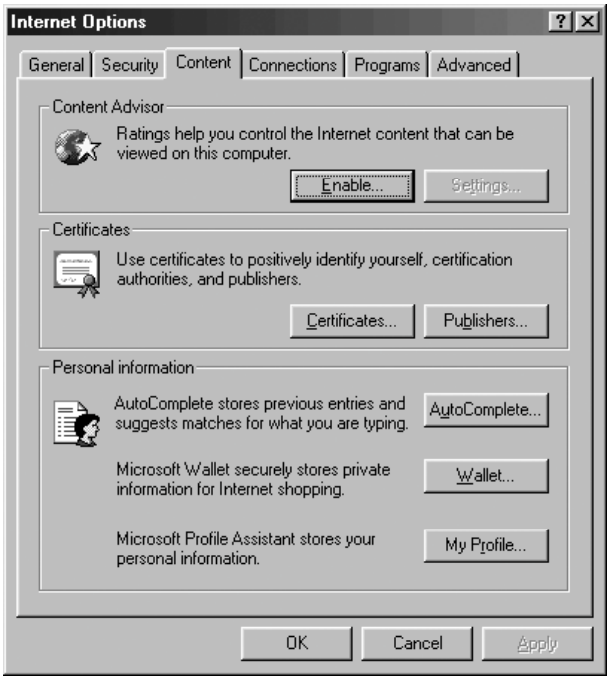
—

Next, click 'other zones' and change security preferences on them to 'High'. This will ensure that all zones other than 'Trusted Sites' zone are as secure as possible. Note that from now on the sites that are not listed in the 'Trusted Sites' category will be limited in their function on your PC. Some may not even load. This may be frustrating at first, but is an excellent way to secure your Internet browsing experience with IE.

Go to the next page, called 'Privacy', and move the bar to the top. This makes sure no cookies from Internet sites are stored on your computer. The pages you have added to your 'Trusted Sites' will still be able to download cookies.



Go to the next page, called "Content", and in it - go to "Autocomplete". Disable all marks. This makes sure that no passwords or forms are saved to the browser that someone might use for malicious purposes. Passwords are meant to be memorised or kept in a password program (see 'Passwords' chapter), not written down anywhere! Also, remember to clear both the passwords and the forms fields. Press OK to go back to rest of the settings.

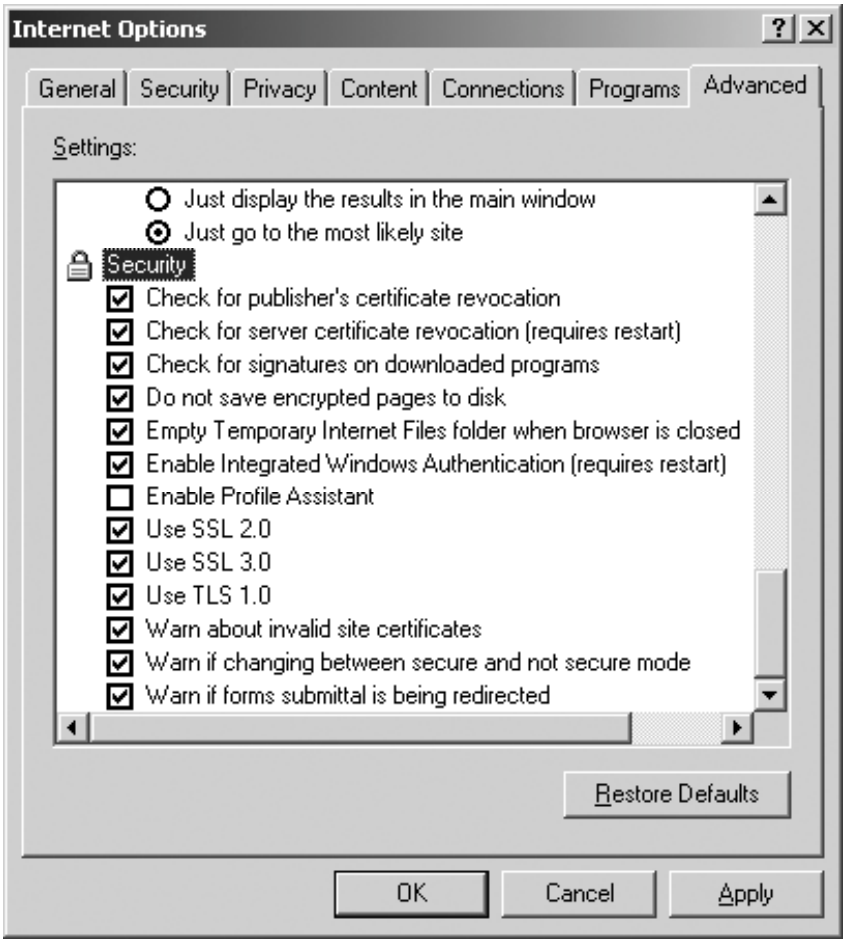


Go to the "Advanced" page and make sure you have the following enabled:

- Automaticaly check for Internet Explorer updates"
- Use SSL 3
- Use TLS 1
- Check for signatures on downloaded programs
- Check for publisher's certificate revocation
- Check for server certificate revocation
- Do not save encrypted pages to disk
- Warn about invalid site certificates

Make sure you have the following disabled:

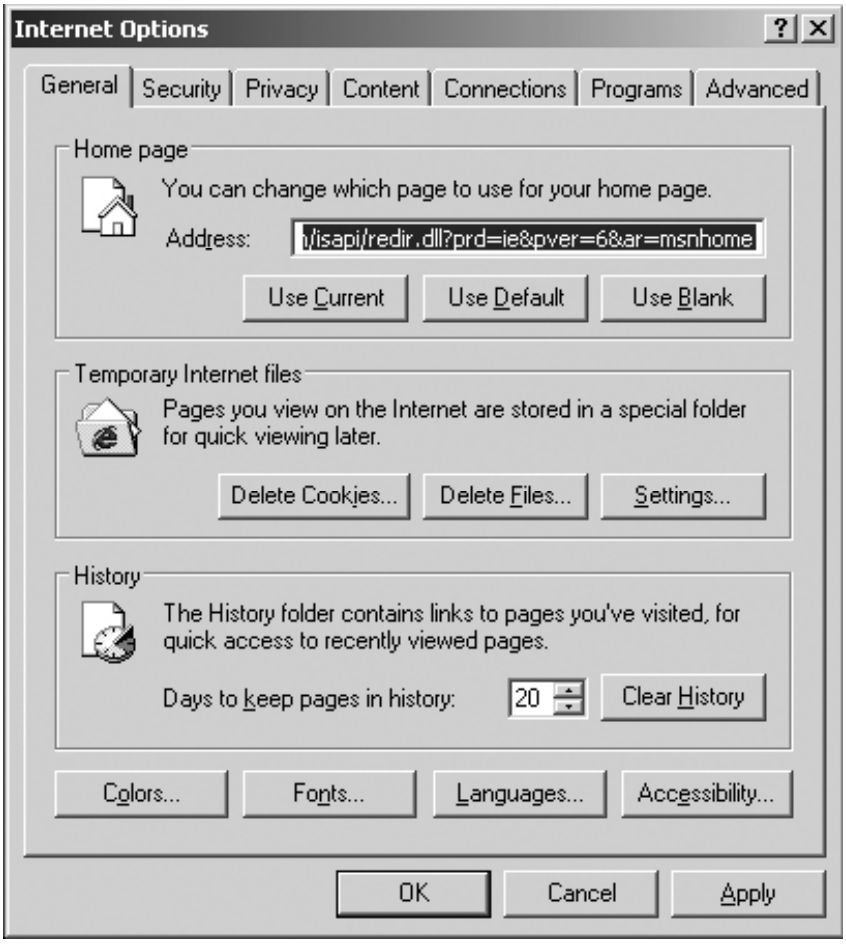
- Install on demand -other
- Use AutoComplete
- Use third-party browser extensions
- Enable install on demand
- Enable integrated Windows authentication



Deleting Temporary Files

It is good practice to delete the temporary files our Internet browser collects during the working session. This is particularly important when using public computers. Even though these actions will not wipe the temporary data (see 'Information Backup, Destruction and Recovery' chapter), they will delete it from immediate access by an outsider. At the end of every session, run the following commands in the IE browser.

Tools > Internet Options
General Page
Click the 'Delete Cookies', 'Delete Files' & 'Clear History' buttons in succession.



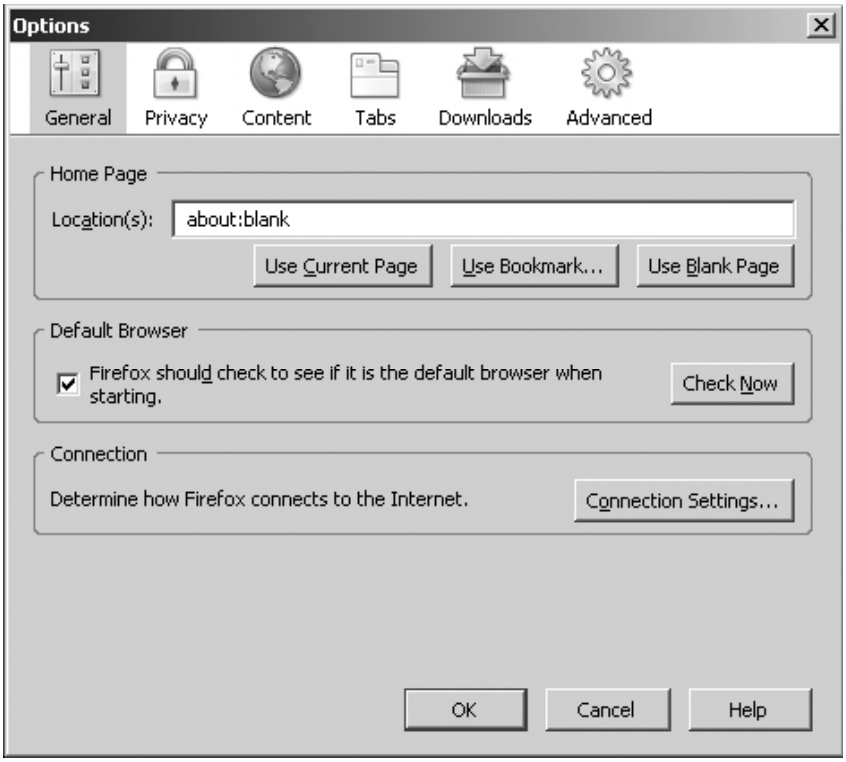
MOZILLA FIREFOX

The Firefox web browser, a recent addition to the world browser market, has proved tremendously popular. It is reclaiming the market monopoly from Internet Explorer. Its main advantages are high security settings, built into the browser by default, and the fact that it is written in open code, meaning that anyone with some programming skills can write an additional program to work alongside it (extensions) or improve the browser's functionality (plug-ins). The majority of existing spyware will not affect your computer, if you browse the Internet through Mozilla Firefox.

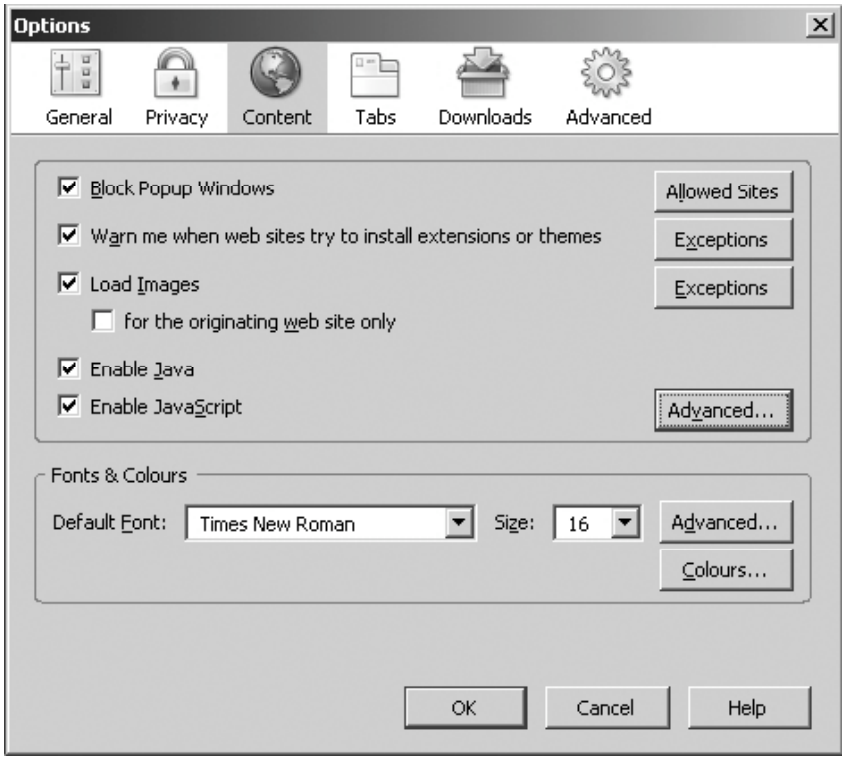
Basic Security Settings

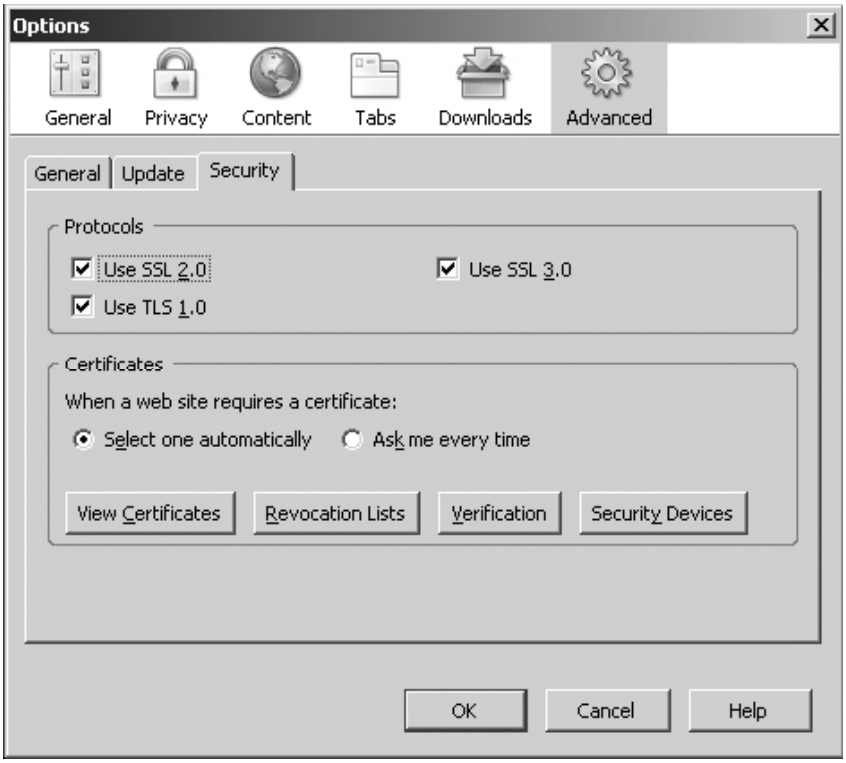
In the Firefox browser go to:
Tools > Internet Options

On the 'Content' page, you can specify Firefox to block pop-ups, run Java and Java script. You can leave these settings as they are, by default, or modify them.



Make sure the 'Advanced' page has all options enabled and for certificates – 'Select one automatically'.



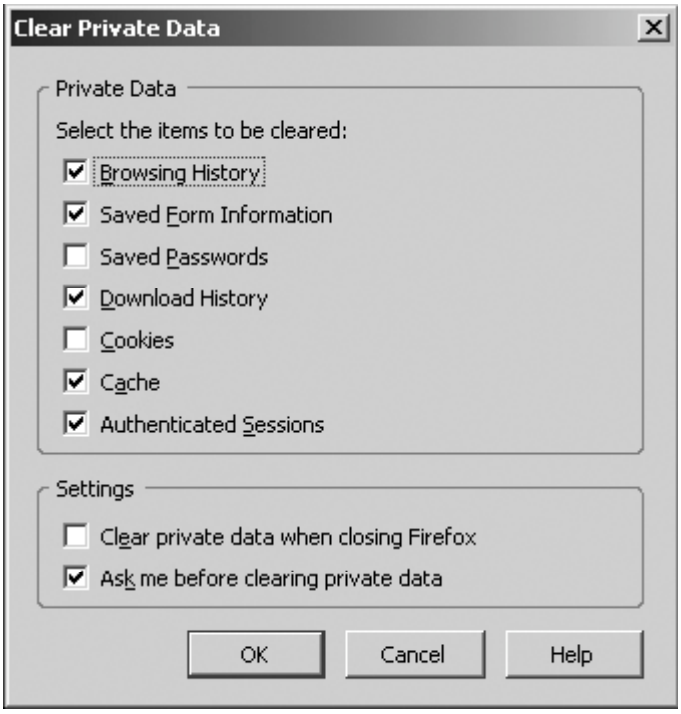


Deleting Tempora ry Files

Firefox makes it very easy to delete temporary data from the computer. In the 'Internet Options' window, click on the 'Privacy' page and the 'Settings' button in the bottom right-hand corner.
Enable all functions to be deleted upon exiting the program.

This will be executed automatically when closing the program down. To enable file deletion whilst using the Firefox browser, go to

`Tools > Clear Private Data`
`Press OK.`



APPENDIX D HOW LONG SHOULD MY PASSWORD BE?

Let's see how long it would take a computer program to guess your password. Assuming your password is made up only of lower-case English letters, we will calculate the maximum number of possibilities the password cracker needs to sort through.

Password Length	**3**	**5**	**7**	**9**
Calculation	*26 x 26 x 26*	*26 x 26 x 26 x 26 x 26*	*26 x 26 x 26 x 26 x 26 x 26 x 26*	*26 x 26 x 26 x 26 x 26 x 26 x 26 x 26 x 26*
Number of possibilities	*17,576*	*11,881,376*	*8,031,810,176*	*54,295,503,678,976*

Now, let's add digits and upper-case letters to our password. This increases the variations of every character to 62 different possibilities.

Password Length	**3**	**5**	**7**	**9**
Calculation	*62 x 62 x 62*	*62 x 62 x 62 x 62 x 62*	*62 x 62 x 62 x 62 x 62 x 62 x 62*	*62 x 62 x 62 x 62 x 62 x 62 x 62 x 62 x 62*
Number of possibilities	*238,328*	*916,132,832*	*3,521,614,606,208*	*13,537,086,546,263,552*

As you can see, the probabilities increase dramatically when you add variation into the password characters and when you increase its length. But how quickly can computers break these passwords? We will assume that a computer processes 100,000 password possibilities per second (modern PC). The table below shows password lengths from 3 to 12 characters. The figures at the top - 26, 36, 52, 68, 94 - indicate the number of characters from which the passwords are formed (assuming the English alphabet is used). 26 is the number of lower-case letters, 36 is letters and digits, 52 is mixed-case letters, 68 is single-case letters with digits, symbols and punctuation.[117]

	26	**36**	**52**	**68**
3	0.18 seconds	0.47 seconds	1.41 seconds	3.14 seconds
4	4.57 seconds	16.8 seconds	1.22 minutes	3.56 minutes
5	1.98 minutes	10.1 minutes	1.06 hours	4.04 hours
6	51.5 minutes	6.05 hours	13.7 days	2.26 months
7	22.3 hours	9.07 days	3.91 months	2.13 years
8	24.2 days	10.7 months	17.0 years	1.45 centuries
9	1.72 years	32.2 years	8.82 centuries	9.86 millennia
10	44.8 years	1.16 millennia	45.8 millennia	670 millennia
11	11.6 centuries	41.7 millennia	2,384 millennia	45,582 millennia
12	30.3 millennia	1,503 millennia	123,946 millennia	3,099,562 millennia

Based on these figures, one can assume that even an 8-character random password using small-case letters and digits will be sufficient in complexity. If your main password to-date has been only 5 characters long, it is possible it has already been compromised, or is likely to be compromised, should the need arise.

Note: the above figures apply to random passwords only. Profiling and dictionary attacks are different, because they only work against 'real word' passwords.

117
Geodsoft.com
'Good and bad passwords – how to'

Glossary

Backdoor – in a computer system, a method of bypassing normal authentication or securing remote access to a computer, while attempting to remain hidden from casual inspection.

Bcc – Blind Carbon Copy. Refers to the practice of sending a message to multiple recipients in such a way that what they receive does not contain the complete list of recipients.

There are a number of reasons for using this feature:

- To send a copy of your correspondence to a third party (for example, a colleague) when you do not want to let the recipient know that you are doing this (or when you do not want the recipient to know the third party's e-mail address).
- When sending an e-mail to multiple recipients, you can hide their e-mail addresses from each other. This is a sensible anti-spam precaution, because it helps to avoid compiling a long list of e-mail addresses available to all the recipients (which is what happens, if you put everyone's address in the To: or CC: fields). For this reason, it often makes sense to use the **Bcc**: field for mailing lists. Some viruses harvest e-mail addresses from users' cache folder or address book, and large CC (Carbon Copy) lists may further the propagation of unwanted viruses, giving another reason to use **Bcc**.

BIOS – stands for **Basic Input/Output System** or **Basic Integrated Operating System**. It refers to the software code run by a computer when first powered on. The primary function of **BIOS** is to prepare the machine so that other software programs stored on various media (such as hard drives, floppies, and CDs) can load, execute, and assume control of the computer.

Blog – a website where entries are made in journal style and displayed in a reverse chronological order. Blogs often provide commentary or news on a particular subject, such as food, politics, or local news; some function as more personal online diaries. A typical **blog** combines text, images, and links to other blogs, web pages, and other media related to its topic. Popular **blog** engines include www.wordpress.com, www.livejournal.com, www.blogspot.com.

Many journalists and human rights defenders use blogs as to communicate vital information, not otherwise available in mainstream media, to the Internet community. This has been labelled 'citizen journalism' - an increasingly popular method of obtaining genuine information on an event or a country.

Control Panel – a Microsoft Windows feature that gives you access to modifying the system settings of your computer, including user management, power features, network access, system drivers and much more.

Circumvention – in this book, circumvention relates to the bypassing of Internet website blocks. This is achieved by using technology which 'goes around' the given obstacle.

Cryptanalysis(st) – studies of methods of obtaining the meaning of encrypted information, without access to the secret information. A cryptanalyst is a person carrying out such studies

Cryptology – a study of mathematical, linguistic, and other coding patterns and their histories.

Cyber-dissident(s) – a person or people who actively opposes an established political structure and gives voice to their political concern through the medium of the Internet.

Denial of Service attack (DOS) – A DOS attack is carried out by repeated computer connection attempts to a website. The purpose of the attack is to overload the web server by making millions of same requests in the shortest possible time. A Distributed DOS (DDOS) attack involves specially pre-programmed computers to attack a single website.

Device drivers – computer code that allows specific hardware to function on your computer.

Digital divide – a gap between those with regular and effective access to digital technologies and those without. Digital divide is related to social inclusion and equality of opportunity. It is seen as a social/political problem and is becoming increasingly topical as industrialized nations are getting more and more dependent on digital technologies.

DSL access – refers to data communications technology that enables faster data transmission over a copper telephone line than a conventional modem can provide. It stands for **Digital Subscriber Line** (with variants of aDSL - Asymmetric and sDSL – Symmetric).

ECHELON – the name to describe a highly secretive world-wide signals intelligence and analysis network run by the UKUSA Community (otherwise known as the "Anglo-Saxon alliance"). It has been reported by a number of sources, including the European Parliament. According to some sources, ECHELON can capture radio and satellite communications, telephone calls, faxes, e-mails and other data streams almost anywhere in the world. It includes computer-automated analysis and sorting of intercepts.

Encryption – the process of obscuring information to make it unreadable without special knowledge.

Firewall – a piece of hardware and/or software that functions in a networked environment to prevent communications forbidden by the security policy.

Internet Service Provider (ISP) – a business or organization that offers users access to the Internet and related services. In the past, most ISPs were run by phone companies. Now, ISPs can be started by just about anyone. They provide services such as Internet transit, domain name registration and hosting, dial-up or DSL access, leased line access and collocation (keeping your own server at the **ISP**'s premises).

ISP – see **Internet Service Provider**

Secure Sockets Layer (**SSL**) – a cryptographic protocol which provides secure communications on the Internet for e-mail, internet faxing, and other data transfers.

Open encryption standards – methods or encryption algorithms whose code is open to the general public for review and improvement. These are considered the safest type of independently tested encryption algorithms. Closed encryption algorithms may have major flaws (unnoticed by its developers), or specially made 'backdoors' that could leak all your information to a third party.

Partition (disk partition) – creation of logical divisions upon a hard disk. Allows the creation of several file systems on a single hard disk and has many benefits: allowing for dual boot setup (for example, to boot Microsoft Windows and Linux), sharing swap partitions between multiple Linux distributions, and protection or isolation of files.

PKE – see Public key cryptography

Proxy server – a computer that enables clients to make indirect network connections to other network services (websites).

Public key cryptography (encryption) – a form of cryptography that generally allows users to communicate securely without having prior access to a shared secret key. This is done by using a pair of cryptographic keys, designated **public key** and **private key**, which are related mathematically.

SORM-2 – (*Sistema Operativno-Rozysknykh Meropriyatii*, literally "System of Operational and Investigative Activities") - a Russian law, updated in 1998, that allows the FSB (Federal Security Service) to monitor Internet communications.

SSL – see **Secure Sockets Layer**

SSL Certificate – is generated for every website that wishes to operate on **SSL**. It serves as a unique identifier proving the website's authenticity and providing necessary information for an encrypted channel between the host and client.

System registry – a list of all software applications, hardware devices and system settings on your computer. Every installed program and component of your computer has to have an entry in the registry. This usually happens automatically. Sometimes, when a program is uninstalled, it does not remove its entry from the registry. This could be a potential security concern. Viruses often attack and corrupt the registry and could damage the functionality of your system. Also known as 'registry' or 'Windows registry'.

Webserver – A computer that hosts one or a number of websites. Also web host, host.

Wiping (file wiping) – the process of overwriting a file, sometimes multiple files, to ensure that all information is deleted. Wiping a file is akin to shredding a document in a paper shredder.

A PROPOSAL FOR THE INTERNET RIGHTS CHARTER

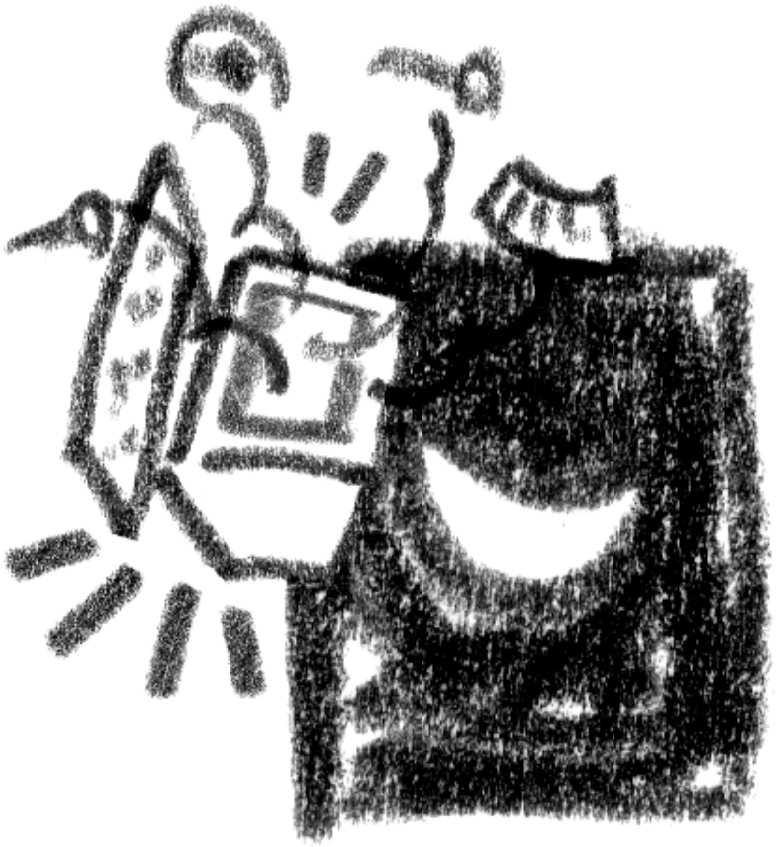
1. The right to access Internet infrastructure irrespective of where you live
2. The right to the skills and knowledge that enable people to use and shape the Internet to meet their needs
3. The right to free and open source software
4. The right to equal access for men and women
5. The right to access and create content that is culturally and linguistically diverse
6. The right to freedom of expression
7. The right to engage in online protest
8. The right to access to knowledge
9. The right to freedom of information
10. The right to access publicly funded information
11. The right to freedom from surveillance
12. The right to use encryption
13. The right to multilateral democratic oversight of the Internet
14. The right to transparency and accessibility of the Internet legislative body
15. The right to a decentralised, collaborative and interoperable Internet
16. The right to rights protection, awareness and education
17. The right to recourse when rights are violated

(For the full text please refer to the original from The Association for Progressive Communications website http://rights.apc.org/charter.shtml)

NOTES

NOTES

NOTES



DIGITAL SECURITY & PRIVACY

FOR HUMAN RIGHTS DEFENDERS

FrontLine
INTERNATIONAL FOUNDATION FOR THE PROTECTION OF HUMAN RIGHTS DEFENDERS

81 Main Street
Blackrock Co. Dublin
Republic of Ireland
Tel: +35 3 1 212 3750
Fax: +35 3 1 2121001
info@frontlinedefenders.org
www.frontlinedefenders.org

Irish Aid
Department of Foreign Affairs
An Roinn Gnóthaí Eachtracha

NGO in a Box
security.ngoinabox.org