From Revenue Assurance to Assurance

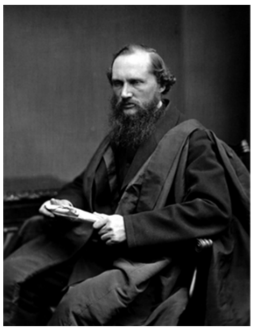
The Importance of Measurement in Computer Security

Peter Gutmann

University of Auckland

Why Measure?

Reason for measurement in science/engineering is usually attributed to Lord Kelvin (William Thomson)



If you cannot measure it, you cannot improve it
— Lord Kelvin, possibly apocryphal

Why Measure? (ctd)

What he actually said:

> In physical science a first essential step in the direction of learning any subject is to find principles of numerical reckoning and practicable methods for measuring some quality connected with it. I often say that when you can measure what you are speaking about and express it in numbers you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind: it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science, whatever the matter may be
>
> — Lord Kelvin, "Electrical Units of Measurement", 1883

- Victorians liked being long-winded

Why Measure? (ctd)

From which we conclude that

- Someone who expresses himself like that is unlikely to have said "if you cannot measure it, you cannot improve it"

Why Measure? (ctd)

Usually quoted in terms of management science, “if you can’t measure it you can neither manage it nor improve it”

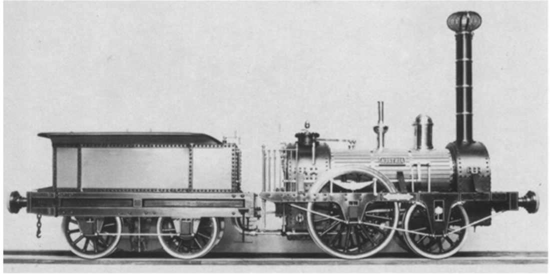
IAN AYRES SUPER CRUNCHERS WHY THINKING-BY-NUMBERS IS THE NEW WAY TO BE SMART
Scorecard Best Practices Design, Implementation, and Evaluation
HOW TO MEASURE ANYTHING FINDING THE VALUE OF INTANGIBLES IN BUSINESS
MAY The New Know Innovation Powered by Analytics
SMART (ENOUGH) SYSTEMS TAYLOR RADEN
Master Data Management
CUSTOMER DATA INTEGRATION

You can’t manage what you can’t measure

— Endless books on management

Improvement through Measurement

In Lord Kelvin’s day improvement-through-measurement was relatively easy



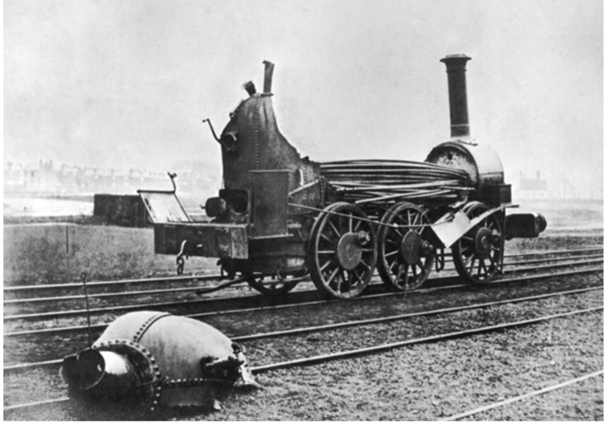
- The first versions of anything were somewhat rudimentary

Improvement through Measurement (ctd)

People just copied each other, with a bit of tweaking

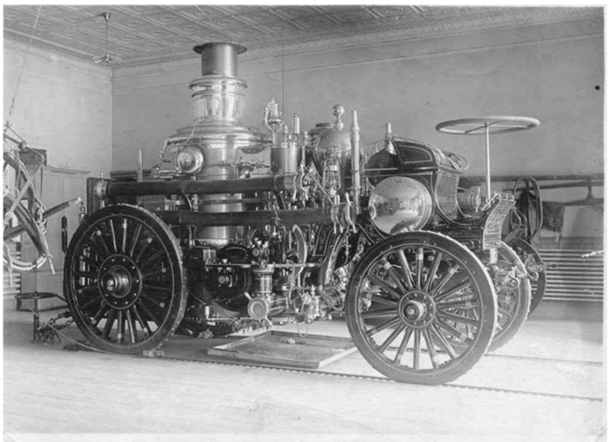
Improvement through Measurement (ctd)

Failures were obvious



Improvement through Measurement (ctd)

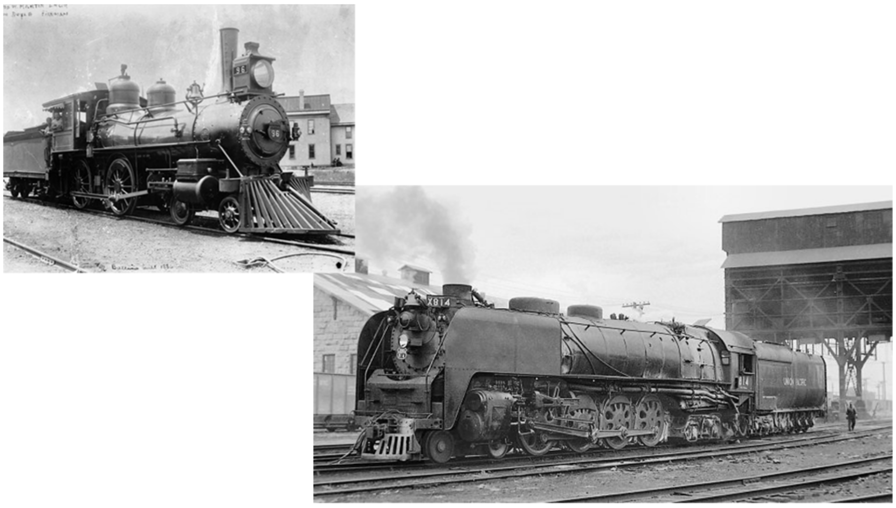
There were lots of knobs and levers to play with



- (It’s like a Firewall-1)

Improvement through Measurement (ctd)

This lead to many improvements

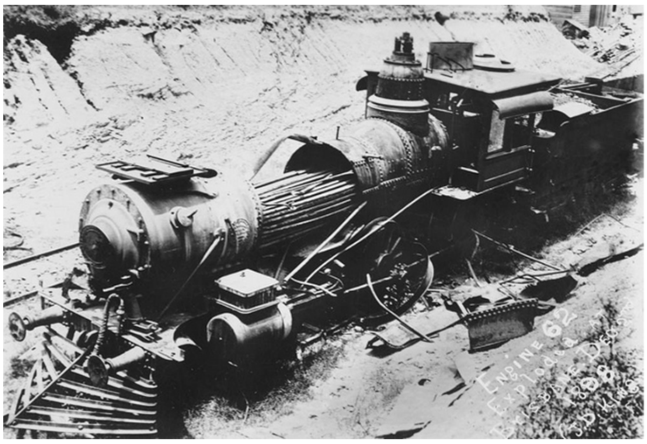


Improvement through Measurement (ctd)

Some of which wouldn’t look out of place today

Improvement through Measurement (ctd)

Failures were still pretty obvious even with modern designs



Improvement through Measurement (ctd)

The exact time of failure can usually be determined by the trained eye

Measurement in Computer Security

A fully-functional firewall

Measurement in Computer Security (ctd)

A catastrophically failed firewall

Measurement in Computer Security (ctd)

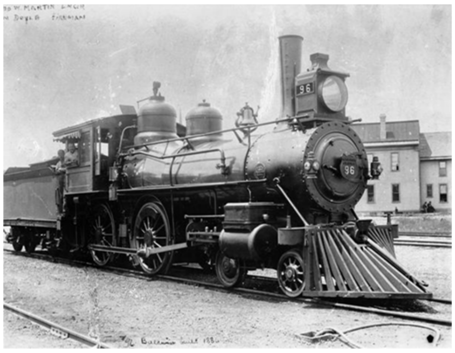
A $20,000 Ethernet cable

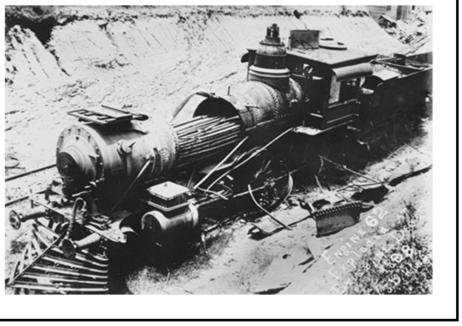
Measurement in Computer Security (ctd)

Can you tell which is which?

Measurement in Computer Security (ctd)

Trains are much easier to detect failures with...





Measurement in Computer Security (ctd)

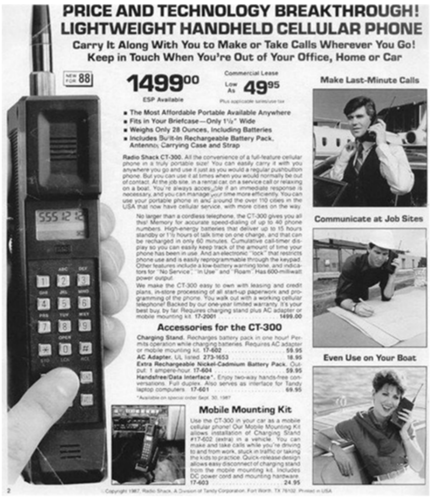
... than computer security gear

Measurement for Revenue Assurance

Some technology companies have already run into this problem in the past

1980s: Telcos roll out cellular services

Measurement for Revenue Assurance (ctd)



PRICE AND TECHNOLOGY BREAKTHROUGH!
LIGHTWEIGHT HANDHELD CELLULAR PHONE

Carry It Along With You to Make or Take Calls Wherever You Go!
Keep in Touch When You're Out of Your Office, Home or Car

NEW FOR 88

1499.00
ESP Available

Commercial Lease
Low As 49.95
Plus applicable sales/use tax

- The Most Affordable Portable Available Anywhere
- Fits in Your Briefcase—Only 1½" Wide
- Weighs Only 28 Ounces, Including Batteries
- Includes Built-In Rechargeable Battery Pack, Antenna, Carrying Case and Strap

Radio Shack CT-300. All the convenience of a full-feature cellular phone in a truly portable size! You can easily carry it with you anywhere you go and use it just as you would a regular pushbutton phone. But you can use it at times when you would normally be out of contact. At the job site, in a rental car, on a service call or relaxing on a boat. You're always accessible if an immediate response is necessary, and you can manage your time more efficiently. You can use your portable phone in and around the over 110 cities in the USA that now have cellular service, with more cities on the way.

No larger than a cordless telephone, the CT-300 gives you all this! Memory for accurate speed-dialing of up to 40 phone numbers. High-energy batteries that deliver up to 15 hours standby or 1½ hours of talk time on one charge, and that can be recharged in only 60 minutes. Cumulative call-timer display so you can easily keep track of the amount of time your phone has been in use. And an electronic "lock" that restricts phone use and is easily reprogrammable through the keypad. Other features include a low-battery warning tone, and indicators for "No Service", "In Use" and "Roam". Has 600-milliwatt power output.

We make the CT-300 easy to own with leasing and credit plans, in-store processing of all start-up paperwork and programming of the phone. You walk out with a working cellular telephone! Backed by our one-year limited warranty. It's your best buy, by far. Requires charging stand plus AC adapter or mobile mounting kit. 17-2001 .... 1499.00

Accessories for the CT-300

Charging Stand. Recharges battery pack in one hour! Permits operation while charging batteries. Requires AC adapter or mobile mounting kit. 17-602 .... 59.95
AC Adapter. UL listed. 273-1653 .... 18.95
Extra Rechargeable Nickel-Cadmium Battery Pack. Output: 1 ampere-hour. 17-604 .... 59.95
Handsfree/Data Interface*. Enjoy two-way hands-free conversations. Full duplex. Also serves as interface for Tandy laptop computers. 17-601 .... 69.95
*Available on special order Sept. 30, 1987

Mobile Mounting Kit

Use the CT-300 in your car as a mobile cellular phone! Our Mobile Mounting Kit allows installation of Charging Stand #17-602 (extra) in a vehicle. You can make and take calls while you're driving to and from work, stuck in traffic or taking the kids to practice. Quick-release design allows easy disconnect of charging stand from the mobile mounting kit. Includes DC power cord and mounting hardware. 17-603 .... 24.95

Make Last-Minute Calls

Communicate at Job Sites

Even Use on Your Boat

© Copyright 1987, Radio Shack, A Division of Tandy Corporation, Fort Worth, TX 76102. Printed in USA

Market uptake was rapid

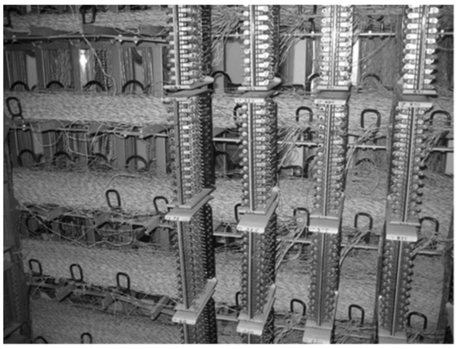
- Not surprising, at these bargain-basement prices

Measurement for Revenue Assurance (ctd)

1990s: Telcos have this sneaking suspicion that they may be missing out on some amount of revenue due to inaccurate billing

Measurement for Revenue Assurance (ctd)

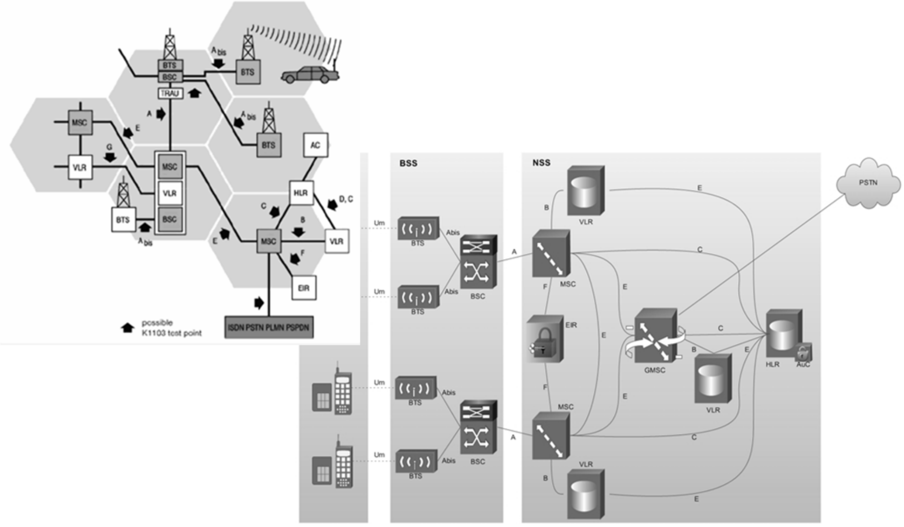
Billing on fixed lines is relatively easy



- Anything going through this port at the exchange gets billed
- Recorded on tape at the switch and periodically dumped to the central office

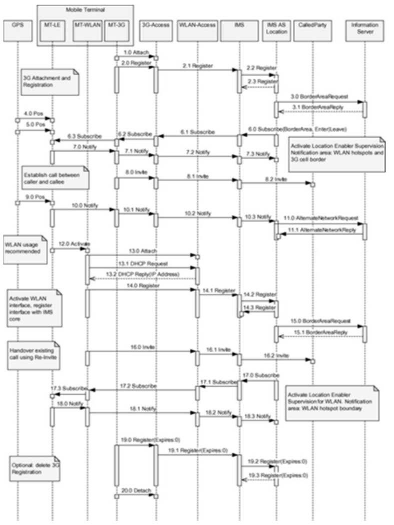
Measurement for Revenue Assurance (ctd)

Mobile billing is really hard



Measurement for Revenue Assurance (ctd)

I mean *really* hard



Measurement for Revenue Assurance (ctd)

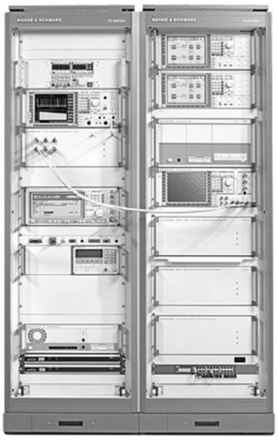
There’s no easy way to measure billing accuracy though

- Surely we're not losing money from this?!?!

Measurement for Revenue Assurance (ctd)

Engineers rigged up systems to place thousands of calls every day

- They knew the time and duration of each call
- Could compare their records with the resulting billing records



Measurement for Revenue Assurance (ctd)

Turns out that the telcos were clueless about the state of their billing

- “We’re sure people are making lots of calls, but *(#&Y*’d if we can figure out how many, or who to”

Measurement for Revenue Assurance (ctd)

Telcos had no idea just how bad things really were

If you cannot measure it, you cannot improve it
— Lord Kelvin (perhaps)

You can't manage what you can't measure
— Management books

If you can't measure it, you don't even know whether it's working or not
— Me, paraphrasing someone possibly paraphrasing
Lord Kelvin

Measurement for Revenue Assurance (ctd)

This helped create the field of revenue assurance

- Formalised the process of verifying that the billing system was working as expected

Measurement for Revenue Assurance (ctd)

Why revenue assurance?

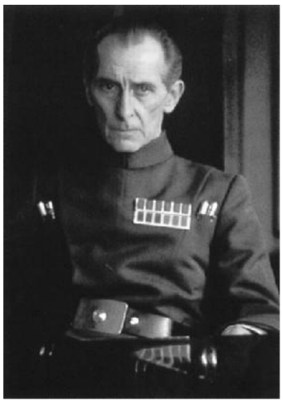
> From service provision to cash collection, there are limitless opportunities for revenue to seep through the cracks
>
> — TM Forum

"If we don't do this then we lose money"

- Like many other things, it started out as a good idea until management got hold of it
- See "TQM"

Measurement for Revenue Assurance (ctd)

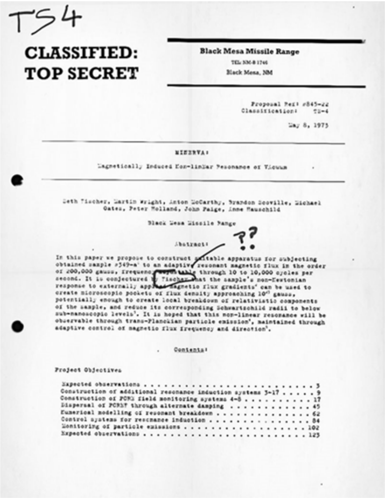
Motivation for revenue assurance



"Fear will keep them in line — fear of ~~this battlestation~~ losing money"

Measurement for Security

How do you get rid of these (on a large scale)?



TS4

CLASSIFIED:
TOP SECRET

Black Mesa Missile Range
TEL: NM-8 1746
Black Mesa, NM

Proposal Ref: #845-22
Classification: TS-4

May 8, 1973

MINERVA:

Magnetically Induced Non-linear Resonance of Vacuum

Seth Fischer, Martin Wright, Anton McCarthy, Brandon Scoville, Michael Gates, Peter Holland, John Paige, Anne Hauschild

Black Mesa Missile Range

Abstract:

??

In this paper we propose to construct suitable apparatus for subjecting obtained sample #349-a[1] to an adaptive resonant magnetic flux in the order of 200,000 gauss, frequency adjustable through 10 to 10,000 cycles per second. It is conjectured by Fischer that the sample's non-Newtonian response to externally applied magnetic flux gradients[2] can be used to create microscopic pockets of flux density approaching 10^{17} gauss, potentially enough to create local breakdown of relativistic components of the sample, and reduce its corresponding Schwartzchild radii to below sub-nanoscopic levels[3]. It is hoped that this non-linear resonance will be observable through trans-Planckian particle emission[4], maintained through adaptive control of magnetic flux frequency and direction[5].

Contents:

Project Objectives

Measurement for Security (ctd)

You do this to them

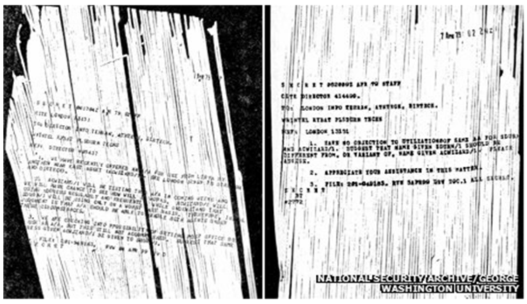
Measurement for Security (ctd)

This was considered good enough for many years…

…until this happened

Measurement for Security (ctd)

The Iranians didn't know that you couldn't recover documents from this form



S E C R E T [illegible] STAFF

CITE DIRECTOR [illegible].

TO: LONDON INFO TEHRAN, [illegible].

[illegible]

REF: LONDON [illegible]

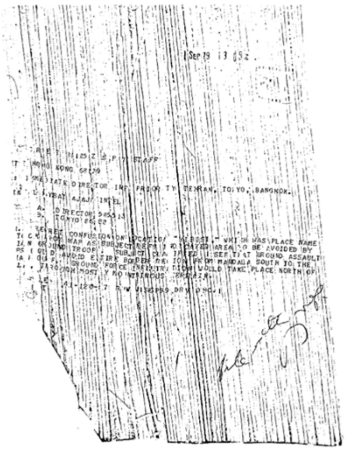
1. HAVE NO OBJECTION TO UTILIZATION OF SAME [illegible] AND ACWILLARD/1. SUGGEST THAT NAME GIVEN [illegible] SHOULD BE DIFFERENT FROM, OR VARIANT OF, NAME GIVEN ACWILLARD/1. PLEASE ADVISE.

2. APPRECIATE YOUR ASSISTANCE IN THIS MATTER.

3. FILE: [illegible] ALL SECRET.

S E C R E T

NATIONAL SECURITY ARCHIVE/GEORGE WASHINGTON UNIVERSITY



1 Sep 79 13 05z

[illegible] STAFF

[illegible] HONG KONG [illegible]

[illegible] DIRECTOR INFO PRIORITY TEHRAN, TOKYO, BANGKOK.

[illegible] INTEL

A. DIRECTOR [illegible]

B. TOKYO [illegible]

1. REGRET CONFUSION ON LOCATION [illegible] WHICH WAS PLACE NAME [illegible] MAP AS SUBJECT [illegible] AREA TO BE AVOIDED BY [illegible] GROUND TROOPS. SUBJECT CLARIFIED [illegible] SEE THAT GROUND ASSAULT [illegible] AVOID ENTIRE BORDER REGION FROM [illegible] SOUTH TO THE [illegible] GROUND FORCE INFILTRATION WOULD TAKE PLACE NORTH OF [illegible] THROUGH MOST[illegible] MOUNTAINOUS TERRAIN.

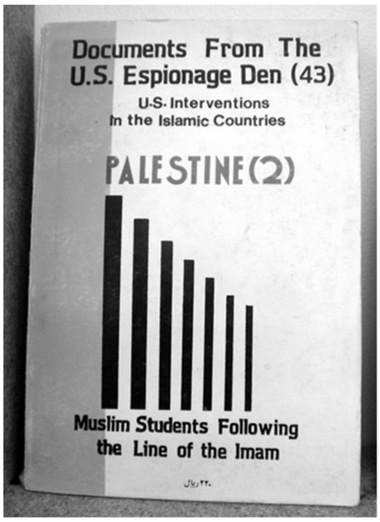
- Used Iranian carpet weavers (according to one version) and/or women (another version) to reassemble the documents

Measurement for Security (ctd)

The Iranians laid the shreds out on a floor and devised a sophisticated procedure for numbering, indexing and reassembling the individual shreds

— BBC

- Published as a 60-volume bestseller(?), “Documents From the U.S. Espionage Den”



Documents From The U.S. Espionage Den (43)

U.S. Interventions In the Islamic Countries

PALESTINE (2)

Muslim Students Following the Line of the Imam

Measurement for Security (ctd)

Short-term outcome

- Assorted revisions of document-destruction requirements

Security standards for document destruction have always been prescriptive rather than descriptive

```
Die Partikelgröße darf 320 Quadrat-Millimeter nicht
überschreiten, wobei allerdings 10% der Partikel eine
Fläche zwischen 320 und 800 Quadrat-Millimeter aufweisen
dürfen. Bei Streifenschnitt darf die Streifenbreite maximal
2 Millimeter betragen.
```

Possibly based around the following thinking

- Commercial shredders come in these performance classes
- Assign a document sensitivity level to each class

Measurement for Security (ctd)

Ongoing problem: Very little published data available on what can and can't be recovered

- Lack of measurement again

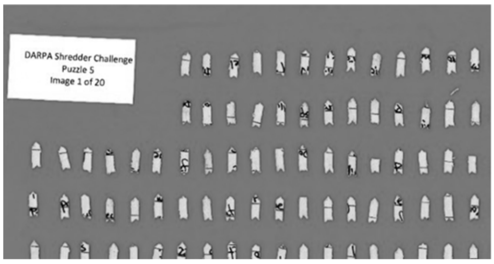
Attempts to evaluate the security of shredded documents barely seem to exist until about five years ago

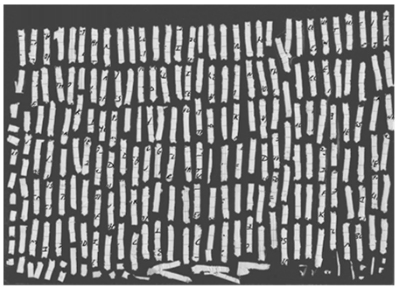
> The problem of automatic shredded document recovery has been sparsely researched to date
>
> — "An Investigation into Automated Shredded Document Reconstruction using Heuristic Search Algorithms", 2006

Measurement for Security (ctd)

Then, in 2011…

- DARPA sponsors the Shredder Challenge





Computer-aided reassembly of shredded documents

- Ranged from 200 to 6,000 fragments
- $50,000 first prize

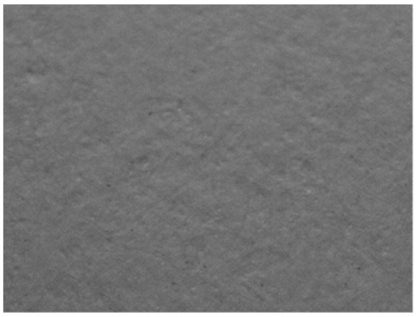
Measurement for Security (ctd)

Teams generally used a technique pretty similar to what the Iranians had done thirty years earlier

- Assign a unique ID to each fragment
- Analyse characteristics like size, colour, edge pattern, font used, graphics
- Perform approximate matching based on this
  - Early work in this area was based on automated jigsaw-puzzle solvers
- Use humans for the final assembly

Measurement for Security (ctd)

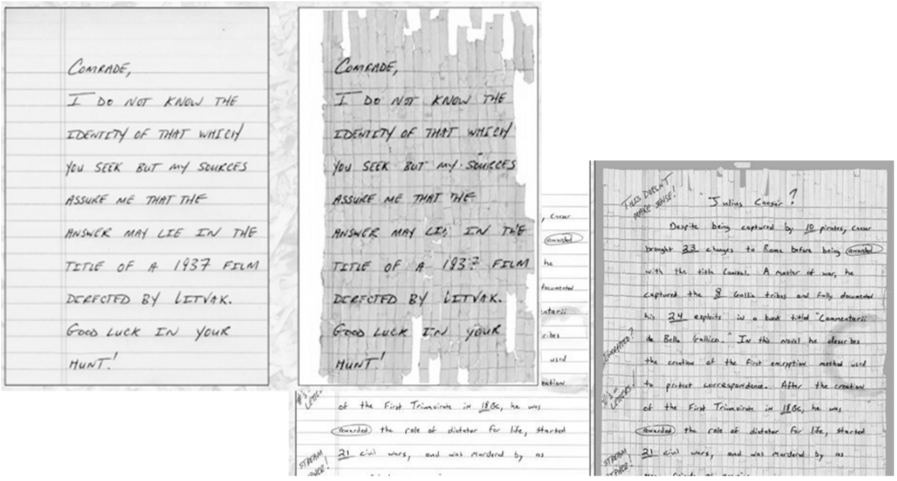
Winning team exploited the fact that the documents were photocopied and contained a pattern of yellow dots used to track the source of printed/copied documents



- Other teams managed to do well even without this inadvertent help from DARPA

Measurement for Security (ctd)

While the results were troubling for people who rely on shredders for document security…



COMRADE,
I DO NOT KNOW THE
IDENTITY OF THAT WHICH
YOU SEEK BUT MY SOURCES
ASSURE ME THAT THE
ANSWER MAY LIE IN THE
TITLE OF A 1937 FILM
DIRECTED BY LITVAK.
GOOD LUCK IN YOUR
HUNT!

THIS DOESN'T MAKE SENSE!

Julius Caesar ?

Despite being captured by 10 pirates, Caesar brought 33 charges to Rome before being arrested with the tith Consul. A master of war, he captured the 8 Gallic tribes and fully documented his 24 exploits in a book titled "Commentarii de Bello Gallico." In this novel he describes the creation of the first encryption method used to protect correspondence. After the creation of the First Triumvirate in 18 BC, he was awarded the role of dictator for life, started 31 civil wars, and was murdered by as

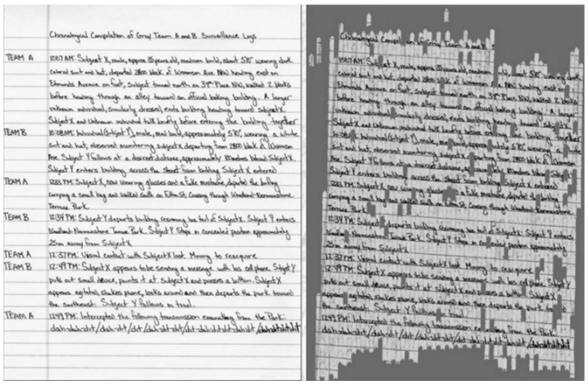
CORRUPTED?

OF LETTERS!

STREAM OF PHRASE!

Measurement for Security (ctd)

…just this *one measurement* has now given us a means of evaluating their effectiveness



Chronological Compilation of Group Team A and B Surveillance Logs

TEAM A 10:07 AM: Subject X, male, approx 35 years old, medium build, about 5'10" wearing dark colored suit and hat, departed 2800 block of Woman Ave NW heading east on Edmunds Avenue on foot, Subject turned north on 31st Place NW, walked 2 blocks before heading through an alley toward an office building. A larger unknown individual, similarly dressed, exits building heading toward Subject X. Subject X and Unknown individual talk briefly before entering the building together

TEAM B 10:08 AM: Individual (Subject Y), male, small build, approximately 5'10", wearing a white suit and hat, observed monitoring Subject X departing from 2800 block of Woman Ave. Subject Y follows at a discreet distance, approximately 100 meters behind Subject X. Subject Y enters building across the street from building Subject X entered

TEAM A 12:23 PM: Subject X, now wearing glasses and a fake mustache, departed the building carrying a small bag and walked south on Fifth St, Crossing through Woodland-Normanstone Terrace Park

TEAM B 12:34 PM: Subject Y departs building resuming his tail of Subject X. Subject Y enters Woodland-Normanstone Terrace Park. Subject Y Stops in concealed position approximately 25m away from Subject X

TEAM A 12:37 PM: Visual contact with Subject X lost. Moving to reacquire

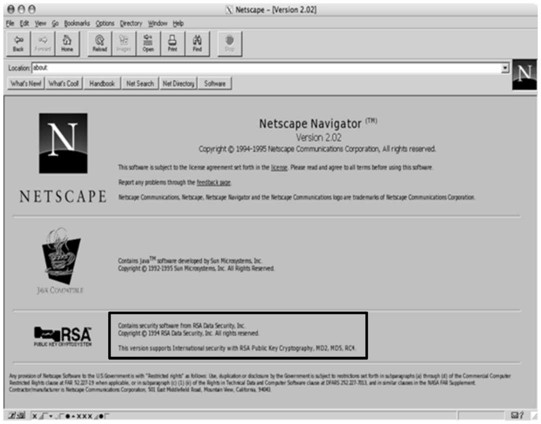
TEAM B 12:49 PM: Subject X appears to be sending a message with his cell phone. Subject Y pulls out small device, points it at Subject X and presses a button. Subject X appears agitated, shakes phone, looks around and then departs the park toward the southeast. Subject Y follows on trail.

TEAM A 12:49 PM: Intercepted the following transmission emanating from the Park:
dah-dah-dit/dah-dit/dit/dah-dit-dit/dit-dah-dit-dit-dah-dit/dah-dit-dit-dit

- Anything up to about DIN level 5 (0.8×12mm, "Classified/Top Secret") probably isn't that secure

Measurement in Computer Security, Part 2

In a few rare cases we've run into the same thing with security


Netscape – [Version 2.02]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Reload Images Open Print Find Stop
Location: about
What's New! What's Cool! Handbook Net Search Net Directory Software
NETSCAPE
JAVA COMPATIBLE
RSA PUBLIC KEY CRYPTOSYSTEM

Netscape Navigator (TM)
Version 2.02
Copyright © 1994-1995 Netscape Communications Corporation, All rights reserved.

This software is subject to the license agreement set forth in the license. Please read and agree to all terms before using this software.

Report any problems through the feedback page.

Netscape Communications, Netscape, Netscape Navigator and the Netscape Communications logo are trademarks of Netscape Communications Corporation.

Contains Java™ software developed by Sun Microsystems, Inc.
Copyright © 1992-1995 Sun Microsystems, Inc. All Rights Reserved.

Contains security software from RSA Data Security, Inc.
Copyright © 1994 RSA Data Security, Inc. All rights reserved.

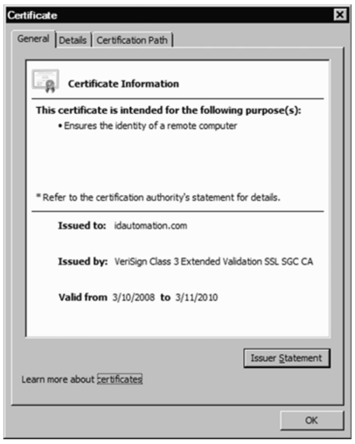
This version supports International security with RSA Public Key Cryptography, MD2, MD5, RC4.

Any provision of Netscape Software to the U.S Government is with "Restricted rights" as follows: Use, duplication or disclosure by the Government is subject to restrictions set forth in subparagraphs (a) through (d) of the Commercial Computer Restricted Rights clause at FAR 52.227-19 when applicable, or in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, and in similar clauses in the NASA FAR Supplement. Contractor/manufacturer is Netscape Communications Corporation, 501 East Middlefield Road, Mountain View, California, 94043.

1990s: Netscape rolls out SSL for the web

Measurement in Computer Security, Part 2 (ct

Handshake is secured using certificates



Certificate Information

This certificate is intended for the following purpose(s):
- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: idautomation.com

Issued by: VeriSign Class 3 Extended Validation SSL SGC CA

Valid from 3/10/2008 to 3/11/2010

Learn more about certificates

- With a certificate "it can be guaranteed that you are actually connecting to" a given site (Google Chrome)

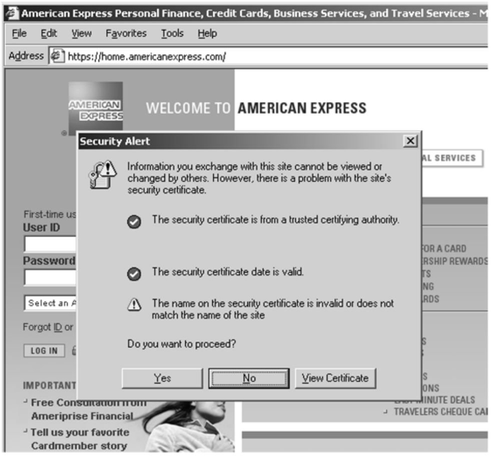
Measurement in Computer Security, Part 2 (ct

Certificates make you secure!

- By emphatic assertion of the browser developers

Measurement in Computer Security, Part 2 (ct

Now there had been a few concerns over the years about just how valid this assertion was...



https://home.americanexpress.com/

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

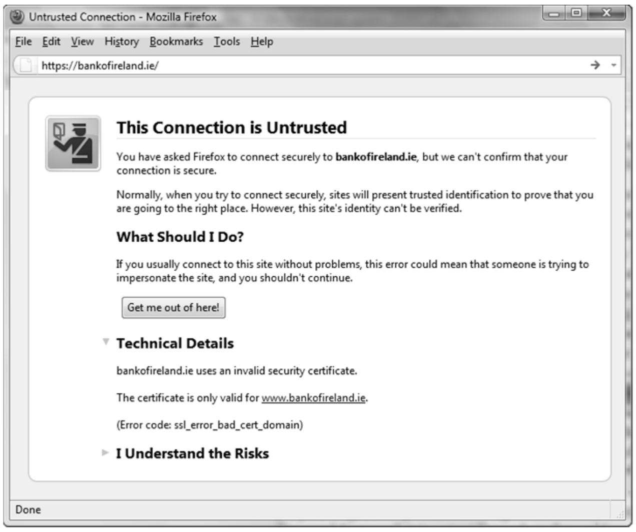
✓ The security certificate is from a trusted certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Measurement in Computer Security, Part 2 (ct


Untrusted Connection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://bankofireland.ie/
Get me out of here!
Done

This Connection is Untrusted

You have asked Firefox to connect securely to **bankofireland.ie**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Technical Details

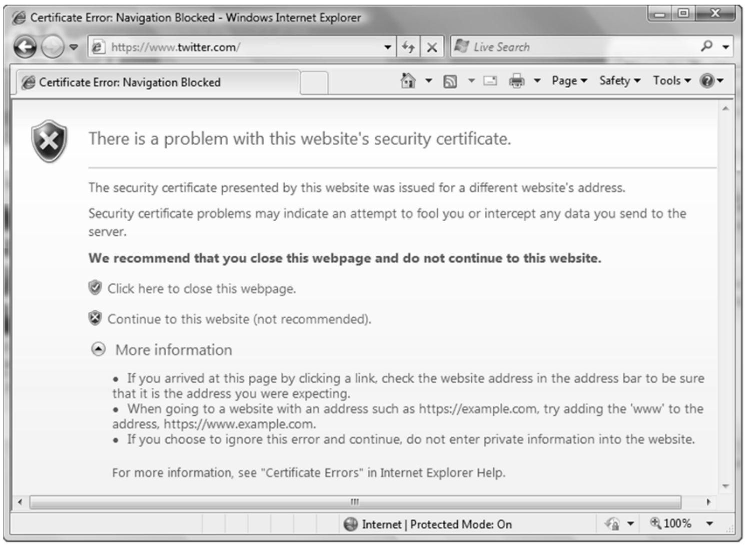
bankofireland.ie uses an invalid security certificate.

The certificate is only valid for www.bankofireland.ie.

(Error code: ssl_error_bad_cert_domain)

I Understand the Risks

Measurement in Computer Security, Part 2 (ct


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://www.twitter.com/
Live Search
Certificate Error: Navigation Blocked
Page ▾ Safety ▾ Tools ▾
Internet | Protected Mode: On
100%

There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

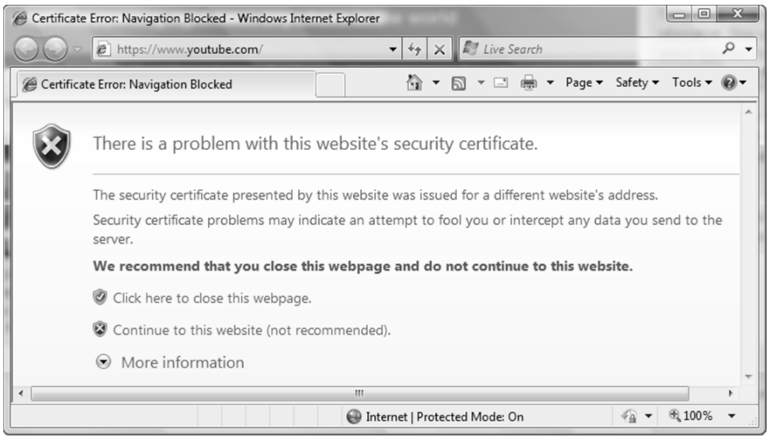
Continue to this website (not recommended).

More information

- If you arrived at this page by clicking a link, check the website address in the address bar to be sure that it is the address you were expecting.
- When going to a website with an address such as https://example.com, try adding the 'www' to the address, https://www.example.com.
- If you choose to ignore this error and continue, do not enter private information into the website.

For more information, see "Certificate Errors" in Internet Explorer Help.

Measurement in Computer Security, Part 2 (ct



Certificate Error: Navigation Blocked - Windows Internet Explorer

https://www.youtube.com/

There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

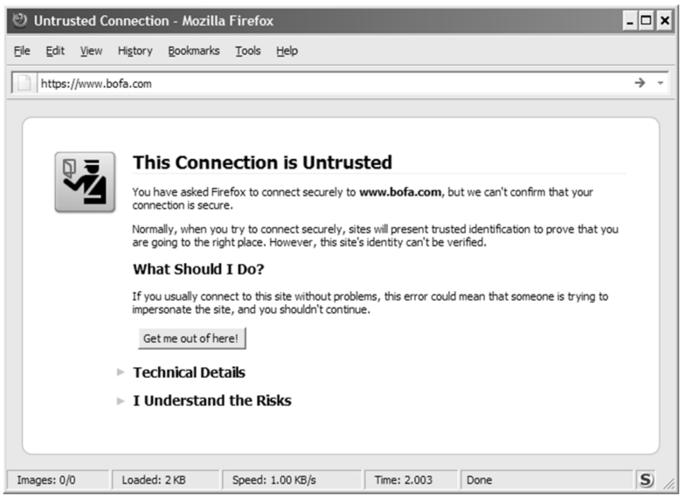
Click here to close this webpage.

Continue to this website (not recommended).

More information

Live Search
Certificate Error: Navigation Blocked
Page ▾
Safety ▾
Tools ▾
Internet | Protected Mode: On
100%

Measurement in Computer Security, Part 2 (ct



Untrusted Connection - Mozilla Firefox

https://www.bofa.com

This Connection is Untrusted

You have asked Firefox to connect securely to **www.bofa.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

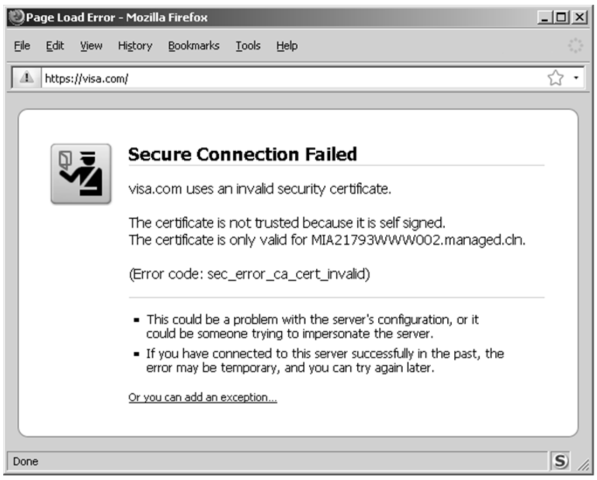
Get me out of here!

▸ **Technical Details**

▸ **I Understand the Risks**

Images: 0/0 | Loaded: 2 KB | Speed: 1.00 KB/s | Time: 2.003 | Done

Measurement in Computer Security, Part 2 (ct


Page Load Error - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://visa.com/
Done

Secure Connection Failed

visa.com uses an invalid security certificate.

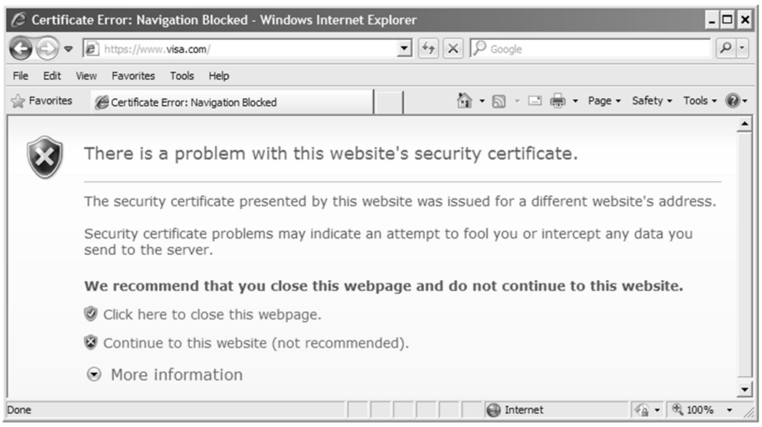
The certificate is not trusted because it is self signed.
The certificate is only valid for MIA21793WWW002.managed.cln.

(Error code: sec_error_ca_cert_invalid)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

Or you can add an exception…

Measurement in Computer Security, Part 2 (ct


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://www.visa.com/
Google
File Edit View Favorites Tools Help
Favorites
Certificate Error: Navigation Blocked
Page Safety Tools
Done
Internet
100%

There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

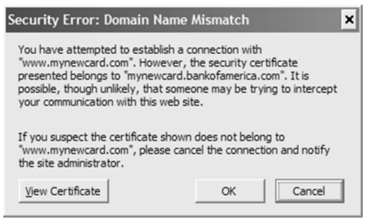
Click here to close this webpage.

Continue to this website (not recommended).

More information

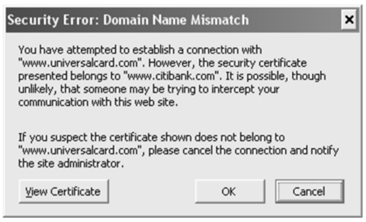
- ISO 9000, demonstrating repeatability of process
- (Finally fixed by redirecting browsers to a non-SSL version of the site)

Measurement in Computer Security, Part 2 (ct


Security Error: Domain Name Mismatch

You have attempted to establish a connection with "www.mynewcard.com". However, the security certificate presented belongs to "mynewcard.bankofamerica.com". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.

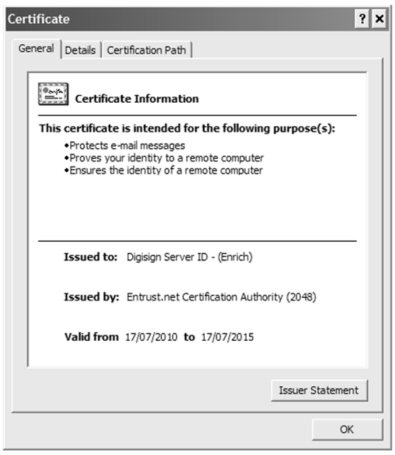
If you suspect the certificate shown does not belong to "www.mynewcard.com", please cancel the connection and notify the site administrator.


Security Error: Domain Name Mismatch

You have attempted to establish a connection with "www.universalcard.com". However, the security certificate presented belongs to "www.citibank.com". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.

If you suspect the certificate shown does not belong to "www.universalcard.com", please cancel the connection and notify the site administrator.

Measurement in Computer Security, Part 2 (ct



Certificate Information

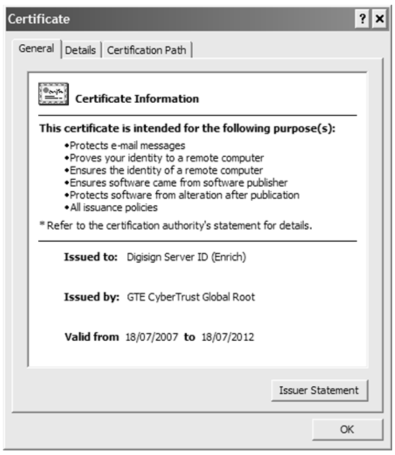
This certificate is intended for the following purpose(s):

- Protects e-mail messages
- Proves your identity to a remote computer
- Ensures the identity of a remote computer

Issued to: Digisign Server ID - (Enrich)

Issued by: Entrust.net Certification Authority (2048)

Valid from 17/07/2010 **to** 17/07/2015



Certificate Information

This certificate is intended for the following purpose(s):

- Protects e-mail messages
- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication
- All issuance policies

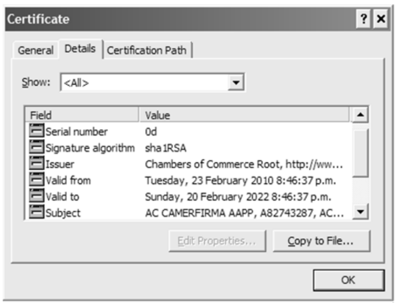
* Refer to the certification authority's statement for details.

Issued to: Digisign Server ID (Enrich)

Issued by: GTE CyberTrust Global Root

Valid from 18/07/2007 **to** 18/07/2012

Measurement in Computer Security, Part 2 (ct

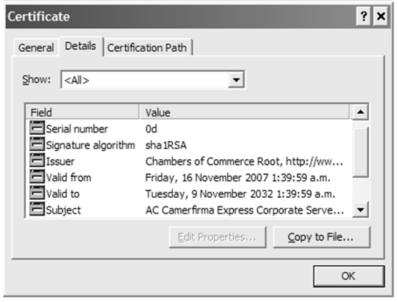


Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Serial number	0d
Signature algorithm	sha1RSA
Issuer	Chambers of Commerce Root, http://ww...
Valid from	Tuesday, 23 February 2010 8:46:37 p.m.
Valid to	Sunday, 20 February 2022 8:46:37 p.m.
Subject	AC CAMERFIRMA AAPP, A82743287, AC...



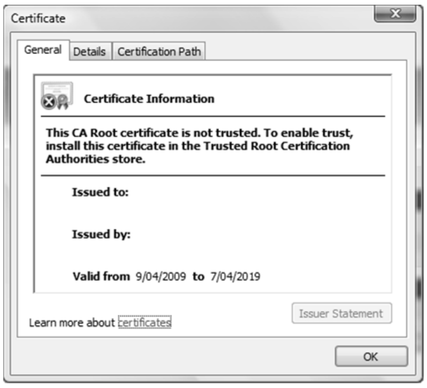
Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Serial number	0d
Signature algorithm	sha1RSA
Issuer	Chambers of Commerce Root, http://ww...
Valid from	Friday, 16 November 2007 1:39:59 a.m.
Valid to	Tuesday, 9 November 2032 1:39:59 a.m.
Subject	AC Camerfirma Express Corporate Serve...

Measurement in Computer Security, Part 2 (ct



Certificate

General | Details | Certification Path

Certificate Information

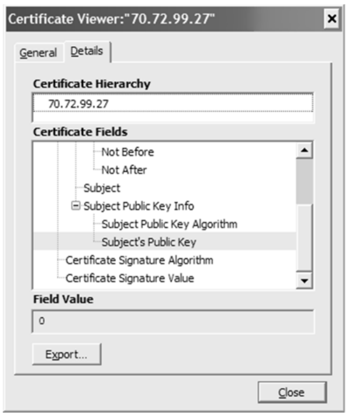
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to:

Issued by:

Valid from 9/04/2009 **to** 7/04/2019

Learn more about certificates



Certificate Viewer:"70.72.99.27"

General | Details

Certificate Hierarchy

70.72.99.27

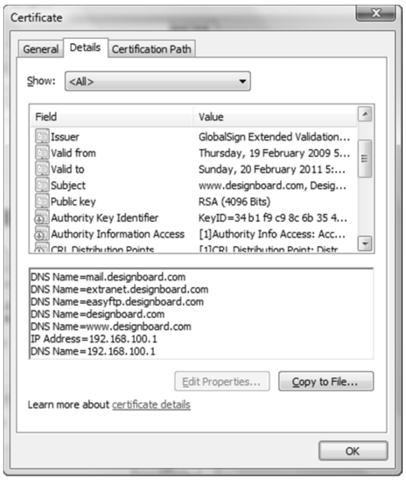
Certificate Fields

```
        Not Before
        Not After
      Subject
    ⊟ Subject Public Key Info
        Subject Public Key Algorithm
        Subject's Public Key
    Certificate Signature Algorithm
    Certificate Signature Value
```

Field Value

0

Measurement in Computer Security, Part 2 (ct

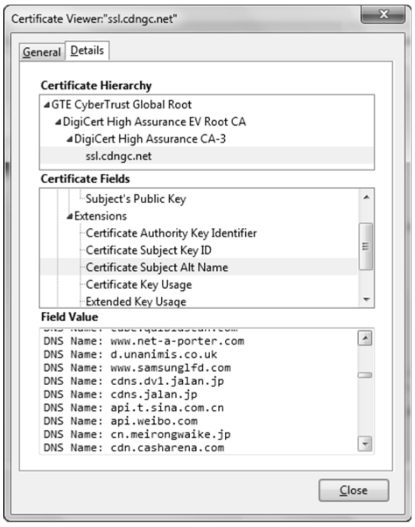


Show: <All>

Field	Value
Issuer	GlobalSign Extended Validation...
Valid from	Thursday, 19 February 2009 5...
Valid to	Sunday, 20 February 2011 5:...
Subject	www.designboard.com, Desig...
Public key	RSA (4096 Bits)
Authority Key Identifier	KeyID=34 b1 f9 c9 8c 6b 35 4...
Authority Information Access	[1]Authority Info Access: Acc...
CRL Distribution Points	[1]CRL Distribution Point: Distr

```
DNS Name=mail.designboard.com
DNS Name=extranet.designboard.com
DNS Name=easyftp.designboard.com
DNS Name=designboard.com
DNS Name=www.designboard.com
IP Address=192.168.100.1
DNS Name=192.168.100.1
```

Learn more about certificate details



Certificate Hierarchy

- GTE CyberTrust Global Root
  - DigiCert High Assurance EV Root CA
    - DigiCert High Assurance CA-3
      - ssl.cdngc.net

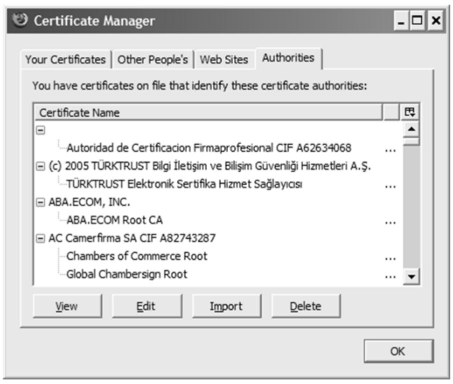
Certificate Fields

- Subject's Public Key
- Extensions
  - Certificate Authority Key Identifier
  - Certificate Subject Key ID
  - Certificate Subject Alt Name
  - Certificate Key Usage
  - Extended Key Usage

Field Value

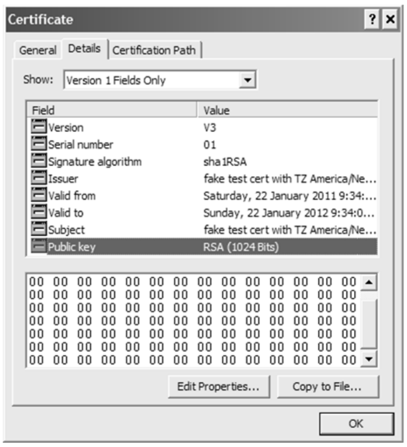
```
DNS Name: www.net-a-porter.com
DNS Name: d.unanimis.co.uk
DNS Name: www.samsunglfd.com
DNS Name: cdns.dv1.jalan.jp
DNS Name: cdns.jalan.jp
DNS Name: api.t.sina.com.cn
DNS Name: api.weibo.com
DNS Name: cn.meirongwaike.jp
DNS Name: cdn.casharena.com
```

Measurement in Computer Security, Part 2 (ct



You have certificates on file that identify these certificate authorities:

Certificate Name	
⊟	
Autoridad de Certificacion Firmaprofesional CIF A62634068	...
⊟ (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.	
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	...
⊟ ABA.ECOM, INC.	
ABA.ECOM Root CA	...
⊟ AC Camerfirma SA CIF A82743287	
Chambers of Commerce Root	...
Global Chambersign Root	...

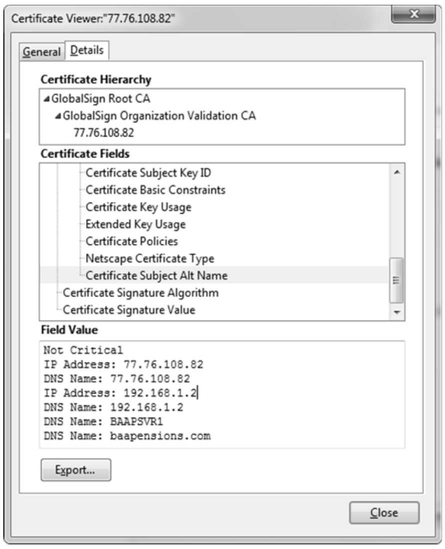


Show: Version 1 Fields Only

Field	Value
Version	V3
Serial number	01
Signature algorithm	sha1RSA
Issuer	fake test cert with TZ America/Ne...
Valid from	Saturday, 22 January 2011 9:34:...
Valid to	Sunday, 22 January 2012 9:34:0...
Subject	fake test cert with TZ America/Ne...
Public key	RSA (1024 Bits)

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Measurement in Computer Security, Part 2 (ct



Certificate Hierarchy

- GlobalSign Root CA
  - GlobalSign Organization Validation CA
    - 77.76.108.82

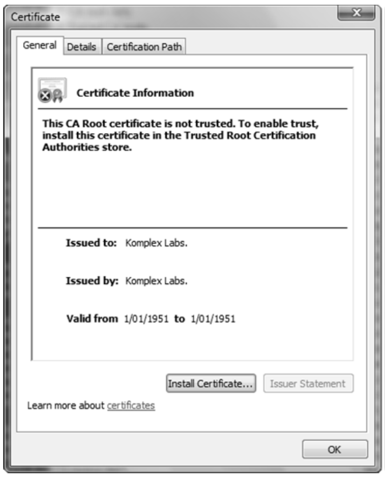
Certificate Fields

- Certificate Subject Key ID
- Certificate Basic Constraints
- Certificate Key Usage
- Extended Key Usage
- Certificate Policies
- Netscape Certificate Type
- Certificate Subject Alt Name
- Certificate Signature Algorithm
- Certificate Signature Value

Field Value

```
Not Critical
IP Address: 77.76.108.82
DNS Name: 77.76.108.82
IP Address: 192.168.1.2
DNS Name: 192.168.1.2
DNS Name: BAAPSVR1
DNS Name: baapensions.com
```

Measurement in Computer Security, Part 2 (ct



Certificate Information

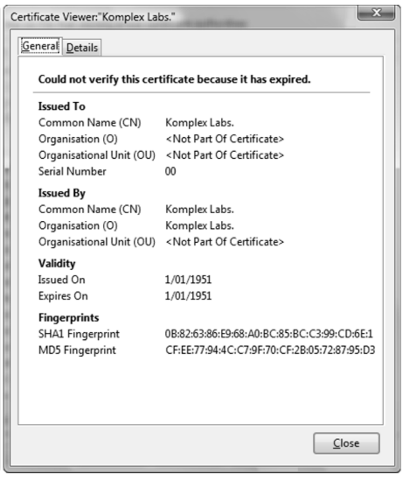
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: Komplex Labs.

Issued by: Komplex Labs.

Valid from 1/01/1951 **to** 1/01/1951

Learn more about certificates



Could not verify this certificate because it has expired.

Issued To

Common Name (CN)	Komplex Labs.
Organisation (O)	<Not Part Of Certificate>
Organisational Unit (OU)	<Not Part Of Certificate>
Serial Number	00

Issued By

Common Name (CN)	Komplex Labs.
Organisation (O)	Komplex Labs.
Organisational Unit (OU)	<Not Part Of Certificate>

Validity

Issued On	1/01/1951
Expires On	1/01/1951

Fingerprints

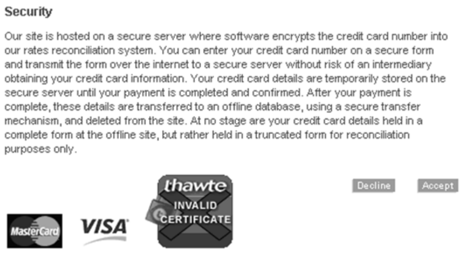
SHA1 Fingerprint	0B:82:63:86:E9:68:A0:BC:85:BC:C3:99:CD:6E:1
MD5 Fingerprint	CF:EE:77:94:4C:C7:9F:70:CF:2B:05:72:87:95:D3

Measurement in Computer Security, Part 2 (ct

```
-----BEGIN CERTIFICATE-----
MIIQojCCCIoCAQAwDQYJKoZIhvcNAQEEBQAwGDEWMBQGA1UEAxMNS29tcGxleCBM
YWJzLjAeFw01MTAxMDEwMDAwMDBaFw01MDEyMzEyMzU5NTlaMBgxFjAUBgNVBAMT
DUtvbXBsZXggTGFicy4wggggMA0GCSqGSIb3DQEBAQUAA4IIDQAwgggIAoIIAQCA
A+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+//////////////////////////////////////////////////////////////+
+//////////////////////////////////////////////////////////////+
+///++++HELLO+THERE++++////////////////////////////////////////+
+//////////////////////////////////////////////////////////////+
+///And/welcome/to/the/base64/coded/x509/pem/certificate/of////+
+//////////////////////////////////////////////////////////////+
+///KOMPLEX/MEDIA/LABS/////////////////////////////////////////+
+///www/dot/komplex/dot/org////////////////////////////////////+
+//////////////////////////////////////////////////////////////+
+///created/by/Markku+Juhani/Saarinen//////////////////////////+
+///22/June/2000///dw3z/at/komplex/dot/org/////////////////////+
+//////////////////////////////////////////////////////////////+
+///You/are/currently/reading/the/public/RSA/modulus///////////+
+///of/our/root/certification/authority/certificate////////////+
+//////////////////////////////////////////////////////////////+
+///Which/happens/to/be/16386/bits/long////////////////////////+
+//////////////////////////////////////////////////////////////+
+///And/fully/working/and/shit/////////////////////////////////+
+//////////////////////////////////////////////////////////////+
+///And/totally/insecure///////////////////////////////////////+
+//////////////////////////////////////////////////////////////+
```

Measurement in Computer Security, Part 2 (ct

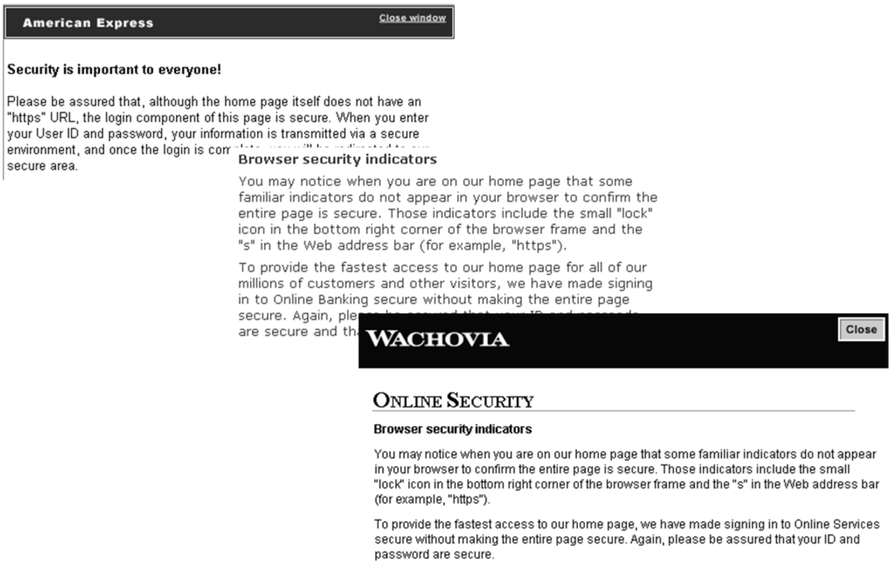
... whether certificates had any effect at all ...



Security

Our site is hosted on a secure server where software encrypts the credit card number into our rates reconciliation system. You can enter your credit card number on a secure form and transmit the form over the internet to a secure server without risk of an intermediary obtaining your credit card information. Your credit card details are temporarily stored on the secure server until your payment is completed and confirmed. After your payment is complete, these details are transferred to an offline database, using a secure transfer mechanism, and deleted from the site. At no stage are your credit card details held in a complete form at the offline site, but rather held in a truncated form for reconciliation purposes only.

Measurement in Computer Security, Part 2 (ct



Security is important to everyone!

Please be assured that, although the home page itself does not have an "https" URL, the login component of this page is secure. When you enter your User ID and password, your information is transmitted via a secure environment, and once the login is com

secure area.

Browser security indicators

You may notice when you are on our home page that some familiar indicators do not appear in your browser to confirm the entire page is secure. Those indicators include the small "lock" icon in the bottom right corner of the browser frame and the "s" in the Web address bar (for example, "https").

To provide the fastest access to our home page for all of our millions of customers and other visitors, we have made signing in to Online Banking secure without making the entire page secure. Again, ple

are secure and th

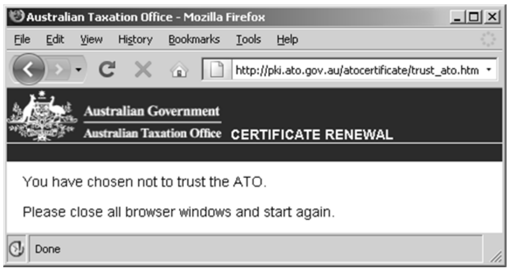
ONLINE SECURITY

Browser security indicators

You may notice when you are on our home page that some familiar indicators do not appear in your browser to confirm the entire page is secure. Those indicators include the small "lock" icon in the bottom right corner of the browser frame and the "s" in the Web address bar (for example, "https").

To provide the fastest access to our home page, we have made signing in to Online Services secure without making the entire page secure. Again, please be assured that your ID and password are secure.

Measurement in Computer Security, Part 2 (ct

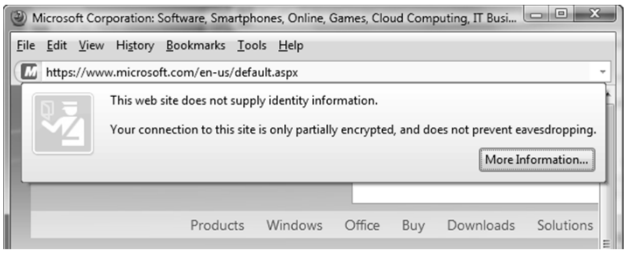


Australian Taxation Office - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
http://pki.ato.gov.au/atocertificate/trust_ato.htm
Australian Government
Australian Taxation Office
CERTIFICATE RENEWAL
Done

You have chosen not to trust the ATO.

Please close all browser windows and start again.

Measurement in Computer Security, Part 2 (ct

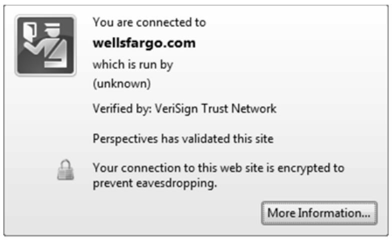

File Edit View History Bookmarks Tools Help
More Information...
Products Windows Office Buy Downloads Solutions

Microsoft Corporation: Software, Smartphones, Online, Games, Cloud Computing, IT Busi...

https://www.microsoft.com/en-us/default.aspx

This web site does not supply identity information.

Your connection to this site is only partially encrypted, and does not prevent eavesdropping.



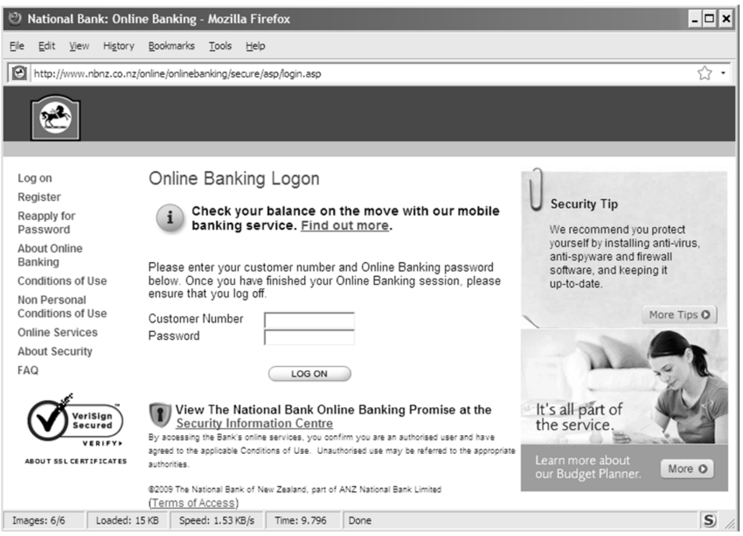
You are connected to
wellsfargo.com
which is run by
(unknown)

Verified by: VeriSign Trust Network

Perspectives has validated this site

Your connection to this web site is encrypted to prevent eavesdropping.

Measurement in Computer Security, Part 2 (ct



National Bank: Online Banking - Mozilla Firefox

http://www.nbnz.co.nz/online/onlinebanking/secure/asp/login.asp

Online Banking Logon

Check your balance on the move with our mobile banking service. Find out more.

Please enter your customer number and Online Banking password below. Once you have finished your Online Banking session, please ensure that you log off.

Customer Number
Password

View The National Bank Online Banking Promise at the Security Information Centre

By accessing the Bank's online services, you confirm you are an authorised user and have agreed to the applicable Conditions of Use. Unauthorised use may be referred to the appropriate authorities.

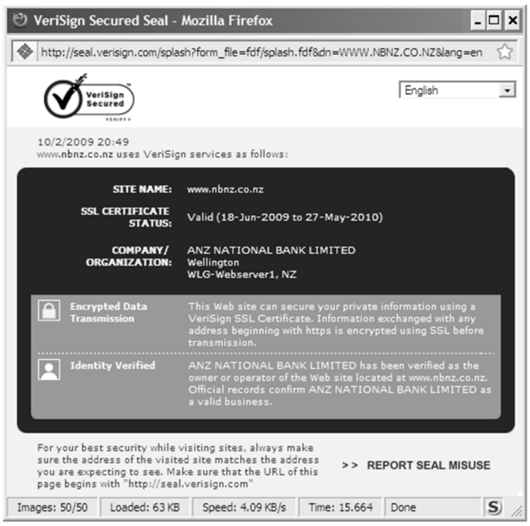
©2009 The National Bank of New Zealand, part of ANZ National Bank Limited
(Terms of Access)

Security Tip

We recommend you protect yourself by installing anti-virus, anti-spyware and firewall software, and keeping it up-to-date.

Images: 6/6 | Loaded: 15 KB | Speed: 1.53 KB/s | Time: 9.796 | Done

Measurement in Computer Security, Part 2 (ct



http://seal.verisign.com/splash?form_file=fdf/splash.fdf&dn=WWW.NBNZ.CO.NZ&lang=en

10/2/2009 20:49
www.nbnz.co.nz uses VeriSign services as follows:

SITE NAME: www.nbnz.co.nz

SSL CERTIFICATE STATUS: Valid (18-Jun-2009 to 27-May-2010)

COMPANY/ ORGANIZATION: ANZ NATIONAL BANK LIMITED
Wellington
WLG-Webserver1, NZ

Encrypted Data Transmission This Web site can secure your private information using a VeriSign SSL Certificate. Information exchanged with any address beginning with https is encrypted using SSL before transmission.

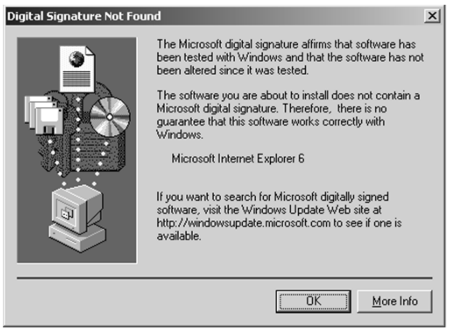
Identity Verified ANZ NATIONAL BANK LIMITED has been verified as the owner or operator of the Web site located at www.nbnz.co.nz. Official records confirm ANZ NATIONAL BANK LIMITED as a valid business.

For your best security while visiting sites, always make sure the address of the visited site matches the address you are expecting to see. Make sure that the URL of this page begins with "http://seal.verisign.com"

>> REPORT SEAL MISUSE

Images: 50/50 | Loaded: 63 KB | Speed: 4.09 KB/s | Time: 15.664 | Done

Measurement in Computer Security, Part 2 (ct



The Microsoft digital signature affirms that software has been tested with Windows and that the software has not been altered since it was tested.

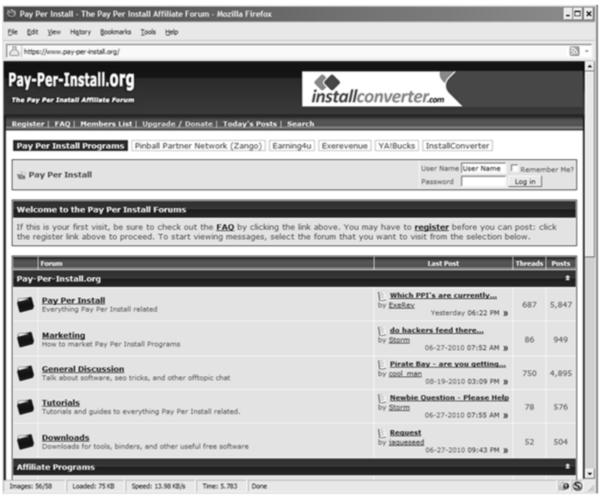
The software you are about to install does not contain a Microsoft digital signature. Therefore, there is no guarantee that this software works correctly with Windows.

Microsoft Internet Explorer 6

If you want to search for Microsoft digitally signed software, visit the Windows Update Web site at http://windowsupdate.microsoft.com to see if one is available.

Measurement in Computer Security, Part 2 (ct

... and whether the bad guys weren’t just getting certificates like everyone else ...

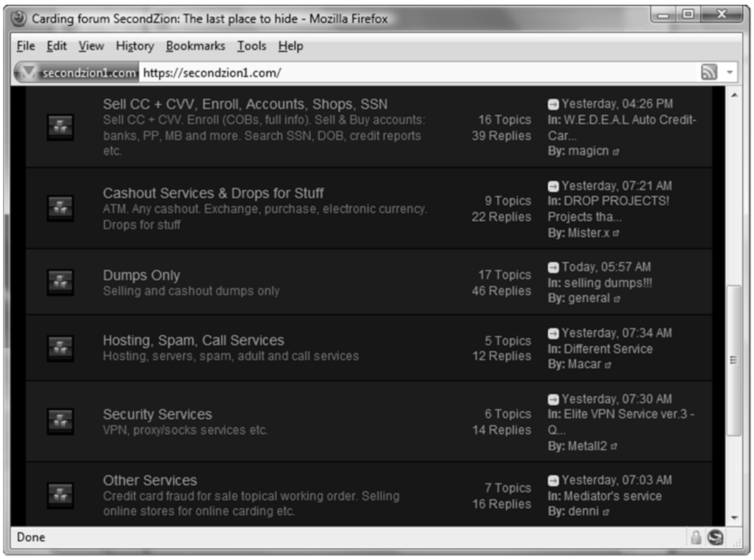

Pay Per Install - The Pay Per Install Affiliate Forum - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www.pay-per-install.org/
Pay-Per-Install.org
The Pay Per Install Affiliate Forum
installconverter.com
Register | FAQ | Members List | Upgrade / Donate | Today's Posts | Search
Pay Per Install Programs
Pinball Partner Network (Zango)
Earning4u
Exerevenue
YA!Bucks
InstallConverter
Pay Per Install
User Name
Remember Me?
Password
Log in

Welcome to the Pay Per Install Forums

If this is your first visit, be sure to check out the FAQ by clicking the link above. You may have to register before you can post: click the register link above to proceed. To start viewing messages, select the forum that you want to visit from the selection below.

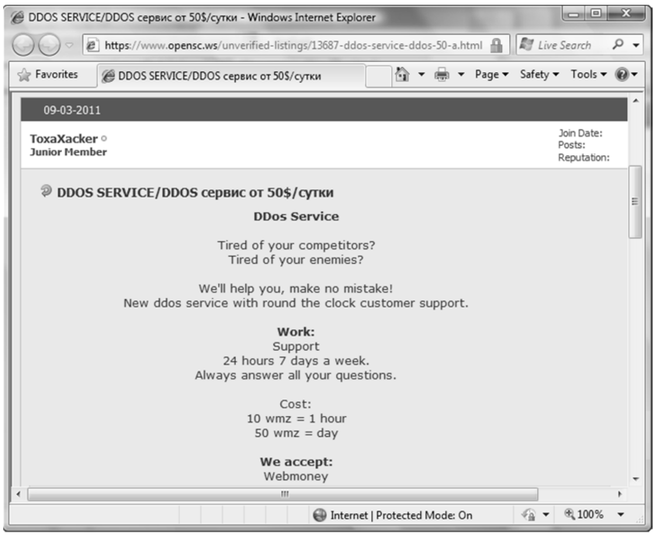
Forum	Last Post	Threads	Posts
Pay-Per-Install.org			
Pay Per Install Everything Pay Per Install related	Which PPI's are currently... by ExeRev Yesterday 06:22 PM	687	5,847
Marketing How to market Pay Per Install Programs	do hackers feed there... by Storm 06-27-2010 07:52 AM	86	949
General Discussion Talk about software, seo tricks, and other offtopic chat	Pirate Bay - are you getting... by cool_man 08-19-2010 03:09 PM	750	4,895
Tutorials Tutorials and guides to everything Pay Per Install related.	Newbie Question - Please Help by Storm 06-27-2010 07:55 AM	78	576
Downloads Downloads for tools, binders, and other useful free software	Request by jaqueseed 06-27-2010 09:43 PM	52	504
Affiliate Programs			

Measurement in Computer Security, Part 2 (ct


Carding forum SecondZion: The last place to hide - Mozilla Firefox
File Edit View History Bookmarks Tools Help
secondzion1.com
https://secondzion1.com/

Sell CC + CVV, Enroll, Accounts, Shops, SSN Sell CC + CVV. Enroll (COBs, full info). Sell & Buy accounts: banks, PP, MB and more. Search SSN, DOB, credit reports etc.	16 Topics 39 Replies	Yesterday, 04:26 PM In: W.E.D.E.A.L Auto Credit-Car... By: magicn
Cashout Services & Drops for Stuff ATM. Any cashout. Exchange, purchase, electronic currency. Drops for stuff	9 Topics 22 Replies	Yesterday, 07:21 AM In: DROP PROJECTS! Projects tha... By: Mister.x
Dumps Only Selling and cashout dumps only	17 Topics 46 Replies	Today, 05:57 AM In: selling dumps!!! By: general
Hosting, Spam, Call Services Hosting, servers, spam, adult and call services	5 Topics 12 Replies	Yesterday, 07:34 AM In: Different Service By: Macar
Security Services VPN, proxy/socks services etc.	6 Topics 14 Replies	Yesterday, 07:30 AM In: Elite VPN Service ver.3 - Q... By: Metall2
Other Services Credit card fraud for sale topical working order. Selling online stores for online carding etc.	7 Topics 16 Replies	Yesterday, 07:03 AM In: Mediator's service By: denni

Measurement in Computer Security, Part 2 (ct


DDOS SERVICE/DDOS сервис от 50$/сутки - Windows Internet Explorer
https://www.opensc.ws/unverified-listings/13687-ddos-service-ddos-50-a.html
Live Search
Favorites
DDOS SERVICE/DDOS сервис от 50$/сутки
Page
Safety
Tools
Internet | Protected Mode: On
100%

09-03-2011

ToxaXacker
Junior Member

Join Date:
Posts:
Reputation:

DDOS SERVICE/DDOS сервис от 50$/сутки

DDos Service

Tired of your competitors?
Tired of your enemies?

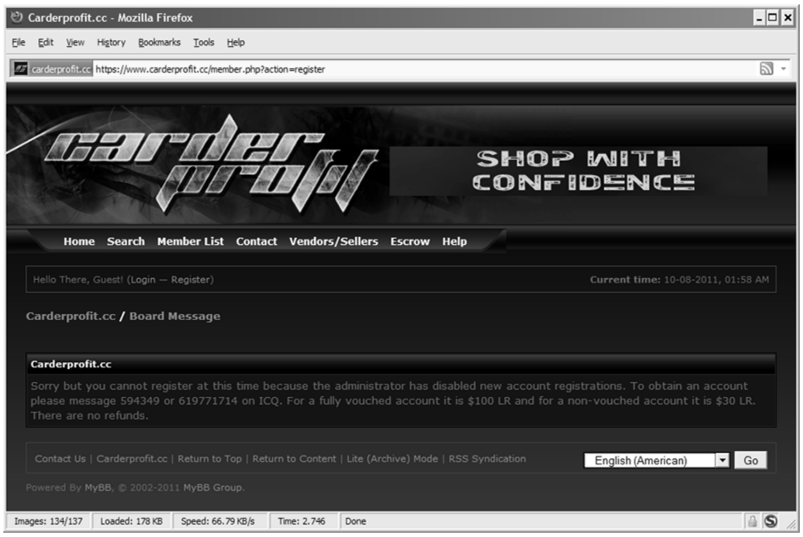
We'll help you, make no mistake!
New ddos service with round the clock customer support.

Work:
Support
24 hours 7 days a week.
Always answer all your questions.

Cost:
10 wmz = 1 hour
50 wmz = day

We accept:
Webmoney

Measurement in Computer Security, Part 2 (ct


Carderprofit.cc - Mozilla Firefox
File Edit View History Bookmarks Tools Help
carderprofit.cc https://www.carderprofit.cc/member.php?action=register
carder profit
SHOP WITH CONFIDENCE
Home Search Member List Contact Vendors/Sellers Escrow Help
Contact Us | Carderprofit.cc | Return to Top | Return to Content | Lite (Archive) Mode | RSS Syndication
English (American)
Go
Images: 134/137 Loaded: 178 KB Speed: 66.79 KB/s Time: 2.746 Done

Hello There, Guest! (Login — Register)

Current time: 10-08-2011, 01:58 AM

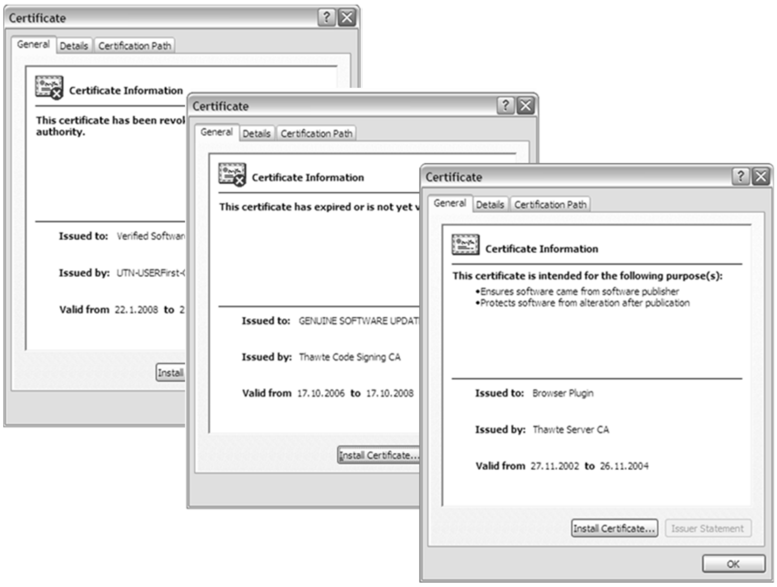
Carderprofit.cc / Board Message

Carderprofit.cc

Sorry but you cannot register at this time because the administrator has disabled new account registrations. To obtain an account please message 594349 or 619771714 on ICQ. For a fully vouched account it is $100 LR and for a non-vouched account it is $30 LR. There are no refunds.

Powered By MyBB, © 2002-2011 MyBB Group.

Measurement in Computer Security, Part 2 (ct



This certificate has been revol
authority.

Issued to: Verified Softwar

Issued by: UTN-USERFirst-(

Valid from 22.1.2008 to 2

This certificate has expired or is not yet v

Issued to: GENUINE SOFTWARE UPDAT

Issued by: Thawte Code Signing CA

Valid from 17.10.2006 to 17.10.2008

This certificate is intended for the following purpose(s):

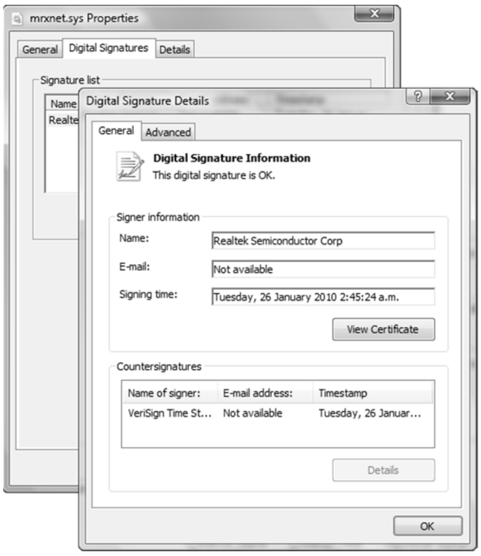
- Ensures software came from software publisher
- Protects software from alteration after publication

Issued to: Browser Plugin

Issued by: Thawte Server CA

Valid from 27.11.2002 to 26.11.2004

Measurement in Computer Security, Part 2 (ct



This digital signature is OK.

Signer information

Name: Realtek Semiconductor Corp

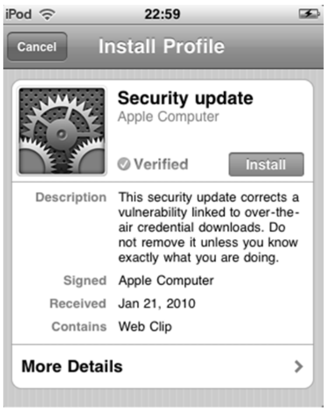
E-mail: Not available

Signing time: Tuesday, 26 January 2010 2:45:24 a.m.

Countersignatures

Name of signer:	E-mail address:	Timestamp
VeriSign Time St...	Not available	Tuesday, 26 Januar...

Measurement in Computer Security, Part 2 (ct



Security update
Apple Computer

✓ Verified

Description: This security update corrects a vulnerability linked to over-the-air credential downloads. Do not remove it unless you know exactly what you are doing.

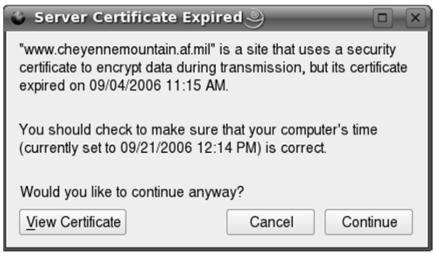
Signed: Apple Computer

Received: Jan 21, 2010

Contains: Web Clip

Measurement in Computer Security, Part 2 (ct

... but luckily no-one was using them for anything too critical



Server Certificate Expired

"www.cheyennemountain.af.mil" is a site that uses a security certificate to encrypt data during transmission, but its certificate expired on 09/04/2006 11:15 AM.

You should check to make sure that your computer's time (currently set to 09/21/2006 12:14 PM) is correct.

Would you like to continue anyway?

Measurement in Computer Security, Part 2 (ct

(That’s this place)

Measurement in Computer Security, Part 2 (ct

The plural of anecdote is not evidence

- I mean how bad can it really be?

Until 2010, no-one had ever tried to measure it

Measurement for Security Assurance

EFF SSL Observatory results

- 7.7M SSL/TLS servers
- 4M distinct certificates
- 1.5M had certificates trusted by major browsers

Experiment was re-run two years later by folks from USCB/UMichigan

- 12.8M SSL/TLS servers
  - Slightly different scanning method
- 5.8M distinct certificates
- 1.9M had certificates trusted by major browsers

Measurement for Security Assurance (ctd)

Two thirds of all “secure” web sites visited result in browser warnings due to untrusted/expired/whatever certificates

- True figure is actually worse than that due to domain mismatches/virtual hosting
- Results in browser warnings even if the certificate is trusted

Measurement for Security Assurance (ctd)

But wait, there's more...

- EFF looked at the contents of the certificates
- Not a very hard look, just some preliminary analysis

Results:

> You name it, it's there
>
> — An Observatory for the SSLiverse

Measurement for Security Assurance (ctd)

Private keys shared across multiple certificates/sites

- Private keys shared across CA certificates (!!)
- Appear to be unrelated, e.g. "American Optimum SSL CA" and "UK ComodoCA"
  - Possibly connected via something called "OptimumSSLCA"
- "UK ComodoCA Limited", "US Positive Software Corporation" (issued by "US USERTRUST"), and another "US Positive Software Corporation" (issued by "Swedish AddTrust")

Measurement for Security Assurance (ctd)

Invalid names (RFC 1918, unqualified names) all over the place

- According to the Belgian GlobalSign, 192.168.1.2 is in the US, the UK, Switzerland, Belgium, and at 77.76.108.82
- Over *six thousand* certificates issued to “localhost”
- Coming from CAs like Comodo , Go Daddy, GlobalSign, Starfield, Equifax, Digicert, Entrust, Cybertrust, Microsoft, and Verisign

Measurement for Security Assurance (ctd)

Other peculiarities

- Hundreds of thousands of certificates with 512-bit keys
- Tens of thousands of certificates with Debian weak keys
- End-entity certificates marked with CA capabilities
  - keyUsage = keyCertSign

Measurement for Security Assurance (ctd)

Arrghhh!!!!!!

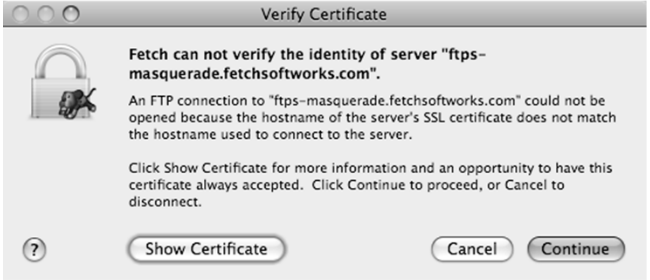
Measurement for Security Assurance (ctd)

It’s not that bad though

Measurement for Security Assurance (ctd)

There's a simple solution…

When a web (or SMTP, or FTP, or IMAP) server with SSL/TLS is set up, it should perform a loopback connection to itself to verify that everything's OK



Verify Certificate

Fetch can not verify the identity of server "ftps-masquerade.fetchsoftworks.com".

An FTP connection to "ftps-masquerade.fetchsoftworks.com" could not be opened because the hostname of the server's SSL certificate does not match the hostname used to connect to the server.

Click Show Certificate for more information and an opportunity to have this certificate always accepted. Click Continue to proceed, or Cancel to disconnect.

- If this happens then there's a problem

Measurement for Security Assurance (ctd)

General rule for all servers

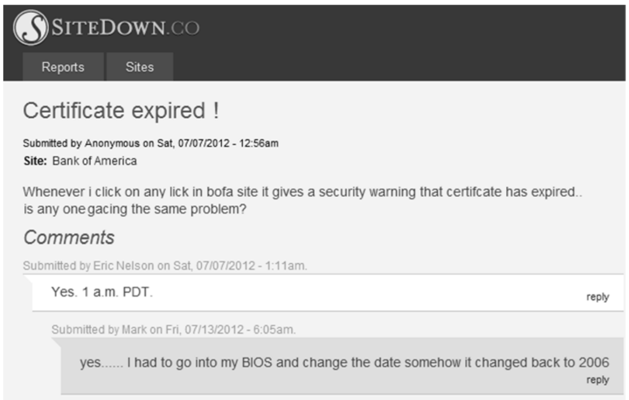
A web server should never announce that it's ready for operation until it's verified that it really is ready

Completely automated process

- Step *n* of the server installation

Measurement for Security Assurance (ctd)

Re-run the check every *n* hours to ensure that everything is still working OK



Certificate expired !

Submitted by Anonymous on Sat, 07/07/2012 - 12:56am

Site: Bank of America

Whenever i click on any lick in bofa site it gives a security warning that certifcate has expired.. is any one gacing the same problem?

Comments

Submitted by Eric Nelson on Sat, 07/07/2012 - 1:11am.

Yes. 1 a.m. PDT.

reply

Submitted by Mark on Fri, 07/13/2012 - 6:05am.

yes...... I had to go into my BIOS and change the date somehow it changed back to 2006

reply

- Customers having to reset their BIOS clock to access your site isn’t a good look for a large bank

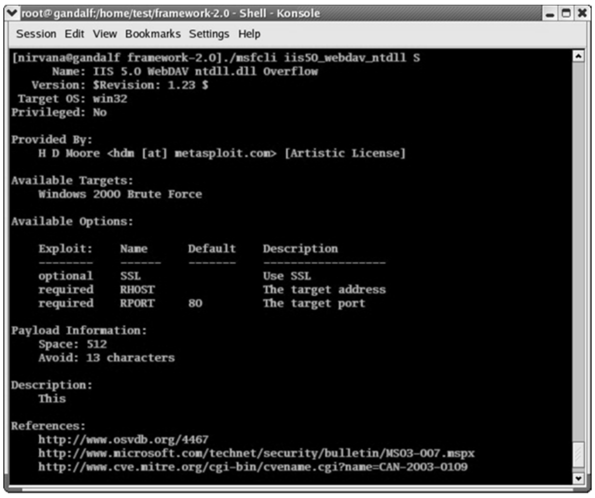
Measurement for Security Assurance (ctd)

This can be generalised to almost any security service

A system should never announce that it’s ready for operation until it’s verified that it really is ready

Measurement for Security Assurance (ctd)

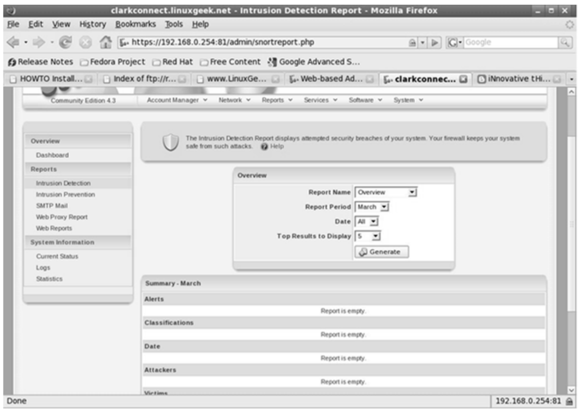
Run metasploit against your servers


root@gandalf:/home/test/framework-2.0 - Shell - Konsole
Session Edit View Bookmarks Settings Help

```
[nirvana@gandalf framework-2.0]./msfcli iis50_webdav_ntdll S
      Name: IIS 5.0 WebDAV ntdll.dll Overflow
   Version: $Revision: 1.23 $
 Target OS: win32
Privileged: No

Provided By:
    H D Moore <hdm [at] metasploit.com> [Artistic License]

Available Targets:
    Windows 2000 Brute Force

Available Options:

    Exploit:    Name      Default    Description
    --------    ------    -------    ------------------
    optional    SSL                  Use SSL
    required    RHOST                The target address
    required    RPORT     80         The target port

Payload Information:
    Space: 512
    Avoid: 13 characters

Description:
    This

References:
    http://www.osvdb.org/4467
    http://www.microsoft.com/technet/security/bulletin/MS03-007.mspx
    http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0109
```

Measurement for Security Assurance (ctd)

If your IDS tells you this ...



The Intrusion Detection Report displays attempted security breaches of your system. Your firewall keeps your system safe from such attacks.

Overview

Report Name: Overview

Report Period: March

Date: All

Top Results to Display: 5

Summary - March

Alerts

Report is empty.

Classifications

Report is empty.

Date

Report is empty.

Attackers

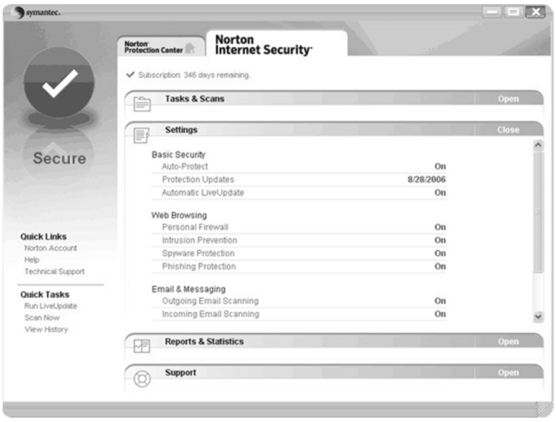
Report is empty.

Victims

... then you’ve wasted your money

Measurement for Security Assurance (ctd)

Drop the EICAR test file on every machine you have



✓ Subscription: 346 days remaining.

Tasks & Scans — Open

Settings — Close

Basic Security

Auto-Protect	On
Protection Updates	8/28/2006
Automatic LiveUpdate	On

Web Browsing

Personal Firewall	On
Intrusion Prevention	On
Spyware Protection	On
Phishing Protection	On

Email & Messaging

Outgoing Email Scanning	On
Incoming Email Scanning	On

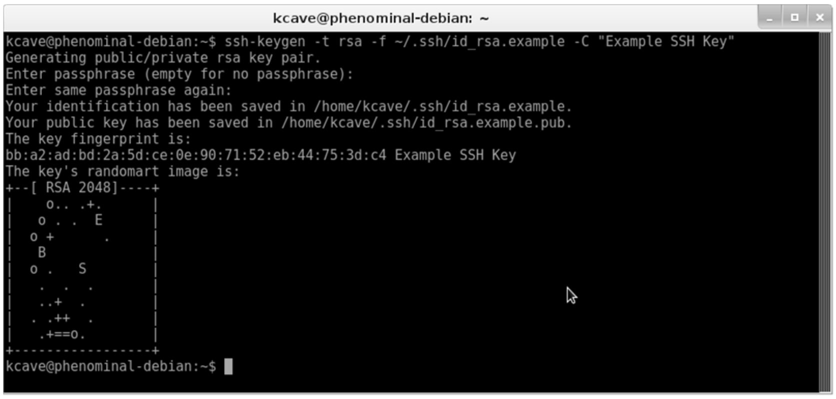
Reports & Statistics — Open

Support — Open

If you get this, you need a new A/V product

Measurement for Security Assurance (ctd)

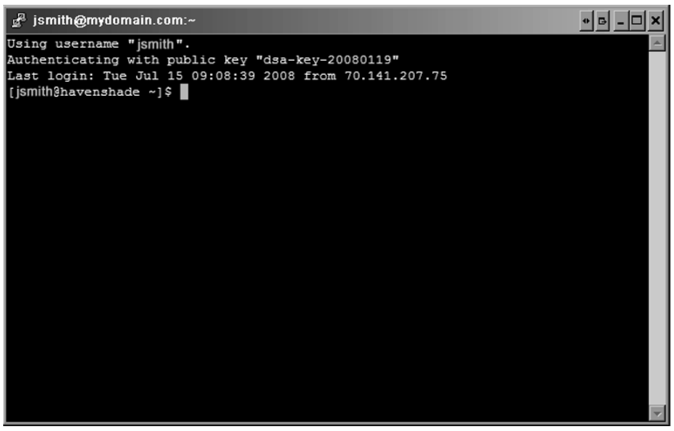
Regenerate your SSH server keys



```
kcave@phenominal-debian:~$ ssh-keygen -t rsa -f ~/.ssh/id_rsa.example -C "Example SSH Key"
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kcave/.ssh/id_rsa.example.
Your public key has been saved in /home/kcave/.ssh/id_rsa.example.pub.
The key fingerprint is:
bb:a2:ad:bd:2a:5d:ce:0e:90:71:52:eb:44:75:3d:c4 Example SSH Key
The key's randomart image is:
+--[ RSA 2048]----+
|    o.. .+.      |
|   o . .  E      |
|  o +      .     |
|   B             |
|  o .   S        |
|   .  .  .       |
|   ..+  .        |
|  . .++  .       |
|   .+==o.        |
+-----------------+
kcave@phenominal-debian:~$ 
```

Measurement for Security Assurance (ctd)

Getting this isn't a good sign



```
Using username "jsmith".
Authenticating with public key "dsa-key-20080119"
Last login: Tue Jul 15 09:08:39 2008 from 70.141.207.75
[jsmith@havenshade ~]$ 
```

Measurement for Security Assurance (ctd)

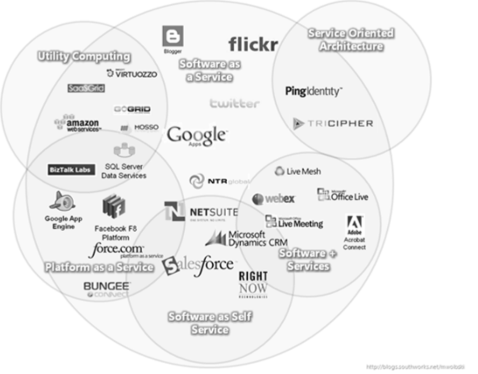
This could be a sign of an existing compromise

- You're connecting to a MITM
- MITM forwards the connecting to the actual server, suppressing the key-changed warning

As for the SSL loopback, checking this ensures that your view of what the server serves up is the same as the rest of the world's view

Measurement for Security Assurance (ctd)

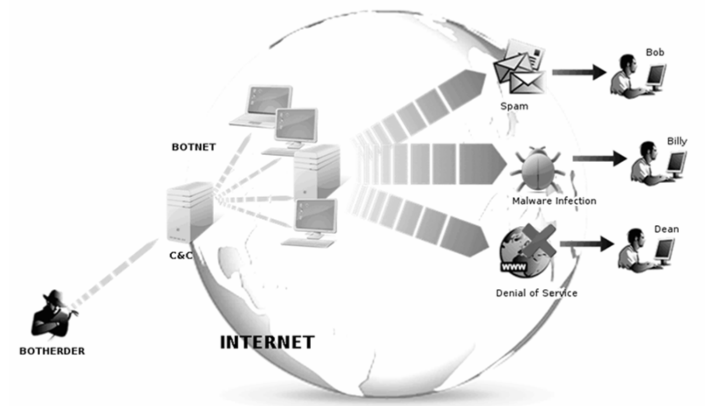
But to do this we’d need to perform the checking from an external site! How can we do that?



- You’d think that someone would have thought about this sort of thing already...

Measurement for Security Assurance (ctd)

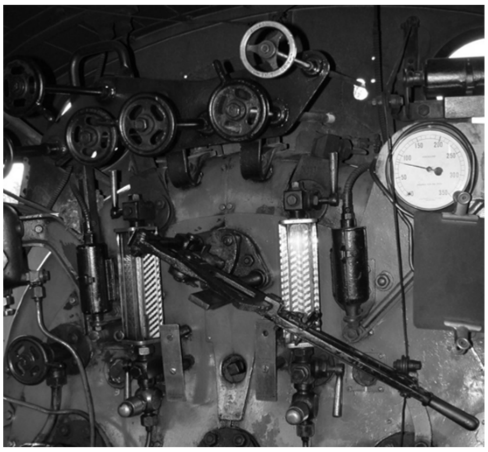
Leverage the synergy of the cloud!



Measurement for Security Assurance (ctd)

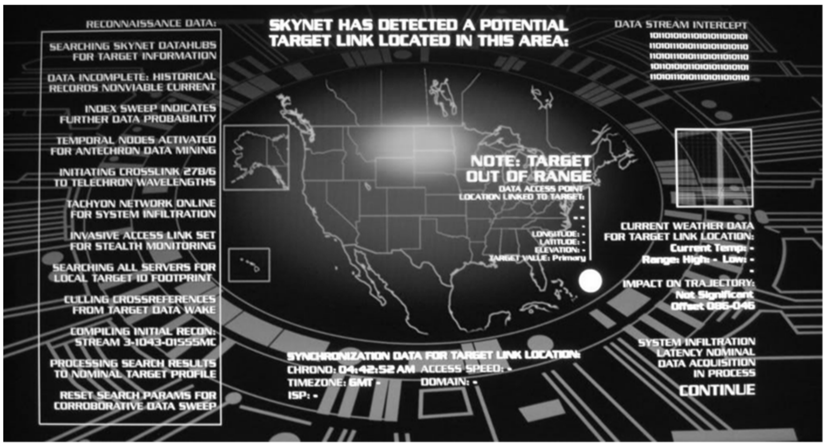
Make your security mechanisms part of an autonomous, self-evaluating system

- Mindlessly repeating boring tasks is what computers are there for
- No need to have humans checking and re-checking the controls



Measurement for Security Assurance (ctd)

Admittedly autonomous systems can be taken a bit too far if you’re not careful...



RECONNAISSANCE DATA:

SEARCHING SKYNET DATAHUBS FOR TARGET INFORMATION

DATA INCOMPLETE: HISTORICAL RECORDS NONVIABLE CURRENT

INDEX SWEEP INDICATES FURTHER DATA PROBABILITY

TEMPORAL NODES ACTIVATED FOR ANTECHRON DATA MINING

INITIATING CROSSLINK 27B/6 TO TELECHRON WAVELENGTHS

TACHYON NETWORK ONLINE FOR SYSTEM INFILTRATION

INVASIVE ACCESS LINK SET FOR STEALTH MONITORING

SEARCHING ALL SERVERS FOR LOCAL TARGET ID FOOTPRINT

CULLING CROSSREFERENCES FROM TARGET DATA WAKE

COMPILING INITIAL RECON: STREAM 3-1043-01555MC

PROCESSING SEARCH RESULTS TO NOMINAL TARGET PROFILE

RESET SEARCH PARAMS FOR CORROBORATIVE DATA SWEEP

SKYNET HAS DETECTED A POTENTIAL TARGET LINK LOCATED IN THIS AREA:

DATA STREAM INTERCEPT
1011010101101010101101010101
1101011101011101010110101110
1101011101011101010110101110
1011010101101010101101010101
1101011101011101010110101110

NOTE: TARGET OUT OF RANGE

DATA ACCESS POINT LOCATION LINKED TO TARGET:
-
- -
-
LONGITUDE: -
LATITUDE: -
ELEVATION: -
TARGET VALUE: Primary

CURRENT WEATHER DATA FOR TARGET LINK LOCATION:
Current Temp: -
Range: High: - Low: -
-

IMPACT ON TRAJECTORY:
Not Significant
Offset 086-046

SYNCHRONIZATION DATA FOR TARGET LINK LOCATION:
CHRONO: 04:42:52 AM ACCESS SPEED: -
TIMEZONE: GMT - DOMAIN: -
ISP: -

SYSTEM INFILTRATION LATENCY NOMINAL DATA ACQUISITION IN PROCESS

CONTINUE

Measurement for Security Assurance (ctd)

Summary

If you cannot measure it, you cannot improve it
— Lord Kelvin (perhaps)

You can’t manage what you can’t measure
— Management books

If you can’t measure it, you don’t even know whether it’s working or not
— Me, paraphrasing someone possibly paraphrasing
Lord Kelvin

If you *don’t* measure it, you won’t even know whether it’s working or not
— Me, corollary to the above