Communications & Networking

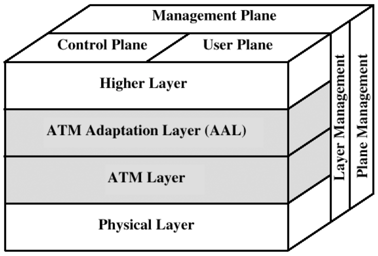
Miscellaneous Topics

ATM (Ch 14), Security (Ch 37), Management (Ch 36)

Asynchronous Transfer Mode (ATM)

- Asynchronous Transfer Mode (ATM) (a.k.a. cell relay) is a technology originally designed for use in wide area networks that is now often used in backbone networks and sometimes to the desktop
- History: Originally proposed by Bellcore, backed by other telecomm companies. One network to carry voice, video, data
  - Intended for WAN or LAN usage
- ATM is the switching and transport technology of the B-ISDN (Broadband ISDN) architecture (1980)
- ATM backbone switches typically provide point-to-point full duplex circuits at 155-622 Mbps but capable of Gigabit speeds over fiber

Protocol Architecture (diag)



ATM VCs

- Focus on **bandwidth allocation** facilities (in contrast to IP best effort)
- ATM main role today: "**switched**" link layer for **IP-over-ATM**
- ATM is a **virtual circuit** transport: cells (53 bytes) are carried on VCs

ATM and 53 byte cells

- Why 53 bytes?
  - 5 bytes for header
  - 48 bytes for payload
- So the real question becomes, why 48 bytes?
  - Voice applications
    - Want as little jitter as possible (variance in delay)
    - Want a short latency (long latency causes echo)
  - Switched virtual circuit will address jitter
  - Small cell size can address latency problem

ATM Cell Size and Latency

- Consider PCM: sample 8 bits at 8000Hz
  - I.e. 1 byte every 1/8000 seconds
  - If packet is 4000 bytes, it takes 4000/8000 or 0.5 seconds just to fill up the first packet! Half second delay right there!
  - If packet is 48 bytes, it takes 48/8000 or 6 milliseconds to start transmitting data
- Listeners for voice want low latency
- Low latency also makes echo cancellation possible (if latency is too high, echo cancellation circuitry gets confused with actual signal).
  - Small cell size helps address both echo cancellation and latency problems

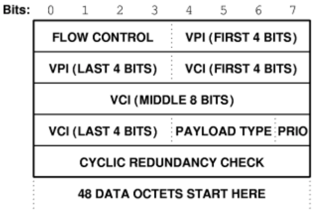
A True Story

- ATM to be a global standard, needed European cooperation
- US wanted 64 byte payload
  - Power of 2
  - Better for data transfers, less overhead, match existing equipment
- Europeans (French to be more specific) wanted 32 byte payload
  - France wanted 32 byte payload, 4 ms. cell fill time
  - Could just barely send voice data across France without need for echo cancellation
    - US needs them anyway
- 1989: CCITT compromised and set the payload at 48
  - Unfortunately, nobody was happy
    - US didn't get a power of 2, 5 byte header is 10% overhead
    - 48 bytes too high and France would need echo cancellators

Asynchronous Transfer Mode (ATM)

- ATM is a switched network but differs from switched ethernet in several ways:
  1. ATM uses fixed-length packets of 53 bytes.
  2. ATM provides no error correction on the user data.
  3. ATM uses a very different type of addressing from traditional data link layer protocols such as ethernet or token ring.
  4. ATM prioritizes transmissions based on Quality of Service (QoS).

ATM Cell Format

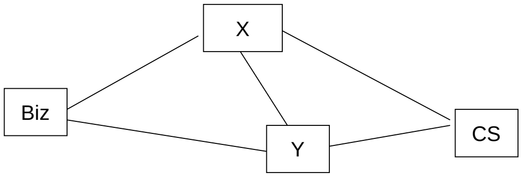


VPI/VCI : Identify address, Virtual Path & Virtual Circuit
Payload Type: Upper layer protocol
Prio: Priority bit to identify if packet can be discarded under congestion

ATM Connections

- Asynchronous Transfer Mode (ATM) is connection-oriented so all packets travel in order through the virtual circuit. A virtual circuit can either be a:
- **Permanent Virtual Circuit** (PVC) - defined when the network is established or modified. Like a leased circuit.
- **Switched Virtual Circuit** (SVC) - defined temporarily for one transmission and deleted with the transmission is completed.

ATM Addressing



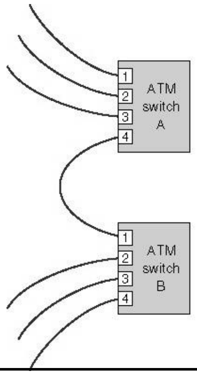
PVC: Always go CS→X→Biz
SVC: Might go CS→Y→Biz, or CS→Y→X→Biz

Routers/Switches decide on the actual path

SVC Example

- Jack in CS wants to videoconference with Jill in Biz
  - First: Establish a virtual circuit
    - Jack's computer establishes QoS parameters with the network server in CS, decides on route CS→X→Biz
    - CS node reserves a switch connection, say VC1
    - CS node sends VC1 to X, say X reserves connection VC2
    - X sends VC2 to Biz, Biz reserves connection VC3
    - Biz finds Jill's computer, sends her VC3. ACK's sent back to finish the connection and Jack gets back VC1
  - Jack→VC1(CS)→VC2(X)→VC3(Biz)→Jill
  - Jill→VC3(Biz)→VC2(X)→VC1(CS)→Jack
  - Reserved connection along the way allows for QoS
- When done, connection torn down, virtual circuits put back into a pool for reuse

Addressing & Forwarding with ATM Virtual Circuits



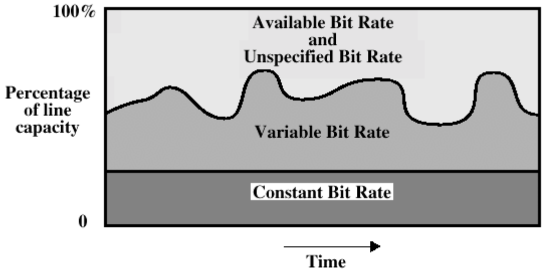
Switch A Circuit Table

Incoming Port	Incoming Circuit	Outgoing Port	Outgoing Circuit
1	1,10	4	3,15
2	3,18	1	2,10
2	2,11	4	2,11
3	4,10	2	3,26
3	4,11	2	1,18
4	5,10	1	4,21

ATM QoS

- When a virtual circuit is established, the Transport Layer (“the customer”) and the ATM layer (“the carrier”) need to agree on the service used. The “contract” has three parts:
  - The traffic to be offered
  - The service agreed upon
  - The compliance requirements
- The contract may be different for each direction. If both sides cannot agree on a contract the virtual circuit won't be setup
- Classes of service:
  - Constant Bit Rate, Variable Bit Rate, Available Bit Rate, Unspecified Bit Rate

ATM Bit Rate Services



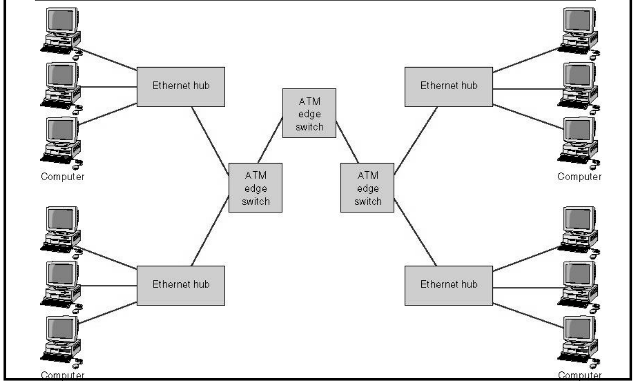
ATM VCs

- In IP over ATM: Permanent VC’s between IP routers
- Scalability problem: *N(N-1)* VCs between all IP router pairs
- Pros of ATM VC approach:
  - Can guarantee QoS performance to a connection mapped to a VC (bandwidth, delay, delay jitter)
- Cons of ATM VC approach:
  - Inefficient support of **datagram** traffic; PVC solution (one PVC between each host pair) does **not scale**;
  - SVC introduces excessive **latency** on short lived connections
  - Can’t support broadcast

ATM and Traditional LANs

- ATM
  - Connection-oriented
  - Small 53-byte fixed length packet
- Ethernet
  - Larger variable length packets
  - Typically connectionless
- Translation must be done to enable the LAN packets to flow over the ATM backbones. There are two approaches LAN encapsulation (LANE) and Multiprotocol over ATM (MPOA) – an extension to LANE

LAN Encapsulation (LANE)



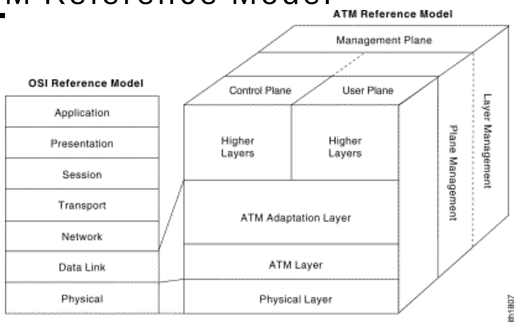
ATM and Traditional LANs

- Translating from ethernet or token ring into ATM is not simple.
- First the ethernet address must be translated into an ATM virtual circuit identifier for the edge switches; hard because there is no easy way to broadcast
- Once the virtual circuit address for the destination data link layer address has been found, it can be used to transmit the packet through the ATM backbone.

ATM and Traditional LANs

- Once the virtual circuit is ready, the LAN packet is broken into the series of ATM cells, and transmitted over the ATM backbone using the ATM virtual circuit identifier.
- Unfortunately this process can cause quite a delay (a reduction up to 50 %).

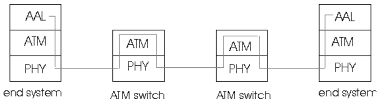
ATM Reference Model



- For an IP client, just replaces the Data Link Layer

Datagram Journey in IP-over-ATM Network

- **At Source Host**:
  - (1) IP layer finds the mapping between IP and ATM exit address (using ARP); then, passes the datagram to ATM Adaption Layer (AAL)
  - (2) AAL **encapsulates** data and **segments** into cells; then, passes down to ATM
- **In the network**, the ATM layer moves cells from switch to switch, along a **pre-established VC**
- **At Destination Host**, AAL **reassembles** cells into original data;
  - if CRC OK, datgram is passed up the IP protocol.



ARP in ATM Nets

- ATM can route cells only if it has the ATM address
  - Thus, IP must **translate** exit IP address to ATM address
- The IP/ATM addr translation is done by **ARP** (Addr Recogn Protocol)
- Generally, ATM ARP table does not store **all ATM addresses**: it must **discover** some of them
- **Two techniques**:
  - broadcast
  - ARP servers

ARP in ATM Nets (more)

- (1) **Broadcast** the ARP request to **all destinations**:
  - (1.a) the **ARP Request** msg is broadcast to all ATM destinations using a special broadcast VC;
  - (1.b) the ATM destination which can match the IP address returns (via unicast VC) the IP/ATM address map;
- Broadcast overhead prohibitive for large ATM nets.

ARP in ATM Nets (more)

⌘ (2) **ARP Server:**

- (2.a) **source IP router** forwards ARP request to an ARP server on dedicated VC
- (2.b) **ARP server** responds to source router with IP/ATM translation

⌘ Hosts must **register** themselves with the ARP server

Comments: more **scaleable** than ABR Broadcast approach (no broadcast storm). However, it requires an **ARP server**, which may be swamped with requests

ATM to the Desktop

⌘ **ATM-25** is a low speed version of ATM which provides point-to-point full duplex circuits at 25.6 Mbps in each direction. It is an adaptation of token ring that runs over cat 3 cable and can even use token ring hardware if modified.

⌘ **ATM-51** is another version designed for the desktop allowing 51.84 Mbps from computers to the switch.

ATM Forum

Standards body for ATM

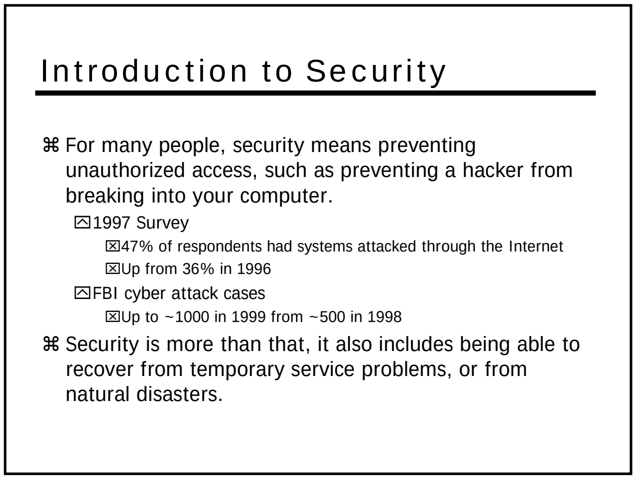
http://www.atmforum.org

Some members

AT&T
Cisco
3Com
IBM
Lucent
LSI Logic

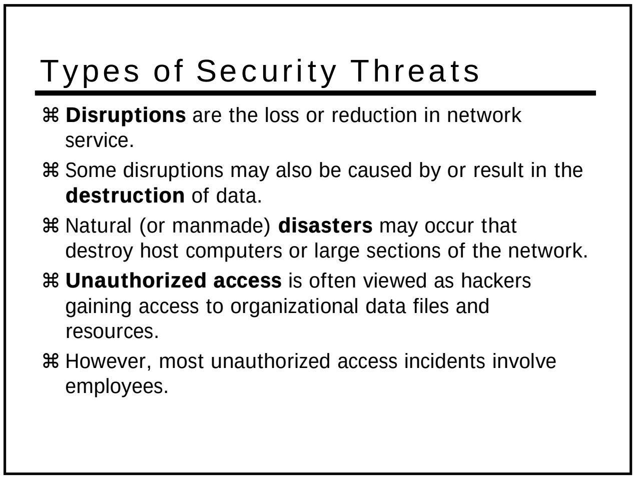
Network Security

Chapter 37



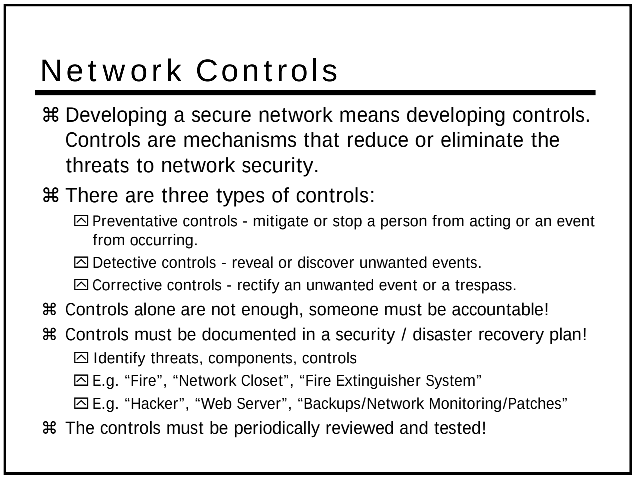
Introduction to Security

- For many people, security means preventing unauthorized access, such as preventing a hacker from breaking into your computer.
  - 1997 Survey
    - 47% of respondents had systems attacked through the Internet
    - Up from 36% in 1996
  - FBI cyber attack cases
    - Up to ~1000 in 1999 from ~500 in 1998
- Security is more than that, it also includes being able to recover from temporary service problems, or from natural disasters.



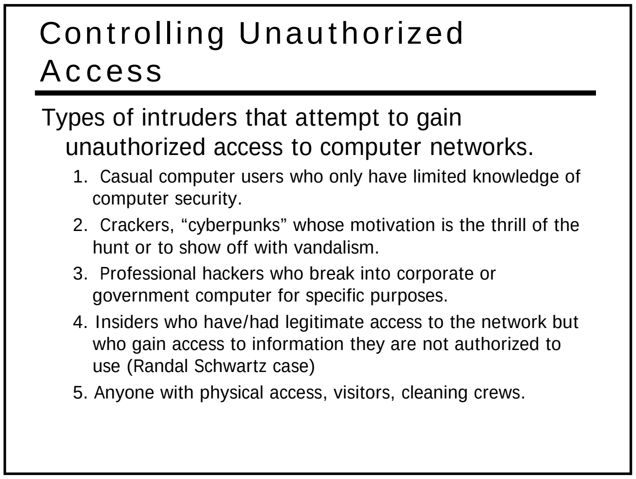
Types of Security Threats

- **Disruptions** are the loss or reduction in network service.
- Some disruptions may also be caused by or result in the **destruction** of data.
- Natural (or manmade) **disasters** may occur that destroy host computers or large sections of the network.
- **Unauthorized access** is often viewed as hackers gaining access to organizational data files and resources.
- However, most unauthorized access incidents involve employees.



Network Controls

- Developing a secure network means developing controls. Controls are mechanisms that reduce or eliminate the threats to network security.
- There are three types of controls:
  - Preventative controls - mitigate or stop a person from acting or an event from occurring.
  - Detective controls - reveal or discover unwanted events.
  - Corrective controls - rectify an unwanted event or a trespass.
- Controls alone are not enough, someone must be accountable!
- Controls must be documented in a security / disaster recovery plan!
  - Identify threats, components, controls
  - E.g. “Fire”, “Network Closet”, “Fire Extinguisher System”
  - E.g. “Hacker”, “Web Server”, “Backups/Network Monitoring/Patches”
- The controls must be periodically reviewed and tested!



Controlling Unauthorized Access

Types of intruders that attempt to gain unauthorized access to computer networks.

1. Casual computer users who only have limited knowledge of computer security.
2. Crackers, “cyberpunks” whose motivation is the thrill of the hunt or to show off with vandalism.
3. Professional hackers who break into corporate or government computer for specific purposes.
4. Insiders who have/had legitimate access to the network but who gain access to information they are not authorized to use (Randal Schwartz case)
5. Anyone with physical access, visitors, cleaning crews.

Some threats from attackers

- Service interruption; denial of service
- Theft and fraud
- Data contamination
- Misappropriation (funds or resources)
- Content alteration (vandalism)
- Masquerade or “look alike” site
- Masquerade as another person
  - Mail Spoofing – Promiscuous mail server
  - Forging fake email from a different sender
  - Oracle lawsuit, NWU Student dismissed

Methods of Attack

- Physical Access
  - Is your machine secure at night? During the day?
  - Unattended terminals, logged in or not?
- Viruses and Trojan Horses
- Local network attacks
  - Improper file permissions
- Protocol Attacks
- Application bugs
  - Out of range input, buffer overflows, syntax checks
  - Debugging code left in, reverse-engineered

Preventing Unauthorized Access

- The key principle in preventing unauthorized access is to be proactive. This means routinely testing your security systems before an intruder does.
- Approaches to preventing unauthorized access:
  - Developing a security policy
  - Developing user profiles
  - Plugging known security holes
  - Securing network access points
  - Preventing eavesdropping
  - Using encryption
- A combination of all techniques is best to ensure strong security.

Developing a Security Policy

- The security policy should clearly define the important network components to be safeguarded and the important controls needed to do that.

- The most common way for a hacker to break into a system , is through social engineering (breaking security simply by asking).

Elements of a Security Policy

⌘Name of responsible individuals

⌘Incident reporting system and response team

⌘Risk assessment with priorities

⌘Controls on access points to prevent or deter unauthorized external access.

⌘Controls within the network to ensure internal users cannot exceed their authorized access.

⌘An acceptable use policy

⌘User training plan on security

⌘Testing and updating plans.

Plugging Known Security Holes

⌘ Many commonly used operating systems and application programs have major security problems well known to potential users (security holes), many of which are highly technical.

⌘ Some security holes are not really holes, but simply policies adopted by computer vendors that open the door for security problems, such as computer systems that come with a variety of preinstalled user accounts (e.g. WinGate software defaults)

⌘ The security personnel should be proactive in looking for known security holes and applying patches.

Sample Security Holes

From bugtraq:

11/29/01: VU#886083: WU-FTPD does not properly handle glob command

The globbing code is designed to recognize invalid syntax and return an error condition to the calling function. However, when it encounters a specific string, the globbing code fails to properly return the error condition. Therefore, the calling function proceeds as if the glob syntax were correct and later frees unallocated memory that can contain user-supplied data. If intruders can place addresses and shellcode in the right locations on the heap using FTP commands, they may be able to cause WU-FTPD to execute arbitrary code by later issuing a command that is mishandled by the globbing code.

Sample Security Holes

11/9/01: Redhat 7.0 Local Root

/usr/sbin/makewhatis

An earlier version(1) of makewhatis had a fault in the handling of compressed files that allowed execution of arbitrary commands as root.

A patch for this problem was developed that seemed to be effective.

However, the patch was not restrictive enough in the metacharacters it filtered out.

It is still possible to perform file creation or overwriting with arbitrary contents, as root.

5/31/00: Vulnerability in the Windows Media Encoder 4.0 and 4.1 which allows a remote user to crash the encoder by connecting to the MSBD service. A bogus packet causes the encoder to attempt to allocate more memory than the computer has resulting in a crash.

6/1/99: OmniHTTPd Web Server comes with a sample CGI that can be used to fill the webservers disk.

Securing Network Access Points

- There are three major ways of gaining access:
  - Using a terminal or computer located in the organization’s offices
  - Dialing into the network via modem
  - Accessing the network from another network to which it is connected (e.g. Internet)
- The physical security of the building or buildings that house any of the hardware, software or communications circuits must be evaluated.

Securing Network Access Points

- With the increasing use of the Internet, and information superhighway, it becomes important to prevent unauthorized access to your network from intruders on other networks.
- A firewall is a router, gateway, or special purpose computer that examines packets flowing into and out of a network and restricts access to the organization’s network.

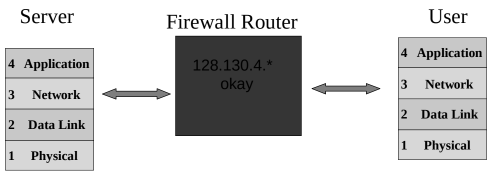
Securing Network Access Points

- A **packet-level** firewall examines the source and destination address of every network packet that passes through it and only allows packets that have acceptable source and destination addresses to pass.

Packet Level Firewall

Filtering at the packet level to deny/admit based on source.

Susceptible to IP Spoofing (forging the source address of a packet)



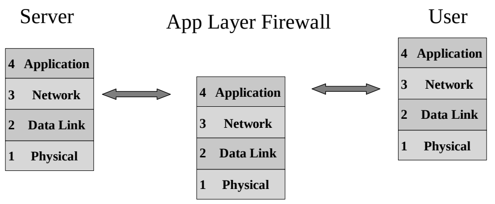
Securing Network Access Points

- An application-level firewall acts as an intermediate host computer or gateway between the Internet and the rest of the organization’s network.
- In many cases, special programming code must be written to permit the use of application software unique to the organization.

Application Level Firewall

More flexible; application program can dictate filtering rules.

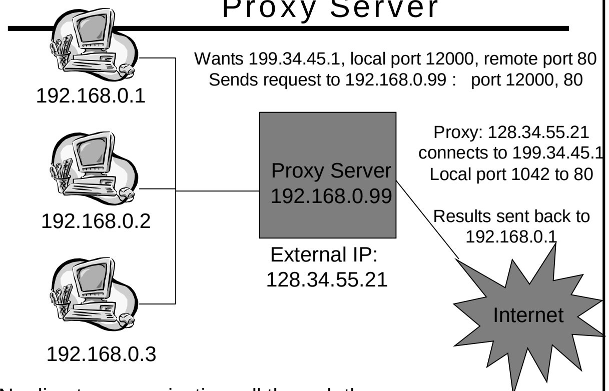
Stateful Inspection Firewall may remember prior data to determine filtering.



Proxy Server

- Proxy servers are used to control outside and inside access.
- The proxy server uses an address table to translate network addresses inside the organizations into fake addresses for use on the Internet (network address translation or address mapping). One standard is the SOCKS proxy.
- This way systems outside the organization never see the actual internal IP addresses.
- Many organizations use a combination of packet-level and application-level firewalls.
- NAT : Network Address Translation, done for you at the network layer

Proxy Server



No direct communication; all through the proxy server

Preventing Eavesdropping

- Another way to gain unauthorized access is to eavesdrop on network traffic, where the intruder inserts a listening device or compute into the organization’s network to record messages.
- Two areas vulnerable to this type of unauthorized access:
  - Network cabling
  - Network devices
  - Ensure network closet is secure, no tampering to cabling, physically secure! (e.g. not lying around outside)

Using Encryption

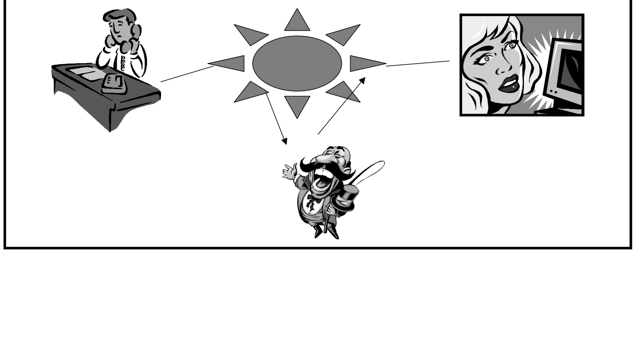
- One of the best ways to prevent unauthorized access is encryption, which is a means of disguising information by the use of algorithms.
- We may skip crypto (the next 20 slides)

Cryptography

- Greek for “secret writing”
- Used for centuries, very ad hoc
  - Spies, government, military
  - German Enigma machine
- 1970’s formalized with mathematical foundation
- Fundamental to secure transactions, commercial applications

Crypto Example

- Bob is a supplier
- Alice is a purchaser
- Communicate over an insecure network



Crypto Example

- Alice wants to make sure she is dealing with Bob, not an imposter (authentication)
- Bob wants to make sure he is dealing with Alice because she gets special prices
- Alice and Bob want to keep the order secret from competitors and other customers
- Alice and Bob want to make sure crackers don't change the price or quantity (integrity)
- Bob wants to make sure that Alice can't deny having placed the order (repudiation)

Issues

- Privacy
  - Message is secret
- Authentication
  - Recipient knows the message is not a forgery
- Integrity
  - Message was not tampered with in transit
- Nonrepudiation
  - Author can't later deny sending the message

Crypto Terminology

- Plaintext – original, non-encrypted message
- Ciphertext – encrypted message
- Key – Information allowing encryption or decryption, just like a physical key or combination lock
- Secret / Symmetric systems – Both encryption and decryption use the same operational key
- Asymmetric systems – Use a different key for encryption than for decryption. Public/Private key.
  - Can also be used to provide digital signatures.
  - Grows to larger worldwide scale more easily

Evaluating Crypto

- Algorithms
  - Method used to encrypt the data
  - Use a well-known algorithm!
- Protocols
  - Ways the algorithms are applied to problems, such as securing a channel or info in a database
- Key Management
  - How to create, store, and distribute keys
  - Often the weakest link in the system!

Cryptographic Strength

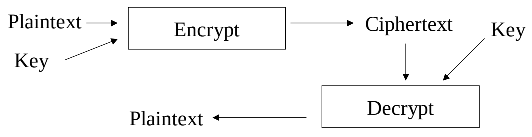
- Assume algorithm is available
- Assume lots of ciphertext available
- Can the plaintext be deciphered?
  - Ex: Substitution cipher, assign different letter to each letter; Y="A", E="Z", S="B" so to encrypt "YES" this becomes "AZB"
  - Can use statistical properties to help deduce guesses
- If ciphertext/plaintext available, can the key be deciphered?
- Try all possible keys: brute force attack
  - Impossible to prevent, but we can make this very expensive to compute

Crypto Strength

- Key length usually measured in bits
- Data Encryption Standard, DES
  - uses 56 bits, so 2^{56} possible keys.
  - About 72 trillion possible values
  - Too many values to search by brute force? Rocke Verser in 1997 broke a DES key using distributed computers on the Internet in about 6 months
- RSA scheme
  - 40 bit key cracked in under 4 hours
  - 48 bit also easy to crack
  - 128 bit not publicly cracked!
  - In 1977, inventors published 428 bit encrypted message
    - $100 prize, estimated 40 quadrillion years
    - Cracked in 1994 using 1600 systems on the Internet
  - 1024 bit version not crackable yet!

Secret Key Crypto

- DES a common example of secret key cryptography

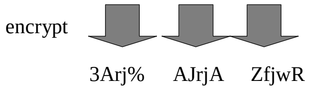


Block Cipher

- Takes a fixed-length block of plaintext, perhaps 64 bits, and encrypts it

Plaintext: ATTACK AT DAWN

Using blocks of 4 chars: ATTA, CK A, DAW, N



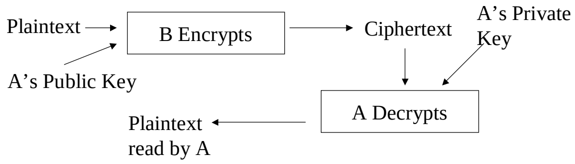
Each block is usually treated as a number.
Most schemes use block ciphers.
There are some modifications to prevent repeating blocks so someone couldn't insert them and confuse the data.

Some secret key systems

- DES
  - 56 bit key 64 bit blocks
- Triple DES
  - Uses three 56 bit DES keys
- IDEA
  - 128 bit encryption
- CAST
  - 40 to 128 bit encryption
  - Used in Pretty Good Privacy PGP system

Public Key Crypto

- Each participant gets two keys
  - Public key is made available to anyone
  - Private key is kept secret
- Like a safe with a slot in the top – anyone can put information in, but only the person with the combo can get it out



Authentication

- Problem with the previous – anyone could have sent the message!
- Solution : double encryption. Design the public and private keys so that they can encrypt or decrypt each other:
  - M = Plaintext Message
  - P = Public Key
  - S = Secret Key
  - Then: M = P(S(M)) and M=S(P(M))
- That is, if we encrypt with the public key, we can decrypt it with the private key. Similarly if we encrypt with the private key, we can decrypt it with the public key.

Crypto Example

- To solve the authentication problem:
- Bob encrypts the message M using his private key to get C1
- Bob encrypts C1 using Alice's public key to get C2 and sends it to Alice
- Alice decrypts C2 using her private key to get C1
- Alice decrypts C1 using Bob's public key
- If this all works, only Alice can read M and only Bob could have sent it! (idea of digital signature)

How it works

- We need a 1-way function (or a close approximation of one).
- A 1-way function is one that is easy to compute in one direction, but hard in the other
- Addition: easy to go both directions
- Factoring large numbers: hard
  - But it’s easy to generate large numbers!
  - We’ll use this as our one-way function. To break the code requires being able to factor humongous numbers quickly, and no fast algorithms are known to do this

RSA CryptoSystem

- Select at random two large prime numbers, *p* and *q* (they might be say, 100 decimals each)
- Compute $n=pq$
- Compute a small value *e* such that *e* is relatively prime to $(p-1)(q-1)$; i.e. $e < (p-1)(q-1)$ and the greatest common divisor of *e* and $(p-1)(q-1)$=1.
- Compute the large integer *d* such that
  - $ed \bmod (p-1)(q-1) = 1$
- Publish the pair (e,n) as the public key
- Keep the pair (d, n) as the secret key
- Given some message block M:
  - PublicKey(M) = M^e mod n
  - PrivateKey(M) = C^d mod n

RSA

- Nice property that PrivateKey(PublicKey(M)) = M
  - $(M^e \bmod n)^d \bmod n = M$
- Basic idea: factoring is hard
  - To break the code, we need to factor *n* into *p* and *q*, which together with *e*, gives us *d*
  - 512 bits requires 3000 MIPS-Years to break using the best known factoring algorithm

RSA Example

- Select two prime numbers, $p=3$, $q=5$
- Calculate $n=pq$ = 3*5 = 15
- Calculate $phi = (p-1)(q-1)$ = 8
- Select *e* such that *e* is relatively prime to *phi*. Pick $e=3$
- Compute *d* such that $de \bmod 8 = 1$. In this case, d=19 because 19 * 3 = 57 = 7*8 +1.

- Pair (3,15) is the public key
- Pair (19, 15) is the private key

RSA Example

- Check if
  - PrivateKey(PublicKey(M)) = M
  - $(M^e \bmod n)^d \bmod n = M$
  - e=3, n=15, d=19
- Say your message is the number 8
- PublicKey(8) = 8^3 mod 15
  - 512 mod 15 = 2
- PrivateKey(2) = 2^{19} mod 15
  - 524288 mod 15 = 8 Our original message!

- PrivateKey(8)=8^{19} mod 15
  - 144115188075855872 mod 15 = 2
- PublicKey(2) = 2^3 mod 15
  - 8 mod 15 = 8 Our original message!

Example of PGP Public Key

http://www.pgpi.org

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i

mQCNAzPUgqkAAAEEAMNwV7EVk0O5abgCOdxhgv2Noi6wBpB0uT2KTAzlOcfV9h+O
78JO/9g+lfBy8qv1tNCk1066AmPtqWHMCvtNDAeCoZjv8z5P9EtXtkMrAaqB9VRD
DsDeEy835Vbo9Zr4WxyQCrOxibjmFTDo8XtpZqhadoYk6by3IAQGtYkKcMZtAAUR
tBtFbG1hciBLLiBCaW5zIDxla2JAaXZtLm5ldD6JAJUDBRAz1IKqBAa1iQpwxm0B
AZJlA/0a8DeBynVVuX3LYw31R3TvwKz+G7rZnQNQCP2Gxi5VpoPwoh17niN3V+1Q
SITnX61WxKA3PwaZJqzAqxJSNkAi4kO4LSMhPSHrsI67+o0T6ZtOPgO+n/726Obf
zkT2hR3KA3d+zLF0UrF345UDNQPPcTvEW6HSJm2H2EwxAoMOObQfRWxtYXIgSy4g
QmlucyA8ZWxtaUBjZXBoaXIuY29tPokAlQMFEDPU3WsEBrWJCnDGbQEBvBED/0XM
n+OAcLenlV003xXjVsKYyGVQPRsjM3opkWUdwVB2HO+obIoJJ8fYomMdjrW10aP9
CnQ8JbMbH93+1rXpLPPNloAbpo/7/xfCyASCED1HyvxdlWalIbM0VYwUif8iU81V
DBU1OOe6JWxCi7mMpnDQBwfTzebW4Pp1jbNbtumUtB9FbG1hciBLLiBCaW5zIDxl
bG1pQGRldGViZS5vcmc+iQCVAwUQM9TdWwQGtYkKcMZtAQF0EwQAoeobmAtOI/Bp
ZlkxX/sjq7qheuM/4HOr3TUp+AiLdKVVF4Qaj+R91v9brz2nTQOKjIIhwhcm0eZE
oej2/DIbgGQWEzeNY5TAN7V0nA76EnZb3MF7ywgjOwzrhj7UZeptyZyotUgy7Alb
/Y3TRKr1WgG4+/QLAnbRyKSRnn67Vpy0HUVsbWFyIEsuIEJpbnMgPGVsbWlAZWxt
aS5vcmc+iQCVAwUQM9TdRAQGtYkKcMZtAQF0LwQApBj3TTY5yY1SE+BYd3ZmNg/p
IEdnf9pwSImqWZwFwLlM62qMNdd6gSvsgGSr/CT3SM8fneGYBs+CrFV5XBYziK+e
1v7/7Xo1GtmcnXoK04+leKVRLQmh9ypjXYqi43OL+BREJQhBTVebN1zB+OB1VGMF
VdtUogWL6bBH7uuFxQs=
=3v/T
-----END PGP PUBLIC KEY BLOCK-----
```

Detecting Unauthorized Access

- Detecting unauthorized access means looking for anything out of the ordinary. It means logging all messages sent and received by the network, all software used, and all logins (or attempted logins) to the network.
  - Increases in the number of logins
  - Unusual number of unsuccessful login attempts to a user's or several users' accounts.
- Regular monitoring should also be extended to network hardware.

Correcting Unauthorized Access

- Once an unauthorized access is detected, the next step is to identify how the security breach occurred and fix it so that it will not reoccur.
- Many organizations have taken their own steps to detect intruders by using entrapment techniques. (The "Honey Pot").
- Those caught breaking into systems can now face severe legal actions, as opposed to very little court action in the past!

Security Tips

- Keep the security system simple
  - Too complex comes with bugs and if it not well understood, there may be backdoors or controls that are left out
- Limit changes to configurations
  - Changes are sources of security problems
- Consider new versions carefully
  - New versions of software may also have unknown features or bugs

Password Security Tips

- Don’t use dictionary words
  - “crack” makes a brute-force attack using dictionary lookup, can find passwords in minutes
- Require regular password changes
- Require upper/lower/numbers/non-chars
- Beware of passwords on multiple sites
- Password storage must be secure

Network Management

Chapter 36

Network Monitoring

- Most large organizations (and many small ones) use network management software to monitor and control their networks.
- The parameters monitored by a network management system fall into two distinct categories:
  - physical network statistics and
  - logical network information.

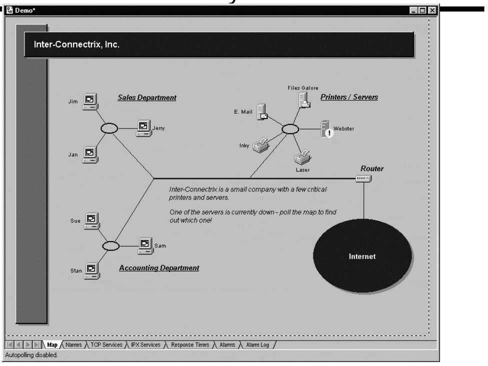
Network Monitoring

- **Physical network parameters** include monitoring the operation of the network;s modems, multiplexers, circuits linking the various hardware devices, and any other network device.
  - E.g. NIC is “Jammed”
  - Many switches can detect and report on these cases
- **Logical network parameters** include performance measurement systems that keep track of user response times, the volume of traffic on a specific circuit, the destination of data routed around various network, and any other indices showing the level of service provided by the network.

Network Management Software

- Network management software is designed to provide automated support for some or all of the network management functions.
- Three types of network management software:
  - Device management software
    - Devices run “agents”
  - System management software
    - Reports across many devices
  - Application management software
    - E.g. mail server down

Network Management: Network Instrument’s Link Analyst

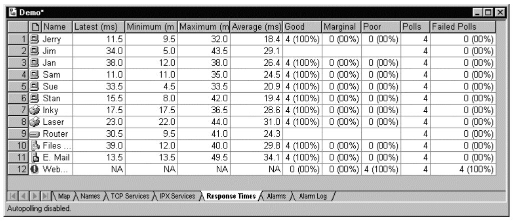


Inter-Connectrix is a small company with a few critical printers and servers.

One of the servers is currently down - poll the map to find out which one!

Autopolling disabled.

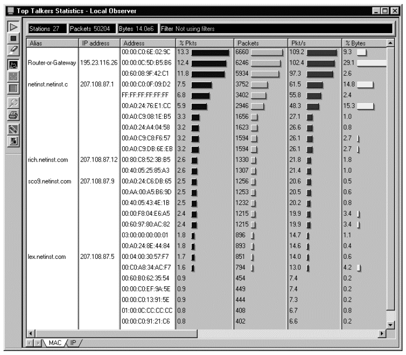
Network Management: Network Instrument’s Link Analyst



	Name	Latest (ms)	Minimum (m	Maximum (m	Average (ms)	Good	Marginal	Poor	Polls	Failed Polls
1	Jerry	11.5	9.5	32.0	18.4	4 (100%)	0 (00%)	0 (00%)	4	0 (00%)
2	Jim	34.0	5.0	43.5	29.1				4	0 (00%)
3	Jan	38.0	12.0	38.0	26.4	4 (100%)	0 (00%)	0 (00%)	4	0 (00%)
4	Sam	11.0	11.0	35.0	24.5	4 (100%)	0 (00%)	0 (00%)	4	0 (00%)
5	Sue	33.5	4.5	33.5	20.9	4 (100%)	0 (00%)	0 (00%)	4	0 (00%)
6	Stan	15.5	8.0	42.0	19.4	4 (100%)	0 (00%)	0 (00%)	4	0 (00%)
7	Inky	17.5	17.5	36.5	28.6	4 (100%)	0 (00%)	0 (00%)	4	0 (00%)
8	Laser	23.0	22.0	44.0	31.0	4 (100%)	0 (00%)	0 (00%)	4	0 (00%)
9	Router	30.5	9.5	41.0	24.3				4	0 (00%)
10	Files ...	39.0	12.0	40.0	29.8	4 (100%)	0 (00%)	0 (00%)	4	0 (00%)
11	E. Mail	13.5	13.5	49.5	34.1	4 (100%)	0 (00%)	0 (00%)	4	0 (00%)
12	Web...	NA	NA	NA	NA	0 (00%)	0 (00%)	4 (100%)	4	4 (100%)

Autopolling disabled.

Network Management: Network Instrument’s Observer

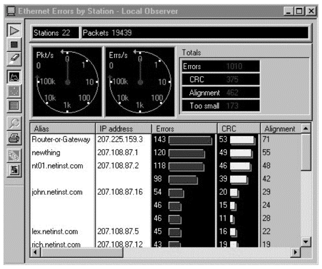


Top Talkers Statistics - Local Observer

Stations 27 | Packets 50204 | Bytes 14.0e6 | Filter Not using filters

Alias	IP address	Address	% Pkts	Packets	Pkt/s	% Bytes
		00:00:C0:6E:02:9C	13.3	6660	109.2	9.3
Router-or-Gateway	195.23.116.26	00:00:0C:5D:B5:B6	12.4	6246	102.4	29.1
		00:60:08:9F:42:C1	11.8	5934	97.3	2.6
netinst.netinst.c	207.108.87.1	00:00:C0:0F:09:D2	7.5	3752	61.5	14.8
		FF:FF:FF:FF:FF:FF	6.8	3402	55.8	2.4
		00:A0:24:76:E1:CC	5.9	2946	48.3	15.3
		00:A0:C9:08:1E:B5	3.3	1656	27.1	1.0
		00:A0:24:A4:04:58	3.2	1623	26.6	0.8
		00:A0:C9:C8:F6:57	3.2	1594	26.1	2.7
		00:A0:C9:DB:6E:EB	3.2	1594	26.1	2.7
rich.netinst.com	207.108.87.12	00:80:C8:52:3B:B5	2.6	1330	21.8	1.8
		00:40:05:25:85:A3	2.6	1307	21.4	1.0
sco9.netinst.com	207.108.87.9	00:A0:24:C6:DB:65	2.5	1256	20.6	0.5
		00:AA:00:A5:B6:9D	2.5	1253	20.5	0.6
		00:40:05:43:4E:1B	2.5	1232	20.2	0.8
		00:00:F8:04:E6:A5	2.4	1215	19.9	3.4
		00:60:97:80:AC:82	2.4	1215	19.9	3.4
		03:00:00:00:00:01	1.8	896	14.7	1.1
		00:A0:24:8E:44:84	1.8	893	14.6	0.4
lex.netinst.com	207.108.87.5	00:04:00:30:57:F7	1.7	851	14.0	0.6
		00:C0:A8:34:AC:F7	1.6	794	13.0	4.2
		00:60:B0:62:35:54	0.9	454	7.4	0.2
		00:00:C0:EF:9A:5E	0.9	449	7.4	0.2
		00:00:C0:13:91:5E	0.9	444	7.3	0.2
		01:00:0C:CC:CC:CC	0.8	408	6.7	0.8
		00:00:C0:91:21:C6	0.8	402	6.6	0.2

Network Management: Network Instrument’s Observer



Ethernet Errors by Station - Local Observer

Stations 22 | Packets 19439

Totals

Errors	1010
CRC	375
Alignment	462
Too small	173

Alias	IP address	Errors	CRC	Alignment
Router-or-Gateway	207.225.159.3	143	53	71
newthing	207.108.87.1	120	49	55
nt01.netinst.com	207.108.87.2	118	46	48
		98	39	42
john.netinst.com	207.108.87.16	54	20	29
		46	15	24
		46	11	28
lex.netinst.com	207.108.87.5	45	16	22
rich.netinst.com	207.108.87.12	43	19	19

Network Management Standards

⌘ One major problem is ensuring that hardware devices from different vendors can understand and respond to the messages sent by the network management software of other vendors.

⌘ The two most commonly used network management protocols are:

- Simple Network Management Protocol (SNMP)
  - ☒MIB - Management Information Base
  - ☒Network management station can access MIBs, send control messages to devices to report on their MIB
  - ☒Problem: Many vendors have their own proprietary entensions to SMTMP
- Common Management Interface Protocol (CMIP)
  - ☒More functionality than SNMP, but not compatible