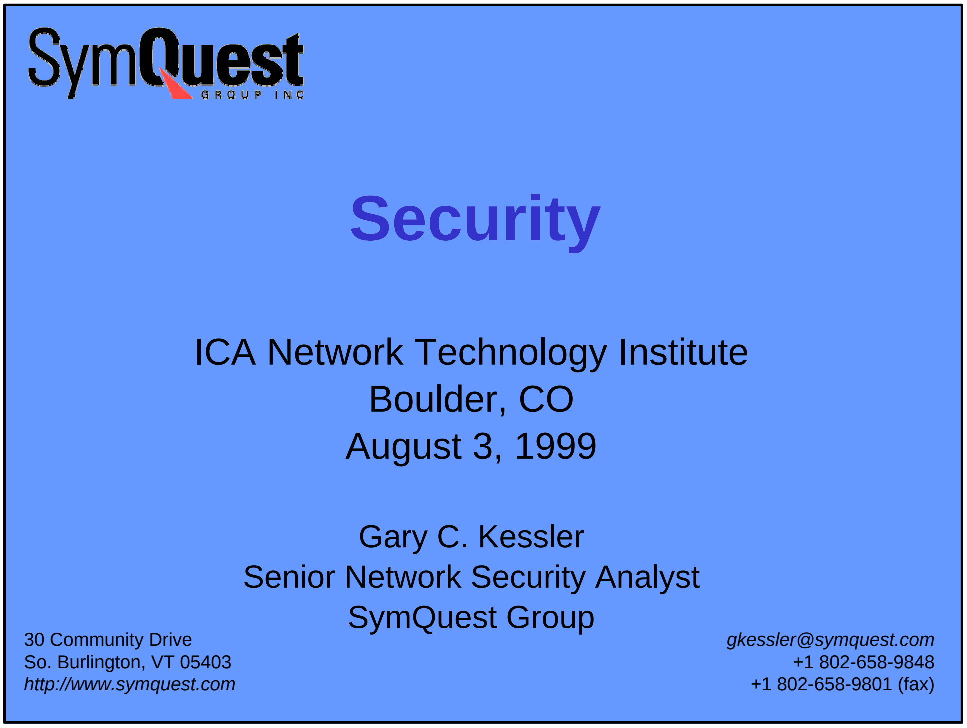


SymQuest GROUP INC

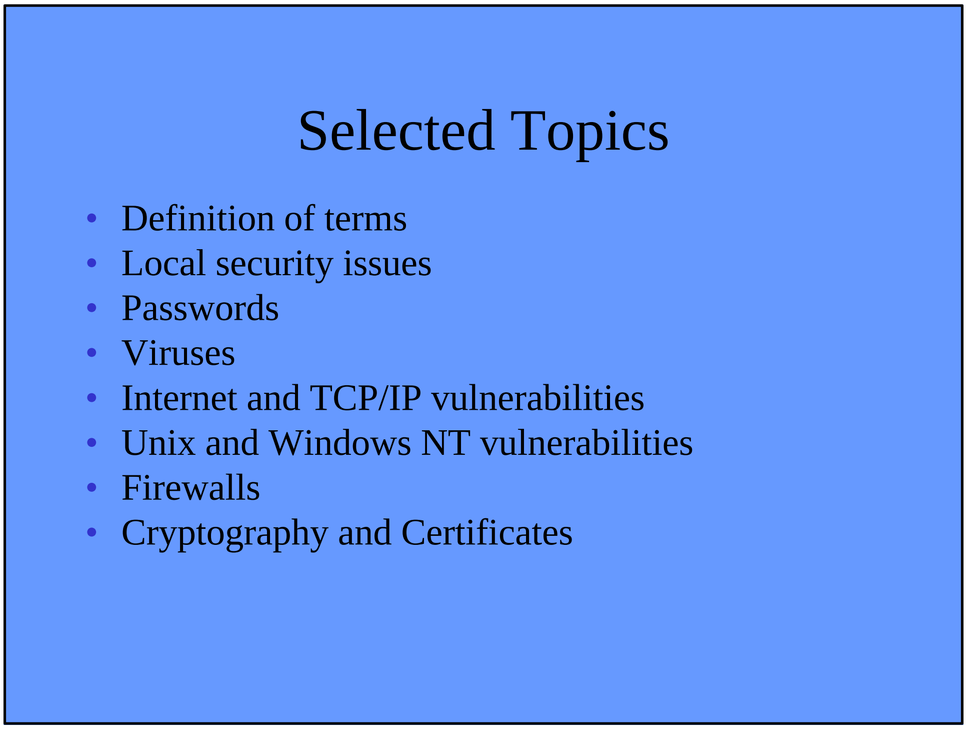
Security

ICA Network Technology Institute
Boulder, CO
August 3, 1999

Gary C. Kessler
Senior Network Security Analyst
SymQuest Group

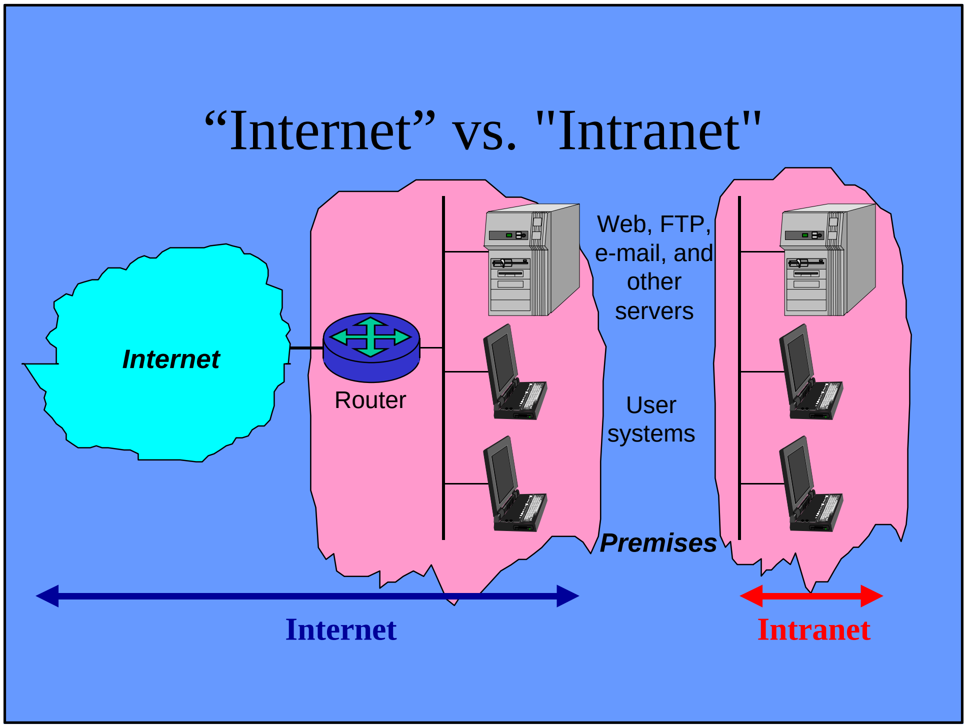
30 Community Drive
So. Burlington, VT 05403
http://www.symquest.com

gkessler@symquest.com
+1 802-658-9848
+1 802-658-9801 (fax)



Selected Topics

- Definition of terms
- Local security issues
- Passwords
- Viruses
- Internet and TCP/IP vulnerabilities
- Unix and Windows NT vulnerabilities
- Firewalls
- Cryptography and Certificates



“Internet” vs. "Intranet"

Internet

Router

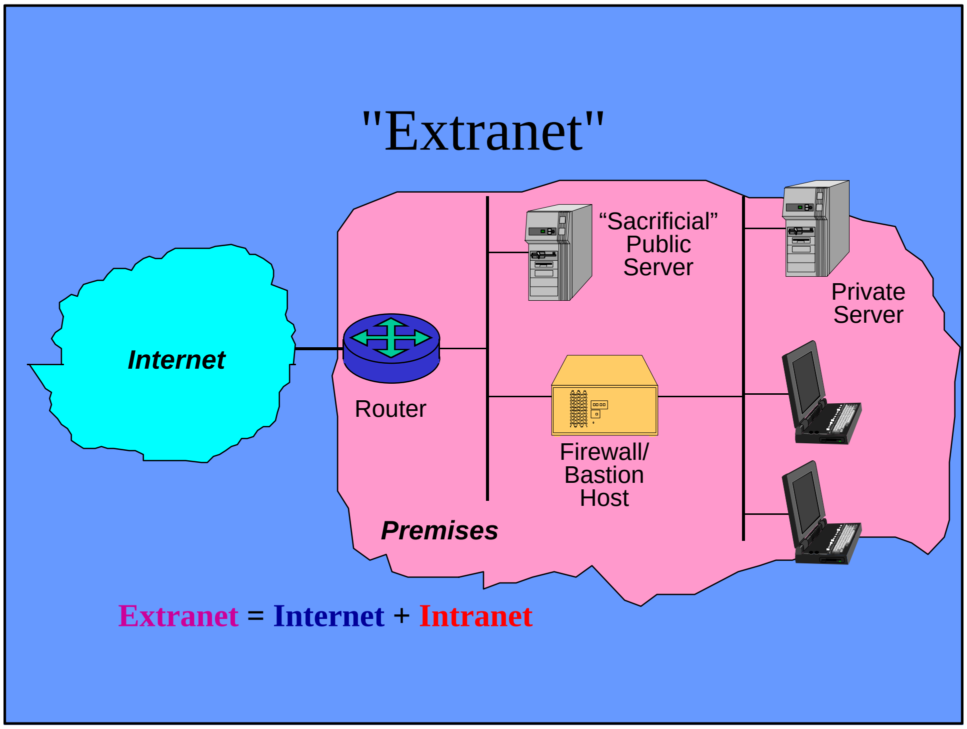
Web, FTP, e-mail, and other servers

User systems

Premises

Internet

Intranet



"Extranet"

Internet

Router

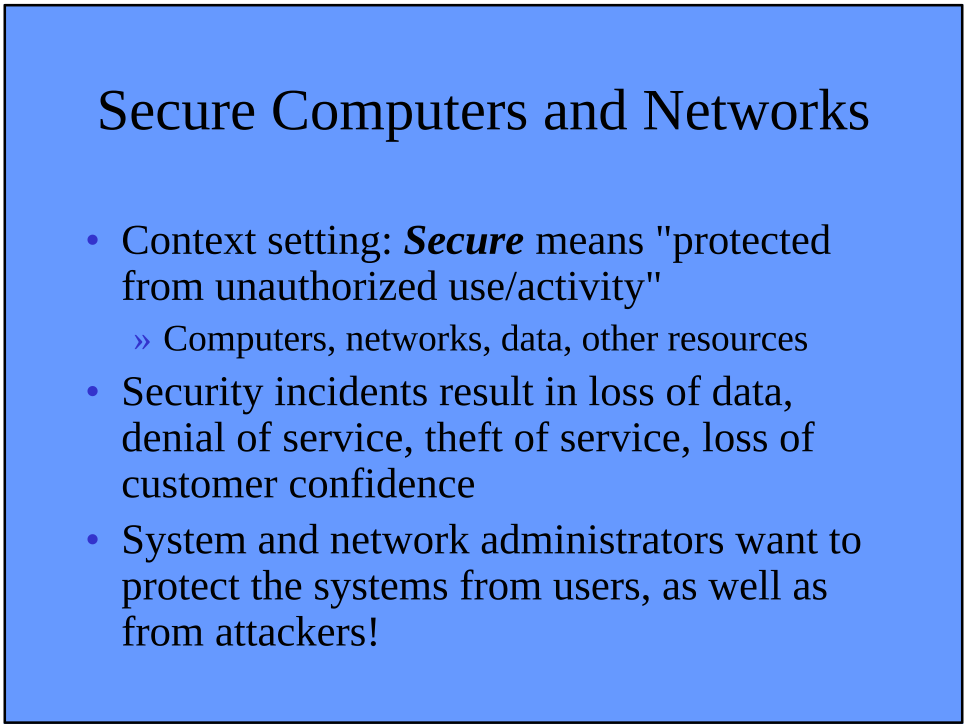
“Sacrificial” Public Server

Firewall/ Bastion Host

Private Server

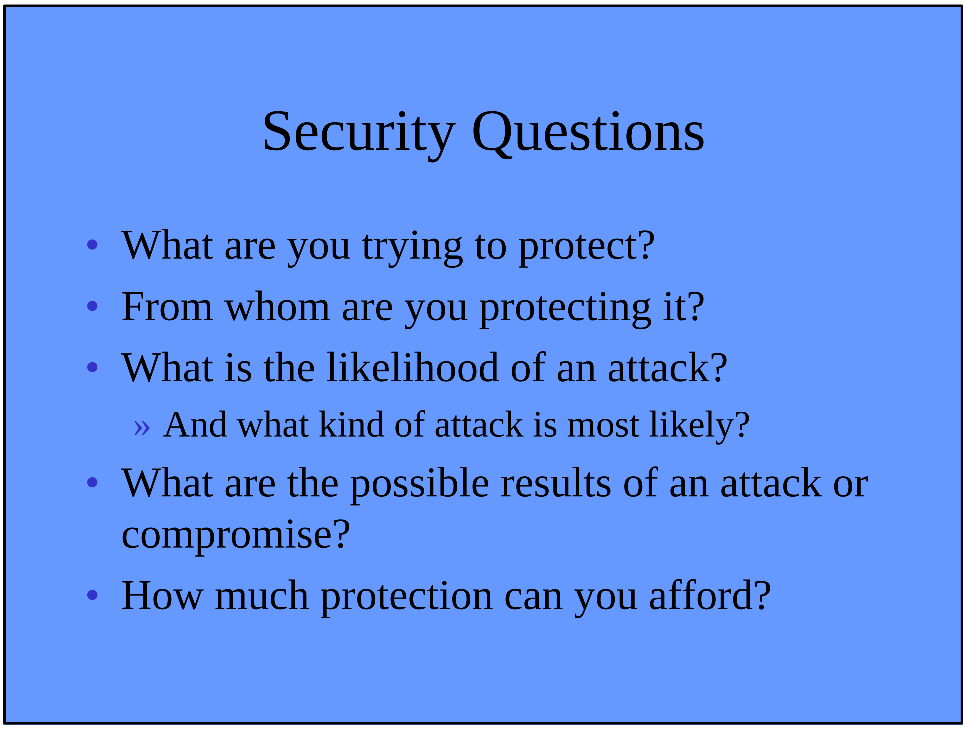
Premises

Extranet = Internet + Intranet



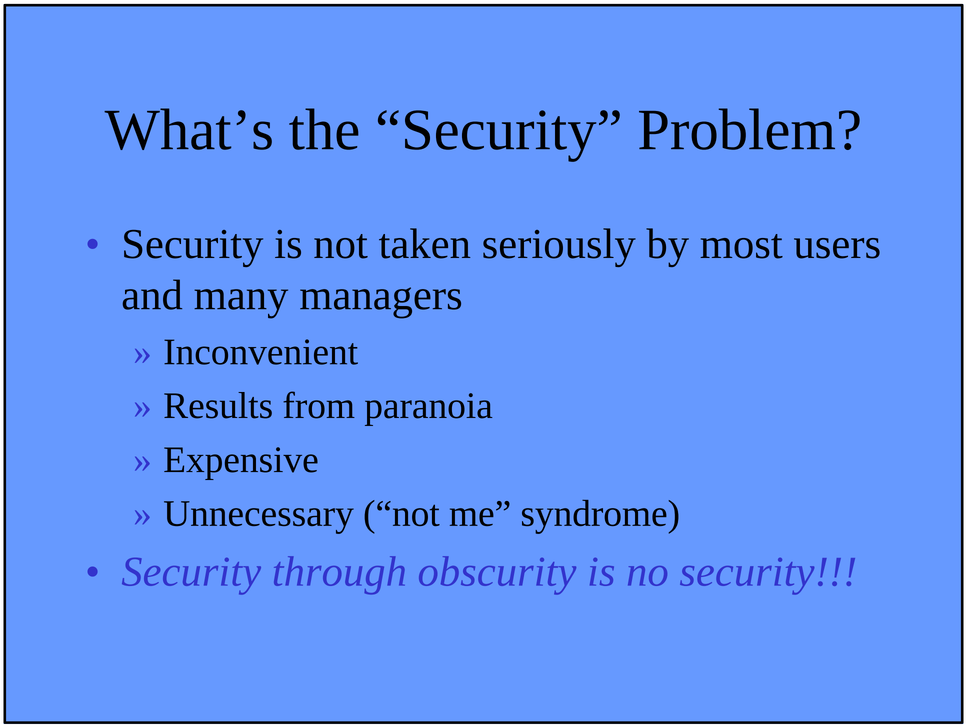
Secure Computers and Networks

- Context setting: ***Secure*** means "protected from unauthorized use/activity"
  - » Computers, networks, data, other resources
- Security incidents result in loss of data, denial of service, theft of service, loss of customer confidence
- System and network administrators want to protect the systems from users, as well as from attackers!



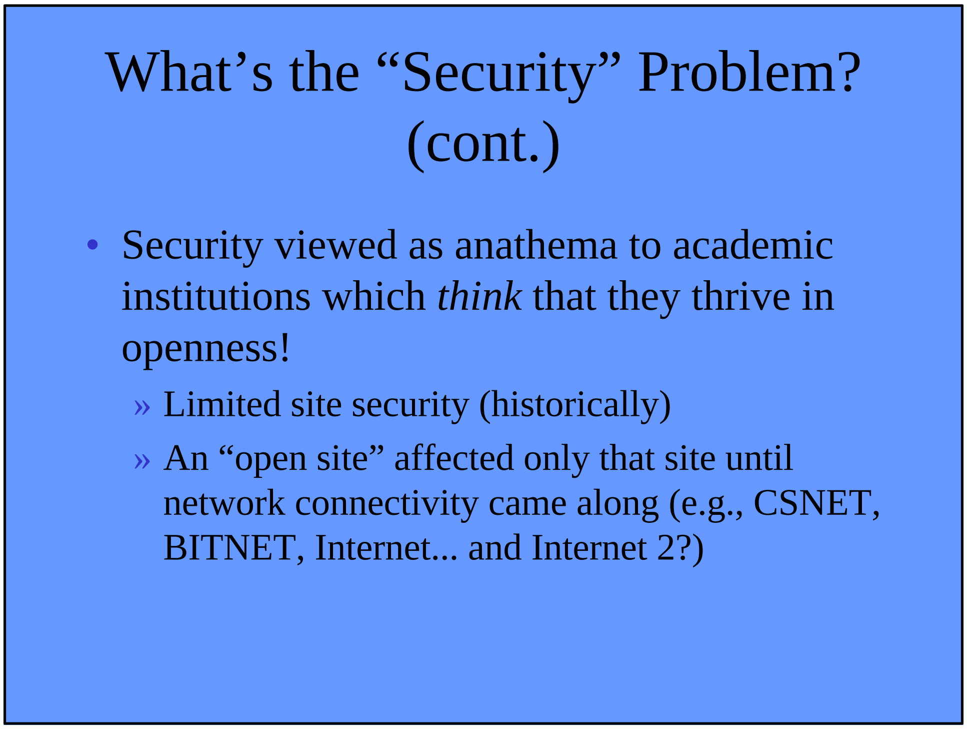
Security Questions

- What are you trying to protect?
- From whom are you protecting it?
- What is the likelihood of an attack?
  - » And what kind of attack is most likely?
- What are the possible results of an attack or compromise?
- How much protection can you afford?



What’s the “Security” Problem?

- Security is not taken seriously by most users and many managers
  - » Inconvenient
  - » Results from paranoia
  - » Expensive
  - » Unnecessary (“not me” syndrome)
- *Security through obscurity is no security!!!*



What’s the “Security” Problem? (cont.)

- Security viewed as anathema to academic institutions which *think* that they thrive in openness!
  - » Limited site security (historically)
  - » An “open site” affected only that site until network connectivity came along (e.g., CSNET, BITNET, Internet... and Internet 2?)

How Big Is The Problem?

- No one knows!!!
  - In the U.S., ~10% of computer crimes are reported; < 2% result in convictions; ~10 people have gone to jail
  - Computer crime costs $1-2B (FBI), $5B (E&Y), or $40B (SEARCH) annually
  - Laptop thefts are on the rise; >300K in 1997

Measuring Risk

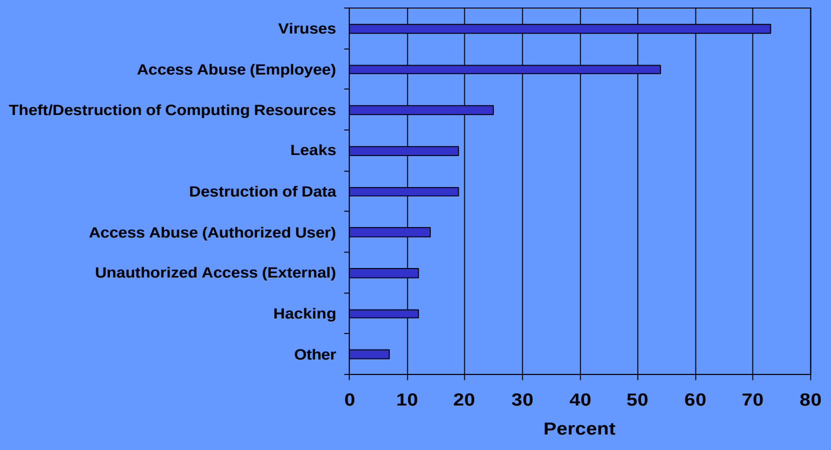
$$R = A \bullet V \bullet T$$

- R: Risk
- A: Asset value
- V: Vulnerability
- T: Threat likelihood

Case Study: DoD Vulnerability

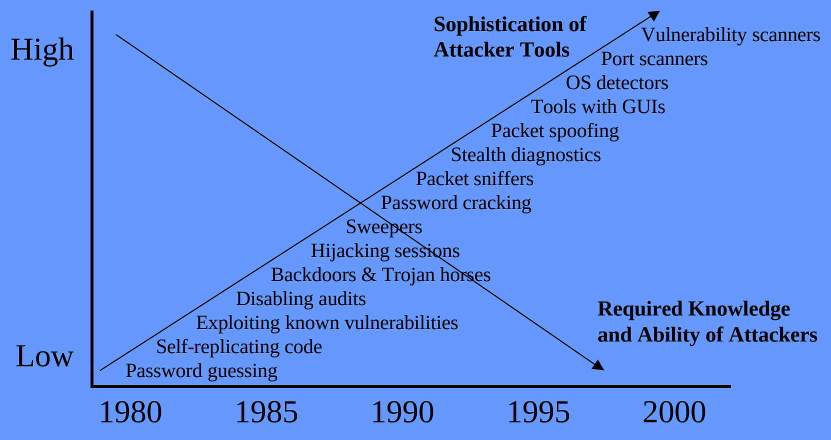
- 1996 General Accounting Office report of 38,000 Defense Information System Agency "attacks" on DoD computers (1992-1995)
  - » 35% were blocked with existing configuration
  - » 62% were successful and undetected
  - » 2% were successful and detected, yet unreported
  - » 1% were successful, detected, and reported

Types of Security Breaches



Source: ICSA, 1998

...And a Proliferation of Tools



Sophistication of Attacker Tools

Vulnerability scanners
Port scanners
OS detectors
Tools with GUIs
Packet spoofing
Stealth diagnostics
Packet sniffers
Password cracking
Sweepers
Hijacking sessions
Backdoors & Trojan horses
Disabling audits
Exploiting known vulnerabilities
Self-replicating code
Password guessing

Required Knowledge and Ability of Attackers

Source: Adapted from GAO, 1996

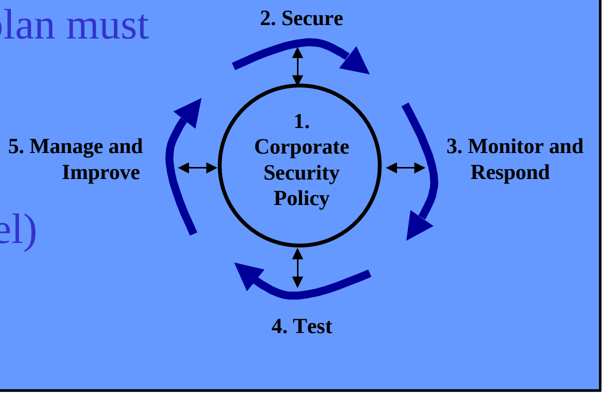
Security and Internet Commerce

- An e-commerce site on the Internet **must** implement adequate security
  - » Protecting your customer's data is roughly as important as protecting your own reputation and maintaining customer confidence
- Customers at your site should be informed about both your security concerns and your security measures

Commerce Over the Internet?

...And A Recurring Theme

- A site's security plan must integrate many aspects of operations and policy
- The security plan must evolve as the organization evolves (the Security Wheel)



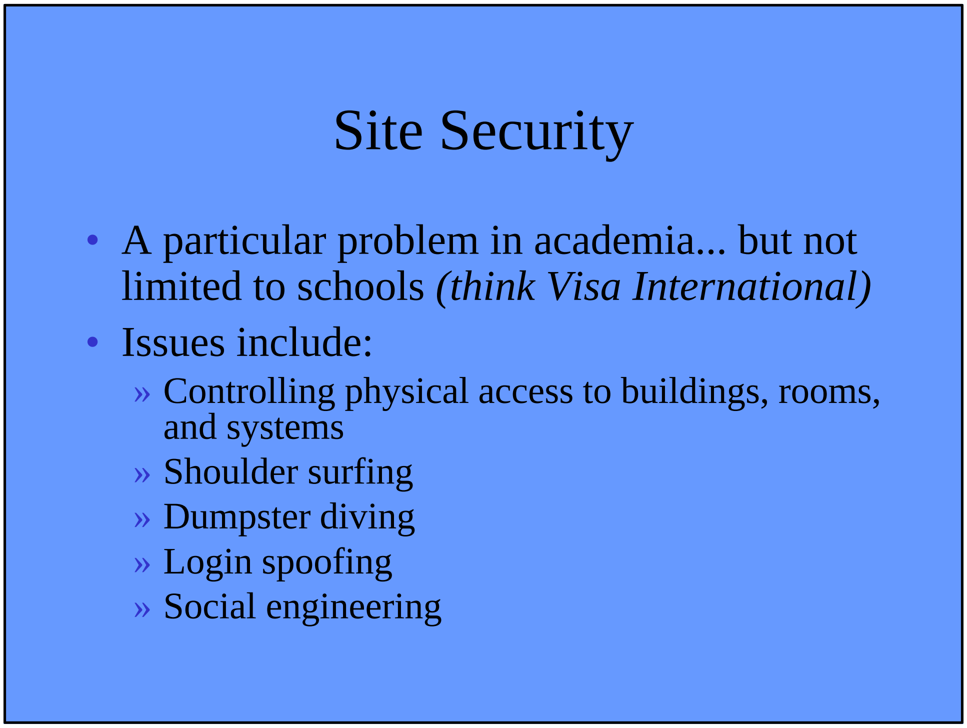
2. Secure

1. Corporate Security Policy

3. Monitor and Respond

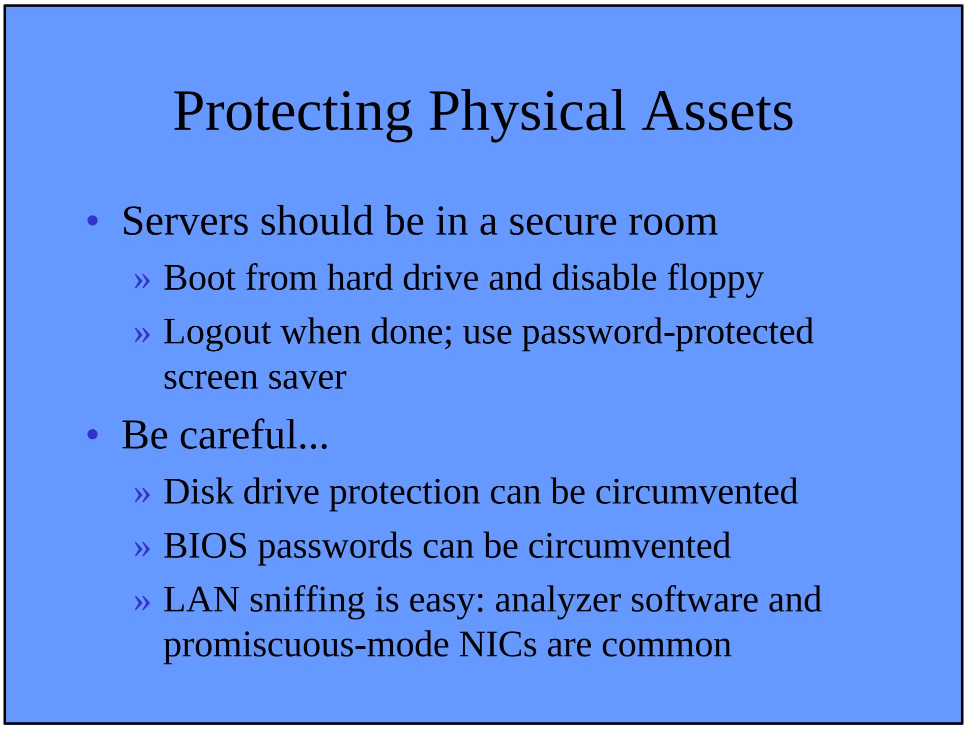
4. Test

5. Manage and Improve



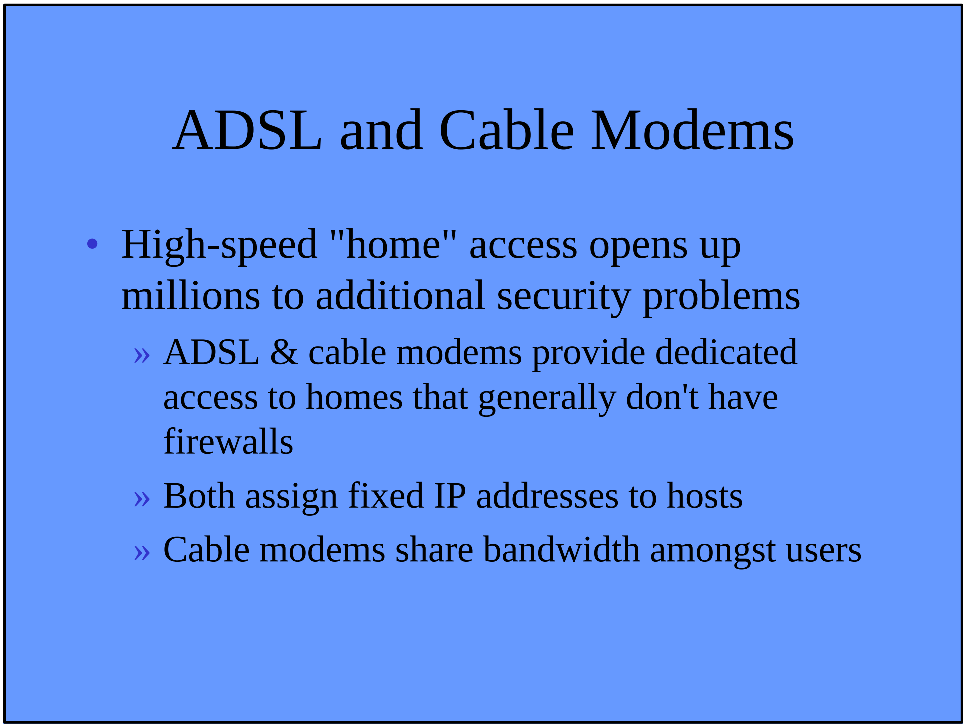
Site Security

- A particular problem in academia... but not limited to schools *(think Visa International)*
- Issues include:
  - » Controlling physical access to buildings, rooms, and systems
  - » Shoulder surfing
  - » Dumpster diving
  - » Login spoofing
  - » Social engineering



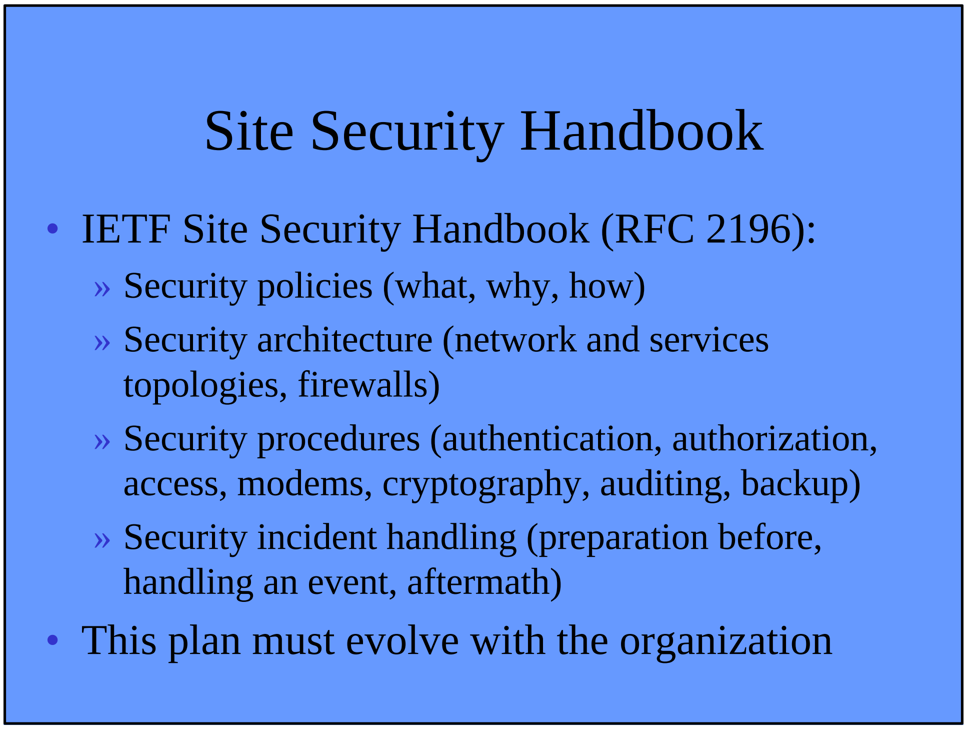
Protecting Physical Assets

- Servers should be in a secure room
  - » Boot from hard drive and disable floppy
  - » Logout when done; use password-protected screen saver
- Be careful...
  - » Disk drive protection can be circumvented
  - » BIOS passwords can be circumvented
  - » LAN sniffing is easy: analyzer software and promiscuous-mode NICs are common



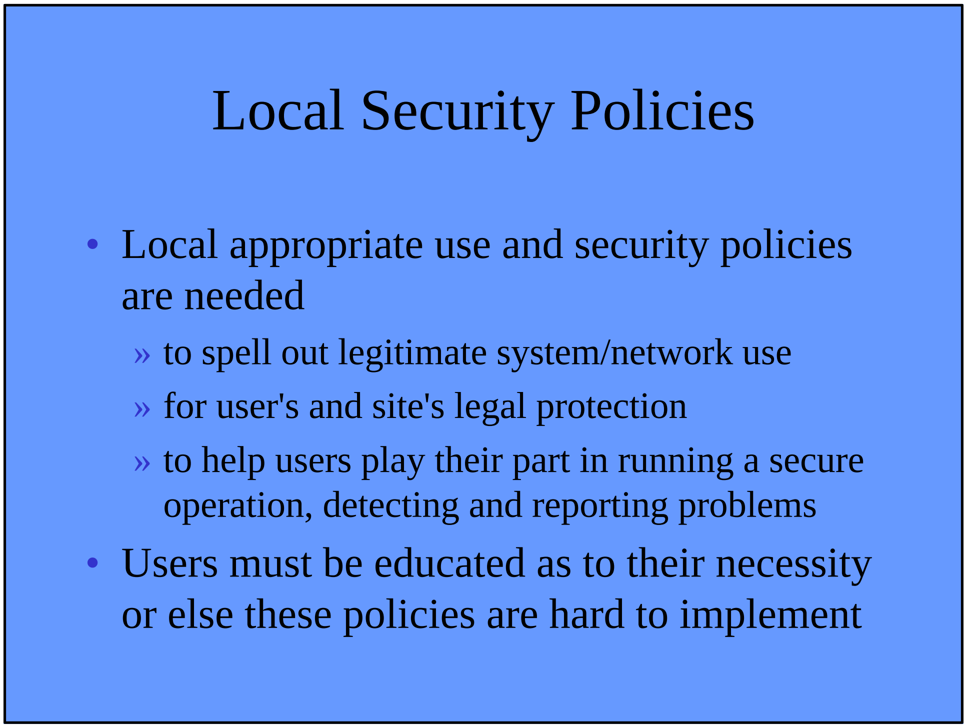
ADSL and Cable Modems

- High-speed "home" access opens up millions to additional security problems
  - » ADSL & cable modems provide dedicated access to homes that generally don't have firewalls
  - » Both assign fixed IP addresses to hosts
  - » Cable modems share bandwidth amongst users



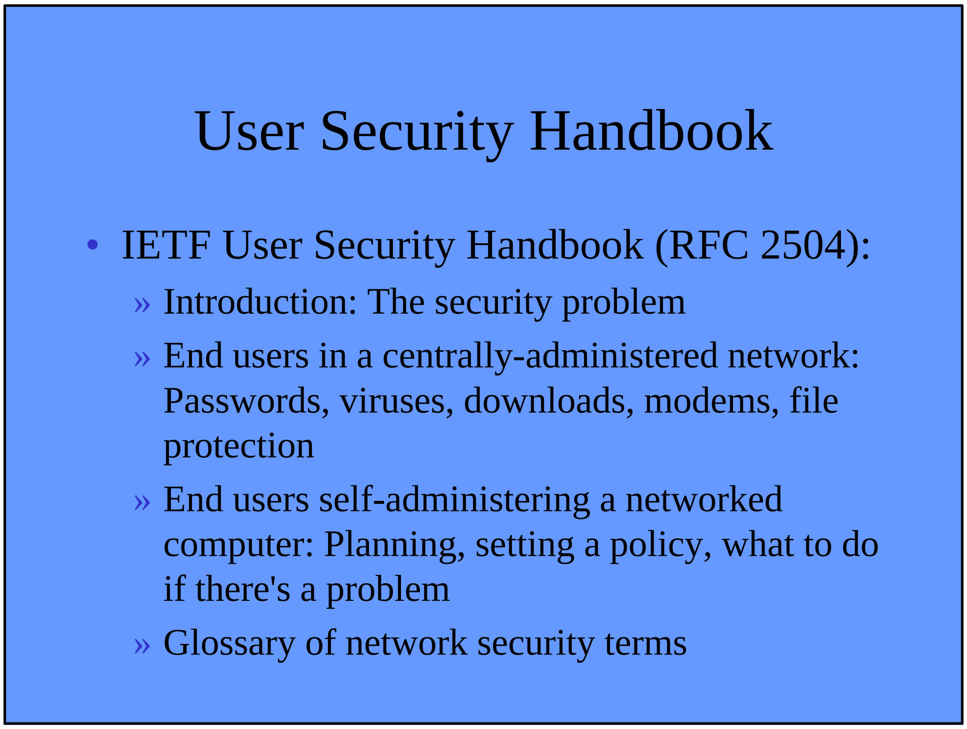
Site Security Handbook

- IETF Site Security Handbook (RFC 2196):
  - » Security policies (what, why, how)
  - » Security architecture (network and services topologies, firewalls)
  - » Security procedures (authentication, authorization, access, modems, cryptography, auditing, backup)
  - » Security incident handling (preparation before, handling an event, aftermath)
- This plan must evolve with the organization



Local Security Policies

- Local appropriate use and security policies are needed
  - » to spell out legitimate system/network use
  - » for user's and site's legal protection
  - » to help users play their part in running a secure operation, detecting and reporting problems
- Users must be educated as to their necessity or else these policies are hard to implement



User Security Handbook

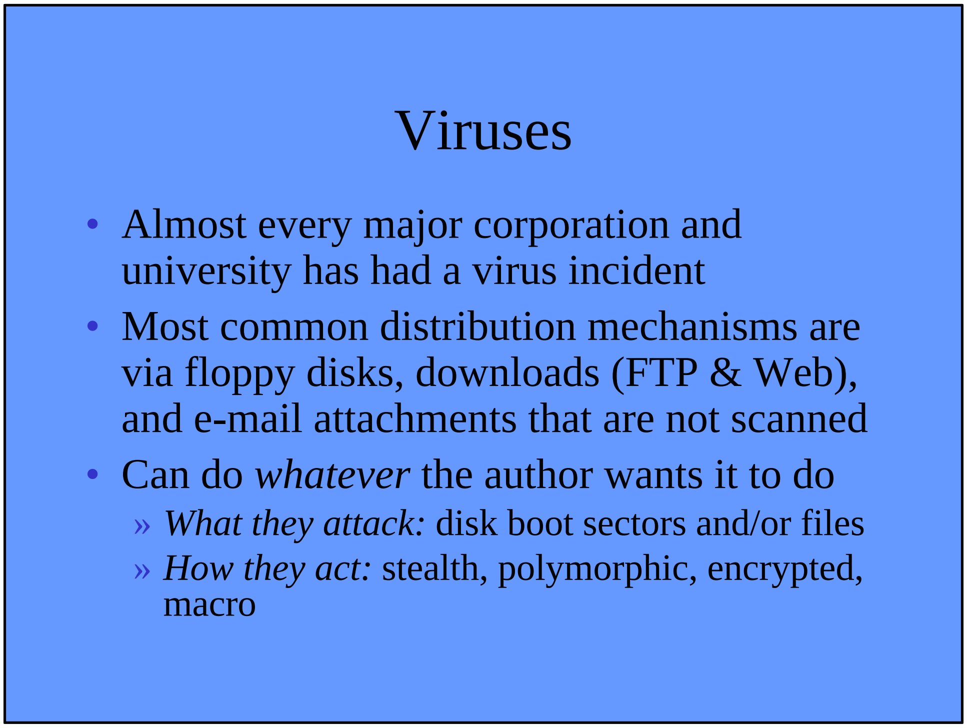
- IETF User Security Handbook (RFC 2504):
  - » Introduction: The security problem
  - » End users in a centrally-administered network: Passwords, viruses, downloads, modems, file protection
  - » End users self-administering a networked computer: Planning, setting a policy, what to do if there's a problem
  - » Glossary of network security terms

Passwords

- Most convenient (and common) form of protection
  - » What you know vs. what you have/are
- Weakest form of protection because people choose bad passwords
  - » Names, numbers, hobbies, username, ...
  - » ...and you only need a few bad ones to open your entire system

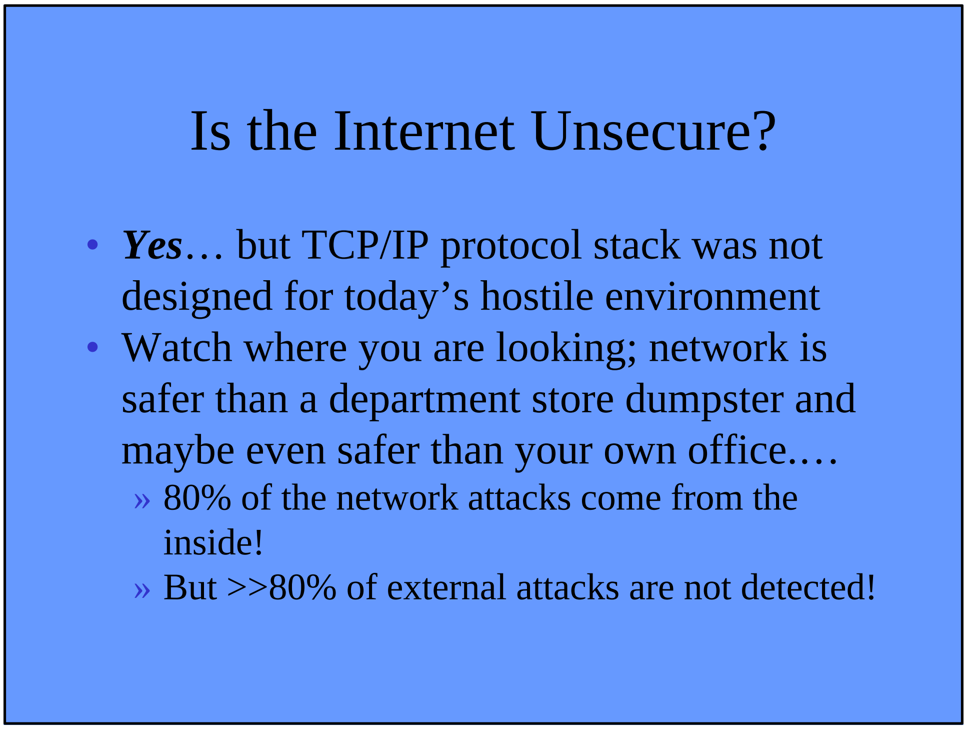
Alternatives to Passwords

- Passwords are "what you know"
- Alternatives include
  - » "What you have"
    - Tokens
    - One-time Passwords
  - » "What you are"
    - Click rate
    - Biometrics: Retina scan, fingerprints, voice prints



Viruses

- Almost every major corporation and university has had a virus incident
- Most common distribution mechanisms are via floppy disks, downloads (FTP & Web), and e-mail attachments that are not scanned
- Can do *whatever* the author wants it to do
  - » *What they attack:* disk boot sectors and/or files
  - » *How they act:* stealth, polymorphic, encrypted, macro



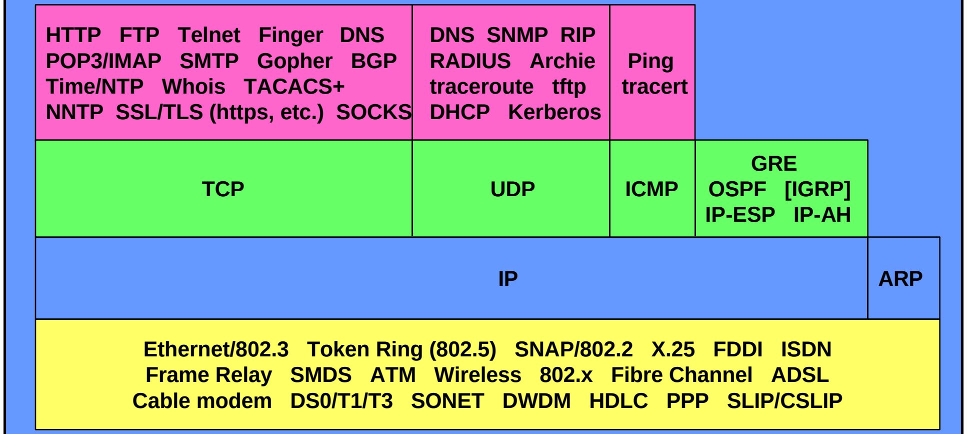
Is the Internet Unsecure?

- ***Yes***… but TCP/IP protocol stack was not designed for today's hostile environment
- Watch where you are looking; network is safer than a department store dumpster and maybe even safer than your own office.…
  - » 80% of the network attacks come from the inside!
  - » But >>80% of external attacks are not detected!

Is the Internet Unsecure? (cont.)

- Philosophy of "experts" differ:
  - » Nefarious people are everywhere! Never send critical data in e-mail or forms
  - » Hackers would prefer to break into a system and steal 20,000 credit cards rather than work so hard to find your credit card
- This might be a good time to read *2600 Magazine* or *Phrack...*

TCP/IP (v4) Protocol Suite



HTTP FTP Telnet Finger DNS POP3/IMAP SMTP Gopher BGP Time/NTP Whois TACACS+ NNTP SSL/TLS (https, etc.) SOCKS	DNS SNMP RIP RADIUS Archie traceroute tftp DHCP Kerberos	Ping tracert		
TCP	UDP	ICMP	GRE OSPF [IGRP] IP-ESP IP-AH	
IP				ARP
Ethernet/802.3 Token Ring (802.5) SNAP/802.2 X.25 FDDI ISDN Frame Relay SMDS ATM Wireless 802.x Fibre Channel ADSL Cable modem DS0/T1/T3 SONET DWDM HDLC PPP SLIP/CSLIP				

TCP/IP Protocol Insecurity

- TCP/IP (1981) was designed for open communications and is *not* inherently secure
- Many security holes in TCP/IP have been used as the basis for well-known attacks:
  - » Sendmail (debug mode), finger (buffer overflow): *Internet worm (11/88)*
  - » IP address spoofing, TCP ISN guessing: *Mitnick vs. SDSC (12/94)*
  - » TCP SYN denial-of-service attacks: *Panix (9/96)*

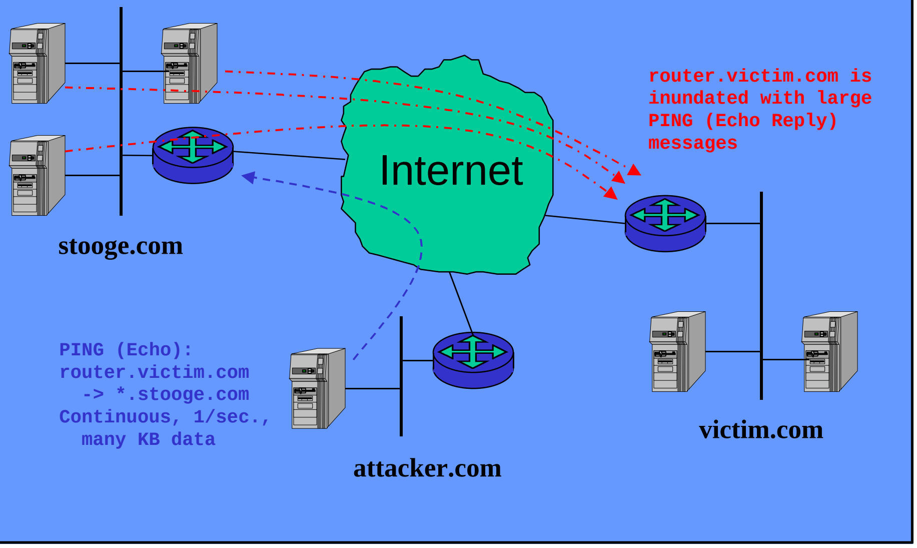
TCP/IP Protocol Vulnerabilities

- IP
  - » Source routing attack, address spoofing
- ICMP
  - » ICMP bombing (*Destination Unreachable, Redirect*), "PING Of Death"
- TCP
  - » TCP splicing, ISN guessing, small packet attack, SYN attack
- UDP
  - » Connectionless; easy to attack

TCP/IP Application Vulnerabilities

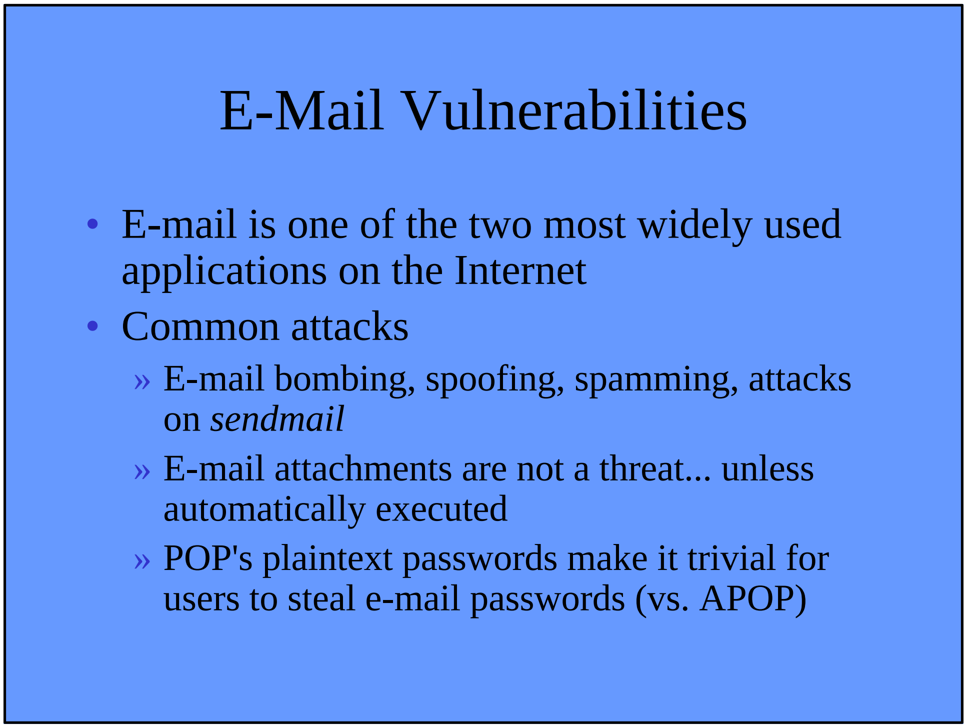
- Bad information can be fed to RIP, OSPF, DHCP, and DNS databases
- FTP: bouncing, caching (must be careful with upload sites), anonymous FTP
- E-mail: spoofing, bombing, spamming, MIME (auto-execution is *bad*)
- The Web: browsers, Java, push technology, CGI, cookies, file transfers circumvent firewall/virus scanners, secret software from Croatia, ...
- Passwords sent in the clear: Telnet, POP, FTP, ...

SMURF DoS Attack



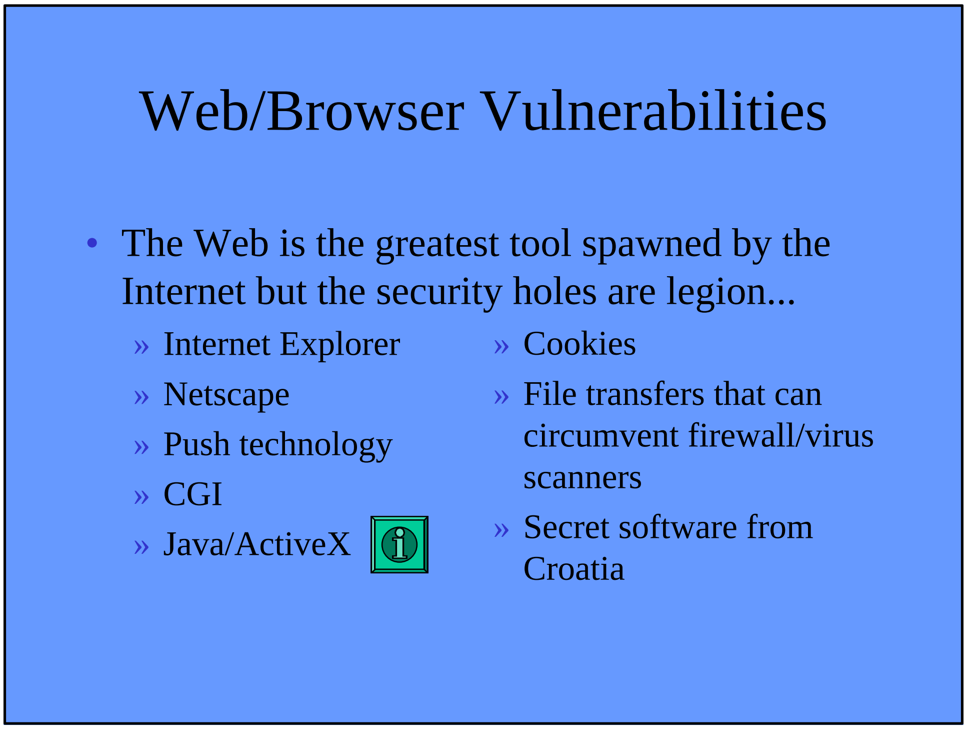
router.victim.com is inundated with large PING (Echo Reply) messages

PING (Echo):
router.victim.com
-> *.stooge.com
Continuous, 1/sec.,
many KB data



E-Mail Vulnerabilities

- E-mail is one of the two most widely used applications on the Internet
- Common attacks
  - » E-mail bombing, spoofing, spamming, attacks on *sendmail*
  - » E-mail attachments are not a threat... unless automatically executed
  - » POP's plaintext passwords make it trivial for users to steal e-mail passwords (vs. APOP)



Web/Browser Vulnerabilities

- The Web is the greatest tool spawned by the Internet but the security holes are legion...
  - » Internet Explorer
  - » Netscape
  - » Push technology
  - » CGI
  - » Java/ActiveX
  - » Cookies
  - » File transfers that can circumvent firewall/virus scanners
  - » Secret software from Croatia

Cookies and IE5

- If you have disabled cookies, the IE5 install re-enables them
  - » You must re-disable
- IE5 install sets *www.msn.com* as default start page, which immediately sets a cookie
  - » Any site with an existing cookie on your system is allowed to silently reset its cookie even if you have asked to be prompted

UNIX Overview

- Created at AT&T Bell Labs in 1969 (PDP-1)
  - » Command line interface, hardware-independent
- Resurgence in 1984; BSD4.2 UNIX bundles in TCP/IP
  - » Only Internet server OS through early 1990s
  - » X-Windows interface becomes available
  - » Multiple flavors of UNIX become available
- Resurgence in 1998; Linux
  - » Competition today from Windows NT

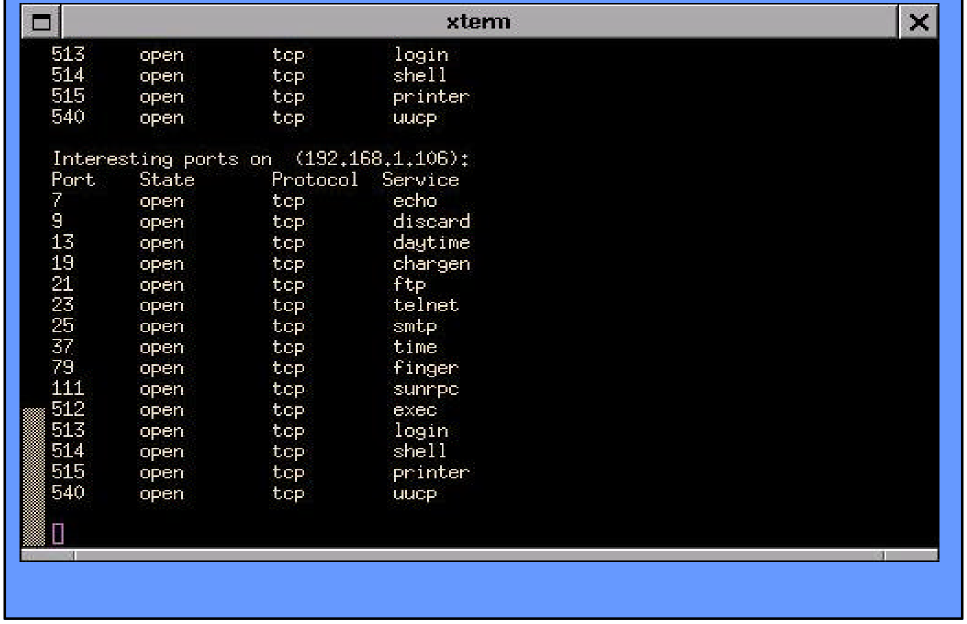
Some UNIX Weaknesses

- Reputation for being unsecure because there are many versions and no unified security mechanisms
  - » ACLs protect file/directory access
  - » Two privilege levels: user and superuser (root)
  - » *setuid* allows user to spoof another user
  - » Many programs don't check input buffer
  - » Almost every common UNIX daemon has a reported security vulnerability

Unix Security Tools (or Weapons)

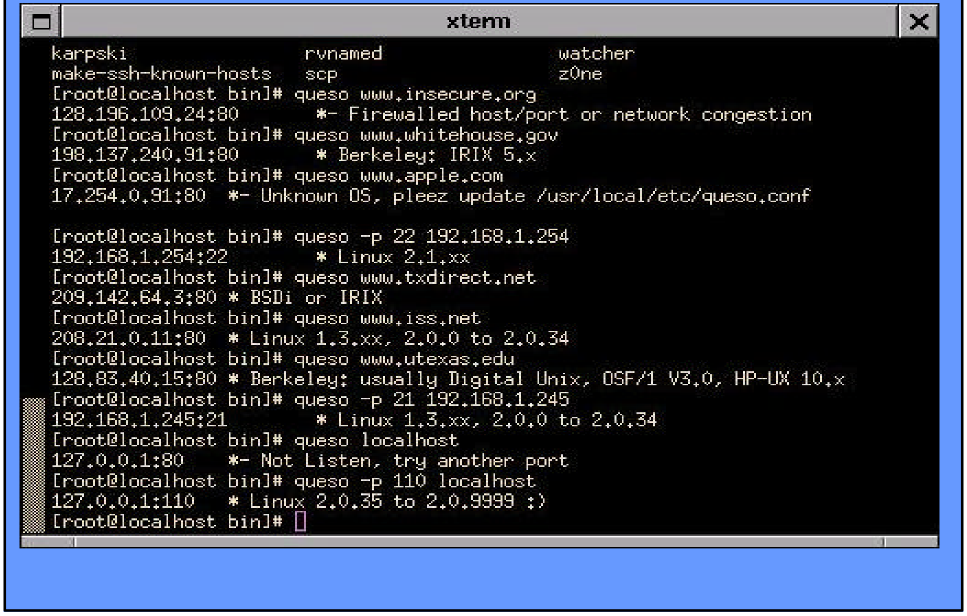
- SATAN -- Vulnerability scanner
- tcpdump, IPgrab, sniffit -- displays network traffic
- queso -- displays host operating system
- nmap -- port scanner (can specify range of hosts), operating system detector
- tcp_scan -- displays version of services
- Rdns -- PING a range of IP addresses

nmap

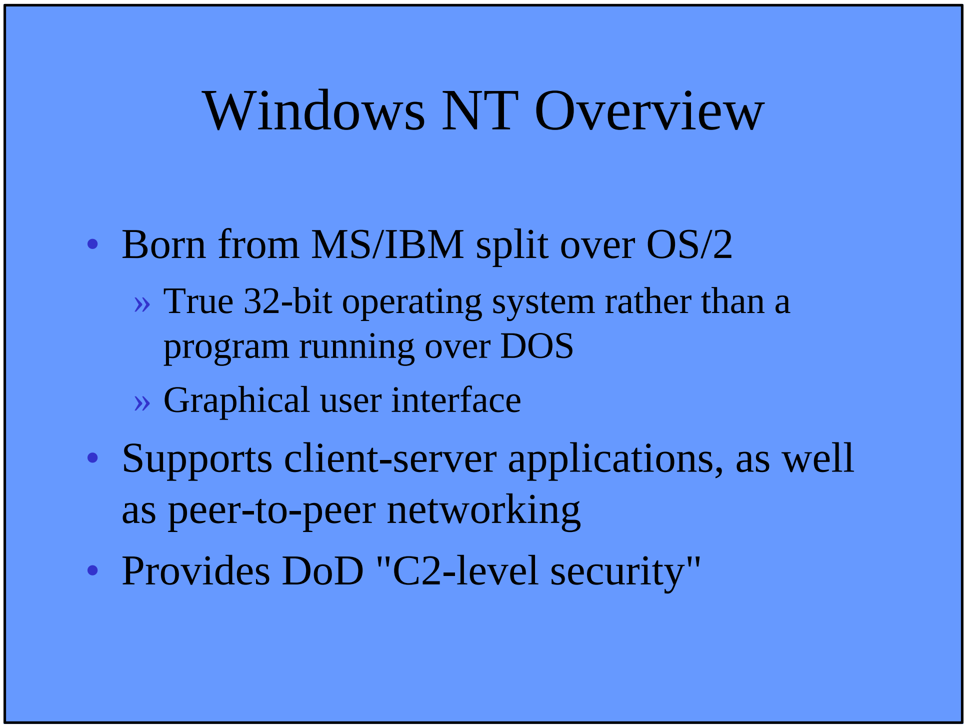


```
513     open        tcp        login
514     open        tcp        shell
515     open        tcp        printer
540     open        tcp        uucp

Interesting ports on  (192.168.1.106):
Port    State       Protocol  Service
7       open        tcp        echo
9       open        tcp        discard
13      open        tcp        daytime
19      open        tcp        chargen
21      open        tcp        ftp
23      open        tcp        telnet
25      open        tcp        smtp
37      open        tcp        time
79      open        tcp        finger
111     open        tcp        sunrpc
512     open        tcp        exec
513     open        tcp        login
514     open        tcp        shell
515     open        tcp        printer
540     open        tcp        uucp
```

queso

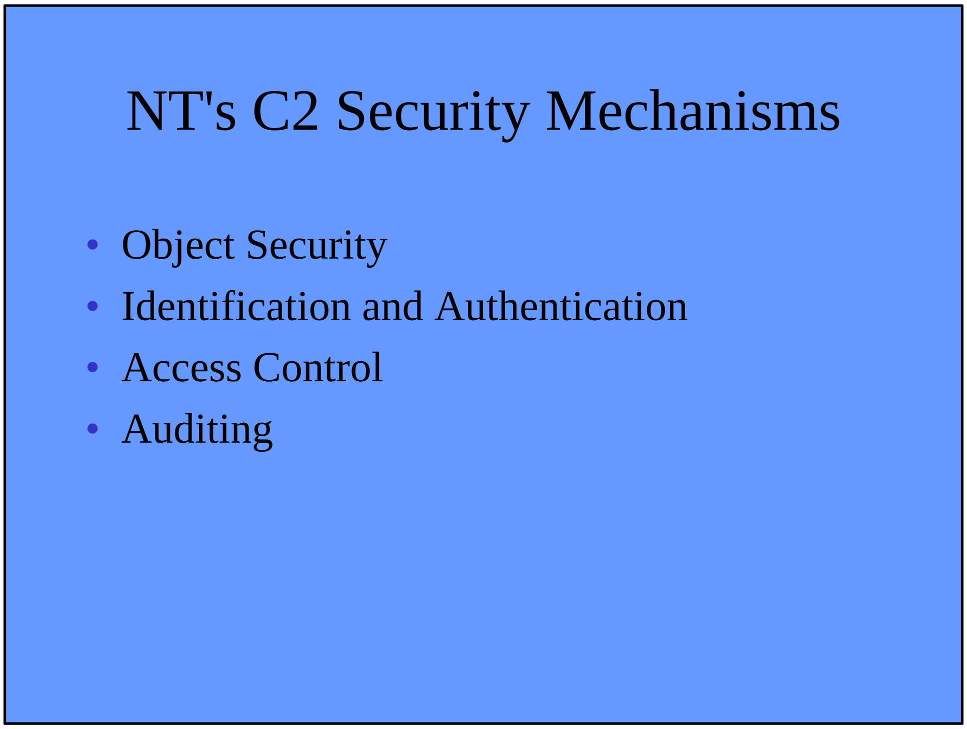


```
karpski                rvnamed                watcher
make-ssh-known-hosts   scp                    z0ne
[root@localhost bin]# queso www.insecure.org
128.196.109.24:80       *- Firewalled host/port or network congestion
[root@localhost bin]# queso www.whitehouse.gov
198.137.240.91:80       * Berkeley: IRIX 5.x
[root@localhost bin]# queso www.apple.com
17.254.0.91:80  *- Unknown OS, pleez update /usr/local/etc/queso.conf

[root@localhost bin]# queso -p 22 192.168.1.254
192.168.1.254:22        * Linux 2.1.xx
[root@localhost bin]# queso www.txdirect.net
209.142.64.3:80 * BSDi or IRIX
[root@localhost bin]# queso www.iss.net
208.21.0.11:80  * Linux 1.3.xx, 2.0.0 to 2.0.34
[root@localhost bin]# queso www.utexas.edu
128.83.40.15:80 * Berkeley: usually Digital Unix, OSF/1 V3.0, HP-UX 10.x
[root@localhost bin]# queso -p 21 192.168.1.245
192.168.1.245:21        * Linux 1.3.xx, 2.0.0 to 2.0.34
[root@localhost bin]# queso localhost
127.0.0.1:80    *- Not Listen, try another port
[root@localhost bin]# queso -p 110 localhost
127.0.0.1:110   * Linux 2.0.35 to 2.0.9999 :)
[root@localhost bin]#
```



Windows NT Overview

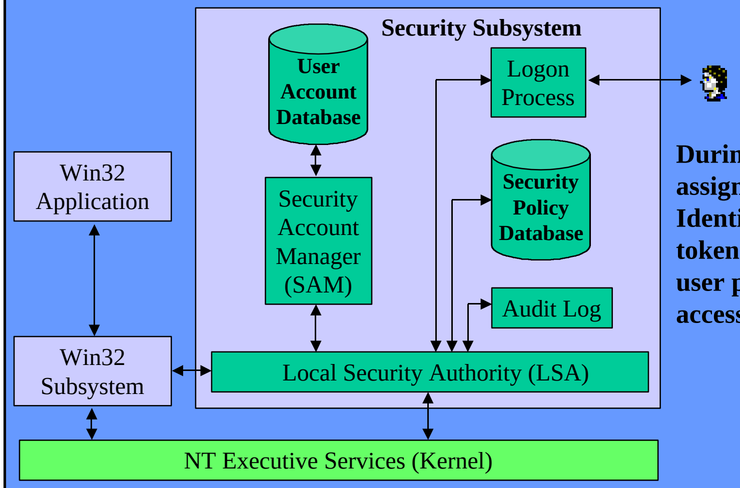
- Born from MS/IBM split over OS/2
  - True 32-bit operating system rather than a program running over DOS
  - Graphical user interface
- Supports client-server applications, as well as peer-to-peer networking
- Provides DoD "C2-level security"



NT's C2 Security Mechanisms

- Object Security
- Identification and Authentication
- Access Control
- Auditing

Windows NT Security Architecture



During logon, LSA assigns user a Security Identifier (SID), a token that describes user permissions, access rights, etc.

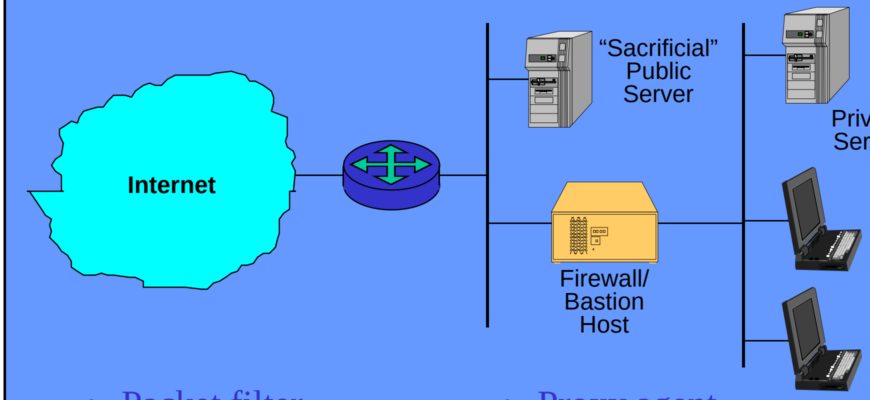
Windows NT Security Tools

- Port scanner (UltraScan, nmap)
- Event log analyzer (DumpEvt, DUMPEL)
- Registry analyzer (DumpReg, RegMon)
- ACL analyzer (DumpACL)
- Vulnerability tester (CyberCop, Internet Scanner, WebTrends Security Analyzer)
- Intrusion detector (NetProwler, RealSecure, Session Wall-3, Tripwire)

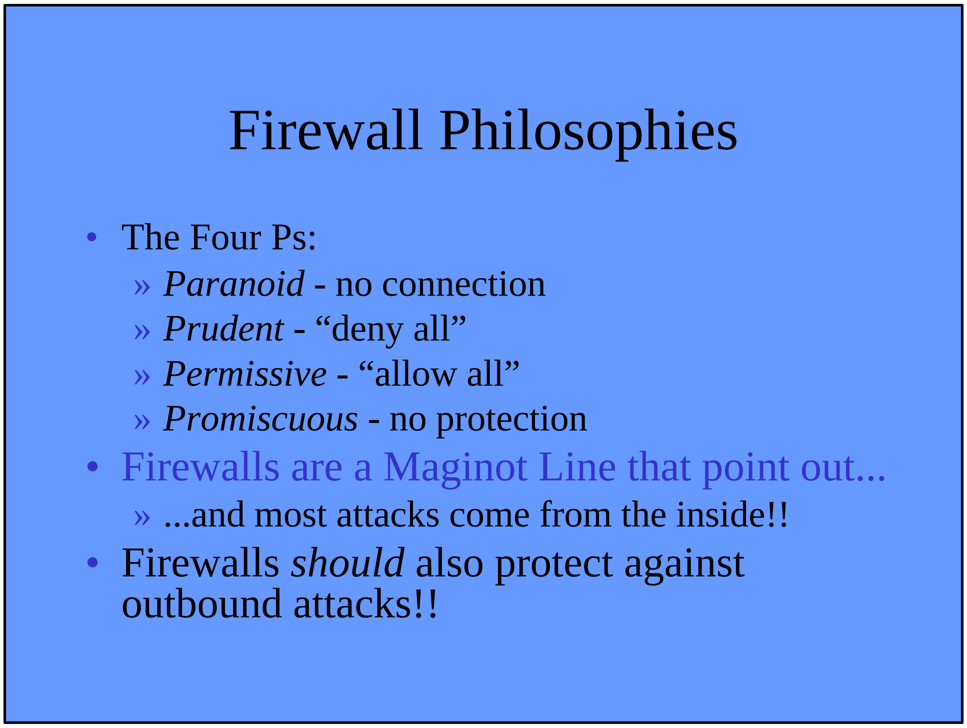
Back Orifice/Back Orifice 2000

- Released by Cult of the Dead Cow (cDc)
- Ostensibly an administrator's tool to test vulnerabilities in Windows NT
- Actually a Trojan horse program that opens access to your system
- BO2k differs from SATAN...
  - » Dan Farmer rejects hacking; cDc does not!

Firewalls

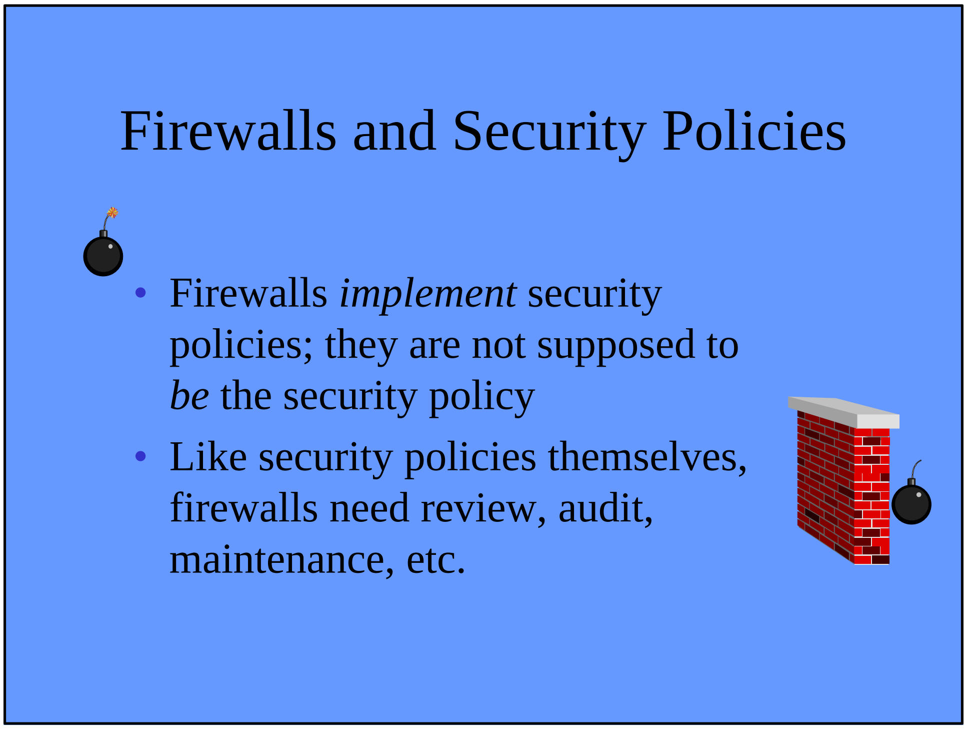


- Packet filter
- Application gateway
- Proxy agent
- "Air gap"



Firewall Philosophies

- The Four Ps:
  - » *Paranoid* - no connection
  - » *Prudent* - “deny all”
  - » *Permissive* - “allow all”
  - » *Promiscuous* - no protection
- Firewalls are a Maginot Line that point out...
  - » ...and most attacks come from the inside!!
- Firewalls *should* also protect against outbound attacks!!



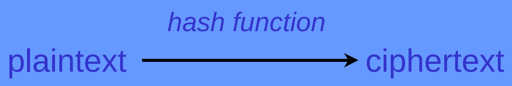
Firewalls and Security Policies

- Firewalls *implement* security policies; they are not supposed to *be* the security policy
- Like security policies themselves, firewalls need review, audit, maintenance, etc.

Private Communication and Transactions on the Internet

- Secure communication requires:
  - » Authentication
  - » Message integrity
  - » Non-repudiation
  - » Privacy/confidentiality
  - » Authorization
  - » Audit

Hash Functions

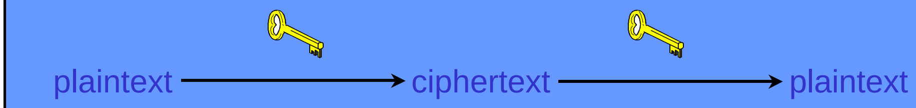


- No key
  - » Plaintext (and length of plaintext) is not recoverable from the ciphertext
  - » Examples: MD2, MD4, MD5, SHA
  - » Also called *message digests* or *one-way encryption*
- Primary use: Message integrity

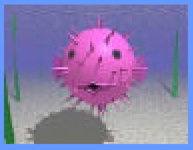
Hashing: UNIX Password File

```
carol:FM5ikbQt1K052:502:100:Carol Monaghan:/home/carol:/bin/bash
alex:LqAi7Mdyg/HcQ:503:100:Alex Insley:/home/alex:/bin/bash
gary:FkJXupRyFqY4s:501:100:Gary Kessler:/home/gary:/bin/bash
todd:edGqQUAaGv7g6:506:101:Todd Pritsky:/home/todd:/bin/bash
sarah:Jbw6BwE4XoUHo:504:101:Sarah Antone:/home/schedule:/bin/bash
josh:FiH0ONcjPut1g:505:101:Joshua Kessler:/home/webroot:/bin/bash
```

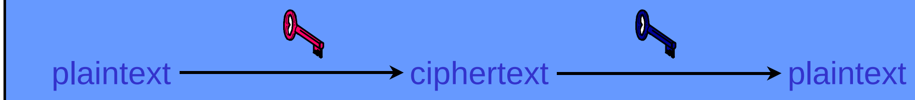
Secret Key Cryptography



- Single key *(symmetric cryptography)*
  - » Same key is used for encryption and decryption
  - » Examples: DES, IDEA, 3DES, RC4, RC5, CAST, Blowfish, Twofish
- Primary use: Privacy



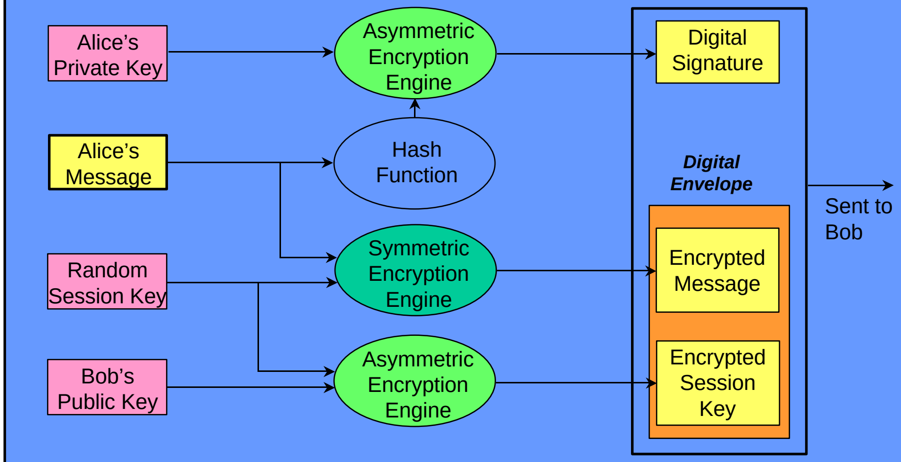
Public Key Cryptography



plaintext → ciphertext → plaintext

- Two keys *(asymmetric cryptography)*
  - » One key is used for encryption and the other for decryption (prime factors of a very large number)
  - » Examples: RSA, DSA, Diffie-Hellman
- Primary uses: Authentication, non-repudiation, key exchange

Sample Application



Alice's Private Key

Alice's Message

Random Session Key

Bob's Public Key

Asymmetric Encryption Engine

Hash Function

Symmetric Encryption Engine

Asymmetric Encryption Engine

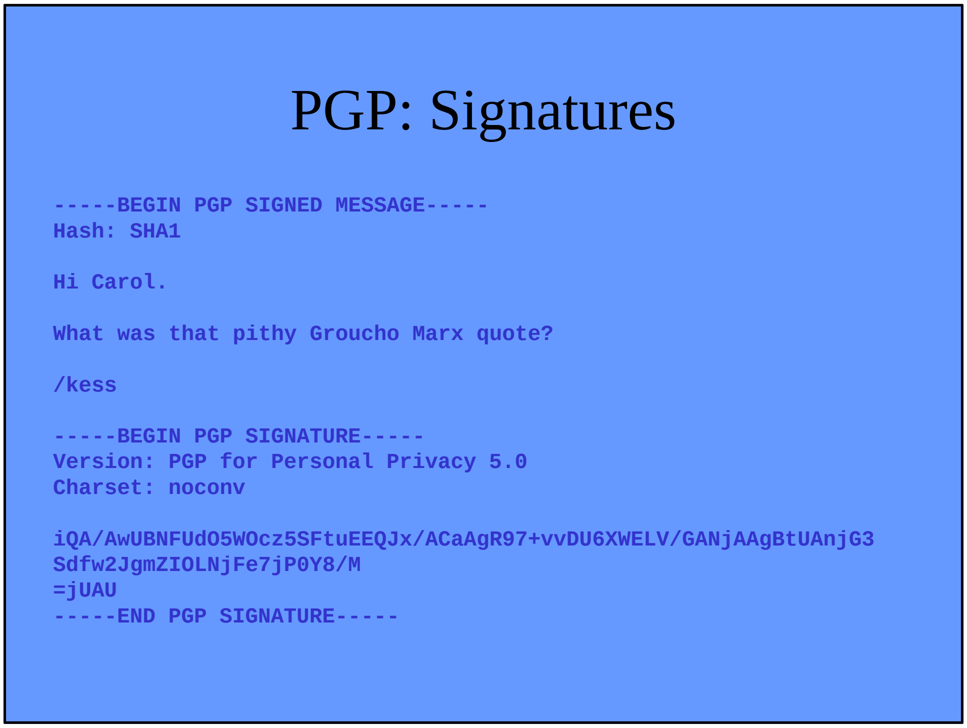
Digital Signature

Digital Envelope

Encrypted Message

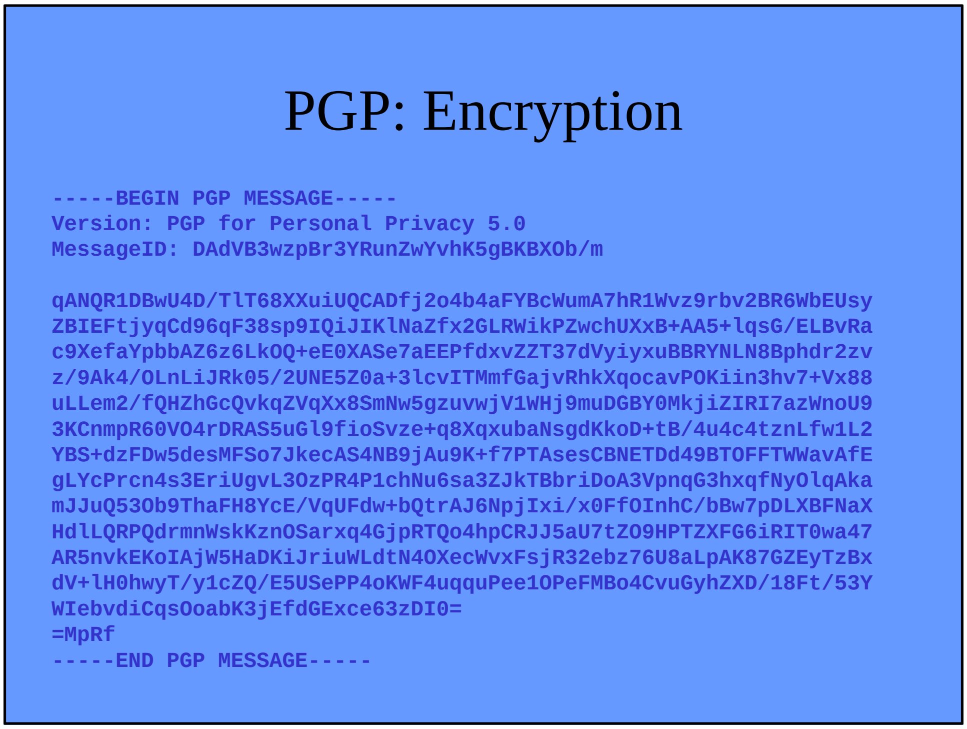
Encrypted Session Key

Sent to Bob



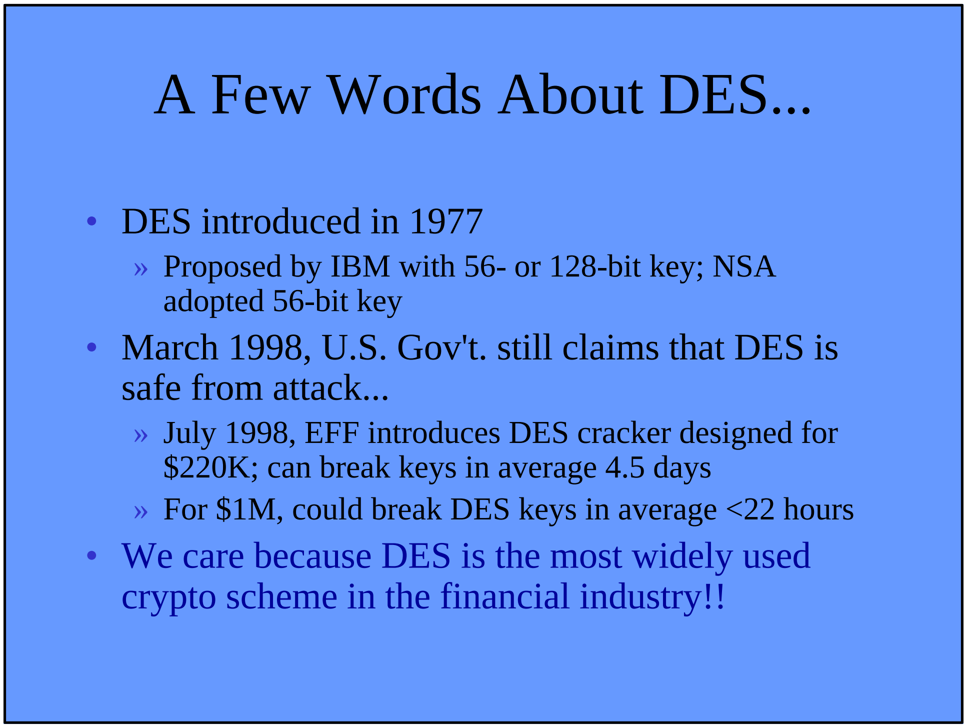
PGP: Signatures

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Hi Carol.

What was that pithy Groucho Marx quote?

/kess

-----BEGIN PGP SIGNATURE-----
Version: PGP for Personal Privacy 5.0
Charset: noconv

iQA/AwUBNFUdO5WOcz5SFtuEEQJx/ACaAgR97+vvDU6XWELV/GANjAAgBtUAnjG3
Sdfw2JgmZIOLNjFe7jP0Y8/M
=jUAU
-----END PGP SIGNATURE-----
```



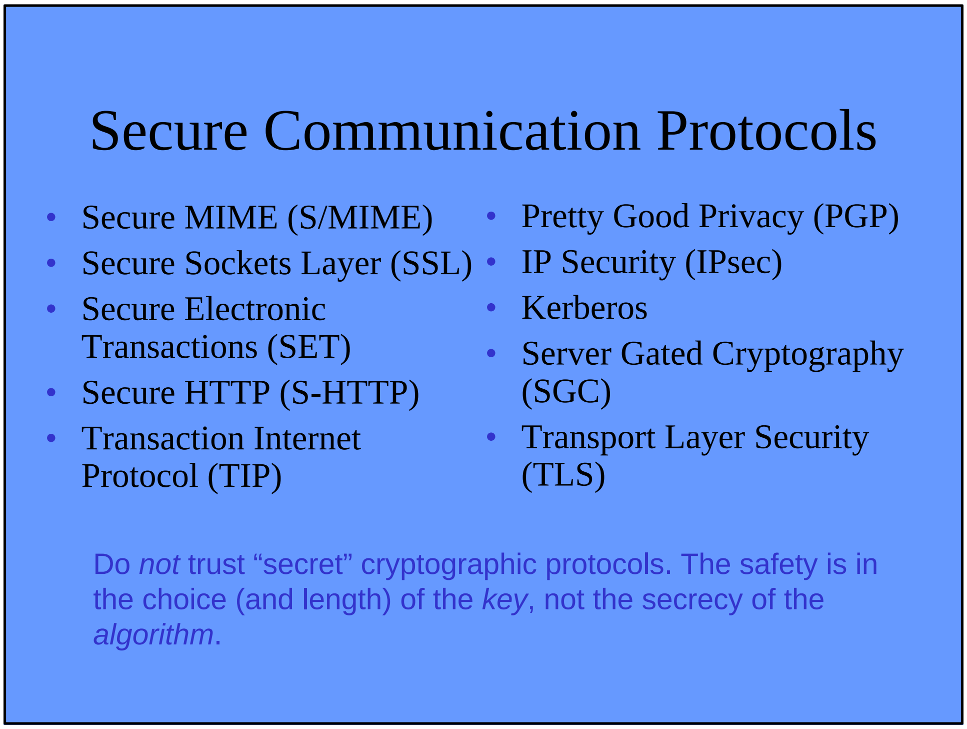
PGP: Encryption

```
-----BEGIN PGP MESSAGE-----
Version: PGP for Personal Privacy 5.0
MessageID: DAdVB3wzpBr3YRunZwYvhK5gBKBXOb/m

qANQR1DBwU4D/TlT68XXuiUQCADfj2o4b4aFYBcWumA7hR1Wvz9rbv2BR6WbEUsy
ZBIEFtjyqCd96qF38sp9IQiJIKlNaZfx2GLRWikPZwchUXxB+AA5+lqsG/ELBvRa
c9XefaYpbbAZ6z6LkOQ+eE0XASe7aEEPfdxvZZT37dVyiyxuBBRYNLN8Bphdr2zv
z/9Ak4/OLnLiJRk05/2UNE5Z0a+3lcvITMmfGajvRhkXqocavPOKiin3hv7+Vx88
uLLem2/fQHZhGcQvkqZVqXx8SmNw5gzuvwjV1WHj9muDGBY0MkjiZIRI7azWnoU9
3KCnmpR60VO4rDRAS5uGl9fioSvze+q8XqxubaNsgdKkoD+tB/4u4c4tznLfw1L2
YBS+dzFDw5desMFSo7JkecAS4NB9jAu9K+f7PTAsesCBNETDd49BTOFFTWWavAfE
gLYcPrcn4s3EriUgvL3OzPR4P1chNu6sa3ZJkTBbriDoA3VpnqG3hxqfNyOlqAka
mJJuQ53Ob9ThaFH8YcE/VqUFdw+bQtrAJ6NpjIxi/x0FfOInhC/bBw7pDLXBFNaX
HdlLQRPQdrmnWskKznOSarxq4GjpRTQo4hpCRJJ5aU7tZO9HPTZXFG6iRIT0wa47
AR5nvkEKoIAjW5HaDKiJriuWLdtN4OXecWvxFsjR32ebz76U8aLpAK87GZEyTzBx
dV+lH0hwyT/y1cZQ/E5USePP4oKWF4uqquPee1OPeFMBo4CvuGyhZXD/18Ft/53Y
WIebvdiCqsOoabK3jEfdGExce63zDI0=
=MpRf
-----END PGP MESSAGE-----
```



A Few Words About DES...

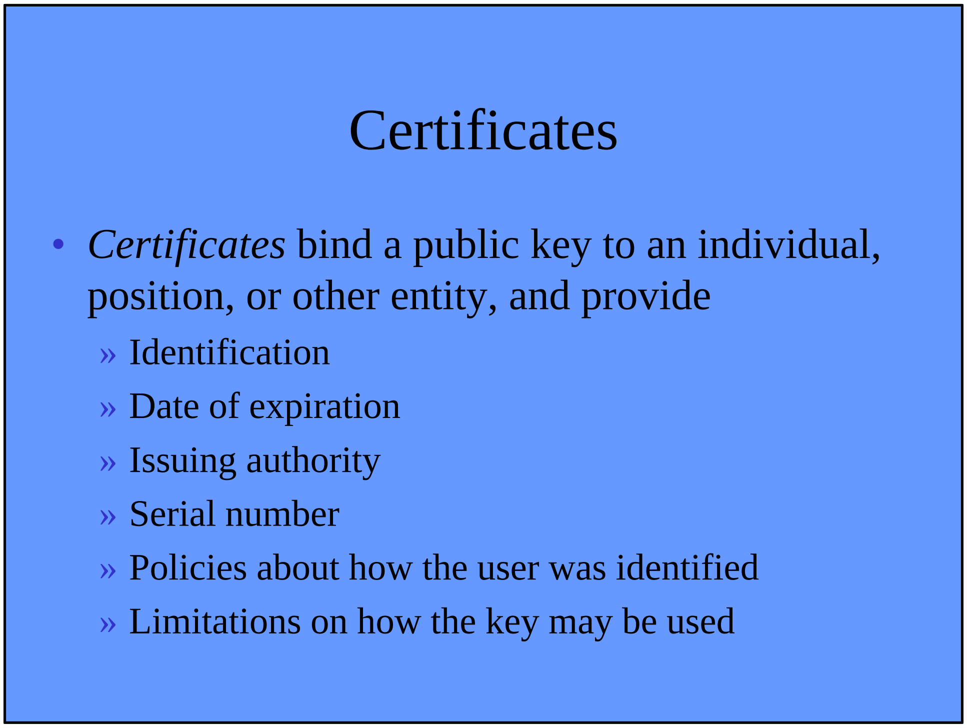
- DES introduced in 1977
  - » Proposed by IBM with 56- or 128-bit key; NSA adopted 56-bit key
- March 1998, U.S. Gov't. still claims that DES is safe from attack...
  - » July 1998, EFF introduces DES cracker designed for $220K; can break keys in average 4.5 days
  - » For $1M, could break DES keys in average <22 hours
- We care because DES is the most widely used crypto scheme in the financial industry!!



Secure Communication Protocols

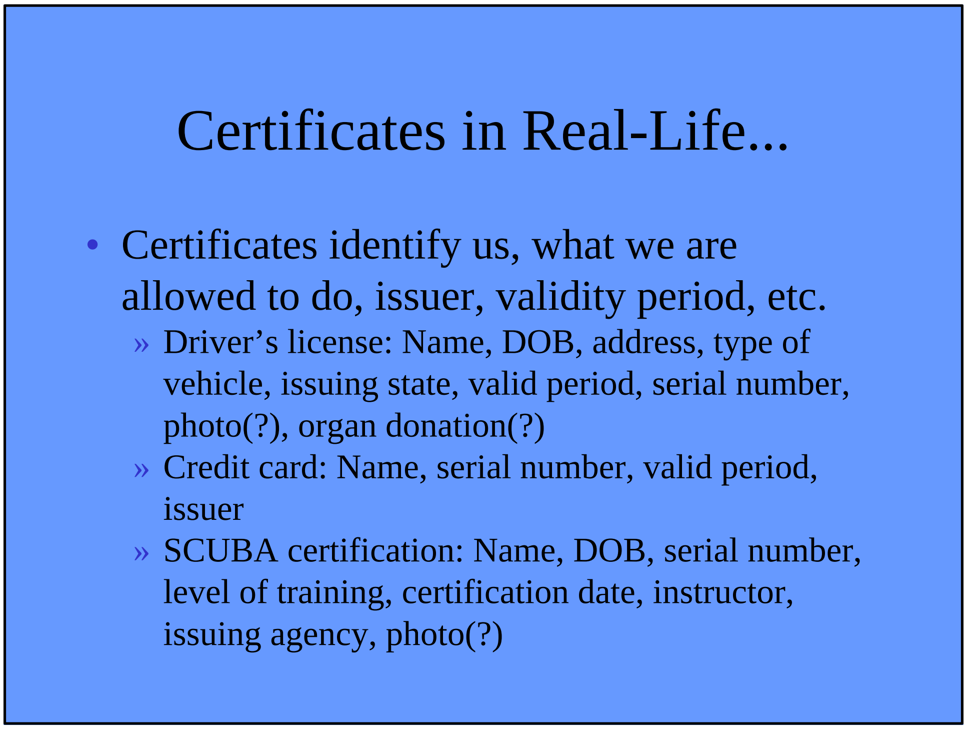
- Secure MIME (S/MIME)
- Secure Sockets Layer (SSL)
- Secure Electronic Transactions (SET)
- Secure HTTP (S-HTTP)
- Transaction Internet Protocol (TIP)
- Pretty Good Privacy (PGP)
- IP Security (IPsec)
- Kerberos
- Server Gated Cryptography (SGC)
- Transport Layer Security (TLS)

Do *not* trust “secret” cryptographic protocols. The safety is in the choice (and length) of the *key*, not the secrecy of the *algorithm*.



Certificates

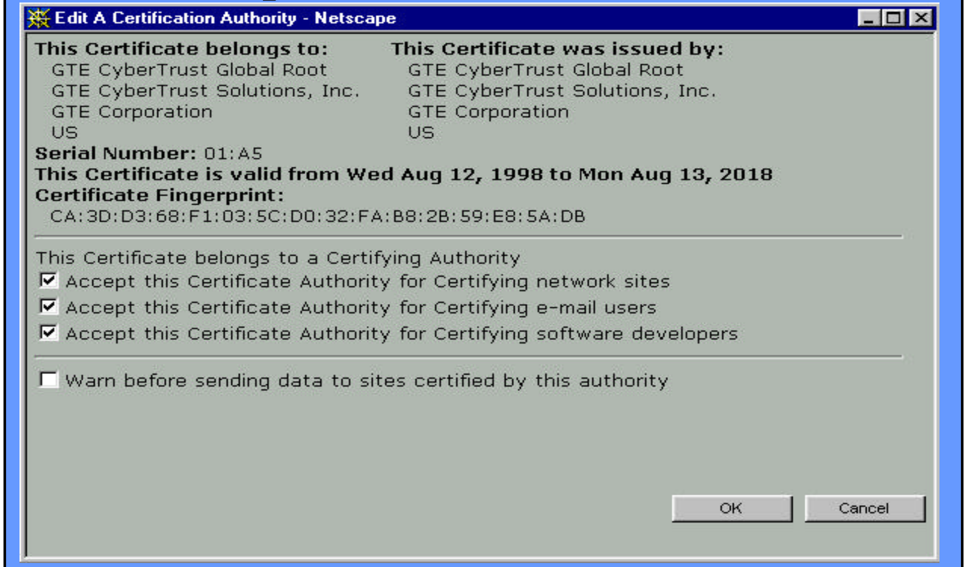
- *Certificates* bind a public key to an individual, position, or other entity, and provide
  - » Identification
  - » Date of expiration
  - » Issuing authority
  - » Serial number
  - » Policies about how the user was identified
  - » Limitations on how the key may be used



Certificates in Real-Life...

- Certificates identify us, what we are allowed to do, issuer, validity period, etc.
  - » Driver’s license: Name, DOB, address, type of vehicle, issuing state, valid period, serial number, photo(?), organ donation(?)
  - » Credit card: Name, serial number, valid period, issuer
  - » SCUBA certification: Name, DOB, serial number, level of training, certification date, instructor, issuing agency, photo(?)

Sample Browser Certificate



This Certificate belongs to:
GTE CyberTrust Global Root
GTE CyberTrust Solutions, Inc.
GTE Corporation
US

This Certificate was issued by:
GTE CyberTrust Global Root
GTE CyberTrust Solutions, Inc.
GTE Corporation
US

Serial Number: 01:A5
This Certificate is valid from Wed Aug 12, 1998 to Mon Aug 13, 2018
Certificate Fingerprint:
CA:3D:D3:68:F1:03:5C:D0:32:FA:B8:2B:59:E8:5A:DB

This Certificate belongs to a Certifying Authority
☑ Accept this Certificate Authority for Certifying network sites
☑ Accept this Certificate Authority for Certifying e-mail users
☑ Accept this Certificate Authority for Certifying software developers

□ Warn before sending data to sites certified by this authority

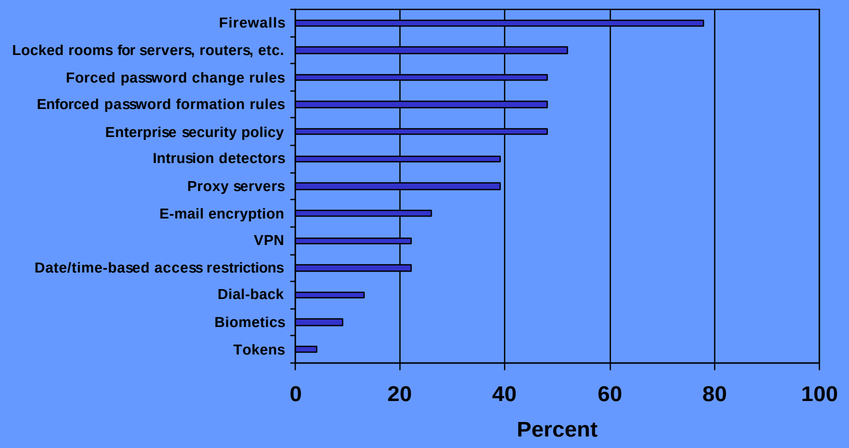
Certificate Chain

- Shopper goes to on-line commerce site
- When entering credit card, starts SSL/TLS
- Secure server returns certificate containing public key and CAs' information signed with issuer's private key
  - » Root CAs' public keys shipped with browsers

Conclusions

- People won't use security tools that inhibit their ability to work
- Fixed, static network defenses are eventually circumvented
- View your network as an attacker would to understand the true threat
- You have to do the basic stuff and maintain vigilance

Security Measures Being Employed

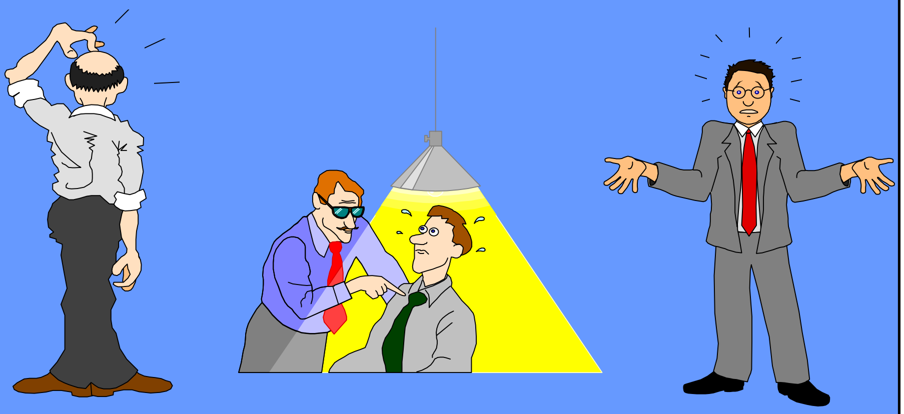


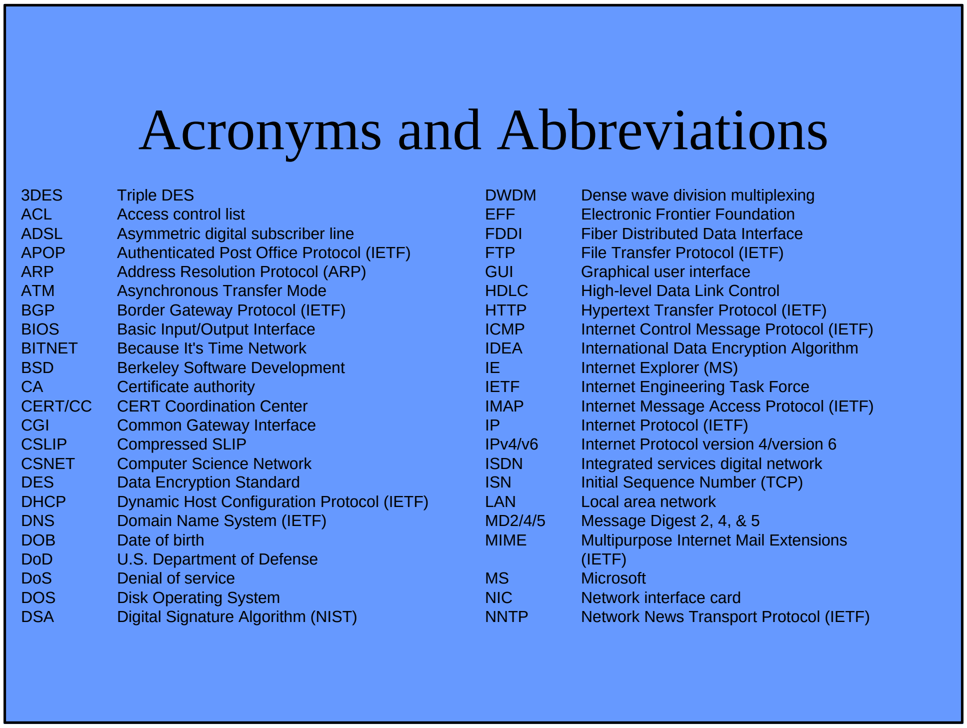
Source: Network Magazine, *5/1999*

For More Information...

- **Books**
  - » *The Happy Hacker*, Meinel (American Eagle)
  - » *Internet Security*, Atkins et al. (New Riders)
  - » *Maximum Security*, Anonymous (SAMS)
- **On the Web...**
  - » CERT/CC (*www.cert.org*)
  - » GCK's security papers (*www.sover.net/~kessfam/gck/library*) and pointers (*www.sover.net/~kessfam/gck/library/securityurl.html)*
  - » International Computer Security Association (*www.icsa.net*)
  - » SANS Institute (*www.sans.org*)

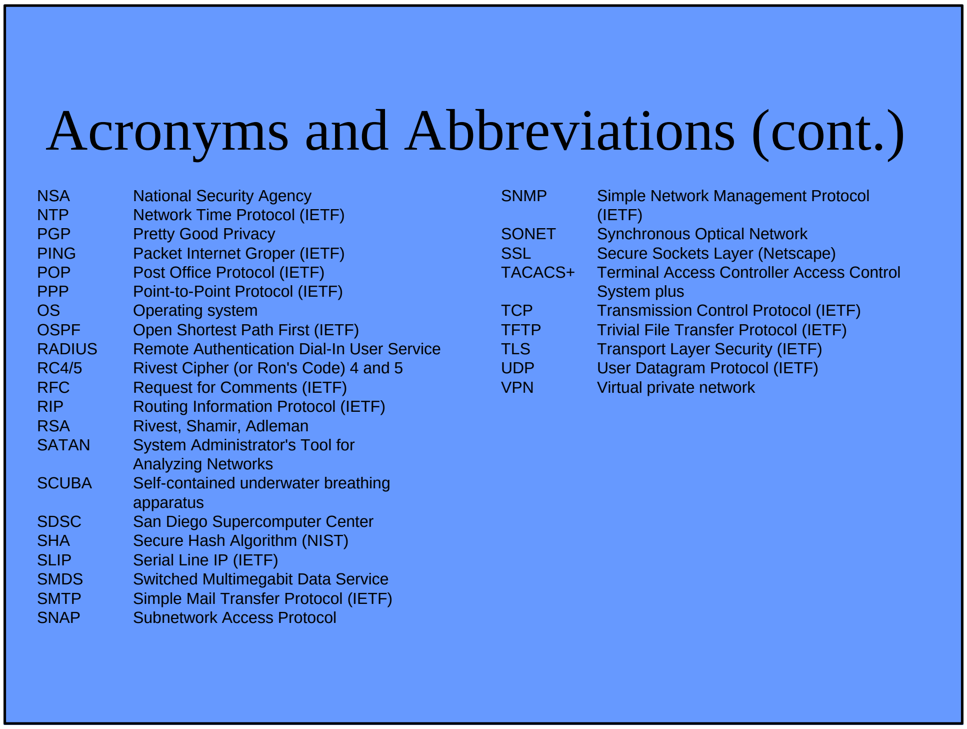
Questions? Comments? Queries?





Acronyms and Abbreviations

3DES	Triple DES
ACL	Access control list
ADSL	Asymmetric digital subscriber line
APOP	Authenticated Post Office Protocol (IETF)
ARP	Address Resolution Protocol (ARP)
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol (IETF)
BIOS	Basic Input/Output Interface
BITNET	Because It's Time Network
BSD	Berkeley Software Development
CA	Certificate authority
CERT/CC	CERT Coordination Center
CGI	Common Gateway Interface
CSLIP	Compressed SLIP
CSNET	Computer Science Network
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol (IETF)
DNS	Domain Name System (IETF)
DOB	Date of birth
DoD	U.S. Department of Defense
DoS	Denial of service
DOS	Disk Operating System
DSA	Digital Signature Algorithm (NIST)
DWDM	Dense wave division multiplexing
EFF	Electronic Frontier Foundation
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol (IETF)
GUI	Graphical user interface
HDLC	High-level Data Link Control
HTTP	Hypertext Transfer Protocol (IETF)
ICMP	Internet Control Message Protocol (IETF)
IDEA	International Data Encryption Algorithm
IE	Internet Explorer (MS)
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol (IETF)
IP	Internet Protocol (IETF)
IPv4/v6	Internet Protocol version 4/version 6
ISDN	Integrated services digital network
ISN	Initial Sequence Number (TCP)
LAN	Local area network
MD2/4/5	Message Digest 2, 4, & 5
MIME	Multipurpose Internet Mail Extensions (IETF)
MS	Microsoft
NIC	Network interface card
NNTP	Network News Transport Protocol (IETF)



Acronyms and Abbreviations (cont.)

NSA	National Security Agency
NTP	Network Time Protocol (IETF)
PGP	Pretty Good Privacy
PING	Packet Internet Groper (IETF)
POP	Post Office Protocol (IETF)
PPP	Point-to-Point Protocol (IETF)
OS	Operating system
OSPF	Open Shortest Path First (IETF)
RADIUS	Remote Authentication Dial-In User Service
RC4/5	Rivest Cipher (or Ron's Code) 4 and 5
RFC	Request for Comments (IETF)
RIP	Routing Information Protocol (IETF)
RSA	Rivest, Shamir, Adleman
SATAN	System Administrator's Tool for Analyzing Networks
SCUBA	Self-contained underwater breathing apparatus
SDSC	San Diego Supercomputer Center
SHA	Secure Hash Algorithm (NIST)
SLIP	Serial Line IP (IETF)
SMDS	Switched Multimegabit Data Service
SMTP	Simple Mail Transfer Protocol (IETF)
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol (IETF)
SONET	Synchronous Optical Network
SSL	Secure Sockets Layer (Netscape)
TACACS+	Terminal Access Controller Access Control System plus
TCP	Transmission Control Protocol (IETF)
TFTP	Trivial File Transfer Protocol (IETF)
TLS	Transport Layer Security (IETF)
UDP	User Datagram Protocol (IETF)
VPN	Virtual private network