15.564 Information Technology I

Computer Security (Parts I & II)

Overview

- Securing communications
- Securing access
- Hacker attacks

What is computer security?

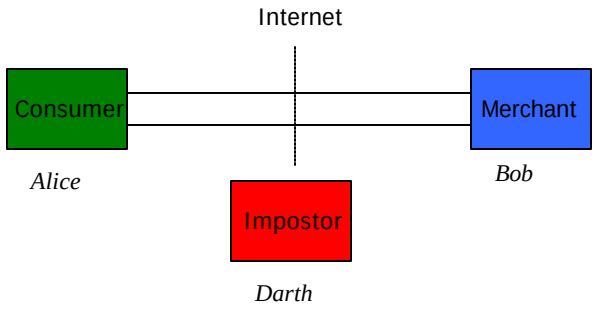
- Securing access to resources
  - Two steps:
    - Authenticate = establish identity of the requestor
    - Authorize = grant or deny access

Topic 1: Securing communications

- What can go wrong?

Communication security issues

- Encryption
  - how do I ensure the secrecy of my transactions?
- Authentication
  - how do I verify the true identity of my counterparts?



Private and public key cryptography

- Secret key cryptography: Based on a secret key
  - Same secret key used for encryption and decryption
  - Problem: How to transmit key securely on the Internet???
- Public key cryptography: Two keys used
  - Public key known to everybody. Used for encryption.
  - Private key known only to owner. Used for decryption.

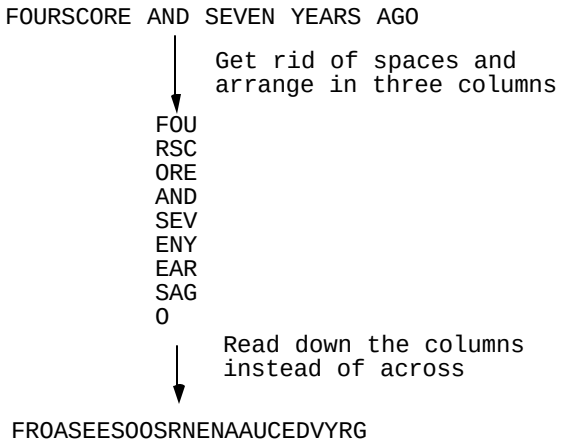
{Message}
encrypted using Bob's public key

Only Bob who knows the corresponding private key can decrypt

Alice ---------- Bob

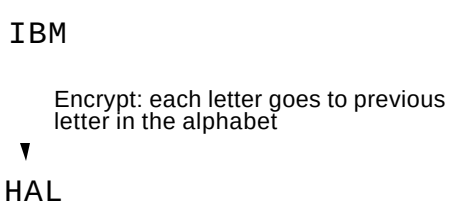
Examples of private key cryptography: Transposition Ciphers

- Don't change any of the bits, just rearrange them



Examples of private key cryptography: Substitution Ciphers

- Substitute for each letter (block of bits)



- How can you crack a substitution cipher?
  - I.e., how can you guess the key?
  - ABCD EFBDH IJK EHNHJ LHIDE IMB

Examples of private key cryptography: One Time Pads

- A substitution cipher, but the substitution method changes for each letter (block)
- Sender and receiver each get identical copies of a set of random numbers
  - Interpret number n as "substitute letter n later in alphabet"
- Provably unbreakable
- Problem is creating and distributing truly random one-time pads

Examples of private key cryptography: The DES algorithm

- DES = Data Encryption Standard
- Private key system
  - Same key used for encryption and decryption
  - Key determines a sequence of permutations and substitutions
  - Process implemented in hardware; only keys are variables
- Developed by IBM in 1970s, with input from NSA
- Official standard for non-classified government comm.
- De facto standard for financial transactions
- Some argue that NSA deliberately made DES weak
  - Keys are 56-bits long
  - IBM had another algorithm available that used 128-bit keys
  - But no one has publicly proven it's breakable

Public Keys

- Each person has a pair of keys e for encryption and d for decryption
- Make e publicly available
- Alice uses Bob's e_B to send him a private message M^{e_B}
- Bob decrypts with d_B
  - $\left(M^{e_B}\right)^{d_B} = M$
  - No one else knows d_B

Alice ——————————— Bob

- Works as long as
  - d is really kept secret
  - Hard to compute d from e
  - Get the correct e from some trusted source

Mathematical basis of PKC: RSA Public Keys

- Start with two large (e.g. 1024-bit) primes p,q
- n mod m denotes the remainder of division n/m
- Choose numbers e, d such that
  - $(e*d) \bmod (p-1)(q-1) = 1$
  - In other words: $e*d = 1 + k(p-1)(q-1)$
  - PUBLIC encryption key: (e, pq)
  - SECRET decryption key: (d, pq)
- Encryption
  - break messages into pieces M such that M<pq
  - transform each piece M into $M^e \bmod pq$

Decrypting in RSA (for aficionados only)

- Useful arithmetic equalities

  $(M^e)^d = M^{ed} = (M^d)^e$ (1) easy

  $M^e M^d = M^{e+d} = M^d M^e$ (2) easy

  $M^{(p-1)(q-1)} \bmod pq = 1$ (3) hard

- Decryption: raise message to power d, mod pq

  $(M^e \bmod pq)^d \bmod pq = M^{ed} \bmod pq = M^{1+k(p-1)(q-1)} \bmod pq$

  because $ed = 1+k(p-1)(q-1)$ ▲

  $M^{1+k(p-1)(q-1)} \bmod pq = (M \bmod pq) * (M^{k(p-1)(q-1)} \bmod pq) =$

  $(M \bmod pq) * (M^{(p-1)(q-1)} \bmod pq)^k =$

  $(M \bmod pq) * (1)^k = M \bmod pq = M$ (because $M < pq$)

  ▲ because of formula (3)

See http://theory.lcs.mit.edu/~cis/pubs/rivest/rsapaper.ps

Why public cryptography works?

- Encryption $M' = (M)^e$ Decryption $M = (M')^d$
  - Public: (e, p*q)
  - Secret: d, p, q
- d too large for trial and error
- Just given p*q and e, unknown how to compute d without knowing p, q
  - $(e*d) \bmod (p-1)(q-1) = 1$
- To compute p,q from p*q, all different combinations of prime factors must be tried
- p*q can't be factored in reasonable time
  - 664bit -> 200 decimal digits -> 3700 years
  - 1024bit -> 308 decimal digits -> 10^{10} years!!!

Public key cryptography works if...

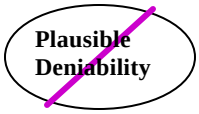
- Private key remains secret
  - Never leaves the owner's computer
  - Typically encrypted and password-protected
- Difficult to guess private key from knowledge of public key
  - Boils down to trying all different key combinations
  - Difficulty of "breaking" the code rises exponentially with the bit length of the key
  - 1024-bit keys require more time than the life of the universe in order to be "broken"
- Reliable public key distributed
  - This is the most difficult problem!

Encryption is not enough: Spoofs

- Pretending to be someone else
- Hard to login without someone's password
- But can send out communications with someone else's name on it
  - email
    - 1993: Dartmouth sent a message saying midterm exam was cancelled
    - Message appeared to come from the Professor!
  - netnews
  - world wide web

Needed: Message Authentication

- Make sure Bob gets the message unaltered
- Don't let Alice deny sending the message



- Don't care about eavesdropper Darth, unless Darth changes the message
- How can cryptography help?

Digital Signatures

- Key property: Public and private keys can be applied in either order
- Alice has message M
  - She applies her private key to it
  - She sends encrypted message to Bob
- Bob decrypts it with Alice's public key
  - gets back original message
  - infers that Alice is indeed the sender (since only Alice has the private key that corresponds to her public key)
- In that way, encrypting a message with one's private key acts as a digital signature!

Public Key Management

- Public key cryptography works as long as
  - ✓ d is really kept secret
  - ✓ Hard to compute d from e
  - – Get the correct e from some trusted source
- Bob can send public key over insecure communication channel
- But how do you know Darth didn't send you his key instead?

A central key distributor

- Alice asks the distributor for Bob's public key
- The distributor sends it to Alice and "digitally signs" it
- Alice knows the key came from the distributor
  - – Now just have to be sure that the distributor is honest and got Bob's key from Bob, not Darth
- Requires one secure communication per user
  - – Bob sends public key to distributor when he joins the system
- Secret keys require secure communication between every pair of users

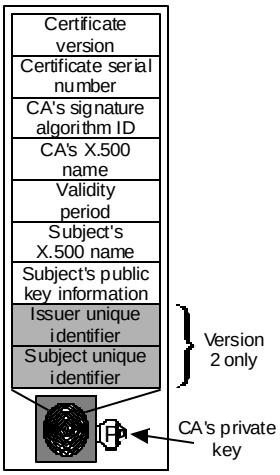
Public Key Infrastructure (PKI)

- Certificate Authorities are Trusted Third Parties charged with the responsibility to generate trusted certificates for requesting individuals organizations
  - Certificates contain the requestors public key and are digitally signed by the CA
  - Before a certificate is issued, CA must verify the identity of the requestor
- These certificates can then facilitate automatic authentication of two parties without the need for out-of-band communication

Overview of PKI

For this diagram, see: Figure 19, "Sample PKI Design" on page 102 of "Risk Management Forecast: 2001." PricewaterhouseCoopers LLP, 2001. ISBN 0-9706535-0-6.

Example: X.509 certificates



PKI Industry

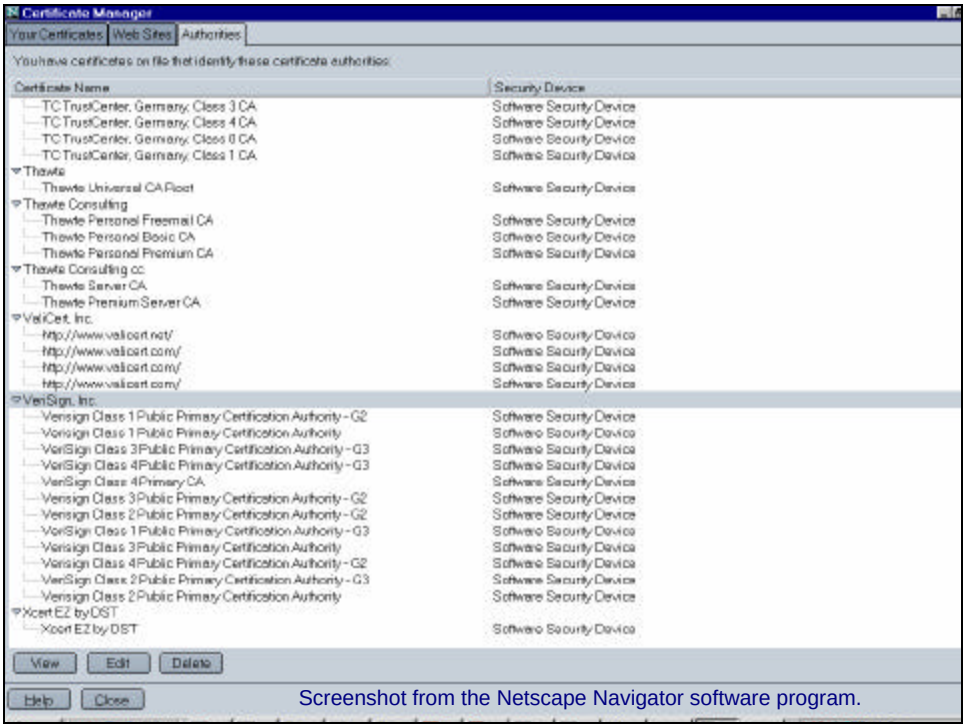
- Main players: trusted third party CAs
  - Verisign
  - Entrust
  - Cybertrust
  - RSA
- Revenue from
  - products (PKI servers for intranets and extranets)
  - services (certificate services for individuals and organizations)
- Revenue predictions (Datamonitor)
  - $330 million for products $347 million for services
  - Figures will grow to $1.2b and $1.4b resp. in 2006
- Mobile devices a big boost

Applications: eCommerce Security

- Needed to transmit sensitive information through the Web
  - credit card numbers
  - merchandise orders
- Requirements
  - sender and receiver must authenticate each other before sending any “real” data
  - all “real” data must flow encrypted through the network
  - no intercepted communication can be used to an intruder’s advantage

SSL Certificates

- Used to certify a user’s identity to another user
  - The certificate issuer's name
  - Who the certificate is being issued for (a.k.a the subject)
  - The public key of the subject
  - Some time stamps
- Digitally signed by issuer
- Issuer must be a trusted entity
- All users must have a reliable public key of the issuer
  - in order to verify signed certificate



Screenshot from the Netscape Navigator software program.

Netscape Secure Sockets Layer (SSL)

- A->B hello
- B->A Hi, I'm Bob, bob's-certificate
- A->B prove it, challenge msg
- B->A {challenge msg} bob's-private-key
- A->B {secret key} bob's-public-key
- B->A {some message} secret-key

SSL Checks

- How can we extend the protocol for 2-way authentication?
  - so that, e.g. a client cannot deny placing an order
- What happens if somebody sniffs and reuses bob's-certificate?
- What happens if somebody intercepts and garbles/replays part of the "real data" communication?

Topic 2: Access Control

For this diagram, see: Figure 53, "Elements of Securing Remote Access" in "Risk Management Forecast: 2001." PricewaterhouseCoopers LLP, 2001. ISBN 0-9706535-0-6.

General Access Control Techniques

- Something you have
- Something you know
- Something you are

System Access Controls "Something you know..."

- Login procedures
  - Usually something you know
- Password leaks
  - Commonly used password
  - Explicitly told
    - Voluntarily
    - Trojan horse
  - Trial and error
  - Intercepted communication
    - paper, camera, wiretap, file on disk, emanations
    - password sniffing on networks
- Passwords are inconvenient
  - In client/server environment, user doesn't want to enter password for every service she connects to

Enter Biometrics...
"Something you are..."

- Fingerprint recognition

- Face recognition

- Voice Authentication

Smart Cards
"Something you have"

- Several subcategories
- One of interest here are cryptographic smart cards:
  - Store user's digital certificate and/or private key
  - Used to prevent private keys from being "hacked" from user's computer
  - What happens if a smart card is stolen?

Overview of access control methods

For this diagram, see Figure 38, "Authentication Alternatives," in "Risk Management Forecast: 2001." PricewaterhouseCoopers LLP, 2001.
ISBN 0-9706535-0-6.

If only life was so simple... Sneaking through the backdoor...

- Strategies whose goal is to gain control by bypassing access control defenses
- Exploit “holes” in applications that connect our machine to the network
  - Viruses
  - Buffer overrun attacks

Viruses and other Critters

- Programs that run on machines where they're not wanted
- Transmitted through I/O channels
- Disguise themselves
  - How?
- Often don't act right away
  - Why not?
- Why hasn't anyone written a definitive virus eliminator?

Denial of service attacks

- Flood a server with fake messages (with "spoofed" IP addresses) so that no legitimate messages can get through
  - Flood someone's mailbox
  - Recent attacks on eBay, Yahoo, etc.
- Difficult to trace since fake messages are sent from a variety of "hijacked" machines

Denial of service explained

Defensive Measures

- Firewalls
- Intrusion Detection Systems

Firewalls

For this diagram, see Figure 60, "Single-Homed Firewall," on page 267 of "Risk Management Forecast: 2001." PricewaterhouseCoopers LLP, 2001. ISBN 0-9706535-0-6.

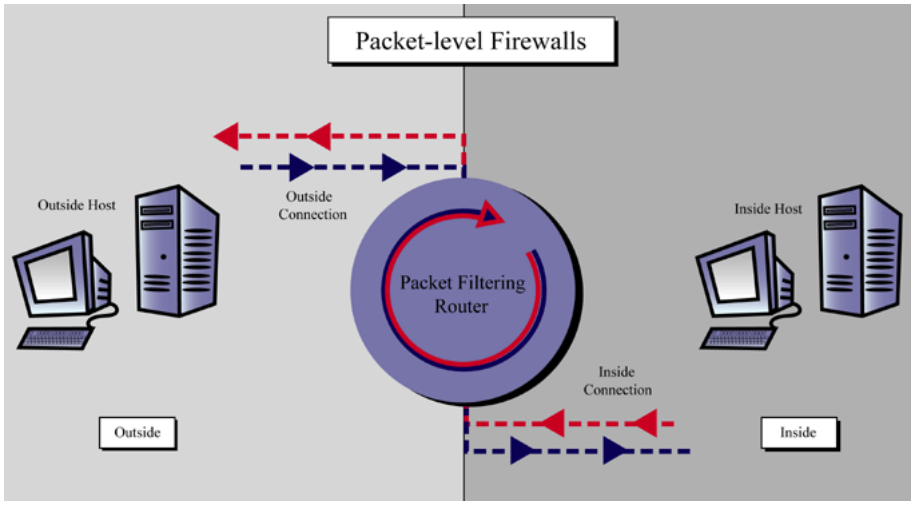
What a firewall does

- Hides the structure of the network by making it appear that all transmissions originate from the firewall.
- Blocks all data not specifically requested by a legitimate user of the network.
- Screens data for source and destination address so you receive data from only trusted locations like people on your approved guest list.
- Screens the contents of data packets for known hacker attacks

Types of firewalls

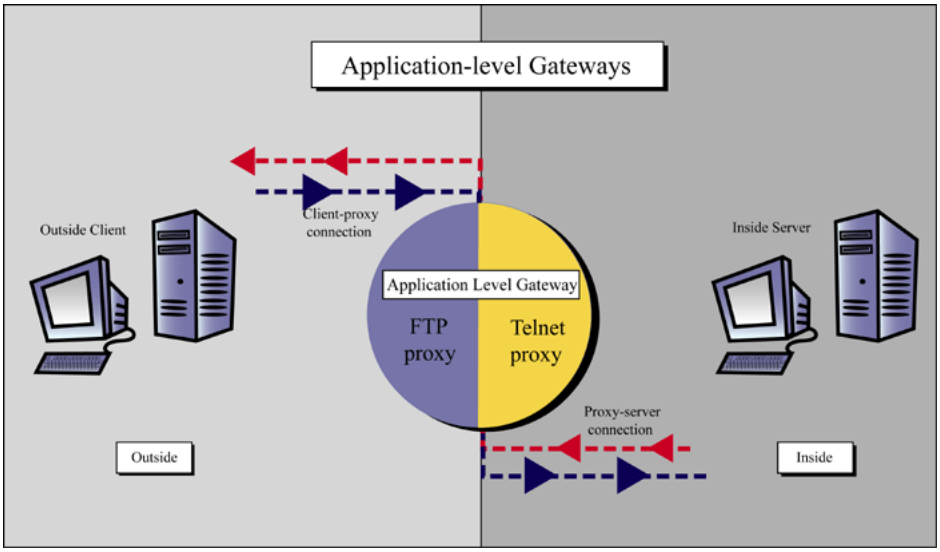
- Packet filter: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules.
- Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers.
- Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses

Packet-level firewalls



Based on Figure 62, "Packet Filter", "Risk Management Forecast: 2001." PricewaterhouseCoopers LLP, 2001, p.268.

Application-level firewalls



Based on Figure 64, "Application-level Gateway","Risk Management Forecast: 2001." PricewaterhouseCoopers LLP, 2001, pp. 269.

Firewall performance/security tradeoffs

For this diagram, see Figure 66, "Firewall Security vs. Performance Tradeoff," on page 271 of "Risk Management Forecast: 2001." PricewaterhouseCoopers LLP, 2001. ISBN 0-9706535-0-6.

Intrusion Detection Systems

For this diagram, see Figure 67, "IDS Characteristics" on page 274 of "Risk Management Forecast: 2001." PricewaterhouseCoopers LLP, 2001. ISBN 0-9706535-0-6.

How does IDS work?

- IDS uses data mining techniques to uncover and report suspicious activities
- Two main strategies:
  - Pattern recognition
  - Anomaly detection

Pattern Recognition

- Developers collect data on all known hacker attacks:
  - Vulnerabilities in OS and applications
  - Know hacker techniques
  - Latest discussions on hacker newsgroups and Bugtraq
- Mine the data for signatures of hacker activity
- Monitor all activity on the host/network for the signatures
- Benefits: Gives a clear understanding of what is happening and how to fix the problem
- But: can't detect newly developed attacks or modifications to older attacks. Likely to report the least serious attacks and miss the most dangerous

Anomaly Detection

- Monitors the hosts/network for a few days
- Collects data on normal types of traffic
- Mines the data to produce signatures of normal traffic
- Monitors all activity again and reports unexpected events
- Benefits: Allows for early notification of new and sophisticated attacks
- But:
  - Gives less understanding of the type of attack and how to recover
  - If you are already being attacked, this is the normal pattern

Pattern Recognition-Practical

- Based on knowing what is the pattern of attack
- Focus on what constitutes an attack
- DM Technique: Neural Net (credit card industry), Genetic Algorithm, rule base decision (cumbersome)

Sample Pattern
If number of failed logins is greater than 5, then this connection is "guess", a guessing password attack.
If the number of hot (count of access to system directories, creation and execution of program) indicators is 3, the number of compromised (count of file/path "not found" errors and "jump to" instructions, etc.) conditions is 2, and a root shell is obtained, then this connection is a buffer overflow attack.
If none of the above, then this connection is "normal".

Anomaly Detection-Practical

- Focus primarily on normalcy and alert on anomaly
- Usual levels of traffic
- Time-based: Logon during hours of operation
- Connection-based: TCP connections time duration
- DM Technique: Neural Net (credit card industry), rule base decision (depends on scope size)

User	Anomaly Description
Programmer2	logs in from beta
Secretary	logs in at night
System Admin.	logs in from jupiter
Secretary	"becomes a manager"
Programmer1	logs in at night
System Admin.	"becomes a programmer"
Manager1	"becomes a system admin."

User	Normal Activities
System administrator	logs in as root, cats the pass -word file, and runs commands such as top.
Programmer1	writes public domain C code, use a vi editor, compiles the C code, reads and sends mail, and executes unix commands.
Programmer2	a similar user profile as in programmer 1, but works in afternoons and evenings.
Secretary	edits latex files, runs latex, reads mail, and sends mail.
Manager1	reads and sends mail
Manager2	reads mail.

Despite all that... security breaches are on the rise

1995: approximately 2,500 incidents
1996: approximately 2,600 incidents
1997: approximately 2,100 incidents
1998: over 3,500 incidents
1999: over 8,000 incidents

Source: Carnegie Mellon University, 2000

See the graph, Figure 51, "Growth in the Number of Incidents Handled by the CERT/CC," on page 255 of "Risk Management Forecast: 2001." PricewaterhouseCoopers LLP, 2001. ISBN 0-9706535-0-6.

.. and require far less technical expertise

For this diagram, see: Figure 52, "Attack Sophistication vs. Intruder Technical Knowledge," on page 255 of "Risk Management Forecast: 2001." PricewaterhouseCoopers LLP, 2001. ISBN 0-9706535-0-6.

Hacker Attacks
A common methodology is the following:

- 1. Gather target information.
- 2. Identify services offered by target to the public (whether intentional or not).
- 3. Research the discovered services for known vulnerabilities.
- 4. Attempt to exploit the services.
- 5. Utilize exploited services to gain additional privileges from the target.

Reiterate steps 1-5 until goals are achieved.

Step 1: Gather target information.

- Domain names, IP address ranges.
- InterNIC contact information.
- Physical addresses.
- Organizational structures.
- Alliances and financial information.
- Names of officers, managers, technical staff.
- Newsgroup posts.

Step 2: Identify services.

- Web servers.
- FTP servers.
- DNS servers.
- e-mail gateways.
- Help desks/phone support.
- Other (gopher, LDAP, irc, etc.)

Port Scanning

Port scanning is used to identify which ports are open and what services are running on those specific ports. Examples of services are:

- ftp (port 21)
- telnet (port 23)
- http (port 80)

Security Scanners

What is a security scanner?

A security scanner is software that will remotely audit a given network and determine whether hackers may break into it or misuse it in some way.

Examples include:

- NMAP
- SAINT™
- Nessus

Step 3: Research vulnerabilities.

- Vendor announcements.
- Default configurations.
- Poor configurations. (i.e. passwords, cleartext protocols)
- Gather available exploits or develop new exploit.
- Derived exploits.
- Some original work.

Step 4: Exploit vulnerabilities.

- Attempt to exploit vulnerabilities to gain access to the target.
- Continue until successful.

Step 5: Utilize increased access.

- Exploit additional vulnerabilities to gain additional access and information to use in penetrating further into an organization.
- The hacker "becomes" a legitimate user (even an administrator).

Sniffing tools

- Monitor all traffic on a LAN
- Can be used to capture usernames, passwords etc.

Example : IIS web exploit.

- Due to a bug, IIS/PWS allows arbitrary commands to be executed by the web server by properly “encoding” them inside a URL request
- Hackers can use this vulnerability in order to
  - Read any file on the machine
  - Execute any application on the machine
  - Download code that will enable them to gain access to the machine
  - ...

Prevention

- Stay current on patch levels for Microsoft's OS and web server.
- Implement a good firewall
- Use an IDS system (or two!).
- Host security is important (Microsoft's "Securing IIS” and “Securing Windows NT” documents).
- Pattern matching intercept proxies.

Security Resources

- www.microsoft.com/security
  - Advisories
  - Patches
  - IIS Security Checklist
- www.securityfocus.com
  - Bugtraq Mailing List
  - Tools, Books, Links
  - Vulnerabilities and Fixes

Recommended Book

Hacking Exposed: Network Security Secrets and Solutions

George Kurtz

Stuart McClure

Joel Scambray