

# Security 2

---

## CERT

Tracks vulnerabilities

<http://www.cert.org/>

<http://www.cert.org/advisories/>

There's some tension about when vendors should be told vs. the general public  
(MS has argued for keeping the public in the dark)

## Attack Categories

Social engineering

Sniffing traffic

Spoof, inject traffic

Trojan horse

Virus, worm

## Attack: Social Engineering

Tricking people socially into moving a file, revealing a password, etc.

This works very well -- send the message "your password has been compromised, please change it to 'nowsafe'" -- send this message to 10,000 AOL users -- you get some.

Call the corporate help desk and pose as a confused user, lost password, etc.

By most accounts, social engineering can be very effective

## Attack: Traffic Sniffing

Looking at packets

Requires access to a machine on the IP route

Observe passwords or other info in the packets

At one time, this was the largest source of problems on campus, but I believe the various Microsoft security holes have taken the lead (in part, because we don't use "password in the clear" protocols)

## Ethernet "promiscuous" mode

Most Ethernet hardware can be set in "promiscuous" mode where it logs all packets on the ethernet segment.

## Script Kiddie / Rootkit

There are pre-made scripts on the net to aid attacks

The bad guys are called "script kiddies" to mock their lack of basic technical skill and maturity (they are often teenagers, using tools they don't really understand)

A "rootkit" used by a bad guy on a machine may...

1. Turn on promiscuous mode to try to capture passwords on the local ethernet
2. Replace the local network utility program with a version that reports that promiscuous mode is off

## 3l337 -- Elite Speak

'leet speak

Substitute digits for letters, and generally hash things up

0wn -- get root access on a machine

31ee7 d00dz

## Attack: Replay, Spoof

Carl observes Alice sending encrypted packets to Bob

Carl cannot read the packets, but he can re-send them later

Problem: Bob gets the "send this order to Alice" 10 times

Solution: include serial numbers, the current time, etc. in each message

Packet spoofing -- bad guy inserts their own packets as if they were part of the stream of packets (difficult)

Solutions: certificates, encryption

## Attack: Password Guessing

Many passwords are just a word, name, date,

Just use brute force

We may need personal id gadgets someday, as human capacity to remember passwords hits its limit

## Bad Guess -- Deactivate DOS

Server could turn off an account if too many bad passwords

Can be used as a DOS attack (below) against someone

e.g. Disable the ebay account of a rival bidder

## Attack: Denial Of Service (DOS)

Make a service unavailable

e.g. SYN flood -- send many SYN packets (to start 3-way handshake) but never complete the handshake to overwhelm the victim

DOS attacks often involve malformed IP packets

Bad guy has robots launch a DOS attack on a server. High volume of traffic, hard to screen, and robots help shield identity of bad guy

Solution: partial solution is to firm up the internal routing protocols so it is harder to send bad packets -- screen them out before they get to the victim.

## Distributed DOS (DDOS)

Distributed DOS -- bad guy takes over many machines for use as "robots". e.g. a Win XP machine on a cable modem

On the Bad guy's signal, the hundreds of robots send traffic to the victim -- greater effect, and it's harder to trace back to the bad guy

## Code From Net = Dangerous

Code is fundamentally dangerous compared to a passive document.

If Carl can execute his code on Alice's machine, Carl, in some sense, has control or use of Alice's machine

## Code Solutions

Solution1: code signing -- the code is signed, so you know who it's from (Microsoft is working on this)

Solution2: sandbox -- the code runs in a limited environment where it can't cause much damage (Java does this and also code-signing)

## Executable Content Vulnerability

A program, such as Internet Explorer, either by design or due to a bug, executes content sent to it

If the bad guy can execute code on a machine, they can use it for their own purposes

This has been a huge source of MS vulnerabilities, as MS frequently used "portable VB script" as a way to integrate programs, not being fully aware of the security implications

## Buffer Overflow Vulnerability

The FTP server is running on Alice's machine

Bob sends an over-sized request to the FTP server, exploiting a bug in the FTP server code that causes the FTP server to come under Bob's control (running on Alice's machine).

There have been many such vulnerabilities -- but they are gradually being closed as programmers learn about that sort of bug.

Code

```
char* input = ...;
char buff[1000];
...
scanf(input, "...%s...", buff);
```

Worm sends large data, which goes past the end of buff and writes things on the stack, altering return addr or something -- very tricky to get details right, depends on stack layout, CPU type, etc.

## Attack: Nimda

Very successful worm, uses many strategies.

1. Attacks many MS IIS web server vulnerabilities
  2. On entry, sends copy of itself as a readme.exe to email addrs from addr book and internet history. These can execute on the recipient machine due to a IE 5,6 vulnerability. From: headers may be forged.
  3. Installs the readme.exe in the web server doc tree, disguised as a .wav, so that all visiting users using IE will be infected when it automatically runs when they see the page
  4. Local network aware -- installs the exploit on locally writeable network shares
- All these exploits were known and patchable, but obviously not 100% of users can have 100% of patches installed at all times.

## Other Recent Attacks

Code Red -- like Nimda, but less sophisticated

Spread versions of worm used same random seed -- therefore they all checked the same hosts -- oops! Fixed in Code Red v. 2

I Love You, etc. -- just use email, disguise executable content to take advantage of IE, Outlook vulnerabilities

Solution: tools need to not execute content without specific action, warning, etc..

Other solutions: code signing, sandboxes

## "Warhol" Worm

"Warhol" worm -- cover the whole Internet in 15 minutes

Use a deliberate strategy to spread from infected to not-yet-infected hosts, without too much duplication or repetition of effort

Nicholas Weaver paper -- How to Own the Internet in your spare time

<http://www.cs.berkeley.edu/~nweaver/cdc.web/>