More on Malware
CS 136
Computer Security
Peter Reiher
March 4, 2008

Outline

- Introduction
- Viruses
- Trojan horses
- Trap doors
- Logic bombs
- Worms
- Botnets
- Spyware
- Some related topics
  - Hoaxes
  - Rootkits

Worms

- Programs that seek to move from system to system
  - Making use of various vulnerabilities
- Other performs other malicious behavior
- The Internet worm used to be the most famous example
  - Blaster, Slammer, Witty are other worms
- Can spread very, very rapidly

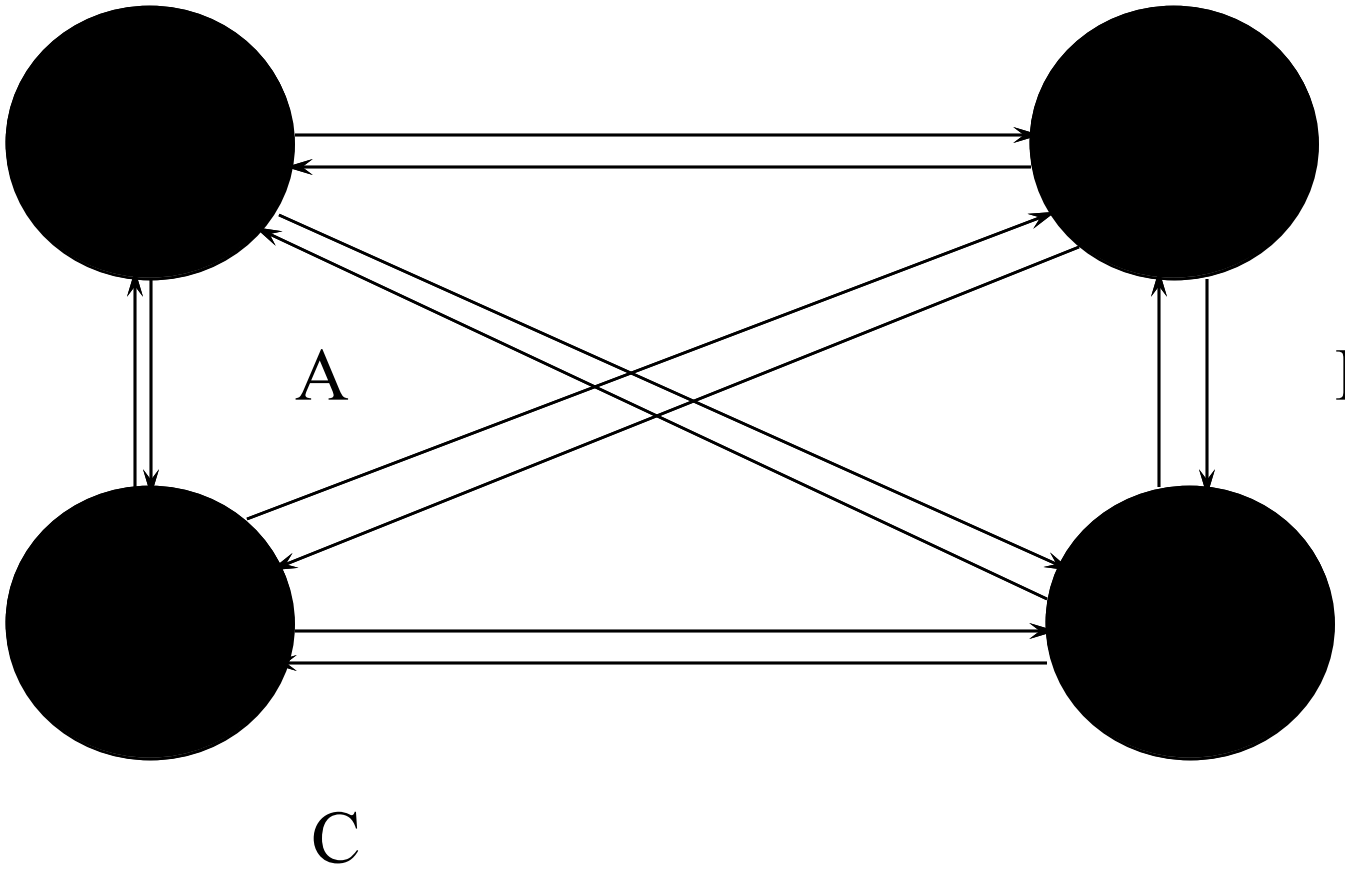
The Internet Worm

- Created by a graduate student at Cornell in 1988
- Released (perhaps accidentally) on the Internet Nov. 2, 1988
- Spread rapidly throughout the network
  - 6000 machines infected

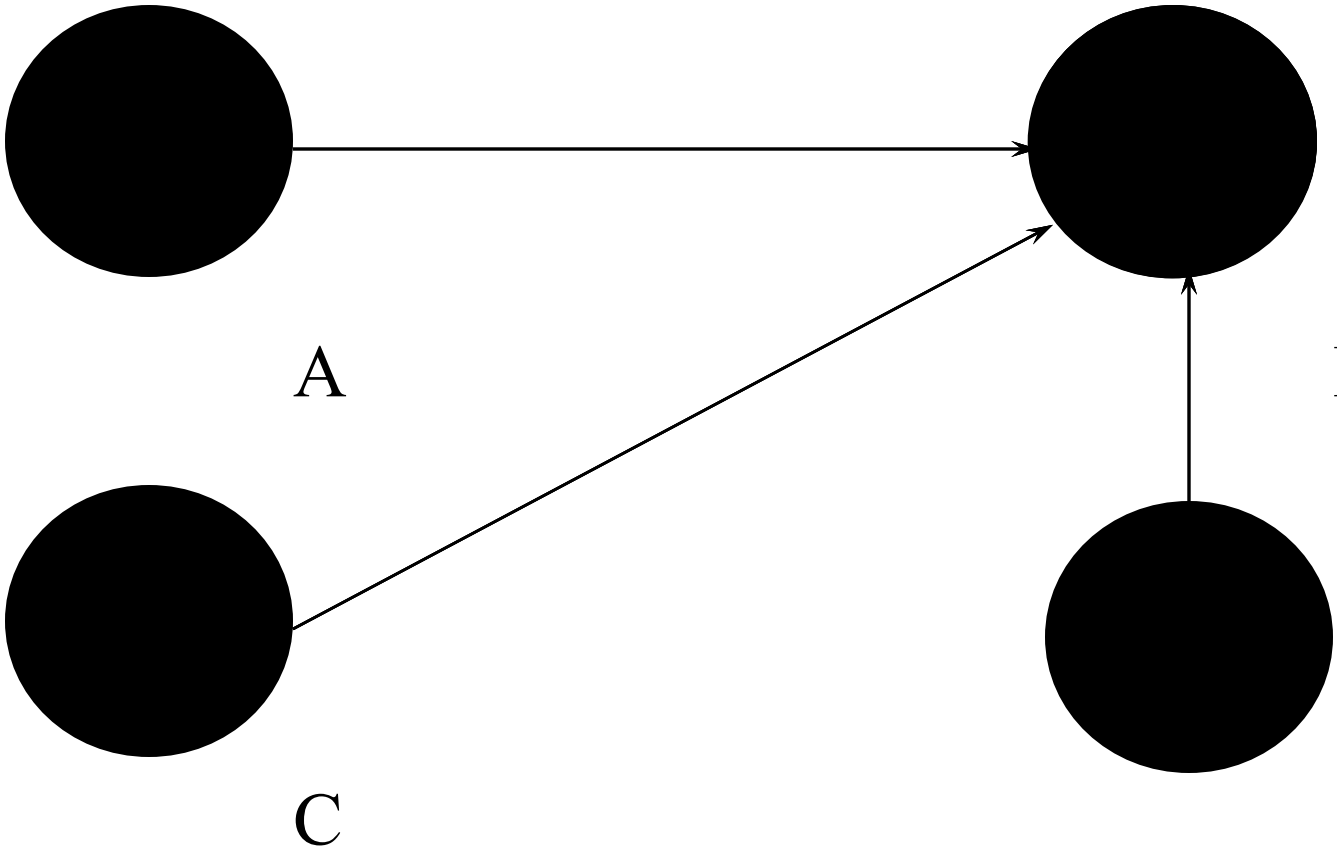
The Effects of the Worm

- Essentially, affected systems ended up with large and increasing numbers of processes devoted to the worm
- Eventually all processes in the process table used up
- Rebooting didn't help, since other infected sites would immediately re-infect the rebooted machine

A Visual Picture of the Infection



And What If Someone Reboots?



How Did the Internet Worm Work?

- The worm attacked network security vulnerabilities in one class of OS
  - Unix 4 BSD variants
- These vulnerabilities allowed improper execution of remote processes
- Which allowed the worm to get a foothold on a system

The Worm's Actions on Infecting a System

- Find an uninfected system and infect that one
- Using the same vulnerabilities
- Here's where it ran into trouble:
  - It re-infected already infected systems
  - Each infection was a new process

The Worm's Breaking Methods

- `rsh` - if the remote host is on the trusted hosts lists, simply `rsh`'ing could work
- `fingerd` - exploit a bug in the `fingerd` program to overwrite a buffer in a useful way
- `sendmail` - invoke a debugging option in `sendmail` and issue commands

What Didn't the Worm Do?

- It didn't attempt to intentionally damage a system
- It didn't attempt to divulge sensitive information (e.g., passwords)
- It didn't try hard to become root
  - And didn't exploit root access if it got superuser access

Stopping the Worm

- In essence, required rebooting all infected systems
  - And not bringing them back on the network until the worm was cleared out
  - Though some sites stayed connected
- Also, the flaws it exploited had to be patched

Effects of the Worm

- Around 6000 machines were infected and required substantial disinfecting activities
- Many, many more machines were brought down or pulled off the net
  - Due to uncertainty about scope and effects of the worm

How Much Did the Worm Cost?

- Hard to quantify
  - Typical for costs of computer attacks
- Estimates as high as $98 million
  - Probably overstated, but certainly millions in down time, sysadmin and security expert time, and costs of disconnections

What Did the Worm Teach Us?

- The existence of some particular vulnerabilities
- The costs of interconnection
- The dangers of being trusting
- Denial of service is easy
- Security of hosts is key
- Logging is important
- We obviously didn't learn enough

Santy Worm

- Exploited a vulnerability in phpBB software (2004)
- Cleverly used Google queries to automatically find systems to infect
- Infected 30,000-40,000
- Demonstrated innovation in finding infectable sites

Code Red

- A malicious worm that attacked Windows machines
- Basically used vulnerability in Microsoft IIS servers
- Became very widely spread and caused a lot of trouble

How Code Red Worked

- Attempted to connect to TCP port 80 (a web server port) on randomly chosen host
- If successful, sent HTTP GET request designed to cause a buffer overflow
- If successful, defaced all web pages requested from web server

More Code Red Actions

- Periodically, infected hosts tried to find other machines to compromise
- Triggered a DDoS attack on a fixed IP address at a particular time
- Actions repeated monthly
- Possible for Code Red to infect a machine multiple times simultaneously

Code Red Stupidity

- Bad method used to choose another random host
  - Same random number generator seed to create list of hosts to probe
- DDoS attack on a particular fixed IP address
  - Merely changing the target's IP address made the attack ineffective

Code Red II

- Used smarter random selection of targets
- Didn't try to reinfect infected machines
- Adds a Trojan Horse version of Internet Explorer to machine
  - Unless other patches in place, will reinfect machine after reboot on login
- Also, left a backdoor on some machines
- Doesn't deface web pages or launch DDoS

A Major Difference

- Code Red periodically turns on and tries to infect again
- Code Red II worked intensively for 24-48 hours after infection
  - Then stopped
- Eventually, Code Red II infected all infectable machines
  - Some are still infected, but they've stopped trying to spread it

Impact of Code Red and Code Red II

- Code Red infected over 250,000 machines
- In combination, estimated infections of over 750,000 machines
- Code Red II is essentially dead
  - Except for periodic reintroductions of it
- But Code Red is still out there

A Bad Secondary Effect of Code Red

- Generates lots of network traffic
- U. of Michigan study found 40 billion attempts to infect 8 fake "machines" per month
  - Each attempt was a packet
  - So that's ~1 billion packets per day just for those eight addresses
- "The new Internet locust[1]"

[1] Farnham Jahanian, talk at DARPA FTN meeting, Jan 18, 2002

Worm, Virus, or Trojan Horse?

- Terms often used interchangeably
- Trojan horse formally refers to a program containing evil code
  - Only run when user executes it
  - Effect isn't necessarily infection
- Viruses seek to infect other programs
- Worms seek to move from machine to machine

Storm Worm

- A mixed threat that isn't ideologically pure about how it gets around
- Uses Trojan horse methods, but also other techniques to spread
- Hundreds of thousands to millions of nodes infected by Storm
- And it's still going strong

What Does the Storm Worm Do?

- Spreads
- Also used for sending spam
  - Stock scams, on-line "pharmacies," etc.
- Launches denial of service attacks on sites it thinks are trying to analyze it
- Authors/controllers keep adapting it

Interesting Storm Features

- Stealth
  - Tries hard not to be noisy/intrusive
- Polymorphism
  - Changes its spreading payload frequently
  - Also has changed basic mechanism (PDF spam, e-cards, YouTube invites)
- Peer control structures
- Use of fast flux technology

Fast Flux

- Constantly changing DNS records
  - Given name serially maps to large number of different IP addresses
- Designed to make it hard to track down attackers
- Can change mapping of name to address every three minutes or so

Status of Storm

- Owners/controllers tracked down to Russia
  - Whose authorities are not cooperative
- Microsoft has issued patches to prevent spread and disinfect
  - Cleaning up ~200,000 machines per month
- Symantec estimates Storm only responsible for .25% of all infections in 2007

Botnets

- A collection of compromised machines
- Under control of a single person
- Organized using distributed system techniques
- Used to perform various forms of attacks
  - Usually those requiring lots of power

What Are Botnets Used For?

- Spam
- Distributed denial of service attacks
- Hosting of pirated content
- Hosting of phishing sites
- Harvesting of valuable data
  - From the infected machines
- Much of their time spent on spreading

Botnet Software

- Each bot runs some special software
  - Often built from a toolkit
- Used to control that machine
- Generally allows downloading of new attack code
  - And upgrades of control software
- Incorporates some communication method
  - To deliver commands to the bots

Botnet Communications

- Originally very unsophisticated
  - All bots connected to an IRC channel
  - Commands issued into the channel
- Starting to use peer technologies
  - Similar to some file sharing systems
  - Peers, superpeers, resiliency mechanisms
  - Storm's botnet uses peer techniques
- Stronger botnet security becoming common
  - Passwords and encryption of traffic

Characterizing Botnets

- Most commonly based on size
  - Reliable reports of botnets of tens of thousands of nodes
  - Less reliable reports of botnets with hundreds of thousands
- Controlling software also important
- Other characteristics less examined

What Do You Do About Botnets?

- A very good question
- Without any good answers, so far
- Hot topic for research for some years
- Without commensurate good answers coming from the research community

Why Are Botnets Hard to Handle?

- Scale
- Anonymity
- Legal and international issues
- Fundamentally, if a node is known to be a bot, what then?
  - How are we to handle huge numbers of infected nodes?

Possible Approaches to Handling Botnets

- Clean up the nodes
  - Can't force people to do it
- Interfere with botnet operations
  - Difficult and possibly illegal
- Shun bot nodes
  - But much of their activity is legitimate
  - And no good techniques for doing so

Spyware

- Software installed on a computer that is meant to gather information
- On activities of computer's owner
- Reported back to owner of spyware
- Probably violating privacy of the machine's owner
- Stealthy behavior critical for spyware
- Usually designed to be hard to remove

What Is Done With Spyware?

- Gathering of sensitive data
  - Passwords, credit card numbers, etc.
- Observations of normal user activities
  - Allowing targeted advertising
  - And possibly more nefarious activities

Where Does Spyware Come From?

- Usually installed by computer owner
  - Generally unintentionally
  - Certainly without knowledge of the full impact
  - Via vulnerability or deception
- Can be part of payload of worms
  - Or installed on botnet nodes

Some Related Topics

- Rootkits
- Hoaxes
- Honeypots and honeynets

Rootkits

- Software designed to allow a user to take complete control of a machine
- Assumes existing ability to run some code
- Goal is to go from foothold to complete control

Use of Rootkits

- Often installed by worms or viruses
- To completely control machines they have infected
- Generally replaces system components with compromised versions
  - OS components
  - Libraries
  - Drivers

Ongoing Rootkit Behavior

- Generally offer trapdoors to their owners
- Usually try hard to conceal themselves
  - And other nefarious activities
  - Conceal files, registry entries, network connections, etc.
- Also try to make it hard to remove them

Virus Hoaxes

- Virus hoaxes are at least as common as real viruses
- Generally arrive in email
- Usually demand instant action, on pain of something really terrible
- It's wise to check with a reliable source before taking action on such email messages
  - Or forwarding them

Honeypots and Honeynets

- A *honeypot* is a machine set up to attract attackers
- Classic use is to learn more about attackers
- Ongoing research on using honeypots as part of a system's defenses

Setting Up A Honeypot

- Usually a machine dedicated to this purpose
- Probably easier to find and compromise than your real machines
- But has lots of software watching what's happening on it
- Providing early warning of attacks

Uses of Honeypots

- To study attackers' common practices
- Very useful for tracking botnets
  - Get a honeypot machine to "join" a botnet
  - Allows inside look at its communications
  - Also gets you a copy of the botnet code

Can a Honeypot Contribute to Defense?

- Perhaps can serve as an early warning system
  - Assuming that attacker hits the honeypot first
  - And that you know it's happened
- If you can detect it's happened there, why not everywhere?

Honeynets

- A collection of honeypots on a single network
  - Maybe on a single machine with multiple addresses
- Typically, no other machines are on the network
- Since whole network is phony, all incoming traffic is probably attack traffic

What Can You Do With Honeynets?

- Similar things to what can be done with honeypots (at network level)
- Also good for tracking the spread of worms
  - Worm code typically knocks on their door repeatedly
- Main tool for detecting and tracking botnets
- Has given evidence on prevalence of DDoS attacks
  - Through *backscatter*
  - Based on attacker using IP spoofing

Do You Need A Honeypot?

- Not in the same way you need a firewall
- Maybe useful if you have a security administrator spending a lot of time watching things
- Or if your job is keeping up to date on hacker activity
- More something that someone needs to be doing
  - Particularly, security experts who care about the overall state of the network world