CS 161: Computer Security
Midterm 3 Review

Part 2

December 4, 2006

Malware

Worms and Viruses

- Worms vs. Viruses
  - Worms replicate and propagate on their own
  - Viruses need human interaction to propagate
  - Worms typically spread via network connections to vulnerable services
  - Viruses typically spread via email or files
- Infection vector
  - Network scanning, email, web sites, executables
- Payload
  - Install bot/rootkit, erase files, launch DDoS, steal information, send spam, serve web pages

Network scanning

- Choose random addresses
- Split up address space
- Pre-generated hitlists
- Propagation rates
  - Random Constant Spread (RCS) model:

$$a(t) = \frac{e^{K(t-T)}}{1 + e^{K(t-T)}} \tag{1}$$

  - $a(t)$ is fraction infected, K is initial compromise rate, T is start time constant

Detection and prevention

- Signatures
- Heuristics, hard-coded rules
- Anomaly detection
- Throttling

Targeted attacks

- Aimed at particular company/individual/organization
- One-of-a-kind means won't have a signature
- Sometimes used for corporate espionage

Botnets

- Network of compromised machines (can be huge)
- Rented out for evil purposes (DDoS, spam, phishing, etc.)
- Can be recruited by worm, virus, spyware

Operating System Security

Memory protection

- Private address space
  - Separate VM table for each address space (process)
  - A program can't even describe another program's addresses
- Kernel maintains page table; process can't alter it

Dual mode operation

- Hardware provides separate *kernel* and *user* modes
- Transition kernel $\rightarrow$ user
  - Create and initialize process address space, prepare hardware settings (registers, tables), switch mode and PC
- Transition user $\rightarrow$ kernel
  - Trap/interrupt (including system call)
  - Execute known code to handle request
  - Certain API, system calls, made available with limitations on functionality
  - All arguments must be checked thoroughly

Rootkits

The basics of rootkits

- Software and tricks to hide presence of malware
- Edit logs, change executables (`ls`, `top`, etc.), alter registry, even intercept system calls
- Hides existence to maintain access/control

How can you tell you've been rooted?

- Strange processes or files
- Extra network connections (seen from outside!)
- Changed configuration (registry, startup)
- Different sources give different information
- In general, very difficult to detect "in-box"

Elections and Electronic Voting

Security goals for an election

- Integrity: No fraud
- Transparency: Verify election conducted properly
- Privacy: No one learns about voter's choices
- Secrecy: Voter cannot prove how he/she voted

Security goals applied to DRE voting machines

- Integrity: Machine must allow each voter to vote once and prevent tampering
- Transparency: Machine should be verifiably trustworthy
- Privacy: Machine should randomize vote order
- Secrecy: Machine must not give receipt

Possible solutions for voting machine security

- Paper receipt dropped into audit box after voter verifies
- Machine prints ballot, which voter places in ballot box