CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

CECS 303: Networks and Network Security

Attack Vectors and Malicious Code

Chris Samayoa

Week 7 – 2nd Lecture
3/3/2022

Course Information

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

- CECS 303
  - Networks and Network Security – 3.0 units
- Class meeting schedule
  - TuTH 5:00PM to 7:15PM
  - Lecture Room: VEC 402
  - Lab Room: ECS 413
- Class communication
  - chris.samayoa@csulb.edu
  - Cell: 562-706-2196
- Office hours
  - Thursdays 4pm-5pm (VEC-404)
  - Other times by appointment only

Objectives

- Attack Vectors
- Malicious Code

Attack Vectors

- Trojan Horse
  - Extra code added manually to web page, program, plugin, etc.
- Viruses
  - Self-propagating (on execution)
  - Contains a malicious payload
- Worms
  - Self-propagating through process exploit.
  - Contains a malicious payload
- Penetration Tools (remote or local)
  - Exploits vulnerabilities to violate policy
  - Injection, Overrun, Logic, other
- Impersonation / Insider

General Actions - Payloads

- Modification of data
- Spying - exfiltration
- Stepping off point for further attacks
- Advertising – and tracking interests
- Self Preservation - Rootkits
- Subversion

Malicious Actions

- Taken when attack vector is activated
- Malware propagation (Viruses and Worms)
- Subversion – Back doors, changes to software base
  - Spyware – Exfiltration of history, data, etc.
  - Zombies or bots or botnets – Remote control of system
  - Extortion (Ransomware) - Destroy system or encrypt data and ask for ransom
  - Cryptocurrency miners
- Malicious code may go undetected if effect is delayed until some external event
  - A particular time
  - Some occurrence
  - An unlikely event used to trigger the logic

Defenses to Malicious Code

- Detection
  - Virus scanning
  - Intrusion Detection
- Least Privilege
  - Don’t run as root
  - Separate users ID’s
- Isolation
  - Mandatory controls on information flow
- Sandboxing
  - Limit what the program can do
- Backup
  - Keep something stable to recover

Categorizing Malicious Code

- How does it propogate??
- Trojan Horses
  - Embedded in useful program that others will want to run.
  - Covert secondary effect
- Viruses (n specialization of a Trojan horse)
  - Tries to propagate itself when the program is started
- Worms
  - Exploits vulnerabilities (bugs) to infect running programs
  - Infection is immediate

Trojan Horses

- People use programs because of a desired and documented effect
- Malicious payload
  - An “undocumented” activity that might be counter to the interests of the user
- Examples: Some viruses; much spyware
- Issues: How do you get a user to run your program?
  - Software that doesn’t come from a reputable source may embed trojans
  - Program with same name as one commonly used can be inserted in search path
  - Depending on settings, visiting a web site or reading an email may cause a program to execute

Computer Virus vs Real Virus

- Both self propagating
- Requires a host (program) to replicate
- Similar strategies
  - If deadly to start then it won't spread very far – it kills the host.
  - If infects and propagates before causing damage - can go unnoticed until it is too late to react

Viruses

- Resides within another program
  - Propagates itself to infect new programs (or new instances)
- May be an instance of Trojan Horse
  - Email requiring manual execution
  - Infected program becomes trojan
- Early viruses used boot sector
  - Instructions for booting system
  - Modified to start virus then system
  - Virus writes itself to boot sector of all media
  - Propagates by shared disks

Viruses (cont'd)

- Some viruses infect program
  - Same concept; on start, program jumps to code for the virus
  - Virus may propagate to other programs at this point
  - Virus may deliver payload
- Viruses via E-mail
  - Use mailbox and address book for likely targets
  - Mail program to targeted addresses
  - Forge sender to trick recipient to open program
  - Exploit bugs to cause auto execution on remote site
  - Trick users into opening attachments

Viruses (cont'd)

- How viruses hide
  - Encrypted in random key to hide signature
  - Polymorphic viruses changes the code on each infection
  - Some viruses cloak themselves by trapping system calls
- Macro viruses
  - Code is interpreted by common application such as word, excel, postscript interpreter, etc.
  - May be virulent across architectures

Zombies / Bots

- Machines controlled remotely
  - Infected by virus, worm, or trojan
  - Can be contacted by master / control server
  - May make calls out so control is possible even through firewall
  - Often uses IRC for control

Spyware

- Infected machines collect data
  - Keystroke monitoring
  - Screen scraping
  - History of URL's visited
  - Scans disk for credit cards and passwords
  - Allows remote access to data
  - Sends data to third party
- Spyware can be local
  - Targeted ads
  - Revenue for referring victim to merchant
  - Might rewrite URL's to steal commissions

Malicious Code - Issue

- Can not detect a virus by determining whether a program performs a particular activity
  - Reduction from the Halting Problem
  - Can use heuristics to fight this problem
- Defenses
  - Detection
    - Signature-based
    - Activity-based
  - Prevention
    - Prevent certain actions in an environment
    - Take action based on detection

Malicious Code - Defenses

- Detection
  - Signature-based
  - Activity-based
- Prevention
  - Prevent certain actions in an environment
  - Take action based on detection
- Sandbox
  - Limits access of running program
  - Program doesn’t have full access or even user-level access
- Detect Modifications
  - Signed executables
  - Tripwire or similar

Root Kits - Subversion

- Hide traces of infection or control
  - Intercept systems calls
  - Return false information that hides the malicious code
  - Return false information to hide effect of malicious code.
  - Some root kits have countermeasures to attempts to detect the root kits
  - “Blue Pill”

Malicious Code - Economics

- Botnets
  - Controlled machines for sale
- “Protection” or “recovery” for sale
- Attack software for sale
- Stolen data for sale
- Intermediaries used to convert online balances to cash
  - These are the pawns and the ones that are most easily caught

Summary

- Common attack vectors
  - Viruses
  - Worms
  - Vulnerabilities
  - Insider threat
- Knowing the “why” of the attack can help to define how to protect