CSF 434/534: Advanced Network and System Security

Week 03 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA SY0-501 Security+ Course Notes

Privilege escalation

Privilege escalation

Privilege escalation

- Gain higher-level access to a system
  - Exploit a vulnerability
  - Might be a bug or design flaw
- Higher-level access means more capabilities
  - This commonly is the highest-level access
  - This is obviously a concern
- These are high-priority vulnerability patches
  - You want to get these holes closed very quickly
  - Any user can be an administrator
- Horizontal privilege escalation
  - User A can access user B resources

Privilege escalation

Mitigating privilege escalation

- Patch quickly
  - Fix the vulnerability
- Updated anti-virus/anti-malware software
  - Block known vulnerabilities
- Data Execution Prevention
  - Only data in executable areas can run
- Address space layout randomization
  - Prevent a buffer overrun at a known memory address

DNS Poisoning and Domain Hijacking

DNS Poisoning and Domain Hijacking

DNS poisoning

- Modify the DNS server
  - Requires some crafty hacking
- Modify the client host file
  - The host file takes precedent over DNS queries
- Send a fake response to a valid DNS request
  - Requires a redirection of the original request or the resulting response

DNS Poisoning and Domain Hijacking

Domain hijacking

- Get access to the domain registration, and you have control where the traffic flows
- You don't need to touch the actual servers
- Determines the DNS names and DNS IP addresses
- Many ways to get into the account
  - Brute force
  - Social engineer the password
  - Gain access to the email address that manages the account
  - The usual things

DNS Poisoning and Domain Hijacking

Domain hijacking (example)

- Saturday, October 22, 2016, 1 PM
- Domain name registrations of 36 domains are changed
  - Brazilian bank
  - Desktop domains, mobile domains, and more
- Under hacker control for 6 hours
  - The bad guys became the bank
- 5 million customers, $27 billion in assets
  - Results of the hack have not been publicly released

Zero-day Attacks

Zero-day Attacks

Zero-day Attacks

- Many applications have vulnerabilities
  - We've just not found them yet
- Someone is working hard to find the next big vulnerability
  - The good guys share these with the developer
- Bad guys keep these yet-to-be-discovered holes to themselves
  - They want to use these vulnerabilities for personal gain
- Zero-day
  - The vulnerability has not been detected or published
  - Zero-day exploits are increasingly common
- Common Vulnerabilities and Exposures (CVE)
  - http://cve.mitre.org/

Zero-day Attacks

Zero-day vulnerabilities

- March 2017
  - CVE-2017-0199 - Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API
  - Open a Microsoft Office or WordPad file
  - SophosLabs documented attacks in the wild since November 2016
- June 2017
  - CVE-2017-8543 | Windows Search Remote Code Execution Vulnerability
  - Send a specially crafted SMB message to the Search service
  - Install programs, view/change/delete data, create new user accounts

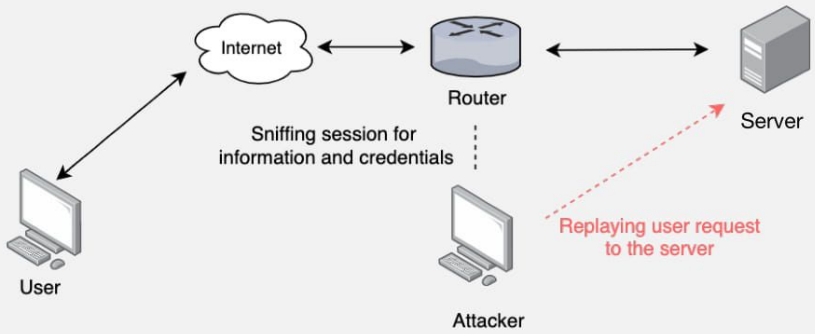
Replay Attack

Replay attack

Replay attack

- Useful information is transmitted over the network
  - A crafty hacker will take advantage of this
- Need access to the raw network data
  - Network tap, ARP poisoning, malware on the victim computer
- The gathered information may help the bad guy
  - Replay the data to appear as someone else
- This is not a MitM attack
  - The actual replay doesn't require the original workstation
- Avoid this type of replay attack with a salt
  - Use a session ID with the password hash to create a unique authentication hash each time

Replay attack



Client Hijacking Attacks

Client Hijacking Attacks

URL Hijacking

- Make money from your mistakes
  - There's a lot of advertising on the 'net
- Sell the badly spelled domain to the actual owner
  - Sell a mistake
- Redirect to a competitor
  - Not as common, legal issues
- Phishing site
  - Looks like the real site, please login
- Infect with a drive-by download
  - You've got malware!

Client Hijacking Attacks

Types of URL hijacking

- Typosquatting / brandjacking
  - Take advantage of poor spelling
- Outright misspelling
  - professormesser.com vs. professermesser.com
- A typing error
  - professormeser.com
- A different phrase
  - professormessers.com
- Different top-level domain
  - professormesser.org

Client Hijacking Attacks

Clickjacking

- You're clicking on a button
  - But you're actually clicking on something else
- Normal web page underneath
  - Invisible layer on the top

Clickjacking your phone

- May 2017
  - Georgia Institute of Technology report
- Cloak & Dagger
  - Android OS up to version 7.1.2
- Invisible information drawn over the screen
  - Monitor keystrokes and record user input

Client Hijacking Attacks

Browser cookies and session ID's

- Cookies
  - Information stored on your computer by the browser
- Used for tracking, personalization, session management
  - Not executable, not generally a security risk
  - Unless someone gets access to them
- Could be considered be a privacy risk
  - Lots of personal data in there
- Session IDs are often stored in the cookie
  - Maintains sessions across multiple browser sessions

Client Hijacking Attacks

Header manipulation

- Information gathering
  - Wireshark, Kismet
- Exploits
  - Cross-site scripting
- Modify headers
  - Tamper, Firesheep, Scapy
- Modify cookies
  - Cookies Manager + (Firefox add-on)

Client Hijacking Attacks

Prevent session hijacking

- Encrypt end-to-end
  - They can't capture your session ID if they can't see it
  - Additional load on the web server (HTTPS)
  - Firefox extension: HTTPS Everywhere, Force-TLS
- Encrypt end-to-somewhere
  - At least avoid capture over a local wireless network
  - Still in-the-clear for part of the journey
  - Personal VPN (OpenVPN, VyprVPN, etc.)
- Use session ID monitors
  - Blacksheep
  - Application-specific

Driver Manipulation

Driver Manipulation

Malware hide-and-go seek

- Traditional anti-virus is very good at identifying known attacks
  - Checks the signature
  - Block anything that matches
- There are still ways to infect and hide
  - It's a constant war
  - Zero-day attacks, new attack types, etc.

Driver Manipulation

Your drivers are powerful

- The interaction between the hardware and your operating system
  - They are often trusted
  - Great opportunity for security issues
- May 2016 - HP Audio Drivers
  - Conexant audio chips
  - Driver installation includes audio control software
  - Debugging feature enables a keylogger
- Hardware interactions contain sensitive information
  - Video, keyboard, mouse

Driver Manipulation

Shimming

- Filling in the space between two objects
  - A middleman
- Windows includes it's own shim
  - Backwards compatibility with previous Windows versions
  - Application Compatibility Shim Cache
- Malware authors write their own shims
  - Get around security (like UAC)
- January 2015 Microsoft vulnerability
  - Elevates privilege

Driver Manipulation

Refactoring

- Metamorphic malware
  - A different program each time it's downloaded
- Make it appear different each time
  - Add NOP instructions
  - Loops, pointless code strings
- Can intelligently redesign itself
  - Reorder functions
  - Modify the application flow
  - Reorder code and insert unused data types
- Difficult to match with signature-based detection
  - Use a layered approach

Spoofing

Spoofing

Spoofing

- Pretend to be something you aren't
  - Fake web server, fake DNS server, etc.
- Email address spoofing
  - The sending address of an email isn't really the sender
- Caller ID spoofing
  - The incoming call information is completely fake
- Man-in-the-middle attacks
  - The person in the middle of the conversation pretends to be both endpoints

Spoofing

MAC spoofing

- Your Ethernet device has a MAC address
  - A unique burned-in address
  - Most drivers allow you to change this
- Changing the MAC address can be legitimate
  - Internet provider expects a certain MAC address
  - Certain applications require a particular MAC address
- It might not be legitimate
  - Circumvent MAC-based ACLs
  - Fake-out a wireless address filter
- Very difficult to detect
  - How do you know it's not the original device?

Spoofing

IP address spoofing

- Take someone else's IP address
  - Actual device
  - Pretend to be somewhere you are not
- Can be legitimate
  - Load balancing
  - Load testing
- May not be legitimate
  - ARP poisoning
  - DNS amplification / DDoS
- Easier to identify than MAC address spoofing
  - Apply rules to prevent invalid traffic, enable switch security

Wireless Replay Attacks

Wireless Replay Attacks

Wired vs. wireless replay

- Similar to a wired replay attacks
  - Wireless doesn't change those attacks
- Wireless adds some additional capabilities
  - This is a big concern for the security professional
- Much easier to capture the data
  - Hotspots are generally in the clear
  - Just like tuning in to a radio station

Wireless Replay Attacks

Cracking WEP

- WEP - Wired Equivalent Privacy
  - A broken security protocol
  - Could not stop the replay of 802.11 packets
- ARP request replay attack
  - Cracking WEP requires thousands of Initialization Vector (IV) packets
  - Wait all day to collect IV information
  - Or replay a ton of ARPs and collect the IV packets
- Now you have many thousands of IV packets
  - You can crack WEP in seconds

Rogue Access Points and Evil Twins

Rogue Access Points and Evil Twins

Rogue Access Points

- A significant potential backdoor
  - Huge security concerns
- Very easy to plug in a wireless AP
  - Or enable wireless sharing in your OS
- Schedule a periodic survey
  - Walk around your building/campus
  - Use third-party tools / WiFi Pineapple
- Consider using 802.1X (Network Access Control)
  - You must authenticate, regardless of the connection type

Rogue Access Points and Evil Twins

Wireless Evil Twins

- Buy a wireless access point
  - Less than $100 US
- Configure it exactly the same way as an existing network
  - Same SSID and security settings
- Overpower the existing access points
  - May not require the same physical location
- WiFi hotspots are easy to fool
  - And they're wide open
- You encrypt your communication, right?
  - Use HTTPS and a VPN

Wireless Jamming

Wireless Jamming

Radio frequency (RF) jamming

- Denial of Service
  - Prevent wireless communication
- Transmit interfering wireless signals
  - Decrease the signal-to-noise ratio at the receiving device
  - The receiving device can't hear the good signal
- Sometimes it's not intentional
  - Interference, not jamming
  - Microwave oven, fluorescent lights
- Jamming is intentional
  - Someone wants your network to not work

Wireless Jamming

Wireless jamming

- Many different types
  - Constant, random bits / Constant, legitimate frames
- Data sent at random times
  - Random data and legitimate frames
- Reactive jamming
  - Only when someone else tries to communicate
- Needs to be somewhere close
  - Difficult to be effective from a distance
- Time to go fox hunting
  - You'll need the right equipment to hunt down the jam
  - Directional antenna, attenuator

WPS Attacks

WPS Attacks

Using WPS

- Wi-Fi Protected Setup
  - Originally called Wi-Fi Simple Config
- Allows "easy" setup of a mobile device
  - A passphrase can be complicated to a novice
- Different ways to connect
  - PIN configured on access point must be entered on the mobile device
  - Or push a button on the access point
  - Near-field communication
    - Bring the mobile device close to the access point
  - USB method - no longer used

WPS Attacks

The WPS hack

- December 2011 - WPS has a design flaw
  - It was built wrong from the beginning
- PIN is an eight-digit number
  - Really seven digits and a checksum
  - Seven digits, 10,000,000 possible combinations
- The WPS process validates each half of the PIN
  - First half, 4 digits. Second half, 3 digits.
  - First half, 10,000 possibilities. Second half, 1,000 possibilities
- It used to take about four hours to go through all of them
  - Lockout and slowdown functions have now been implemented
  - Takes one day to one week

WPS Attacks

Other WPS Attacks

- Walk up to the access point
  - Default PIN may be written on the device
  - Or just push the WPS button on the front
- Pixie Dust - Summer 2014
  - WPS PIN may be poorly encrypted
  - Based on the wireless chipset
  - Offline WPS brute force
  - Takes a few minutes or less
  - So much for slowdowns and lockouts
- WPS is just awful
  - Make sure it's disabled

CSF 434/534: Advanced Network and System Security

Week 03 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA SY0-501 Security+ Course Notes