



Security+

Domain 2: Threats, Vulnerabilities, and Mitigations

SY0-701

Brian Olliff

Defensive Engineering Instructor

Topics

Threat Actors
Attacker Motivations
Threat Vectors
Attack Surfaces
Vulnerabilities
Malicious Indicators
Mitigation
System Hardening

Learning Objectives

- Understand various types of threat actors and their motivations
- Explain common threat vectors and attack surfaces
- Be familiar with multiple types of vulnerabilities
 - + Hardware, software, physical, and cryptographic
- Understand how to use indicators to identify potential threats
- Explain how mitigation techniques can help secure an organization
- Understand various methods to secure and harden systems

Attackers



Threat Actors

- External - no account or authorization on network/system
 - Unskilled attacker -> well-funded nation states
- Internal - has been granted some level of authorization
 - Employees, vendors, business partners, etc
- All attackers have some sort of motivation & intent
 - Financial, political, curiosity, etc
 - Data theft, vandalism, etc
- Various levels of skill, funding, and resources
 - Unskilled using “commodity” malware and tools
 - Custom zero-day exploits, with government funding

Nation-state Actors

- Threat actor supported by resources of host country
 - Military, government, financial, etc
- Most developed countries have some sort of cyber attack capabilities
- Separated from host government/country
 - Unofficial support
 - Pose as “hacktivists” or independent groups, other countries
 - Provides plausible deniability to government
- Advanced Persistent Threat (APT)
 - Sophisticated, sustained attack by skilled threat actors
 - Frequently nation-state

Organized Crime

- Threat actor group, not necessarily tied to specific country
- Very similar to typical organized crime syndicates
 - Cyber attacks vs physical attacks
- May span multiple regions, jurisdictions
 - Complicates prosecution
- Common goals are financial profit
 - Carried out through financial fraud and extortion

Hacktivists

- Groups of threat actors motivated by political and social causes
 - Anonymous, WikiLeaks
- Common goals
 - Data theft with intention to release
 - Defacement of public sites
 - DoS (denial of service) attacks
- Attribution can be very difficult
- Often target political and financial groups
 - May also target media organizations and other companies
 - Targets depend solely on groups' goals

Unskilled Attackers

- “Script kiddies”
- Threat actors who may have minimal skills and knowledge
 - Can still cause significant harm and financial damage
- Normally use commonly available tools and malware
 - “Commodity malware” - can easily be purchased on dark web
- May not understand tools or tactics they are using
- Often have no specific target or goals
 - Gaining attention, proving their skills & abilities

Internal Threats

- Intentional insider threat
 - May have malicious intent, or acting on opportunity
 - Main motivations are often sabotage, financial gain, data theft
- Unintentional insider threat
 - Users without any malicious intent
 - Commonly exploited by external actors
 - Arise from lack of effective security training for employees
- Shadow IT
 - Individuals or departments introducing hardware/software without IT auth
 - Normally does not go through proper procurement process
 - Creates unmonitored, unsecured attack surface inside network

Attacker Motivations



Motivations

- Reason for attacking
 - Greed, curiosity, financial gain, political reasons, etc
- Different threat actors often have different motivations
 - Hacktivists - political motivations
 - Organized crime - financial motivations
 - Common for attackers to have multiple/overlapping motivations
- Service disruptions
 - Prevents organization from working normally
 - Can be sole purpose, or combined with other motives
- Data exfiltration
 - Stealing sensitive data, possible threat to release
- Disinformation
 - Posting false information, altering public websites, etc

Disruptions

- Early attacks - sole purpose was chaos
 - Defacing websites without any other purpose
 - Taking down networks
- Vandalism for its own sake occurs less now
- Disruption attacks often have other motives as well
 - Blackmail, political purposes
 - Nation-state attacks
 - Distraction to cover up other attacks
 - Revenge from insider (or former insider)

Financial

- Cyber attacks can be very profitable (if not caught)
- Data can be stolen and sold on dark web
- Blackmail
 - Demanding payment to prevent release of information
- Extortion
 - Demanding payment to prevent/stop attack
 - Common in modern ransomware attacks
- Fraud
 - Altering records/data for financial gain
 - Internal or external attackers

Political

- Attackers attempt to bring about some sort of change
- Nation-states
 - Disruption, exfiltration, etc against other nations/governments
 - Often used during times of war
 - Espionage commonly used even during peace times
 - Attempting to learn secrets, rather than use for financial gain
- Employees stealing/releasing data acting as whistleblowers
- Ethical or philosophical concerns from outside organizations
- Hacktivist organizations often have political motivations

Attack Surfaces



Attack Surface

- Any point where an attacker can exploit a vulnerability
- Network, hardware, software, etc
- Varies depending on type of threat actor
 - Internal vs external
- Goal in security - minimize the available attack surface
 - Restrict availability of endpoints, open network ports, vulnerable software
 - Proper monitoring in place for attack surface that is still available
- Common attack surfaces
 - Public firewall & open ports on firewall
 - Insecure networks (esp wireless)
 - Email systems
 - People

Insecure Networks

- Wireless
 - Improper SSID configuration
 - Non-enterprise security options
 - Open networks connected to enterprise network
 - Overpowered radio
- Wired
 - Improper port security and monitoring
- Bluetooth
 - Misconfigured/vulnerable devices
 - Often personal devices

Email

- Both an available attack surface AND attack vector
- Email systems require endpoint connected to internet
 - This endpoint is publicly accessible
 - Must have open ports for email traffic to flow
- Attackers send malicious files/links via email
 - Often use social engineering
- Attacks commonly target to use in further attacks
 - Compromised mailboxes and servers to send malicious emails
 - Servers to use in botnets
 - Use to gather information about organization and partners

People

- Hardest attack surface to secure
 - Technical controls can only go so far against social engineering attacks
 - Security training most important part
- Most people are naturally trusting
 - Must be trained to recognize malicious attempts
- Recognize suspicious emails and how to handle
- Don't click on unknown links, files
- Know how to handle suspicious phone calls
- Easy and convenient means of reporting any suspicious activity

Threat Vectors



Threat (Attack) Vector

- Path that an attacker takes to gain unauthorized access
- Attack surface and attack vector can overlap
 - Messaging systems
 - Wireless networks
 - People
- Common attack vectors
 - Removable storage
 - Software/hardware vulnerabilities
 - Unsupported or out-of-date systems
 - Images and malicious files
 - Open ports
 - Supply chain

Removable Storage

- USB thumb drives, portable HDs, memory cards, (less frequently) CDs
- Attackers can conceal malware on removable media
 - Run automatically when inserted
 - Run when application on drive launched
- USB drop attack
 - Attackers place removable media around specific locations
 - Relies on users picking up drive and inserting out of curiosity
- Attacks may run automatically, may require user action
 - If action required, social engineering to trick user
- Form of “lure-based” attack vector
 - Something interesting looking or attractive - prompts curiosity

Malicious Files

- One of most common methods for spreading malware
- Malware can be embedded in legitimate files
 - Weaponized applications
 - Macros in Word documents & PDF files
 - Steganography
 - Concealing information within other messages
 - Commonly used with image files
- Frequently combined with other vectors to deliver files
 - Email delivery
 - Removable storage

Messaging-Based Vectors

- Email
 - One of most common attack vectors
 - Phishing emails, malicious attachments and links in message body
- SMS
 - Frequently used to bypass MFA restrictions
 - Can also compromise mobile devices
 - Attackers send malicious links/files via SMS
- Instant Messaging
 - Similar to SMS, but available on more systems
 - Typically more secure than SMS, but can still contain vulnerabilities
- Social engineering is common thread among message vectors

Vulnerable & Unsupported Systems

- Attackers frequently look for and exploit vulnerabilities
 - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source - NIST
- Vulnerabilities are very common in all systems
 - Software & hardware
 - Zero-day - new vulnerability that is being exploited, no fix yet
- Unsupported systems
 - Not actively maintained or supported by vendor/manufacturer
 - Commonly do not receive security updates
 - Contain multiple vulnerabilities and outdated security measures

Network Vectors

- Open ports - should be restricted to only necessary ports
 - Any open port can be used as attack vector
 - VPN
 - Web server
- Wired networks
 - Unprotected physical network ports
 - Can allow eavesdropping, on-path (MITM), DoS attacks, etc
- Wireless networks
 - Compromised/cracked credentials
 - Spoofed AP names for credential harvesting other attacks

Network Vectors

- Bluetooth connections
 - Misconfigured/vulnerable devices
- Default credentials
 - Any device still using vendor-assigned username/password
 - Likely published in vendor documentation

Supply Chain

- Process for designing, manufacturing, distributing products/services
- Attackers can compromise one entity in chain
 - Potentially compromises rest of downstream
- Managed service provider (MSP)
 - Configures and manages IT infrastructure
 - Can be less expensive than in-house IT
 - Multiple angles to compromise (employees, systems, etc)
- Suppliers - purchases directly from manufacturer
- Vendor - purchases from supplier and sells to retail or customer
- Business partners
 - Two or more companies working together
 - Shared goals, marketing, etc
 - Can also be any of above roles

Social Engineering



Social Engineering

- “Hacking the human”
- Attempting to get information from someone or getting them to perform certain actions
 - Normally involves building/abusing some sort of trust or authority
 - May include sense of urgency
- Can be used for reconnaissance or intrusion purposes
- Examples
 - Carefully crafted email prompting to user to click link and enter credentials
 - Attacker calling user to obtain information
 - Attacker causing disruption at facility to perform physical intrusion
 - Carrying multiple items, asking someone to hold door open to secure area

Impersonation

- Pretending to be someone else
- Basis of most social engineering attacks
- Attackers will typically use one of two tactics
 - Persuasion - convince user that request is routine and should not refuse
 - Coercion - intimidation, sense of urgency, penalty for noncompliance
- Pretexting
 - Using carefully crafted story to attempt to convince or intimidate
 - Requires reconnaissance prior to attack

Phishing

- Email attack, commonly involving spoofed email addresses
 - May also originate from compromised, otherwise trusted addresses
- Designed to persuade/trick user into performing action
 - Clicking link, opening attachment, replying with information
- Frequently uses fake landing page with link in email
 - Shipping company, webmail page, etc
- Different levels targeting different individuals in organization
 - Spear phishing - attacker has some info, targets specific individuals
 - Whaling - phishing attack against senior leadership members (CEO, etc)
- Attackers use for multiple goals
 - Gathering credentials
 - Installing malware for persistence

Vishing and Smishing

- Vishing
 - Phishing attack conducted over the phone (voice phishing)
 - Similar tactics and goals as phishing
 - Normally used for gathering information (CC info, PWs, etc)
 - Attackers impersonate leadership, helpdesk, etc.
 - Attackers may use to compromise internal helpdesk, posing as users
 - Use of deep fake technology will likely increase these attacks
- Smishing
 - Phishing attack performed over SMS channels (SMS phishing)
 - Very similar goals and tactics as others, with different attack vector
- Pharming
 - Redirecting from legitimate website to malicious site

Business Email Compromise

- More sophisticated campaign than normal phishing attacks
- Attackers pose as employee, vendor, etc.
 - Likely has performed recon prior to attempting attack
- Often have financial motivations
 - Persuade user with access to finances to perform/auth fraudulent transaction
 - Purchase gift cards and send codes
 - Pay fake invoice
- May involve brand impersonation
 - Duplicating logos, formatting, websites, etc
 - Attempt to get fake site ranked higher in search engines
 - Use of dis/misinformation to convince users to visit fake site

Typosquatting

- Addresses (normally domain names) registered very similar to others
 - Can be difficult to identify due to font in address bar or email clients
- Take advantage of user error with spelling mistakes, typos, etc.
 - Also exploit tendency to overlook minor errors when in a hurry
- Examples:
 - Used as phishing link
 - gmail.com -> grnail.com
 - Taking advantage of typos
 - google.com -> gooogole.com or gogle.com
 - microsoft.com -> micorsoft.com

Watering Hole

- Relies on group of targets using same third-party site
- Attacker must first compromise site to deliver malware
- Lower risk for attacker
 - Does not need to directly interact with targets
- Target visits compromised site
 - Normally multiple individuals with same organization or industry
- Site delivers malware, which then potentially infects organization

Vulnerabilities



Zero-day Vulnerabilities

- Brand new vulnerability
- Exploited before patch or fix is available
 - Often before vendor is aware
- AV/EDR software may not be able to detect exploit
- EternalBlue (MS17-010)
 - NSA developed exploit, leaked publicly in 2017 by Shadow Brokers
 - Reportedly used for 5 years before leak
 - Exploited vulnerability in SMB
 - WannaCry ransomware
- Extremely valuable to attackers (financially and operationally)
 - Frequently used in advanced & high-value attacks

Misconfigurations

- Many attacks are the result of improperly configured systems
- Default settings and passwords
- Insecure administrative accounts
 - Should use very secure passwords and MFA if possible
- Improper permissions
- Excessive open ports
 - Local (device/OS-level) and network firewalls to block unnecessary ports
- Unsecure protocol usage
 - Especially for management purposes (SSH vs telnet, SFTP vs FTP, etc)
- Temporarily disabling security settings while troubleshooting
- Not using effective change management processes

Supply Chain Vulnerabilities

- Every organization relies on suppliers and vendors for services/products
 - Creates a chain of companies relying on other companies - supply chain
 - Any part of this chain can become compromised
- Attack/compromise upstream in chain will have downstream effects
 - Firewall vendor compromised, delivers exploited software to customers
- Mitigation requires careful vendor selection, management, and oversight
 - Security audits & certification (usually by third-party)
- NotPetya (2017)
 - Ukrainian tax preparation program (M.E.Doc) servers compromised
 - Attackers introduced backdoor into the software
 - Updated (compromised) software pushed out to customers

Supply Chain Vulnerabilities

- Service providers
 - Any entity that provides an external service for organization
 - Cloud providers, 3rd party developers, etc
- Hardware suppliers
 - Used by all organizations
 - Compromises before hardware purchase are difficult to detect
 - Firmware, low-level drivers, intentional backdoors
- Software providers
 - Software bill of materials (SBOM)
 - Inventory of all components in a specific product
 - Provides transparency into supply chain

Mobile Vulnerabilities

- Sideloading
 - Typically only associated with Android devices
 - Installing applications from sources other than official app stores
 - Apps not scanned or verified, pose significant risk to org
- Jailbreaking
 - Removing limitations on iOS devices to gain full access to device
- Mobile device management (MDM)
 - Can monitor and control devices that have access to org resources
 - Capable of blocking devices with certain configurations

Cryptographic Vulnerabilities

- Any sort of weakness in system, protocol, or algorithms
 - Example: using MD5 or SHA-1 for hashing
- Usage of weak keys
 - Easier to brute force and crack
 - DES - uses 56-bit key
 - RSA - strong algorithm, but using small key sizes negates that
- Key security
 - Protecting keys using in cryptography is crucial
 - Using HSM or KMS can help protect
 - Ensure proper workflows and key lifecycle procedures
 - Monitor access to keys

Application & Web Vulnerabilities



Application Vulnerabilities

- Memory injection
 - Security flaw - attackers can inject malicious code into app process memory
 - Specifically designed code to provide unauthorized access, etc
 - Injected code runs with same privilege level as application
 - Can result in full system compromise
- Buffer overflow - type of memory injection attack
 - Buffer - area of memory reserved by application to store expected data
 - Passes data to deliberately “overflow” the reserved space
 - Can allow attacker to destabilize or run arbitrary code on system
 - Modern hardware and OS can provide effective mitigation

Race Conditions

- Software flaw with timing or order of events in applications
 - May be manipulated by attackers
- Software logic may fail to check/enforce expected order
 - Can result in data corruption, unauthorized access, etc
- Time-of-check to time-of-use (TOCTOU)
 - Type of race condition vulnerability
 - System state changes between check and use stages
- Normally require mitigation by developers

Operating System Vulnerabilities

- Most application exploits run in context of user application was run as
- OS exploits more likely to run as system- or kernel-level
 - More likely to provide privilege escalation capabilities
 - Can result in easy full control/compromise of system by attacker
- Identify through
 - Security bulletins from vendor (Microsoft, Apple, Linux distro)
 - Vulnerability scans
 - Threat intelligence

SQL Injection (SQLi)

- Structured Query Language
 - Read/write information in a database
- Web servers send queries to DB server and return responses
- SQLi attack
 - Attacker modifies query by adding specific code to input on webpage
 - Allows execution of attacker's SQL query
- Can allow attacker to extract sensitive information from DB
 - Delete, update information
 - Possibly execute code
- Best defense is stored queries and input sanitization

Cross-Site Scripting (XSS)

- Scripts are part of most modern websites
- Browsers tend to trust scripts on trusted websites
- XSS attacks insert malicious scripts that appear to be part of website
 - Normally through input fields that do not validate input
- Nonpersistent (Reflected)
 - Attacker creates link to perform injection against trusted site
- Persistent (Stored)
 - Attacker inserts code into backend of site
 - Submitting a post to forum that contains malicious code
- DOM Based (Document Object Model)
 - Does not modify the site, but modifies behavior of user's browser
 - Specially crafted URL from attacker results in page executing differently

Cloud-specific

- Most cloud services operate on “shared responsibility” model
 - Cloud provider responsible for security of the cloud services themselves
 - Organization responsible for security of systems & data in cloud service
- Organization responsibilities
 - Ensure data properly secured (same as on-premise)
 - Compliance requirements
 - Third-party and vendor access
 - Configuration of purchased services
- Other vulnerabilities are cloud provider responsibility
 - Hardware and firmware patches
 - Underlying software vulnerabilities

Cloud Access Security Brokers (CASB)

- Provides visibility into how users/devices use services
 - Monitor users/audit activity
 - Can scan for malware, rogue devices, etc.
 - Help prevent data exfiltration
- Forward proxy
 - Installed on enterprise network perimeter
 - May require configuration of devices
 - Can scan all traffic, but may reduce performance
- Reverse proxy
 - Installed at cloud provider edge
 - Requires provider support
- API (Application programming interface)
 - Provides extra functionality and integration

Hardware & Virtualization Vulnerabilities



Hardware Vulnerabilities

- Firmware
 - Vulnerabilities not limited to just applications - BIOS/UEFI vulns exist
 - All hardware uses firmware, all can have vulnerabilities
 - Can be much more difficult to patch or mitigate
- End of life (EOL)
 - System or application is no longer supported by the vendor/developer
 - Or reaching this point
 - All products (hardware, software) reach this phase at some point
 - No more feature or security updates (usually)
 - Extended support may be available (LTS)
- Legacy - outdated technology, use continues
 - Similar to EOL, but may still receive support
 - Usually no LTS available

Virtual Machine Escape

- Malware running on a guest machine can “escape” to another guest or VM host
- Attacker first must identify the machine they are on is virtualized
 - Multiple ways to perform this (fingerprinting, timing attacks, etc)
- Exploit vulnerable hypervisor
- Permits attacker to access other VMs running on the same host
- Can also allow them access to the network, depending on configuration
- Mitigations
 - Monitor vendor notifications, patch as necessary (always consider critical)
 - Do not host sensitive servers on same hardware as lower security
 - Properly architect network to limit connectivity

VM Resource Reuse

- Virtual machines commonly use shared resources
 - Disk, memory, etc
- When deleted/migrated, resources may not be properly sanitized
 - Process varies based on infrastructure
- Can result in sensitive data being leaked between VMs
 - Old data from deleted VM could be accessed by new VM
- Mitigate risk
 - Effective data sanitization practices
 - Data encryption with proper key management
 - Effective data management lifecycle

Malware Attacks



Malware

- Software that does something bad, from user perspective
 - Malicious software
- Various classifications of malware
 - Virus, worms
 - Trojans
 - Ransomware
 - Potentially unwanted programs (PUPs)
 - Adware/spyware
 - Remote access trojan (RAT)
 - Rootkits
 - Logic bombs

Viruses

- Virus - malware that can copy itself (replicate) and spread
 - Often without knowledge of user
- Non-resident or file
 - Virus contained and runs in executable process
 - May try to infect other files as well
- Memory-resident
 - Virus runs from original executable, remains in memory after process ends
- Boot
 - Code written to boot sector of disk, executes when OS starts
- Script and macros
 - Powershell, VBS, WMI, PDF w/JS, etc.

Worms

- Memory-resident malware
 - Fileless - does not write *itself* to disk
 - “Live off the land” - makes use of legitimate system tools
- Runs without user intervention
 - Virus requires user to run
 - Worm can run by exploiting vulnerabilities automatically
- Replicates across various medium
 - Network resources/shares
 - Removable storage
- Often designed for DoS attacks and other disruptions
 - May carry other payloads

Ransomware

- Malware that attempts to extort victim for money to recover data
 - Most will encrypt and only provide decryption after payment
 - Crypto-ransomware
 - Some is only threatening, without blocking access
- Will prominently display notice(s) demanding payment or other action
- Encryption-based can only be remediated by restoring data
 - Possibly by paying ransom - but almost never recommended
 - Sometimes illegal
- Demand payment via various methods, often cryptocurrency

Wana Decrypt0r 2.0



Ooops, your files have been encrypted!English

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
CMT from Monday to Friday

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

 **bitcoin**
ACCEPTED HERE

Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMwCopy

Check PaymentDecrypt

Remote Access

- Trojan
 - Program that hides execution of other processes, usually malicious
- RAT - Remote Access Trojan
 - Remote Administration Tool
 - Provides attacker with backdoor access to system
 - May be used to install bots and connect to botnet
- Command & Control
 - Attacker controlled infrastructure that compromised systems connect to
 - C&C or C2
 - Often use disguised DNS or HTTPS traffic to hide usage

Potentially Unwanted Programs (PUP)

- Not all are malicious or cause harm
- Tracking cookies
 - Embedded into most websites, allow various tracking and analytics
- Adware
 - Form of bloatware - may reconfigure browser
 - Allow cookies, change search provider, open sponsor pages, etc
- Spyware
 - Designed to collect data and monitor system usage
 - Can take screenshots or activate microphones and webcams
 - Keyloggers - records all keystrokes
 - Hardware and software
 - May store locally, or upload to other location

Advanced Malware

- Rootkit
 - Malware that can run as unrestricted system processes
 - Can compromise critical system files and be difficult to detect
 - High level of access results in effective masking, difficult discovery
 - Often erases logs to hide evidence of infection
 - Modern OSes have mechanisms to help prevent
- Logic bomb
 - Malware designed to not run immediately
 - Can wait for predetermined date/time or specific event before executing
 - Not necessarily typical malware
 - Disgruntled system admin leaving a scripted trap

Physical & Network Attacks



Physical Attacks

- Any attack targeting physical infrastructure
 - Hardware, cabling, facilities, etc.
- Brute force
 - “Hit it with a hammer” attack
 - Smashing physical locks
 - Breaking into wiring closets/cabinets, buildings, etc
- Environmental
 - Cutting cables (electrical, network, etc)
 - Disrupting cooling systems
 - Typically DoS goals
- RFID cloning
 - Making copies of existing RFID access card
 - Skimming - using counterfeit reader to capture card info

Distributed Denial of Service (DDoS)

- Denial of service (DoS) - attack designed to disrupt systems
 - Consuming available bandwidth, system resources, etc
- Distributed - DoS attack from multiple locations, systems
 - Typically involves botnet
- Amplified
 - Request portion of attack small, but requests large amount of data
 - NTP - small query to request last 500 machines that contacted
- Reflected
 - Attacker spoofs target's IP address
 - Sends request to (often third-party) site, with fake reply IP
 - Server then sends reply to target's IP
- Combined amplification/reflection attacks

DNS Attacks

- On-path
 - ARP poisoning to respond to DNS queries with spoofed replies
- Client cache poisoning
 - Modifying local hosts file to redirect domains to attacker controlled IP
 - Most OS check hosts file before querying DNS server
- DNS Server cache poisoning
 - DoS attack against DNS server
 - Spoof replies to requests destined for attacked server
 - Force DNS server to query authoritative server
 - Attacker spoofs authoritative server and sends malicious replies
 - May also include numerous fake records

Wireless Attacks

- Rogue AP
 - Access point installed on network without authorization
 - May not be malicious intent
 - Evil twin - rogue AP masquerading as legitimate AP
- Disassociation attack
 - Forcing victim device(s) to disconnect from wireless network
 - DoS purpose or may also involve replay attack
 - After disconnection, client attempts to reconnect
 - Attacker attempts to capture network keys
- Jamming
 - Rogue AP with more powerful radio, or dedicated device
 - Often implemented alongside replay attacks

On-Path Attacks

- Attacker gains position between two devices on network
 - Attacker controls resource on network
 - Able to capture, monitor, and relay traffic between hosts
 - Capable of modifying traffic
 - DNS responses
 - Website traffic
- Can be launched at any network layer
 - ARP poisoning broadcasts ARP replies
 - ARP has no security controls, so all ARP information is trusted
- Can also be called adversary-in-the-middle attack

Credential Replay

- Mostly target Windows AD networks (in network attack context)
- LSASS (Local Security Authority Subsystem Service) caches secrets
 - Cached in memory and SAM (Security Account Manager) database
 - Kerberos TGT/session key
 - Service tickets
 - NT hash of accounts recently signed in
 - Secrets are commonly purged soon after user logs out
- Attackers can gather these secrets to perform various attacks
- Disabling legacy NTLM auth can help mitigate some attacks
- Windows Credential Guard helps protect
- Mitigations
 - Up to date patches
 - Proper security hardening and controls

Application-based Attacks



Privilege Escalation

- Attackers' goals are to gain as much access as possible
 - Usually to run some sort of malicious processes
 - Arbitrary code execution
 - Remote code execution (RCE)
- When first compromising system, permissions may vary
 - Depend on how compromise was performed, application/user level, etc
- Vertical privilege escalation (elevation)
 - User or application can access data that should not be available
 - Usually performed through vulnerability exploitation
- Horizontal privilege escalation
 - Accessing functionality or data that is intended for another user

Buffer Overflow

- Attacker submits input/data too large to be stored in designated space
 - May result in application/system crash
 - Carefully crafted may allow for code execution
- Stack overflow is one of most common
 - Stack - specific area of memory used by subroutine
 - Includes return address - local of program that called subroutine
 - Attack uses buffer overflow to modify return address
 - Allows attacker to run arbitrary code
- Modern operating systems have various protections
 - Address space layout randomization (ASLR)
 - Data Execution Protection (DEP)

Replay Attacks

- Common technique used to gain access in web applications
 - Often used to to compromise session tokens/cookies
- Cookie
 - Name and value, may also have security and expiration info
 - Nonpersistent - stored in memory, deleted when browser closed
 - Persistent - stored in browser cache until deleted or expired
 - Frequently used for session verification (HTTP is stateless)
- Attackers can gain access to session cookies
 - Compromised browsers, on-path attacks, brute force, etc
- Submit stolen cookie to re-establish a session as user

Forgery

- Hijacking an authenticated session without user's consent
- Cross-site request forgery (CSRF)
 - Can exploit apps that uses cookies to authenticate users
 - Attacker convinces user to start session with legitimate target site
 - Sends an HTTP request to victim browser
 - Spoofs legitimate action on target site
 - Since user is authenticated, request is accepted - even though malicious
- Server-side request forgery (SSRF)
 - Cause server to process request that targets another service
 - Ex: front-end web server requesting from DB server
 - Exploits lack of authentication between services, and weak input validation

Injection Attacks

- Exploits insecure ways that applications may process requests/queries
- Persistent XSS and SQLi are types of injection attacks
- XML injection
 - Extensible Markup Language
 - Used by apps for various data exchange
 - If transmitted without encryption or validation
 - vulnerable to spoofing, forgery, code injection
- LDAP injection
 - Lightweight Directory Access Protocol
 - Can be exploited (if unauthenticated requests allowed)
 - Modify settings
 - Create/delete/modify accounts
 - Gather intelligence, bypass controls

Directory Transversal

- Type of injection attack against a web server
- Allows attacker to gain access to files outside of web server directory
 - Submitting different path in input field
 - ../ (parent directory)
 - ../../../../etc/config
- Canonicalization attack
 - With some input validation, ../../ may not be permitted
 - %2e%2e%2fetc/config may be allowed
- Requires proper permissions and input validation to mitigate

Cryptographic & Password Attacks



Cryptographic

- Downgrade attack
 - Requesting a server use a lower specification protocol
 - Weaker ciphers and smaller key lengths
 - Often used to facilitate an on-path attack
- Collisions
 - In hashing, where two different inputs result in the same hash value
 - Often used to forge digital signatures
- Birthday attack
 - Birthday paradox - How large must a group of people be so that the chance that two of them share the same birthday is 50%? (23)
 - Attack - process of creating two files/documents/etc, with minor changes
 - Chance of matching hash outputs can be greater than 50%, depending on changes

Online vs Offline Password Attacks

- Online attack
 - Attacker interacts with service/app directly
 - Can show up in audit logs as multiple failed logins
 - Followed by successful login if attack succeeds
- Offline attack
 - Attacker does not directly interact with resource
 - Obtains copy of password hash database
 - Attacker then uses brute force methods to attempt to crack passwords
 - Only indicator would be file access log

Password Attacks

- Password spraying
 - Online attack
 - Attacker uses a list of passwords and tries them against multiple accounts
 - Passwords often from list of compromised passwords
 - Also use common, frequently used passwords
- Brute force
 - Online or offline attack
 - Password attempts using every possible combination of characters
 - Effectiveness is determined by org password requirements
 - Can take an extended amount of time to crack passwords, if successful
- Dictionary attack
 - Uses list of known, non-complex values to guess password
 - Can be coupled with brute force attack

Indicators of Compromise



TTPs

- Tactics, techniques, and procedures
- Tactic
 - High-level description on behavior (recon, persistence, privilege escalation)
- Techniques
 - More detailed description
 - Reconnaissance via social media scraping or port scanning
- Procedures
 - Exactly how the attack is performed
 - What tool is used and how it is used

Indicators

- Indicator of compromise (IoC)
 - Some sign that a network or asset is actively being attacked (or has been)
 - Evidence of a tactic, technique, or protocol
- Thousands of different possible IoCs
 - New ones constantly discovered and released
 - Documented and published by numerous threat researches
- Examples
 - Connection logs to C2 servers
 - Disabled backups
 - Deleted or modified logs
 - Changed registry settings

Malware Indicators

- AV/EDR alerts
 - May only detect most obvious malware, not more covert types
- Excessive resource usage
 - CPU, memory, disk
 - Does not necessarily indicate malicious activity
- Resource inaccessibility
 - Typically indicates a DoS attack
 - Multiple resources could indicate ransomware
- File system indicators
 - Malware may not always run from disk, but still modify files/registry
 - Logs showing restricted files/resources with access attempts

Malware Indicators

- Account compromise indicators
 - Account lockouts - may be legitimate
 - Concurrent session usage
 - Impossible travel
 - Account logged in at office; 5 minutes later, another continent
- Logging
 - Missing or altered logs - typically easy to detect
 - Individual log entries removed
 - Spoofed log entries
 - Out-of-cycle logging
 - Manipulated logs to alter timestamps
- Sandbox detonation/execution
 - Useful for manually gathering indicators for suspected malware

Specific Indicators

- DNS
 - Event logs on DNS server
 - Types of queries individual hosts perform, including source IP
 - Anomalies in traffic behavior
- Malicious code
 - Presence or use of shellcode
 - Minimal pieces of code written to exploit vulnerabilities
 - Usually followed by network traffic to download additional payload
 - Credential dumping
 - Accessing or attempting to copy password databases
 - Use of PSEXec or suspicious PowerShell
 - Persistence in form of autorun, scheduled tasks, WMI subscriptions, etc

URL Analysis

- Can assist in identifying session hijacking and replay, forgery, injection
- Actions can be encoded into URL
 - GET - retrieve some resource from server
 - POST - send data to server for processing
 - PUT - create or replace data on server

`http://trustedsite.com/upload.php?post=DATA`

- Data may be obfuscated or otherwise encoded
- URLs can only contain certain characters
 - Percent encoding used to submit other characters
 - %21 = !, %2A = *

Mitigation Techniques



Least Privilege

- Central concept behind security hardening and controls
- Only grant minimum permissions necessary, nothing more
- Requires auditing roles, responsibilities, privileges
 - Understand what each individual needs to perform their job
 - Controls and permissions adjusted to adopt least privilege
- Regular reviews of rights to remove unnecessary permissions
 - Old accounts that are no longer used
 - Permissions that are no longer required
- Role based access controls (RBAC)
 - Permissions assigned based on predefined roles
 - Users assigned to role, which receive inherited permissions

Network Segmentation

- Practice of physically or logically separating parts of network
 - Reduce attack surface, limit spread of traffic
- Systems divided into segments or subnets
 - Each will have its own distinct controls and permissions
- Goal to complicate attacker's efforts
- Provides more granular control over data access
- Methods
 - Physically separated networks
 - VLANs (Virtual LANs), ACLs
- Device isolation
 - Segregation of individual devices within network
 - Limits and restricts network interaction to prevent spread of threats

Monitoring

- Monitoring is critical step in mitigation and hardening
- Helps enforce and maintain security controls
 - Assists with ensuring controls stay in place and are effective
- Detect changes that may weaken hardened config
 - Disabled service is enabled
 - Port that was previously blocked now listening
- Data for compliance and auditing
 - Supported by logging systems
 - Status reports that endpoints still have required configurations

ACLs (Access Control Lists)

- List of rules/entries that specify allowed/denied actions & traffic
 - Enforce access control policies
- Network and file system security purposes
- Each entry contains
 - Subject/object that permissions apply to
 - Associated permissions or other qualifiers
 - Allow or deny
 - Order of ACLs is important
- File systems
 - Each object has an associated ACL
 - Contains list of principals and permissions
 - Used & enforced in multiple types of file systems

Decommissioning

- Devices and systems constantly retired
- Often still contain data, some potentially sensitive
 - Including specific system configurations - could be exploited
- Documented process when system retired
 - Securely erase all sensitive data
 - Reset devices to factory defaults
 - Update inventory systems
- Same principles apply no matter what type of system/device
 - Individual hard drives
 - Full systems with integrated storage
- May involve physical destruction of components

Endpoint Mitigation and Protection



Application Allow & Block Lists

- Allow list
 - Applications cannot run without being in list
 - “Deny unless listed”
 - Component of least privilege model
 - Can result in some necessary applications not functioning properly
 - Especially after updates
 - Implementation requires risk analysis, business impact analysis, etc
- Block list
 - All applications allowed, except those in list
 - “Allow unless listed”
 - Easier to manage, but higher risk

Configuration Enforcement

- Methods to ensure devices adhere to security configurations
- Required capabilities
 - Standardized baselines
 - NIST, CSF, etc
 - Used for benchmarking how systems should be configured
 - Automated configuration management tools
 - Apply and maintain standardized configuration baselines
 - Continuous monitoring and compliance checks
 - Detect deviations from baseline
 - Change management
 - Configuration changes properly reviewed, tested, approved

Patching

- Every system, device, application will require updates
 - New features, bug fixes, vulnerability remediation, etc
- Smaller networks may use auto update on each individual system
 - Can introduce performance issues
- Larger organizations require patch management systems
- Careful testing of patches and updates, in isolated environment
 - Compatibility issues
 - Flaws in patches, bug introduction
 - Supply chain attacks
 - Other new vulnerabilities
- Downtime scheduling often required
- Legacy & proprietary systems many need compensating controls

Encryption

- Full disk encryption - entire contents of drive encrypted
 - Encryption usually performed by OS
 - Requires storage of key, normally in TPM
 - May also be able to use USB storage for key - not as secure
 - Recovery password/key for use if drive moved or TPM damaged
- Self-encrypting drives (SED)
 - Encryption operations handled by drive instead of OS
 - Uses symmetric data/media encryption key (DEK/MEK) for data encryption
 - DEK encrypted with asymmetric key pair - authentication key (AK)
 - Also called key encryption key (KEK)
 - Authenticated by user password
- Removable/portable device encryption

System Hardening Techniques



Endpoint Protection Clients

- Anti-Virus (AV)
 - Mostly signature-based detection of multiple types of malware
- Endpoint Detection & Response (EDR)
 - Greater protection and featureset than AV
 - Designed to analyze and contain malware, prevent spread
- Data Loss Prevention (DLP)
 - Designed to prevent removal of sensitive data from organizational control
 - Enforces policies to prevent copying, emailing, printing, etc
- Planning and best practices
 - Create deployment plan with standardized configurations
 - Automate initial deployment and updates/patches
 - Monitor clients for alerts and to ensure operation
 - Centralize management

Encryption

- Full disk encryption (FDE)
 - Entire drive fully encrypted
 - Helps protect any locally stored data in case of theft
 - BitLocker and FileVault
- Removable storage
 - Ensures data remains protected after physically removed
 - Common with SD cards and USB drives
- Virtual private networks (VPNs)
 - Provides secure communication route
 - Protected against eavesdropping, on-path attacks, etc
- Email encryption
 - Protects sensitive information sent via email
 - PGP, S/MIME (Secure/Multipurpose Internet Mail Extensions)

Host-based Protections

- Host-based Intrusion Detection/Prevention System (HIDS/HIPS)
 - Analyzes local device for potential malicious activity
 - Known malicious patterns or suspicious anomalies
 - Similar features to network-based intrusion detection/prevention
- Host-based firewalls
 - Example - Windows Defender Firewall
 - Similar to network firewall, but focuses on local hosts
 - Filtering based on IP, protocol, services, etc
 - Policies and rules can be configured & enforced via central management
 - Default-deny policies to block all traffic unless allowed
- Logs integrated with SIEM systems

Defaults

- Change all default passwords
 - All types of systems - endpoints, servers, network devices, etc
 - Default passwords are well known and well documented
- Change default usernames if possible
 - Windows built-in administrator account
 - Not possible on many types of systems
- Disable all default network ports unless needed
 - Ports will vary depending on system
 - Method will also depend on system (local settings, network rules, etc)
 - Secure protocols for all remote management
 - SSH instead of telnet
 - SFTP instead of FTP

Physical Port Protection

- Minimize physical interfaces available
- Multiple methods available
 - Completely disable ports as needed (USB, serial, etc)
 - In operating system, or through UEFI/BIOS
 - Use software to allow only authorized devices
- Devices available to attackers
 - USB drives that automatically install malware
 - Hardware keyloggers/keystroke injectors
 - Malicious USB cables to steal data
- Can also help reduce data theft/leakage

Unnecessary Software & Services

- Uninstall any included software that is not required
 - Workstations, servers, etc
 - Can allow for unmanaged, unknown vulnerabilities
- Disable and/or uninstall any services that are not required
 - Can provide another attack vector locally or via network
 - Be cautious - many unfamiliar services may be system critical
 - Consult vendor support info and documentation
- Goal to reduce attack surface

EXPERTS AT MAKING YOU AN EXPERT

