Security+ Cheat Sheet

Chapter 1: Introduction to Security

CIA : Confidentiality, Integrity, Availability

- Confidentiality : Prevents disclosure of information to outside party
- Integrity : Guarantees data has not been tampered with
- Availability : Resources can be accessed when needed

AAA : Authentication, Authorization, Accounting(non-repudiation)

- Authentication : Confirms one's identity
  e.g.) username/password, biometrics, signature etc
- Authorization : Allows one to access certain materials
  e.g.) ACL(Access Control Lists), Linux permission bits etc
- Accounting : Tracking of data/comp./netwrk resources usage for individuals
  e.g.) Logging, auditing, data/network monitoring

Types of Threats

- Malicious Software
- Unauthorized Access
- System Failure
- Social Engineering

Physical, Technical, Administrative Security plans

- Physical : Physical security systems such as alarms, ID cards, CCTV etc
- Technical : Smart cards, ACLs, encryption etc
- Administrative : Policies, procedures, DRP(Disaster recovery plan) etc

Protection Methods

- User Awareness
- Authentication
- Anti-malware
- Data Backups
- Encryption
- Data Removal

*Good security plan + Good protection method = Solid defense (Defense in depth)

Types of Hackers

- White Hat
- Black Hat
- Grey Hat
- Blue Hat (Bounty Hunters)
- Elites (Zero day discoverers)

Types of Attackers

- Script Kiddie
- Hacktivist

- Organized Crime
- APT(Advanced Persistent Threat aka Nation state attacker)

Chapter 2 : Computer Systems Security Part 1 (Malware)

Types of Malware

- Viruses
  - Malicious code executed by the user, lives on a file
  - > Boot Sector : Placed in first hard drive sector
  - > Macro : Placed into documents
  - > Program : Infects executables
  - > Encrypted : Avoids detection through encryption
  - > Polymorphic : Decryption module changes with every infection
  - > Metamorphic : Whole virus code changes with every infection
  - > Stealth
  - > Armored : Misdirects antivirus away from its actual location
  - > Multipartite : Hybrid of boot sector and program
- Worms
  - Malicious code that replicates, standalone program, may spread automatically
- Trojans
  - Appear to be beneficial but contain malicious code
  - > Keygens
  - > RAT Trojans
- Ransomware
  - Encrypts files and data and demands payment to unlock
  - Often propagates as a Trojan or a worm
- Spyware
  - Usually hidden inside third party applications
  - Logs various user activities and sends it to attacker
  - Also associated with Adware and Grayware
- Rootkits
  - Designed to gain administrative control over a machine
  - Hard to detect b/c it targets low level(UEFI/BIOS, kernel etc)
  - Activates before Antivirus/OS
- Spam
  - Abuse of electronic messaging system

Malware Delivery

Treat Vector vs Attack Vector

- Software, Messaging and Media
  - > Emails, FTP, P2P/torrent file downloads
  - > Removable Media
- Typosquatting

- Exploit kit
- Botnets and Zombies
    > Also used for DDOS or financial gain
- Active Interception (MITM)
- Privilege Escalation
- Backdoor
    > Authentication bypass mechanisms built into the program itself
- Logic Bombs
    > Triggers malware on certain condition(date, OS type etc)

Malware Prevention / Troubleshooting

Common Symptoms : Slow computer speed, crashes, incorrect home page, popups

Common Prevention

> Antivirus : Regular updates and scans
Detects : worms, viruses and Trojans
Does not detect : Botnet activity, rootkits, logic bombs

> Firewalls and Regular OS updates

> Separation of OS and data

> Hardware + Software based firewall (e.g. router + Windows Firewall)

> Encryption for confidentiality (Windows EFS)

Common Steps to Malware Removal

1. Identify Symptoms
2. Quarantine infected system / drive to clean machine
3. Disable System Restore
4. Remediate affected system
    > Update AV / Scan and removal
5. Schedule scans and run update
6. Enable system restore and set new restore point
7. Educate end user

Worms and Trojans

> Antivirus, Regular maintenance and vigilance

Spyware

> Antivirus, browser security settings, remove unnecessary application

> End user education

Rootkits

> Antivirus, Rootkit detectors (USB bootable OS)

> Use UEFI over BIOS (GPT over MBR)

> Wipe the entire drive & reinstall OS

Spam

> Spam filter, whitelisting/blacklisting, close open mail relays

Chapter 3 : Computer Systems Security Part 2

Security Applications

- Personal Firewalls (Host based firewalls)
  - > Windows Firewall
  - > ZoneAlarm
  - > Packet Filter and IP Firewall (Mac OSX)
  - > iptables (Linux)
- IDS (Intrusion Detection System)

  Host Based : Loaded onto individual machine

  Analyzes and monitors that one machine state

  Can interpret encrypted traffic

  Network Based : Either loaded onto a machine or standalone device

  Monitors every packet going through network interface

  Monitors multiple devices, less expensive

  Cannot monitor what happens in an OS

  Monitoring Types – Statistical Anomaly vs Signature

  > Statistical Anomaly

  Establishes baseline and compares current performance

  > Signature

  Network traffic analyzed to find predetermined patterns

  HIDS examples

  > Trend Micro OSSEC (freeware)

  > Verisys (Commercial, Windows)

  > Tripwire (Commercial)

  * Make sure to protect HIDS database with encryption and access control
- Popup Blockers

  Ad filtering & Content filtering
- DLP (Data Loss Prevention)

  Monitors data in use / in motion / at rest

  Prevents unauthorized use and leakage of data

  Types of DLP

  > Endpoint DLP : Runs on single machine, software based

  > Network DLP : Software/hardware, installed on network perimeter

  > Storage DLP : Installed in data centers/server rooms

Securing Computer Hardware and Peripherals

Examples of peripherals: USB flash drives, SATA external HDD, optical disks

Securing BIOS

- Flashing (Updating) BIOS firmware
- BIOS password

- Configure BIOS Boot order
- Secure boot (disables unsigned device drivers, UEFI)
* UEFI and Root of Trust, secure/measured boot, attestation

Securing Storage Devices

- Removable Storage
  > Typically prohibits all removable storage besides specific ones
  > Removable Media Controls
    USB Lockdown (BIOS), limit USB use, malware scans, audits
- NAS (Network Attached Storage)
  > Built for high availability (no downtime)
  > Commonly implemented as RAID array (levels depend on situation)
  > Use encryption, authentication, secure logging etc
- Whole Disk Encryption
  > Requires either self encrypting or full disk encryption SW
  > Windows BitLocker requirements
    1) TPM or External USB key with encrypted keys
    2) Hard drive with 2 volumes(1 for boot, 1 to be encrypted)
  > Double Encryption – BitLocker + EFS
- HSM (Hardware Security Modules)
  Vs TPM
    TPM handles key storage with limited cryptographic function
    HSM handles mainly quick crypto functions with key storage
  Found in USB attachment or network attached device

Securing Wireless Peripherals

- Force devices to use AES or WPA2 encryption for data transmission

Securing Mobile Devices

General Security

- Keep phone number secure and do not respond to unsolicited calls
- Update mobile device OS
- Complex password and limit downloads to device

Malware

- Install & update mobile device AV
- Take use of built in security features
- Avoid following links, don’t store information on device
- Don’t post info on social media

Botnet Activity

- Follow anti-malware procedures
- Avoid rooting / jailbreaking phones

SIM Cloning

- A cloned SIM redirects all calls and texts to its own device

- Able to hijack messages intended for original SIM card owner

Wireless Attacks

- Bluejacking
- Bluesnarfing

Theft

- Full device encryption(FDE)
- Set up GPS tracking
- Remote lock & Remote wipe technology

Mobile Application

- Mobile key management : use Third party software (Verisign)
- Application whitelisting / blacklisting
- Strong SMS application and endpoint security
- Mobile payment : avoid public networks, user education
- Geotagging : Disable GPS depending on situation
- BYOD concerns
    - > Storage Segmentation : divide corporate vs private data storage
    - > Mobile Device Management systems for corporations

Chapter 4 : OS Hardening and Virtualization

OS Hardening

Motivation : Out of the box OS is vulnerable by default,
Need to customize settings to make it more secure

Concept of Least Functionality

- Restrict and remove any functionality not required for operation
- NIST CM-7 control procedures
- Target features
  - > Applications
  - > Ports
  - > Services (daemons)
- Consider backwards compatibility when removing obsolete applications
- SCCM (System Center Configuration Manager) for multiple machines
- Application blacklisting / whitelisting
- Service configuration commands
  - > Windows : services.msc, net stop, sc stop
  - > Linux : /etc/init.d/<service> stop, service <service> stop etc
  - > OSX : kill command

Update, Patches, Hotfixes

- TOS (Trusted Operating System)
  - : Certified OS considered secure by gov standards
- Update Categories
  - > Security Update : Product specific, security related
  - > Critical Update : critical, non security related bug fix
  - > Service Pack : Cumulative set of updates, now discontinued
  - > Windows Update : Noncritical fixes, new features and updates
  - > Driver Update : Beware driver shimming / refactoring
- Hotfixes and patches are now used interchangeably

* Disable automatic updates to synchronize versions and updates

Patch Management

- Process of planning, testing, implementing and auditing patches
  - > Planning : Deciding which patches are required
    Checking Compatibility
    Plan how the patch will be tested / deployed
  - > Testing : Test the patch on one machine / small system
  - > Implement : Patch deployment to all machines
    Use SCCM or other centralized management system
  - > Auditing : Confirm patch is live on system
    Check for any failures or changes due to the patch

Group Policies, Security Templates, Configuration Baselines

Group Policy : Used in Windows to set group configurations

* gpedit.msc

Hardening File Systems and Hard Drives

a) Use a secure file system

> NTFS for Windows, allows encryption, ACLs, logging

Use chkdsk and convert commands

> ext4 for Linux

Use fdisk -l or df -T

b) Hide important files (System files, personal etc)

c) Manage hard drives

> Delete temp files

> Periodically verify system files integrity

> Defrag hard drives

> Backup data

> Restore points

> Whole disk encryption

> Separate OS system and personal data

Virtualization

Virtualization : Creation of virtual machines housed in an OS

VM(Virtual Machines) and VDE(Virtual Desktop Environment)

- Pros

> Flexible and portable

> Safe testing of malware in a controlled environment

- Cons

> Resource intensive

> Vulnerable to hardware failures

VM Categories

1. System virtual machine : Runs an entire OS

2. Process virtual machine : Runs a single application (browser)

* Virtualization ↔ Emulation ↔ Simulation

* Virtual Appliance ↔ Image ↔ Virtual Machine

Other forms of virtualization

> VPN (Virtual Private Network)

> VDI (Virtual Desktop Infrastructure)

> VLAN (Virtual Local Area Network)

Hypervisor (Virtual Machine Manager)

- Allows multiple virtual OS to run concurrently

Type 1 vs Type 2 Hypervisor

- Type 1 - Native
  - > Runs directly on host hardware
  - > Flexible and efficient
  - > Strict hardware/software restrictions, less common
- Type 2 – Hosted
  - > One level removed from host hardware
  - > More available to most OS and hardware
  - > Resource intensive

Application Containerization

- Runs distributed applications w/o running an entire VM
- Efficient but less secure

Securing Virtual Machines

Generally equivalent to securing regular OS, but with little more work

1. Update virtual machine software (e.g. VirtualBox)
2. Be wary of VM-VM and VM-host network connections
3. Protect NAS and SAN from virtual hosts
4. Disable unnecessary USB and external ports on VMs
5. Alter boot priority for virtual BIOS
6. Limit and monitor VM resource usage to prevent DOS attacks
7. Protect raw virtual machine image
   - > Snapshots, Encryption, Access permission and signatures

Virtualization Sprawl : When there are too many VMs to manage at once

> Employ a VMLM (Virtual Machine Lifecycle Management) tool

Chapter 5 : Application Security

Securing Web Browsers

- Avoid newest versions and disable auto update (new versions are unstable)
- Consider organizational requirements and OS
- General Browser Security Procedures
    - > Implement Policies
        - Hand written, browser settings, GPO(Windows), OS setting etc
    - > Train Users
    - > Use proxy and content filter
        - Proxy serves as an intermediate cache between server and client
        - Configured in browser settings / domain controller
        - Beware of malicious proxy configurations
    - > Secure against malicious code
        - Configure Java, ActiveX, Javascript, Flash media etc
- Web Browser Concerns and Security Methods

    Basic Methods

    - > Timely Updates
    - > Adblock, pop up blocking
    - > Implement security zones
    - > Control ActiveX/Java/Plugins
    - > Avoid jailbreaking (mobile)

    Cookies

    - > Configure and control through browser settings
    - > Related threat : Session Hijacking

    LSO(Locally Shared Objects - Flash)

    - > Flash version of cookies, may be used to track users
    - > Configure and control in Flash Player Settings Manager

    Addons / Plugins

    - > Inherent security risk, disable all

> Most IE plugins made with vulnerable ActiveX

Advanced Browser Security

> Browser temp files – configure to automatically flush

> Disable saved passwords

> Configure a minimum version limit on TLS/SSL

> Disable all 3rd party plugins

> Consider using a VPN or virtual machine for extra separation

Securing Other Applications

Principle of Least Functionality – don't give tools users don't need

User Account Control (Windows)

- Keeps everyone on regular user level of access by default
- Prompts required to access any admin right required things

Create Policies (Prioritize app. Whitelisting over blacklisting)

Securing common Windows programs

1. Outlook

> Install latest update, upgrade to newer version of Office

> Use email whitelisting to remove junk email

> Read email in text format instead of HTML

> Enable attachment blocking

> Use encryption - SPA (Secure Password Authentication), PGP, SSL

2. Word

> Using passwords for opening/modifying documents

> Read only settings

> Digital certificates

3. Excel

> Password protected worksheets, no macro

> Excel encryption

Mobile Applications

- Disable GPS

- Configure strong passwords

Server Applications

- e.g. FTP, Email, Web, SQL database
- Change default username / passwords
- Don’t consolidate multiple services into single machine

Secure Programming

SDLC (Software Development Life Cycle)

- Waterfall
  > Traditional method
  > Requirements are decided before development
- Agile
  > RAD (Rapid Application Development) approach
  > Relatively new, Breaks development down to incremental changes
  > Requires high dedication from members
- DevOps
  > Deployment tool, often used together with Agile method

Core SDLC and DevOps Principles

- Preserving CIA of software development
- Secure code review
  > In depth code review for security bugs
  > Included before fuzzing or penetration testing
- Threat Modeling
  > Identifying and prioritizing potential threats
- Common Security Principles
  1. Least Privilege
  2. Defense in Depth
  3. Never trust user input
  4. Minimizing attack surface
  5. Secure defaults

6. Provide authenticity and integrity (program signatures)

7. Fail securely (Error handling)

8. Thorough testing of security fixes and patches

Program Testing Methods

1. White box vs Black box testing

> white box, black box, gray box, stress testing, pentesting etc

2. Compile time vs runtime errors

> Reminder that both software and hardware has runtime errors

> SHE (Structured Exception Handling) deals with both SW/HW

3. Input Validation

> Perform on both client and server side

> Key factor of SQL injections and XSS

4. Static vs Dynamic code analysis

> Static : No code execution, examines code with automated tools

> Dynamic : Runtime examination of code behavior for bugs

* Fuzzing is a form of dynamic code analysis

5. Fuzz Testing

> Input of large amounts of random data until code errors

Program Vulnerability and Attacks

1. Backdoors

> Preprogrammed authentication bypasses built into system

> Updates usually remove these, job rotation, code cross checking

2. Memory / Buffer Vulnerabilities

> Buffer overflows (Stack, heap)

> Integer overflows (integer wrapping)

> Memory leaks : Degrades system performance

> Nullptr dereference

> ASLR and DEP is common defense against buffer overflows

3. Arbitrary and Remote Code Execution

    > Shellcode injections

    > Strong input validation, fuzz testing

4. XSS / XSRF

    > Common browser based attacks, uses HTML code injection

5. Other Code injections

    > SQL Injection

    > LDAP Injection

    > XML Injection

6. Directory Traversal

7. Zero Days

Chapter 6 : Network Design Elements

Network Design

OSI Model

- Goals

1. Explain network connection between hosts on LAN/WAN

2. Present a categorization system for communication protocols

3. Shows how different protocol suits communicate

- Overview

Layer	Name	Usage	Units
1	Physical	Physical and Electrical medium	Bits
2	Data link	Establishes, maintains and decides how data transfer is accomplished over the physical layer	Frames
3	Network	Routing and Switching	Packets
4	Transport	Manages/ensures error free transmission between hosts through logical addressing/port assignment	Segments(TCP) Datagrams(UDP)
5	Session	Establishment, termination and synchronization of sessions within the OS over the network and between hosts	Messages
6	Presentation	Sender to receiver data translation, Code conversion, data compression and file encryption	Messages
7	Application	FTP, HTTP and SMTP end user protocols	Messages

Network Devices

- Switch

> Central connection device, replaces hubs and bridges

> Translates MAC and MAC+IP into physical ports to route messages

> Attacks

1. MAC Flooding : Uses up the CAM to force switch into broadcast

2. MAC Spoofing : Masks network adapter MAC with different value

3. Physical Tampering : Vulnerable management ports, Looping

* Use hierarchial router structure or spanning tree

protocol to prevent looping

- Bridges
    - > Used to separate physical LAN into two logical networks
    - > Works on layer 2 (Data link), now obsolete
- Router
    - > Used to connect two or more networks
    - > Works on network 3 (Network)
    - > Various forms : SOHO, servers configures as routers, Cisco black box
    - > Attacks : DOS, malware intrusions etc
    - > Defenses
        1. Secure configurations
        2. Firewalls
        3. IPS
        4. Secure VPN Connectivity
        5. Content filtering
        6. ACL (Access Control Lists)

NAT (Network Address Translation), Private vs Public Addresses

- NAT : Process of changing IP in transit
- Motivation
    - > Allow a large private address space mapped to a smaller public one
    - > Firewall effect (hides internal IPs)
    - * Static NAT : Only one machine uses the router that does NAT
- Private IP
    - > Invisible to public(internet)
    - > Assigned automatically by SOHO router or DHCP server
    - > Within predetermined range
- Public IP
    - > Visible to public, anyone can attempt connection
    - > Assigned by ISP DHCP servers
- * IPv6 Vulnerability

> By default attempts to automatically connect to other IPv6 addresses

> Make sure to secure both IPv4 and IPv6

Network Zones and Interconnections

- LAN (Local Area Network)

> Group of interconnected computers contained in a small space

> Usually uses private IPs behind a firewall

> By default does not have internet access, but may connect to an Internet proxy to do so

- WAN (Wide Area Network)

> Network of two or more interconnected LANS

> Covers a larger geographical area

> Requires telecomm/datacomm service company

- Internet

> Worldwide interconnected network

> Must secure all transmission that happens over the internet

- DMZ (Demilitarized Zone)

> Special subnetwork designed for external client access

> Common web/FTP/email/database etc services reside in DMZ

> Can also be accessed by LAN clients

> Often placed in a separate LAN network from the rest of system

> Common 3-leg perimeter configuration

- Intranets & Extranets

> Used to share company data securely through the internet

> One company = intranet, multiple companies involved = extranet

> Never store confidential+ data in these networks

> Crucial to properly implement firewall

NAC (Network Access Control)

- Denies network access until client obtains proper security measures

- Antivirus, system updates etc

- Preinstalled clientside software (agent) or remote scan (agentless)

- Persistent vs Dissolvable agents

    > Persistent : Designed for multiple use

    > Dissolvable : Designed for one time authentication

- Agentless offers less control for more flexibility

- Cisco offers hardware solutions

Subnetting

- Process of creating logical subnetworks through IP manipulation

- Benefits

    1. Compartmentalizes network, increasing security

    2. Efficient use of IP address

    3. Reduces IP collision and broadcast signals

- Overview

    1. Class A : Large network, 255.0.0.0

    2. Class B : Medium network, 255.255.0.0

    3. Class C : Small network, 255.255.255.0

    Example : 192.168.1.0/28 □ 28 is total number of bits used
    Class C Network

    255.255.255.240 □ 1111 1111 . 1111 1111 . 1111 1111 . 1111 0000

    First 3 octets are Class C mask

    First 4 bits of last octet is subnet mask, 2^4 = 16 subnets

    Last 4 bits of last octet is host ID, 2^4-2 = 14 hosts

VLAN(Virtual LAN)

- Segments various networks sharing the same switch, reduce collision,

  Organize network, boost performance and security

- Works on Layer 2 (Data link frames)

- Allows admins to group hosts connected on different switches together

- VLAN Hopping : Methods of gaining access to other VLANs on switch

    1. Switch Spoofing

    2. Double Tagging

Telephony

- Provides voice communications, fax etc
- Now computers are involved in telephony as CTI
- Modems
    > Still often used to connect to networking equip. via dial up
    > Very insecure (War dialing)
    > Protections : Callback, username/pw, hide modem number

PBX(Private Branch Exchange)

- Makes internal phone connections, connects to PSTN
- New added features now make them less secure

VoIP

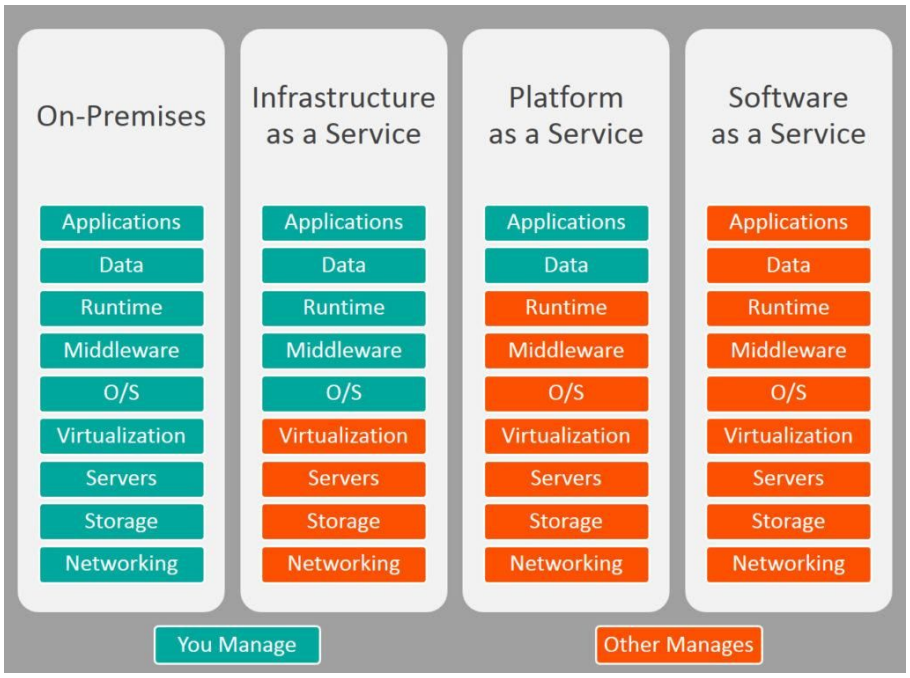
- Broad term for voice data over IP networks
- IP phones exploited the same way as regular computers
- Home VoIP solutions use SIP(Session Initiation Protocol) vulnerable to MiTM

Cloud Security and Server Defense

Definition of Cloud : Any network between two organization borders

Cloud Computing

- A method of offering on demand services normal users don’t have
- SaaS (Software as a Service)
    > Allows user to have access to software they don’t have on host
- IaaS (Infrastructure as a Service)
    > Offers networking, routing, VM hosting and other networking
- PaaS (Platform as a Service)
    > Offers virtual development of application
- SECaaS (Security as a Service)
    > Offers security services to be integrated into existing infra.



Different Types of Cloud

- Public Cloud : Full public access, low security
- Private Cloud : Full private access, high security
- Hybrid Cloud : Utilize both private and public depending on handled data
- Community Cloud : Private to specific group, good for collab projects

Cloud Security

- Depends on the amount of security control the admin has
- Defenses for sending data to cloud
    1. Passwords : 10 char general case, 15 for confidential data
    2. Multifactor authentication
    3. Strong data access policy : passwords, multifactor, group policy
    4. Encryption : strong PKI encryption on all files
    5. Programming standardization
    6. Data protection

* Unconventional data channels : Social media, P2P, dark net

Server Defenses

- Servers are most important part of network to secure
- Contains all data and services

1. File Servers

    > Stores, transfer, migrate, synchronize and archive files

    > Identical vulnerability to malware that target desktop PCs

    > Hardening, updates, AV, SW/HW firewall, HIDS, encryption, monitoring

2. Network Controllers

    > Central repo of all user and computer accounts

    > LDAP injection, Kerberos vulnerabilities privilege escalation

    > Updates, hot fixes

3. Email Servers

    > Deals with email, texting, fax, chat etc

    > May run multiple services and ports, POP3, SMTP, IMAP, Outlook

    > XSS, DDOS, SMTP memory exploits, directory traversal etc

    > Updates, quarantine, HW/SW spam filter, DLP, encryption (TLS/SSL)

4. Web Servers

    > Provide web and website services to users

        Ex) Microsoft IIS, Apache HTTP, lighthttp, Oracle iPlanet

    > DDOS, overflow attacks, XSS, XSRF, remote code exec., backdoors

    > Secure programming, updates, HW firewall, HTTPS

    * Darkleech : Apache based attack using malicious Apache modules

5. FTP Servers

    > Basic file access (public/private)

    > Web shells, weak authentication, bounce attacks, buffer overflow

    > Strong password, secure encrypted FTP, dynamic port assignment

Chapter 7 : Networking Protocols and Threats

Ports and Protocols

Port Ranges, Inbound vs Outbound, Common Ports

Ports : Logical communication endpoints

TCP vs UDP

- TCP : Ordered, guaranteed connection oriented sessions
- UDP : Unordered, streaming real time connection

Total of 65536 ports

Port Ranges

- 0 – 1023 : Well known ports
- 1024 – 49151 : Registered ports for proprietary applications
- 49152 – 65535 : Dynamic and private ports, cannot be registered

Inbound vs Outbound Port

Inbound : Usually leaves well known ports on server open

Needs to be secured by an Admin

Outbound : Used to initiate connections to servers

Dynamic Port assignment enhances security

Well Known Ports

Port	Protocol	TCP/UDP	Secure Version	Usage
21	FTP	TCP	FTPS, 989/990	Transfer Files from host to host
22	SSH	TCP/UDP		Secure Shell Connection
23	Telnet	TCP/UDP		Remote administration (deprecated)
25	SMTP	TCP	SMTP w/ TLS, 465/587	Sends Email
49	TACACS+	TCP		Remote Authentication
53	DNS	TCP/UDP	DNSSEC	Hostname to IP resolution
69	TFTP	UDP		Basic version of FTP
80	HTTP	TCP	HTTPS, 443	Transmit web page data
88	Kerberos	TCP/UDP		Network Authentication using tickets
110	POP3	TCP	POP3 w/ TLS, 995	Receives Email
119	NNTP	TCP		Transport Usenet Articles
135	RPC	TCP/UDP		Locate DCOM ports
137-139	NetBIOS	TCP/UDP		Name quering, sending data, NetBIOS connection
143	IMAP	TCP	IMAP4 w/ TLS, 993	Email retrieval
161	SNMP	UDP		Remote network device monitoring
162	SNMPTRAP	TCP/UDP		Traps/InformRequests sent to SNMP manager
389	LDAP	TCP/UDP	LDAP w/ TLS, 636	Maintain user and other object directory
445	SMB	TCP		Shared access to files and resources
514	Syslog	UDP	Syslog w/ TLS, 6514	Computer message logging

860	iSCSI	TCP		IP based protocol for linking data storage facilities
1433	Ms-sql-s	TCP		Opens MS SQL server queries
1701	L2TP	UDP		VPN protocol with no security, used with IPsec
1723	PPTP	TCP/UDP		VPN protocol with security
1812/ 1813	RADIUS	UDP		AAA protocol for authentication, authorization and accounting
3225	FCIP	TCP/UDP		Encapsulate Fibre channel frames
3389	RDP	TCP/UDP		Remote Desktop Protocol for Windows
3868	Diameter	TCP		AAA protocol that can replace RADIUS

Malicious Attacks

DOS – Resource depletion attack

- Flood Attack

> Ping floods : Uses ICMP packets (disable ICMP to protect servers)

> Smurf attack : Redirects ICMP echoes to spoofed IP

> Fraggle : Redirect UDP echoes (port 7 and 19) to spoofed IP

> SYN flood : sends large amount of TCP SYN packets to target

> Xmas flood : Aims to reboot routers

- Ping of Death

Sends oversized/malformed packets to crash services

Mostly automatically blocked by modern OSes

- Teardrop Attack

Sends mangled IP fragments to crash IP reassembly code

- Permanent DOS

Flashes custom images onto routers and network devices

- Fork bomb

Forces numerous processes that saturates processor capacity

DDOS

Utilizes a botnet to flood and DOS a host

Common defenses similar to DOS defenses

ACL routers, firewall, IPS, simulated servers effective

DNS amplification – another reflective spoofed IP attack

Sinkholes & Blackholes

Sinkhole : DNS server configured to give false data to bots

Abused to maliciously redirect users to false sites

Blackhole : List of domains known to be malicious and blocked

Spoofing

Impersonation of various URI (Uniform Resource Identifier)

MitM attacks, IP spoofing, MAC spoofing, session hijacking etc

WWN spoofing : World Wide Names are unique identifiers to SAN (like MACs)

* SAN (Storage Area Network)

Session Hijacking

- Session Theft
  - > Typical cookie hijacking in browser (application) level
  - > Use different nonces for session keys & encryption
- TCP/IP Hijacking
  - > Predicts next sequence number in a TCP session to inject data
  - > PKI encrypted traffic to counter TCP/IP Hijacking
- Blind Hijacking
  - > Randomly injects data hoping it works
- Clickjacking
- MitM
- MitB (Man in the Browser)
  - > Infected browser modifies user input data when packets are sent
  - > Third party transaction verification and antivirus counters this
- Watering Hole
  - > Plants malicious code into high traffic sites

Replay Attacks

Attacker saves and reuses valid packets at a future date

Defenses

> Session tokens, timestamping & synchronization, crypto and nonces

Null Session

Uses port 139 & 445 (NetBIOS and SMB)

Abuses built in unauthenticated connection enabled by default on old Windows

Transitive Access and Clientside Attacks

Compromising a trusted user of a server in turn compromises the server

* Transitive trust is dangerous, only establish trust in a temporary fashion

DNS Poisoning

Improper modification of DNS information redirects users to malicious sites

Targets DNS server caches

Defenses : TLS, DNSSec, TSIG (Transaction Signature), Server patches

* Unauthorized zone transfers

Attacker gains quick reconnaissance by replicating DNS data

Gains various hostnames and IP addresses

Windows host files are also a common target

> hosts file used to locally resolve hostname to IP addresses

> When compromised can result in data leak or malicious redirection

> When compromise detected delete and remake hosts file w/ read-only

Pharming : A poisoned DNS cache/hosts redirects users to malicious sites

Domain name kiting : Repeatedly reregistering domain name to use it for free

ARP Poisoning

ARP resolves IP to MAC addresses

Use VLAN segmentation and separation to minimize damage

Chapter 8 : Network Perimeter Security

Firewalls and Network Security

Firewalls

- Prevents unwanted access to networks by blocking ports & IP
- ACL (Access Control List) decisde which packets to allow
- Packet Filtering : Inspects and filters unwanted packets
    1. Stateless : Does not keep track of previous packets
    2. Stateful : Keeps a record of previous packets for cumulative filter
- NAT Filtering : Filters according to matching inbound/outbound ports
- Application Level Gateway : Security measures applied to a specific app
- Circuit Level Gateway : Only checks if a connection is valid
  Ignores validity of individual packets
- Firewall Logging : Logs all connection and blocked packets
- Types of Firewalls
    1. Packet Filtering
        > Most basic form
        > Observes packet headers to see if they violate firewall rule
    2. Stateful Firewalls
        > Keeps track of established sessions
        > Filters unwanted request to open new connections
    3. Application Firewalls
        > Blocks or allows specific applications to communicate
    4. Web App Firewalls
        > Specifically designed for HTTP sessions

Proxy Servers

Acts as an intermediary between LAN clients and outside servers

Types of Proxies

1. IP Proxy : Uses NAT to hide client IP address. Basic router function
2. Caching : Saves remote server data for efficiency

Commonly used in HTTP proxies

Disable PAC (proxy auto configuration) files

3. Reverse : Protects LAN servers from outside clients

4. Application : Acts as a remote connection application

Proxies generally modify client requests for anonymity and security.

Those that do not are called **transparent proxies.**

Internet Content Filtering : Can be installed on each host, but more efficient to install on a proxy

Web Security Gateways : Active monitoring and filtering of user data streams

* UTM (Unified Threat Management)

Honeypots / Honeynets

Composed in various sizes (1 machine, file to a network of machines)

Used to study and analyze attacker behavior

DLP (Data Loss Prevention)

Stops leakage of confidential information through content inspection

Detects company confidential information and prevents it from exiting network

If data is stored on cloud/BYOD, cloud based DLP is more suitable

NIDS vs NIPS

NIDS (Network Intrusion Detection System)

Attempts to detect malicious network activities (port scans, DDoS)

Common solutions : Snort (open source), Bro (open source)

Placed before a firewall, but also placed in key network locations

* Promiscuous mode on NIDS adapter allows examination of all network packets

Sometimes effective enough to remove most HIDS solutions

Pros

Effective detection of network intrusion

Installed on only a few machines for whole network

Cons

Cannot read encrypted traffic

Cannot monitor individual machine

- Passive (does not prevent attacks)

NIPS (Network Intrusion Prevention System)

- Inspects packets and removes/redirects malicious traffic
- Application aware device – able to associate packets to specific applications
- Pros
  - Can protect non computer based network devices (routers, switches)
  - Prevent attackers from entering the network (Active)
  - Able to read encrypted traffic
- Cons
  - Single point of failure, can bring down entire network if knocked out
  - Prone to false positive/negatives
  - Fail open/close
  - Uses more resources

Protocol Analyzer

- Captures and analyzes packets, allowing inspection of packet content

UTM (Unified Threat Management)

- Culmination of various network defenses in a single device
- All-in-one device or NGFW (Next Generation Firewall)
- Can also be a single point of failure

Chapter 9 : Securing Network Media and Devices

Wired Networks

Vulnerabilities

Various types of devices – routers, switches, firewalls, NIDS/NIPS etc

1. Default Accounts

Default username/password of many devices are public knowledge

Make sure to change username/password before connecting device to web

2. Weak Passwords

3. Privilege Escalation

Escalation to kernel, DRM bypass, jailbreaking, malware etc

- Vertical Privilege Escalation

Lower privilege accessing higher privilege, user admin

- Horizontal Privilege Escalation

User access function of another user, user1 user2

4. Backdoors

Bypasses traditional authentication, faulty code, RAT software/rootkit

5. Network Attacks

DOS/DDoS, Spoofing etc (refer to Ch 7)

Cable Media Vulnerabilities

Types of Cables

- Twisted pair

- Fiber optic

- Coax

1. Electromagnetic / Radio Frequency Interference

Creates noise and unwanted signals, use cable shielding

2. Crosstalk

Wires placed in proximity affect one another’s signals

Use twisted pair cables to minimize/eliminate crosstalk

NEXT (Near End Crosstalk)

Measurement of interference at the point closest to noise source

FEXT (Far End Crosstalk)

Measurement of interference at the point furthest from noise src

3. Data Emanation

Data leakage through EM field generations (side channels)

Use shielded cables or faraday cages to prevent EM field

Refer to US govt. TEMPEST guidelines

4. Wiretapping

a) Employing a butt set to RJ11/punch block

b) Plugging into open twisted pair ports on routers/switch/hub

c) Splitting twisted pair connections and cables

d) Spectral Analyzers to detect electric signals on cables

e) Passive optical splitter (fiber optics wiretapping)

* Wiring Closets

1. IDF (Intermediate Distribution Frame) : one per each floor

2. MDF (Main Distribution Frame) : All IDFs connect to the MDF

One for building, connects to ISPs

3. SNMP monitored devices(PDU, UPS etc) can be used by attackers to bypass security measures to attack IDF/MDF

Securing Wireless Networks

Vulnerabilities

1. Administration Interface(Romming)

Default username/password on administration consoles

2. SSID Broadcasting

Disable it under normal circumstances, enable only when connecting new device

3. Rogue Access Point

Keep track of all legitimate access points with graphing tools

Investigate any undocumented AP showing up

4. Evil Twin

Rogue AP that uses same SSID as legitimate AP

Use VPN that requires another authentication step

5. Weak Encryption

Current standard is WPA2, PSK wireless transport layer security

Protocol	Description	Key Size
WEP	Wired Equivalent Privacy (Deprecated)	64 bit
WPA	WiFi Protected Access	128 bit
WPA2	WiFi Protected Access version 2	256 bit
TKIP	Temporal Key Integrity Protocol (Deprecated)	128 bit
CCMP	Counter Mode with CBC-MAC Protocol	128 bit
AES	Advanced Encryption Standard	128/192/256 bit
WTLS	Wireless Transport Layer Security	Based on TLS

6. WPS (Wireless Protected Setup)

Should be disabled in all cases, can easily be brute forced and broken

7. Ad Hoc Networks

Wireless connection between clients without central control

Obviously massively insecure, should be disallowed in all cases

8. VPN over Open Wireless

All wireless VPN should be accompanied by suitable encryption protocol

(PPTP, IPSec etc)

Wireless Access Point Security Strategy

- Minimize external signal bleeding and employ EM shielding
- Wireless site survey to gauge various signal strength / locate interference
- Employ WAP built in firewall and NAT and MAC filtering if possible
- AP isolation – Segment each client on the WAP, prevent client-client comms
- Encryption on application layer as well

- WLAN controller to centralize WAP management

Wireless Transmission Attacks

1. War Driving/War chalking
2. IV attack
3. MAC Spoofing
4. Deauth
5. Dictionary/Brute Force WAP passwords

Bluetooth and Other Devices

Bluetooth and NFC (Near Field Communicator) can also be an attack vector

Bluejacking : Unsolicited Bluetooth messages

Bluesnarfing : Unauthorized access of information from Bluetooth devices

RFID

- Generally used in authentication
- Up to date chips have better encryption and shielding, more secure
- Uses very close range NFC (4 cm) to communicate/authenticate

Other Wireless Technologies

Cell Signals : Generally disabled within company premises

Chapter 10 : Physical Security and Authentication Models

Identification : Something that identifies a person

Authentication : When a person's identity is confirmed or verified

Authorization : When a user is given permission to access certain materials

Happens after authentication

Physical Security

1. Perimeter security : Ample lighting, no hidden corners, CCTV/guards etc
2. Server Room
   - Position on elevated levels, avoid water damage
   - Cables and physical locks to deter theft/tampering
3. Door Access
   - Should be implemented according to local crime rate and data within
   - Use electronic keycards and cardkey controllers
     * Hardware based tokens and OTP generators also secure
   - Smart cards for authentication
     Eg) PIV (Personal Identity Verification, government employees)
     CAC (Common Access Card, DoD/military personnel)
   - Also employ mantraps to avoid tailgating
4. Biometrics
   - Beware of false acceptance/rejection rates
   - Crossover Error Rate should be minimized
     (When False Acceptance Rate = False Rejection Rate)

Authentication Models and Components

1. Authentication Models
   a) Username/Password
   b) Multifactor Authentication (MFA), more secure but also costly
   c) Context Aware Authentication
   d) Single Sign On (SSO)
   e) Federated Identity Management

f) Web based SSO

2. Localized Authentication Technology

Ways to authenticate users connecting to a LAN

1. 802.1X and EAP

Way of ensuring port security, uses data link layer protocols

1 – **Authenticator** detects new **client**, initiates 802.1X

2 – **Authenticator** sends EAP requests to new **client**, **client** responds with EAP responses which are forwarded to **Authentication Server**

3 – **Authentication Server** responds with request for an EAP method which is forwarded to the **client**

4 – EAP request/responses are sent between server and client until authentication is successful

Types of EAP Methods

a) EAP-MD5

b) EAP-TLS

c) EAP-TTLS

d) EAP-FAST

e) PEAP

802.1X is often used as port layer security along with VLANs

3. LDAP (Lightweight Directory Access Protocol)

Used most often in MS Active Directory

Protocol used to access and maintain directory servers

Default port 389, SSL enabled secure port 636

4. Kerberos and Mutual Authentication

Used in client-server model for mutual authentication

Protection against eavesdropping/replay attacks

Builds off of symmetric key crypto and trusted third parties

Relies on a central server (could become single point of failure)

5. Remote Desktop Services

Remote control of a Windows machine from a client

Well known port, weak encryption, no multifactor authentication

More secure third party options exist, adding security costs $$$

3. Remote Authentication Servers

Examples : RAS, VPN, RADIUS, TACACS+, CHAP

1. RAS (Remote Access Service)

Def : Any combination of HW/SW that allows remote access tools

Common measures to secure RAS

- Deny access to those who don't need it
- Monitor daily usage logs
- Set up RAS authentication

2. CHAP (Challenge-Handshake Authentication Protocol)

1 – **Authenticator** sends challenge to **client**

2 – **Client** responds with hash of challenge + secret(password)

3 – If correct maintain connection, else terminate

MS-CHAPv2 is recommended b/c it provides mutual authentication

3. VPN

Connects two computers through hostile network via tunneling

Common Protocols : PPTP, L2TP

VPN remote access vs Site to site configuration

* Split Tunneling

Allows a client to connect to both WAN & LAN-via-VPN

May bypass higher level security measures placed on LAN

GRE(Generic Routing Encapsulation) by Cisco

Sometimes used to encapsulate PPTP/IPSec for VPN

4. RADIUS vs TACACS+

RADIUS

Provides centralized authentication for dialup VPN/wireless

EAP/802.1X compatible

Network of RADIUS servers called a federation is also used

TACACS+

Mainly used on UNIX environments as a daemon

Chapter 11 : Access Control Methods and Models

Access Control Models : How admission to physical areas and computer systems are managed

1. Discretionary Access Control (DAC)
    - Determined by owner of file/folder
    - Owner decides how each user/group accesses his file
2. Mandatory Access Control (MAC)
    - Strictest form of access control, need to know basis
    - Each user is given clearance level and can only access files within level

        Eg) FOUO, Confidential, Secret, Top Secret
    - Rule based access control

        Access determined by comparing label to clearance level
    - Lattice based access control

        More complex, involves set mathematics
3. Role Based Access Control (RBAC)
    - Access controlled by a central authority
    - Various roles that have overlapping privileges are assigned to users
4. Attribute Based Access Control (ABAC)
    - Dynamic and context aware access control

Basic Access Control Practices

1. Implicit Deny
2. Least Privilege
3. Separation of Duties
4. Job Rotation

Rights, Permissions and Policies

Users, Groups and Permissions

Windows Active Directory

- Users can be added to specific OUs or Users folder
- Logon times and valid login dates can also be configured
- Consolidate multiple accounts with Federated Identity Management/SSO

- Group users with similar permissions together

- NTFS Permissions
    1) Full Control
    2) Modify
    3) Read & Execute
    4) List Folder Contents
    5) Read
    6) Write

Permission Inheritance and Propagation

- Default behavior is child folder inherits parent folder permissions
- Cannot change without disabling permission inheritance
- Moving vs Copying data
    Copy : Inherits permission of destination folder
    Move : Retains original permission

Username and Passwords

- Weak and old pw is common avenue for data exfiltration
- Never use default username/pw for admin (or anything)
- Disable guest and unnecessary accounts
- Ctrl + Alt + Delete to log in, ensures users are using keyboard Vs network connection
- Use policy management

Policies

- Enforced rules configured either on individual machine or network
- Password Policies
    1. Enforce password history
    2. Min – Max password age
    3. Minimum pw length
    4. Complexity requirements
- Most are configured on OS level with AD domain controller

UAC (User Account Control)

- By default keeps all non-admin users without full admin rights

Chapter 12 : Vulnerability and Risk Assessment

Conducting Risk Assessment

General Risk Management Strategies

1. Transfer risk to third party
2. Avoid the risk by not using specific tech/equipment
3. Reduce risk by minimizing damage and attack surface, implement defense
4. Accept the consequence

Risk Assessment

1. Identify company assets
2. Identify vulnerabilities
3. Identify threats and likelihood
4. Identify monetary impact

* Risk Register : Record of risk assessment, often referenced and updated

Qualitative vs Quantitative Risk Assessment

Qualitative Risk Assessment

Assigns numeric values to probability of risk and impact

Difficult to estimate exact values, must rely on history and survey

Quantitative Risk Assessment

Attempts to measure risk using exact monetary losses

1) Single Loss Expectancy (SLE)

2) Annual Rate of Occurrence (ARO)

3) Annual Loss Expectancy (ALE) = SLE X ARO

4) Mean time between failures (MTBF)

Average # of failures in a million hours of operations

Active vs Passive Security Analysis (Active vs Passive Reconnaissance)

Active Security Analysis

Employs actual testing (may interfere with regular operations)

Active Scanning

Passive Security Analysis

Analyzing network documentation

Passive fingerprinting

Security Controls

Categorical

1. Management : Focus on executive level decisions and risk management

2. Operational : Focus on individuals

User awareness, incident handling, fault tolerance

3. Technical : Focus on the system, firewall configurations, IPS/IDS

Definitive

4. Preventative : Employed before an event, designed to prevent

5. Detective : Employed during an event to find malicious activity

6. Corrective : Employed after an event to minimize damage

Vulnerability Management

Five step process

1. Define a desired state of security

2. Create a baseline

3. Vulnerability prioritization

4. Mitigate vulnerability

5. Monitor environment

Penetration Testing

A demonstration of vulnerabilities found in step 3 through exploits

Black box (no knowledge), Gray box(limited knowledge), Glass box

Pivot – Launching additional exploits after gaining network foothold

Persistence and Backdoors

Race Conditions

Basic Methodologies

1. OSSTMM

2. NIST Pen Testing Standard

OVAL – Standardized secure transfer of information on security

Assessing Vulnerabilities with Security Tools

Network Mapping

- Draw out the physical and logical connections of the network
- Use Network Topology Mapper
- AirMagnet(WiFi)
- Things to include in the diagram
  - Devices
  - IP Address
  - Role
  - Connections

Vulnerability Scanning

- Nessus – Basic vulnerability scanner
- Nmap – Basic port scanner
- Network Enumeration and Banner Grabbing

Network Sniffing

- Process of capturing and analyzing packets on a network
- Wireshark – Basic packet analyzer
- Fluke Networks – Hardware based network tester

Password Analysis

- Use password crackers to test strength of passwords
- Cain and Abel – Basic password cracker
- John the Ripper, Hydra, Aircrack-ng suite etc
- Password Storage locations
  - Windows – SAM hive, encrypted binary
  - Linux - /etc/passwd or /etc/shadow, encrypted

Chapter 13 : Monitoring and Auditing

Monitoring Methodologies

- Focus on Automated Monitoring
  1. Signature based monitoring
     - Matches predetermined attack patterns and packets/frames
     - Vulnerable to false negatives, need constant updates
  2. Anomaly based monitoring
     - Establishes a baseline and detects deviations from this baseline
     - Inaccurate baseline leads to false positives
  3. Behaviour based monitoring
     - Compare previous application behavior and detects current anomalies
     - Prone to false positive due to application diversity

Using Tools to Monitor Systems and Networks

- Performance Baselining
  - Baseline vs Baseline reporting
  - Security posture vs Security Poster Assessment
- Protocol Analyzer
  - Promiscuous vs Non-promiscuous mode for network adapters
  - Broadcast Storm Analysis
  - Header Manipulation Detection
  - TCP Handshake Analysis
  - Wireshark : Promiscuous mode capturing vs port mirroring vs network tap
  - Tcpdump for Unix/Linux
- SNMP (Simple Network Management Protocol)
  - TCP/IP, helps monitor network attached machines
  - Typical usage scenarios
    a) Managed Devices
    b) Agents
    c) Network Management System

- Inbound vs Outbound management

Analytical Tools

- compmgmt.msc & openfiles, net file & suite/netstat (Windows)
- lsof(list openfiles) & netstat (Linux)
- Static and Dynamic Tools
  - Static : openfiles, netstat that takes snapshot of network
  - Dynamic : Task Monitor, wireshark that captures packets over time

Conducting Audits

- Manual Assessment
  - Review of security logs, ACLs, user rights, permissions, group policy
  - Vulnerability scans
  - Personnel Interviews
- Overall Process
  1. Define audit target
  2. Create backups
  3. Scan, analyze and create a list of vulnerabilities/issues
  4. Calculate risk
  5. Develop a plan to minimize risk and fix issues
- Auditing Files
  - Able to set auditing and logging for file, folder and user
  - Review logs to ensure non-repudiation & beware of permission hierarchy
- Logging
  - compmgmt.msc in Windows allows viewing of security logs
  - Also pay attention to system and application logs
  - Syslog centralized log monitoring
- Log File Maintenance and Security
  - Logfile size, configuration and encryption
  - Backups and manually clear log files
- Auditing System Security Settings

Manage shared folders and user privileges in compmgmt.msc

Chapter 14 : Encryption and Hashing Concepts

Types of Data

a) Data in Use

b) Data at Rest

c) Data in Transit

Symmetric vs Asymmetric Algorithms

Symmetric : Uses same key for encryption/decryption

ex) DES, AES, RC, Kerberos (Key distribution center)

Stream vs Block Cipher modes

Suited for large volumes of data, fast and efficient

Asymmetric : Uses different keys for encryption/decryption

ex)RSA, Diffie-Hellman, Elliptic curve

Public and private keys are created for asymmetric key scheme

Key Management : Generation and secure storage of strong passwords

Steganography : Art of hiding information in various file formats, usually image files

Encryption Algorithms

DES/3DES

DES – 64 bit block cipher with 56 bit key

3DES – 64 bit block cipher with 168 bit key

AES

128 bit block size, variable key length (128, 192, 256 bit)

Current standard, fast and suited for hardware acceleration

RC

Widely used stream cipher, but vulnerable

Currently up to RC6

Blowfish/Twofish

128 bit block size with ~256 bit key size

RSA

1024/2048 bit key size

- Slow, suited for signing or specific encryption
- Vulnerable to MitM attacks, reliant on PKI and digital certificates

Diffie-Hellman

- Secure key exchange algorithm
- Also vulnerable to MitM attack, reliant on authentication methods
- Used in TLS
- Can also employ Ephemeral keys (EDH) for perfect forward secrecy

Elliptic Curve Crypto (ECC)

- Used in similar fashion to DH but faster and more compact
- Can be adopted into other algorithms
- Used in VoIP, IPSec
- Vulnerable to side channel and fault injection

Other Encryption Algorithms

- One time pads
  - Fast, theoretically pefect information secrecy
  - Practically dependent on security of PRNG
- PGP
  - Uses various ciphers but mainly employs RSA
  - Requires same versions to communicate properly, limitation
- PRNG
  - Written in C or Java for efficiency
  - Serves as a foundation for many cryptosystems
  - Weak PRNGs are often a vulnerability
- Emerging : AI, Genetic algorithms and stylometry

Hashing Basics

Provides message integrity

Cryptographic Hash Functions

- MD5
  - Used commonly for file integrity
  - Prone to MD5 hash collision attacks

SHA

Current standard is 256/512 bit SHA-2

RIPEMD & HMAC

LANMAN, NTLM, NTLMv2

Series of password hashing algorithms

LANMAN

Old Windows password hash based on DES

Deprecated and now considered a liability

Disable on either registry or local security policy

NTLM/NTLMv2

NTLM : Based on RC4, now broken

NTLMv2 : Based on HMAC-MD5

However, most Windows opt to use Kerberos instead

Hashing Attacks

Pass the Hash

Uses the saved password hash value to create an authenticated session

Mostly targets Windows/Kerberos for SSO function abuse

Use unique session tokens, multifactor, least privilege

Birthday Attack

Attempt to create a message with hash collision to original message

Targets hashes with weak hash collision resistance

Additional hashing concepts

Key Stretching / Salting

Chapter 15 : PKI and Encryption Protocols

PKI (Public Key Infrastructure)

A system of trust that uses public key crypto to bind a certificate to an identity

Certificates

Digitally signed electronic documents that binds a public key with an entity

Mostly based on X.509 format to facilitate SSO

Contains the following

a) User information and public key

b) Certificate authority information

- Name, digital signature, serial number, issue/expiration date

Mostly used for HTTPS connections, but can also be used for local encryption

Types of SSL Certificates

- Domain Validation
- Organizational Validation
- Extended Validation
- Wildcard Certificates

Single sided vs Double sided certificates

Single sided – validates the server to its user/clients

Double sided – Both server and user validates to each other

Certificate Chain of Trust

Used to validate different pieces of hardware & software

Also provides scalability and flexibility

Certificate Formats

Identifying certificate formats by extension and encoding

X.609 Encoding Rules

a) BER (Basic Encoding Rule)

b) CER (Canonical Encoding Rule)

c) DER (Distinguished Encoding Rule)

Certificate Formats and Extensions

1. PEM

ASCII encoded, contains “Begin/End Certificate” stmts

.pem/.crt/.cer/.key extensions

Uses DER, .der is in pure binary

2. P12/PFX

Pure binary encoding

.pfx/.p12 extensions

Used to import/export certificates and private keys

Certificate Authorities

Entity : Server that issues certificates to users

Trust third party, often used in HTTPS connections

Clicking on HTTPS padlock allows one to view cert details

Invalid certs are placed on certification revocation list

SSL pinning – attempts to prevent MitM

Online certificate status protocol

Key escrow

Key recovery agent

CA hierarchy w/ offline root CA

Web of Trust

Decentralized, self sign/publishing certificate system

Used by PGP

Security Protocols

Overview

Email : S/MIME, PGP

Web Login : SSL, TLS

Direct Conn. : SSH

Virtual Conn. : PPTP, L2TP

S/MIME

Used for authentication, message integrity and non-repudiation

Requires a digital ID certificate in MS Outlook to use

SSL/TLS

Used for secure internet communication such as browser, VoIP, email etc

Relies on PKI for obtaining and validating certificates

Asymmetric encryption (public key) Symmetric encryption (session key)

Can employ SSL/TLS accelerator

Also heavily used in E-commerce in HTTPS

Downgrade attack (FREAK & DROWN)

SSH

Uses public key crypto to establish remote authenticated connections

Also serves as basis for SFTP, SCP

PPTP, L2TP, IPSec

PPTP

Protocol used for VPNs

Supports PPP packets, designed for dial up but no security

Considered insecure in most cases

L2TP

By default has no encryption or security, but powerful when combined -

- with IPSec

Uses PKI when installed on Windows servers

IPSec

Authenticates and encrypts IP packets

Operates on lower levels of OSI (Network)

Made of 3 different protocols

1. Security Association (SA)
2. Authentication header
3. Encapsulating Security Payload

2 Modes of Implementation

1. Transport mode

Secure transfer of data, encrypted packet payload

Used within LAN or private network

2. Tunnel mode

   Entire packet is encrypted

   Facilitates VPN through internet

Chapter 16 : Redundancy and Disaster Recovery

Redundancy Planning

Redundancy is key to avoiding single points of failure

Redundant Power

Keep servers and networks alive in failures

Keep accessibility and minimize damage

Common electrical problems

1. Power Surges & Spikes

2. Sags, brownouts and blackouts

3. Power supply failure

Redundant Power Supplies

Enclosure that contains two or more power supplies

Common Vendors : HP, Cisco, Termaltake, Enlight

UPS(Uninterruptable Power Supplies)

Combined surge protector and backup battery (decoupling capacitors)

Cleans up dirty/noisy power like line conditioners

Considered temporary 5-30 min solution to resupply main or backup power

SPS(Standby power supply) vs UPS(Uninterruptable power supply)

Backup Generators

Serves as emergency power supply for an entire system

Standby Generators – automatically operates in a power outage

Types of Generators

a) Portable Gas Engine

b) Permanently Installed

c) Battery Inverter

Considerations

1. Price

2. Manual vs Automatic Operation

3. Uptime / Capacity, Power Output

4. Fuel Source

Common Vendors : Generac, Gillette, Kohler

Redundant Data

RAID Arrays

RAID 0 – Data Striping

RAID 1 – Data Mirroring

RAID 5 – Striping with parity

RAID 6 – Striping with double parity

RAID 10 – 2 RAID 1 mirrors striped

RAID Classification

a) Failure Resistant

b) Failure Tolerant

c) Disaster tolerant

* a < b < c in terms of protection scope

Redundant Networking

Server Network Adapters

Plan to install multiple redundant adapters

Consider centralized network adapter management software

Main switch/router connection

Always have spare switches/routers

Avoid pure star topologies and single points of failures

Internet Connection

Dual and redundant ISP internet connections

Consider mirror sites for web content

Redundant Servers

Goal : Minimize server downtime in failure and maximize throughput

Failover clusters

Designed so that secondary server takes over when primary fails

Provides high availability

Load balancing clusters

- Several servers share CPU, RAM, hard disk resources
- Commonly used in DNS, IRC and FTP servers
- Can also employ failover measures by replicating data between servers

- Redundant Sites (Physical locations)
  - Hot site – Complete replication of entire network, servers & phone lines
  - Warm site – Partial replication with some data recovery
  - Cold site – Minimal equipment replication
- Redundant people
  - Employ role takeover & primary/secondary personnel protocols

Disaster Recovery Plans and Procedures

- Data Backup
  - Tape Backup
    1. Full backup
    2. Incremental backup
    3. Differential backup
  - Backup Schemes
    1. 10 tape rotation
    2. Grandfather-father-son scheme (Daily, weekly, monthly)
    3. Tower of Hanos scheme
  - Snapshot backups
- DR Planning
  - Types of Disasters
    1. Fire
    2. Flood
    3. Long term power loss
    4. Theft and attack
    5. Loss of building access
  - Disaster Recovery Plans
    - Only include necessary information
    - Things to Include

- Contact Info
- Impact Evaluation : Asset loss and replacement costs
- Recovery Plan
- Business continuity plan
- Copies of various agreements
- Disaster recovery drills
- Critical system and data list

Chapter 17 : Social Engineering, User Education and Facilities Security

Social Engineering Scenarios

1. Pretexting
2. Malicious Insider
3. Diversion Theft
4. Phishing
    - Spearphishing
    - Whaling
5. Hoax
6. Shoulder Surfing
7. Eavesdropping
8. Dumpster Diving
9. Baiting
10. Piggybacking/tailgating
    - employ mantraps
11. Watering Hole attack

Facilities Security

Fire Suppression

a) Fire extinguishers

Fires are classified according to their source

Most fire extinguishers will also cause damage to electronics

1. Class A : Solid combustibles	Green Triangle
2. Class B : Flammable liquid and gas	Red Square
3. Class C : Electrical (use CO2 extinguisher)	Blue Circle
4. Class D : Metals (Magnesium, lithium etc)	Yellow Decagon
5. Class K : Cooking oil	Black Hexagon

Currently most electronics friendly extinguisher use FE-36 Halotron

b) Sprinkler

Wet pipe : Most common type

Dry pipe : Supply water only when needed

Pre-Action : Prevents accidental water discharges

c) Special Hazard Protection Systems

Uses special liquid FM-200

Electronics safe

d) HVAC (Heating, Ventilation and Air Conditioning)

Manages temperature and humidity

Hot and cold aisles

SCADA Industrial Control Systems

e) Shielding

STP wires to prevent cable interference

HVAC shielding

Faraday cages

TEMPEST guidelines

Vehicles

Disable mobile tethering in vehicles

CAN (Control Area Network, vehicle’s onboard network) vulnerabilities

GPS systems vulnerabilities

Airgapped Control Systems

Drones