CISSP & Security+ Cheat Sheet

Symmetric – Performance

Algorithm	Cipher Type
Hieroglyphics – First Known Cipher	None
Scytale (400 BC by the Spartans)	Transposition
Caesar	Mono-Substitution
Vigenere	Poly-Substitution
Vernam (One Time Pad) – Used in WWII in the German Enigma	XOR
DES [Lucifer] (56 bits)	Block
3DES (2 keys – 112 bits & 3 keys - 168 bits)	Block
AES [Rijndael] (128, 192, 256 bits)	Block
Blowfish	Block
Twofish	Block
IDEA	Block
RC2	Block
RC4 (used by WEP and WPA)	Stream
RC5	Block
RC6	Block
CAST	Block
MARS	Block
Serpent	Block
Twofish	Block
E0 (used by BlueTooth)	Stream

Asymmetric (Public Key Crypto) – Key Exchange

Diffie-Hellman Key Exchange (DH)

Digital Signature Algorithm (DSA)

El Gamal Encryption Algorithm

Elliptic Curve Cryptography (ECC)

Rivest, Shamir & Aldeman Encryption Algorithm (RSA)

Knapsack - *Defunct*

Goals of Cryptography	Achieved By
Confidentiality	Asymmetric (Public Key) & Symmetric Encryption
Authenticity/ Authentication/ Accountability	Asymmetric Encryption (Private Key), MAC/MIC, & Digital Signature
Integrity	Hashing, Checksum, Parity, & Check Digit
Non-Repudiation	Digital Signature (*Only*)

Hashing Algorithms - Integrity

Secure Hash Algorithm (SHA) [created by US Gov't] – 160 bit digest

Message Digest Series Algorithm (MD) [created by RSA] – 128 bit digest

Others: HAVAL, Tiger, WHIRLPOOL

Key Strength symmetric vs asymmetric

64 bit symmetric key strength =
512 bit asymmetric key strength

112 bit symmetric key strength =
1792 bit asymmetric key strength

128 bit symmetric key strength =
2304 bit asymmetric key strength

Remote Access

802.11, VPN, DUN (RADIUS, TACACS, TACACS+, SSL, Packet-level auth via IPSec Layer3

Access Control

MAC, DAC and RBAC (Rule or Role)

Basic Network Security Devices

Firewalls

Packet Filtering (Layer3)

Proxy Service

Circuit Level (Layer 3)

Application level (Layer 7)

Stateful Inspection (Layer 7)

Routers

Forward packets between subnets
RIP, IGRP, EIGRP, OSPF, BGP, EGP, IS-IS

Switches

Segment broadcast networks

Ports

Port	Use
21	FTP – usually in DMZ
22	SSH

Key Management and Certificate Lifecycle

Key Generation – a public key pair is created and held by the CA

Identity Submission – The requesting entity submits its identity to the CA

Registration – the CA registers the request and verifies the submission identity

Certification - The CA creates a certificate signed by its own digital certificate

Distribution – The CA publishes the generated certificate

Usage – The receiving entity is authorized to use the certificate only for its intended use

Revocation and expiration – The certificate will expire or may be revoked earlier if needed

Renewal – If needed, a new key pair can be generated and the cert renewed

Recovery – possible if a vertifying key is compromised but the holder is still valid and trusted

Archive – certificates and users are stored

Authentication

Kerberos – ticket based system, symmetric key KDC

CHAP – exchange of hashed values

Certificates used w/I a PKI for Asymmetric key

Username & **Password** most common

Token-based auth requires possession of token

Biometric authentication

Certificates

X.509 – User's public key, the CA (Certificate Authority) distinguished name, and the type of symmetric algorithm used for encryption.

SSL

The Secure Sockets Layer Protocol has two parts. **First**, the **SSL Handshake Protocol** establishes the secure channel. **Next**, the **SSL Application Data Protocol** is used to exchange data over the channel. 6 Steps in the handshaking process.

ISAKMP

(Internet Security Association and Key Management Protocol) used to negotiate and provide authenticated keying material for security associations in a protected manner

Authentication of peers
Threat management
Security association creation and management
Cryptographic key establishment and management

Bell La-Padula access control model

SOAS
subjects
objects
access modes
security levels

Diffie-Hellman algorithm

a secret key exchange over an insecure medium without any prior secrets.

Intrusion Detection

active responses

- collect additional information
- change the environment
- take action against the intruder

Based on **Console** and **Sensor**

IP Addresses

Class A	Class B	Class C
1-127	128-191	192-223
10.0.0.0	172.16.0.0 – 172.31.0.0	192.168.0.0
255.0.0.0	255.255.0.0	255.255.255.0
	65,000	

SQL

actions
objects
users

ATTACKS

DOS – Denial of Service

Smurf - Based on the ICMP echo reply

Fraggle - Smurf Like attack based on UDP packets

Ping Flood - Blocks Service through repeated pings

SYN Flood - Repeated SYN requests w/o ACK

Land – Exploits TCP/IP stacks using spoofed SYNs

Teardrop – An Attack using overlapping, fragmented UDP packets that cant be reassembled correctly

Bonk – An attack of port 53 using fragmented UDP packets w bogus reassembly information

Boink – Bonk like attack but on multiple ports

Backdoor

NetBus, Back Orifice

Spoofing

Process of making data look like it was from someone else

Man in the Middle

Intercepting traffic between 2 systems and using a third system pretending to be one of the others

Replay attack

posting of captured data

TCP/IP hijacking

session state is altered in a way that intercepts legitimate packets and allow a third party host to insert acceptable packets.

Mathematical attacks

(Key guessing)

Password guessing, brute force, dictionary attacks
guessing logons and passwords

Malicious Code

Viruses – Infect systems and spread copies of themselves

Trojan Horse – Disguise malicious code within apparently useful applications

Logic Bombs – Trigger on a particular condition

Worms – Self replicating forms of other types of malicious code

Java and Active X control – Automatically executes when sent via email

Social Engineering

Manipulating people – the most vulnerable point in a network

Business Continuity Plan

risk and analysis business
impact analysis strategic
planning and mitigation training
and awareness maintenance
and audit
Documentation and security labeling

Virus

replication mechanism
activation mechanism
objective

Wireless

WAP model – based on www model – Client, Gateway and Original Server

WEP – Wired Equivalent Privacy

23	Telnet
25	SMTP
49	TACACS
53	DNS
67 & 68	DHCP
80	HTTP
110	POP3
143	IMAP4
161	SNMP
389 & 636	LDAP
443	HTTPS / SSL
UDP 1701	L2TP
TCP 1723	PPTP

- **Integrity** - Assuring the recipient that a message has not been altered in transit. ensures all data is sequenced, and numbered.
- **PPTP** only works over **IP**.
- **Asymmetric encryption scheme** relies on both the sender and receiver to use different keys to encrypt and decrypt messages. Encryption and authentication can take place without sharing private keys. encrypt symmetric keys
- The **integrity** of a cryptographic system is considered compromised if the **private** key is disclosed.
- **WTLS** (Wireless Transport Layer Security) provides privacy, data integrity and authentication for handles devices in a wireless network environment.
- File encryption using symmetric cryptography satisfies **authentication**
- The primary DISADVANTAGE of **symmetric** cryptography is **key distribution**.
- **SYN Flood** - A network attack that misuses TCP's (Transmission Control Protocol) three way handshake to overload servers and deny access to legitimate users.
- When a user digitally signs a document an asymmetric algorithm is used to encrypt **hash** results
- **Least privilege** – need to know security basis.
- Applying **ingress filtering** to routers is the best method to prevent ip spoofing attacks.
- **MD5** (Message Digest 5) - A common algorithm used to verify the integrity of data from a remote user through a the creation of a 128-bit hash from a data input
- Worms are self replicating, Trojans are not.
- **Message authentication codes** are used to provide **integrity**.
- **False positive** - Incorrectly detecting authorized access as an intrusion or attack.
- **ICMP quoting** - What fingerprinting technique relies on the fact that operating systems differ in the amount of information that is quoted when ICMP (Internet Control Message Protocol) errors are encountered
- **SSL** - protocol typically used for encrypting traffic between a web browser and web server. Available in **40** and **128** bit encryption.
- **IPSec** - a popular VPN (Virtual Private Network) protocol operating at OSI (Open Systems Interconnect) model **Layer 3**.
- **Digital signatures** provide **authentication** and non-repudiation - not confidentiality.
- **DAC** (Discretionary Access Control) relies only on the identity of the user or process. Each object has an owner, which has full control over the object
  Access controls that are created and administered by the data owner
- **MAC -** Access controls based on security labels associated with each data item and each user. use levels of security to classify users and data
- **DEN** is **not** inferior to **SNMP**
- **Kerberos** - Time synchronization services for clients and servers..
- A **malformed MIME** (Multipurpose Internet Mail Extensions) header can cause an email server to crash.
- **Passive detection** – analyzing log files after an attack begins.
- the best defense against **man in the middle** attacks is **strong encryption, auth**
- Systems identified in a formal risk analysis process should be included in a disaster recover plan.
- **Certificate policy** - A PKI (Public Key Infrastructure) document that serves as the vehicle on which to base common interoperability standards and common assurance criteria on an industry wide basis.
- **Buffer overflow** – sends more traffic to a node than anticipated.
- **Differential** backup methods copies only modified files since the last full backup
- **IM** is a peer-to-peer network that offers most organizations virtually no control over it. Most vulnerable to sniffing
- **Decentralized** privilege management environment, user accounts and passwords are stored on each **individual** server.
- A **FTP bounce** attack is generally used to establish a connection between the FTP server and another computer
- **Network Based IDS** - a system for an internal network that will examine all packets for known attack signatures.
- **Ping of Death Attack** A network attack method that uses ICMP (Internet Control Message Protocol) and improperly formatted MTUs (Maximum Transmission Unit) to crash a target computer
- By **SSO**, the **authentication** problem of **multiple usernames and passwords** is addressed, browse multiple directories
- **PKI** (Public Key Infrastructure) - the best technical solution for reducing the threat of a man in the middle attack
- Security controls may become vulnerabilities in a system unless they are **adequately tested**.
- The standard encryption algorithm based on **Rijndael** is known as **AES.**
- **misuse detection** - Management wants to track personnel who visit unauthorized web sites.
- **Hosting** included in a **SLA** (Service Level Agreement) to ensure the availability of server based resources rather than guaranteed server performance levels
- **SSL** uses an **asymmetric** key and operates at the **session** layer
- **RAID** supports **High Availability**
- **Common Criteria -** The defacto IT (Information Technology) security evaluation criteria for the international community
- **Crime scene technician -** Tag, bag, and inventory evidence
- **Audit Log -** A collection of information that includes login, file access, other various activities, and actual or attempted legitimate and unauthorized violations
- **VLAN** - originally designed to decrease broadcast traffic but is also beneficial in reducing the likelihood of having information compromised by sniffers
- **Active detection** IDS systems may break off suspicious connections or shut down the server or service
- **CRL and OCSP** - two common methods when using a public key infrastructure for maintaining access to servers in a network
- **IPSec** Provides the Authentication Header (AH) for data integrity and Encapsulation Security Payload (ESP) for data confidentiality.
- **TCP SYN scan** - used to see what ports are in a listening state and then performs a two way handshake
- **NAT** (Network Address Translation) can be accomplished with **static** and **hide** NAT (Network Address Translation) and **PAT** (Port Address Translation)
- **Due care** - Policies and procedures intended to reduce the likelihood of damage or injury
- **Business impact analysis** - obtain formal agreement on maximum tolerable downtime
- Documenting change levels and revision information is most useful for **Disaster recovery**
- **worm** is able to distribute itself without using a host file
- **Single servers** are frequently the targets of attacks because they contain **credentials** for many systems and users
- **Multi-factor authentication** may be needed when a stored key and memorized password are not strong enough and additional layers of security is needed
- **VPN Drawback -** a firewall CAN NOT inspect encrypted traffic
- **man trap** - physical access control most adequately protects against physical piggybacking
- **LDAP** directories are arranged as Trees
- Data integrity is best achieved using a **Message** digest
- minimum length of a password be to deter **dictionary** password cracks 8
- **CRL** certificates that have been **disabled** before their scheduled expiration.
- **logging** - to keep a record of system **usage**
- **Security controls** may become vulnerabilities in a system unless they are **adequately tested**
- **RBAC** Access control decisions are based on responsibilities that an individual user or process has in an organization
- The start of the LDAP directory is called the **root**
- **HAS** encryption - **128** bits.
- **SSLv3**.0 (Secure Sockets Layer version 3.0) added the ability to **force client side authentication via digital certificates**
- **virus** - replication mechanism, activation mechanism and objective
- **Hashed passwords** subject to man in the middle attacks
- *The Secure Sockets Layer (**SSL**) protocol uses both **asymmetric** and **symmetric** key exchange. Use asymmetric keys for the SSL handshake. During the handshake, the master key, encrypted with the receiver public passes from the client to the server. The client and server make their own session keys using the master key. The session keys encrypt and decrypt data for the remainder of the session. Symmetric key exchange occurs during the exchange of the cipher specification, or encryption level.
- **PKI** technical solution for reducing the threat of **a man in the middle** attack
- **CRL** (Certificate Revocation List) query that receives a response in near real time **does not guarantee** that fresh data is being returned.
- **multi-homed** firewall If the firewall is compromised, only the systems in the DMZ (The main purpose of digital certificates is to bind a public key to the entity that holds the corresponding private key
- One of the factors that influence the lifespan of a public key certificate and its associated keys is the Length of the asymmetric hash.
- In order for a user to obtain a certificate from a trusted CA (Certificate Authority), the user must present proof of identity and a Public key
- What is the primary DISADVANTAGE of a third party relay Spammers can utilize the relay.
- The greater the keyspace and complexity of a password, the longer a attack may take to crack the password brute force
- The WAP (Wireless Application Protocol) programming model is based on the following three elements Client, gateway, original server
- What is a good practice in deploying a CA (Certificate Authority create a CPS (Certificate Practice Statement).
- What is the default transport layer protocol and port number that SSL (Secure Sockets Layer) uses TCP (Transmission Control Protocol) transport layer protocol and port 443
- What has 160-Bit encryption? SHA-1
- Which of the following is typically included in a CRL certificates that have been disabled before their scheduled expiration
- DDoS (Distributed Denial of Service) is most commonly accomplished by multiple servers or routers monopolizing and over whelming the bandwidth of a particular server or router.
- IMAP4 requires port ____ to be open 143

- **Extranet -** allows a business to securely transact with other businesses
- Controlling access to **information systems and associated networks** is necessary for the preservation of their **Confidentiality, integrity and availability** (Their CIA)
- **dual key pair** - Using distinct key pairs to separate confidentiality services from integrity services to support non-repudiation
- **Single Loss Expectancy** - **SLE** - is the cost of a single loss when it occurs - compiling estimates on how much money the company could lose if a risk occurred one time in the future.
- **Non-repudiation** is generally used to prevent the sender or the receiver from denying that the communication between them has occurred
- **Confidentiality** - The protection of data against unauthorized access or disclosure
- **Firewall** to allow employees in the company to DL FTP – set outbound port 23 allowed
- **SYN Attack –** exploits in the hand shaking
- During the digital signature process, hashing provides a means to verify what security requirement data integrity
- File encryption using symmetric cryptography satisfies what security requirement Authentication
- Which authentication protocol could be employed to encrypt passwords CHAP (Challenge Handshake Authentication Protocol)
- When User A applies to the CA (Certificate Authority) requesting a certificate to allow the start of communication with User B, User A must supply the CA (Certificate Authority) with User A’s public key only
- Demilitarized Zone) are exposed
- A common algorithm used to verify the integrity of data from a remote user through a the creation of a 128-bit hash from a data input is MD5 (Message Digest 5)