Domain 1: Security & Risk Management

CISSP Cheat Sheet Series comparitech

CIA Triad

Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Note – Encryption (At transit – TLS) (At rest - AES – 256)
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Availability	Ensuring timely and reliable access to and use of information by authorized users.

***Citation:** https://www.isc2.org/Certifications/CISSP/CISSP-Student-Glossary

Achieving CIA - Best Practices

Separation of Duties	Mandatory Vacations	Job Rotation	Least Privileges	Need to know	Dual Control

Availability Measuring Metrics	RTO/MTD/RPO, MTBF, SLA

D.A.D.

Disclosure	Alteration	Destruction
Opposite of Confidentiality	Opposite of Integrity	Opposite of Availability

IAAAA

Identification	Unique user identification
Authentication	Validation of identification
Authorization	Verification of privileges and permissions for authenticated user
Accountability	Only authorized users are accessing and use the system accordingly
Auditing	Tools, processes, and activities used to achieve and maintain compliance

Plans

Type	Duration	Example
Strategic Plan	up to 5 Years	Risk Assessment
Tactical Plan	Maximum of 1 year	Project budget, staffing etc
Operational Plan	A few months	Patching computers Updating AV signatures Daily network administration

Protection Mechanisms

Layering	Abstractions	Data Hiding	Encryption

Data classification

Entails analyzing the data that the organization retains, determining its importance and value, and then assigning it to a category.

Risk Management

- No risk can be completely avoided .
- Risks can be minimized and controlled to avoid impact of damages.
- Risk management is the process of identifying, examining, measuring, mitigating, or transferring risk

***Citation:**https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-and-risk-management/

Solution – Keep risks at a tolerable and acceptable level.
Risk management constraints – Time, budget

Risk Terminology

Asset	Anything of value to the company.
Vulnerability	A weakness; the absence of a safeguard
Threat	Things that could pose a risk to all or part of an asset
Threat Agent	The entity which carries out the attack
Exploit	An instance of compromise
Risk	The probability of a threat materializing

***Citation:**https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-and-risk-management/

Risk Management Frameworks

Preventive Ex ISO 27001	Deterrent Ex ISO 27000	Detective	Corrective	Recovery
Security Policies	Security Personnel	Logs	Alarms	Backups
Security Cameras	Guards	Security Cameras	Antivirus Solutions	Server Clustering
Callback	Security Cameras	Intrusion Detection Systems	Intrusion Detection Systems	Fault Tolerant Drive Systems
Security Awareness Training	Separation of Duties	Honey Pots	Business Continuity Plans	Database Shadowing
Job Rotation	Intrusion Alarms	Audit Trails		Antivirus Software
Encryption	Awareness Training	Mandatory Vacations		
Data Classification	Firewalls			
Smart Cards	Encryption			

Risk Framework Types

- Security and Risk Management
- Asset Security
- Security Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

Risk Management Life Cycle

Assessment	Analysis	Mitigation / Response
Categorize, Classify & Evaluate Assets	Qualitative vs Quantitative	Reduce, Transfer, Accept
as per NIST 800-30:	Qualitative – Judgments	Reduce / Avoid
System Characterization	Quantitative – Main terms	Transfer
Threat Identification	AV – Asset Value	Accept / Reject
Vulnerability Identification	EF – Exposure Factor	
Control Analysis	ARO – Annual Rate of Occurrence	
Likelihood Determination	Single Loss Expectancy = AV * EF	
Impact Analysis	Annual Loss Expectancy = SLE*ARO	
Risk Determination	Risk Value = Probability * Impact	
Control Recommendation		
Results Documentation		

Security Governance

- BS 7799
- ISO 17799 & 2700 Series
- COBIT & COSO
- OCTAVE
- ITIL

The 6 Steps of the Risk Management Framework

- **Categorize**
- **Select**
- **Implement**
- **Asses**
- **Authorize**
- **Monitor**

Threat Identification Models

S.T.R.I.D.E.	**S**poofing - **T**ampering - **R**epudiation - **I**nformation Disclosure - **D**enial of Service - **E**scalation of Privilege
D.R.E.A.D.	**D**amage - **R**eproducibility - **E**xploitability - **A**ffected - **D**iscoverability
M.A.R.T.	**M**itigate - **A**ccept - **R**eject - **T**ransfer

Disaster Recovery / Business Continuity Plan

- Continuity plan goals
- Statement of importance
- Statement of priorities
- Statement of organization responsibility
- Statement of urgency and timing
- Risk assessment
- Risk acceptance / mitigation

Types of Law

- Criminal law
- Civil Law
- Administrative Law
- Comprehensive Crime Control Act (1984)
- Computer Fraud and Abuse Act (1986)
- Computer Security Act (1987)
- Government Information Security Reform Act (2000)
- Federal Information Security Management Act (2002)

Intellectual Property

- Copyright
- Trademarks
- Patents
- Trade Secrets
- Licensing

Classification Levels

Military Sector	Private Sector
Top Secret	Sensitive
Secret	Confidential
Confidential	Private
Sensitive but unclassified	Company restricted
	Company confidential
Unclassified	Public

Typical Data Retention Durations

Business documents	7 years
Invoices	5 years
Accounts Payable / Receivable	7 years
Human Resources - Hired	7 years
Human Resources - Unhired	3 years
Tax records	4 years
Legal correspondence	Permanently

Data Security Controls

Data in Use	Scoping & tailoring
Data at Rest	Encryption
Data in Motion	Secure protocols e.g. https

Data Ownership

Data Ownership	Data Custodian	Systems Owners	Administrators	End User
Top level/Primary responsibility for data Define level of classification Define controls for levels of classification Define baseline security standards Impact analysis Decide when to destroy information	Grant permissions on daily basis Ensure compliance with data policy and data ownership guidelines Ensure accessibility, maintain and monitor security Data archive Data documentation Take regular backups , restore to check validations Ensure CIA Conduct user authorization Implement security controls	Apply Security Controls	Grant permission for data handling	Uses information for their job / tasks Adhere to security policies and guidelines

Data Remanence

Sanitizing	Series of processes that removes data, completely
Degaussing	Erase form magnetic tapes etc to ensure not recoverable
Erasing	Deletion of files or media
Overwriting	Writing over files, shredding
Zero fill	Overwrite all data on drives with zeros
Destruction	Physical destruction of data hardware device
Encryption	Make data unreadable without special keys or algorithm

Data Classification Criteria

Value - Usefulness - Age - Association

Data Retention Policies

The State of Florida Electronic Records and Records Management Practices, 2010
The European Documents Retention Guide, 2012

Security Policies, Standards & Guidelines

Regulatory	Required by law and industrial standards
Advisory	Not compulsory, but advisable
Informative	As guidance to others
Information Policy	Define best practices for information handling and usage -Security policies: Technical details of the policies i.e. SYSTEM security policy: lists hardware / software in use and steps for using policies
Standards	Define usage levels
Guidelines	Non-compulsory standards
Procedures	Steps for carrying out tasls and policies
Baseline	Minimum level of security

Standards

NIST	National Institute of Standards Technology
NIST SP 800 Series	Computer security in a variety of areas
800-14 NIST SP	Securing Information Technology systems
800-18 NIST	Develop security plans
800-27 NIST SP	Baseline for achieving security
800-88 NIST	Guidelines for sanitation and disposition, prevents data remanence
800-137	Continuous monitoring program: define, establish, implement, analyze and report
800-145	Cloud computing standards
FIPS	Federal Information Processing Standards

Security Models and Concepts

Security architecture frameworks	
Zachman Framework	A 2D model considering interrogations such as what, where and when with, etc. With various views such as planner, owner, designer etc.
Sherwood Applied Business Security Architecture (SABSA)	To facilitate communication between stakeholders
Information Technology Infrastructure Library (ITIL)	Set of best practices for IT service management
Security architecture documentation	
ISO/IEC 27000 Series	Establish security controls published by Standardization (ISO) and the Electrotechnical Commission (IEC)
Control Objectives for Information and Related Technology (CobiT)	Define goals and requirements for security controls and the mapping of IT security controls to business objectives.
Types of security models	
State Machine Models	Check each of the possible system state and ensure the proper security relationship between objects and subjects in each state.
Multilevel Lattice Models	Allocate each security subject a security label defining the highest and lowest boundaries of the subject's access to the system. Enforce controls to all objects by dividing them into levels known as lattices.
Matrix Based Models	Arrange tables known as matrix which includes subjects and objects defining what actions subjects can take upon another object.
Noninterference Models	Consider the state of the system at a point in time for a subject, it consider preventing the actions that take place at one level which can alter the state of another level.
Information Flow Models	Try to avoid the flow of information from one entity to another which can violate the security policy.
Confinement	Read and Write are allowed or restricted using a specific memory location, e.g. Sandboxing.
Data in Use	Scoping & tailoring

Security Modes

Dedicated Security Mode	Use a single classification level. All objects can access all subjects, but users they must sign an NDA and approved prior to access on need-to-know basis
System High Security Mode	All users get the same access level but all of them do not get the need-to-know clearance for all the information in the system.
Compartmented Security Mode	In addition to system high security level all the users should have need-to-know clearance and an NDA, and formal approval for all access required information.
Multilevel Security Mode	Use two classification levels as System Evaluation and Assurance Levels

Virtualization

Guest operating systems run on virtual machines and hypervisors run on one or more host physical machines.

Virtualization security threats	Trojan infected VMs, misconfigured hypervisor
Cloud computing models	Software as A Service (SaaS), Infrastructure As A Service (IaaS), Platform As A Service (PaaS)
Cloud computing threats	Account hijack, malware infections, data breach, loss of data and integrity

Memory Protection

Register	Directly access inbuilt CPU memory to access CPU and ALU.
Stack Memory Segment	Used by processors for intercommunication.
Monolithic Operating System Architecture	All of the code working in kernel mode/system.
Memory Addressing	Identification of memory locations by the processor.
Register Addressing	CPU access registry to get information.
Immediate Addressing	Part of an instruction during information supply to CPU.
Direct Addressing	Actual address of the memory location is used by CPU.
Indirect Addressing	Same as direct addressing but not the actual memory location.
Base + Offset Addressing	Value stored in registry is used as based value by the CPU.

*Citation CISSP SUMMARY BY Maarten De Frankrijker

Cryptographic Terminology

Encryption	Convert data from plaintext to cipher text.
Decryption	Convert from ciphertext to plaintext.
Key	A value used in encryption conversion process.
Synchronous	Encryption or decryption happens simultaneously.
Asynchronous	Encryption or decryption requests done subsequently or after a waiting period.
Symmetric	Single private key use for encryption and decryption.
Asymmetrical	Key pair use for encrypting and decrypting. (One private and one public key)
Digital Signature	Use to verify authentication and message integrity of the sender. The message use as an input to a hash functions for validating user authentication.
Hash	A one-way function, convert message to a hash value used to verify message integrity by comparing sender and receiver values.
Digital Certificate	An electronic document that authenticate certification owner.
Plaintext	Simple text message.
Ciphertext	Normal text converted to special format where it is unreadable without reconversion using keys.
Cryptosystem	The set of components used for encryption. Includes algorithm, key and key management functions.
Cryptanalysis	Breaking decrypting ciphertext without knowledge of cryptosystem used.
Cryptographic Algorithm	Procedure of enciphers plaintext and deciphers cipher text.
Cryptography	The science of hiding the communication messages from unauthorized recipients.
Cryptology	Cryptography + Cryptanalysis
Decipher	Convert the message as readable.
Encipher	Convert the message as unreadable or meaningless.
One-time pad (OTP)	Encipher all of the characters with separate unique keys.
Key Clustering	Different encryption keys generate the same plaintext message.
Key Space	Every possible key value for a specific algorithm.
Algorithm	A mathematical function used in encryption and decryption of data; A.K.A. cipher.
Cryptology	The science of encryption.
Transposition	Rearranging the plaintext to hide the original message; A.K.A. Permutation.
Substitution	Exchanging or repeating characters (1 byte) in a message with another message.
Vernam	Key of a random set of non-repeating characters. A.K.A. One time pad.
Confusion	Changing a key value during each circle of the encryption.
Diffusion	Changing the location of the plaintext inside the cipher text.
Avalanche Effect	When any change in the key or plaintext significantly change the ciphertext.
Split Knowledge	Segregation of Duties and Dual Control.
Work factor	The time and resources needed to break the encryption.
Nonce	Arbitrary number to provide randomness to cryptographic function.
Block Cipher	Dividing plaintext into blocks and assign similar encryption algorithm and key.
Stream Cipher	Encrypt bit wise - one bit at a time with corresponding digit of the keystream.
Dumpster Diving	Unauthorized access a trash to find confidential information.
Phishing	Sending spoofed messages as originate from a trusted source.
Social Engineering	Mislead a person to provide confidential information.
Script kiddie	A moderate level hacker that uses readily found code from the internet.

Requirements for Hashing Message Digest

Variable length input - easy to compute - one way function - digital signatures - fixed length output

MD Hash Algorithms

MD2	128-bit hash, 18 rounds of computations
MD4	128-bit hash. 3 rounds of computations, 512 bits block sizes
MD5	128-bit hash. 4 rounds of computations, 512 bits block sizes, Merkle–Damgård construction
MD6	Variable, 0<d≤512 bits, Merkle tree structure
SHA-0	Phased out, collision found with a complexity of 2^33.6 (approx 1 hr on standard PC) Retired by NIST
SHA-1	160-bit MD, 80 rounds of computations, 512 bits block sizes, Merkle–Damgård construction (not considered safe against well funded attackers)
SHA-2	224, 256, 384, or 512 bits, 64 or 80 rounds of computations, 512 or 1024 bits block sizes, Merkle–Damgård construction with Davies–Meyer compression function

Security Models

MATRIX (Access control model)	- Provides access rights including discretionary access control to subjects for different objects. - Read, write and execute access defined in ACL as matrix columns and rows as capability lists.
BELL-LAPADULA (Confidentiality model)	-A subject cannot read data at a higher security level. (A.K.A simple security rule) - Subject in a defined security level cannot write to a lower security level unless it is a trusted subject. (A.K.A *-property (star property) rule - Access matrix specifies discretionary access control. - subject with read and write access should write and read at the same security level (A.K.A Strong star rule :) - Tranquility prevents security level of subjects change between levels.
BIBA (Integrity model)	- Cannot read data from a lower integrity level (A.K.A The simple integrity axiom) - Cannot write data to an object at a higher integrity level. (A.K.A the * (star) integrity axiom) - Cannot invoke service at higher integrity. (A.K.A The invocation property) - Consider preventing information flow from a low security level to a high security level.
CLARK WILSON (Integrity model)	User: An active agent • Transformation Procedure (TP): An abstract operation, such as read, writes, and modify, implemented through Programming • Constrained Data Item (CDI): An item that can be manipulated only through a TP • Unconstrained Data Item (UDI): An item that can be manipulated by a user via read and write operations - Enforces separation of duty - Requires auditing - Commercial use - Data item whose integrity need to be preserved should be audited - An integrity verification procedure (IVP) -scans data items and confirms their integrity against external threats
Information flow model	Information is restricted to flow in the directions that are permitted by the security policy. Thus flow of information from one security level to another. (Bell & Biba).
Brewer and Nash (A.K.A Chinese wall model)	- Use a dynamic access control based on objects previous actions. - Subject can write to an object if, and only if, the subject cannot read another object in a different dataset. - Prevents conflict of interests among objects. Citation https://ipspecialist.net/fundamental-concepts-of-security-models-how-they-work/
Lipner Model	Commercial mode (Confidentiality and Integrity,) -BLP + Biba
Graham-Denning Model Objects, subjects and 8 rules	Rule 1: Transfer Access, Rule 2: Grant Access, Rule 3: Delete Access, Rule 4: Read Object, Rule 5: Create Object, Rule 6: destroy Object, Rule 7: Create Subject, Rule 8: Destroy
Harrison-Ruzzo-Ullman Model	Restricts operations able to perform on an object to a defined set to preserve integrity.

Web Security

OWASP	Open-source application security project. OWASP creates guidelines, testing procedures, and tools to use with web security.
OWASP Top 10	Injection / SQL Injection, Broken Authentication, Sensitive Data Exposure, XML External Entity, Broken Access Control, Security Misconfiguration, Cross-Site Scripting (XSS), Insecure Deserialization, Using Components with Known Vulnerabilities, Insufficient Logging and Monitoring
SQL Injections:	Attackers try to exploit by allowing user input to modify the back-end/server of the web application or execute harmful code which includes special characters inside SQL codes results in deleting database tables etc.
SQL Injection prevention:	Validate the inputs and parameters.
Cross-Site Scripting (XSS)	Attacks carryout by inputting invalidated scripts inside webpages.
Cross-Request Forgery	Attackers use POST/GET requests of the http web pages with HTML forms to carry out malicious activity with user accounts. Prevention can be done by authorization user accounts to carry the actions. Eg. using a Random string in the form, and store it on the server.

Cryptography

Cryptography Goals (P.A.I.N.)	• P - Privacy (Confidentiality) • A – Authentication • I - Integrity • N - Non-Repudiation. • Key space = 2n. (n is number of key bits)
Use of Cryptography	• Confidentiality • Integrity • Proof of origin • Non-repudiation • Protect data at rest • Protect data in transit

Codes vs. Ciphers

Classical Ciphers	Substitution cipher, Transposition cipher, Caesar Cipher, Concealment.
Modern Ciphers	Block cipher, Stream cipher, Steganography, Combination.
Concealment Cipher	Cipher converts Plaintext to another written text to hide original text.
Substitution Ciphers	Uses a key to substitute letters or blocks of letters with different letters or block of letters. I.e. One-time pad, stenography.
Transposition Ciphers	Reorder or scramble the letters of the original message where the key used to decide the positions to which the letters are moved.

Common Algorithms

Algorithm	Symmetric/ Asymmetric	Key length	Based on	Structure
DES	Symmetric	64 bit	Lucifer algorithm	64 bit cipher block size and 56 bit key with 8 bits parity. • 16 rounds of transposition and substitution (ECB, CBC, CFB, OFB, CTR)
3 DES or TDES (Triple DES)	Symmetric	56 bit*3	DES	3 * 56 bit keys • Slower than DES but higher security (DES EE3, DES EDE3 ,DES EEE2, DES EDE2)
AES	Symmetric	128,192 or 256 bit	Rijndael algorithm	Use 3 different bit size keys Examples Bitlocker, Microsoft EFS Fast, secure 10,12, and 14 transformation rounds
IDEA	symmetric	128 bit		64 bit cipher blocks each block divide to 16 smaller blocks Each block undergo 8 rounds of transformation Example PGP
Skipjack	Symmetric	80 bit		64 bit Block cipher
Blowfish	Symmetric	32-448bit		64 bit Block cipher
TwoFish	Symmetric	128, 192, 256		128 bit blocks
RC4	Symmetric	40-2048		Example SSL and WEP • Stream cipher • 256 Rounds of transformation
RC5	Symmetric	2048		255 rounds transformation • 32, 64 & 128 bit block sizes
CAST	Symmetric	CAST 128 (40 to 128 bit) CAST 256 (128 to 256 bit)		64 bit block 12 transformation rounds 128 bit block 48 rounds transformation
Diffie - Hellman	Asymmetric			No confidentiality, authentication, or non-repudiation • Secure key transfer
RSA	Asymmetric	4096 bit		Uses 1024 keys • Public key and one-way function for encryption and digital signature verification • Private key and one-way function for decryption and digital signature generation • Used for encryption, key exchange and digital signatures
Elgamal	Asymmetric	Any key size	Diffie - Hellman algorithm	Used for encryption, key exchange and digital signatures • Slower
Elliptic Curve Cryptosystem (ECC)	Asymmetric	Any key size		Used for encryption, key exchange and digital signatures • Speed and efficiency and better security

Cryptographic Attacks

Passive Attacks	Use eavesdropping or packet sniffing to find or gain access to information.	**Algebraic Attack**	Uses known words to find out the keys
Active Attacks	Attacker tries different methods such as message or file modification attempting to break encryption keys, algorithm.	**Frequency Analysis**	Attacker assumes substitution and transposition ciphers use repeated patterns in ciphertext.
Ciphertext-Only Attack	An attacker uses multiple encrypted texts to find out the key used for encryption.	**Birthday Attack**	Assumes figuring out two messages with the same hash value is easier than message with its own hash value
Known Plaintext Attack	An attacker uses plain text and cipher text to find out the key used for encryption using reverse engineering or brute force encryption.	**Dictionary Attacks**	Uses all the words in the dictionary to find out correct key
Chosen Plaintext Attack	An attacker sends a message to another user expecting the user will forward that message as cipher text.	**Replay Attacks**	Attacker sends the same data repeatedly to trick the receiver.
Social Engineering Attack	An attacker attempts to trick users into giving their attacker try to impersonate another user to obtain the cryptographic key used.	**Analytic Attack**	An attacker uses known weaknesses of the algorithm
Brute Force	Try all possible patterns and combinations to find correct key.	**Statistical Attack**	An attacker uses known statistical weaknesses of the algorithm
Differential Cryptanalysis	Calculate the execution times and power required by the cryptographic device. A.K.A. Side-Channel attacks	**Factoring Attack**	By using the solutions of factoring large numbers in RSA
Linear Cryptanalysis	Uses linear approximation	**Reverse Engineering**	Use a cryptographic device to decrypt the key

System Evaluation and Assurance Levels

Trusted Computer System Evaluation Criteria (TCSEC)	Evaluates operating systems, application and systems. But not network part. Consider only about confidentiality. Operational assurance requirements for TCSEC are: System Architecture, System Integrity, Covert Channel analysis, Trusted Facility Management and Trusted recovery.
Orange Book	A collection of criteria based on the Bell-LaPadula model used to grade or rate the security offered by a computer system product.
Red Book	Similar to the Orange Book but addresses network security.
Green Book	Password Management.
Trusted Computer System Evaluation Criteria (TCSEC)	Evaluates operating systems, application and systems. But not network part. Consider only about confidentiality. Operational assurance requirements for TCSEC are: System Architecture, System Integrity, Covert Channel analysis, Trusted Facility Management and Trusted recovery.
ITSEC	Consider all 3 CIA (integrity and availability as well as confidentiality

TCSEC	Explanation
D	Minimal protection
C1	DAC; Discretionary Protection (identification, authentication, resource protection)
C2	DAC; Controlled access protection
B1	MAC; Labeled security (process isolation, devices)
B2	MAC; Structured protection
B3	MAC; security domain
A	MAC; verified protection
Common criteria assurance levels	
EAL0	Inadequate assurance
EAL1	Functionality tested
EAL2	Structurally tested
EAL3	Methodically tested and checked
EAL4	Methodically designed, tested and reviewed
EAL5	Semi-formally designed and tested
EAL6	Semi-formally verified, designed and tested
EAL7	Formally verified, designed and tested
ITSEC security evaluation criteria - required levels	
D + E0	Minimum Protection
C1 + E1	Discretionary Protection (DAC)
C2 + E2	Controlled Access Protection (Media cleansing for reusability)
B1 + E3	Labelled Security (Labelling of data)
B2 + E4	Structured Domain (Addresses Covert channel)
B3 + E5	Security Domain (Isolation)
A + E6	Verified Protection (B3 + Dev Cycle)
Common criteria protection profile components	
Descriptive Elements • Rationale • Functional Requirements • Development assurance requirements • Evaluation assurance requirements	
Certification & Accreditation	
Certification	Evaluation of security and technical/non-technical features to ensure if it meets specified requirements to achieve accreditation.
Accreditation	Declare that an IT system is approved to operate in predefined conditions defined as a set of safety measures at given risk level.
NIACAP Accreditation Process	
Phase 1: Definition • Phase 2: Verification • Phase 3: Validation • Phase 4: Post Accreditation	
Accreditation Types	
Type Accreditation	Evaluates a system distributed in different locations.
System Accreditation	Evaluates an application system.
Site Accreditation	Evaluates the system at a specific location.

Symmetric vs. Asymmetric Encryption

Symmetric Algorithms	Use a private key which is a secret key between two parties. Each party needs a unique and separate private key. Number of keys = x(x-1)/2 where x is the number of users. Eg. DES, AES, IDEA, Skipjack, Blowfish, Twofish, RC4/5/6, and CAST.
Stream Based Symmetric Cipher	Encryption done bitwise and use keystream generators Eg. RC4.
Block Symmetric Cipher	Encryption done by dividing the message into fixed-length blocks Eg. IDEA, Blowfish and, RC5/6.
Asymmetric Algorithms	Use public and private key where both parties know the public and the private key known by the owner .Public key encrypts the message, and private key decrypts the message. 2x is total number of keys where x is number of users. Eg. Diffie-Hellman, RSA, El Gamal, ECC, Knapsack, DSA, and Zero Knowledge Proof.

Symmetric Algorithms	Asymmetric Algorithms	Hybrid Cryptography
Use of private key which is a secret key	Use of public and private key pairs	Use of both Symmetric and Asymmetric encryption. Eg. SSL/TLS
Provides confidentiality but not authentication or nonrepudiation	Provides confidentiality, integrity, authentication, and nonrepudiation	Provide integrity. One way function divides a message or a data file into a smaller fixed length chunks.
One key encrypts and decrypts	One key encrypts and other key decrypts	Encrypted with the private key of the sender.
Larger key size. Bulk encryptions	Small blocks and key sizes	Message Authentication Code (MAC) used to encrypt the hash function with a symmetric key.
Faster and less complex. Not scalable	Slower. More scalable.	Allows for more trade-offs between speed, complexity, and scalability.
Out-of-band key exchange	In-band key exchange	Hash Functions and Digital Certificates Hashing use message digests.

Key Escrow and Recovery

Secret key is divided into two parts and handover to a third party.

PKI

confidentiality, message integrity, authentication, and nonrepudiation

Receiver's Public Key-Encrypt message
Sender Private Key-Decrypt message
Sender Private Key-Digitally sign
Sender's Public Key - Verify Signature

PKI Structure

Certificates	Provides authorization between the parties verified by CA.
Certificate Authority	Authority performing verification of identities and provides certificates.
Registration Authority	Help CA with verification.
Certification Path Validation	Certificate validity from top level.
Certification Revocation List	Valid certificates list
Online Certificate status protocol (OCSP)	Used to check certificate validity online
Cross-Certification	Create a trust relationship between two CA's

Digital Signatures

• Sender's private key used to encrypt hash value
• Provides authentication, nonrepudiation, and integrity
• Public key cryptography used to generate digital signatures
• Users register public keys with a certification authority (CA).
• Digital signature is generated by the user's public key and validity period according to the certificate issuer and digital signature algorithm identifier.

Digital Certificate - Steps

Enrollment - Verification - Revocation

Cryptography Applications & Secure Protocols

Hardware -BitLocker and truecrypt	• **BitLocker:** Windows full volume encryption feature (Vista onward) • **truecrypt:** freeware utility for on-the-fly encryption (discontinued)
Hardware-Trusted Platform Module (TPM)	A hardware chip installed on a motherboard used to manage Symmetric and asymmetric keys, hashes, and digital certificates. TPM protect passwords, encrypt drives, and manage digital permissions.
Link encryption	Encrypts entire packet components except Data Link Control information.
End to end encryption	Packet routing, headers, and addresses not encrypted.
Email (PGP)	Privacy (Encrypt), Authentication (Digital signature), Integrity, (Hash) and Non-repudiation (Digital signature) Email (Secure MIME (S/MIME): Encryption for confidentiality, Hashing for integrity, Public key certificates for authentication, and Message Digests for nonrepudiation.
Web application	SSL/TLS. SSL encryption, authentication and integrity.
Cross-Certification	Create a trust relationship between two CA's
IPSEC	(Privacy, authentication, Integrity, Non Repudiation). Tunnel mode encrypt whole packet (Secure). Transport mode encrypt payload (Faster)
IPSEC components	Authentication Header (AH): Authentication, Integrity, Non repudiation. Encapsulated Security Payload (ESP): Privacy, Authentication, and Integrity. Security Association (SA): Distinct Identifier of a secure connection.
ISAKMP	Internet Security Association Key Management Protocol Authentication, use to create and manage SA, key generation.
Internet Key Exchange (IKE)	Key exchange used by IPsec .Consists of OAKLEY and Internet Security Association and Key Management Protocol (ISAKMP). IKE use Pre-Shared keys, certificates, and public key authentication.
Wireless encryption	Wired Equivalent Privacy (WEP): 64 & 128 bit encryption. Wi-Fi Protected Access (WPA): Uses TKIP. More secure than WEP WPA2: Uses AES. More secure than WEP and WPA.

Hardware architecture

Multitasking	Simultaneous running of two or more tasks.
Multi programming	Simultaneous running of two or more programs
Multi-processing	CPU consists or more than one processor
Processing Types	
Single State	One security level at a time.
Multi State	Multiple security levels at a time.
Firmware	Software built in to in the ROM.
Base Input Output System (BIOS)	Set of instructions used to load OS by the computer.

Mobile Security

Device Encryption • Remote wiping • Remote lock out • Internal locks (voice, face recognition, pattern, pin, password) • Application installation control • Asset tracking (IMIE) • Mobile Device Management • Removable storage (SD CARD, Micro SD etc.)

IoT & Internet Security

Network Segmentation (Isolation) • Logical Isolation (VLAN) • Physical isolation (Network segments) • Application firewalls • Firmware updates

Physical Security

Internal vs external threat and mitigation	
Natural threats	Hurricanes, tornadoes, earthquakes floods, tsunami, fire, etc
Politically motivated threats	Bombs, terrorist actions, etc
Power/utility supply threats	General infrastructure damage (electricity telecom, water, gas, etc)
Man Made threats	Sabotage, vandalism, fraud, theft
Major sources to check	Liquids, heat, gases, viruses, bacteria, movement: (earthquakes), radiation, etc
Natural threat control measures	
Hurricanes, Tornadoes, Earthquakes	Move or check location, frequency of occurrence, and impact. Allocate budget.
Floods	Raised flooring server rooms and offices to keep computer devices .
Electrical	UPS, Onsite generators
Temperature	Fix temperature sensors inside server rooms , Communications - Redundant internet links, mobile communication links as a back up to cable internet.
Man-Made Threats	
Explosions	Avoid areas where explosions can occur Eg. Mining, Military training etc.
Fire	Minimum 2 hour fire rating for walls, Fire alarms, Fire extinguishers.
Vandalism	Deploy perimeter security, double locks, security camera etc.
Fraud/Theft	Use measures to avoid physical access to critical systems. Eg. Fingerprint scanning for doors.

Site Selection

Physical security goals	Deter Criminal Activity - Delay Intruders - Detect Intruders - Assess Situation - Respond to Intrusion
Site selection issues	Visibility - External Entities - Accessibility - Construction - Internal Compartments
Server room security	• Middle of the building (Middle floor) • Single access door or entry point • Fire detection and suppression systems • Raised flooring • Redundant power supplies • Solid /Unbreakable doors
Fences and Gates	8 feet and taller with razor wire. Remote controlled underground concealed gates.
Perimeter Intrusion Detection Systems	Infrared Sensors - Electromechanical Systems - Acoustical Systems - CCTV - Smart cards - Fingerprint/retina scanning
Lighting Systems	Continuous Lighting - Standby Lighting - Movable Lighting - Emergency Lighting
Media storage	Offsite media storage - redundant backups and storage
Electricity	Faraday Cage to avoid electromagnetic emissions - White noise results in signal interference - Control Zone: Faraday cage + White noise
Static Electricity	Use anti-static spray, mats and wristbands when handling electrical equipment - Monitor and maintain humidity levels.
HVAC control levels	Heat - High Humidity - Low Humidity
HVAC Guidelines	• 100F can damage storage media such as tape drives. • 175 F can cause computer and electrical equipment damage. • 350 F can result in fires due to paper based products. • HVAC: UPS, and surge protectors to prevent electric surcharge. • Noise: Electromagnetic Interference (EMI), Radio Frequency Interference Temperatures, Humidity • Computer Rooms should have 15° C - 23°C temperature and 40 - 60% (Humidity)
Voltage levels control	• Static Voltage • 40v can damage Circuits, 1000v Flickering monitors, 1500v can cause loss of stored data, 2000v can cause System shut down or reboot, 17000 v can cause complete electronic circuit damage.
Equipment safety	Fire proof Safety lockers - Access control for locking mechanisms such as keys and passwords.
Water leakage	Maintain raised floor and proper drainage systems. Use of barriers such as sand bags
Fire safety	Fire retardant materials - Fire suppression - Hot Aisle/Cold Aisle Containment - Fire triangle (Oxygen - Heat - Fuel) - Water, CO2, Halon

Fire extinguishers

Class	Type	Suppression
A	Common combustible	Water , SODA acid
B	Liquid	CO2, HALON, SODA acid
C	Electrical	CO2, HALON
D	Metal	Dry Powder

Water based suppression systems	Wet pipes - Dry Pipe - Deluge
Personnel safety	• HI VIS clothes • Safety garments /Boots • Design and Deploy an Occupant Emergency Plan (OEP)
Internal Security	• Programmable multiple control locks • Electronic Access Control - Digital scanning, Sensors • Door entry cards and badges for staff • Motion Detectors- Infrared, Heat Based, Wave Pattern, Photoelectric, Passive audio motion
Key management	Create, distribute, transmission, storage - Automatic integration to application for key distribution, storage, and handling. Backup keys should be stored secure by designated person only.
Testing	Pilot testing for all the backups and safety systems to check the working condition and to find any faults.

OSI Reference Model

7 layers, Allow changes between layers, Standard hardware/software interoperability.

Tip, OSI Mnemonics
All **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing
Please **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way

Layer	Data	Security
Application	Data	C, I, AU, N
Presentation	Data	C, AU, Encryption
Session	Data	N
Transport	Segment	C, AU, I
Network	Packets	C, AU, I
Data link	Frames	C
Physical	Bits	C

C=Confidentiality, AU=Authentication, I=Integrity, N=Non repudiation

Layer (No)	Functions	Protocols	Hardware / Formats
Physical (1)	Electrical signal Bits to voltage		Cables, HUB, USB, DSL Repeaters, ATM
Data Link Layer (2)	Frames setup Error detection and control Check integrity of packets Destination address, Frames use in MAC to IP address conversion.	PPP - PPTP - L2TP - - ARP - RARP - SNAP - CHAP - LCP - MLP - Frame Relay - HDLC - ISL - MAC - Ethernet - Token Ring - FDDI	Layer 2 Switch - bridges
Network layer	Routing, Layer 3 switching, segmentation, logical addressing. ATM. Packets.	ICMP - BGP - OSPF - RIP - IP - BOOTP - DHCP - ICMP	Layer 3 Switch - Router
Transport	Segment - Connection oriented	TCP - UDP datagrams. Reliable end to end data transfer - Segmentation - sequencing - and error checking	Routers - VPN concentrators - Gateway
Session Layer	Data, simplex, half duplex, full dupl Eg. peer connections.	TCP - UDP - NSF - SQL - RADIUS - and RPC - PPTP - PPP	Gateways
Presentation layer	Data compression/decompression and encryption/decryption	TCP - UDP messages	Gateways JPEG - TIFF - MID - HTML
Application layer	Data	TCP - UDP - FTP - TELNET - TFTP - SMTP - HTTP CDP - SMB - SNMP - NNTP - SSL - HTTP/HTTPS.	Gateways

TCP/IP Model

Layers	Action	Example Protocols
Network access	Data transfer done at this layer	Token ring • Frame Relay • FDDI • Ethernet • X.25
Internet	Create small data chunks called datagrams to be transferred via network access layer	IP • RARP • ARP • IGMP • ICMP
Transport	Flow control and integrity	TCP • UDP
Application	Convert data into readable format	Telnet • SSH • DNS • HTTP • FTP • SNMP • DHCP

TCP 3-way Handshake

SYN - SYN/ACK - ACK

LAN Topologies

Topology	Pros	Cons
BUS	• Simple to setup	• No redundancy • Single point of failure • Difficult to troubleshoot
RING	• Fault tolerance	• No middle point
Start	• Fault tolerance	• Single point of failure
Mesh	• Fault tolerance	• Redundant • Expensive to setup

Types of Digital Subscriber Lines (DSL)

Asymmetric Digital Subscriber Line (ADSL)	• Download speed higher than upload • Maximum 5500 meters distance via telephone lines. • Maximum download 8Mbps, upload 800Kbps.
Rate Adaptive DSL (RADSL)	• Upload speed adjust based on quality of the transmission line • Maximum 7Mbps download, 1Mbps upload over 5500 meters.
Symmetric Digital Subscriber Line (SDSL)	• Same rate for upstream and downstream transmission rates. • Distance 6700 meters via copper telephone cables • Maximum 2.3Mbps download, 2.3Mbps upload.
Very-high-bit-rate DSL (VDSL)	• Higher speeds than standard ADSL • Maximum 52Mbps download, 16 Mbps upload up to 1200 Meters
High-bit-rate DSL (HDSL)	T1 speed for two copper cables for 3650 meters
Committed Information Rate (CIR)	Minimum guaranteed bandwidth provided by service provider.

LAN Packet Transmission

Unicast	Single source send to single destination
Multicast	Single source send to multiple destinations
Broadcast	Source packet send to all the destinations.
Carrier-sense Multiple Access (CSMA)	One workstations retransmits frames until destination workstation receives.
CSMA with Collision Detection (CSMA/CD)	Terminates transmission on collision detection. Used by Ethernet.
CSMA with Collision Avoidance (CSMA/CA)	Upon detecting a busy transmission, pauses and then re-transmits delayed transmission at random interval to minimise two nodes re-sending at same time.
Polling	Sender sends only if polling system is free for the destination.
Token-passing	Sender can send only when token received indicating free to send.
Broadcast Domain	Set of devices which receive broadcasts.
Collision Domain	Set of devices which can create collisions during simultaneous transfer of data.
Layer 2 Switch	Creates VLANs
Layer 3 Switch	Interconnects VLANs

LAN / WAN Media

Twisted Pair	Pair of twisted copper wires. Used in ETHERNET. Cat5/5e/6. Cat5 speed up to 100Mbps over 100 meters. Cat5e/6 speed 1000Mbps.
Unshielded Twisted Pair (UTP)	Less immune to Electromagnetic Interference (EMI)
Shielded Twisted Pair (STP)	Similar to UTP but includes a protective shield.
Coaxial Cable	Thick conduit instead of two copper wires. 10BASE-T, 100BASE-T, and 1000BASE-T.
Fiber Optic	Uses light as the media to transmit signals. Gigabit speed at long distance. Less errors and signal loss. Immune to EMI. Multimode and single mode. Single mode for outdoor long distance.
Frame Relay WAN	Over a public switched network. High Fault tolerance by relaying fault segments to working.

Secure Network Design - Components

Network address translation (NAT)	Hide internal public IP address from external internet
Port Address Translation (PAT)	Allow sharing of public IP address for internal devices and applications using a given single public IP address assigned by ISP
Stateful NAT	Keeps track of packets transfer between source and destinations
Static NAT	One to one private to public IP address assigned between two end devices
Dynamic NAT	Pool of internal IP maps one or several public IP address

Common TCP Protocols

Port	Protocol
20,21	FTP
22	SSH
23	TELNET
25	SMTP
53	DNS
110	POP3
80	HTTP
143	IMAP
389	LDAP
443	HTTPS
636	Secure LDAP
445	ACTIVE DIRECTORY
1433	Microsoft SQL
3389	RDP
137-139	NETBIOS

Attacks in OSI layers

Layer	Attack
Application	Phishing - Worms - Trojans
Presentation	Phishing - Worms - Trojans
Session	Session hijack
Transport	SYN flood - fraggle
Network	smurfing flooding - ICMP spoofing - DOS
Data link	Collision - DOS /DDOS - Eavesdropping
Physical	Signal Jamming - Wiretapping

Hardware Devices

HUB	Layer 1 device forward frames via all ports
Modem	digital to analog conversion
Routers	Interconnect networks
Bridge	Interconnect networks in Ethernet
Gateways	Inbound/outbound data entry points for networks
Switch	Frame forward in local network.
Load balancers	Share network traffic load by distributing traffic between two devices
Proxies	Hide internal public IP address from external public internet /Connection caching and filtering.
VPNs and VPN concentrators	Use to create VPN or aggregate VPN connections provide using different internet links
Protocol analyzers	Capture or monitor network traffic in real-time ad offline
Unified threat management	New generation vulnerability scanning application
VLANs	Create collision domains. Routers separate broadcast domains
IDS/IPS	Intrusion detection and prevention.

Firewall and Perimeter Security

DMZ (Demilitarized zone)	Secure network between external internet facing and internal networks.

Bastion Host - Dual-Homed - Three-Legged - Screened Subnet - Proxy Server - PBX - Honey Pot - IDS/IPS

Network Attacks

Virus	Malicious software, code and executables
Worms	Self propagating viruses
Logic Bomb	Time or condition locked virus
Trojan	Code and/or executables that act as legitimate software, but are not legitimate and are malicious
Backdoor	Unauthorized code execution entry
Salami, salami slicing	A series of small attacks and network intrusions that culminate in a cumulative large scale attack
Data diddling	Alteration of raw data before processing
Sniffing	Unauthorized monitoring of transmitted data
Session Hijacking	Monitor and capture of authentication sessions with the purpose of finding and hijacking credentials
DDoS (Distributed Denial of Service)	Overloading a server with requests for data packets well beyond its processing capacity resulting in failure of service
SYN Flood	Combination of a DDoS attack and TCP 3-way handshake exploit that results in denial of service
Smurf	Particular kind of DDoS attack using large numbers of Internet Control Message Protocol (ICMP) packets
Fraggle	Smurf with UDP instead of TCP
LOKI	Uses the common ICMP tunnelling program to establish a covert channel on the network
Teardrop	A type of DDoS attack that exploits a bug in TCP/IP fragmentation reassembly by sending fragmented packets to exhaust channels
Zero-day	Exploitation of a dormant or previously unknown software bug
Land Attack	Caused by sending a packet that has the same source and destination IP
Bluejacking, Bluesnarfing	Anonymously sending malicious messages or injecting code via bluetooth to unprotected devices within range
DNS Spoofing, DNS Poisoning	The introduction of corrupt DNS data into a DNS servers cache, causing it to serve corrupt IP results
Session hijacking (Spoofing)	Change TCP structure of the packet to show the source as trusted to gain access to targeted systems.
A TCP sequence prediction / number attack	A successful attempt to predict a TCP number sequence resulting in an ability to compromise certain types of TCP communications

Email Security

LDAP (Lightweight Directory Access Protocol)	Active directory based certificate management for email authentication.
SASL (Simple Authentication and Security Layer)	Secure LDAP authentication.
Client SSL Certificates	Client side certificate to authenticate against a server.
S/MIME Certificates	Used for signed and encrypted emails in single sign on (SSO)
MOSS (MIME Object Security Services)	Uses the multipart/signed and multipart/encrypted framework to apply digital signatures.
PEM (Privacy-Enhanced Mail)	A sequence of RfCs (Request for Comments) for securing message authenticity.
DKIM (Domainkeys Identified Mail)	Technique for checking authenticity of original message.
OAuth	An open protocol to allow secure authorization using tokens instead of passwords.

IP Addresses

Public IPv4 address space	• Class A: 0.0.0.0 – 127.255.255.255 • Class B: 128.0.0.0 – 191.255.255.255 • Class C: 192.0.0.0 – 223.255.255.255
Private IPv4 address space	• Class A: 10.0.0.0 – 10.255.255.255 • Class B: 172.16.0.0 – 172.31.255.255 • Class C: 192.168.0.0 – 192.168.255.255
Subnet Masks	• Class A: 255.0.0.0 • Class B: 255.255.0.0 • Class C: 255.255.255.0
IPv4	32 bit octets
IPv6	128 bit hexadecimal

Network Types

Local Area Network (LAN)	Geographic Distance and are is limited to one building. Usually connect using copper wire or fiber optics
Campus Area Network (CAN)	Multiple buildings connected over fiber or wireless
Metropolitan Area Network (MAN)	Metropolitan network span within cities
Wide Area network (WAN)	Interconnect LANs over large geographic area such as between countries or regions.
Intranet	A private internal network
Extranet	connects external authorized persons access to intranet
Internet	Public network

Networking Methods & Standards

Software defined networking (SDN)	Decoupling the network control and the forwarding functions. Features -Agility, Central management, Programmatic configuration, Vendor neutrality.
Converged protocols for media transfer	Transfer voice, data, video, images, over single network.
Fibre Channel over Ethernet (FCoE)	Running fiber over Ethernet network.
Multiprotocol Label Switching (MPLS)	Transfer data based on the short path labels instead of the network IP addresses. No need of route table lookups.
Internet Small Computer Interface (ISCI)	Standard for connecting data storage sites such as storage area networks or storage arrays. Location independent.
Multilayer Protocols	Encryption and different protocols at different levels. Disadvantages are hiding coveted channels and weak encryptions.
Voice over Internet Protocol (VoIP)	Allows voice signals to be transferred over the public Internet connection.
Asynchronous transfer mode (ATM)	Packet switching technology with higher bandwidth. Uses 53-byte fixed size cells. On demand bandwidth allocation. Use fiber optics. Popular among ISPs
X25	PTP connection between Data terminal equipment (DTE) and data circuit-terminating equipment (DCE)
Frame Relay	Use with ISDN interfaces. Faster and use multiple PVCs, provides CIR. Higher performance. Need to have DTE/DCE at each connection point. Perform error correction.
Synchronous Data Link Control (SDLC)	IBM proprietary protocol use with permanent dedicated leased lines.
High-level Data Link Control (HDLC)	Use DTE/DCE communications. Extended protocol for SDLC.
Domain name system (DNS)	Map domain names /host names to IP Address and vice versa.

Leased Lines

T1	1.544Mbps via telephone line
T3	45Mbps via telephone line
ATM	155Mbps
ISDN	64 or 128 Kbps REPLACED BY xDSL
Reserved	1024-49151
BRI B-channel	64 Kbps
BRI D-channel	16 Kbps
PRI B & D channels	64 Kbps

Port Ranges

Point to Point Tunneling Protocol (PPTP)	Authentication methods: • PAP=Clear text, unencrypted • CHAP=unencrypted, encrypted • MS-CHAP=encrypted, encrypted
Challenge-Handshake Authentication Protocol (CHAP)	Encrypt username/password and re-authenticate periodically. Use in PPP.
Layer 2 Tunneling Protocol (L2TP)	Use with IPsec for encryption.
Authentication Header (AH)	Provide authentication and integrity, no confidentiality.
Encapsulating Security Payload (ESP)	Encrypted IP packets and preserve integrity.
Security Associations (SA)	Shared security attributes between two network entities.
Transport Mode	Payload is protected.
Tunnel Mode	IP payload and IP header are protected.
Internet Key Exchange (IKE)	Exchange the encryption keys in AH or ESP.
Remote Authentication Dial-In User Service (RADIUS)	Password is encrypted but user authentication with cleartext.
SNMP v3	Encrypts the passwords.
Dynamic Ports	49152 - 65535

Remote Access Services

Telnet	Username /Password authentication. No encryption.
Remote login (rlogin)	No password protection.
SSH (Secure Shell)	Secure telnet
Terminal Access Controller Access-Control System (TACACS)	User credentials are stored in a server known as a TACACS server. User authentication requests are handled by this server.
TACACS+	More advanced version of TACACS. Use two factor authentication.
Remote Authentication Dial-In User Service (RADIUS)	Client/server protocol use to enable AAA services for remote access servers.
Virtual private network (VPN)	Secure and encrypted communication channel between two networks or between a user and a network. Use NAT for IP address conversion. Secured with strong encryptions such as L2TP or IPSEC.

VPN encryption options

Point-to-Point Tunneling Protocol (PPTP)	• PPP for authentication • No support for EAP • Dial in • Connection setup uses plaintext • Data link layer • Single connection per session
Layer 2 Tunneling Protocol (L2TP)	• Same as PPTP except more secure • Commonly uses IPsec to secure L2TP packets
Internet Protocol Security (IPsec)	• Network layer • Multiple connection per session • Encryption and authentication • Confidentiality and integrity

Communication Hardware Devices

Concentrator	Divides connected devices into one input signal for transmission over one output via network.
Multiplexer	Combines multiple signals into one signal for transmission.
Hubs	Retransmit signal received from one port to all ports.
Repeater	Amplifies signal strength.

WAN Transmission Types

Circuit-switched networks	• Dedicated permanent circuits or communication paths required. • Stable speed. Delay sensitive. • Mostly used by ISPs for telephony.
Packet-switched networks	• Fixed size packets are sending between nodes and share bandwidth. • Delay sensitive. • Use virtual circuits therefore less expensive.

Wireless Networking

Wireless personal area network (WPAN) standards

IEEE 802.15	Bluetooth
IEEE 802.3	Ethernet
IEEE 802.11	Wi-Fi
IEEE 802.20	LTE

Wi-Fi

Standard	Speed	Frequency (GHz)
802.11a	54 Mbps	2.4
802.11b	11 Mbps	5
802.11g	54 Mbps	2.4
802.11n	200+ Mbps	2.4/5
802.11ac	1Gbps	5

• 802.11 use CSMA/CA protocol as DSSS or FHSS
• 802.11b uses only DSSS

Wireless Security Protocols

Ad-hoc Mode	Directly connects peer-to-peer mode clients without a central access point.
Infrastructure Mode	Clients connect centrally via access point.
WEP (Wired Equivalent Privacy)	Confidentiality, uses RC4 for encryption.
WPA (Wi-Fi Protected Access)	Uses Temporal Key Integrity Protocol (TKIP) for data encryption.
WPA2	Uses AES, key management.
WPA2-Enterprise Mode	Uses RADIUS
TKIP (Temporal Key Integrity Protocol)	Uses RC4 stream cipher.
EAP (Extensible Authentication Protocol)	Utilizes PPP and wireless authentication. Compatible with other encryption technologies.
PEAP (Protected Extensible Authentication Protocol)	Encapsulates EAP within an encrypted and authenticated TLS tunnel.
Port Based Authentication	802.1x, use with EAP in switching environment

Wireless Spread Spectrum

FHSS (Frequency Hopping Spectrum System)	Uses all available frequencies, but only a single frequency can be used at a time.
DSSS (Direct Sequence Spread Spectrum)	Parallel use of all the available frequencies leads to higher throughput of rate compared to FHSS.
OFDM (Orthogonal Frequency-Division Multiplexing)	Orthogonal Frequency-Division Multiplexing

Firewall Generation Evolution

First Generation Firewalls	• **Packet Filter Firewalls:** Examines source/destination address, protocol and ports of the incoming packets. And deny or permit according to ACL. Network layer, stateless.
Second Generation Firewalls	• **Application Level Firewall / Proxy Server:** Masks the source during packet transfer. Operating at Application layer, stateful.
Third Generation Firewalls	• **Stateful Inspection Firewall:** Faster. State and context of the packets are inspected.
Fourth Generation Firewalls	• **Dynamic Packet Filtering Firewall:** Dynamic ACL modification • **Packet Filtering Routers:** Located in DMZ or boundary networks. Includes packet-filter router and a bastion host. Packet filtering and proxy • **Dual-homed Host Firewall:** Used in networks facing both internal and external • **Screened-subnet Firewall:** Creates a Demilitarized Zone (DMZ) - network between trusted and untrusted
Fifth Generation Firewalls	• **Kernel Proxy Firewall:** Analyzes packets remotely using virtual network
Next-generation Firewalls (NGFW)	• **Deep packet inspection (DPI) with IPS:** Integrated with IPS/IDS

Three-factor Authentication (3FA)

Knowledge factor	Something that is known by the user
Ownership factor	Something that the user possesses, like a key or a token.
Characteristic factor	A user characteristic, such as biometrics; fingerprints, face scan, signature.

Knowledge –Type/category 1 – something you know

Password authentication, Secret questions such as mother's maiden name, favorite food, date of birth, key combination / PIN.

Terminology and concepts

Salted hash	Random data added to a password before hashing and storing in a database on a server. Used instead of plaintext storage that can be verified without revealing password.
ComplEg. password	Alphanumeric, more than 10 characters. Includes a combination of upper and lower case letters, numbers and symbols.
One-time password (OTP)	Dynamically generated to be used for one session or transaction.
Static password	Password does not change. To be avoided.
Cognitive password	Something used to identify a person, i.e. pets name, favorite color, mother's maiden name etc, place of birth etc.
Password Hacking	Unauthorized access of a password file
Brute force attack	Multiple attempts using all possible password or pin combinations to guess the password.
Dictionary attack	Type of brute force attack that uses all the words from the dictionary.
Social engineering attack	Gain access by impersonating a user by establishing legitimate user credentials through social manipulation of trusted parties or authorities.
Rainbow Tables	Precomputed table for reversing cryptographic hash functions and cracking passwords.

Ownership –Type/category 2 – Something you have

Synchronous token	Create password at regular time intervals.
Asynchronous token	Generate a password based on the challenge-response technique.
Memory card	A swipe card containing user information.
Smart Cards or Integrated Circuit Card (ICC)	A card or dongle that includes a chip and memory, like bank cards or credit cards.
Contact Cards	Swiped against a hardware device.
Contactless Cards or Proximity Cards	Simply need to be within proximity to the reader device.
Hybrid Cards	Allows a card to be used in both contact and contactless systems.
USB drive	Bespoke USB with access credentials
Static password token	Simplest type of security token where the password is stored within the token.
Challenge/response token	A challenge has to be met by the correct user response.

Characteristic –Type/category 3 – Something you do / are

Biometric technology allows the user to be authenticated based on physiological behavior or characteristics.
• Physiological i.e. Iris, retina, and fingerprints.
• Behavioral i.e. Voice pattern

Physiological Characteristics

Fingerprint	Scans the thumb or edge of the finger.
Hand Geometry	Size, shape, bone length, finger length, or other layout attributes of a user's hand are taken.
Hand Topography	Hand peaks and valleys pattern.
Palm or Hand Scan	Fingerprint and geometry combination of palm.
Facial Scan	Facial features such as bone, eye length, nose, chin shape etc.
Retina Scan	Retina blood vessel scan.
Retina blood vessel scan	Scans the colored part of the eye around the pupil.
Vascular Scans	Scans the pattern of the veins in the users hand or face.
Voice print	Verify speech sound patterns.

Scanning Behaviors

Signature Dynamics	Pen pressure and acceleration is measured.
Keystroke Dynamics	Scan the typing pattern.
Voice Pattern / Print	Measures the sound pattern of a user read particular word.
Biometric Considerations	Does not change throughout human life and unique. High accuracy rate.
Enrollment Time	Sample processing for use by the biometric system.
Feature Extraction	The process of obtaining the information from a collected sample.
Accuracy	Scan the most important elements for correctness.
Throughput Rate	The rate which the system can scan and analyze.
False Rejection Rate (FRR)	The percentage of valid users that will be falsely rejected. Type 1 error.
False Acceptance Rate (FAR)	The percentage invalid users that will be falsely accepted. Type 2 error.
Crossover Error Rate (CER)	The point at which FRR equals FAR. This is expressed as a percentage - lower CER is better.
Biometric scans	Order of effectiveness and accuracy: Iris Scan • Retina Scan • Fingerprint • Hand Geometry • Voice Pattern • Keystroke Pattern • Signature Dynamics.

Terminology

Access	Action required to allow information flow between objects.
Control	Security measures taken to restrict or allow access to systems.
Subject	An entity which requires access to an object or objects.
Object	Entity which consists information.

Levels of Access & Control

Centralized administration	Only one component can control access. Highly restricted level where control done centrally.
Decentralized administration	Access is controlled by information owners, Can be less consistent.
Hybrid	Combination of centralized and decentralized.

Access stances	**allow-by-default** or **deny-by-default**

Single Sign-On (SSO)	• A.K.A federated ID management • Pros – ComplEg. passwords, easy administration, faster authentication. • Cons – Risk of all systems comprised by unauthorized access of a key or keys.

Authorization

Access control policies: Level of access and controls granted for a user.

Separation of duties	Assigning different users different levels of access to protect privacy and security.
Dual Controls	Access to perform specific functions is granted to two or more users.
Split Knowledge	No single user can have full information to perform a task.
Principle of Least Privilege	User is given minimum access level needed to perform a task.
Need-to-Know	Minimum knowledge level to perform a task.
No Access	User is not assigned any access for any object.
Directory Service	Centrally managed database for user objects management. i.e. LDAP
Kerberos	Client /server model authentication protocol. • Symmetric Key Cryptography • Key Distribution Center (KDC) • Confidentiality and integrity and authentication, symmetric key cryptography
Realm	Authentication administrative domain. Uses symmetric-key cryptography
KDC (Key Distribution Center)	Issues tickets to client for server authentication • Stores secret keys of all clients and servers in the network • AS (Authentication Server) • TGS (Ticket Granting Server)
The Kerberos logon process	• User input username/password in client PC/Device. • Client system encrypts credentials using AES to submit for KDC. • KDC match input credentials against database. • KDC create a symmetric key and time-stamped TGT to be used by the client and the Kerberos server. • Key and TGT are encrypted using client password hash. • Client installs the TGT and decrypts the symmetric key using a hash.

Authorization Methods

Discretionary Access Control (DAC) • Mandatory Access Control (MAC) • Role-based Access Control (role-BAC) • Rule-based Access Control (Rule-BAC).

Discretionary Access Control (DAC)	Uses access control lists (ACLs - Access-control lists).
Mandatory Access Control (MAC)	Subject authorize according to security labels. Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects.
Role-BAC (RBAC)	Task-based access controls - subjects require access an object based on its role or assigned tasks.
Rule-BAC	Uses a set of rules or filters to define what can or cannot be done on a system.
Hybrid RBAC	Limited RBAC
Lattice based / Label	Objects are classified based on control level using a label.
Non-discretionary access / Mandatory-Access control	Based on policies defined by a central authority. Role based or task based.

Authorization Methods / Concepts

Constrained Interface Applications	Restrict actions which can be performed with given privileges.
Content-Dependent	Restrict access to data depends on the content of an object.
Context-Dependent	Granting users access after a specific condition. Eg. after specific date/time.
Work Hours	Context-dependent control
Least Privilege	Subjects are given access to object only to perform what they need to have. • No more or no less!
Separation of Duties and Responsibilities	Tasks split to be performed by two or more people.
User Accountability	Auditing and Reporting • Vulnerability Assessment • Penetration Testing • Threat Modeling
Auditing and Reporting	Users are responsible for what actions they have performed. Events to be monitored for reporting: Network Events • Application Events • System Events • User Events • Keystroke Activity

Access Control Types

Type	Scope / Purpose	Example
Administrative Controls	Administration of organization assets and personal.	Data classification, data labeling, security awareness training.
Logical / Technical Controls	Restrict access.	Firewalls, IDS's/ IPS's, encryption, biometrics, smart cards, and passwords.
Physical Controls	Protect organization's infrastructure and personnel.	Perimeter security, biometrics and cabling.

Procedure for user account management

Regular user account review and password changes, track access authorization using a procedure, regularly verify the accounts for active status.

Access Control Requirements

CIA Triad: **C**onfidentiality - **I**ntegrity - **A**vailability (See Domain 1 cheat sheet!!!!!)

Identity Management

IAAA – **I**dentification - **A**uthentication - **A**uthorization - **A**ccountability.

Identification	• Registration verification of user identity and add an identifier to system. • Assign user the proper controls • Commonly use user ID or username.
Authentication	• User verification process • Commonly used passwords
Authorization	• Defining resources for user access
Accountability	• Person responsible for the controls, uses logs.

SESAME (Secure European System for Applications in a Multi-vendor Environment)

Public Key cryptology only authenticates initial segment without authenticating full message. Two separate tickets are in use one for authentication and other one defines the access privileges for user. Both symmetric and asymmetric encryptions are used.

SAML - (SOAP/XML)	Exchange authentication and authorization information between security domains and systems. • Components: Principal User • Identity provider • Service provider. • Use in directory federation SSO.

Authorization Concepts

Security domain	Set of resources having the same security policies.
Federated Identity	Organization having a common set of policies and standards within the federation.

Federation Models

Cross-Certification Model	Every organization is certified and trusted by the other organizations within the standards defined internally by said organizations.
Trusted Third-Party / Bridge Model	Every organization adheres to the standards set by a third party.
IDaaS (Identity as a Service)	Identity and access management is provided by a third party organization.
SSO (Single sign-on)	Access management for multiple similar, yet independant systems. Primarily used for the cloud and SaaS based system access.
Cloud Identity	User account management (Office 365)
Directory Synchronization	On-premises identity provider (Microsoft Active directory)
Federated Identity	On-premises identity provider for managing login request. (MS AD)

Access Control Models

Implicit Deny	By default access to an object is denied unless explicitly granted.
Access Control Matrix	Table which included subjects, objects, and access controls / privileges.
Capability Tables	List access controls and privileges assigned to a subject. • ACLs focus on objects whereas capability lists focus on subjects.
Permissions	Access granted for an object.
Rights	Ability/access to perform an action on an object.
Privileges	Combination of rights and permissions.

Access Control Categories

Category	Scope / Purpose	Example
Compensative	Risk mitigation action.	Two keys or key and combination to open a safety locker.
Corrective	Reduce attack impact.	Having fire extinguishers, having offsite data backups.
Detective	Detect an attack before happens.	CCTV, intrusion detection systems (IDS).
Deterrent	Discourages an attacker.	User identification and authentication, fences
Directive	Define and document acceptable practices within an organization.	Acceptable Use Policy (AUP)
Preventative	Stop an attack.	Locks, biometric systems, encryption, IPS, passwords.
Recovery	Recovery of a system after an attack.	Disaster recovery plans, data backups etc.

Vulnerability Assessment

Personnel Testing • Physical Testing • System and Network Testing

Penetration Testing and Threat Modeling

Simulate an attack to determine the probability of the attack to the application systems

Steps	1. Record information about the system
	2. Collect information about attack against the system
	3. Discover known system vulnerabilities
	4. Perform attacks against the system attempting to gain access
	5. Document the outcome of the penetration test

Penetration Test Types

Blind Test	Organization knows about possible attack but very limited knowledge.
Double-Blind Test	Organization doesn't know about incoming attack except for very few people in the organization who do not exchange information.
Target Test	Organization has prior knowledge of the attack, including key details

Penetration Strategies

Zero-Knowledge Test	Test team doesn't know any information about the target network A.K.A. black box testing.
Partial Knowledge Test	The testing team knows public knowledge about the organization's network.
Full Knowledge Test	The testing team knows all available information regarding the organization's network.

Password types

Simple Passwords	Single word usually a mixture of upper and lowercase letters.
Combination / Composition Passwords	Combination of two unmatching dictionary words.
Passphrase Passwords	Requires that a long phrase be used.
One-Time or Dynamic Passwords	Passwords that are valid for a single session login.
Graphical Passwords (CAPCHA)	Uses of character images or graphics as a part of the authentication.
Numeric Passwords	A password that only uses numbers.

Software Testing

Static Testing	Software security analysis using automated tools. Do not analyze either the source code or the compiled application. Eg. Buffer overflow
Dynamic Testing	Analyze and test using running environment. Use to test software provided by third parties where no access to software code. Eg. cross-site scripting, SQL injection
Fuzz Testing	Type of dynamic testing which use specific inputs to detect flaws under stress/load. Eg. input invalid parameters to test
Mutation / Dumb Fuzzing	Using already modified input values to test.
Generational / Intelligent Fuzzing	Inputs models of expected inputs.
Misuse Case Testing	Evaluate the vulnerability of known risks and attacks.
Interface Testing	Evaluate performance of software modules against the interface specifications to validate working status.
Application Programming Interfaces (APIs)	Test APIs to verify web application meets all security requirements.
User Interfaces (UIs)	Includes graphic user interfaces (GUIs) and command-line interfaces (CLI). Review of user interfaces against requirement specifications.
Physical Interfaces	Eg. in physical machines such as ATM, card readers etc.
Unit Testing	Testing a small part of the system to test units are good for integration into final product.
Integration Level Testing	Transfer of data and control between program interfaces.
System Level Testing	Verify system has all the required specifications and functions.

Log Management System

OPSEC process	Analyze daily operations and review possible attacks to apply countermeasures.
Pen-test	Testing of network security in view of a hacker.
Port scanner	Check any port or port range open in a computer.
Ring zero	Internal code of the system.
Operational assurance	Verify software meets security requirements.
Supervisor mode	Processes running in internal protected ring.

Threat Assessment Modeling

STRIDE	Evaluate threats against applications or operating systems.
Spoofing	Use of false identity to gain access to system identity. Can use IP/ MAC address, usernames, wireless network SSIDs.
Tampering	Cause unauthorized modifications of data in transit or in storage. Results in violation of integrity as well as availability.
Repudiation	Deny an action or activity carried out by an attacker.
Information disclosure	Distribution of private/confidential or restricted information to unauthorized parties.
Elevation of privilege	Attack result in increase the level privileges for a limited user account.
Regular monitoring of key performance and risk indicators including	Number of open vulnerabilities and compromised accounts, vulnerability resolve time, number of detected software flaws etc.
Vulnerability scans	Automatically probe systems, applications, and networks.
TCP SYN Scanning	Sends a packet with SYN flag set. Also known as “half-open” scanning.
TCP Connect Scanning	Perform when a user running the scan does not have the necessary permissions to run a half-open scan.
TCP ACK Scanning	Sends a packet with the ACK flag set.
Xmas Scanning	Sends a packet with the FIN, PSH, and URG flags set.
Passive Scanning	Detect rogue scanning devices in wireless networks.
Authenticated scans	Read-only account to access configuration files.

Software Development Security Best Practices

WASC	Web Application Security Consortium
OWASP	Open Web Application Security Project
BSI	the Build Security In initiative
IEC	The International Electrotechnical Commission

Security Testing

To make sure security controls are properly applied and in use. Automated scans, vulnerability assessments and manual testing.

Software Threats

Viruses	Stealth virus • Polymorphic virus • Macro virus • • Spyware/Adware • Botnet • worm
Rootkit	Kernel-mode Rootkit • Bootkit • User-mode Rootkit • Virtual Rootkit • Firmware Rootkit
Source Code Issues	Buffer Overflow • Escalation of Privileges • Backdoor
Malware Protection	Antivirus software • Antimalware software • Security Policies

Considerations

• Resources availability
• Level of critical and sensitiveness of the system under testing
• Technical failures
• Control misconfigurations result in security loopholes
• Security attack risks
• Risk of performance changes
• Impact on normal operations

Verification & Validation

• Verification – SDLC design output meets requirements
• Validation – Test to ensure software meets requirements

Security Software

• Antimalware and Antivirus – Scan and log malware and virus detection
• IDS/IPS = Real time and promiscuous monitoring for attacks
• Network-based IDS
• Local network monitoring and passive and header level scanning .No host level scan.
• HOST BASED
• Monitor hosts using event logs
• Intrusion prevention system (IPS) – Attack detects and prevent
• Remote Access Software Should be access via a VPN
• Vulnerability assessment Software – should be updated and patched
• Routers – policy based access control

Logs

Network Flow	Network traffic capture
Audit logging	Events related to hardware device login and access
Network Time Protocol (NTP)	Should synchronize across entire network to have correct and consistent time in logs and device traffic flows.
Syslog	Device event message log standard.
Event types	Errors, Warnings, Information, Success Audits, Failure
Simple Network Management Protocol (SNMP)	Support for different devices such as Cisco.

Monitoring and auditing

Define a clipping level. A.K.A BASELINE
• Audit trails – event/transaction date/time, author /owner of the event
• Availability – Log archival
• Log Analysis – examine logs

Code Review and Testing

Person other than the code writer/developer check the code to find errors

Fagan inspections – steps	Planning • Overview • Preparation • Inspection • Rework • Follow-up
Code Coverage Report	Details of the tested code structure
Use cases	Percentage of the tested code against total cases
Code Review Report	Report create in manual code testing
Black-box testing	Test externally without testing internal structure
Dynamic Testing	Test code in run time
White-box testing	Detailed testing by accessing code and internal structure
CVE	Common Vulnerability and Exposures dictionary
CVSS	Common Vulnerability Scoring System
NVD	National Vulnerability Database
Regression Testing	Verify the installations required for testing do not have any issues with running system
Integration Testing	Test using two or more components together

Incident Scene

Assign ID to the scene • Incident environment protection • ID and possible sources of evidence • Collect evidence • Avoid or minimize evidence contamination

Locard's Exchange Principle	In a crime the suspected person leaves something and takes something. The leftovers can be used to identify the suspect.

Live Evidence

Primary Evidence	• Most reliable and used by trial • Original documents–Eg. Legal contracts • No copies or duplicates
Secondary Evidence	• Less powerful and reliable than primary evidence. • Eg. Copies of originals, witness oral evidence. • If primary evidence is available secondary of the same content is not valid.
Direct Evidence	Can prove without a backup support. • Eg. witness testimony by his/her own 5 senses.
Conclusive Evidence	• Cannot contradict, conditional evidence, no other supportive evidence requires • Cannot be used to directly prove a fact
Corroborative Evidence	• Use as substantiate for other evidence
Hearsay Evidence	• Something heard by the witness where another person told

Asset Management

Preserve Availability • Authorization and Integrity • Redundancy and Fault Tolerance • Backup and Recovery Systems • Identity and Access Management

Storage Management Issues	• Hierarchical Storage Management (HSM): continuous online backup system Using optical storage. • Media History: Media usage log • Media Labeling and Storage: safe store of media after labeling sequentially • Environment: Temperature and heat Eg. Magnetic media
Sanitizing and Disposing of Data	• Data Purging: degaussing Archived data not usable for forensics • Data Clearing: Cannot recover using keyboard • Remanence: Data left in media deleted
Network and Resource Management	• Redundant hardware • Fault-tolerant technologies • Service Level Agreements (SLA's) • MTBF and MTTR • Single Point of Failure (SPOF)
Incident Response - steps	1. Detect • 2. Respond • 3. Report • 4. Recover • 5. Remediate • 6. Review
Change Management	• Changes should be formally requested • Analyze requests against goals to ensure validity • Cost and effort estimation before approval • Identify the change steps after approval • Incremental testing during implementation • Complete documentation
Threats and Preventative Measures	• Clipping levels: Define a baseline for normal user errors, • Modification from Standards Eg. DDOS • Unusual patterns or events • Unscheduled reboots: Eg. Hardware or operating system issue • Input/output Controls

Intrusion Detection & Prevention Systems (IDS & IPS)

IDS (Intrusion Detection System)	Automated inspection of logs and real-time system events to detect intrusion attempts and system failures. IDSs are an effective method of detecting many DoS and DDoS attacks.
IPS (Intrusion Prevention System)	A IDS with additional caabilities to stop intrusions.

Firewalls

HIDS (Host-based IDS)	Monitor and analyze the internals of a computing system, including its network connection points. Eg. Mainframe computer
NIDS (Network-based IDS)	Hardware based device or software applications used to monitor and analyse network activity, specifically scanning for malicious activities and policy violations.

Hierarchical Recovery Types

1. Manual
2. Automatic Recovery

Types of System Failure

• System reboot
• Emergency restart
• System cold start

Data Destruction and Reuse

Object reuse	Use after initial use
Data remanence	Remaining data after erasure Format magnetic media 7 times (orange book
Clearing	Overwriting media to be reused
Purging	Degaussing or overwriting to be removed
Destruction	Complete destruction, preferably by burning

Disaster Recovery Planning

Disaster recovery process	Teams responsible for DR implementation - Salvage team - Work on normal /primary site to make suitable for normal operations
Other recovery issues	• Interfacing with other groups • Fraud and Crime: Eg. vandalism, looting • Financial disbursement • Documenting the Plan - Required documentation • Activation and recovery procedures • Plan management • HR involvement • Costs • Internal /external communications • Detailed plans by team members

Characteristics of Evidence

Sufficient	Validity can be acceptable.
Reliable	Consistent facts. Evidence not tampered or modified.
Relevant	Reasonable facts, with proof of crimes, acts and methods used, event documentation
Permissible	Evidence obtained lawfully

Interviewing and Interrogation

Interviewing	Collect facts to determine matters of the incident.
Interrogation	Obtain a confession by evidence retrieval method. • The Process: Prepare questions and topics, summarize information
Opinion Rule	Witnesses test only the facts of the case, not used as evidence.
Expert Witnesses	Can be used as evidence.

Network Analysis

Use of existing controls to inspect a security breach incident. Eg. IDS/IPS, firewall logs
• **Software Analysis:** Forensic investigation of applications which was running while the incident happened.
• **Hardware/ Embedded Device Analysis:** Eg. review of Personal computers & Smartphones

Governing Laws

• Common law - USA, UK Australia, Canada
• Civil law - Europe, South America
• Islamic and other Religious laws – Middle East, Africa, Indonesia, USA

The 3 Branches of Law	• Legislative: Statutory law - Make the laws • Executive: Administrative law - Enforce the laws • Juridical: Interpret the laws
Categories of law	• Criminal law –violate government laws result in commonly imprisonment • Civil law – Wrong act against individual or organization which results in a damage or loss. Result in financial penalties. • Administrative/Regulatory law – how the industries, organizations and officers should act. Punishments can be imprisonment or financial penalties
Uniform Computer Information Transactions Act (UCITA)	Common framework for the conduct of computer-related business transactions. A federal law Eg. Use of software licensing
Computer Crime Laws 3 types of harm	• Unauthorized intrusion • Unauthorized alteration or destruction • Malicious code
Admissible evidence	• Relevant, sufficient, reliable, does not have to be tangible
Hearsay	• Second hand data not admissible in court
Enticement	• Is the legal action of luring an intruder, like in a honeypot
Entrapment	• Is the illegal act of inducing a crime, the individual had no intent of committing the crime at first

Data Loss Prevention (DLP)

Scans data for keywords and data patterns. Protects before an incident occurs.

Network-based DLP	Data in motion. Scans all outbound data looking for anomalies. Place in edge of the network to scan all outgoing data.
Endpoint-based DLP	Data in use. Scans all internal end-user workstations, servers and devices.

Digital Data States

Data at Rest	Data that is stored on a device or a backup medium.
Data in Motion	Data that is currently travelling across a network or on a device's RAM ready to be read, updated, or processed.
Data in Use	Data that is being inputted, processed, used or altered.

Backup Types

Full	All files backed up, archive bit and modify bit will be deleted
Incremental	Backup files changed after last full backup, archive bit deleted.
Differential	Only modified files are backed up, do not delete archive bit. Need last full backup and last incremental backup for a full restore.
Redundant servers	Eg. RAID, adding disks for increased fault tolerance.
Server clustering	Set of servers that process traffic simultaneously.

Disaster Recovery Test

Desk Check	Review contents of the plan
Table-top exercise	Disaster recovery team members gather and roleplay a disaster scenario
Simulation test	More intense than a roleplay, all support and tech staff meet and practice against disaster simulations
Parallel tests	Personnel are taken to an alternative site and commence operations of critical systems, while original site continues operating
Full-implementation tests	Personnel are taken to an alternative site and commence operations of all systems, main site is shut down

BCP Plan Development

Define the continuity strategy	• Computing: strategy to protect - hardware, software, communication links, applications, data • Facilities: use of primary or alternate/remote site buildings • People: operational and management • Supplies and equipment
Roles and responsibilities	• BCP committee: senior staff, business units, information systems, security administrator, officials from all departments
Physical security	• CCTV • Fences-Small mesh and high gauge • Alarms • Intrusion detection: electromechanical, photoelectric, passive infrared, acoustical detection • Motion: wave pattern motion detectors, proximity detector • Locks: warded lock, combination lock, cipher lock, device lock, preset / ordinary door lock, programmable locks, raking lock • Audit trails: date and time stamps, successful/unsuccessful attempts, who attempted, who granted/modified access controls • Security access cards: Photo ID card, swipe cards, smartcards • Wireless proximity cards: user activated or system sensing field powered device

Evidence Lifecycle

1. Discovery
2. Protection
3. Recording
4. Collection and identification
5. Analysis
6. Storage, preservation, transportation
7. Present in court
8. Return to owner

Digital Evidence

Six principles to guide digital evidence technicians

• All general forensic and procedural principles apply.

• Upon seizure, all actions should not change the data.

• All people accessing the data should be trained

• All actions performed on the data should be fully documented and accessible.

• Anyone that possesses evidence is responsible for all actions taken with it while in their possession.

• Any agency that possesses evidence is is responsible for compliance with these principles.

Media Analysis

Part of computer forensic analysis used for identification and extraction of information from storage media. Eg. Magnetic media, Optical media, Memory (e.g., RAM)

Admissible Evidence

Relevant to the incident. The evidence must be obtained legally.

Digital Forensics

Five rules of evidence:
Be authentic • Be accurate • Be complete • Be convincing • Admissible

Investigation - To Determine Suspects

Types:
Operational • Criminal • Civil • eDiscovery

Security Incident and Event Management (SIEM)

Log review automating
Real-time analysis of events occurring on systems

Transaction Redundancy Implementations

Electronic Vaulting • Remote Journaling • Database shadowing

System Hardening

" • Uninstall unnecessary applications
• Disable unnecessary services
• Deny unwanted ports
• External storage device restriction
• Monitoring and Reporting
• Vulnerability Management System
• IDP/IPS: Attack signature engine should be updated regularly

System Recovery

1. Rebooting system in single user mode, recovery console
2. Recovering all file systems active before crash
3. Restore missing / damaged files
4. Recover security and access controls

Configuration Management (CM)

An ITILv2 and an ITSM process that tracks all of the individual Configuration Items (CI)

Configuration Items (CI)	Version: state of the CI, Configuration - collection of component CI's that makes another CI
Building	Assembling a component with component CI's Build list
Artifacts	Recovery procedures. Eg. system restart. Should be accessed by authorized users from authorized terminals.

Incident Response

Lifecycle	Response Capability • Incident response and handling • Recovery • Feedback
Mitigation	Limit the impact of an incident.

Root Cause Analysis (RCA)

Fault tree analysis (FTA)	Top down deductive failure analysis using boolean logic.
Failure mode and effects analysis (FMEA)	Review of as many components, assemblies, and subsystems as possible to identify potential failure modes.
Pareto Analysis	Looks at the predominant likely causes to deal with them first.
Cause mapping	Connects individual cause-and-effect relationships to give insights into the system of causes within an issue.

Disaster Recovery Methods

Hot Site	A real-time mirror of your system and network activity running in sync. Allows for minimum disruption and downtime.
Cold Site	An alternative workspace with power and HVAC setup, but no hardware. All recovery efforts will be technician heavy.
Warm Site	A middle-ground solution which includes skeletal hardware, software and connectivity to restore critical functionality.
Service Bureau	Contract with a service bureau to provide backup services.
Multiple centers / sites	Process between multiple data centers
Rolling / mobile sites	Mobile homes or HVAC trucks.
Recovery Time Objectives (RTOs)	• Hot site RTO: 5 minutes or hours • Warm site RTO: 1-2 days • Mobile site RTO: 3-5 days • Cold site RTO: 1 to 2 weeks

RAID, SAN, & NAS

RAID	Redundant Array of Independent / Inexpensive Disks
Disk Mirroring	Writing the same data across multiple hard disks, slower as data is written twice, doubles up on storage requirements
Disk Striping	Writes data across multiple disks simultaneously, provides higher write speed.
RAID 0	• Writes files in stripes across multiple disks without using parity information • 2 or more disks required • Fast reading and writing but no redundancy
RAID 1	• Creates identical copies of drives - has redundancy • Space is effectively utilized, since half will be given to another disk • Expensive
RAID 3	Byte level data striping across multiple
RAID 4	Block level data striping across multiple
RAID 5	Data and parity Information is striped together across all drives
RAID 0+1	Stripes data across available drives and mirrors to a seperate set of disks
RAID 1+0 (RAID 10)	Each drive in a set is mirrored to an equivalent drive in another set
Storage Area Network (SAN)	Typically use Fibre Channel and iSCSI. High speed blick level storage.
Network-Attached Storage (NAS)	Typically an NFS server, file-level computer data storage server connected to a computer network.

Disaster Recovery Terminology & Concepts

MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
MTBF	Mean Time Between Failures, MTTF + MTTR
Transaction Redundancy Implementations	Electronic Vaulting • Remote Journaling • Database shadowing

Business Continuity Planning

Business Continuity Plan (BCP)	Concerns the preservation and recovery of business in the event of outages to normal business operations.
Business Impact Analysis (BIA)	The process of assessing the impact of an IT disruption. BIA is part of BCP
Disaster Recovery Plan (DRP)	A framework of steps and actions that need to be taken to achieve business continuity and disaster recovery goals. End Goal – Revert back to normal operations - planning and development must be done before the disaster - BIA should be complete
Business Continuity Steps	1. Scope and plan initiation 2. BIA - assess impact of disruptive processes 3. Business Continuity Plan development - Use BIA to develop BCP - Testing 4. Plan approval and implementation - management approval

Trusted Recovery

Breach Confirmation	Confirm security breach not happen during system failure.
Failure Preparation	Backup critical information to enable recovery
System Recovery	After a failure of operating system or application, the system should work enough to have the system in a secure state

Software Development Lifecycle (SDLC)

Understand and integrate security throughout the software development lifecycle (SDLC)

Development Methodologies

Build and fix	• No key architecture design • Problems fixed as they occur • No formal feedback cycle • Reactive not proactive
Waterfall	• Linear sequential lifecycle • Each phase is completed before moving on • No formal way to make changes during cycle • Project ends before collecting feedback and re-starting
V-shaped	• Based on the waterfall model • Each phase is complete before moving on • Verification and validation after each phase • No risk analysis phase
Prototyping	• Rapid prototyping - quick sample to test the current project • Evolutionary prototyping - incremental improvements to a design • Operational prototypes - incremental improvements intended for production
Incremental	• Multiple cycles (~ multiple waterfalls) • Restart at any time as a different phase • Easy to introduce new requirements • Delivers incremental updates to software
Spiral	• Iterative • Risk analysis during development • Future information and requirements considered for risk analysis • Allows for testing early in development
Rapid Application Development (RAD)	• Rapid prototyping • Designed for quick development • Analysis and design are quickly demonstrated • Testing and requirements are often revisited
Agile	• Umbrella term - multiple methods • Highlights efficiency and iterative development • User stories describe what a user does and why • Prototypes are filtered down to individual features

DevOps (Development & Operations)

Software Development • Quality Assurance • IT Operations

Software Development Methods

Database Systems

Database	Define storing and manipulating data
DBMS (database management system)	Software program control access to data stored in a database.
DBMS Types	Hierarchical • Network • Mesh • Object-orientated • Relational
DDL	Data definition language defines structure and schema DML
Degree of Db	number of attributes (columns) in table
Tuple	row
DDE	Dynamic data exchange
DCL	Data control language. Subset of SQL.
Semantic integrity	ensure semantic rules are enforced between data types
Referential integrity	all foreign keys reference existing primary keys
Candidate Key	an attribute that is a unique identifier within a given table, one of the candidates key becomes primary key and others are alternate keys
Primary Key	unique data identification
Foreign Key	reference to another table which include primary key. Foreign and primary keys link is known as referential integrity.
DBMS terms	• Incorrect Summaries • Dirty Reads • Lost Updates • Dynamic Lifetime Objects: Objects developed using software in an Object Oriented Programming environment. • ODBC - Open Database Connectivity. Database feature where applications to communicate with different types of databases without a program code. • Database contamination - Mixing data with different classification levels • Database partitioning - splitting a single database into multiple parts with unique contents • Polyinstantiation - two or more rows in the same relational database table appear to have identical primary key and different data in the table.

Programming Language Types

Machine Languages	Direct instructions to processor - binary representation
Assembly Language	Use of symbols, mnemonics to represent binary codes - ADD, PUSH and POP
High-Level Language	Processor independent programming languages - use IF, THEN and ELSE statements as part of the code logic
Very high-level language	Generation 4 languages further reduce amount of code required - programmers can focus on algorithms. Python, C++, C# and Java
Natural language	Generation 5 languages enable system to learn and change on its own - AI

Database Architecture and Models

Relational Model	Uses attributes (columns) and tuples (rows) to organize data
Hierarchical Model	Parent child structure. An object can have one child, multiple children or no children.
Network Model	Similar to hierarchical model but objects can have multiple parents.
Object-Oriented Model	Has the capability to handle a variety of data types and is more dynamic than a relational database.
Object-Relational Model	Combination of object oriented and relational models.

Database Interface Languages

Open Database Connectivity (DOBC)	Local or remote communication via API
Java Database Connectivity (JDBC)	Java API that connects to a database, issuing queries and commands, etc
XML	DB API allows XML applications to interact with more traditional databases
Object Linking and Embedding Database (OLE DB)	is a replacement for ODBC

Knowledge Management

Expert Systems	Two main components: 'Knowledge base' and the 'Inference engine' • Use human reasoning • Rule based knowledge base • If-then statements • Interference system
Expert Systems (Two Modes)	• Forward chaining: Begins with known facts and applies inference rule to extract more data unit it reaches to the goal. A bottom-up approach. Breadth-first search strategy. • Backward chaining: Begins with the goal, works backward through inference rules to deduce the required facts that support the goal. A top-down approach. Depth-first search strategy.
Neural Networks	Accumulates knowledge by observing events, measuring their inputs and outcome, then predicting outcomes and improving through multiple iterations over time.

Covert Channels (Storage & Timing)

Executable content Mobile code	ActiveX controls, Java applets, browser scripts
Virus	Propagates with help from the host
Worm	Propagates without any help from the host
Logic Bomb/Code Bomb	Run when a specific event happens
Buffer Overflow	Memory buffer exhaustion
Backdoor	Malicious code install at back end with the help of a front end user
Covert Channel	Unauthorized information gathering
Botnet	Zombie code used to compromise thousands of systems
Trojan	Malicious code that outwardly looks or behaves as harmless or necesary code

Data Warehousing and Data Mining

Data Warehousing	Combine data from multiple sources.
Data Mining	Arrange the data into a format easier to make business decisions based on the content.

Database Threats

Aggregation	The act of combining information from various sources.
Inference	Process of information piecing
Access Control	• Content Dependent Access Control: access is based on the sensitivity of the data • Context Dependent Access Control: access via location, time of day, and previous access history.
Access Control Mechanisms	• Database Views: set of data a user or group can see • Database Locks: prevent simultaneous access • Polyinstantiation: prevent data interference violations in databases

A • C • I • D

Atomicity	Database roll back if all operations are not completed, transactions must be completed or not completed at all
Consistency	Preserve integrity by maintaining consistent transactions
Isolation	Transaction keeps separate from other transactions until complete
Durability	Committed transaction cannot be roll backed

Traditional SDLC

Steps	Analysis, High-level design, Detail Design, Construction, testing, Implementation
Phases	• Initiation: Feasibility, cost analysis, risk analysis, Management approval, basic security controls • Functional analysis and planning: Requirement definition, review proposed security controls • System design specifications: detailed design specs, Examine security controls • Software development: Coding. Unit testing Prototyping, Verification, Validation • Acceptance testing and implementation: security testing, data validation

Object-oriented technology (OOT) - Terminology

Objects contain both data and the instructions that work on the data.

Encapsulation	Data stores as objects
Message	Informs an object to perform an action.
Method	Performs an action on an object in response to a message.
Behavior	Results shown by an object in response to a message. Defined by its methods, which are the functions and subroutines defined within the object class.
Class	Set of methods which defines the behavior of objects
Object	An instance of a class containing methods
Inheritance	Subclass accesses methods of a superclass
Multiple Inheritance	Inherits characteristics from more than one parent class
Polyinstantiation	Two or more rows in the same relational database table appear to have identical primary key elements but contain different data
Abstraction	Object users do not need to know the information about how the object works
Process isolation	Allocation of separate memory spaces for process's instructions and data by the operating system.

Trusted Computer Base (TCB)

The set of all hardware, firmware, and/or software components that are critical to its security. Any compromises here are critical to system security.

Input/output operations	May need to interact with higher rings of protection - such communications must be monitored
Execution domain switching	Applications that invoke applications or services in other domains
Memory protection	Monitoring of memory references to verify confidentiality and integrity in storage
Process activation	Monitor registers, process status information, and file access lists for vulnerabilities

Security Assessment & Testing Terms

Cross-site request forgery (CSRF / XSRF)	Browser site trust is exploited by trying to submit authenticated requests forcefully to third-party sites.	Penetration Testing	A process of identifying and determining the true nature if system vulnerabilities
Cross-site scripting (XSS)	Uses inputs to pretend a user's browser to execute untrusted code from a trusted site	Patch management system	Manages the deployment of patches to prevent known attack vectors
Session Hijacking	Attempts to obtain previously authenticated sessions without forcing browser requests submission	Open system	System with published APIs - third parties can use system
SQL Injection	Directly attacks a database through a web app	Closed system	Proprietary system - no third-party involvement
Hotfix / Update / Security fix	Updates to operating systems and applications	Open-source	Source code can be viewed, edited and distributed free or with attribution or fees
Service Pack	Collection of patches for a complete operating system	API Keys	Used to access API. Highly sensitive - same as passwords

Change Management Process

Request Control	Develop organizational framework where users can request modifications, conduct cost/ benefit analysis by management, and task prioritization by developers
Change Control	Develop organizational framework where developers can create and test a solution before implementation in a production environment.
Release Control	Change approval before release

Configuration Management Process

Software Version Control (SVC)	A methodology for storing and tracking changes to software
Configuration Identification	The labelling of software and hardware configurations with unique identifiers
Configuration Control	Verify modifications to software versions comply with the change control and configuration management policies.
Configuration Audit	Ensure that the production environment is consistent with the accounting records

Capability Maturity Model

Reactive	1. Initiating – informal processes, 2. Repeatable – project management processes
Proactive	3. Defined – engineering processes, project planning, quality assurance, configuration management practices 4. Managed – product and process improvement 5. Optimizing – continuous process improvement

Project Management Tools

Gantt chart	Type of bar chart that illustrates the relationship between projects and schedules over time.
Program Evaluation Review Technique (PERT)	Project-scheduling tool used to measure the capacity of a software product in development which uses to calculate risk.

Phases of object-oriented design

OORA (Requirements Analysis)	Define classes of objects and interactions
OOA (Analysis)	Identify classes and objects which are common to any applications in a domain - process of discovery
OOD (Design)	Objects are instances of classes
OOP (Programming)	Introduce objects and methods
ORBs (Object Request Brokers)	Work as middleware locators and distributors for the objects
CORBA (Common object request)	Architecture and standards that use ORBS to allow different systems and software on a system to interfce with eachother
Cohesion	Work independently without help from other programs • High cohesion – No integration or interaction with other modules • Low cohesion – Have interaction with other modules • Coupling - Level of interaction between objects

Virus Types

Boot sector	Boot record infectors, gain the most privaleged access and can be the most damaging
System infector	Infects executable system files, BIOS and system commands
UEFI	Infects a system's factory installed UEFI (firmware)
Companion	Virus stored in a specific location other than in the main system folder. Example NOTEPAD.EXE
Stealth	Any modifications to files or boot sector are hidden by the virus
Multipart	Infects both boot sector and executable files
Self-garbling	Attempts to hide from anti-virus by changing the encoding of its own code, a.k.a. 'garbling'
Polymorphic	The virus modifies the "garble" pattern as it spreads
Resident	Loads as and when a program loads to the memory
Master boot record / sector (MBR)	Infects the bootable section of the system

Anti-Virus Types

Signature based	Not able to detect new malware a.k.a. Zero-day attacks
Heuristic based	Static analysis without relying on signatures

Protection Rings

Layer 0	Operating system kernel
Layer 1	Parts of the operating system other than the kernel
Layer 2	I/O drivers and utilities
Layer 3	Applications and programs