SSCP / CISSP Notes I Used To Pass

I passed CISSP at 100 questions in 60 minutes in 06/2020.

These notes were initially compiled for myself and tailored to my knowledge. It does not contain **all** content.
I have expanded on the content since passing to include more topics.
It will likely help you after you've completed the initial round of studying of all domains.

These notes are a consolidation of knowledge gathered from Adam Gordon's notes and questions, ITProTV's test answers, Boson's explanations from his tests, the Sunflower notes, Wentz Wu's questions and many other sources.

Feel free to share the link to these notes if you find them useful.
Tell me about mistakes in or improvements to my notes!
Say hello to me (@Lance) at https://discord.gg/certstation

LinkedIn: https://www.linkedin.com/in/lance-li-sheng-ceo-at-searix-cissp-cism-pmp-escmc-286a6956/

Lance's How To: Tackle CISSP

1. As everyone has said, your role is a **risk management advisor**, ***NOT*** a **technician**.

2. We often hear "Mile Wide, Inch Deep" for CISSP, but I would like to add - **FOR BASIC TOPICS, DIG DEEP, BUT NOT TOO DEEP**.

   It's important to understand the "process" for **basic topics** - the "why" and "how". Apply the style of questioning below and you will be prepared. Using the example of a SIEM (which is NOT a basic topic in CISSP), you know what it is, but have you asked...

   - When do you need it?
   - Let's say you decide that you need it, how is that decision made? Qualitatively? Quantitatively? Why?
   - Who would be the one usually spotting that it's needed and recommending so? Who makes the decision? Why?
   - Who will be operating it? What kind of access controls are required? How are they defined? What are the steps involved? Why?
   - Who will be auditing it? Should it be internal or external? What's the benefits / disadvantages to each?
   - How does this fit into Continuous Monitoring efforts? Who will be creating the relevant policies for it? Why?
   - Who will be implementing them? What are the steps to doing so? Who approves / certifies / accredits that and when? Why?
   - What are the potential supply chain issues with it? Who evaluates them? How are they evaluated? Why?
   - When are the risks of implementation evaluated? Who evaluates them? How are they evaluated? Why?
   - Where does it get implemented in the architecture? What are the advantages / disadvantages?
   - What could be the security-related issues with it? How are they mitigated?
   - What are the privacy-related issues with it? Which clauses in the GDPR / other laws? How are they mitigated?

   But don't lose yourself going too deep. Stay focused on topic. Do **NOT** ask questions like...

   ~~- What are the configuration settings I should set in a SIEM?~~
   ~~- What is included in the Protection Profiles are SIEMs?~~
   ~~- How does a SIEM compare with a SEM or SIM (both not covered)? I need a comparison matrix...~~

3. Adam Gordon constantly suggests - Answer what the question asks, not what you THINK it's asking. Nothing else exists outside the context of the question.

4. Kelly Handerhan suggests - think of the end game. Which option demonstrates the **ultimate** purpose?

5. Larry Greenblatt suggests - let Captain Kirk and Spock decide. What answers can be eliminated? Which answer is more likely?

6. **IMPORTANT: Don't struggle with too many practice questions. FOCUS on the understanding of the topics and analysis process of the options.**

Key Regulations

4th Amendment	US Constitution. No unreasonable searches or seizures
Patriot Act	Provide appropriate tools required to intercept and obstruct terrorism
HIPAA	aka Kennedy-Kassebaum Act. Healthcare security and privacy.
PCI DSS	Payments. E2EE: Encrypts at point of swiping, may get decrypted on merchant device or at payment gateway because key is negotiated between merchant and gateway, not processor. P2PE: Uses verified hardware, software and processor. Does not allow key management by merchant.
Sarbanes-Oxley	aka SOX. Publicly-traded companies must report their financial status
GLBA of 1999	Gramm-Leach-Bliley Act. Financial institutions only. Provide customers with privacy notice annually.
FISMA of 2002	Federal Information Security Management Act. All federal agencies
OMB Circular A-130	Managing information as a strategic resource. Help reduce paperwork.
EU Privacy Law	Safe Harbour -> Privacy Shield Framework

Key Standards

Name	Type / Description	Key Concepts / Knowledge
NIST SP 800-14	Generally Accepted Principles and Practices for Securing IT Systems	
NIST SP 800-30	Risk Management Guide for Information Technology Systems	OCTAVE, PUSH
NIST SP 800-34	Contingency Planning Guide for IT Systems	
NIST SP 800-37	Risk Management Framework	
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations	
NIST SP 800-86	Guide to Integrating Forensic Techniques into Incident Response	
NIST SP 800-88	Guidelines for Media Sanitization	Purge, Sanitize, Destroy
NIST SP 800-137	Information Security Continuous Monitoring	
NIST SP 800-145	The NIST Definition of Cloud Computing	
ISO/IEC 27001	Information Security Management Systems (Governance)	From BS 7799
ISO/IEC 27002	Security Controls	Originally ISO/IEC 17799. From BS 7799
ISO/IEC 15408	Common Criteria	
FIPS 140		Security requirements for hardware and software cryptographic modules

COSO - Financial reporting and disclosure objectives

1	Control Environment
2	Risk Assessment
3	Control Activities
4	Information and Communication
5	Monitoring

COBIT - Assessment of high-level control objectives (GOVERNANCE)

1	Evaluate, Direct and Monitor (EDM)
2	Align, Plan and Organize (APO)
3	Build, Acquire and Implement (BAI)
4	Deliver, Service and Support (DSS)
5	Monitor, Evaluate and Assess (MEA)

SABSA - Security Architecture Framework

6 Perspectives: Analysis of Business Security Requirements
Includes chain of traceability through each phase

Contextual	Conceptual
Logical	Physical
Component	Operational

https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/enterprise-security-architecturea-top-down-approach

TOGAF - Developing an IT architecture to align with the goals of the business

Architecture Development Method (ADM):
Exclusively uses business requirements as central point of comparison for every phase of development

4 domains:
Business, Application, Data, Tech

ITIL - Controls for IT service management

1	Service Strategy
2	Service Design
3	Service Transition
4	Service Operation
5	Continual Service Improvement

EU Privacy Principles on Employee Data Monitoring

Finality	Employee monitoring for data usage
Necessity	Choose least intrusive method
Transparency	Complete disclosure
Legitimacy	Must be backed by legal requirement
Proportionality	Customized to risk level that is incurred
Data Accuracy	
Security	Take precautions to protect confidentiality
Awareness of Staff	

CPTED - Crime Prevention Through Environmental Design

Territorial Reinforcement	*Premise: Boundaries define users' familiarity with the surroundings. Easy to identify intruders.* - Natural to protect a territory that they feel is their own - Fences, pavement treatment, art, signs, good maintenance and landscaping
Natural Surveillance	*Premise: Criminals do not like to be observed.* - Flow of activities channelled to put more people near a potential crime area - Improve line of sight with windows, lighting, and removal of obstructions
Natural Access Controls	*Premise: Deterrent to keep unauthorized persons away* - Doors, shrubs, fences, locks, barriers - Properly locate entrances and exits to guide people there - Landscaping and footpaths to direct traffic - Psychological barriers: signs, paving textures (announce integrity and uniqueness of the area)
Maintenance & Management	*Premise: The more run-down an area is, the more likely there'll be crime, i.e. Broken Window Theory* - Clear sub-division of space into degrees of public / semi-public / private areas

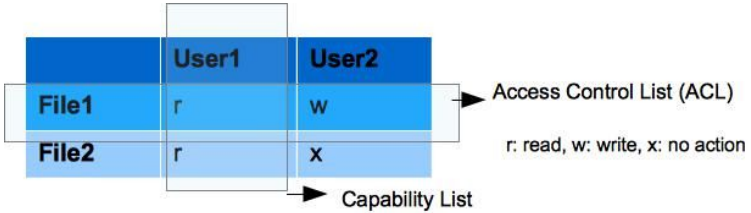
PHYSICAL protection systems (e.g. gate / doors) focus on: **PEOPLE**, **PROCEDURES** & **EQUIPMENT**

Smart Cards

Certificate (containing public key) is accessible at any time. PIN unlocks the private key. Challenge is issued from authenticator, encrypted with private key and sent back. Authenticator uses public key from certificate to decrypt.	
Contact	Electrical "fingers" wipe against exact point of chip contacts, providing it power and data I/O
Contactless	Has antenna surrounding perimeter of card that gets activated in electromagnetic field, generating power
Hybrid	Dual-chip, can be contact or contactless
Combi	Single-chip, can also be contact or contactless

Access Controls

Discretionary	Data owner decides permissions.
Non-discretionary	Administrator decides arbitrary permissions
Mandatory	Uniform implementation. All subjects cannot change constraints (passing info, granting access) Clearances and data classifications are used as labels. [Hierarchical, Compartmentalized, Hybrid]
Role-based	Permissions based on job title. Can be used to implement MAC or DAC.
Attribute(s)-based	Combine multiple attributes about subject, object and environment. AKA policy-based
Context-based	Usually for firewalls. Can detect and prevent DoS and provide real-time alerts and audit trails.



Transient authentication = something you have (worn token)

MAC Security Modes

	Clearance	Approval	Need to Know
Dedicated	ALL	ALL	ALL
System High	ALL	ALL	SOME
Compartmented	ALL	SOME	SOME
Multi-level	SOME	SOME	SOME

Access Controls

Deterrent	Barriers, fences, lighting, guard dogs, alarms
Preventive	IPS, guards, ID cards, locks, mantrap
Detective	IDS, motion detectors, logs, job rotation IR: Beam IR. Passive IR. Request to Exit. Wave Pattern: Ultrasonic / Microwave Capacitance: Electrical / Magnetic Photoelectric: Visible light levels (dark areas e.g. safe) BMS: Magnetic contact on door & frame Coaxial Strain-Sensitive Cable: Electric field to detect strain

Identity Management Lifecycle

Provisioning	Identity proofing, assigning privileges
Review	Prevents privilege creep
Revocation	Different from deletion (implies loss of information)

Access Control Roles

Data Owner	Responsible for classification of data. Holds legal rights and complete control over data they create
Data Controller	Determines purpose(s) for which and the manner in which data is to be processed. Due Diligence.
Data Steward	Responsible for data content (i.e. what's in the data field) via policies, guidelines, etc.
Data Custodian	Responsible for technical environment, data storage and maintenance (e.g. DB Admin)
Data Processor	Process data on behalf of Data Controller, ensures adherence, accessibility & maintenance. Due Care.
Data Subject	Individual who is the subject of personal data

Federation / SSO Technologies (Relying Party = Service Provider)

SAML	*[Identity Provider, Service Provider, User]* **Authentication** and **Authorization**. XML. Token-based
OAuth	*[Resource Server, Resource Owner, User]* **Authorization** framework. Can be used with XACML. Allows access tokens to be issued to third-party clients by authorization server, with approval of resource owner. The third party then uses the access token to access protected resources hosted by the resource server.
OAuth 2.0	Provides specific **authorization** flows for web applications, desktop applications, mobile phones, and smart devices. Not backward-compatible with OAuth.
OpenID	*[Application, Relying Party, User]* **Decentralized Authentication**. Register/login with account on another service.
OpenID Connect	*[RESTFUL HTTP JSON API, Authorization Server, User]* **Authentication** layer on top of OAuth 2.
XACML	*[PolicySet / Policy / Rule affects Subject / Resource / Action / Environment]* Manages **authorization**. Uses ABAC. Provides access control architecture and policy language to define them.

Security Control Implementations

Management	Uses planning and assessment methods to reduce and manage risk e.g. Perform risk assessment annually, ensure inventory exists for all hardware, penetration testing
Operational	Implements security as a continuous process e.g. backups, audit trail, ensuring all users have signed AUP, training program, configuration management
Technical	Uses technology to reduce risk e.g. display warning during login process, configure password expiry, encryption, IDPS, firewalls

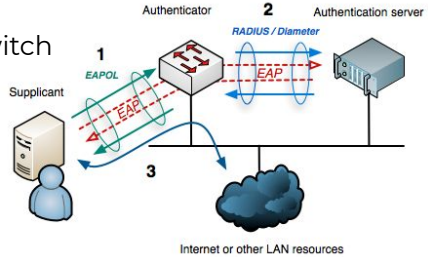
EAP - Authentication framework provides some common functions and negotiation of authentication methods called EAP methods

LEAP	Developed prior to 802.11i, used in WEP. Considered insecure. Replaced with PEAP or EAP-TLS.
EAP-TLS	Requires client-side X.509 certificate unlike HTTPS implementation of TLS. Private key of certificate can be stored in smart card for high security.
EAP-IKEv2	May be used with IPSec

802.1x - Encapsulates EAP over IEEE 802, i.e. EAPOL

Supplicant: Client
Authenticator: Access Point / Switch

Authenticator uses RADIUS to check for authentication before controlling access of supplicant to network.

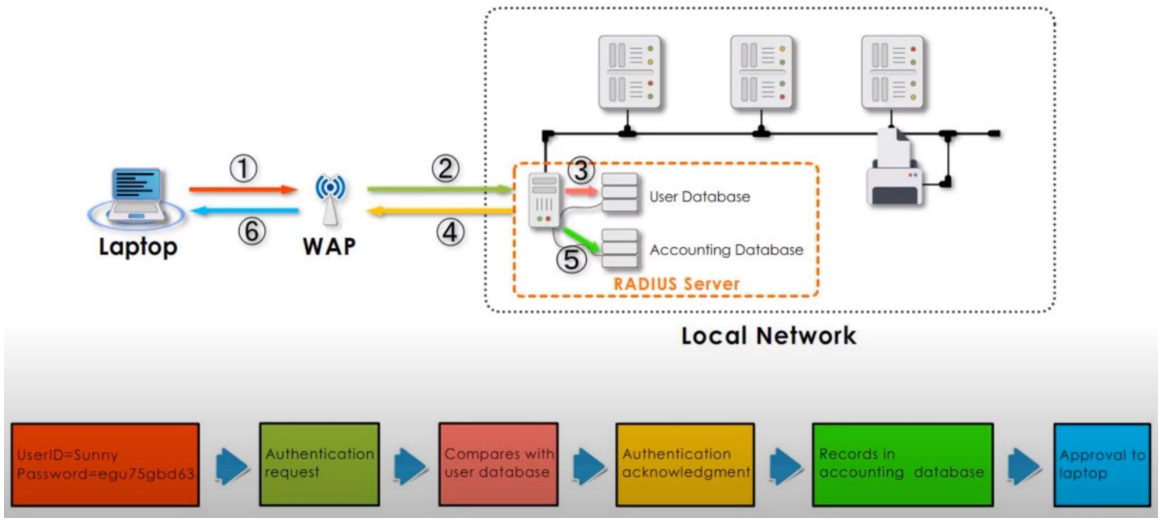


802.11i - Authentication protocol implemented as WPA2

4-way handshake for mutual authentication
Initial authentication process uses either PSK or EAPOL
Uses CCMP, i.e. AES CCM + AES CTR
Potentially vulnerable to KRACK (Key-Reinstallation)

RADIUS, TACACS, XTACACS, TACACS+ & Diameter

RADIUS	Client/Server - Server cannot initiate communication. Only provides **Reject / Challenge / Accept** response to user/pass authentication. Uses shared secret key and MD5 when transmitting passwords. Username in plaintext.
TACACS	Client/Server. Proprietary RADIUS. Provides AAA.
XTACACS	Client/Server. Separates AAA processes
TACACS+	Client/Server. Extends XTACACS with 2FA and dynamic passwords. **NEW PROTOCOL. NOT BACKWARD COMPATIBLE.**
Diameter	Peer-to-Peer model - allows server to request for credentials for access attempts or to proactively disconnect users. Has more AVPs than RADIUS. Allows different services (VoIP, MoIP, FoIP) to be authenticated in one architecture instead of individual architectures or over PPP and SLIP connections only. Can work with TLS and IPSec.



Attribute-Value Pairs (AVPs) outline how communication will take place between entities. More AVP = more functionality.

User profiles are maintained.

Pre-configured profile is assigned after successful authentication to control access rights

WATCH: https://www.youtube.com/watch?v=feHpDc1cLXM

Key Ciphers

Cipher	Type / Description	Rounds	Key Length	Block Size
RC2	Block / Insecure Key attack methodology: Chosen plaintext	18	Variable (Default 64 bits)	64 bits
RC4	**Stream** / Insecure implementation in TLS and WEP	1	40 - 2048 bits	N/A
RC5	Block		32 / 64 / 128 bits	0-2048
DES	Block. ECB < CBC < CFB < OFB < CTR	16	56 + 8 bits parity	64 bits
2DES	Block. Key attack methodology: Meet-in-the-Middle	32	112 + 16 bits parity	64 bits
3DES	Block	48	168 + 24 bits parity	64 bits
AES / Rijndael	Block (Original Rijndael: any key length in multiples of 32 bits between 128 and 256 bits) Key attack methodology: Side channel	10 12 14	128 bits 192 bits 256 bits	128 bits
Blowfish	Block	16	Variable	64 bits
Twofish	Block / One of the finalists for AES	16	128 / 192 / 256 bits	128 bits
IDEA	Block. Replacement for DES.	8.5	128 bits	64 bits
Skipjack	Uses Clipper chip	32	80 bits	64 bits
Camellia	Block / Standard cipher in IPSec, TLS, S/MIME, Kerberos, OpenPGP	18 / 24 / 24	128 / 192 bits / 256 bits	128 bits

DES Modes

Better Security ↓

Mode	Description	Uses IV	Propagates Errors
ECB	Each block encrypted individually. Vulnerable to known ciphertext attacks. Easiest and fastest. Commonly used for database encryption because of its speed.	No	No
CBC	Block mode chaining uses previous encrypted block to encrypt each subsequent block Used for authentication.	Yes	Yes
CFB	Stream mode chaining (feedback) uses previous encrypted bits to encrypt each subsequent bit. Used for authentication.	Yes	Yes
OFB	Stream. Uses encryption subkey before it is XORed with plaintext. Used for authentication	Yes	No
CTR	Stream. Uses 64 bit counter for feedback. Counter does not depend on results of previous bits or blocks of encryption. CTR can perform multiple encryptions in parallel, increasing speed. (Slower than ECB, but used in highly sensitive databases because it still allows for indexing)	Yes	No

Concepts

Confusion & Diffusion	Confusion: Substitution. Diffusion: Transposition. Both required for a strong cipher.
Link Encryption	Encrypts all information including header, trailer and routing information.
Stream vs Block	Stream ciphers are often used when the data has no fixed size (e.g. call, continuous data transfer). Stream ciphers are better used in hardware because of the bit-level XORing functions. Main problem with stream ciphers is proper implementation.
Perfect Forward Secrecy	Key is frequently changed so that if the latest key is compromised, only a small (latest) portion of data is.

Crypto Lifecycle

Pre-operational	Create cryptographic key, initialize by setting core attributes.
Operational	Normal usage
Revocation / Expiry	Stronger cryptosystem = shorter time to expiry
Post-operational	Keys are backed up for data reconstruction
Destroy	Only when compromised or fully retired

Key Management

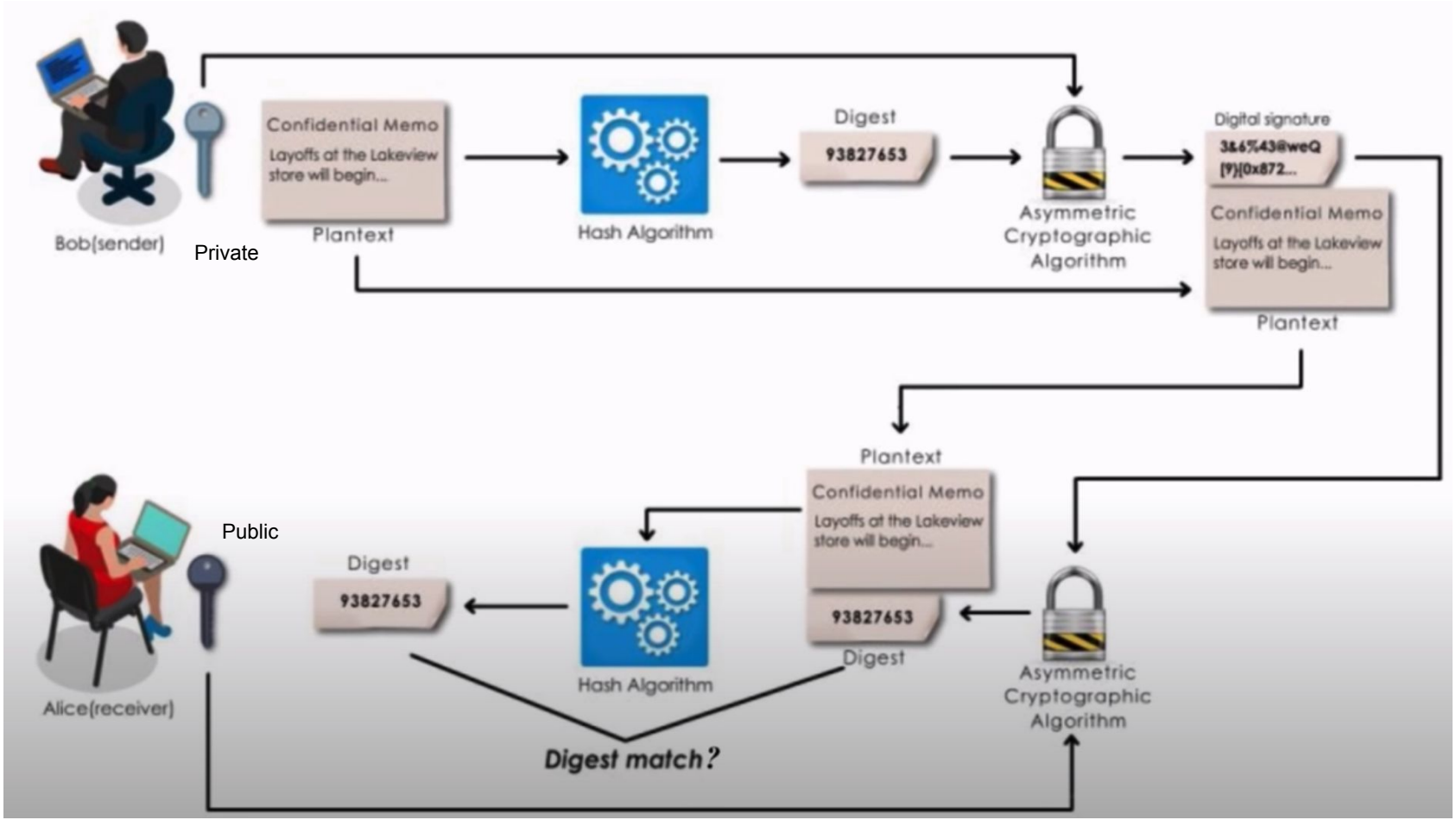
Recovery Agency	Given access to the key / cryptosystem. Provides the key / recovery process in the event it is lost.
Key Escrow	Given the key itself and is to access sensitive data under specific circumstances

Attacks / Exploits / Malware

FREAK	Cipher / Man-in-the-Middle, forced usage of weak keys
DROWN	Cipher (server configuration) / Exploited usage of still-supported SSLv2
BEAST	Cipher / Violated same-origin constraints to exploit CBC weakness in TLS 1.0
CRIME & BREACH	CRIME targeted compression over TLS, BREACH was an instance of CRIME on HTTP
POODLE	Cipher / Affected all block ciphers in SSL 3.0. Variant also affected TLS 1.0 to 1.2. Caused SSL migration to TLS.
Heartbleed	Cipher / Affected OpenSSL (an implementation of TLS)
Meltdown	Hardware / Intel x86 processors, race condition + side channel attack allowed rogue process to read of all memory regardless of authorization
Spectre	Hardware / Microprocessors with branch prediction. Side channel + timing attack
Cryptolocker	Ransomware / Encrypted local + network files using RSA
Wannacry	Ransomware / Old versions of Windows (SMB protocol), affected healthcare services
Mirai	IoT botnet causing DDoS

Digital Signatures

WATCH: https://www.youtube.com/watch?v=TmA2QWSLSPg



Certificates - X.509. Provide authentication before securely sending information to a server

Level 1 Assurance	Only requires email address
Level 2 Assurance	Verifies a user's name, address, social security number and other information against a credit bureau database

How They Work

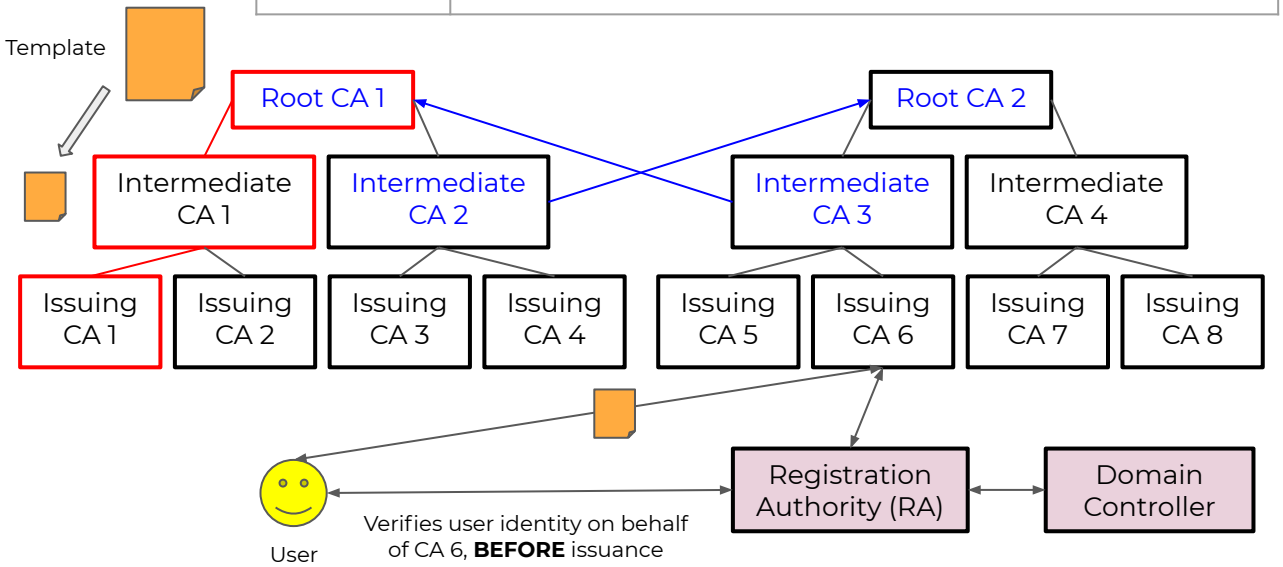
Alice	Requests for certificate via Certificate Signing Request (CSR)	sign($Alice_{Public}$, $CA_{Private}$)
Bob	Verifies Alice's certificate	verify($Alice_{Cert}$, CA_{Public})

Revocation

CRL	List of certificate serial numbers. Revoked or Hold (Temporary). Vulns: Large in size. SPOF, vulnerable to DoS. Fail-open.
OCSP with stapling	Contains less data than CRL. Less network bandwidth. Real-time status checks for high volume operations.

Certification Path Validation:
- Checks authenticity of certificates
- Checks CRL / OCSP
- Mitigates MITM

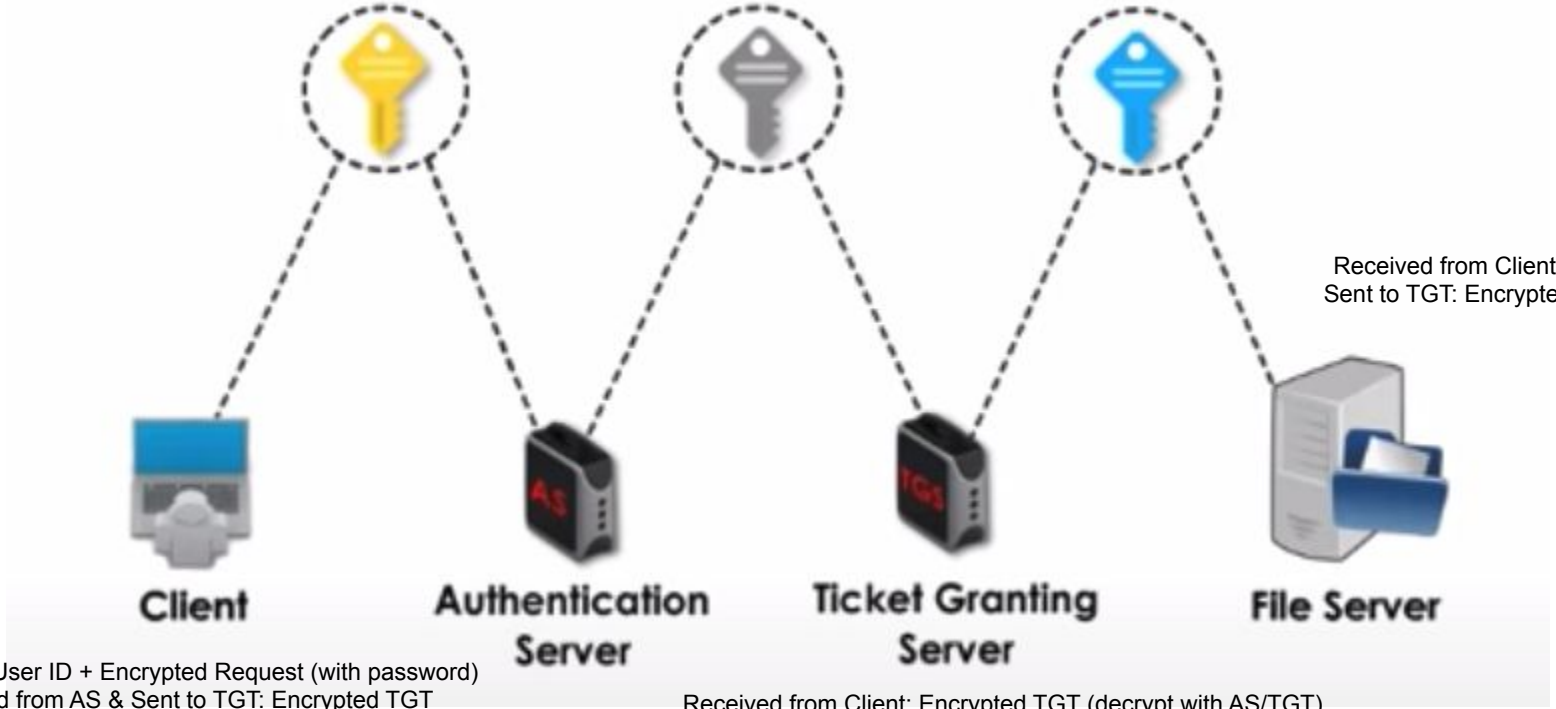
Cross Certification:
- Establish trust between different PKI
- Build overall PKI hierarchy
- Allow users to validate each other's certificate under different hierarchies
- Trust relationship, e.g. *Root CA 1* signing for *Intermediate CA 3*



Kerberos

Requires time synchronization (over NTP) to prevent relay attacks.

Received from Client: Encrypted Request (decrypt with password)
Sent to Client: Encrypted TGT (AS/TGS)



Received from Client: Token
Sent to TGT: Encrypted Token

Sent to AS: User ID + Encrypted Request (with password)
Received from AS & Sent to TGT: Encrypted TGT
Received from TGT: Token for FS
Sent to FS: Token

Received from Client: Encrypted TGT (decrypt with AS/TGT)
Sent to Client: Token for FS
Received from FS: Encrypted Token

WATCH: https://www.youtube.com/watch?v=_44CHD3Vx-0

BC/DR Processes

1	Develop BCP policy statement	Defined by C-suite, aka mission statement
2	Conduct BIA (aka functional analysis)	**Conduct** BIA to identify time-sensitive critical business functions and processes and the resources that support them
3	Identify preventive controls	**Identify**, **document** and implement to recover critical business functions and processes. **Data loss** causes most devastation.
4	Develop recovery strategies	
5	Develop IT contingency plans	**Organize** a **team** and compile a **BCP** to manage a business disruption. May include multiple contingency plans. Scope > Key Business Areas > Critical Functions > Depencies > MTD
6	Perform DRP training & testing	**Approval & Implementation** **Conduct training** for business continuity team and testing and exercises to evaluate recovery strategies and the plan
7	Perform BCP/DRP maintenance	Tested at least annually

Risk Management

Process
Frame
Assess
Respond
Monitor

Framework
Prepare
Categorize
Select Controls
Implement Controls
Assess Controls
Authorize Controls
Monitor Controls

Quantitative assessments are harder and for assessors with experience.

Qualitative assessments are solely done when there is insufficient time.

BC/DR Teams

Business Continuity Planning	IT, legal, media relations, network recovery, relocation, security, telecommunications. Has senior management. Usually doesn't include CEO.
Risk Management	Involved in planning, not execution
Incident Response	Responds to security incidents, not part of execution of contingency plan
Damage Assessment	
Recovery	Gets critical functions back up running
Salvage / Restoration	Restore to **primary** site. Can declare when primary site is available again. **LEAST** critical functions get restored first at primary site.

BC/DR Plans

Continuity of Operations	Restoring mission-essential functions (MEF) to alternate site, including management succession and HQ re-establishment
Business Continuity	Long term, strategic. e.g. backups
Disaster Recovery	Tactical. Primarily a site-specific plan developed with procedures to temporarily move operations.
Information Systems Contingency Plan	Covers recovery of systems regardless of site or location.
Occupant Emergency Plan	First-response procedures for occupants of a facility, including health and safety of personnel
Crisis Comms Plan	Internal and external comms to both employees and public, not IS-focused. May be used alone during public-exposure event.

Transportation of backup tapes must be included in RTO!!

Electronic Vaulting
Bulk. Full backups.

Remote Journaling
Transaction logs.

RAID

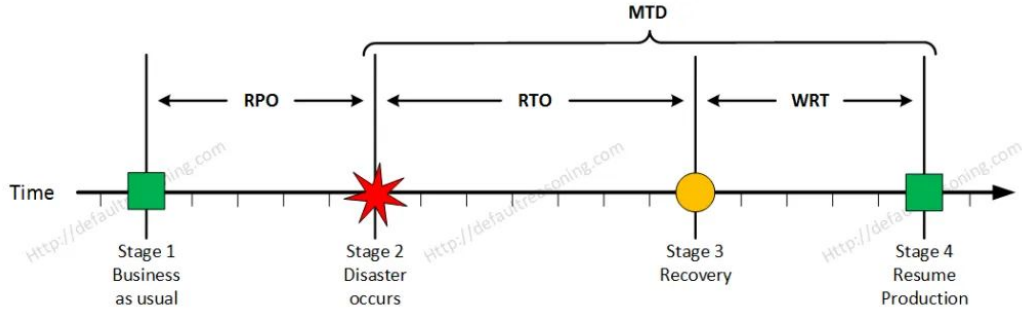
0	Striping (for high speed). No fault tolerance (no mirror, no parity)
1	Mirror 1-to-1. No striping. Very costly.
3	Striped mirror with parity in **dedicated** (bottleneck) drive. Minimum of 3 drives.
5	Mirror with parity striped together **across** all drives. Minimum of 3 drives.
1+0	2 or more mirrors in a stripe. No parity. Minimum of 4 drives.

System Crash Procedure

1	Enter Single-User Mode
2	Recover damaged file system files
3	Identify cause of reboot and repair
4	Validate critical config and system files
5	Reboot system as normal

Data Remanence

Clearing / Erasing
Purging / Sanitizing
Destroying



RTO: Per APPLICATION basis!
Might not need to be 100%

MTO: Operation in recovery mode.

Patch Management

Evaluate (“Do I need?”)
Test (“Does it work?”)
Approve (“OK.”)
Deploy
Verify (“Does it work?”)

Change Management

1	Request
2	Analyze
3	Document
4	Approval
5	Document
6	Test
7	Implement
8	(Rollback)
9	Document
10	Notify

Incident Response Steps

1	Prepare	Pre-incident. Includes training, policies definition, etc.
2	Detect	SIEM. IDPS. A/V software. Continuous Monitoring. End-user Awareness.
3	Respond / Contain	CSIRT / CIRT. Forensic backup. Isolate. Volatile memory dump. Power off as last ditch.
4	Mitigate / Eradicate	Analyze helps proper clean-up. May include root cause analysis. Restore to functioning state. Patch.
5	Report	
6	Recover	Restore to operational state.
7	Remediate	Starts from Mitigate phase. Core: Root cause analysis
8	Lessons Learned	

Event >> Incident
All incidents are events with negative outcomes vis-a-vis CIA.
Computer security incidents are incidents as a result of deliberate attacks / malicious action.

Fire Extinguishers

Class	Name	Suppression Material
A	Common Combustibles	Water, Soda Acid
B	Liquids & Gas (UK: C)	CO2, Halon Equivalent, Soda Acid
C	Electrical (UK: E)	CO2, Halon Equivalent
D	Metal	Dry Powder

Gas Systems (~~Halon~~)

FM-200	CEA-410 or 308
Argon	Argon-K

Good Temperature & Humidity

60 - 75 Fahrenheit
15 - 23 Celcius

Humidity: 40% - 60%
Corrosion (high) / Static (low)

Sprinklers

Wet Pipe	Constant supply, discharge immediate
Dry Pipe	Compressed air. Discharge after all air escaped. Prevents water freezing in pipes.
Pre-action	Detection system. No false activations. Water held back until detectors activated.
Deluge	Dry-pipe. All heads open at once to cover area. Large volume. No heat sensing elements.

Pressurized Rooms

Positive	Air can flow out of room
Negative	Air can flow into room

Lighting

Continuous
Standby
Movable
Emergency
Egress

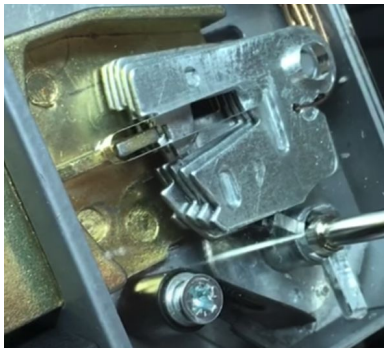
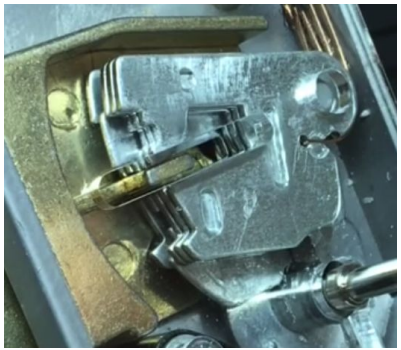
Location	Lighting Levels (fc) 1 fc = 10.7 lumen
Building entrances	5
Walkways	1.5
Parking garages	5
Walkways in parking garages	15 - 20
Over parked cars in garages	10 - 12
Areas around building	1

Power Concerns

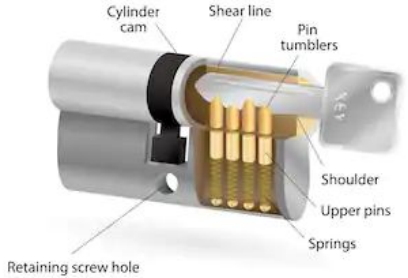
Spike	Short voltage ⇧
Surge	Long voltage ⇧
Sag	Short voltage ⇩
Brownout	Long voltage⇩
Fault	Short power ❌
Blackout	Long power ❌
Transients	Noise on power lines
Common Noise	Hot & Ground Wires EMI
Traverse Noise	Hot & Neutral Wires EMI

Tumbler Locks

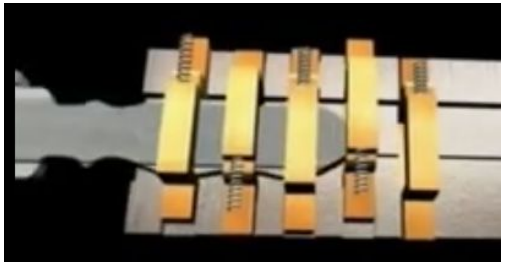
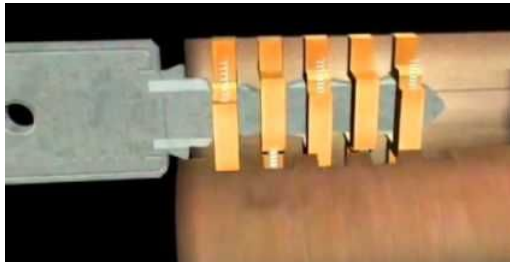
Lever Tumbler Lock

Pin Tumbler Lock



Wafer Tumbler Lock

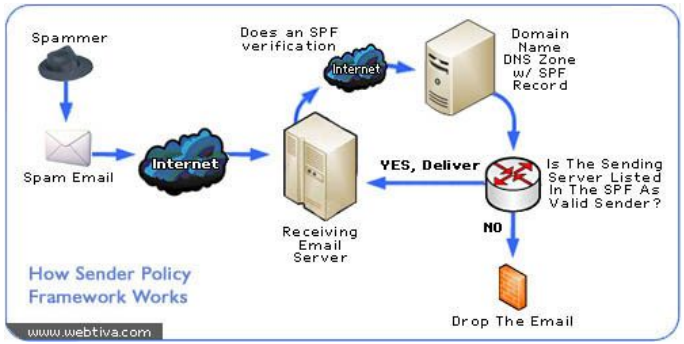



Relocks

Thermal	Engage extra lock when temperature is met, e.g. due to drilling of a safe
Passive	Engage internal bolts when tempering is detected

Email Security

System	Description	Crypto
Secure Multipurpose Internet Mail Extension (S/MIME)	Signed: Integrity, Authentication, Non-repudiation Enveloped: Integrity, Authentication, Confidentiality	X.509, SHA-1
MIME Object Security Services (MOSS)	Authentication, Confidentiality, Integrity and Non-repudiation	MD2 & MD5 RSA, DES
Privacy Enhanced Mail (PEM)	Authentication, Confidentiality, Integrity, Non-repudiation	RSA, DES, X.509
Message Security Protocol (MSP)	Used by military to sign and encrypt	
DomainKeys Identified Mail (DKIM)	Assertion that an email was sent by an organization	-
Pretty Good Privacy (PGP)	Phil Zimmerman, Asymmetric. Can also encrypt disk drives.	RSA, IDEA, SHA-1
Opportunistic TLS for SMTP Gateways	**Attempts** to setup encrypted connection with mail servers	[TLS]
Sender Policy Framework (SPF)	Spam Protection. Verifies with DNS for SPF record.	-



Viruses

Resident	Waits for programs to be executed then infects them.
Non-resident	Actively infects selected files without waiting for execution
Companion	Virus abuses “extension search order” (execution order) - .com, .exe then .bat - by naming itself the same as legitimate .exe but as .com
Boot-sector	Boots with virus in memory. Requires both disks to be connected to the same system for replication.
Tunneling	Installs itself under the A/V system and intercepts calls A/V system makes to the OS
Stealth	Hides the changes it makes as it replicates. Can intercept OS calls.
Self-garbling	Formats its own code to prevent A/V from detecting it
Polymorphic	Can produce multiple operational copies of itself. Mutates while retaining original functionality
Multipart	Can infect system files and boot sectors and restore itself upon deletion of a part
Shellcode	Wraps around an application so it is executed before the application
Retrovirus	Attacks / bypasses A/V system by destroying virus definitions or creating bypasses for itself
Phage Virus	Modifies other programs and databases. Only way to remove is to reinstall infected applications
Armoured	Includes protective code that prevents examination of critical elements and destruction

SCAP - Security Content Automation Protocol

CVE	Naming system for vulnerabilities
CVSS	Scoring system for severity of vulnerabilities Base score affects Temporal Score Temporal Score affects Environmental Score (Final)
CCE	Naming system for system config problems
CPE	Naming system for OS, applications and devices
XCCDF	Language format for security checklists
OVAL	Language format for security testing procedures

Side Channel Attacks

Covert Storage	High-level process writes, Low-level process reads
Covert Timing	High-level process transmits, Low-level process reads.

eDiscovery

1	Information Governance
2	Identification
3	Preservation
4	Collection
5	Processing
6	Review
7	Analysis
8	Production
9	Presentation

Evidence Types

Real / Object Evidence - Rare! *May be conclusive if incontrovertible*
Documentary / Written Evidence *Experts may be called to testify* Best (Original) Evidence (No Copies) Parol Evidence Rule (No Verbal Override)
Testimonial (Witness) Evidence Direct Evidence / Expert Opinion / Hearsay Evidence (incl. unauth'ed log)
Secondary Evidence Copies of original evidence

Admissible Evidence

Relevant
Material
Competent

Forensic Procedures

All principles must be applied
Actions when seizing evidence should not change evidence
Original evidence should only be handled by trained professionals
All activity must be fully documented
Individual possessing evidence is responsible for all actions taken
Any agency that handles evidence must comply with principles

Computer Crime

Computer-Assisted *Computer used as tool. Attack servers to obtain confidential data, attack financial systems to steal money*
Computer-Targeted *Computer is victim. B/O, DDoS, Virus destroy data*
Computer-Incidental Involved incidentally, not victim nor tool
Computer-Prevalence Violation of copyrights, software piracy

5 Be's of Evidence

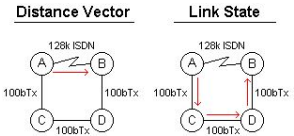
Authentic
Accurate
Complete
Convincing
Admissible

OSI Layers

Layer	Description	Unit	Protocols
Physical	Media, Signal and Binary Transmission Hardware: Network Card (NIC), Hub, Repeater, Concentrator	Bits	Coax, Fiber, Wireless, SONET, HSSI, EIA/TIA
Data Link	MAC (>> EUI-64) and LLC (Physical Addressing) Flow control, error notification Hardware: Switch, Bridge	Frames - Ethernet (IEEE 802.3), Token Ring, 802.11, FDDI	SLIP, PPP (pre-PPTP), ARP, ISDN, L2F + PPTP = L2TP (+ IPSec = VPN)
Network	Path Determination & IP (Logical Addressing) Routing: Ensures packet can reach its destination Hardware: Router / Bridge Router (Brouter - route first then bridge if fail)	Packets	IPv4, IPv6, IPSec, ICMP, RIP (DV), BGP (DV), OSPF (LS) IGMP, NAT, SKIP, IPX
Transport	End-to-End Connections and Reliability Segmentation: Divides data into transmittable packets	Sockets Segments (TCP) Datagram (UDP)	TCP, UDP, [SSL, TLS]
Session	Interhost Communication Authentication: Verifies remote host, data received is authentic	Data	APIs, Sockets, RPCs
Presentation	Data Representation and Encryption	Data	File formats e.g. JPG, MIDI
Application	Network Process to Application	Data	HTTP, FTP, SSH, SMTP, DNS, DHCP

Encapsulation

Distance Vector: Choose route with least number of hops based on distance. (RIP, BGP, IGRP)
Link State: Choose fastest path. Neighbour Table, Topology Table, Routing Table. Measures cost to each neighbour, construct shortest path. (OSPF)



Packets with internal source addresses should never originate from outside the network, so they should be blocked from entering the network.
Packets with external source addresses should never be found on the internal network, so they should be blocked from leaving the network.
Private IP addresses should never be used on the Internet, so packets containing private IP addresses should be blocked from leaving the network.

IGP & EGP

IGP	Internal routing within an autonomous system (e.g. organization-controlled network)	
	IGRP	[DV] Uses 5 criteria to make a “best route” decision. Network admin can set weightage. Cisco.
	RIP	[DV] Standard that outlines how routers exchange routing table data. Slow, legacy. V1 has no authentication. V2 sends passwords in cleartext or MD5.
	OSPF	[LS] Sends out routing table information (smaller, more frequent updates). Replaced RIP. Optional authentication
EGP	External routing between separate autonomous systems	
	BGP	Enables routers on different AS to share routing information. Commonly used by ISPs to route data.

Common Ports

0 - 1023	System / Well-known
1024 - 49151	Registered / User
49152 - 65535	Dynamic

DHCP	UDP 67 / 68
TFTP	UDP 69
Kerberos	88
NetBIOS	137 - 139
ActiveDirectory	445
MsSQL	1433
RDP	3389
Syslog	514
Printers	515 / 9100
SMTP	25 / [S] 465 / 587
POP3	110 / [S] 995
IMAP	143
RADIUS	UDP 1812 / TCP 2083
IPSec - ISAKMP	UDP 500
L2TP	1701

Firewalls

Stateful	Dynamic Packet Filtering (Layers 3 & 4) Can assemble IP packets to understand context and filter
Stateless	Static Packet Filtering (Layer 3) Only looks at each individual packet to filter
Circuit-Level	Layer 5
Deep Packet Inspection	WAF (Layer 7)
Proxy Firewall	Mediate communication between trusted and untrusted end-points. Can hide source of network connections.

Proxy Types

Circuit-Level	Trusted host can communicate with untrusted host. Data field is not inspected before being forwarded. Networking only. E.g. **SOCKS** -- transport layer for socket security
Application-Level	Relays traffic from trusted end-point running specific application to untrusted end-point. Analyzes data field for common attacks.
Multi-Homed	At least 2 network interfaces (inbound / outbound)

Switches & IDS

- Promiscuous Mode Port: All traffic passing through a switch can be monitored.
- a.k.a. Switched Port Analyzer (SPAN) Port or Mirror Port.
- Can also be achieved using a hub or Test Access Port (TAP).

IPSec - Combines IKEv1/IKEv2, AH and ESP

IKE	Start of process. Purpose: Negotiate SA (agreement on how to do crypto). After SAs negotiated, can protect with AH or ESP. Phase 1: Negotiate ISAKMP SA (bi-directional) Defines policy set (hash/encryption algo, DH, etc.) used to communicate about management issues about the tunnel Same settings should be defined on both sides of the tunnel on router / firewall Phase 2: Negotiate IPSec SA (uni-directional, therefore 2 are required per connection) Defines transform set used to communicate data, using tunnel settings derived from Phase 1 Has unique SPI for each SA (1 for inbound, 1 for outbound) but no port numbers IKEv1: Uses preshared keys IKEv2: Extended with EAP, allowing for certificates / tokens to be used
AH	Provides authentication and integrity check of the **full traffic including headers**, but not encryption of payload. Hates NAT. Digitally signs a packet for authentication, providing non-repudiation.
ESP	Provides authentication and encryption of payload, but **outer IP header is not checked for integrity**. Works with NAT.

IPSec Modes

Transport	Encrypts IP packet data only, but not header
Tunnel	Encrypts **WHOLE** IP packet, adds new header Encapsulation

	AH	**ESP**
Transport	Authenticated Packets (Digitally signed)	Authenticated Packets Encrypted Payload
Tunnel	Authenticated Packets (Digitally Signed) Tunneled Payload	Authenticated Packets & Header Tunneled & Encrypted Payload

Subnetting

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/24	/25	/26	/27	/28	/29	/30	/31	/32

Network ID	Subnet Mask	Host ID Range	# of Usable Host	Broadcast ID
192.168.4.0	/26	192.168.4.1-192.168.4.62	62	192.168.4.63
192.168.4.64	/26	192.168.4.65-192.168.4.126	62	192.168.4.127
192.168.4.128	/26	192.168.4.129-192.168.4.190	62	192.168.4.191
192.168.4.192	/26	192.168.4.193-192.168.4.254	62	192.168.4.255

ARP Poisoning - Spoofing of MAC address for a requested IP address, to force redirection to alternate systems

Impacts	DoS (affects availability), Session Hijacking, MITM	
Mitigations	Use Static ARP	Use VPN
	Use IDS (on promiscuous port mode)	Use packet filtering firewall

DNS Poisoning - Spoofing of pointer (HOSTS file or Access Point) to alter DNS resolution

Mitigations	Only allow authorized changes to DNS information	Restrict zone transfers
	Log all DNS activity	

DNS Hijacking - Spoofing of replies sent to a caching DNS for non-existent subdomains, allow attacker to take over entire DNS

Mitigations	Use DNSSEC	

Eavesdropping Attacks - Listening in on communications

Mitigations	Encryption	Physical access control

Replay Attacks - Use of captured information via eavesdropping to re-establish a session

Mitigations	Authentication expiry mechanisms	Use sequenced / set expiry for session IDs

Modification Attacks - Alteration and use of captured data

Mitigations	Digital signature	Packet checksum verification

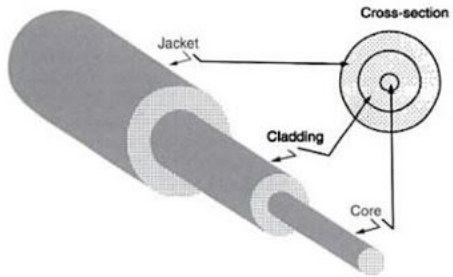
UTP Types

Std	Speed	Description
CAT 1	4 Mbps	2 pairs Voice only, no data
CAT 2	4 Mbps	4 pairs
CAT 3	10 Mbps	4 pairs
CAT 4	16 Mbps	4 pairs. Token Ring.
CAT 5	100 Mbps	4 pairs. 100 MHz RJ-45. Token Ring. 1[x]BaseT
CAT 5e	1 Gbps	350 Mhz
CAT 6	1 Gbps	
CAT 6e	1 Gbps	
CAT 7	10 Gbps	

Cable Types

Cable	Type	Speed	Distance
xBase**y**	UTP	***x*** Mbps	-
xBaseT**y**	UTP	***x*** Mbps	100m, except...
10GBaseT	UTP / STP	***10G***bps	Cat 6: 55m Cat 6a: 100m
xBaseF**y**	Fibre	***x*** Mbps	2km mmhd: 412m mmfd: 2km smhd: 10km
10Base2 Thinnet	Coaxial	10 Mbps	185m (~200m)
10Base5 Thicknet	Coaxial	10 Mbps	500m

Fibre



WiFi

Std	Speed	Freq
802.11	2 Mbps	2.4 GHz
802.11a	54 Mbps	5 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	54 Mbps	2.4 GHz
802.11n	200+ Mbps	2.4 / 5 GHz
801.11ac	1 Gbps	5 GHz

To add: EMI susceptibility

VoIP Vulnerabilities

Caller ID falsification / spoofing - vishing (VoIP phishing) or Spam over Internet Telephony (SPIT) attacks
O/S vulnerabilities - unpatched call manager systems and VoIP endpoints (phones)
MITM - spoofing of call manager or endpoint connection negotiation and responses
VLAN / VoIP hopping - VoIP and computer systems in same switches
Eavesdropping can occur due to unencrypted traffic - mitigated by using Secure Real-Time Transport Protocol (SRTP)
The current Internet architecture over which voice is transmitted is less secure than physical phone lines
Softphones (software phone, e.g. Skype) make an IP network more vulnerable than hardware-based IP phones

Phreaking Methods

Black Box	Used to manipulate line voltage to steal long-distance service
Red Box	Used to simulate tones (coins dropping)
Blue Box	Used to simulate the 2600 Hz tones to interact directly with phone system backbone
White Box	Used to control phone system using dual-tone multifrequency generator (keypad handset)

Callback Modes

User gets a dial-back on a predefined number that is associated with the user
Caller-ID mode requires user to dial in from the pre-defined number in order to get the call-back

Virtual Circuits - logical communication pathway created over a packet-switched network

Permanent Virtual Circuits (PVC)	Dedicated circuit that always exists and is available to the customer
Switched Virtual Circuits (SVC)	Like a dial-up connection, available on-demand, but must be setup for each use and is then torn down immediately after use

WAN Technologies

Dedicated Lines / Lease Lines

Uses all channels.

Always available and reserved for single customer. SDLC / HDLC used as L2 protocol.

Each channel: 64 Kbps
24 channels: 1.54 Mbps

European version has 32 B & 2 D channels.

34 channels: 2.18 Mbps

Technology	Connection Type	Speed
DS-0	Partial T1	64 Kbps - 1.54 Mbps
DS-1	T1	1.54Mbps
DS-3	T3	44.74 Mbps
Cable		10+ Mbps
European DTF 1	E1	2.18 Mbps
European DTF3	E3	34.368 Mbps

Non-Dedicated Lines

Connection must be made before data transmission, e.g. modems, DSL, ISDN (digital voice + data)

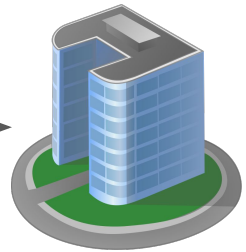
ISDN BRI: Two B channels for data, one D channel for management

ISDN PRI: 2 to 23 B channels, one D channel for management

HQ

PVC. T*x* / E*x* line.

SDLC / HDLC



Branch Office

ATM over T*x* / E*x* line
DSL (PPPoA / PPPOE)

PVC / SVC. SMDS.
Links multiple LANs
to form a MAN.

Local Telco
Internal mesh,
external star

PVC or SVC. SDH / SONET

Mesh or Ring

Telco

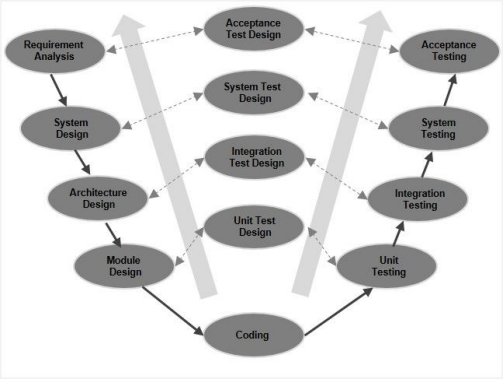
WAN Connection Technologies

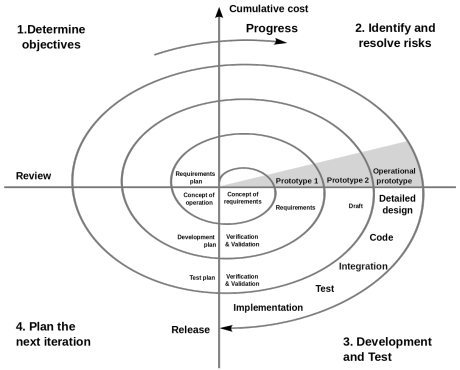
X.25 / Frame Relay	Old. Packet switching. Used PVC.
ATM	Cell switching. Either PVC or SVC.
Switched Multimegabit Data Service (SMDS)	Connectionless packet switching. Forms Metropolitan Area Network.
Synchronous Digital Hierarchy (SDH)	Fibre from ITU. Uses Synchronous Time Division Multiplexing to high-speed duplex. Mesh or Ring.
Synchronous Optical Network (SONET)	Fibre from ANSI. Mesh or Ring.
Synchronous Data Link Control (SDLC)	Polling on permanent connections at Layer 2 to provide connectivity on mainframes.
High-level Data Link Control (HDLC)	Refined SDLC. Full Duplex. Uses polling at Layer 2.

SONET	SDH	Rate
STS-1 / OC-1	STM-0	51.84 Mbps
STS-3 / OC-3	STM-1	155.52 Mbps
STS-12 / OC-12	STM-4	622.08 Mbps
STS-40 / OC-40	STM-16	2.488 Gbps
STS-96 / OC-96	STM-32	4.876 Gbps
STS-192 / OC-192	STM-64	9.953 Gbps
STS-768 / OC-768	STM-256	39.813 Gbps

SDLC

IDIOD	CBK	
Initiation	Initiation	Project Charter, business case, benefits, high-level risk assessment. Early involvement of security.
	Requirements	Identify stakeholders, functional requirements. Cost-benefit analysis. Create risk management plan.
	Architecture	
Design	Design	
Implementation	Development / Acquisition	
	Testing	Functional: Unit Testing / Integration Testing / System Testing | Non-Functional
Operation	Release	Operations & Maintenance. Certification & Accreditation (Full / Provisional)
Disposal	Disposal	Data retention policies. Data disposal policies. NIST 800-88: Erase / Sanitize / Destroy





REST Architecture

Uniform Interface (Modular)
Stateless (Info Within Request)
Cacheable
Client-Server
Layered System
Code on Demand (Optional)

Software Acquisition

Planning
Contracting
Monitoring & Acceptance
Follow On

Expert System - Uses AI and datasets to model decision-making

Forward Chaining	Reasoning approach that uses if-then-else rules to obtain more data than is currently available. Used when there are few solutions compared to number of inputs
Backward Chaining	Begin with a possible solution (goals), then use dataset to justify the solution.

Data Attack Methods

Mining	Spotting **trends / patterns** in data sets
Aggregation	**Accumulated** non-confidential information **directly forms** confidential information
Inference	**Logical jump / deduction** required to derive confidential information from knowledge

OWASP

Injection	Original: `select * from `users` where `username` = "administrator" and `password` = "input";` Example 1: `select * from `users` where `username` = "administrator";--" and password = "input";` (-- indicates comment) Example 2: `select * from `users` where `username` = "administrator" and password="input" or "a"="a";` Mitigated by validation.
XSS	Reflected: User input is immediately printed out again for user to make changes, and in the process, attack code is executed. Transient. Stored: Attack code is stored in the database and output repeatedly. DOM-based: Attack code is generated via user input. Mitigated by validation.
CSRF	Attacker utilizes a victim's pre-authenticated session to carry out a transaction without their knowledge. Mitigated by MFA / CSRF Tokens.

ACID Model

Atomicity: Complete transactions. e.g. two-phase commit
Consistency: Valid states & transactions
Isolation: of each transaction
Durability: Permanent results

DBMS & Commands

DDL	Data Definition Language	`CREATE`, `DROP`, `ALTER`, `TRUNCATE`
DQL	Data Query Language	`SELECT`
DML	Data Manipulation Language	`INSERT`, `UPDATE`, `DELETE`
DCL	Data Control Language	`GRANT`, `REVOKE`
TCL	Transaction Control Language	`COMMIT`, `ROLLBACK`

Database Shadowing (read-only) is NOT Database Replication

Database Taxonomy

Tuple	Row
Cardinality	Number of rows
Degree	Number of columns
Domain	Allowable values that an attribute can have

Database Connections

ODBC	API that allows any application to connect
JDBC	API that allows any JAVA application to connect
OLE DB	Method of linking data from different DBs together
DDE / OLE	Allows processes to exchange data with each other

Database Keys

Primary	Unique key (usually auto-increment) that identifies each row in a table.
Foreign	References the primary key of another table

Database Integrity

Referential	Foreign keys must reference existing rows. Prone to human error, error-cascading.
Entity	Primary key to ensure each row can be uniquely referred
Semantic	Ensures data entered in a row is within allowable domain

To add: REST vs SOAP, RPC

Maturity Models

SSE-CMM: - Covers entire lifecycle - Whole organization - Concurrent interaction with other disciplines - Interactions with other orgs	**IDEAL** Initiate, diagnose, establish, act, learn

Software CMM

Initial	State of flux. Ad-hoc decisions.
Repeatable	Can be repeated with some form of consistency. Not rigorous. Not documented.
Defined	Documented SOPs, but may not be sufficiently implemented. Developmental stage.
Managed	Processes tested, refined / optimized. Able to demonstrate competence across conditions. No measurable loss in quality.
Optimizing	**CONTINUOUS PROCESS.** Addresses common causes of statistical variances in processes. Changes processes to improve performance.

Product Evaluation Models

TCSEC	ITSEC	CC	Protection	Usage
D	F-D + E0	EAL 0/1	Minimal Protection / Functionally Tested	
C1	F-C1 + E1	EAL 2	Discretionary Security / Structurally Tested	Users process info at same sensitivity level. Low security.
C2	F-C2 + E2	EAL 3	Controlled Access / Methodically Tested & Checked	Authentication and auditing enabled. Granular access control, no object reuse.
B1	F-B1 + E3	EAL 4	Labelled Access / Methodically Designed, Tested & Reviewed	OS & products. Governments.
B2	F-B2 + E4	EAL 5	Structured Security / Semi-formally Designed & Tested	Trusted path, no backdoors. Lowest level for trusted facility management.
B3	F-B3 + E5	EAL 6	Security Domains / Semi-formally Verified, Designed & Tested	Trusted recovery
A1	F-B3 + E6	EAL 7	Verified Design & Protection / Formally Verified, Designed & Tested	

TSEC comes from the Orange Book. Only addresses confidentiality. Based on functionality, effectiveness, assurance.
ITSEC is European version of TSEC. Addresses CIA.

TSEC C: DAC | TSEC B: MAC based on Bell-LaPadula, uses security labels.

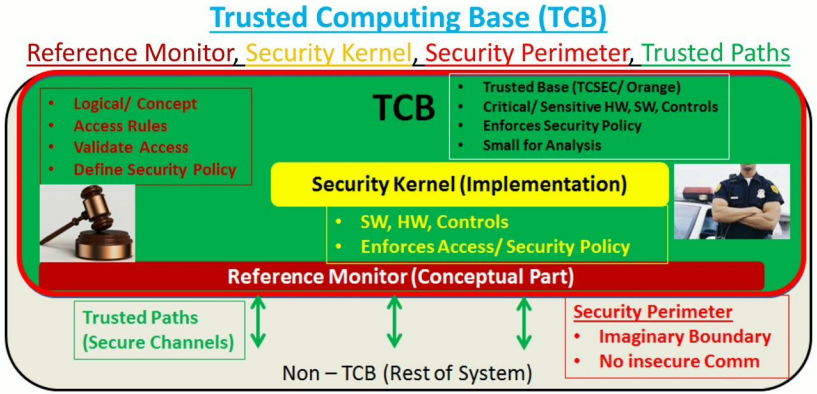
ITSEC defines functionality (AAA) and assurance (performing consistently, i.e. develop practices, documentation and configuration management) separately because two distinct systems may have the same functionality but different assurance levels.

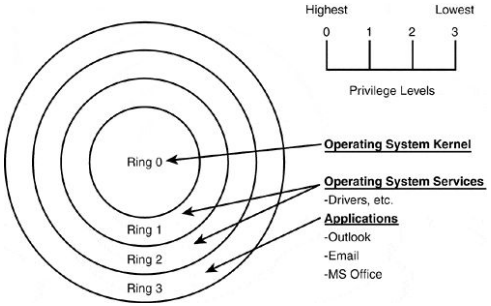
Common Criteria:

- Mainly targets consumers, developers & evaluators
- Security Target (ST): Security profile of TOE, compared both before and after evaluation
- Protection Profile (PP): Standard/Baseline
- Outcome of TOE: Objective, Repeatable, Defensible Evidential results

Trusted Recovery Types

Manual	If system fails, does not fail secure. Must have intervention.
Automated	Can perform trusted recovery to restore itself against at least one type of failure
Automated w/o Undue Loss	Automated + Mechanisms to ensure that specific objects are protected to prevent their loss
Function	Can automatically recover system functions in case of failure





Reference Monitor: Abstract concept of ACL implementation, tamper-proof, small enough to test.

Kernel: Made up of all components of TCB. Responsible for implementing security policy and reference monitor. To be secure, kernel must be complete, isolated and verifiable.

Execution Domain Switching: The TCB allows processes to switch between domains in a secure manner

Execution Domain:
Isolated area used by trusted processes when they run in privileged state.

Protection Domain:
Memory space isolated from other processes in the multi-processing system.

Trusted Path:
Communication channel between applications and kernel in TCB

Trusted Channel:
Communication channel between **EXTERNAL** applications and the TCB

Processor Privilege States

User / Process / Problem / Program	Processor limits access to system data and hardware granted to the running process
Kernel / Supervisor	Has access to all resources and can execute both priv & non-priv instructions

CPU Architectures

Von Neumann / Princeton	Data and instructions are the same, use the same bus. Leads to injections. Instruction fetch and data operations cannot occur at the same time. Bottlenecked system performance.
Harvard	Separates data and instructions into different buses

CPU Components

Control Unit (CU)	Fetches and interprets code, oversees execution of instruction sets. Determines priority and time slice.
Arithmetic Logic Unit (ALU)	Performs calculations
CPU	General registers: hold variables and temporary results as ALU works through execution steps Special / dedicated registers: Hold info e.g. program counter (holds next instruction to be fetched), stack pointer, program status word (PSW)

CPU Pipeline

Each instruction is loaded after previous is pushed to next. Increases performance.

1	Fetch
2	Decode
3	Execute
4	Write

Multithreading: Divides CPU time among child processes.
Multitasking: Divides CPU time among multiple processes, each given slice of time, then moves on to the next task. Cycles back after all tasks are each given slice of time. Cooperative (legacy) / Pre-emptive: OS controls how long a process can use the resource.
Multiprocessing: Divides load among multiple CPUs. Does not divide CPU time among child processes. Symmetric Multiprocessing (SMP) uses single OS to manage every CPU. Asymmetric Multiprocessing (AMP) uses separate OS installation per CPU.
Scalar Processing: Executes 1 instruction at a time
Reduced Instruction Set Computing (RISC): Simpler instructions, less clock cycles to execute
Complex Instruction Set Computing (CISC): Instructions that perform many operations per instruction

Memory Manager Responsibilities

Relocation	Move / swap content between RAM and HDD as needed, provide pointers to applications
Protection	Provide access control for memory segments
Sharing	Allow multiple users with different access levels to interact with application / process while running. Enforce confidentiality & integrity controls between processes using shared memory segments
Logical Organization	Segmentation of all memory types, provide addressing scheme at abstraction level and allow for sharing of software modules e.g. DLL modules
Physical Organization	Segmentation of physical memory space for allocation

Memory Address Types

Absolute / Explicit	Physical memory address
Relative	
Content-addressable	aka associative memory. Memory used in complex searches for a specific data value
Logical	Index memory addresses that softwares use

Memory Protection Methods - failure results in system going into maintenance mode

Kernel-mode system components can only be used while in kernel mode. Attempts will generate a fault and create access violation
Address Space Layout Randomization (ASLR): Virtual memory mapped to sporadic allocation of physical memory
Hardware / software controlled memory protection, such as read/write access. Data Execution Protection (DEP): Requires DEP-enabled CPU. Prevents executable code from executing within data pages.
Access control lists to protect shared memory objects. Forced security checks
Heap Metadata Protection: Microsoft protection that forces application to fail if pointer is freed incorrectly. Required in Microsoft SDL.
Pointer Encoding: XOR random values with pointers. Attack would need to guess the right XOR. Not required in Microsoft SDL.
Virtual Memory: Maps hardware memory address to applications. Enables multitasking by sharing libraries between applications, enabling more than one application to access the same information from the same memory address. Allows swapping and paging.
Paging: Moves fixed-length block of memory to disk (secondary memory). When it is required by OS, info is retrieved and loaded back.
Swapping: Copies entire process to disk (secondary memory).

Process Isolation & Memory Protection Methods

Encapsulation	No process can interact with internal of another process
Time Multiplexing	Provide structured, controlled, managed access to resources
Naming Distinctions	PID. Each process is assigned unique identity in OS
Virtual Address Memory Mapping	Allows each process to have its own memory space, enforced through Memory Manager, which provides - 1. Abstraction level for programmers 2. Maximize performance of RAM 3. Protection of OS and applications once loaded into memory

Interrupted processes can create security breaches when the current process is given a clearance level of the previous process.

Program counter register contains memory address of next instruction to be fetched.

Adam Gordon's CISSP Questions

1. https://www.surveymonkey.com/r/Z9TJ75G	21. https://www.surveymonkey.com/r/XPBJXGT	41. https://www.surveymonkey.com/r/GPZHYGX
2. https://www.surveymonkey.com/r/G37CSJT	22. https://www.surveymonkey.com/r/Q9ZYQ87	42. https://www.surveymonkey.com/r/RPB5HBR
3. https://www.surveymonkey.com/r/SVCS6DH	23. https://www.surveymonkey.com/r/NKFS2FZ	43. https://www.surveymonkey.com/r/HKRX28T
4. https://www.surveymonkey.com/r/SVCS6DH	24. https://www.surveymonkey.com/r/GGZSH7Y	44. https://www.surveymonkey.com/r/DC9HZHM
5. https://www.surveymonkey.com/r/QFZDGYS	25. https://www.surveymonkey.com/r/6CB3J8F	45. https://www.surveymonkey.com/r/B55YZ78
6. https://www.surveymonkey.com/r/M589TPY	26. https://www.surveymonkey.com/r/GSHRS39	46. https://www.surveymonkey.com/r/F8SX3V2
7. https://www.surveymonkey.com/r/BFBDWMF	27. https://www.surveymonkey.com/r/C9CQHFN	57. https://www.surveymonkey.com/r/MJJZTGQ
8. https://www.surveymonkey.com/r/JRMWPTY	28. https://www.surveymonkey.com/r/VHBLHJ5	
9. https://www.surveymonkey.com/r/DB9TFMS	29. https://www.surveymonkey.com/r/G5G3NRD	
10. https://www.surveymonkey.com/r/8YTYHZD	30. https://www.surveymonkey.com/r/6LVY8L9	
11. https://www.surveymonkey.com/r/2RVV3DY	31. https://www.surveymonkey.com/r/8DXLJT3	
12. https://www.surveymonkey.com/r/NZZTSJ6	32. https://www.surveymonkey.com/r/L2NFNTG	
13. https://www.surveymonkey.com/r/223KBDH	33. https://www.surveymonkey.com/r/2H8MR2R	
14. https://www.surveymonkey.com/r/VQW6PZB	34. https://www.surveymonkey.com/r/FG39W6W	
15. https://www.surveymonkey.com/r/36LJZVC	35. https://www.surveymonkey.com/r/XP9GRLV	
16. https://www.surveymonkey.com/r/DZ98W5Q	36. https://www.surveymonkey.com/r/VB9H597	
17. https://www.surveymonkey.com/r/6BV3H9X	37. https://www.surveymonkey.com/r/LFFVZS7	
18. https://www.surveymonkey.com/r/HS6CXMR	38. https://www.surveymonkey.com/r/XQ2ZY25	
19. https://www.surveymonkey.com/r/KJK5LZ2	39. https://www.surveymonkey.com/r/9QYQ2W2	
20. https://www.surveymonkey.com/r/9ZDD8KW	40. https://www.surveymonkey.com/r/Z72FNMH	

Wentz Wu's Question of the Day

Thor's Practice Questions