Structured Cyber Security Brainmaps V1.0

By
Haseeb Nasir Ali

- Please do not modify this document and only use for its intended purpose that is to seek knowledge
- Please Do Not Duplicate

CREDITS AND BOOKS REFERENCED

- All-in-One Exam Guide CISSP, 8th Edition by Shon Harris & Fernando Maymi
- Study Notes and Theory Website
- e-Authentication Token Types by New York State Information Technology Standard
- NIST Computer Security Incident Handling 800-61
- NIST Contingency Planning Guide 800-34
- NIST Definition of Cloud Computing 800-145
- NIST Guide for Developing Security Plans for Federal Information Systems 800-18
- NIST Guide to Information Technology Security Policy 800-35
- NIST Information Security Continuous Monitoring (ISCM) 800-137
- NIST Information Security Handbook 800-100
- NIST Information Security Testing and Assessment 800-115
- NIST Security and Privacy Controls 800-53
- ISC2 CISSP Study Guide by Mike Chapple

Security & Risk Management

- Basics
  - Confidentiality — Data/Information accessible/available/readable to authorized source/subject
  - Integrity — No modification, keep originality
  - Availability — Available when required
  - Subject — Who take action, who performs, who acts — Active
  - Object — Acted upon — Passive
  - Data States
    - In storage (at rest)
    - In transit (moving)
    - In process (in transient state)
- Confidentiality
  - Basics
    - No authorization, no access
    - May be authorized to view, but not modify (C and I are connected)
  - Confidentiality drivers
    - Secrecy - keeping secret (meaning not even telling people)
    - Concealment - hiding (meaning people know but hiding)
    - Seclusion - keeping out of the way location
    - Privacy - personally identifiable information
    - Isolation - keeping seperate to ensure no intermingling
- Integrity
  - Features meaning data should remain
    - Genuine
    - Unaltered
    - Complete — Not missing any relevant details
    - Comprehensive — All required elements are in place
    - True
  - Must be maintained while
    - Data in process
    - Data in transport
    - Data in storage
  - meaning
    - Allow only authorized change from authorized subject
    - Prevent unauthorized change from authorized subject
    - Keep data in tact — Main element and sub elements of data don't loose its veracity
  - To implement
    - Non-repudiation — Subject cannot deny what he did
      - Part of accountability
    - Authorization
    - Authentication
    - Accounting — Keep track who is doing what
- Availability
  - Basics — Object/data remains accessible
  - 3 main features
    - Timely Access — Accessible when required
    - Concurrent Access — Accessible even when multiple subjects are accessing
    - Useable Access — Operational when accessed
- Security Governance
  - Basics/ Concepts
    - It is not only IT, it is an Organizational Security where IT is one part
    - Its key is – implementation of security solution and its management
    - Its objective is – business continuity and business growth through security principles
    - It is only one element of Organizational Governance
    - It is spearheaded by Security Board or Board of Governors
    - NIST Guidelines are – 800-53/800-100
    - Regulatory or Legal Compliance requirements also influence on security governance in order to comply with them
  - Security Policy and Security Management — **Continued next sheet**
    - Senior Management defines policy and middle manage/technical implements — Recommended Top-Down approach
    - Team function should be autonomous – to keep organizational influence minimum — Team is lead by CISO
    - Roles and responsibilities should be defined, who will do what in terms of security
    - Senior Management buyout is very important
- Protection Mechanisms utilized by CIA
  - Layering
    - Multiple layers of security concept
    - Layers in series, one after another
    - Defense in depth technique
  - Abstraction
    - Grouping of Objects to simplify view and apply consolidated security controls
    - Key concept – Simplified application of security controls by grouping of similar objects
  - Data Hiding
    - Intentional placement of data as such that it is not accessible to unauthorized users
    - Ex, within system, application cannot access particular data, it is Data Hiding
  - Encryption
    - Encrypt data so that it is not readable for unauthorized subject
    - More applicable for data in transit, however, equally useful for data at rest/storage
- Legally Defensible Security
  - For legal restitution, organization must b able to prove a "crime" and "subject's" identity
- Audit and Accountability Relation
  - Audit is collecting information and storing so that Accountability can be executed — Auditing not possible without Monitoring (monitors what is happening), Auditing keeping records of what happened
  - Accountability is to connect Identity/ Authentication with Human — Without strong authentication, accountability is difficult to materialized
- Related Concepts
  - I-dentification — Who you are? — Username/ID Cards example — It is Public
  - A-uthentication — Prove you are who you are! — Password/Pin/ Token — AU and IDEN are related, the way system identifies US
  - A-uthorization — Because we know who you are so you can do what we allow — Controls what "authenticated" identities can do. It is Granular
  - A-udit — We will keep check what you do
  - A-ccountability — You are accountable for what you do!
- CIA or AIC??
  - Military/Government — Prefer CIA
  - Private — May be CIA or AIC
  - OT Systems (SCADA/PLC) — AIC (Availability is important!)

Security & Risk Management

- Security Documentation
  - 1. Security Policy
    - Key Items
      - Types
        - Acceptable Use Policy
          - Acceptable behavior/use of resources by security role
        - Informative Policy
          - Provides strategic information (objectives, awareness knowledge
        - Advisory Policy (most policies are this!)
          - Advise to management about risk/threats and how to mitigate
        - Regulatory Policy
          - Address how any regulatory/ compliance requirements met
        - System Specific Policy
          - Focus on specific system
        - Issue Specifc
          - Policy focus on specific issue
        - Organizational Security Policy
          - Security Objectives focus on entire organization
      - Security Objective
        - Why we need security? What we want to achieve
      - Risks and Risk Management
        - What are risks? How big they are? What is impact
      - Senior Management Viewpoint
    - Step by step detailed instructions of implementation steps of particular (system specific/hardware specific) deployment
  - 2. Standards
    - Define usage guidelines, how to use, how to interpret the system, how baselines and standards are implemented, Can be modified with change/time
  - 3. Baseline
    - It's a baseline. Minimum security standard that must be met by all IT systems
    - Define standards so that homogenous approach can be taken for security implementation. Tactical Document/ Plan
  - 4. Guidelines
  - 5. Procedures
  - Recommendations for Security Documentation
    - 1. keep all documentation types separate, do not produce 1 document that covers all aspects
    - 2. benefit is it keeps focus on specific, easier to change later, easier to manage and distribute
- Due Diligence (Mgmt must show it)
  - Required efforts are put to sustain the successful operation of security solution to protect business
- Due Care (Mgmt must show it)
  - Making sure that required attention is given to enable Security Solution and practice Security Management to protect business
- Security Control Standard/ Framework
  - Method to map security solution to business needs
    - Mostly used standard is COBIT (Control Objective for Information and Related Technology)
      - E.g created Security Solutions framework
      - 5 key principles
        - Meet business needs
        - Cover end to end
        - Integrated Approach
        - Holistic Approach
        - Detach governance from management
- Information Security Roles
  - Senior Manager (SM)
    - Responsible for overall security implementation and protection of assets
      - Responsible for overall fail/success of security solution
      - Doesn't define security policy on its own, but endorse the policy (made by Board/Cheifs)
  - Information Security Officer/ Computer Incident Response Team (CIRT)
    - Implementers - they implement what is endorsed/dictated by SM
  - Data Owner
    - Senior Position who owns Data
      - Ultimately responsible for data protection
        - Example Registrar and student's data
  - Data Custodian
    - Who aims to protect data
      - Implementer for data owner
  - User/Operator
    - Who are allowed to use data under restricted guidelines
  - Auditors
    - Review security policy for check compliance/effectiveness and present report for senior manager
    - Need Users/operators so that they do activity for Auditors to audit
- Data Ownership (must be defined) – Data Owners
  - Information Systems (IT) Data
    - Administrator
      - If not Admin, then Subject who creates an Object
  - Physical and Intangible Data
    - Ownership difficult to define and manage – Owner is identified by organization
- Data Classification (con.. From right)
- Security Management Plans
  - Strategic Plans
    - 5 years/reviewed annually strategic plans defining security strategy
  - Tactical Plans
    - Under guideline from Strategy plans, mid term
      - Hiring Plans
      - Project Plans
      - Acquisition Plans
  - Operational Plans
    - Focused on implementation of specific task
      - System deployment plans
      - Resource Allocation Plans
  - Key Thoughts
    - They are on-going because security management is on-going
    - Plans should be made, deployed and maintained
- Organizational Process for optimized Security Management
  - Process when Acquisition and Divestiture happens
    - Acquisitions and Divestitures are high risk probability time - needs attention
  - Change Control Management
    - Primary Goal – to reduce impact of change on security
    - All changes can be rolled back
    - All changes can be tested and verified systematically after the change
    - All changes must be approved by Change Control/Advisory Board
    - No change should result in compromised or minimize security
  - Data Classification
    - Main Objective
      - Classify data based on "data classification factors" so that appropriate security solution be applied to protect data
    - Data Classification Factors
      - Data Sensitivity
      - Data required condifdentiality
      - Damage if data is accessible by unauthorized subject
      - Damage if data is revealed
      - Damage if data is modified
      - Data retention time (how old is data!)
      - So on...
    - Data Classification Method
      - Put classification label (explicit classification)
      - When data is behind a particular security solution, it is classified based on that solution (implicit/unsolicited classification)
    - Data Classification Steps
      - Identify who is data custodian? Ultimately responsible for data
      - Identify evaluation criteria for data (based on above mentioned)
      - Put label on data
      - Select Security Controls need to be applied
      - Identify declassification criteria (if data needs to be declassified later!
      - Run enterprise wise awareness campaign to let everyone know about classification/data importance
- Data Classification Categories
  - Basics
    - Classification based on damage if data is disclosed unauthorized
    - Do not reveal level of classification of data to unauthorized, this is violation
  - Military/ Government
    - Classified Data
      - Top Secret
        - Disclosure can cause grave damage to national security
      - Secret
        - Disclosure can cause critical damage to national security
      - Confidential
        - Disclosure can cause severe damage to National security
      - Sensitive But Unclassified (SBU)
        - Data For Office Use Only (FOUO), if disclosed, violate privacy rights of a person
      - Unclassified
        - Rest of data. After above
    - Unclassified Data
  - Enterprise/ Business
    - Confidential
      - Private (almost same as confidential, however, mostly use for personal data
    - Sensitive
      - Public (anything that does not come under any above)

Security & Risk Management

Risk Management applicable to Supply Chain

Factors

- Several suppliers/manufacturers are involved in producing final product and hence there is an inherent risk
- There is an inherent risk that comes with new company acquisition — Acquisitions and Mergers
- Must be trusted and authenticated — Suppliers
- Pose inherent risk — 3rd Party Contractors

How to manage this risk

- Try to mitigate any risk in product in the beginning of lifecycle before coming into production
- Visit On-Site of org/com to see how security is practiced
- Ask for their own Security Procedures/ Documentation/Policy review
- Involve 3rd party auditors to do unbiased auditing

Threat Modeling

Threat Reduction

Decomposition

Breakdown system into smaller domains to focus on sub-domains. Focus on 5 areas

- Locations/elements where trust is changing — Identify Trust Boundaries
- How traffic will flow — Data Flow Paths
- Places where external input is received — Input Points
- Meaning where higher privilege is required to execute certain operation — Point where privilege change is required
- As per policy and priority, what needs to be protected and how much? — Identify/clarify security objective
- Assign numbers 1 to 10 and find XxY = (Product)

Threat Prioritization

- Identify Threat Probability and Damage it can cause for every threat
  - Option-1: Probability x Damage
  - Option- 2 Assign Values
    - High (Immediate Attention
    - Medium (Attention but later)
    - Low (may be attention if cost/ expenditure allows)
  - Option-3 Follow DREAD Method
    - How much damage is possible with this threat? — D-amage
    - How feasible for attacker to reproduce this threat — R-eproductibility
    - Chance that this threat can be exploited — E-xploitation
    - How many users can be affected it is exploited — A-ffected Users
    - How hard it is for attacker to discover this vulnerability — Discoverability

Objectives

- Identify Threats
- Categorize Threats
- Analyze Threat
- Reduce/Mitigate Threat
- Prioritized Threats against assets so that protect the right assets

Approaches

- Proactive
  - Starts in product development phase
  - Produce better products in long run
  - Delays launch dates
  - Also called Defensive Approach
- Reactive
  - Starts when product is launched (either in test environment or general release
  - Add patches/updates to mitigate threat, at the loss of user-friendliness/functionality of product
  - Ethical Hacking/Fuzz testing etc are methods used in this approach to find threats
  - Also called Adversarial Approach

Threat Identification, 3 approaches

- Threats focusing on assets — What are the assets and what threats are targeting those assets
- Focusing on attackers — Who is the Attacker and what threat he can pose? — Disadvantage – new attackers can appear anytime
- Focusing on software — What are my softwares and what are the threats for that? — This is mostly for orga/bus that develops softwares

Threat Identification, another approach (by aim of attacker)

- Wants to make system disable/unuseable
- Wants to gain access to data
- Wants to corrupt data (integrity attack)

Threat Categorization (different models available)

- Microsoft model is STRIDE
  - S-poofing — Falsified identity and gain access
  - T-ampering — Modify/tamper data, integrity violation
  - R-epudiation — We cannot prove that identified attacker is “indeed” a attacker
  - I-nformation Disclosure — Disclose information to an unauthorized recepient
  - D-os Attack — Service disruption (temporary or permanent
  - E-levation of Privelege — Gain more than eligible access
- Process of Attack Simulation and Threat Analysis (PASTA) — This process is based on risk-centric. Assets with higher value/risk and protected first
- Trike — Trike is also risk based model. It provides methods to asses risk against assets and then derive a solution to mitigate those risks
- Vast — Threat Modeling concept based on Agile

Threat from Individuals

From individuals (disgruntled employee, 3rd party contractor also exist

Threat from Nature

Earthquake, hurricanes etc

Threat Analysis

Picture the threat and attack as a diagram

- Identify hardware/servers/applications
- Identify traffic flow
- Identify security boundaries
- Then identify what attacks are possible where and to whom so we can identify threats

Security & Risk Management

Risk Management

Basics

- Process by which risks analysis is conducted and risks are managed to reach "acceptable level"
- Risk is any threat that can result in data disclosure or affect any element of CIA
- IT Risks are not always from IT. It can be physical also!

Asset

- Anything of value to an org.
- Hardware/software/document/process/furniture, whatever!
- Monetary Value + Intangible value (reputation/ market name etc!

Asset Valuation

- Quantity an asset, value of asset

Vulnerability

- Weakness or absence of safeguard
- That can be exploited

Threat

- Occurrence of an event that can result in data loss or any attack on CIA of any nature

Threat Agent

- Element that when "acts", threat occurs
- Could intentional or accidental
- Humans

Exposure

- Damage that can happen if threat is materialized
- Worst that could happen!

Attack

- Execution of an action by Threat Agent

Breach

- Bypass of a system/infrastructure, but not yet exploited so attack is not initiated

Safeguard

- Security Control to minimize risk and mitigate threat

Risk

- Probability that "threat" can exploit "vulnerability" using "threat agent" and can initiate "attack" by bypassing or defeating "safeguard" that can result in comprising of an "asset" (in any form of CIA)

Threat x Vulnerability

- Threat can come from anywhere (IT threats can come for non-IT e.g physical damage to servers due to fire
- This constitutes basics for Risk Management
- Threat/vulnerability identification

Risk Analysis (RA)

Quantitative RA

- Identify Asset and determine Asset Value (AV
- Identify Threat to asset and determine Exposure Factor (EF)
- Determine loss if threat is realized once (Single Loss Expectancy SLE)
- Determine chance of occurrence of that threat realization (Annual Rate of Occurrence)
- Product SLE x ARO to get ALE (Annual Loss of Occurrence)
- Consider Safe Guard for each threat and how much will it cost to implement
- See change in ARO and ALE after Safe Guard
- Conduct Cost Benefit Analysis to see feasibility of Safe Guard

Cont...

Qualitative RA

To be discussed later (next page)

Security Governance (focus on 3rd Party Governance for this chap)

- Ultimate objective is risk reduction/mitigation/management
- Until documentation part is satisfactory, no moving fwd
- Documentation review is next step and very important (before any on-site assessment is started
- Reason to set right expectation between organization and vendor/3rd party
- Before auditing, security documentation/policies must be exchanged
- Can be carried out by Auditors (independent or chosen 3rd party
- Purpose is to mandate implementation/management of security to achieve business objective and ensure business continuity

Privacy Laws

- Several Laws (to be discussed later next chap.)
- Whatever privacy laws/rules are, must be captured in security policy and shared with individuals so that they know

Personnel Security

Basics

- Humans are the weakest link in security management
- Humans are also real threat as they can find ways to circumvent any security control
- Job Descriptions Plays v.important role in personnel security
- Job Description — Defines job responsibilities (what someone will do?
- Role Description — Defines output/objective of a particular position in organization
- Defining Job Role is 1st step in security management of personnel

Job Description (3 elements)

- Seperation of Duties
  - Tasks/work required is distributed among multiple
    - It prevents Collusion (deterrent to Collusion
    - Collusion is when 2 more workers perpetrate
  - Follow principle of Least Privelege
    - Only give access that is really required
- Job Responsibiities
  - Exact tasks that supposed to be done
  - Again, follow Principle of Least Privilege
- Job Rotation
  - Move personnel between roles/ jobs
    - Again, it is deterrent to collusion
    - Helpful to create a backup person
    - RISK is – Privilege Creep meaning employees keeps on getting privileges (Manager must check, withdraw what not required
    - Prevent privilege misuse as employees always remain out of comfort zone
- Finally – keep them updated (manager's task
  - Few Org must do it to comply ISO 27001

Candidate Screening/Hiring

- Screening related to sensitivity of a position. More screeninng if more sensitive
- Online/educational/ employment/etc checks

Employment Contracts

- Selected candidates signs Employ Contracts
- Employment Details + Acceptable Use/Violation Policy
- NDA and/or NCA (Non compete)

On-Going Review and Mandatory vacations

- Managers must review JDs/privileges on-going to avoid privilege creep
- Mandatory vacation gives time for employee audit in his absence

On Boarding

- Creating User Account in IAM (Identity and Access Management
- Employee introduction to new organization

Termination

- Do Not Inform/or get informed anytime sooner
  - Imposes great risk
- Disable IAM Access immediately at the same time or just before informing of termination
- Take all belongings back
- Escort employee outside the building
- It's a careful process, should be defined and followed
- During Exit Interview, review NDA and other obligations

Third Party Contracts/ Agreements

- For contractors/vendors/ consultants/service providers

SLAs

- Main objective is risk reduction when 3rd party is involved
- Clear documentation so that both parties are aware of expectations/deliverables
- Availability in %
- Downtime Duration
- Recovery Time
- Compensation if not compliant with anything

Compliance for Personnel

- Conditions/rules/actions to follow/to adhere
- If personnel is not compliance, it can affect organization as a whole (performance, external outlook)
- Personnel must be trained for compliance, only then they can be held accountable for not being compliant

Privacy (components/ statements

PII (Personally Identifiable Data

- Main Focus for "person" privacy (social security number/credit card number etc.)

Views

- For some, it is sensitive and must be protected
- For some, if person is using in public forum, then privacy cannot be justified

Security & Risk Management

Key Ingredients of selected countermeasure/safeguard

- Cost of implementation and sustain should be less than the value of asset trying to protect
- Cost should be less than derived benefit, ALE1-ALE2 > Safeguard cost
- Should increase cost for perpetrator such that it exceeds benefit that he/she will get from attack
- Should be exposable/publicable meaning should not offer “security through obscurity”
- Should be tamper proof and provide consistent protection across all platforms (homogenous approach)
- Should be operational with minimal human intervention

Classification of Security Controls

- Administrative Controls — Policies, Procedures, Background Checks, Mentoring, awareness training etc
- Technical/Logical controls — Hardware (routers, IPS, IDS, Firewalls), software (ACLs, AAA implementation
- Physical Controls — Guards, cameras, fencing, access cards etc

Based on what action implemented security control would do, what will it achieve, hence “same control” can be in more than 1 type

Types of controls

- Deterrent — Warning signs, fence, login banner, security guards — Discourage attacker to initiate attack
- Preventive — Routers, firewalls, security guards, fence — Actually prevent attacker from attack
- Detective — IDSs, video recording from camera, activity logs etc — Detect what went wrong after attack. They only “detect”, does not correct
- Compensating — Encryption of PII data while in server is “preventive”, however it is clear text while in transit, so “compensating” control will encrypt PII also in transit — Supports/add/compensate to existing control to achieve its objective
- Corrective — Backup config, retrieval of backup data etc — Correct/normalize after threat is realized
- Recovery — DR/redundant sites (in BCP), server imaging etc — Enhanced form of corrective, after threat is realized, it will recover the environment back
- Directive — Exit directions, warning signs, meeting point, fire instructions — Persuades/guides/direct subject to execute in a particular way to compliance with security

Security Control Assessment and Monitoring/Measurement

Controls are assessed to calculate their effectiveness

- Can be done only if controls are properly monitored and have tools to be measured
- That can then report on security improvement or degradation based on monitoring
- Baseline must be known for comparison analysis be done (before and after)
- Effectiveness of control may noy always be quantified – it can be qualitative also (example increased productivity
- NIST has a guideline 800-53A (For Assessing Security Controls for Federal Information Systems

Asset Valuation

Quantitative + Qualtitative — Process to put $ to an asset

What can be considered as asset value

- Development Cost
- Acquiring Cost
- Maintenance Cost
- Value to competition
- Intellectual Property

Annual SG Cost < ALE of an asset (feasibility check

Risk Reporting

Essential part of Risk Analysis

- Reporting of risk to higher management
- Clearly outline cost-benefit analysis
- It is continuous process (yearly)

New Topic

Continuous Improvement

Risk analysis/reporting is on-going coz threats/vul are on-going
Needs continuous imporvements/check

Risk Analysis (cont…)

Exposure Factor (EF) — Expressed in % — % loss of Asset Value AV if risk is materialized

- SLE — Expressed in $ — AV x EF
- ARO — Annual Rate of Occurrence (a number,value) — Depends upon factors (e.g) may be a particular threat x number of threat agents that can attack
- ALE — Expressed in $ — ARO x SLE

Safe Guard (SG) — Annual Cost to implement Safe Guard (value in $) — Cost of deployment + hardware + maintenance (these are quantifiable — Qualitative (damage to environment) not very imp to consider

A catch! — SG may not minimize EF (coz EF is loss “if” risk is realized, so may be SG is not able to stop realization of risk so EF remains same, however, SG reduced ARO which then reduces ALE

Find ALE after SG implementation

Finally COST Benefit Analysis — ALE before SG – ALE after SG – ACS (Annual cost of safe guard) — If +ve, SG is good to implement, if -ve no benefit of implementing SG

Above is pure “quantify/numbers etc.”, we must consider Qualitative as well to reach final decision

It is guiding factor to tell us which Safeguard is better to implement to manage which risk, but that is not the “only” factor, other factors (compatibility of proposed SG with existing infrastructure, for e.g)

Qualitative Risk Analysis

Can employ different methods

- Brainstorming
- Survey
- Questionnaire
- Delphi Technique — Reaching anonymous consensus about threat/ safeguards using anonymous feedback

Main Concept — Get opinion about threats and respective safeguards to align of effectiveness on every SG against every threat against every asset

Hybrid Analysis

Combining Quantitative and Qualitative to produce final face of Risk Analysis is called Hybrid Analysis technique

Risk Response

Once Risk Analysis is completed, next step is to “response” to that risk

- Mitigation/ Reduction — SG is implemented and risk is mitigated/reduced — **Remember**! Risk Mitigation is process of Risk Management which is after Risk Analysis
- Avoidance — Implemented an action through which risk is avoided — Example, FTP is removed from server to avoid FTP based attacks. SG is not implemented, rather an action is taken to avoid risk
- Deterrent — Controls are put in place to deter the risk — Example, implement security cameras/security guards
- Transfer or Assign — Expected loss from risk is transferred to other “entity”, e.g is taking insurance
- Accept — Risk is accepted, e.g cost of SG is more than ALE so SG is not implemented — Needs management approval and sign-off by Authority to accept that risk is indeed accepted
- Rejection — Risk is rejected meaning “assuming” that risk will never materialized and hence no SG is implemented and no action is taken. Not an acceptable response

Finally! Risk response or risk management is on-going process and should be continued through life cycle of security management

Residual Risk

Remaining risk after implementation of Safe Guard

Controls Gap

- It is Total Risk – Controls Gap = Residual Risk
- It is risk reduced after implementation of Safeguard

Total Risk

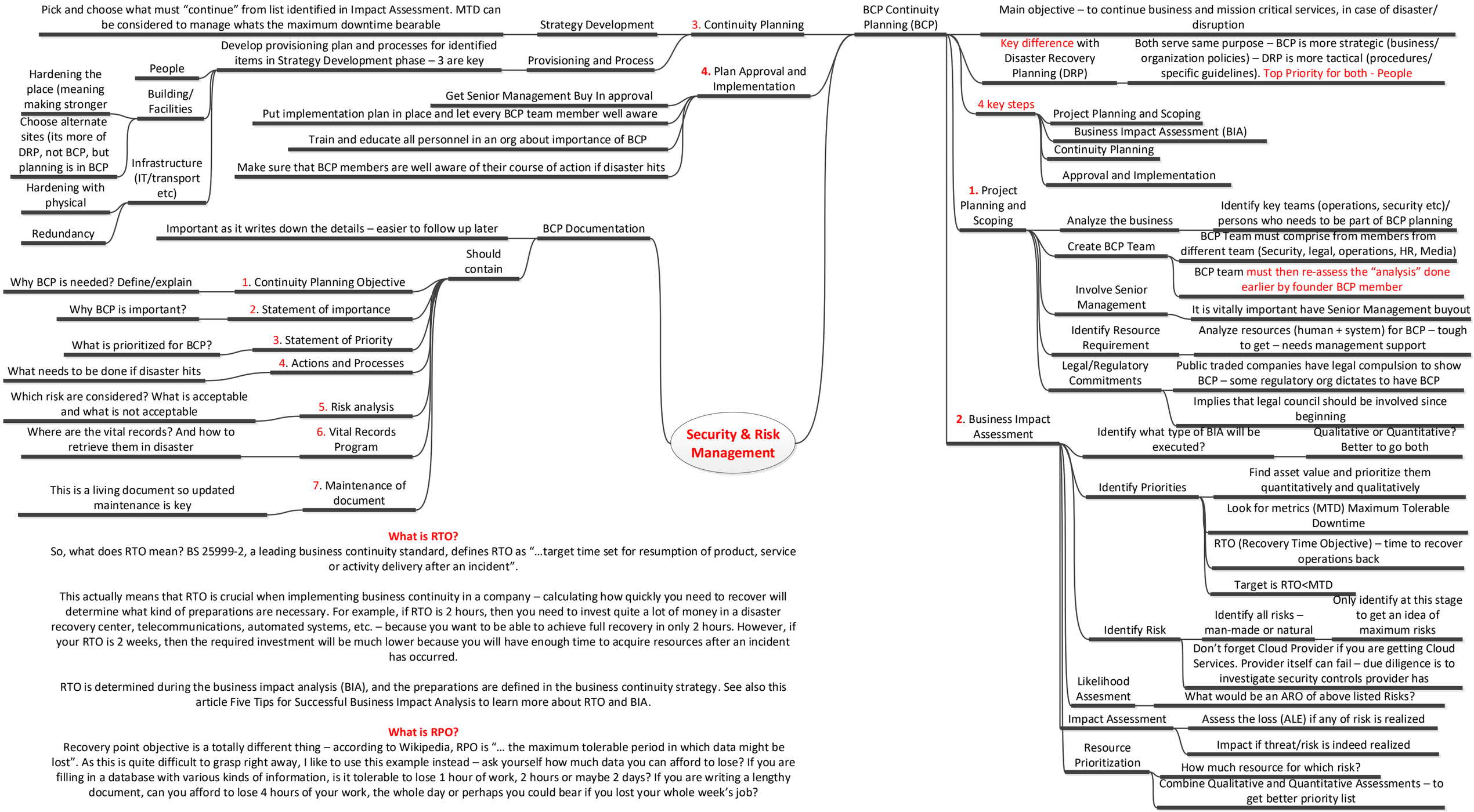
Product of Threat x Vulnerability x Asset Value

Above is not pure mathematical formula, rather showing relationship

Characteristic	Qualitative	Quantitative
Employs complex functions	No	Yes
Uses cost/benefit analysis	No	Yes
Results in specific values	No	Yes
Requires guesswork	Yes	No
Supports automation	No	Yes
Involves a high volume of information	No	Yes
Is objective	No	Yes
Uses opinions	Yes	No
Requires significant time and effort	No	Yes
Offers useful and meaningful results	Yes	Yes

Security & Risk Management

- Management of Security Function
  - Basic objective of Security Function management is to keep security system as per defined business objectives
  - Meaning security implementations
    - Must reap benefits
    - Must be measureable
    - If risk management, then control should reduce risk/reduce attacks/thwart attempts
    - Must be effective in its objective to achieve
    - Must be flexible to cope with advancements
    - Must be economical and withing budget
    - Must be long term and sustainable
- Risk Management Framework (RMF)
  - Basics
    - Risk Framework is about
      - How risk is assesed
      - How it is resolved
      - How risk is then monitored
    - Most popular and focus of CISSP, NIST RMF 800-37
  - NIST RMF 800-37
    - 6 principles
    - 1. Categorize asset/information systems “system”
      - Based on risk assessment
    - 2. Select appropriate security control
      - What to implement to mitigate/reduce
    - 3. Implement the security control
      - Implement what is selected
    - 4. Assess the control
      - Assess and evaluate the method that is implemented
    - 5. Authorize the control to be in use
      - If assessment is fine, authorize control to be in production
    - 6. Monitor
      - Monitor the control
- Training, Education and Awareness
  - Is an essential part to create “security” awareness
  - Users need to be trained so that all are on same page in understanding important of security function
  - Training needs to be updated to keep it fresh
  - Awareness
    - Through many ways posters, t-shirts, knowledge of security guidelines/ principles, emails, brochures
  - Education
    - More formal and detailed than Training
      - For professionals in organization who seek to become security personel



What is RTO?

So, what does RTO mean? BS 25999-2, a leading business continuity standard, defines RTO as "…target time set for resumption of product, service or activity delivery after an incident".

This actually means that RTO is crucial when implementing business continuity in a company – calculating how quickly you need to recover will determine what kind of preparations are necessary. For example, if RTO is 2 hours, then you need to invest quite a lot of money in a disaster recovery center, telecommunications, automated systems, etc. – because you want to be able to achieve full recovery in only 2 hours. However, if your RTO is 2 weeks, then the required investment will be much lower because you will have enough time to acquire resources after an incident has occurred.

RTO is determined during the business impact analysis (BIA), and the preparations are defined in the business continuity strategy. See also this article Five Tips for Successful Business Impact Analysis to learn more about RTO and BIA.

What is RPO?

Recovery point objective is a totally different thing – according to Wikipedia, RPO is "… the maximum tolerable period in which data might be lost". As this is quite difficult to grasp right away, I like to use this example instead – ask yourself how much data you can afford to lose? If you are filling in a database with various kinds of information, is it tolerable to lose 1 hour of work, 2 hours or maybe 2 days? If you are writing a lengthy document, can you afford to lose 4 hours of your work, the whole day or perhaps you could bear if you lost your whole week's job?

This number of hours or days is the RPO. Recovery Point Objective is crucial for determining one element of business continuity strategy – the frequency of backup. If your RPO is 4 hours, then you need to perform backup at least every 4 hours; every 24 hours would put you in a big danger, but if you do it every 1 hour, it might cost you too much.

Security & Risk Management

Trademarks

- Trademark should not be descriptive of products that company sells
- Trademark should not be confusing with others
- Reg done for 10 years (extendable unlimited time multiple 10 yrs
- To register, 2 key req.
  - Once registered, then formally protected. Use “R”!
  - Legally protected once started using, not necessarily required to be registered. Use “TM”!
- Recognize your organization

Copyright

- Copies are destroyed as soon as objective is achieved
- Copies are made for acceptable use (system backup)
- Copy of copyright material is allowed IF
- No copies of work are held by ISP for unreasonable duration
- Data transmission is automatic (routing/switching etc.)
- Data is not modified in transit through ISP
- Make liability of ISP limited in case of copyright violation by someone IF;
- Punishment for anyone tries to circumvent copyright protected material
- Up to $1million/10 years prison
- Digital Millennium Copyright Act (3 key provisions)
- Enacted 1998
- When the original work is created, it is under “copyright” protection legally immediately, registration with government is only a formalization of this
- Protects legally rights of original creator of creative work
- Literature, architecture design, audio/video, sound, music, sculpture etc.
- Provides protection for 70 years after the death of creator/last creator if group. For work for hire/ anonymous, 95 yrs from date of publication or 120 yrs from date of creation

Federal Sentencing Guidelines

- Enacted in 1991
- Issued to assist judges to give fair punishments
- 3 guidelines
  - Prudent Man Rule – executive must act as Prudent as any sensible person would act
  - Person will be held responsible if he was legally given that task to be held accountable for certain job/task
  - 3 reasonable proofs be provided to held any person responsible/ accountable for misconduct

Intellectual Property - 4 types

- Copyright
- Trademark
- Patent
- Trade Secret

6.Federal Information System Modernization Act(FISMA)

- Yes this is also called FISMA!
- Enacted in 2014 to modernize 2002 FIMSA!
- Key – assign Department of Homeland Security to take responsi of cyber security for all Federal Institutes (except 2)
  - Defense (goes to Sec of Defense
  - Intelligence (goes to Director of Intelligence)
- Assign NIST responsibility to develop nationwide cyber security standards. 3 are key
  - 800-53 (Security and Privacy Controls for Federal systems
  - 800-171 (Policy for managing unclassified information by non-federal agencies
  - NIST Cyber Security Framework
  - Must compliance for fed contractors
- Give responsibility to Dept of Homeland Security to establish National Cybersecurity Integration and Communication Center, why?
  - To bridge between federal organiz and civil institutes for cyber security related
- Also added Cybersecurity Enhancement Act
- Also Added National Cybersecurity Protection Act

Classification of laws

- Criminal Law
  - Federal Laws and State Lawsl
    - Federal Law applies Inter state, out of state boundaries or directly related to federal organiza
  - Murder, theft etc (some also deals with computer crime
  - Government fully involves (law enforcement agencies get involve)
- Civil Law
  - Federal and State laws
  - Government only provides administrative assistance, unless requires by court
  - Contract/employment disputes etc
- Administrative Law
  - Law governs Federal Agencies in US that work under government
  - Also helps to implement Criminal and Civil laws

Common with all laws

- Must be passed by Senate and House of Representatives to get implemented
- Operate under US Constitution and Unite States Code (USC)
- Go through Judicial review and Judiciary can override law if deemed necessary

Computer Protection Laws

- 1. CCCA (Comprehensive Crime Control Act)
  - Initiated 1984
  - Had some legislations (high level) for computer crime
  - Focused on crimes directed to Federal computers
- 2. CFAA (Computer Fraud and Abuse Act
  - Initiated 1986
  - First major legislation that covers Computer Crimes
  - Expands on CCCA
  - Instead of only Federal Computers, it covers “federal interest” computers – banks, financial institutions etc and any US government
  - Treated as harsh law because it insist to even follow website policies
- 3. Computer Abuse Amendment Act (CAAA)
  - Initiated in 1994
  - Amendment to CFAA
  - Allows imprisonment of offenders
  - Broaden the scope by including any computer
  - Outlaw creation of any malicious code
  - Computers used in Inter-State commerce
- 4. National Information Infrastructure Protection Act
  - Enacted in 1996
  - Amendment to CFAA
  - 3 key additions
    - Computers used in International Commerce
    - Infrastructure such as rail roads, telecom circuits, gas pipelines includes in protection act
    - Any misuse with national infrastructure treated as felony
- 5. Federal Information Security Management Act(FISMA)
  - Enacted in 2002
  - Security management guidelines for Federal Agencies + Contractors
  - Guidelines developed by NIST
    - Have risk assessment and risk management policies/ procedures
    - Security implementation process/proced for federal systems
    - Education/awareness training for emply+contrac
    - Periodic assessment and validation of policies
    - Lifecycle management of security solution/ implementation

38. C. The Code of Federal Regulations (CFR) contains the text of all administrative laws promulgated by federal agencies. The United States Code contains criminal and civil law. Supreme Court rulings contain interpretations of law and are not laws themselves. The Compendium of Laws does not exist.

Security & Risk Management

Privacy

4th Amendment of US Constitution
- Key objective is to protect people/and their houses to be searched by government/agencies without proper warrant

Privacy Act of 1974
- 1st legislation that dealt with personal privacy in detail
- It only applies to Government Agencies
- It legislates that government agencies cannot share the private information of individuals with any other entity with prior written consent AND agencies must protect private data AND destroy data once not required

Electronic Communications Privacy Act (ECPA)
- Enacted in 1986
- It protects privacy for any electronic communications (email/ voicemail/even mobile calls)

Communications Assistance for Law Enforcement Act
- Enacted in 1994
- It actually modifies ECPA of 1986 by allowing to wiretap any electronic communications if court order are issues to assist Law Enforcement

Health Information Portability and Accountability Act (1996)
- Enacted in 1996
- Strict legislation for Health and Insurance providers
- 2 are key
  - 1. Security for physicians/hospitals/ insurance companies as per standard
  - 2. Rights of insurance holders made very clear and order the providers to provide/ display those rights in writing to them

Health Information Technology for Economic and Clinical Health ACT (2009)
- Enacted in 2009
- It modifies/adds HIPAA of 1996
- 2 key modifications
  - 1. Business Associates (3rd party that provides services to Insurance Providers and deals with health data) must sign business agreement with the Provider-then all HIPAA regulations be applicable on Business Associate also
  - 2. if any data breach happens to HIPAA covered entity, then those affected must be informed

Children Online Privacy Protection Act (1998)
- Enacted 1998
- Effective from 2000
- 3 key provisions
  - 1. Websites give clear notice before collecting any info from children and where this info be used?
  - 2. Parents must have access to that collected info and that can be deleted when required
  - 3. Parents must give verifiable consent to collect info for children younger than 13 yrs

Gramm Leach Bliley Act 1999
- Enacted 1999
- Focused on financial institutions
- main provisions
  - Restriction between companies (even subsidiaries) the information they can share between each other of their subscribers, focused on financial institutes/banks etc.
  - Financial institutions should provide in written their privacy policies to their customers

USA PATRIOT Act 2001
- In response to 2001 Attacks, changes legislation for privacy
- 3 main provisions
  - One blanket license to wiretap a person, rather than 1 specific one for every communication
  - ISPs allowed to share user info/activities under subponea
  - Further expand CFAA act by providing sentence up to 20 yrs for computer abuse
- Trivia: USA PATRIOT act expires in 2015-Then another US Freedom Act enacted June 2015 also expiring in Dec 2019

Identity Theft and Assumption Deterrence Act
- 1 Key provision- 15 yrs prison or $250K fine for any one who theft identity of anyone for defraud
- Enacted in 1998

Family Educational Rights and Privacy Act
- Enacted in 1974
- Valid for schools that receives federal grant
- 3 main provisions
  - 1. Students/parents can inquire what info is saved about them by school
  - 2. That information can be corrected, if errnoeus
  - 3. School cant share that info with anyone, few exceptions

Patents
- Protect inventors inventions
- For registration of patents, 3 key req;
  - Invention must be original
  - Invention must be useable
  - Invention must not be obvious,it must be orignally thought and created
- Registered for 20 years and cant be extended
  - After 20 years, it loses "exclusivity" status

Trade Secrets
- Secrets of your business that is utterly important for business survival
- In fact, legal advise to protect trade secret is "not to register with anyone", keep it with you ONLY!
- Copyright and Patents does not provide required "trade secrecy" because
  - You have to announce your creation/invention publicly
  - They expire after "certain" time
- Economic Espionage Act of 1996
  - Enacted in 1996
  - Key objective – to protect trade secrets leakage
  - If trade secret is stolen and shared with foreign government – 15 yrs + $0.5m fine
  - If trade secret is stolen for any other reason – 10 yrs + $0.25m fine
  - This relates to Privacy! It extends definition of "property" to add "proprietary economic information" such as bank account. So any theft with that is then crime!

Software Licensing
- 4 types
  - 1. Contractual – Written agreement b/w software manufacturer and user – mostly for high end sophisticated software
  - 2. Shrink Wrap – Licensing T&Cs mentioned on the wrap – you accept as you tear off the wrap
  - 3. Click Through – Tc&Cs must be accepted when you install on machine and click to accept
  - 4. Cloud Services – Ts&Cs mentioned when accessing cloud services and click on radio button accept
    - Caution! Read before accept specifically if for on behalf of organization

Import/Export
- To regulate export/ import of computer/ security products
- **2** sets of regulations are key
  - ITAR – International Traffic in Arm Regulations
    - Regulate items specifically related to military
  - EAR – Export Administration Regulation
    - Regulate other commerce items (most security related items here)
    - Managed by Department of Commerce
    - Itemized list called Commerce Control List
- Regulations about Computer and Encryption Export
  - High End computer export is okay (except banned countries)
  - Encryption software are okay, if software's are reviewed by Department of commerce and get approval

Security & Risk Management

Compliance

- Basics: Meeting required regulatory requirement for Information technology
- Example is PCI-DSS
  - Payment Card Industry – data Security standard
  - Some key requirements by PCI-DSS that is required by regulatory to be compliant
    - 1. Have firewall to keep credit card info safe
    - 2. protect data from physical access
    - 3. encrypt data if going to public
    - 4. malware/patchware/anti-virus are updated
  - Above and more is regulatory requirement that is contractually binding card information holder and processor and user
- Basics are
  - Regulatory can ask organz to provide audit report for compliance
  - Organiz may do 3rd party audit or internal audit, but must do!

Security/Privacy concerns for Procurement/Contracting

- Appear because many org use 3rd party for contract/ procurement
  - Things to consider are; what security standard contractors/procurement have?
  - Details about security controls
  - If encryption is used, what are the protocols
  - If they have own 3rd party, how is that managed?

Privacy

- Expected privacy in an office environment
  - If employers communication equipment is used by employee for personal use and employer have notified through email/contract/ banners, then privacy should not be expected by employee
- European Union Privacy Law
  - Passed 1995
  - But enacted in 1998
  - Personal Data processing meets one of it
    - Consent
    - Contract
    - Legal Obligation
    - Interest of data subject
    - Balanced interest of data holder and data subject
  - Privacy Shield Protection Agreement b/w EU and US
    - If data goes out of EU then needs to be protected under Privacy Law b/w EU and US and must obliged with 7 conditions, if companies like to be protected under Privacy Shield Protetion
    - 1. Informs data owner about their rights
    - 2. Dispute Resolution in case of dispute
    - 3. cooperate with dept of commerce
    - 4. Maintain data integrity
    - 5. if data be shared with 3rd party, commit same level on integrity
    - 6. Public any assessment in case if compliance with Privacy Shield is broken
    - 7. keep the compliance even if not operating under Privacy Shield if data is still possessed and assessed
- European Union General Data Protection Regulation (GDPR)
  - Formulated in 2016
  - Enacted in 2018
  - Extend scope of earlier EU Privacy Law, adds all organizations (national/ international) until they have data from EU resident
  - 5 key provisions
    - 1. every EU state have central data protection/ processing authority
    - 2. Personals have access to their data
    - 3 Data portability, data share b/w organizations at data owner consent/ request
    - 4. Data breach notification to authorities in 72 hrs
    - 5. “right to be forgotten”, forget the data/destroy once use/purpose is completed

Asset Identification and Security

A Service Organization Control 1, or SOC 1 engagement, is an audit of the internal controls at a service organization which have been implemented to protect client data. A SOC 1 assessment is comprised of control objectives, which are used to accurately represent internal control over financial reporting (ICFR). In other words, if you are hosting financial information that could affect your client's financial reporting, then a SOC 1 audit report makes the most sense for your organization to pursue, and will likely be requested of you.

If you are hosting or processing other types of information for your clients that does not impact their financial reporting, then you may be asked for a SOC 2 audit report. In this instance, your clients are likely concerned whether you are handling their data in a secure way, and if it is available to them in the way you have contracted it to be. A SOC 2 report, similar to a SOC 1 report, evaluates internal controls, policies, and procedures. However, the difference is that a SOC 2 reports on controls that directly relate to the security, availability, processing integrity, confidentiality, and privacy at a service organization. These criteria are known as the Trust Services Principles, and are the foundation of any SOC 2 audit engagement.

Handling Data and Assets

Data States and Protection

- Data at Rest: Data saved in a hardware/USB/media
- Data in Transit: Handed off by media and transported into network
- Data in Use: Received by application and currently in a temporary memory (RAM) so that application can use it
- Example:
  1. Credit card info is saved in database server (at rest, encrypted)
  2. Web application requests that data to be used, server will encrypt data for transportation and send to application (data in transit/motion)
  3. Application will decrypt data and while in use, keep in temporary memory (data in use), after destroy data so that no residual remains

Mark data/asset properly

- Physical marking like storage disks/printed docs with label
- Computer/system marking like banner on screen/tag on computer
- Example, organizations buy Red USB drives to save sensitive data. Then assign Unique Identification Code to these drives for better recognition, DLP software then identifies these USBs and encrypt data properly
- In case if "marking" is to be downgraded for an asset, then recommended practice is to destroy, rather than downgrading. If downgrading is essential, then strict process be in place
- Same applies to computer that process "confidential" data, rather than sanitizing computer, better to destroy

Handling Sensitive Information

- Sensitive info must be handled as it "deserved", with attention, don't take for granted
- Specifically backup data tapes. Backup tapes are as important as data if tapes are backing up Sensitive Data

Storing sensitive data

- Data at rest scenario-store data with AES256 encryption
- Physical tapes (USB/media) must have strong physical security
- Physical media on which sensitive data is stored, should be of high quality (protect from light/humidity)

Destroying Sensitive Data

- Destroying sen data is as important as protecting data!
- Strict guidelines to follow, if to be destroyed, do it properly, if media to be kept, sanitize properly
- NIST 800-88 r1(revision1) Data Sanitization Guideline

Removing Data Remanence

- From Magnetic Media (CDs/floppytapes)
  - Degaussing is the method that realigns magnetic field and any data remanence is destroyed
- From SSD Media (SSD drive)
  - Degauss doesn't work here coz data is in integrated circuits, not magnet, best way is to completely destroy using Security Agency recommended method
  - Simply execute "delete" operation
    - Only removes link to data/folder/file
    - So essentially overrides bits and bytes on top of original data
      - Doesn't actually remove "bits & bytes" of data on a drive, data can be retrieved
      - Limitation is doesn't override certain sectors of hard drive
  - Fills unclassified data's bits and bytes into media
    - Advanced form of Clearing
      - Runs "clearing" multiple times
      - Only works on Magnetic Media
        - Doesn't work on Optical Media
        - Combine it with degaussing, Still not recommended for top secret data, though it gives confidence that data is not recoverable using any known methods

Data Destruction Methods

1. Erasing
2. Clearing
3. Purging
4. Degaussing
5. Destruction
   - This is physical disintegraion/destruction
     - This is recommended for Top Secret Data

Identity and Classify Assets

- Baseline: Assets identification, then classification, then protection/security
- Baseline: Identification (done during Security Policy development),then labels are assigned based on that identification/classification
- Baseline: Asset is
  1. Information
  2. Media where information is stored
  3. Machine that processes the information

Data Identification

1. Sensitive Data
   - Any data that is not public OR that is not classified
2. Personally Identifiable Information(PII)
   - Any info that can identify a person
   - Social Security Number/Passport/ ID
   - Or that can link to a person
   - E.g Employment history
3. Protected Health Information (PHI)
   - Collected by hospitals/insurers/school etc.
   - Any info related to health
   - Past and Present, historical info
4. Proprietary Data
   - Any info that can harm organization if leaked (trade secrets, intellectual property/process etc
   - Always remain under threat by competitors
   - Example APT-1 (Advanced Persistence Threat-1)
     - Chinese group identified as threat
   - Example APT-28 and 29, Russian group

Data Classification

- Military
  - Classified
    - Top Secret: Can cause grave damage if leaked
    - Secret: Can cause severe damage
    - Confidential: Can cause noticeable damage
  - Unclassified
    - FOUO (For office use only)
    - Sensitive but unclassified
- Private: Though not standard, but classification can be done as below, objective is whatever seems okay, but classification if necessary
  - Confidential: Leak of this can cause grave damage to organization
  - Private: It should also not leak out
  - Sensitive: Confidentiality of this data is also necessary
  - Public

Key Point: For CISSP, any data that is not classified or that is not public, is "sensitive" and its protection is important

Remember data is also asset, hardware that stores or process data is also "asset". Asset classification should match data classification. We cant expect "top secret" data to be stored on "unclassified hardware"

Asset Classification

Data Security Controls

Now as data is "identified" and "classified", it needs to be "protected" as per classification

- Example "email" protection requirement as detailed in "security policy"
  - Confidential emails (e.g)
    - AES 256 encrypted (emails + attachments)
    - Only allowed to internal recepients
  - Private Emails (e.g)
    - Cant be printed
- Security controls (as chosen by Security Managers) need to satisfy this requirement (key is AES 256)

Note: Data Loss Prevention software identify data (email), user can apply classification label, software then apply required security protection

Media Declassification Rule

Media that was previously used for classified data, is now requited to be used in unclassified environment

Efforts require to make this media "clean" worth more than buy new media

Recommended is to destroy completely, use new

Asset Identification and Security

Data Processors

- As per GDPR (EU), data processor is an entity that processes data on behalf of data controller
- Example, org that collects personal data of employees for payroll (data controller) and 3rd party processes that data (data processor)
- In US-EU context, org must comply with Privacy Shield if would like to do business between US-EU
- US Companies can comply for privacy shield with US Dept of Commer by filling in self-filled detailed questionnaire

Compliance Points (repeating)

1. Collect personal data only for specific purpose
2. Protect data
3. Provide access to that data to personnel
4. If shared with 3rd party, they also compliance with protection and security

Manipulating Data

- 2 security controls that are effective in data security are “encryption” and “data coding/or manipulation”
- Data Coding is like replacing data with something that makes data incomprehensible/unintelligible

Pseudonymization

- You take data and assign a “dummy label” to it, like medical record of Haseeb as “123456", like coding to make PII identifiable more difficult
- So real data is saved somewhere else and shown is pseudocodes

Anonymization or Masking

- Another technique of data coding
- Say Data is dispersed in different sheets/columns/databases and they are mixed or masked
- Original Data remains same, but what exposed is masked data, that is unintelligible & hence cannot be retrieved back to original by hacker/ attacker

Both these techniques help to minimize more stringent requirements of GDPR data protection as real data is not exposed, still encryption is better option

Few more roles

They manage access to data, assign privileges for users to access data. Do it as “principle of lease privilege”

- Administrators
- Data Owners assign responsibility to Custodian to manage day-to-day data operations, like making sure data security/taking backups
- Custodian
- End User who access data to perform their daily tasks
- Users

Protecting Privacy

- For org, it is mandatory to protect privacy by many laws
- Laws such as GDPR, Privacy laws in California etc
- It is the responsibility of org to know and to adhere to all applicable Privacy Laws
- Personal information collection should only be for specific reason and collected info should only be used for that purpose and must not be shared with any other entity unless permitted by that person

Security Baseline

- Minimum security level that every system is supposed to have in an org
- One way to implement is to do “imaging” meaning that prepare one system as baseline security and then copy that to all systems
- NIST 800-53 doc has guidelines for baseline security to adopt
- Security controls are deployed to achieve baseline security. These controls are like low-impact, medium-impact or high-impact based on the impact that any risk can have on the system and choose controls accordingly

Tailoring and Scoping

- Scoping means that look at list of baseline security controls and see what applies in your case
- Tailoring means that tailor a specific control so that it can be applicable as baseline for the systems

Selecting controls that adhere to Baseline

- While implementing baseline, org need to comply with external security standards e.g payment card processing org must comply with PCI DSS
- So choose controls that are applicable for those standards need to be adhered by org

Data Encryption Standards

- Categorized as encryption for data at rest and for data in transit
- Data at rest can use Symmetric Encryption
  - Require same key to encrypt and decrypt
- AES/DES/3DES/Blowfish examples of symmetric encry
- AES uses 128/192/256 bits
  - DES uses 56 bits, 3DES uses 56/112/168 bits
- NIST recommended AES 256 as standard even to encrypt confidential data
- 3DES is used by Master Card for eg for payments + with PIN
- Blowfish is also sym encr, used by Linux, uses 32 to 448 bits

Data in Transit Security

- Web Transport
  - HTTPS is transport (underline TLS 1.1 is encryption) for web
  - Predecessor was SSL developed by NetScape. TLS standardized by IETF
- VPN Transport
  - IP Sec and TLS
  - IP Sec uses AH (for authen + integrity) and ESP (for confidentiality)
- Internal Network
  - IPSec and SSH
  - SFTP and SCP (Secure Copy) for encrypted file transfer
  - SSH for Device Management

Asset Retention

Requirement to retain asset until require

- Media refresh need to happen (3 to 5 years) so this be considered while planning retention
- But define retention time, else security professional either destroy data before time or keep data after time
- Asset retention time dictated by either regulatory/business/enterprise/law
- Asset is “data” or “media”

Determining Ownership

Data Owners

Typically holds full responsibility of data

- Typically they are CEOs/Department Head (DH)
- NIST 800-18 has Data Owner tasks
  - 1. define who can access data?
  - 2. once accessed, how data can be used (AUP) Acceptable Use Policy
  - 3. Define/explains how to protect data? Like security controls etc.

System Owners

Also called Asset Owners

- They are called “asset owners” because they actually own system that has “data” so in essence system + data = asset

NIST 800-18 here also

1. Make sure required security controls in place
2. Users of data are well informed of usage guidelines of data
3. Security controls are updated
4. data processed on the system remains secure

NOTE: Data Owners and Asset Owner are typically same, but not necessary

Business Owner/ Mission Owners

- Those that owns a complete process which utilizes data + system
  - Like “Sales”
- Example company that sells on a web – data in this case is whole sales inventory with pricing – system owner is may be IT/database team, business owners is sales team who actually uses this whole chain to generate revenue

Security Architecture

Mathematics in Cryptography

- Mathematics is key to cryptography and specifically Binary
- 1 is Current ON, 0 is Current OFF
- 1 is TRUE and 0 is FALSE
- OR Function
  - Output = TRUE, only if at least 1 bit is TRUE
- AND Function
  - Output = TRUE, only if BOTH bits are TRUE
- NOT Function
  - Inverse the bit
- XOR Function
  - Output = TRUE, only if only 1 bit is TRUE
- Modulo Function
  - Tells "Remainder"
  - 10 mod 2 = 0
  - 10 mod 3 = 1
- One Way Function
  - Inputs are defined and output is achieved, however, reverse engineering output to get back to inputs not possible
  - Example input are 3 prime numbers, each 5 digit that gives product of "10718488075259"! How can we find those 3 number? Difficult!
- Nonce
  - Nonce is randomly generated number that acts like "place holder"
  - That place holder can be used for a function to produce a output
  - Example is IV (initialization vector), random bit string that is generated each time, when unique cipher text is required to be created. IV is XORed with real data and produce cipher text. Every time unique IV is generated so IV here is Nonce
- Zero Knowledge Proof or Zero Knowledge Protocol
  - In cryptography, it is the method or process to prove to verifier a knowledge of something without disclosing knowledge itself
  - Example prover has a "password" and it can prove to verifier that I have a password without revealing that password to prover e.g on page 379 is good!
- Split Knowledge concept
  - Concept that defines in order to gain access to authorized/secret database, more than one users/credentials are required
  - Best example is Key Escrow, account where encrypted keys, digital certificates, digital signatures are saved and if access is required to that then M of N controls are required, meaning 2 of 5 (example) users/agents/ identifies are required. M is either < or = to N

Work Function in Cryptography

- A function to determine strength of cryptographic system
- Determines work (time & effort) required to break/brute force a certain cryptographic system
- Output of work function need to be slightly higher than value of asset we are trying to protect. Its like not too much and not too less (one is waste and other is risk!)

Code & Ciphers

- Thought used interchangeably – Code and Ciphers are different
- Code
  - May not always hide a message, example, SOS is a code that means save us from distress, that's a code, but it is know publicly
  - Codes work on words and phrases (eagle has arrived) eagle may mean enemy that is only understood by sender and receiver
- ciphers
  - Ciphers on other hand always meant to hide a real message/data
  - Ciphers works on individual bits and characters
  - Bit Basis – meaning cipher every single bit
  - Character Basis – meaning cipher every character
  - Block basis – meaning a segment of the message ciphered in bits

Types of Ciphers

- Transposition Ciphers
  - Ciphers that transpose characters of a message in another format based on secret key that defines as a baseline for transpose
  - Example, choose secret word ATTACKER and assign value as 17823546 (assign ascending numbers based on alphabets 1st A=1, 2nd A=2,C=3 so on
  - Then using Columnar Transposition (any message can be encoded) example on page 382
- To be coninued!!

Cryptography History

- Ceaser used Ceaser Cipher in Romans War, cipher uses substituted words, D for A,G for D, meaning ROT3 (rotate 3 letters to right). Frequency analysis can "crack it" easily!
- In American Civil War, Flag System was used for encrypting messages/signals
- In World War 2, Germans developed Enigma for encrypting messages/texts, Only way to decrypt was to use same Enigma at other end of transmission!
- Polish decrypted Enigma, they called that project Ultra
- Basics of all is – encrypt original communication

Goals of Cryptography

- 4 key goals
  - 1. Confidentiality
    - Most well known goal of cryptography
  - 2. Authentication
  - 3. Integrity
  - 4. Non Repudiation
    - Achieved through Digital Signatures that we will study later!

1. Confidentiality

- When data at rest
- When data in transit
- When data in use
- We can support
  - Symmetric cryptosystems
    - Shared key that is used by every user
  - Asymmetric cryptosystems
    - Each user has its own pair of public/ private key

2. Integrity

- Basic concept, no data alteration if not authorized
- Another form is "message integrity"
  - Meaning message sent and received by other end as it is, done through digital signatures

3. Authentication

- Basic concept – prove that you are who you are claiming to be!
- Handshake-Challenge is one way
  - Authenticator send challenge and expect response that is known only to "2 persons" who are in communication

4. Non Repudiation

- Making sure that message coming from a source that we know what the source is and source cannot deny that message is indeed sent by that source
- That cannot be achieved by shared key coz anyone in the shared circle can use that key and send encrypted message, so non repudiation is achieved through public/private key

Basic Cryptographic Concept

- Cryptography is based on "algorithms" that encrypt plaintext into ciphers
- That encryption is done using "keys", keys are nothing but bits (0s and 1s)
- Key Space or Key Range is number of keys that an "algorithm" can use
- If algorithm use key of 2 bits, it means that it has 0 to 2^2 keys available, 00,01,10,11
- If 3 bits, 000, 001, 010,011, 100, 101, 110,111, you got it!
- Also data at the end is also 0s and 1s, function is executed b/w original simple data and keys to make to complicated or encrypted
- The most important thing is to "protect" the keys, no one should know what keys we have used to encrypt (and to decrypt). That's where our security lies!

Kerckhoffs's principle

- States that cryptography system should be secure even if everything about the system is public, except "crypto keys". OR remember "The enemy knows the system"!

Key Definitions

- Crypto Keys
  - Keys defined by cryptosystem to encrypt/decrypt information using specific algorithm. Keys are also called "crypto variables"
- Cryptosystem
  - System that when operates, creates crypto keys
- Algorithm
  - Mathematical script/instructions that can run and define crypto keys
- Cryptography
  - The study/process to implement cryptography systems to create secret codes and ciphers
- Cryptanalysis
  - The art of decoding/breaking ciphers/codes created by cryptography
- Cryptology
  - The study of cryptography and cryptanalysis is called Cryptology

FIPS 140-2

- Federal Information Processing Standard 140-2 defines hardware/software requirements to implement cryptographic modules
- You cannot install normal hardware/software for cryptographic modules/system

Security Architecture

Modern Cyrptography

Basics – Modern cryptography is based on large key sizes and then implied algorithms that can work with those keys to produce ciphers/encrypted text

In past, approach was to hide encryption/algorithm functions to achieve secrecy that is like "security through obscurity". In modern, approach is to public encryption details but hide/protect keys. Making encryption/algorithm public helps to find bugs in it

DES (56 bits) when launched was supposed to be enough, but now at least 128 bit key is used. Future we don't know and the keys requirements will become more and more!

NOTE: Modern encryption algorithms are divided into 3 categories; symmetric, asymmetric and hashing

Symmetric Algorithm

Shared secret/private key is shared among users that will then be used by algorithm to encrypt traffic

That's why also called Shared secret or private key cryptography

NOTE: don't get confused with "private key" because in asymmetric algorithm also we use public-private key pair, here it is in context that key is private among group of users

Advantages/Pros

Symm algorithms are quite fast in processing, 100 to 1000 times faster than asymmetric, due to simple nature of symm algorithm

Easy to use for bulk encryption as it shares same key so single generated key can be used for bulk encryption

Disadvantages /Cons

Cant be used nonrepudiation as everyone in group uses same key

Distribution of keys is a challenge

Key needs to be regenerated often (imagine 1 user left and he knows all the keys earlier, all those need to be discarded then!)

Not scalable because for every user to user session we need kind of a full mesh. N(n-1)/2 is number of keys required, if n users would like to communicate with everyone exclusively. However if every user is only required to communicate at once with a community then only 1 key is required that everyone can have

Asymmetric Algorithm

This has a key pair, a public key and a private key

Public Key is known by everyone and private key is only known to a "user/owner". Always works in pair!

If Bob needs to send message to Alice, Bob will encrypt message using Alice Public key, and Alice will then decrypt message with a paired private key

In addition, assymetric keys can be used to generate digital signatures, how?

If Bob needs to send a message with digital signature to ANYONE who has Bob Public Key, then Bob hash the message using hashing algorithm to create message digest, then bob encrypts that message digest with its private key and anyone can decrypt that message using Bob's Public Key. This is to ensure that message sent by Bob is indeed Bob

Pros/Advantages of Assyme algorit

Easy to add or remove user as only that user specific key pair (pub/pri) needs to be created

Authentication, integrity and nonrepudiation are possible (nonrepud as user can sign message)

Scalable as number of keys required is much less as compared to # of users as they increase

No preexisting link/connection is required to start communication between users. Just user needs to publish its Public Key and done, other users can start communicating

Key distribution is simpler process

Cons/ Disadvantage

Its only disadvantage is that its slow. So many applications first start establish Assymetric connection, then start symmetric within that assymetric by distributing symm keys first and start data exchange within that assym session

Symmetric	Asymmetric
Single shared key	Key pair sets
Out-of-band exchange	In-band exchange
Not scalable	Scalable
Fast	Slow
Bulk encryption	Small blocks of data, digital signatures, digital envelopes, digital certificates
Confidentiality	Confidentiality, integrity, authenticity, nonrepudiation

Types of Ciphers

Substitution Ciphers

This substitutes the plaintext (P) with Cipher (C)

Substitution can be based on algorithms, example Polyalphabetic Substitution that substitute each P with C based on Alphabet Table and secret key. It is also called Vigenere Cipher!

Alphabetic Table is produced using define algorithmic steps (page 385), then using that table and secret key, every P is replaced with C

Can also be defined as Function, for example ROT3 (Caesar Cipher), is function C = (P+3) mod 26 where alphabets A to Z are assigned numbers 0 to 25

One Time Pad

Very powerful cipher technique, used for highly secret comms in WW2

Mathematical function of One Time Pad is C=(P+K) mod 26

One Time Pads are actually One Time generated secret keys that changes P into C following specific algorithm

4 key requirements to successfully implement One-time Pad

1. Pad must be randomly generated
2. Pad must be used once, no repetition
3. Pads must also be physically protected, no leakage. Pads are actually physically pads
4. Pad length (Key Length) must be same as P (plain text message) to be ciphered coz each character of key is used to cipher each alphabet of P

NOTE: Ceaser Cipher, Vigenere Cipher and One Time pad are all actually doing one thing, Replacing original plaintext with Cipher, the complexity lies in key size. Ceaser has key size of 1 only, Vigenere has key size say equal to word or sentence, One Time Pad has much higher key size, same as Plain text length

Running Key Ciphers

This actually solves problem of One Time Pad that has key size as long as message to be encrypted however One Time Pads are physical and difficult to transport/carry so to solve, Sender and Receiver can assume any random text as a key example 3rd para of Harry Potter book1 page 10 and using that as key and then applying any function, say mod 26, cipher text can be produced. Following reverse methodology, plain text can be produced from that cipher

Block Ciphers

These work on encrypting entire block/segment of the message. Example is Transposition Cipher that takes a whole message, apply key to that message, passed through algorithm and produces Cipher text. Most modern encryption algorithm implement some type of block cipher

Stream Ciphers

These work on bit by bit/character by character to encrypt. Example One Time Pad or Substitution Cipher. By the way, stream cipher can work as block cipher, in which the buffer is accommodated/created that fills certain block of data (Block Cipher) which then is encrypted using Stream Cipher

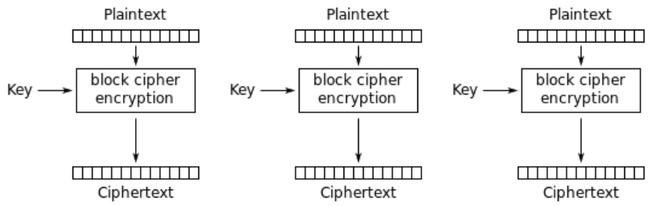
Confusion and Diffusion Concept

Confusion

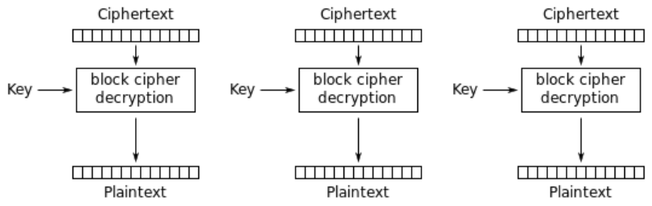
When relationship between P (plain text) and K (key) is so complicated than cryptanalyst cannot identify what's the key even after many attempts of changing P to C (cipher) and try to decipher key

Diffusion

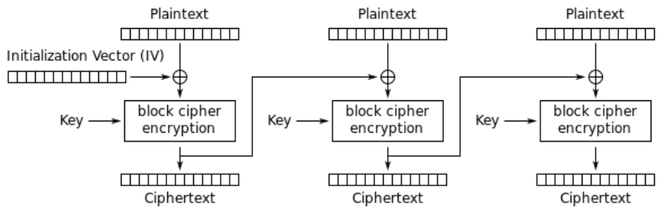
Diffusion meaning that changing one element of P produces several changes in C. Example 1st P changed to C using Substitution Cipher and then C further complicated by Transposition Cipher so if small change is done in P, multiple changes will appear in C



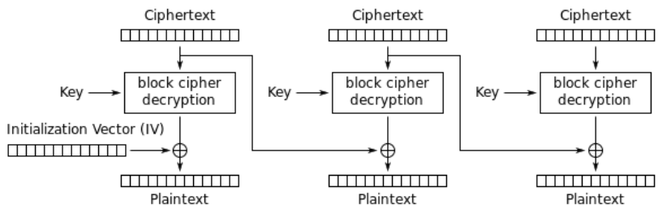
Electronic Codebook (ECB) mode encryption



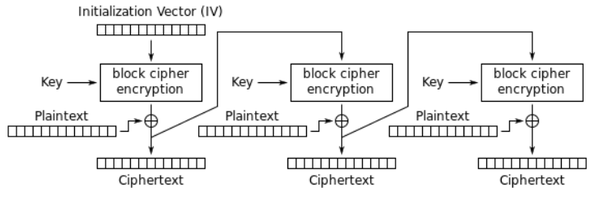
Electronic Codebook (ECB) mode decryption



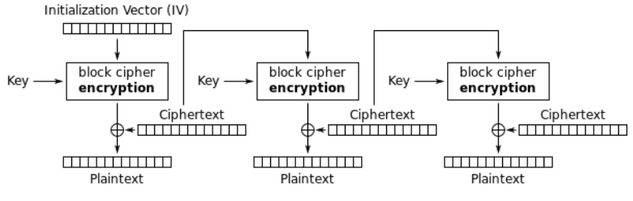
Cipher Block Chaining (CBC) mode encryption



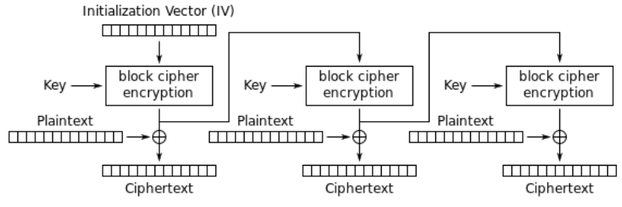
Cipher Block Chaining (CBC) mode decryption



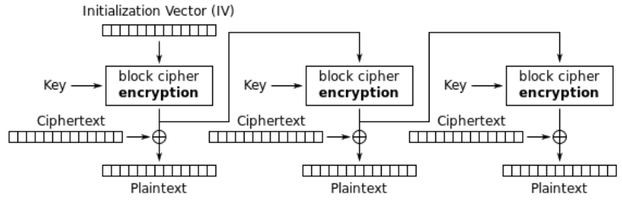
Cipher Feedback (CFB) mode encryption



Cipher Feedback (CFB) mode decryption



Output Feedback (OFB) mode encryption



Output Feedback (OFB) mode decryption

- Security Architecture
  - Symmetric algorithms
    - NOTE: now we will focus on different types of Symmetric Algorithms
    - DES
      - Digital Encryption Standard
        - US Govt published in 1977 as proposed encry standard for all government communications
        - Uses 56 bit key
        - Works in 64 bits data blocks
        - Utilized XOR operation
        - To produce encryption, runs 16 rounds of XOR
      - Modes of Operation of DES
        - Electronic Code Book (ECB) Mode
          - Simplest mode, simply take 64 bits block of P and encrypts using 56 bits to produce C
          - Implies that if anytime 64 bits block of P is somehow similar, then it will produce similar type of Cipher Text/code
          - So hackers can actually create a code book of all having 64 bits C and if any C is similar in pattern then they can identify algorithm
          - Hence this mode is only used for short communication say only to exchange keys for other modes
        - Seed Value Concept
          - Before we go into other modes, we need Seed Value concept. Seed Value is an output for Key + Initialization vector when they run through encryption
          - Seed Value is only required at the beginning data and then it continues as on-going part of operation in one way or other depending upon mode
        - Cipher Block Chaining (CBC) Mode
          - The concept is simple, before getting into concept, understand that message/data message is consists of several 64 bits block meaning many 64 bits block makes 1 message, depends upon message size. Now continue!
          - In CBC, we take 1st block of 64 bits of Plain Text, we XOR it with IV (initialization vector, randomly generated acting as seed value) and then we run it through DES algorithm with key as input, it then produces Cipher Text. That Cipher Text is then XOR with next block of 64 bits plaintext, which then goes through DES algorithm with key as input and cycle continues. It means that every subsequent output of cipher text depends upon previous cipher text. Hence in case if one 64 bit Plaint text block is errored, then it is impossible to take only that block and decrypts it, it will remain as error
        - Cipher Feedback (CFB) Mode
          - CFB works exactly as CBC. The only difference that CBC works with pre-existing data, say data stored in a server/database, while **CFB works with streaming realtime data say video/voice**, so it has a buffer of 64 bits, as streaming data keeps on coming, that buffer fills and when buffer fills full, 64 bits, it starts exactly same operations as CBC
        - Output Feedback (OFB) Mode
          - In OFB, we take a Initialization Vector as 1st seed value and we run algorithm with that and key as input and we have encryption output (this will act as Seed Value for next block of data!, this is not Cipher Text yet, it will be produced later when plain text will be XORed with this encryption output), which then XORs with clear text to produce Cipher Text that will then proceed to transmission. Because OFB does not depends directly only on encrypted Ciphertext, rather on Output of algorithm hence if there is any error in encryption, it will not be transported till end, it can be contained within that data block only
        - Counter Mode
          - Works exactly like CFB or OFB in terms of concept. The difference that it uses a counter for every data block as seed value, so there is no concept of using previous cipher or previous encryption output as seed value for next data block. As it uses **Counter** for every data block, it thus can be used parallel computing because every data block (encryption and decryption) is identified as separate unique number hence parallel computing can work well

Protocol	Block Size	Key Size	Comments
DES	64 bits	56 bits	Electronic Code Book (ECB) Mode Cipher Block Chaining (CBC) Mode Cipher Feedback (CFB) Mode Output Feedback (OFB) Mode Counter (CTR) Mode
3DES	64 bits	112 bits 168 bits	EEE3 (Encryption with 3 keys) EDE3 (Encryption/Decryption with 3 keys) EEE2 (Encryption with 2 keys) EDE2 (Encryption/Decryption with 2 keys)
IDEA (International Data Encryption Alogrithm	64 bits	128 bits	Used in PGP (Pretty Good Privacy)
Blowfish	64 bits	32 to 448 bits	Used in SSH
Skipjack	64 bits	80 bits	
Rivest Cipher 2 (RC2)	64 bits	12 bits	
Rivest Cipher 5 (RC5)	32/64/128 bits	0-2040 bits	
AES	128 bits	128/192/256 bits	Encryption standard developed by NIST for use by US Gov in 2001 superseded DES (announced in FIPS 197), but now widely used
Rijndael	Variable	128/192/256 bits	
Twofish	128 bits	1-256 bits	

- **Security Architecture**
  - Symmetric Key Management
    - Secure exchange and then management of symmetric keys between communicating parties is very important as by its very nature same keys is used for encryption and decryption
    - There are 3 methods for key exchange
    - Physical/Offline Key Exchange
      - Lot of manual work and inherent risk if anyone can see those keys (in paper/USB/media)
    - Public Key Method
      - Start with public/private key establishment session (asymmetric) and within that session exchange symmetric keys to continue with symmetric encryption coz its much faster
    - Diffie Helman key exchange algorithm
      - Say Richard-R and Sue-S would like to exchange symmetric keys
      - 1. S and R choose 2 numbers, p(large prime number) and g(large integer), such that 1<g<p
      - 2. R choose another large number-r and calculates R=g^r mod p
      - 3. S choose another large number-s and calculates S=g^s mod p
      - 4. Richard share R with Sue and Sue share S with Richard
      - 5. Then R calculates K=S^r mod p
      - 6. Then S calculates K=R^s mod p
      - 7. This K must be same, then this K then be used as a secret key
    - Key Storage & Destruction
      - Key should not be saved on the same system where encrypted data is present (it will make things easier for hackers)
      - While saving key, apply split knowledge principle meaning that whole key is distributed into sub-elements that will be owned by different individuals so that not anyone has whole key info
    - Key Escrow and Recovery
      - From concept its simple, key is kept by 3rd party and when govt entity requires that key becomes accessible by the order of court to decrypt messages. There are 2 approaches;
      - 1. Fair Cryptosystems
        - Meaning key is held by 2 or more parties and key can be recollected by approaching both parties and get the part
      - 2. Escrow Encryption
        - Similar to 1. key is escrowed by 2 different entities and when required each part of key is obtained for decryption
  - 3-DES
    - Or Triple DES
      - Uses 3 keys, each of 56 bit (56 x 3 = 168 it should be!)
      - Due to attackers knowledge, effective key length is reduced to 112 bits
    - Uses 4 modes
      - EEE3 (meaning 3 times encryption function with 3 keys) — C=E(K1,E(K2,E(K3,P)))
      - EDE3(meaning 2 times encryption and 1 time decryption function with 3 keys) — C=E(K1,D(K2,E(K3,P)))
      - EEE2 (meaning 3 times encryption function with 2 keys) — C=E(K1,E(K2,E(K1,P)))
      - EDE2(meaning 2 times encryption and 1 time decryption function with 2 keys) — C=E(K1,D(K2,E(K1,P)))
  - IDEA
    - International Data Encryption Alogrithm
      - Came into existence due to key limitations of DES and 3DES
      - Works with 64 bits Plaintext/Ciphertext blocks
      - Its key size is 128 bits, however, it divides this 128 bit key into 52 sub-keys each of 16 bit, then runs its algorithm
      - It was patented till 2012, then it is widely used in developing another encryption algorithm called Pretty Good Privacy (PGP) used widely for email encryption
      - Supports all modes of operation that are supported by DES
  - Blowfish
    - It is unlicensed so that's the key, can be used by anyone
    - Key size is from 32 to 448 (obviously 448 requires much more processing
    - In use by several applications
    - Works on again 64 bits data block
  - Skipjack
    - Approved for use by FIPS (Federal Information Processing Systems)
    - Developed by US National Security Agency
    - Works on 64 bits plaintext block (as other encryption techniques!
    - Key size is 80 bits
    - It has this unique/unsecure feature of "key escrow" meaning that its key can be stored by Dept of Treasury and NIST (National Institute of Science and Technology). Law enforcement agencies can request these 2 dept to acquire keys in case if any investigation is required to be done
  - Rivest Cipher 5 (RC5)
    - Developed and patented by Rivest Shamir Adleman
    - Its cipher/plaintext block size is 32 or 64 or 128 bits
    - Its key size is 0 to 2040 bits
    - As per hackers community, it took 4 years to decrypt 64 bit key encrypted message by RC5
  - Advanced Encryption Standard (AES)
    - Encryption standard developed by NIST for use by US Gov in 2001 superseded DES (announced in FIPS 197), but now widely used
    - AES is based on Rjindael cipher protocol and AES standard is built out of Rjindael specs
    - It uses 128 or 192 or 256 bit key size
      - 128 bit key requires 10 rounds of encryption
      - 192 bit key requires 12 rounds of encryption
      - 256 bit key requires 14 rounds of encryption
    - Block size is 128
    - Another protocol that was AES finalist was Twofish
      - Developed by same person who developed Blowfish
      - It uses 128 bit BLOCK and 1-256 bit Key
      - It uses Pre-Whitening and Post-Whitening
      - Pre-Whitening meaning that XOR plaintext with a separate key before 1st round of encryption
      - Post-Whitening meaning that XOR plaintext with a separate key after 16th round of encryption
  - Cryptographic Lifecycle
    - Every cryptographic system/method (except one time pad as it is one-time) has lifespan
    - Because computers are increasingly becoming powerful (Moore's law say that every 2 years computing power is doubled)
    - When designing cryptographic systems, designer must consider
      - Encryption Protcol
      - Key Length
      - Secure transaction protocols (SSL/TLS) that may be used

Security Architecture

Hash Functions

Main purpose of Hash Functions is to ascertain the sender and data integrity, also used in Digital Signatures

Basics of Hashing

- Take large message as input
- Produce message digest(MD) using original message as input and hash as a function
- MD is mostly 128 bits or higher
- Sender can send original message and MD to receiver, which then take the original message and runs through same hash function to see if it also gets same MD to confirm that message is not modified in transit

Features of Hashing function

1. Input can be of any length
2. MD must be of same length
3. MD must be one way, meaning not possible to get original input simply looking at MD
4. MD should be easy to compute for any message
5. must be collision Free, no same MD for two different inputs

Hashing Algorithms

SHA

- Called Securing Hash Algorithm
- Promoted by government as standard hashing algorithm
- In government called, FIPS-180 standard and SHS (Secure Hash Standard)

SHA-1

- 1st type, MD size is 160 bit and data size it works on 512 bit block
- Due to SHA-1 weakness, SHA-2 appears, have 4 variations

SHA-2

- MD is 256 bit and data block is 512 bits — SHA-256
- MD is 224 bit and data block is 512 bits — SHA-224
- MD is 512 bit and data block is 1024 bits — SHA-512
- MD is 384 bit and data block is 1024 bits — SHA-384

SHA-3

Though SHA-2 has larger MD size but inherent same weakness as SHA-1, hence SHA-3 introduced in 2015. SHA-3 has same MD and data block-size as SHA-2 support but it is stronger. It is based on Keccak algorithm

MD-2

For MD-2, data block must be 16 bytes multiple (or 16 bytes), if not then MD-2 adds padding

Then it appends 16 Bytes of checksum to data block and then produces MD of 128 bit

It was discovered that MD-2 is not one way (dangerous!) and if 16 bytes checksum is not appended then collision may occur in MD

It was developed to provide secure has function for 8 bit processor

MD-4

It works on data block that is 64 bits less than multiple of 512, if smaller than that, then it pads

It then produces 128 bit MD by going through 3 rounds of computation

It is not secure hash and demonstrated in 1996 that good computer can find collision for MD-4 in less than a minute

It was developed to provide secure has function for 32 bit processor

MD-5

It works on data block that is 64 bits less than multiple of 512, if smaller than that, then it pads (same as MD-4)

It then produces 128 bit MD by going through 4 rounds of computation

In 2005, it was demonstrated that MD-5 is vulnerable to collision (2 digital certificates can be produced using 2 private keys, and they can produce same MD-5 Digest)

Hash of Variable Length (HVAL)

- It works on data blocks of 1024 bits
- Produces MD of 128, 160, 192, 224 and 256 bits
- It is a modification of MD-5

Asymmetric Cryptography

Meaning that keys are not same, one is public and other is private

- Public Key — Key which is PUBLIC, known to everyone
- Private Key — Key only known to THAT user for whom message is addressed
- Communication — Simply sender takes P, runs algorithm using receiver Public Key and produces C
- Receiver receives C, runs decryption algorithm using its Private Key and get P
- Beauty — Is that once sender encrypts using public key, even he cannot decrypt without having private key, so one way operation
- Also no sharing of private key is required, only public key is enough for sender to send cipher data

1. RSA Algorithm

Published in 1977

Operates on the basis of product of large prime numbers is a one way function

To Keys using this algorithm follow as

1. choose 2 large (200 digits above) prime numbers, p and q
2. n = p x q
3. Choose another number e such that, e <n and product of (p-1)(q-1) & e has only 1 common factor that is 1 (implies that they are prime)
4. choose another number d such that (ed-1)mod(p-1))q-1)=1
5. now d is private key and e & n are public key

In order to encrypt (P, plaintext), C=P^e mod n

In order to decrypt, P=C^d mod n

Importance of Key Lengths

Key Length is directly proportional to security level it provides & resources it require to process

Key Length can be chosen by Security Admin and this selection is important

So chosen key lengths should be as per data trying to protect and also for how long that data needs to be protected. Consider the higher processing power computers that are in place and that come into future

RSA 1024 bits, DSA 1024 bits and Elliptic Curve 160 bit — They all provide same level of encryption security/protection

2. El Gamal

Another algorithm for asymmetric key exchange

Dr El Gamal published in 1985 and made it free for public, not patented (at that time RSA was patented)

Algorithm explained how Diffie Hellman can be further extended to support whole public cryptographic solution

Disadvantage was that El Gamal algorithm doubles the size of any message that it encrypts and hence difficult to propagate through narrow channel

3. Elliptic Curve Cryptography(ECC)

In same year 1985, ECC was proposed by 2 different mathematician individually

The basic of this cryptography is

- Any elliptical curve can be defined by equation y2=x3+ax+b, where a,b,x,y are all integers
- Along with every elliptical curve, there is Elliptical Curve Group that includes all points on the curve and point at infinity represented by O
- So any 2 points (say P & Q) within that curve group can be added, P+Q
- Further relation between these 2 points be Q=xP meaning that Q is multiple of P
- So algorithm says that finding this x is much harder then finding prime factors in RSA for example, that depicts from fact that 160 bit key of ECC is as powerful as 1024 bit key of RSA or DSA

Algorithm Name	Hash/Message Digest Length	Data Block	Comments
SHA-1	160 bits	512 bits	Recommended by Government(NIST), FIPS-180 is a standard
SHA-256	256 bits	512 bits	Flavor of SHA-2 & SHA-3 (SHA-3 is stronger and based on Keccak Algorithm
SHA-224	224 bits	512 bits	Flavor of SHA-2 & SHA-3 (SHA-3 is stronger and based on Keccak Algorithm
SHA-512	512 bits	1024 bits	Flavor of SHA-2 & SHA-3 (SHA-3 is stronger and based on Keccak Algorithm
SHA-386	386 bits	1024 bits	Flavor of SHA-2 & SHA-3 (SHA-3 is stronger and based on Keccak Algorithm
MD-2	128 bit	16 Bytes Multiple	
MD-4	128 bit	64 bits less than 512 bits	128 bit MD is generated after 3 rounds encryption
MD-5	128 bit	64 bits less than 512 bits	128 bit MD is generated after 4 rounds encryption
HVAL	128/160/192/224/256	1024	Modification of MD-5

Security Architecture 5

Public Key Infrastructure

In order to make secure communication work between unknown parties spread across Internet, it requires a solid infrastructure with many components, these components (assyme/symmet encryption, public keys, digital signatures, certificates etc.) creates PKI. Here we will discuss each component

1. Certificates

Simply digital certificates

Are endorsed (attested) copy of "entity's" public key (meaning confirmation that this public key is indeed correct/attested/owned by that entity

This certificate is issued by CA (Certificate Authority) reputed org that issues endorsed/attested digital certificates

Standard of these certificates is X.509 (current version is 3) that contains following in issued certificate

- Certificate Number
- Name of entity who issued certificate
- Name of entity for whom certificate is issued
- Validity Start Date and Expiry Date
- Algorithm used to sign this certificate
- KEY ITEM: The public key (yes this certificate contains public key and now this public key is endorsed/attested)

Optional: X.509 v3 can have some additional bits that can be added to certificate to facilitate tracking of certificate etc (may be those bits can be used for some other purpose)

2. Certificate Authorities (CA)

These are trusted organizations that issues Digital Certificates

Some top one are Comodo, Symantec, Amazon Web Services, GoDaddy etc.

In Internet communication, from end host to server there may be more than one certificate (may be multiple entities involved) required to complete communication, this is a chain of trust, called Certificate Path Validation, meaning this is a validation to make sure that all certificates in the path are trusted and validated

Most browser developer config by default to trust certificates from trusted CA. if one certificate is trusted from CA then all certificates from that CA will be trusted

3. Registration Authority (RA)

Only assists CA to validate end users (entity/organziation/company) for whom CA is about to issue a certificate, RA doesn't itself issue certificates, it only assists CA

4. Digital Certificate Creation, Management and Destruction

Several steps involved as mentioned below

1. User/Entity enrollment

You must identify yourself to CA (either physically/someone from community identifies you/or credit report data

2. certificate creation

Then you give your public key to CA, they provide you with X.509 digital certificate containing your public key after signing that with their private key

Then you can share this certificate with anyone you would like to establish secure communication with

3. Certificate Verification

If you receive CA signed certificate from someone who would like to start communication with you, then you first must verify its authenticity

Check CRL (certificate revocation list) and Online Certificate Status Protocol (OCSP) to validate that certificate is still valid and not revoked. This check is normally built in the browser already by default

Also note that CA has endorsed what that is included data in certificate and not anything else, example if email is only thing added in certificate, then CA has ony validated email, but not may be a person behind that email. Hence this point needs to be covered in point 1 (user/entity identi)

4. Certificate Revocation

This is required sometime

- If private key of certificate owner is compromised
- If CA issued certificate erroneously
- If certificate needs to be modified
- If certificate for which it was issued, has changed domain/ownership/responsibility/become non-functional

2 methods for certificate revocation

- CRL (manually you have to download list provided by CA and validate manually with cross reference, it is delayed process but widely used
- OCSP: Run this protocol between machine validating certificate & CA server, it will check and revert back with either **valid/invalid/unknown**

Digital Signatures

Basic Concept: Digitally sign the message before sending so that receiver is ascertain that messages indeed comes from "sender" & "message is not modified/altered in transit"

Steps of operation

1. Take plaintext message and produce hash using hashing algorithm (say SHA3-512
2. Take that hash and sign that hash with private key
3. append original PT message to hashed and signed message and send to the receiver
4. Receiver gets the hash by decrypting the message with sender public key. Receiver now knows what the hash is that is sent by Sender
5. Receiver now takes original message (that was appended earlier by Sender) and produces hash using same hashing algorithm as sender
6. receiver now compares hash that is just generated and that was sent by sender
7. if these 2 hash match, it is confirmed that message is indeed sent by sender and not modified in transit (provides authentication, integrity and non-repudiation)

Note: note that Digital Signatures itself doesn't provide encryption/security, if it is required, then in step 3, sender can take hash and appended PT and then encrypt them with receiver public key so that now the digital signature is also encrypted

HMAC

Hashed Message Authentication Code

Meaning Plantext + Symmetric Key + Hashing Function = HMAC (meaning hash is calculated along with using key)

This adds that "authentication" part as well making sure that message indeed comes from sender because it is hashed when key was also part of hashing algorithm

Key exchange should already be in place for this to function properly

Digital Signature Standatrd

Short as DSS, issued by NIST to guide digital signature for Federal Information systems

Standard number is 186-4

Dictates that all Digital Signature algorithm used by Federal must use SHA3 as hashing algorithm

Following are approved encryption algorithm that can be used to support Digital Signature

- RSA
- DSA (Digital Signature Algorithm)
- Elliptic Curve DSA
- Schnorr Algorithm (just remember the name)
- Nyberg Rueppel (just remember the name)

Which key to use when?

When someone else wants to decrypt your message or want to verify your signature, they use your public key

When you want to decrypt message sent by someone else, us their public key

When you want to encrypt your message, use your private

When you want to sign your message, use your private key

Security Architecture

Cryptography in Networking

- Used for protecting network/links
- 2 types where encryption is implemented
  - Link Encryption
  - End to End Encryption
- Link Encryption
  - When only the network link is encrypted (gateway to gateway) like a tunnel. The whole packet is encrypted (headers also) hence at each hop packet be decrypted to check next hop IP and then re-encrypted)
- End to end encryption
  - When end to end (client to client) communication is encrypted (host to host). Only the payload is encrypted, header is not, hence it is fast compared to Link Encryption
- Example of SSH
  - SSH is end to end encryption protocol. Replacement of FTP/ telnet etc that are unsecure. SSH versions are 1&2. V1 supports DES/3DES/IDEA/Blowfish, V2 doesn't support DES/IDEA but has added several other protocols support
- IP Sec
  - IETF standard. It's an open framework to provide network security. Works along with L2TP to provide complete network protection
  - Has 2 major components (AH and ESP)
    - AH (Authentication Header) provides authentication, access control, non-rep and protection from replay attack
    - ESP provides confidentiality/ integrity, some level of authen and protection from replay attack
  - Operates in 2 modes
    - Tunnel mode (whole packet is encrypted) used for gateway to gateway to commu
    - Transport Mode (only payload is encrypted) used for peer to peer comm
  - Creates SA (security association) for every communication and its 1 way, meaning from bidirectional comm, we need 2 SAs
  - ISAKMP is supporting protocol for IPSEC. It authenticate peers, it creates and manages SA, it protects communication, it provides key generation mechanism

Asymmetric Key Management

- Important to manage keys carefully
- Rotate keys timely and keep private keys safe
- Update browser as a routine to keep it updated with all required certificates
- Backup your keys securely, you can use also key escrow accounts
- Another option is to use Hardware Security Modules (HSM), these are specialized hardware to provide key management

Application of Cryptography

- Real world scenarios meaning protection/encryption data at rest/transit/process
- Data at rest
  - Portable Devices
    - Latest OS (Windows) have EFS (encryption files system) and BitLocker
    - MAC has FileVault
    - VeraCrypt is open standard
  - Trusted Platform Module
    - This is actually a chip on the motherboard that manages keys
    - It avoids cases where hacker can remove physical hard drive from system
    - It offers FDE (Full Disk Encryption)
    - There are other solutions that are available and their usability and advantages is also based on the fact that how they can integrate with TPM
- Data in Transit
  - Email
    - Email security should only be implemented if it is really required (no wastage of resources!)
    - If you want confidentiality, then encrypt your message
    - If you want confidentiality + integrity, then encryption + hashing
    - If you want confidentiality + integrity + non-repudiation then encryption + hashing + digital signature
    - Sender of email has to make sure that he is sending email with attributes that is expected
    - Recently email cryptography was difficult option with several manual configs required, now things have changed and pre-packaged applications/software can offer the required services
    - Pretty Good Privacy (PGP)
      - This is used for email encryption and implemented as "web of trust" concept
      - Web of Trust is like decentralized approach to CA
      - You as a user develop trust with other users and you will then rely on trust that they have developed and chain continues
      - This is the basic for PGP Email encryption
      - Commercial version of PGP uses RSA for key exchange, IDEA for encryption and MD5 for hash
      - Free version of PGP uses DH for key exchange, CAST (what the hell is CAST, search) for encryption and SHA1 for hash
    - S/MIME
      - Secure Multipurpose Internet Mail Extension (Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of email messages to support text in character sets other than ASCII, as well attachments of audio, video, images, and application programs)
      - Became de facto standard for secure email
      - It uses X.509 standard for exchange of digital certificates and these certificates, as we know, have public keys and exchange of public key exchange happens like this
      - S/MIME uses RSA for Asymmetric encryption and once established then uses AES/3DES for symmetric encryption
      - RSA is only public key protocol supported by S-MIME
  - Digital Rights Management (DRM)
    - Technique to impose protection/restriction for media content (music/video/books)
    - Music DRM
      - Not well received, faces opposition by end user as it deprives them to even take legitimate copies for backup
    - Movie DRM
      - 2 techniques were deployed to implement video DRM. However, not successful, as hackers released keys for decryptions
    - E-Book DRM
      - Comparatively used successfully. Adobe has ADEPT (Adobe Digital Experience Protection Technology) to implement DRM for its products
    - Video Game DRM
      - This implementation requires users to be connected to Internet ALL the time while playing game and hence faces extensive opposition from end users, so then stopped
    - Document DRM
      - Though not used very often, provide controls like (not allowed to print file, or take screen shot of file or not allowed to save file). These are all part of document DRM
  - Steganography
    - A technique to hide a message into another message/file
    - Basic concept is that every file/image is actually "bits", so take lease significant bits of that file and alter them to produce new image/file that would contain original data + added data that would be very difficult to catch/inspect. So simply manipulation of bits!
    - For legitimate purpose, it can be used to ensure copyright, where original file/text is produced using water mark so if any one makes a copy of that document, water mark can assist original owner to trace that copy. Water Mark is also modification of bits actually!
  - Web Applications
    - Uses HTTPS (HTTP over SSL/TLS), tcp port 443
    - SSL is old, now called TLS i.e enhanced version of SSL
    - Works between browser and web server
    - When browser connects to server, it extracts public key of server from server digital certificate. Then browser generates random symmetric key and send that key to server using encryption with server public key (that it extracts earlier). Then communication continues using symmetric key. Classic example of symmetric encryption using public key infrastructure. Hence communication is faster because of symmetric keys within public keys
    - When SSL was stopped, it was SSL v3.0, hence TLS sometimes is called SSL v3.1

- **Security Architecture**
  - Wireless Security
    - Another example of Cryptography in network
    - Wireless networks are quite susceptible for attacks
    - There are 2 security standards for Wireless
      - WEP (Wired Equivalent Privacy)
      - WPA (WiFi Protected Access)
    - Another one is 802.1x (but that is not dedicated for wireless, it can be used for wired also)
    - WEP is not recommended and not secure. It is defined in IEEE 802.11 and offers 64 & 128 bit encryption
    - WPA is enhanced. In fact WPA version 2 offers AES encryption as well. WPA provides security between mobile user and Access Point but not end to end, once traffic reaches access points and leaves then not under WPA
    - 802.1x works between user and authentication server. User is called Supplicant that supplies credentials to Authentication Server, once authenticated, user is allowed to access network (either wired or wireless)
  - Cryptographic Attacks
    - Analytic Attacks
      - Attackers try to understand logic behind the algorithm to conduct these attacks
    - Implementation Attacks
      - Attackers try to understand implementation of cryptographic system, that is actually a software code so they target softwares
    - Statistical attacks
      - Attacker analyze stats about how cryptographic algorithm has performed in the past and then tries to find errors in one of that event
    - Brute Force
      - Attackers try every possible combination to find cryptographic keys, and ultimately it becomes successful however needs lots of attempts and number of attempts required increase with every addition of bit in the key as it doubles the # of keys
      - Attackers also try to use Rainbow Table or Dictionary (a table that provide precomputed values for all hashes and hence by identifying a pattern of those hashes, brute force can be quick!
    - Salting Saved Passwords can defend well with Brute Force attacks. Salting means that adding extra random value in front of password before hashing it and saving it (salt is saved with hash in password file) so that when user enters password, system can add that salt before hashing to compare hash that was saved and one appears when user entered PW
    - Known Ciphertext and Frequency Analysis attack
      - The attacker knows the Ciphertext. It then analyzes the C and observe frequency of particular character. If repeated character is one of more popular characters such as ETAOIN, then it could be transposition (meaning that the position of characters is changed only to produce Cipher), if repeated characters are not common one, then it could be substitution attack where more plaintext is replaced with some uncommon characters
    - Known Ciphertext and Known Plaintext
      - Now attacker tries to find a key that is used between P and C
    - Choosen Ciphertext or Plaintext
      - In both cases, attacker knows one of 2 variables, either chosen part of P or chosen part of C and tries to identify Key/encryption
    - Basics: So the basic is that there are 4 variables, that are plaintext, ciphertext, key and algorithm, attackers starts by knowing 1 parameter out of them and then work out to identify rest (meaning key is to find Key and Algorithm that is running behind encryption technique)
    - Meet in The Middle Attack, the classic example is 2DES (attackers know the plaintext, they encrypt P using every possible key and then decrypt C using again every possible key. When the 2 key matches, 2DES is broken
    - Replay and Man in the Middle Attack, both these attacks focus on capturing packets by attacker sitting in the middle, attacker then creates 2 individual sessions, with one originator and one with destination to impersonate genuine originator and genuine destination, while itself sitting between as attacker
    - Birthday Attack: In this attack, the attacker tries to produce same hash as any existing one using different plaintext, meaning that it's a hash collision, this is used mainly to adulterate the data and playing a trick with destination to accept the illegal traffic as legitimate

Security Architecture

Concept of Trust and Assurance

- Trusted System (or Trust on any system) meaning that the system is loaded with required security controls that are capable to protect system as per define security requirements
- Assurance is the confirmation that Trusted System that has specific controls is working as per requirement. So Assurance is usability test meaning that validation that trusted controls are working as required

Security Models

- Next topics related to discussion about Security Models and how these models operate and what re the components of these models
- Security Model is a methodology to assist designers to produce a system/program/ hardware that can be built on the basis of defined security model
- In order to establish a system based on such model, we need a method to identify security attributes attached with the Object, according to those attributes the developers identify the security requirement to protect it and built the system

Security Token

- Token is like an independent object that defines security attributes. Then the token can be used to define an object, so object can be defined with multiple tokens to explain security attributes of that object. When subject likes to access that object, object presents that token to subject and then access control method identifies if access is allowed for that subject or not

Capabilities List

- This is also like Security Attributes but in the style of matrix/list with rows defining security attributes, concept is like Token but in a different way. List of valid actions that can be taken on objects

Security Label

- Label is like permanent security label that defines permanent security attribute for an object. The basic difference between label & other identification methods is that label is permanent and hence have very less chance to be altered

NOTE

- These secuirty models are actually more focused on developing Operating System/Hardware Architecture from scratch such as example an iPhone, a new laptop or a new smart phone!

Definition of Trusted Computing Base (TCB)

- TCB is the set of trusted components (hardware/ software/controls) of the system that defines minimum security criteria/requirement for that system
- This defines the baseline for all Security Models because all models work/operate/built on the defined basis of TCB
- TCB is defined as standard in DoD Criteria as Trusted Computer System Evaluation Criteria (TCSEC)
- Note that not all components should be at TCB, but there are some specific components in the system that must be labelled as TCB
- TCB components in a system control access into the system and also activities of the components outside TCB
- It is the responsibility of TCB to ensure that system behaves within defined security expectations and adheres to it
- Security Perimeter is an imaginary perimeter that detach TCB from rest of the components. If TCB components would like to connect to any non-TCB component, they must do it via Trusted Path (trusted link)
- Reference Monitor is the concept of monitoring done by TCB components to manage authorized access of subjects to objects and block unauthorized access
- Reference Monitor operates using Security Kernel (a control that manages access), so role of Security Kernel is like real Colonel to protect the system
- Security Kernel takes assistance from Tokens/Capabilities List/Security Labels to understand that are the security requirements/level of an Object

Concept of Security Perimeter, Reference Monitor & Security Kernel

FROM WIKIPEDIA: The trusted computing base (TCB) of a computer system is the set of all hardware, firmware, and/or software components that are critical to its security, in the sense that bugs or vulnerabilities occurring inside the TCB might jeopardize the security properties of the entire system. By contrast, parts of a computer system outside the TCB must not be able to misbehave in a way that would leak any more privileges than are granted to them in accordance to the security policy.

The careful design and implementation of a system's trusted computing base is paramount to its overall security. Modern operating systems strive to reduce the size of the TCB[not verified in body] so that an exhaustive examination of its code base (by means of manual or computer-assisted software audit or program verification) becomes feasible. TCB is like a CASTLE in CHESS!

Main topic is implementation of engineering processes using security design principles. First we need to understand concepts

Closed & Open System

- Closed System is built on proprietary information and work well with integration with components from same manufacturer
  - Less susceptible to attack because due to closed nature, vulnerabilities are not exposed well
  - Disadvantage is difficult in integration because built on proprietary knowledge
- Open System is built on standards and multi vendor technologies can integrate in Open System
  - More susceptible to attacks as vulnerabilities are exposed
  - Advantage is easier integration with other vendors
- Open & Closed systems are based on classification of system built with proprietary and standards (that's it). It has no connection if the system is public or private meaning exposed to public or private, Closed System can also be exposed to Public (this will come later in Open Source & Closed Source)

Object & Subject

- Object is an entity/resource/piece of information on which subject acts
- Subject is an entity who asks/demands/requires info/access to/from object. Subject works/acts on Object
- Transitive Trust
  - Concept is A demands info from B, in order to get info B demands it from C. So 1st case, A is subject, B is Object, for 2nd, B is Subject and C is object so B's role is dual (implies that we must treat Subject/Object only based on specific request scenario. Also A trusts B, B trusts C, implies A trusts C, this called Transitive Trust (can be serious risk!)
  - Serious, e.g company blocks access to Internet. So employees (A) cannot access Internet C, so A uses VPN (B) to access C. so now A gets access to B (meaning A built trust with B and then B gets C for A. This scenario creates Transitive Trust that has breached company policy

Open Source and Closed Source

- Open Source where source/code/program of system is made public
- Closed Source where source/code/program is not made public
- Open Source depends upon improvement from public view/comments as public use, then comments and then program improves
- Closed Source program improves upon company strategy and programmers own coding/improvement skills
- NOTE that Closed Systems (above def) can also have Open Source Program and vice versa because Open and Closed Program classification only based on if code is made public or not, it has nothing to do if code is proprietary or not

Methods to implement CIA

Next few topics about methods/tools to implement CIA, lets go term by term

Confinement

Confine application/software to access only certain parts of memory. So actually limiting what an application can access in whole scenario of operating system

Bounds/ Bounding

Its like a control of access/authority that application/software can do, meaning that certain applications can only access particular part of operating system

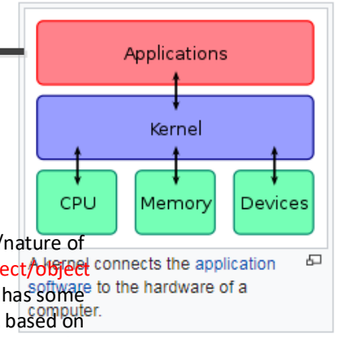
Isolation

When confinement and bounding works together, that particular application/execution operates in an Isolation, that means that it helps to protect Kernel (brain) of OS

NOTE

In order to understand above concepts, we need to have an understanding of components that make operating system/application works, that is show below in some pictures with explanation

- Kernel is core of computer system, see it interacts with Applications (software programs) and CPU/Memory/Devices hardware
- Kernel is saved in separate memory space called Kernel Space
- User programs are saved in User Space of memory



Controls

Controls are put in place to achieve CIA and to built a kind of filter/firewall between subjects and objects (define a condition a check that what objects can subject access. There are 2 types of those access controls

Mandatory Access Controls (role based)

These are controls that are based on static attributes/nature of Subjects and Objects meaning particular role that subject/object plays, hence role based. See every subject and object has some static features that define those subjects and objects, based on those definitions, some mandatory access needs to be granted to subjects

Discretionary Access Control (specific subject based

These are the controls that can be altered based on subject based on defined limits (limits are important), meaning that subject (specific subject based) is granted a kind of flexible authority to access objects under certain define conditions

Security Architecture

Bell Lapadula Model

Basic is that this model describes how to manage “confidentiality” and “access control” of information/resources by subjects. It does not address “integrity or availability”, it only addresses confidentiality. Developed by DoD in 1970s

It explains method of “data confidentiality” mathematically meaning you need to envision the whole confidentiality model in terms of functions/states/properties (mathematics in mind)

Model is based on multilevel secuirty

Model is based on classification of data

Model is base do access control matrix

When you study this model, always recall “data classification” of government and private

Model describes that subject who is cleared at a certain level cannot access resources at a higher level, and also within the level it is cleared for, it can access resources only as “need to know” basis if that level is considered as “sensitive/classified”. If that cleared level of subject is “unclassified or public”, then it can access object/resources without need to know basis. This is to ensure that sensitive/classified info is protected even if subject is cleared to have access

Bell Lapadula and Lattice Based Access model work in parallel so we also need to understand basics of Lattice Based Access model

In Lattice Based Access model, objects are distributed in a kind of “lattice” where each level of lattice defines the level of importance/confidentiality of that data. Subjects are then placed within that Lattice and access to objects for those subjects is based on the location of that subject within Lattice. As per rule, Subject can access objects at higher level that are LUB (least upper bound) meaning closest to subject in upper direction) and can access objects at lower level that are GLB (Greatest Lower Bound) meaning closest to subject in lower direction). It means that it is very strict access model so for Private Org standard (Confidential, Proprietary, Private, Sensitive, Public), if subject is at Private and Sensitive, it can access only Private and Sensitive and not even Public, forget about higher!

Final Concept of Bell Lapadula is State Machine Concept

In this concept, treat the whole data confidentiality/access requirement as State Machine that has states, inputs, flow of data and then state changes due to inputs or flow of data

That State Machine has 3 Properties

Simple Security Property that states subject at a level cannot “read” from an object at higher level (that simple because object at higher level is at higher classified info and subject cant access). Simple = Read

Star (*) Security Property states that subject at a level cannot write to objects at lower level (this is very intelligent, because if subject at higher level can write at objects at lower then it has higher chance that data at higher level may be exposed to lower level) = Star (*) = Write

Discretionary Security Property states that subjects can access objects based on access matrix

So if we combine these Property with State Machine Model, then it means if our SYSTEM is following these Properties and State change is monitored then system will be secure for every state change. As notice, this model only talks about Confidentiality, and does not address Availability or Integrity

TABLE 8.1 An access control matrix

Subjects	Document file	Printer	Network folder share
Bob	Read	No Access	No Access
Mary	No Access	No Access	Read
Amanda	Read, Write	Print	No Access
Mark	Read, Write	Print	Read, Write
Kathryn	Read, Write	Print, Manage Print Queue	Read, Write, Execute
Colin	Read, Write, Change Permissions	Print, Manage Print Queue, Change Permissions	Read, Write, Execute, Change Permissions

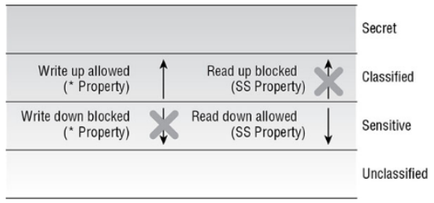


FIGURE 8.3 The Bell-LaPadula model

Biba Model

First things first, Biba model only looks at “data integrity”

Again based on State Machine Principle and Property

Property of Biba Model is invert of Bell Lapadula Model. (Biba was developed after Bell Lapadula)

Simple Integrity Prop states that subject at a level cannot read down at lower level (no-read-down)

Star (*) Integrity Model states that subject cannot write at an object at higher level (no-write-up)

Simple Integrity model is bit confusing, why subject at a level cannot read an object at a lower level, this is only to protect integrity (remember Biba Model is about integrity) so stopping reading at a lower level is actually preventing data contamination because subject can read at a lower level and then write at a lower level (that’s allowed) that has probability of data contamination!

Biba Model has limitations and critiques!

Does not define any process for access matrix (only integrity focus)

Address protection from external channels (no focus on Internal protection meaning encryption/hash etc)

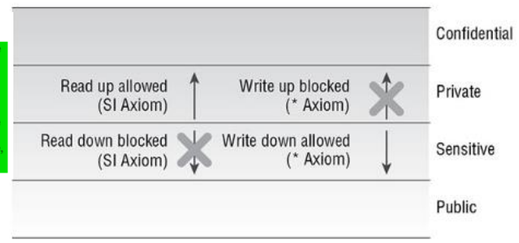
Core Focus of Biba Model was

Prevent unauthorized subjects

Prevent authorized subjects to make unauthorized changes

Keep object consistent

Figure 8.4 illustrates these Biba model axioms.



NOTE — Now we will discuss about Security Models

State Machine Model

In order to understand State Machine Model (or any other model for say), we first need to have a concept of FSM (Finite State Machine)

FSM is a model that has these components

- State (meaning state/condition of a system at the given instance of time)
- Transition (change of state from A to B)
  - Transition can happen when there is an input OR if there is a change in state due to an event within a system

Security State Machine Model states that every state of a system should be secure in order for that system to comply with Security State Machine Model, meaning every state of system is secure

Information Flow Model

This mode is also actually based on State Machine Model, with the fact that when information flows, state is bound to change

Bella Lapadula is State Machine and Biba model is State Machine + Information Flow are based on Information Flow (be discussed later)

So the basic concept is that flow of information is determined and controlled based on different security levels of objects and subjects and classification of those objects and subjects. Objective is to allow authorized access and information flow and block unauthorized, irrespective of fact that information flows within same security level or different level

Composition Theories – part of Information Flow model is Composition Theories in real world that defines the interaction between systems, not within systems. Meaning that information flow from one system gets to another system, that flow could be as data flow or an input so it means that systems are connected as “cascade” meaning that output from one system could be an input to another system. Any other such relevant design comes under Composition Theories

Non-Interference Model

This model is also actually based on Information Flow

The basic concept is non-interference between subjects of different security level operating on a system. Subject at a higher level should not impact on a subject at a lower level and vice versa. Any such interference can result in disruption or in security violation

If subject at higher security level interferes with subject @ lower security level then it can actually impact on the operation/working scenario of that lower security subject

Take-Grant Model

This mode defines how rights can be taken or removed from Subject to another subject or from subject to an object

Actually this is a mathematical function so we need to understand it in the form of function, where there is an input and then process/function and expected output. Take Grant model has also the same function!

It has 4 functions

- Grant — Subject can grant rights to an object/another subject
- Take — Subject can take rights from an object/another subject
- Create — Subject can create new rights
- remove — Subject can remove rights that were previously granted

Access Control Matrix

Whenever any one of this action happens, it is a “change”

So that change in that point of time defines “system security” at that time

So in essence this model deals with change at the time when any change has happened in executing rights of subject/object

This is a matrix table that is used by system to manage access between subjects and objects

Table has columns (tied to objects and showing what actions can be done on the object), called ACL

Table has rows (tied to subject and showing what each subject can do on every object), called Capabilities List

So access management based on subjects (capabilities list) is difficult because if we need t change access of every subject individually, then we need to go to each subject. However, if we need to change control of all subjects for specific object, we only need to change that object (ACL) that is easier

Finally REMEMBER that access to objects can be subject based (discretionary) and role based (mandatory, any subject in that role can have that right to access). If we need to show Role Based access then in Matrix Table, specific Subjects are replaced by Roles

Security Architecture

System Evaluation Criteria

Criteria based on which systems/computers can be evaluated for security & functionality

- In 1980s/by DoD — Trusted Computer System Evaluation Criteria — TCSEC
- In 1990s/by Europe — Information Technology Security Evaluation Criteria — ITSEC
- In 2005, by both, US and Europe — Common Criteria

These standard publications called Rainbow Series due to different cover colors of these publications

TCSEC Classification

TCSEC criteria classify the evaluation criteria in 4 classes that are (covered in Orange Book)!

- Class D (Minimal Control): This is the lowest. Anything that is not classified in any above criteria (B,C or A) is listed there. Class D system are not recommended for any data protection
- Class C (Discretionary Control): This emphasize on access control to system. Users must identify and then based on that identification, access is provided
- Class B (Mandatory Control): This also emphasize on access control to system, but it gives more granular tools to define subject/object access relationship. Class B evaluated systems can be used for securing classified data
- Class A (Verified Protection): This provides same level of assurance as Class B, however, Class A systems are those that built and designed from scratch considering required security parameters at every stage of development. Obviously they can also be used to protect classified data

TCSEC Redbook: Orange book discusses only standalone systems, Redbook discuss systems connected to networks

TCSEC Greenbook: Greenbook discuss about Password creation and management

TCSEC is outdated now!: Outdated because it only focuses on confidentiality and access control, and also it does not address specifically about how to implement that confidentiality, it only focus on defining guidelines/standards

ITSEC Criteria

ITSEC was Europe's equivalent of TCSEC

Establishes criteria for 2 items; assurance and functionality. Assurance to assure that system is secure at a certain level and functionality to validate that system is useable at a certain level

Basic difference between TCSEC and ITSEC is ITSEC focus not only on Confidentiality, but also on Integrity and Availability

TOE (Target of Evaluation), term used by ITSEC for any system that is required to be evaluated

Common Criteria (CC)

Built on coordination between all parties and then ISO standardized it as ISO 15408 document

Its objective was to:
- World wide standardize IT security products criteria
- Make easier for vendors to choose products based on evaluated ratings by CC
- To minimize efforts and duplication of work in order to evaluate IT security products

2 important elements of CC:
- Protection Profile: Its like wish list of items required by user to see as security in the product (what I want)
- Security Targets: These are the features that vendor will produce in a product (what I can give)

CC helps buyers/users to choose products based on level of evaluation as per CC

CC has evaluation levels (0 to 7): 0 is the least and 7 is max, these levels increase and show stricter standards growing from 1 (test only functionality), 2&3&4(test, verify and check functionality and method) and further 5&6&7 (test all above plus design and verify design) so this is in ascending order and increasing level of standard

Shortfall of CC: It does not address issues such as effect of behavior of data when user will act on it, also does not address specific security controls to be deployed for different protection mechanism, does not define method of how product would act if threat is issued. It solely focus on building/designing/ manufacturing the system, not on the under stress functionality

TABLE 8.4 Comparing security evaluation standards

TCSEC	ITSEC	CC description	
D	F-D+E0	EAL0, EAL1	Minimal/no protection
C1	F-C1+E1	EAL2	Discretionary security mechanisms
C2	F-C2+E2	EAL3	Controlled access protection
B1	F-B1+E3	EAL4	Labeled security protection
B2	F-B2+E4	EAL5	Structured security protection
B3	F-B3+E5	EAL6	Security domains
A1	F-B3+E6	EAL7	Verified security design

Clark Wilson Model

Also focus on data integrity

Based on relationship called Access Control Triple (or simply triple)

Basic concept is, Subject cannot access Object directly. It can access only through intermediary Portal/Interface/Program that has info about object's security labels and on the basis of these labels, it grants access for subject to objects

So Triple or Access Control Triple is a relationship between Subject/Program/Object or Subject/ Transaction/Object, transaction is here "an action" that resulted in action on object by Subject

4 terms that this model describes:
- Constrained Data Item (CDI): A data items that needs to be protected using this model
- Unconstrained Data Item (UDI): Data item that is not protected under this model. It can be invalidated input data (meaning data that is not validated as it is not covered under this model) or any output (because output is deliverable of function hence this model does not dictate how function can produce output)
- Transformation Procedure (TP): Procedures that are allowed to change CDI, Only TPs can modify CDI
- Integrity Verification Procedure (IVP): Procedure to check data integrity after TP has executed

Brewer Nash Model (Integrity Model)

Called Chinese Wall Model also

Based on managing access of subject to object dynamically and largely based on subject's activity in previous session

Also limiting subject's access to particular data object only when subject is operating on that object to avoid conflict of interest (meaning that minimizing chance that subject can temper or unwantedly alter data point in another conflicting database)

Because it creates a type of isolation hence it is called Chinese Wall!

Commercially, this model is used by consulting firms (consultant working with firm-A not allowed to access data for firm-B, when firm-A and B are competition to each other)

Goguen-Meseguer Model (Integrity Model)

This is a non-interference model, meaning that subjects at different level of access are kept isolated from each other's activity so that low privilege subject does not interfere with high privilege subject. Predermined Subjects will be allowed to access Predetermined Objects!

Sutherland Model

Is also Integrity Model!

Itself, doesn't define a specific process to achieve integrity

Instead define initial state, transition and final state. If states defined do not match with system behavior/changes, it means that integrity is compromised

Graham Denning Model

Defines "how to procedure" for creating, deleting and managing rights of subjects & objects

Defines 8 actions on which model is based:
- How to securely create object
- How to securely create subject
- How to securely delete object
- How to securely delete subject
- How to securely give grant access rights
- How to securely give delete access rights
- How to securely give transfer access rights
- How to securely give read access rights

Security Architecture

Security Capabilities of Information Systems

These are the capabilities of Information Systems that can be used to implement security

Memory Protection: It means that particular process is only allowed to access allotted segment of memory and no other! If this is not implemented then leakage on info/DOS attacks can happen (NOTE: Meltdown and Spectre is one attack that happened!)

Virtualization
- It enables operation of multiple Operating Systems within single piece of hardware. It logically means disengagement of OS from hardware so its like isolation of OS from rest of the hardware and errors/risks is localized

Trusted Platform Module (TPM) or Hardware Security Module (HSM)
- TPM is specification as well as a chip/hardware to implement/ save/process cryptographic keys for digital/signature/encryption
- TPM is actually HSM. HSM are independent hardware modules installed in a system to process/save cryptographic keys and encryption
- If full hard drive encryption is enabled, through use of TPM, then use must provide password/keys/ to access!

Interfaces
- Interface is actually "between faces" and these faces are application and user. So it is the capability to protect what user can see/access in an application
- So this is a tool/feature that is used to control access between application & users

Fault Tolerant
- It is the tolerance level to tolerate fault and recover if fault appears. RAID (disks)/backup power are all examples of Fault Tolerance

Few Other standards

PCI DSS
- Payment Card Industry Data Security Standard
- Focus on financial transaction security
- About networks/software/processing/storing/protecting of payment data

ISO
- Largest international standards org body. Publish standards, technical reports, guidelines and publicly available technical data/standards

Certification and Accreditation

These 2 processes are to test/evaluate a system and then accept the system for operational use

Certification means that every component of the system is tested and evaluated based on pre-set criteria (chosen by organization going to use that system) and all security controls (technical/non-technical/administrative/physical) are tested given under specific environment/condition/ configuration. If any one of these parameters change, then system needs to be re-certified because certification of the system is under specific conditions

After certification is completed, organization who is going to use the system need to formally approve and accepts it as per security guidelines of that organization. This is called accreditation. It is iterative process as during accreditation, organization may request changes in the system/controls that will then go again through certification. Once accredited, it means that org has accepted the specific system with defined controls/parameters and associated risk under specific conditions. Accreditation can be done by organization itself, however, mostly it is done by 3rd party and once done, it can remain valid for any entity who trust that 3rd party

Technical Terms for Accreditation
- DAA (Designated Approving Authority)
  - As per latest RMF (Risk Management Framework), DAA is called Authorization Approval (for internal accreditation) and Security Control Assessor (SCA) for external accreditation)

Current government standards for accreditation
- 2 current standards
- RMF that we already discussed earlier
- CNSSP (Committee for National System Security Policy)

Process steps for Accreditation

Both standard follow 4 steps for accreditation
- 1. Define (that involves creation of System Security Authorization Agreement (SSAA), the working document that sets base for accreditation to start and reach till end
- 2. Verification
- 3. Validation
- 4. Post Accreditation

Accreditation Types

Explains what type of accreditation is achievable
- 1. Site Accreditation
  - Systems and applications at specific site are accredited
- 2. Type Accreditation
  - Specific type of application/system is accredited so can be used anywhere
- 3. System Accreditation
  - Specific system or application is accredited

Security Architecture

Hardware Based Multistate System Protection

This is achieved through "protection mechanisms"

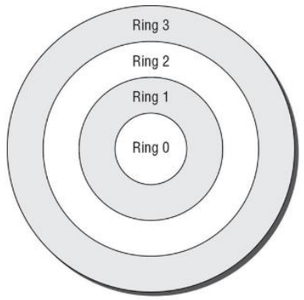
Protection Rings

This is a method to protect Operating System and its components in Multistate System

Concept is that OS and related other components of the system are divided in Rings (Ring 0 through 3) where Ring 0 is the highest priority/privilege and Ring 3 the least

- Has core of Operating System called Kernel — Ring 0
- Has all other remaining parts of OS — Ring 1
- Has drivers and IO peripherals access codes — Ring 2
- Has all users applications/programs — Ring 3

Every Ring has its allotted "memory location" and that location can be accessible by that ring or rings above that (Ring 1 can access Ring 2/3 location but not Ring 0)



Ring 0: OS Kernel/Memory (Resident Components)
Ring 1: Other OS Components
Ring 2: Drivers, Protocols, etc.
Ring 3: User-Level Programs and Applications

Rings 0–2 run in supervisory or privileged mode.
Ring 3 runs in user mode.

As computer runs several processes, so every component of particular ring has some processes associated that helps driving operation of components of that ring, Ring 0 processes has higher priority than Ring 1 and so on so forth!

So access of components between rings is controlled by "mediate access control" that checks and allows access

These access requests are checked and validated and then access is granted using a request system called "system requests or system call

So Protection Rings provides "isolation concept" between System mode (Ring 0 through 2) and User Mode (Ring 3). Modern computers also divides memory in 2 segments, system segment that runs in privilege mode and user segment that runs in user Mode

Process States

This is a method to schedule and control the execution of processes. Remember that processes run in a queue

These states define the treatment of a particular process and its state compared to other processes in the system

Process States of Operating System

OS runs in either 1 of 2 modes (Supervisory State-full privilege or Problem State

Supervisory state is full privilege state meaning that there is no user access right now and OS has nothing to decide and sitting with full access to resources

Problem State/Running State (User Mode), state where now user has requested something, process is started and process would like to either complete that request or wait for any other resources/timeslot for that process to get it completed if it is interrupted in the middle. Problem state is called such because this state is prone to problems due to "user request" nature/ interaction

Process States for Users

- Ready – the process is just ready to be running
- Waiting – process is halted and waiting for some input or interrupt for it to be completed
- Stopped: Process is stopped coz its completed or terminated
- Running/Problem State: the process is running now
- Supervisory State: user needs to perform an action that require higher privileges that user has so process must check eligibility and then run in Supervisory State

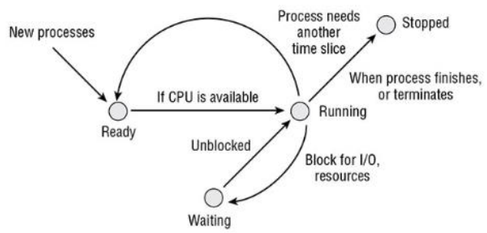


FIGURE 9.2 The process scheduler

This chapter starts with Computer Architecture and its basic components

- Hardware — Component that can be touched/tangible e.g hard drive (obviously not data inside hard drive!)
- Processor — Brain of computer. Processes every function on computer (bits & bytes). However, this is the responsibility of Operating System to provide info to processor after compiling this info in a language understandable by processor. This info comes from Applications (programs) that we run. So applications are built in high level language, processor understands low level language (such as assembly) so OS & Compilers takes info from Applications and translate them for Processor

This above steps leaves processor to process at glazing speed and leave rest of stuff to OS

Processor Execution Terminology

- Multi Tasking — Single Processor juggling between multiple tasks as same time, however, doing actually 1 task at a time but juggling
- Multi Core Processor — 1 Processor Chip having multiple Cores (meaning Processing Unit). Modern computers are all Multicore
- Multiprocessing — Multiple processors processing at same time (simultaneously, not juggling)

Symmetric Multiprocessing (SMP), in this, multiple Processors share same OS and data bus (transfer link from OS to processor), example is Database query in a server, where OS of server balances that query among multiple processors, each one working at the same time

Massively Parallel Processing (MPP), in this, there are again many multiple processors but each one with its own OS, so its like multiple computer acting at once. In this model, main OS assigns task to one specific CPU for computationally heavy application, then that CPU further sub-assign that task to multiple CPUs, get the result and then each CPU reverts back to that 1st CPU so only 1 CPU is leading for 1 request but distributing to other CPUs

MPP is required by very intensive applications (engineering/mathematics etc)

- Multi Programming — Its bit similar like Multi Tasking

SO example with single processor and OS, you may run 2 programs at the same time, when one program waits for an input (say from user) 2nd program can start executing, while 1st stay tuned, waiting for input from user. Then once 1st program gets input, it starts working and 2nd program goes in standby. This is how it works. It is beneficial only when multiple programs run and all would like to get similar treatment. Its anyhow old technology now

- Multi Threading

Thread is a series of instructions actually that operates between CPU and Process, while process is come into being when any application/program is executed and then OS takes control of that program and assigns it space in memory. So threads run between process and CPU to instruct CPU what to do or in return CPU tells Process what to do. This is managed by OS

So Multi Threading means that using single process, multiple tasks can be completed because of multi threading (sending multiple instructions from process to CPU & vice versa). Eg single process of word though you open multiple word documents!

So understand as "ability to send multiple instructions at the same time to processors to execute"

Processing Types

Here it is referred specifically to "data processing types" meaning if there are different types of data (as per data classification secret, top secret etc.) then how would that be processed to assure integrity and confidentiality. Here see how computer system processing helps to implement it

2 methods actually, 1st is Policy Based (called Single State) and 2nd is Hardware Based (called Multistate)

Policy Based (Single State) is simple! Computer system will be limited to access only 1 type of data (say top secret). Administrator now needs to make sure that only users with Top Secret clearance can access that system. This is policy based processing!

Hardware Based (Multistate) is complicated! In this, one particular system will be handling multiple types of data (secret, top secret, confidential etc) at same time. The protection between them must be built by implementing Hardware based configs/policy. On left side now, we will see how this Hardware Based protection is achieved! (these types of system are quite expensive and used only when really high processing is required for multiple types of data, then rather than using multiple system, one system is acquired and hardware based protection is implemented)

Security Architecture

Operating Modes of Computer

Always operates in either of 2 modes, USER mode OR SUPERVISOR/SYSTEM/ KERNEL/PRIVILEGE mode

USER Mode

ALL users application (even administrator run) are executed in this mode

CPU gives access to its limited instructions set to OS so that OS can run a process for user application

Each User Applications run in its own "virtualized" environment where that environment has its own isolated memory space

SUPERVISOR/ SYSTEM/KERNEL/ PRIVILEGE MODE

CPU opens its all Instructions Set for OS

OS runs only those processes in this mode that are "system" process, not any user process

If any User Application wants access to system process, Kernel/supervisor manages that request, BUT never allow user process to run in this mode

Primary Memory (mean memory readily accessible to CPU to process)

Computers have several types of Primary Memory

ROM (Read Only)

Only reading, no writing. Non Volatile

Contains Bootstrap and basic drivers, system use it load initially at bootup

In basic ROM, bootstrap is loaded by manufacturer, user cant change/alter

Various type of ROM

Manufacturer keeps it empty, so user can load program/software it, once loaded then user cant change!

PROM (Programmable ROM)

More flexibility, PROM can be erased and reprogrammed!

EPROM (Erasable PROM)

EEPROM (Electrically EPROM)

UVEPROM (Ultra Violet EPROM)

RAM (Random Access Memory

Volatile Memory. Read & Write

Temporary storage for quick access to achieve faster processing

Different types of RAM

Primary Memory/Real Memory; hardware chip with multiple memory storage. CPU needs to refresh for optimized usage

Cache RAM; present directly on the component e.g CPU/ Printer for really quick access/processing. On printer, helps to process print jobs independently without CPU assistance every time print is required

Dynamic RAM v/s Static RAM, classification based on how RAM keeps data. Dynamic RAM needs refresh from CPU periodicaly as data is saved using capacitors that may loose charge and needs review; Static RAM doesn't need that and old data can simply be rewritten for usage

Registers

This is very fast and readily accessible small memory on the CPU itself

Secondary Memory

Not readily available to CPU to access!

Hard Drive/Flash Drive/ CD/DVD are examples

Virtual Memory

Artificial way to represent RAM

Previously used, but not recently used, data from RAM is moved to any Secondary Memory. That data is called Page File and process is called paging

When CPU needs it, it asks for it! Its slow however, compared to the speed at RAM operates, but its cheaper

Memory Addressing

CPU needs to access different memory locations (using memory address) to process instructions

- Register Address: Memory address for data on the register
- Immediate Address: Memory address of data on any memory location along with data instructions (e.g add 2 to data at memory address A
- Direct Address: Memory address of data on any memory (except Register)
- Indirect Address: Reference to memory address of data on any memory
- Base + Offset Address: Memory address of data on the memory explained by memory location + offset

Memory Security Issues

Key issues for Memory Security are

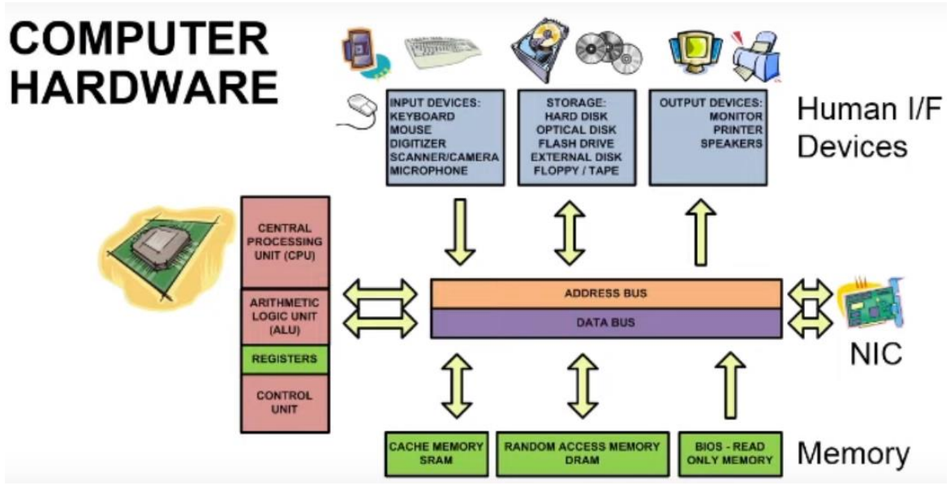
- Leakage of data from one memory location to another while processes are running
- Data Residual or Permanent data saved either in volatile or non-volatile memory

Computer System Access Security Modes as per US Government, read from Wikipedia, better explanation is there!

	Security Clearance	Data Access Clearance	Data Need to Know Clearance
Dedicated Mode	For all users, for all data	For all users, for all data	For all users, for all data
System High	For all users, for all data	For all users, for all data	For all users, only for data they are required to access
Compartment Mode	For all users, for all data	For all users, only for data they are required to access	For all users, only for data they are required to access
Multilevel Mode	Some users may not have valid clearance for all data	Users must have for data they are required to access	Users must have for data they are required to access

It defines access for users based on users security clearance and access level

Briefly, how computer systems work?

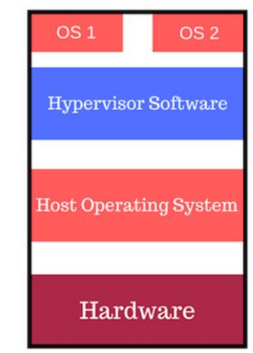


So that's the simple computer architecture

- Human I/F Devices: That's how we human interface with computer, we talk to computer
- Address Bus & Data Bus: Address Bus that transports address of memory where "data" is stored
- Memory: Data bus is a "track" where data travels within computer
  - Cache Memory: Small memory to assist CPU to store limited data for time being
  - Random Access (RAM): Larger than Cache, that stores quick accessible items required by CPU and others, while processes are running
  - BIOS (Basic Input/Output): Read Only, small memory used when system boots up to load basic drivers and bit of OS so that system can start kickin!
- Left (Processing Part: Brain of computer, that's where instructions are processed and delivered
  - It has "Registers", very small but extremely fast accessible memory (like writing registers) that CPU can use
- NIC: Interface that connects computer to Network!
- Execution Steps: Action comes from Human I/F, That uses or access any application/program, OS takes that request and converts it to Process and assigns a place in Memory for that process, the Process is then executed by CPU that works on process by giving Threads (instructions) to its components what to do, the output from CPU resulted in Output Devices understandable by us Human!

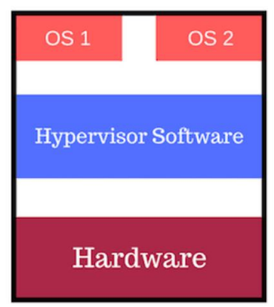
Security Architecture

- Database, its components and related security
  - Database security is extremely important. Specific terms related to database security
- Aggregation
  - Meaning to conclude a upper level unauthorized result by applying mathematical aggregation function to available lower level data
- Inference
  - Meaning concluding unavailable & unauthorized result by using human inference/common sense & access to available data
- Control for above 2
  - Is to have strict access control, monitoring and analyzing audit results
- Data Warehouse
  - Extremely large raw volume of data that records historical trends. Not accessible for current use and hence saved in warehouse
- Data Dictionary
  - Data knowledge base that defines data set with its attributes (type, usage, format etc)
- Data Mining
  - Outcome in the shape of concentrated data, after brushing through Data Warehouse. Crux of interested data!
- Metadata
  - Is data about data, meaning data that gives information/reference about other data. This is more secure than data and hence saved in a separate location than warehouse, called DataMart. Metadata is more specific!
- Data Analytics
  - Is analytical view and then extraction of required information from metadata or raw data, whichever is available and accessible. With extremely large amounts of data now, it is not possible to conduct data analysis with standard tools; high power machines & processing is required!
- Big Data
  - General name given to extremely large volume of data along with its attributes that defines that data. Analysis of Big Data is executed through Massive Parallel Processing
- Large Scale Parallel Data Processing
  - Big Data processing requires Large Scale Parallel Data Processing that can be subdivided as below
  - Asymmetric Multiprocessing
    - Multiple processors with their own OS and data to process
  - In Massive Parallel Processing, several Asymmetric Processing works in conjunction to process a specific set of data
  - Next processing platform for Big Data would be Cloud Computing, peer-to-peer computing or grid computing
- Distributed Network Architecture and End Point Security
  - Network Design is evolved from terminal/host design (where all services, processes and data was available at a particular terminal) to client-server design (where clients have their own local data/processes as well as access to centralized resources at a server)
  - It implies security consideration at several points, including servers, network, desktops, laptops, mobiles and tablets. Considerations like policies, procedures, controls, backups, auditing, analysis, training, detection, prevention etc. Don't loose any point in the network, it should end to end holistic approach with multilayer security called defense in depth!
- Cloud Based Systems, Storage & Computing
  - Cloud Services is a concept that storage and processing of data/application is done in cloud, and not locally. Concept of virtualization!
  - Concepts related to Cloud Systems
  - Hypervisor is a component (a software program actually) in virtualization to create & manage virtual machines. 2 main type
  - Type-1 Hypervisor
    - Type where Hypervisor is installed directly on the hardware that needs to act as Virtual System. Once HV is installed, it can then create Virtual Machines. Hypervisor will be called Host OS and Virtual Machines will be called Guest OS. Good for Virtual Servers
  - Type-2 Hypervisor
    - Type where Hypervisor is installed on the standard operating system already installed in the computer. Once HV is installed, it can then create Virtual Machines. Standard Operating System will be called Host OS and Virtual Machines will be called Guest OS. Good for Desktop machines



Standard Hosting Architectur

Type-2 Hypervisor



Bare Metal With Hypervisor

Type-1 Hypervisor

- Storage Devices
  - Have same concept as Memory. By definition, Memory is a data itself, while Storage Device is a piece of hardware where that memory is stored!
- Random and Sequential Storage Devices
  - In Random storage (RAM/DVDs/CDs), CPU access data at any memory address and start reading, without reading through all data before that! Its easy, fast and flexible
  - In Sequential Storage, CPU need to read through all, before reaching its desired location. It is slow but inexpensive and large memory, e.g Magnetic Tapes used for colleting backups
- Security Concern for Secondary Storage devices
  - Storage devices must be properly sanitized because of data remnance
  - Physically must be secure
  - Strict Access Control must be in place
- Security Concerns related to I/O Devices
  - Monitor; rays can be collected and data in display can be read. TAMPEST technology by US Security Agency has this technology! Shoulder spying is still biggest threat!
  - Printer; susceptible to physical and spy attacks
  - Key Board and Mouse: Susceptible to interference and spy attack!
  - Modems: very vulnerable for network attacks and data expose to outside world
- Firmware
  - Also called Microcode! Minimum basic instructions and drivers to load the system at startup
  - 2 types of Firmware
    - 1st i.e installed on the Computer Machine, its called BIOS and more recently UEFI (Unified Extensible Firmware Interface
    - 2nd i.e installed on the device (printer/scanner) itself to offload work from OS to device
- Client Based Systems (Summary & Security)
  - Client Based Systems are also target for attacks, not only Server!
  - 2 vulnerable components that are!
  - Applets are programs/applications hosted and then sent by Server **to** clients to operate on clients machine & execute specific task. This helps to offload task from Server to client. Poses risk as Applets can contain Trojan without client's knowledge. Applets are outdated, though still supported, 2 types are common!
  - 1. Java Applet (from Sun/Oracle), OS independent so client downloads Java Virtual Machine (JVM) and then execute Java Applet independent of client OS. Sun/Oracle produces Sandboxing so that applet cannot access any other memory location
  - 2. ActiveX, Microsoft equivalent of Java. Only runs on Microsoft Machines and does not offer Sandboxing so not that flexible and secure as Java!
  - Local Cache Attack & Vulnerability for Clients
    - Local Cache is available in clients and vulnerable to attack. 3 caches needs attention!
    - ARP cache, if poisoned, can result in man-in-the-middle attack
    - DNS Cache can also result in man-in-the-middle attack. For internal traffic, only Internal DNS Server should be considered and any traffic to DNS port 53 should be monitored
    - Local Internet Cache is susceptible by attackers to send Trojan Horse script into local machines
- Quick note for Server Based Systems
  - Data Flow and its proper management is critical for server based systems. It can be managed through load balancing. Constant monitoring and logging is required for stable servers

Security Architecture

5th, 6th & 7th Vulnerability

- XML Injection, XSS (Cross Site Scripting) and XSRF (Cross Site Request Forgery)
- XML Injection/exploitation, meaning send false information to visitor of website or steal their information for login
- XSS is loading malicious script in web server such that it is transferred to other users when they login to same web server
- XSRF, similar to XSS, but targets browser of another user (not the web server itself) and forge user information such that user is not aware and then uses that info to login (say bank accounts and steal money). Mitigation is web server patch, double authentication, traffic monitoring

Vulnerability and Security in Mobile Devices

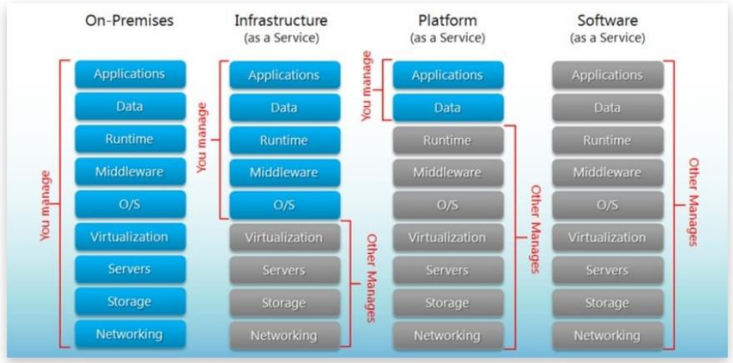
- Any personal portable device is Mobile Device that can be used for security break and are vulnerable
- Android
  - Linux based open platform OS for mobile devices
  - Vulnerable to get to root access by attacker, can be mitigated by installing some secure apps.
- iOS
  - Apple OS, vulnerable to jail brake, meaning root access/low level config
- Remote Wiping
  - Option to remotely wipe/delete data
- Screen Locks
  - Note that Screen Locks can also be opened by NFC (Near Field Communication)
- Storage Segmentation
  - Feature to segment personal and professional data in a phone
- Mobile Device Management
  - Can assist in implementing policy and analyze devices config/logs
- On-The-Go (OTG) Cable
  - That is required to connected mobile device with external storage (eg USB). Security Risk!
- Application Security
  - Securing apps in mobile devices is as important as securing device itself. Related concepts are;
- Key Management
  - For encryption is a challenge, mobile devices doesn't have TPM normally
- Geo Tagging can locate movement, better to disable it!
- BYOD (devices & policy)
  - BYOD has security concerns so there are alternatives
  - COPE (Company Owned, Personally Enabled), owned by company so can give standard compliant device
  - CYOD (Choose Your Own Device) company approved list of devices and you can choose
  - VDI (Virtual Desktop Interface), virtual interface physically on a server that users can access from mobile through independent network
- Core Statement
  - Mobile Device Policy/BYOD Policy should be comprehensive enough to address concerns related to security, data management, AUP and other operational tasks in detail and personnel must give their consent

Concept of Embedded Devices and Cyber Physical

- Embedded Devices are those that have built-in processor/controller that performs device functions (like smart TV, smart vehicle)
- Cyber Physical
  - Computational devices that control physical movement/action in real world (robotics, sensors etc)
- Static System definition
  - Systems that do not change by themselves once manufacturer has built & defines their specific purpose (smart TV decoders, old vehicle controllers)
- Securing Methods
  - Traffic & Network Segmentation
    - Segment traffic & network
  - Firewalls
    - Application & Network
  - Patches/Firmware Updates
    - Preferably manual due to static nature of devices
  - Wrapping (I like this term!
    - Meaning encapsulation simply, before upgrading firmware/patch, wrap it to better protect

Cloud Services

- Software as a Service
  - Didn't need to manage anything, the final software is provided as a service
- Platform as a Service
  - You need to manage your applications
- Infrastructure as a Service
  - You need to manage your applications and any related data or software
- On-Premise
  - You own everything & manage it



- Security for Cloud Services is a concern since your data is hosted and even managed in some cases by 3rd party

Cloud Services Deployment Models/ Classes

- Private Cloud
  - Enterprise cloud services not going through Internet. Simply like Enterprise transfers its servers/services to cloud with Intranet access
- Public Cloud
  - General public cloud, accessible through Internet
- Hybrid Cloud
  - Design where enterprise has Private Cloud for its employees, but then also have Public Cloud for partners/vendors etc.
- Community Cloud
  - Cloud services for certain community to access & share

Cloud Services related concepts

- Cloud Access Security Broker (CASB)
  - Company that provides secure access to the cloud for an enterprise

Security while using cloud services

- Security as a Service (SECaaS)
  - In cloud services deployment, security offered for Intrusion detection, traffic monitoring etc. This services is focused mostly on deploying software at end clients and does not involved hardware within organization
- A big concern, areas such as Disaster Recovery, organization security policy implementation, compliance with regulations, all 3 CIA items, network tapping, man in the middle

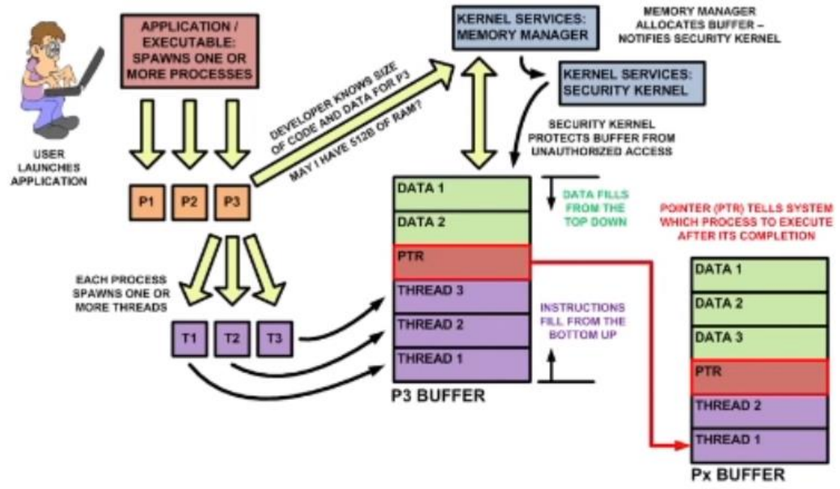
2 more Computing Models

- Grid Computing
  - Like large network of computers performing specific functions with coherent approach to get to specific outcome. Computers are distributed very largely geographically. Once they complete the task, report to central server that collects the result and unify it with other results
  - Security concerns are much higher with all three elements of CIA affected
- Peer to Peer
  - P2P model where operation and task is conducted between 2 networking end points only (Skype is P2P). Security is a concern as can affect availability with high usage and confidentiality by traversing traffic through P2P tunnel

Vulnerabilities in Web Based System

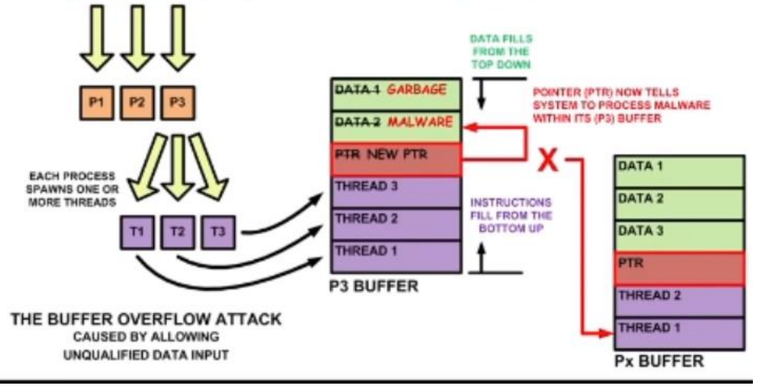
- Web Based Systems are those that on front end offer Websites/http access and at backend have servers/database that serve particular user/applications. Typical eg Online Bank account
- 1st vulnerability is SQL injection that through the use of web page, attacker inject SQL code that can corrupt/give access to backend database connected with web front. Mitigation is to check for metacharacters (#!|^ etc) that has special programming meaning. It is also called Input Validation
- 2nd and 3rd are LDAP Injection and XML injection, both inject codes, but target other servers behind web, not specifically database. Mitigation is Input Validation
- 4th is Directory Traversal, attacker can gain access to a different directory/file system on a web server, rather than Web Root on which it lands by default. Check for input characters & filter text

PROCESSES AND BUFFERS



THE BUFFER OVERFLOW ATTACK

- Caused by improperly validating buffer input
- Could be avoided!



Security Architecture

- Security Implementation Components for Computer System
  - Layering: Creating different access and privilege levels for processes with logical layers
  - Abstraction: Posing simplified view or hiding details that users/subject doesn't need to know to perform its job
  - Data Hiding: Hiding data available to 1 layer from another layer based on privilege/access level
  - Process Isolation: Isolate Processes from each other; separate memory space, even with separate virtual machines within a computer
  - Hardware Segmentation: Though expensive and rare to see, complete physical isolation is also possible
- Architectural & Design Flaws
  - Flaws that are during design/creation of computer system/OS
  - Covert Channels: Secret communication channel that doesn't use normal data path for communication and hence remains undetected. Created due to flaw in programming code
  - Backdoors: Unintentionally left open doors to enter into OS while developing OS
  - Maintenance Hooks/Doors: Intentional backdoor left to leave a channel to circumvent access control in case if all access are lost
  - Absence of Trusted Recovery: In case of system crash, while system is recovering, it ensures that security doors remain intact. If trusted recovery is absence, can introduce security risk
  - Buffer Overflow: Very common! when developer doesn't define expected amount of data that program/OS can take within a Task, it can then produce buffer overflow (more than required data is entered in a Task, risky!
  - Data Diddling or Salami/Slow Attacks: Refers to attacks that take place slowly, unnoticeable slight changes, takes day by day. Salami is variation where attacker executes minor financial transaction takes place
  - TOCTOU Attacks: TOC is Time of Check and TOU is Time of Use. There is a slight (nanosec) time difference between TOC (object is checked) and TOU (object is used on), within that small variation, attacker can penetrate
  - EM (Electromagnetic Radiation): Risk is to recreate key strokes/data from electromagnetic radiation, solution is Faraday cage (cage protects EM)

Security Architecture

Evidence Storage
- Specific storage to save/preserve IT evidences (logs, screen shots, snap shots etc)
- Hash and Encrypt evidences in storage to make sure their integrity (evidence need to be preserved!)

Concept of Work Area Division/Security
- Concept/method is called Sensitive Compartmented Information Facility (SCIF)
- Divide work areas based on its sensitivity level & grants access to individuals accordingly

Electric Circuit Protection
- Clean stable power is required
- UPS can be used, 2 types of UPS
  - Standard UPS that takes main supply, passed through battery, then from battery release power out
  - Line Interactive UPS takes power from main, then go through stabilizer, then to equipment (battery is not in path in main, if there is outage, then batter will supply!

Specific terms related to Electric Circuits
- Brownout (constant low voltage)
- Sag (temporary low voltage)
- Surge (constant high current)
- Spike (temporary high current)

RFI/EM(Radio Frequency/ Electromagnetic Interference)
- Due to RF transmissions, electric circuits
- When electric voltage varies between Live and Ground or Live and Neutral

Noise (ref is Electric Noise)

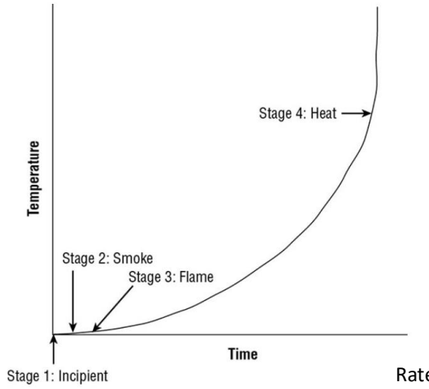
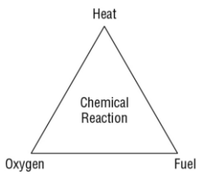


TABLE 10.2 Fire extinguisher classes

Class	Type	Suppression material
A	Common combustibles	Water, soda acid (a dry powder or liquid chemical)
B	Liquids	CO_2, halon*, soda acid
C	Electrical	CO_2, halon*
D	Metal	Dry powder

* Halon or an EPA-approved halon substitute



4 elements of fire and fire stages

Fire Detection Systems
- Fixed Temperatures Sensors sense configured fixed temperature
- Rate of temperature rise extinguisher, sense rate of temperature change
- Smoke Detectors detect smoke

Fire Types and Extinguisher

Fire Extinguisher Systems
- 1. Water Based, most suitable is Pre-Fire System that uses water, along with pressurized gas
- 2. Gas Based, it is Halon/CO_2 or its derivatives, that reduces Oxygen. Not suitable for human environment, also Halon is not ozone friendly. Now its derivatives are used

Physical Security Elements

Perimeter Security
- Around the building
  - Lighting, fence, security guards, dogs, mantraps, turnstiles are key elements
  - Mutiple layers of physical security preferred (lights + guards for e.g)
  - Delay Feature is an attribute that if intruder is not authorized, entrance will be locked for a duration until police/guards arrives to handle with Intruder

Electronic Access Locks
- Have electromagnetic locks + card reader identify the pin code

Motion Detectors and their generated alarms
- Motion detectors (infrared, photoetectric,wavebased) generates alarm when notice abnormal motion
- Deterrent alarms (lock the doors), repellent alarms (make sound, turn on lights), notification alarms send message to guards

Secure Facility
- Physical Facility is focus here!
- Critical Path Analysis
  - Analysis to identify items/elements interdependent to achieve secure facility design, it must be planned!
  - Identify threats here that can cause harm!
- Site Selection
  - Choose physical site that is safe, consider all relevant elements that can affect site's physical security
- Physical security is 1st line of defense
- Visibility
  - Considering visibility close to location is also important!
- Other items are surrounding area, weather hazards, people hazards, fire/theft etc.

Security Controls for Site and Facility
- 3 main types of control for physical security as well
  - Administrative
    - Policies/training
  - Technical
    - Camera, motion sensors
  - Physical
    - Gates & locks
- Physical Control selection criteria in order
  - Deterrent (discourage intruder)
  - Deny (deny intruder's access to control)
  - Detect (if deny doesn't work, then detect intruder, where he is?
  - Delay (keep delaying intruder so that security staff can stop)
- Equipment Failure also comes under physical control
  - Equipment support in case of failure and redundancy should be considered
  - Terms to look (MTBF Mean Time between failure and MTTR Mean time to Repair and MTTF Mean Time To Failure (equipment life) actually
- Cable Distribution System/Wiring Closet
  - All terms are standard, 1 term that is Horizontal Cable Distribution System is wiring scheme to serve individual apartments/offices on a floor i.e horizontally!

Note about Data Centre and Server Rooms
- Data Centre/server room walls should be at least 1 hour fire resistant

Access Control Cards
- Smart Cards (also called ISO 7816 interface card)
  - Have integrated chip that can save and process small data. It has magnetic field so is processed when it gets in contact with electrical field/magnetic field
- Memory Card
  - Its bank card, it has memory chip to retain some basic info
- Proximity Reader
  - This has 2 components, reader and passive card, when card comes close to reader, it disturbs magnetic field and hence reader manages authorization

Intrusion Detection Systems
- Remember that Security Guards are also considered as IDS system (after all they can detect intrusion!
- Physical IDS has 2 main components; detector and alarm, both must work, along with communication path to alarm!

Access Abuse
- Masquerading
  - Using someone's else ID to access
- Piggybacking
  - Accessing with/behind someone else bypassing security

Electromagnetic (EM) Radiation Security
- Also called Emanation Security. Emanation is general term for EM radiation!
- Protection is generally under umbrella of Tampest (government standard/ study for EM protection)
- Faraday Cage – method to block legible radiations to go outside so that hackers cant intercept them
- White Noise – deliberately generated noise to protect legible signals

Media Storage Protection
- Control Zone, same concept as protection, within a specific boundary
- Hackers can intercept EM radiation to extract legible information
- Storage where media (hard drives, disks, tapes etc) are saved
- Concept of media library is important, place where media is all held and then audited and tracked
- Zeroisation process is important, when reusable media is retuned back, it should be sanitized and zeroid (meaning rewrite media with garbage 0000)

Network Security

TCP Wrapper — Software based basic firewall/ACL that filters traffic based on port#, user IDs, systems IDs

TCP Acknowledgement — In TCP session, sender keeps on sending segments to receiver, until receiver replies with acknowledgement having last seq # segment received, this tells sender what last seq# is received by receiver. Number of packets sent by sender before receiving any acknowledgement from receiver is called Window S

Smurf Attack — Broadcast Ping

Ping of Death — Ping of very high packet size to crush the system

FTP & TFTP Difference — FTP is TCP Port 20 (for data transfer) & 21 (for control). FTP supports authentication/TFTP UDP port 69 does not require authentication

POP3, TCP port 110. pulls email message from email server and traverse to email client

IMAP (TCP Port 143), more secure than POP3, does same things as POP, however you can also delete message directly from server without downloading to client!

DHCP, UDP port 67 and 68

LPD Line Print Daemon to send prints to printer, TCP port 515

- *Top-level domain (TLD)*—The `com` in www.google.com
- *Registered domain name*—The `google` in www.google.com
- *Subdomain(s)* or *hostname*—The `www` in www.google.com

Every registered domain name has an assigned authoritative name server. The *primary authoritative name server* hosts the original zone file for the domain. *Secondary authoritative name servers* can be used to host read-only copies of the zone file. A *zone file* is the collection of *resource records* or details about the specific domain.

When client send DNS query, it includes Query ID (QID), the response back from server must also include that Query ID, if not then client will ignore that response. In DNS spoofing attack, attacker must include correct QID in response

Resource Records Example

Record	Type	Description
A	Address record	Links an FQDN to an IPv4 address
AAAA	Address record	Links an FQDN to an IPv6 address
PTR	Pointer record	Links an IP address to a FQDN (for reverse lookups)
CNAME	Canonical name	Links an FQDN alias to another FQDN
MX	Mail exchange	Links a mail- and messaging-related FQDN to an IP address
NS	Name server record	Designates the FQDN and IP address of an authorized name server
SOA	Start of authority record	Specifies authoritative information about the zone file, such as primary name server, serial number, time-outs, and refresh intervals

Wireless Access Implementation 2 modes

Ad-Hoc mode, 2 wireless access devices can communicate directly (laptop to laptop

Infrastructure Mode, wireless access devices must communicate through WAP. This is recommended mode

Concept of SSID

SSID is not wireless network name. It is Service Set Identifier meaning identifying either a network or hardware

ESSID is Extended SSID identifies wireless network in which more than 1 WAPs are used, BSSID is Basic SSID that identifies that hardware WAP (MAC address) is that is used within ESSID

Wireless Networks announce their SSIDs frequently using beacon frame, rather than disable this announcement to tackle threat, use WPA

WEP & WPA

WEP is weak (uses TKIP), uses same key with all hosts and WAP

WPA negotiates dynamic key with every wireless user to be used with WAP

However WPA uses single pass phrase to connect/authorize 1st time with WAP and this can be dangerous

WPA2 is 802.11i (WPA2 is not related to WPA, in fact they are different technologies!) WPA2 uses Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), AES 128bit encryption

Guidelines for Wireless Network Security — Treat WAP as external network and blocks its access using firewall!

The WEP protocol uses the RC4 algorithm

The 802.11i standard can be understood as three main components in two specific layers. The lower layer contains the improved encryption algorithms and techniques (TKIP and CCMP), while the layer that resides on top of it contains 802.1X. They work together to provide more layers of protection than the original 802.11 standard.

OSI Layers — Layers communicate with above & below layer, as well as peer layer, simultaneously

Layers & data representation

Application	Protocol data unit (PDU)
Presentation	Protocol data unit (PDU)
Session	Protocol data unit (PDU)
Transport	Segment (TCP)/Datagram (UDP)
Network	Packet
Data Link	Frame
Physical	Bits

Layer 2 Protocol

- Serial Line Internet Protocol (SLIP)
- Point-to-Point Protocol (PPP)
- Address Resolution Protocol (ARP)
- Layer 2 Forwarding (L2F)
- Layer 2 Tunneling Protocol (L2TP)
- Point-to-Point Tunneling Protocol (PPTP)
- Integrated Services Digital Network (ISDN)

Layer 3 — Manages data errors aka traffic control as well

Transport Layer — Gets PDU from Session Layer and then creates Segment. L4 creates session between peers and define session parameters such as data size, window size etc.

Transport Layer Protocols

- User Datagram Protocol (UDP)
- Sequenced Packet Exchange (SPX)
- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)

Session Layer Protocols — Establish, manages communication session between 2 end computers, dialogue control (duplex, half duplex, full duplex)

- Network File System (NFS)
- Structured Query Language (SQL)
- Remote Procedure Call (RPC)

NFS TCP Port 2049

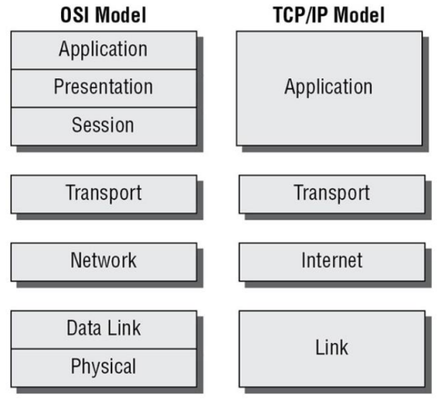
Presentation Layer Formats — Presentation layers also does encryption and compression

- American Standard Code for Information Interchange (ASCII)
- Extended Binary-Coded Decimal Interchange Mode (EBCDICM)
- Tagged Image File Format (TIFF)
- Joint Photographic Experts Group (JPEG)
- Moving Picture Experts Group (MPEG)
- Musical Instrument Digital Interface (MIDI)

Application Layer — This layer interface between Application and Protocol Stack

An Application itself is not located at this layer, rather, the protocols support that application, are located in this layer

- Line Print Daemon (LPD)
- Simple Mail Transfer Protocol (SMTP)
- Telnet
- Trivial File Transfer Protocol (TFTP)
- Electronic Data Interchange (EDI)
- Post Office Protocol version 3 (POP3)
- Internet Message Access Protocol (IMAP)
- Simple Network Management Protocol (SNMP)
- Network News Transport Protocol (NNTP)
- Secure Remote Procedure Call (S-RPC)
- Hypertext Transfer Protocol (HTTP)
- File Transfer Protocol (FTP)



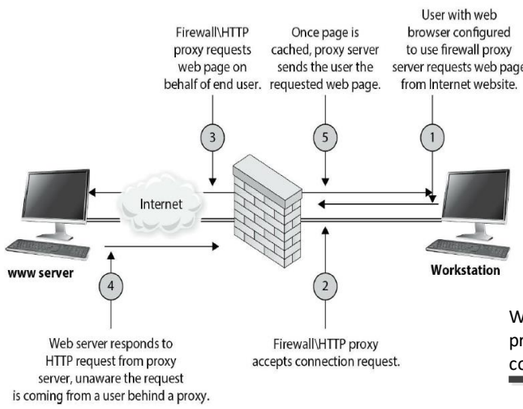


Figure 4-52 Proxy firewall breaks connection

Proxy Firewall

Application-Level Proxy Firewalls

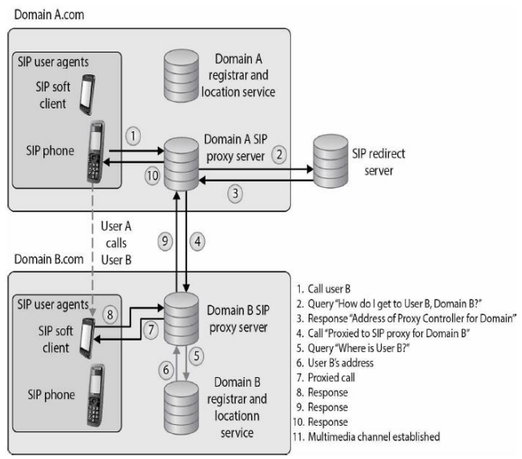
Application-level proxy firewalls, like all technologies, have their pros and cons. It is important to fully understand all characteristics of this type of firewall before purchasing and deploying this type of solution.

Characteristics of application-level proxy firewalls:

- They have extensive logging capabilities due to the firewall being able to examine the entire network packet rather than just the network addresses and ports.
- They are capable of authenticating users directly, as opposed to packet-filtering firewalls and stateful-inspection firewalls, which can usually only carry out system authentication.
- Since they are not simply layer 3 devices, they can address spoofing attacks and other sophisticated attacks.

Disadvantages of using application-level proxy firewalls:

- They are not generally well suited to high-bandwidth or real-time applications.
- They tend to be limited in terms of support for new network applications and protocols.
- They create performance issues because of the necessary per-packet processing requirements.



SIP Network

Stateful-Inspection Firewall Characteristics

The following lists some important characteristics of a stateful-inspection firewall:

- Maintains a state table that tracks each and every communication session
- Provides a high degree of security and does not introduce the performance hit that application proxy firewalls introduce
- Is scalable and transparent to users
- Provides data for tracking connectionless protocols such as UDP and ICMP
- Stores and updates the state and context of the data within the packets

Where a circuit-level proxy only has insight up to the session layer, an application-level proxy understands the packet as a whole and can make access decisions based on the content of the packets.

Kernel proxy firewalls are faster than application-level proxy firewalls because all of the inspection and processing takes place in the kernel and does not need to be passed up to a higher software layer in the operating system.

The use of secure cryptographic protocols such as TLS ensures that all SIP packets are conveyed within an encrypted and secure tunnel

Extensible Authentication Protocol (EAP) is also supported by PPP. Actually, EAP is not a specific authentication protocol as are PAP and CHAP. Instead, it provides a framework to enable many types of authentication techniques to be used when establishing network connections. As the name states, it extends the authentication possibilities from the norm (PAP and CHAP) to other methods, such as one-time passwords, token cards, biometrics, Kerberos, digital certificates, and future mechanisms. So when a user connects to an authentication server and both have EAP capabilities, they can negotiate between a longer list of possible authentication methods.

Incorrect. A listing of ICMP messages includes:
0 Echo reply (ping reply)
3 Delivery failure (host unknown, network unreachable)
4 Source quench
8 Echo request (ping request)
11 Time to live (TTL) expired (used by traceroute)
12 IP header was bad
13 Communication administratively prohibited

Next Question

Network Security

802.1AE is the IEEE MAC Security standard (MACSec)

When a frame arrives at a device that is configured with MACSec, the MACSec Security Entity (SecY) decrypts the frame if necessary and computes an integrity check value (ICV) on the frame and compares it with the ICV that was sent with the frame.

The IEEE 802.1AR standard specifies unique per-device identifiers (DevID)

802.1AF carries out key agreement functions for the session keys used for data encryption.

An ad hoc WLAN has no APs; the wireless devices communicate with each other through their wireless NICs instead of going through a centralized device

OFDM is a modulation scheme that splits a signal over several narrowband channels. The channels are then modulated and sent over specific frequencies.

Within DNS servers, DNS namespaces are split up administratively into zones. One zone may contain all hostnames for the marketing and accounting departments, and another zone may contain hostnames for the administration, research, and legal departments. The DNS server that holds the files for one of these zones is said to be the authoritative name server for that particular zone. A zone may contain one or more domains, and the DNS server holding those host records is the authoritative name server for those domains.

The primary and secondary DNS servers synchronize their information through a zone transfer.

IMAP is a store-and-forward mail server protocol that is considered POP's successor. IMAP also gives administrators more capabilities when it comes to administering and maintaining the users' messages.

Another way to deal with the problem of forged e-mail messages is by using Sender Policy Framework (SPF), which is an e-mail validation system designed to prevent e-mail spam by detecting e-mail spoofing by verifying the sender's IP address

A spear phishing attack zeroes in on specific people.

In a whaling attack an attacker usually identifies some "big fish" in an organization (CEO, CFO, COO, CSO)

Wormhole Attack: An attacker can capture a packet at one location in the network and tunnel it to another location in the network. In this type of attack, there are two attackers, one at each end of the tunnel (referred to as a wormhole). Attacker A could capture an authentication token that is being sent to an authentication server and then send this token to the other attacker, who then uses it to gain unauthorized access to a resource.

A translation bridge is needed if the two LANs being connected are different types and use different standards and protocols

At least two firewalls, or firewall interfaces, are generally used to construct a DMZ.

Packet filtering was the first generation of firewalls, and it is the most rudimentary type of all of the firewall technologies.

What is important is that a proxy firewall breaks the communication channel; there is no direct connection between the two communicating devices.

A system is considered a bastion host if it is a highly exposed device that is most likely to be targeted by attackers.

Screened Host A screened host is a firewall that communicates directly with a perimeter router and the internal network.

A screened-subnet architecture adds another layer of security to the screened-host architecture. The external firewall screens the traffic entering the DMZ network. However, instead of the firewall then redirecting the traffic to the internal network, an interior firewall also filters the traffic. The use of these two physical firewalls creates a DMZ.

A honeypot is a network device that is intended to be exploited by attackers, with the administrator's goal being to gain information on the attack tactics, techniques, and procedures

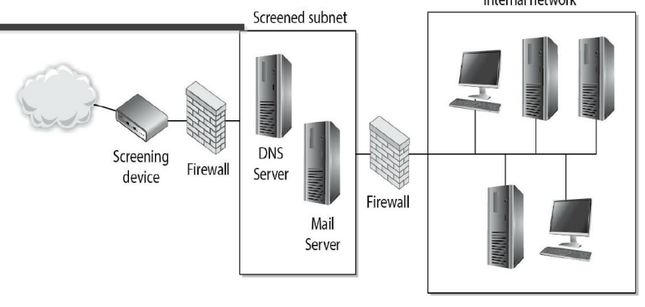


Figure 4-56 With a screened subnet, two firewalls are used to create a DMZ.

Identity Management Components

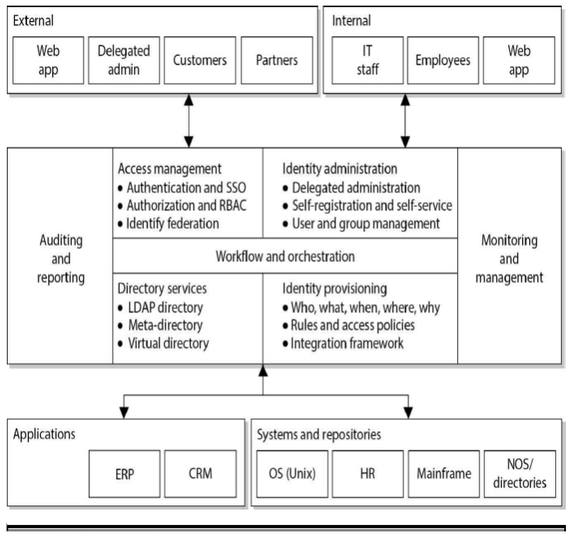


Figure 5-6 Enterprise identity management system components

WAM (Web Access Management)

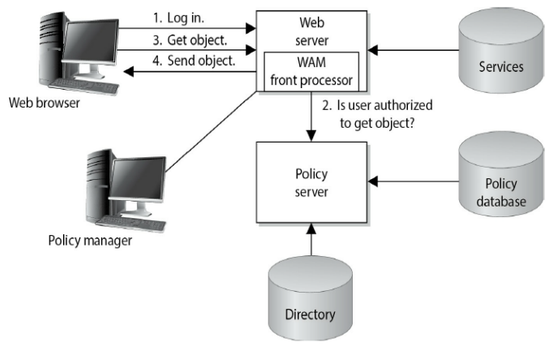


Figure 5-5 A basic example of web access control

1. User sends in credentials to web server.
2. Web server requests the WAM platform to authenticate the user. WAM authenticates against the LDAP directory and retrieves authorizations from the policy database.
3. User requests to access a resource (object).
4. Web server verifies that object access is authorized and allows access to the requested resource.

Identity and Access Management

- Authentication
  - Key component of Authentication
  - Credential Management System
    - Central database to store all Identities
    - Identity Repository
      - hierarchical tree-like structure system that tracks subjects and their authorization chains. Requires also for regulatory/compliance purpose
      - Authoritative System of Records (ASOR)
- Creating user accounts on all systems, assigning and modifying the account details and privileges when necessary, and decommissioning the accounts when they are no longer needed
  - Reduce the potential errors in account config, also logs and tracks each step, this allows for accountability, applies correct config for accounts and checks if any orphaned account is left. Auditors love this workflow!
  - Automated Workflow
    - Should follow well defined approval structure. All directories must be integrated centrally for knowing/managing user accounts
    - Account Registration
      - Creation, maintenance, and deactivation of user attributes and allow access to services
      - User Provisioning
        - Collection of all information of specific user, linked with its ID
        - User Profile
- Approach that user to maintain just one password across multiple systems. Password must be complicated enough!
  - Password Synchronization
- Single Authentication and access to multiple applications. Risky because only one authentication provides access to multiple applications, hackers can target
  - SSO Produtcs
- Biometrics
  - 2 classification – physiological (what you are, eye/retina scan) and behavioral (what you do, signatures/voice recognition)
  - Error Types – Type-1 False Rejection (reject where it should be accepted), Type-2 False Acceptance (accept when it should be rejected, more dangerous)
  - Evaluation of biometric system is done through a scale called CER (Crossover Error Rate) or ERR (Equal Error Rate). Point at which false rejection and false acceptance will be same. Lower is better!
  - Remember that Biometric is also data meaning bits, so it can also be saved on smart card (chance of misuse then!). Hence things like hash/encryption can happen on biometric data also!
  - **NOTE**: Retina scans are extremely invasive and involve a number of privacy issues. Since the information obtained through this scan can be used in the diagnosis of medical conditions, it could very well be considered protected health information (PHI) subject to HIPAA
  - Sampling the iris offers more reference coordinates than any other type of biometric. Mathematically, this means it has a higher accuracy potential than any other type of biometric.
  - Captures a writing style (any writing, not specific signatures)
  - Keystroke Dynamics
- Passwords
  - one of the weakest security mechanisms available
  - Authentication Server has password file, must protect it!
  - Clipping Level – lockout after # of failed states
- Read statement about Rainbow attack on page 907
- Unix/Linux save password in a file called “shadow”, passwords are hashed

- Subject — Is active entity that works or access object
- Object — Is passive entity
- Access Management — Authentication (who can access = confidentiality) and Authorization (what can access = integrity)
- To allow Subject to “successfully” access an Object, 4 steps must happen
  - Identification — Who the subject is?
  - Authentication — Confirmation that subject really is as per his identity
  - Authorization — What subject can do?
  - Accountability — Monitoring of actions of subject
- RACE Condition
  - When Authentication and Authorization are 2 separate processes and attacker gains authorization before authentication
- Multifactor Authentication (MFA) — Authentication based on more than 1 factor
  - Something you know (PIN/Password
  - Something you have (Access Card)
  - Something you are (finger or retinal sacn)
  - Any more than 1 method is used for MFA
- Identity Attributes — Identity – an attribute that identifies a person or system/machine
  - Must be unique, must be non-descriptive and must be able to be issued
- Identity Management (IdM) — Access, authentication and authorization of a subject to access an object based on subjects identity. All done automatically
  - Also called Identity and Access Management (IAM)
  - Its complex due to many different resources, user profiles and access requirements in an organization
- Directory — A large database of objects, its attributes and its profile. Developed in a Tree Structure, having Parent-Child relationship between upper and lower level
- Directory Service — A service that helps managing and operating objects listed in Directory based on Objects profile. Example Active Directory in Windows is Directory Service
  - Example in Windows, we login Domain Controller (DC) that connects us to Directory that has Active Directory service running. We get access to objects based on our (Subject) identity access
- namespace — Objects are identified in a Directory based on namespace assigned to every object
- X.500 — Database standard – Directory is based on this standard! (At the end, Directory is actually a database!
- LDAP — Lightweight Directory Access Protocol — Protocol to access and manage X.500 based Directory
- DN — Distinguished Name — Namespace that LDAP assigns to Objects
- Centralized Directory approach in IdM/IAM — Central Database to query for Objects
- Meta-Directory — Approach such that Meta-Direc talks to different resources and collects information at one central database
- Web Access Management (WAM)
  - Platform that managed access to web server offering multiple services using WAM platform. Supports full IdM and SSO (Single Sign On)
  - WAM sits between User (subject) & Web Server (Object)
  - SSO is managed with the help of Cookie that is provided to Web Browser at first login. Then it monitors Stateful web access

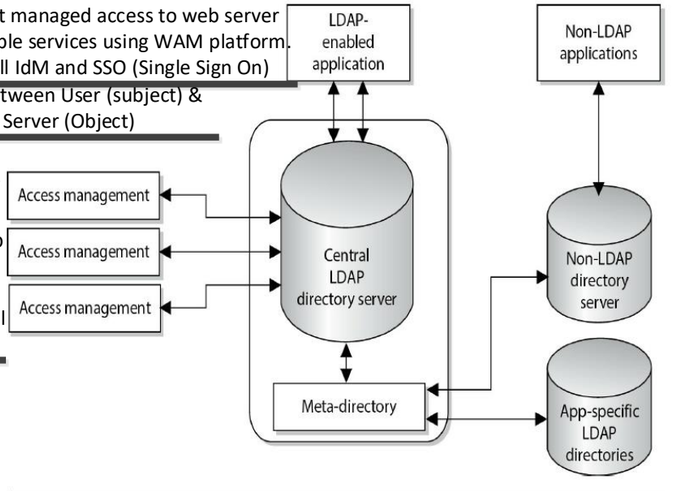


Figure 5-4 Meta-directories pull data from other sources to populate the IdM directory.

Identity and Access Management

Kerberos is an example of an SSO system for distributed environments

Becoming a standard

This open architecture also invites interoperability issues.

Kerberos uses symmetric key cryptography and provides end-to-end security.

Components of Kerberos

Key Distribution Center (KDC) is the most important component within a Kerberos environment. The KDC holds all users' and services' secret keys. It provides an authentication service, as well as key distribution functionality.

The KDC provides security services to principals, which can be users, applications, or network services. The KDC must have an account for, and share a secret key with, each principal.

A ticket is generated by the ticket granting service (TGS) on the KDC and given to a principal when that principal, let's say a user, needs to authenticate to another principal

So far, we know that principals (users and services) require the KDC's services to authenticate to each other; that the KDC has a database filled with information about each and every principal within its realm; that the KDC holds and delivers cryptographic keys and tickets; and that tickets are used for principals to authenticate to each other

Unique prearranged symmetric keys exist between Principal and KDC. Using those keys, Tickets are verified to access services

Time stamps and sequence number are 2 key parameters to implement security and stop replay attacks in Kerberos

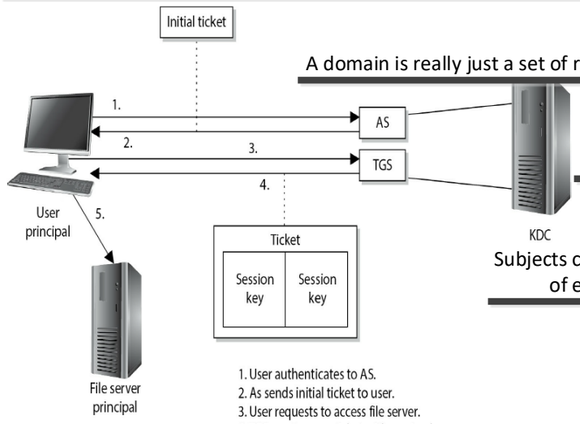


Figure 5-10 The user must receive a ticket from the KDC before being able to use the requested resource.

Single Sign-On Technologies: A Summary

- Kerberos Authentication protocol that uses a KDC and tickets, and is based on symmetric key cryptography
- Security domains Resources working under the same security policy and managed by the same group
- Directory services Technology that allows resources to be named in a standardized manner and access control to be maintained centrally
- Thin clients Terminals that rely upon a central server for access control, processing, and storage

Weakness of Kerberos on page 928

Definition of Domain

A domain is really just a set of resources available to a subject

Security Domain

The common trust level that allows entities to be managed by one single security policy

Subjects can access resources in domains of equal or lower trust levels

Thin Clients are also example of SSO because clients do not even have OS and they download OS from Server/Mainframe that then defines authorization

Authentication

Authentication by knowledge means that a subject is authenticated based upon something she knows

One Time Password

Time Synchronization

Physical token and Authentication server will keep on updating passwords at same time

Counter Synchronization

Token and Authentication Servers are synched by counter, when user wants to use password, it pushes the button on its device, then next password after that is hashed and shown on user's screen. Server will also have the same password as it will know through counter synch

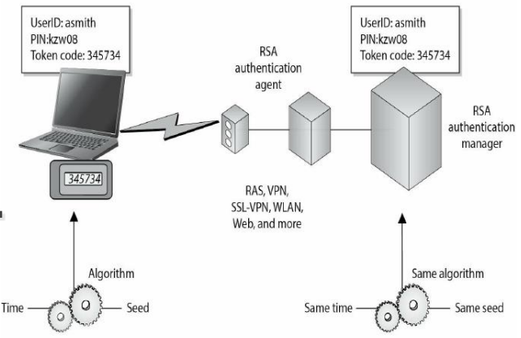
Asynchronous is based on challenge/response mechanisms, while synchronous is based on time- or counter driven mechanisms.

Synchronous Token

SecurID

SecurID, from RSA Security, Inc., is a well-known time-based token. One version of the product generates the OTP by using a mathematical function on the time, date, and ID of the token card. Another version of the product requires a PIN to be entered into the token device.

RSA SecureID Time-Synchronous Two-Factor Authentication



Used by permission of RSA Security, Inc., © Copyright RSA Security, Inc. 2012

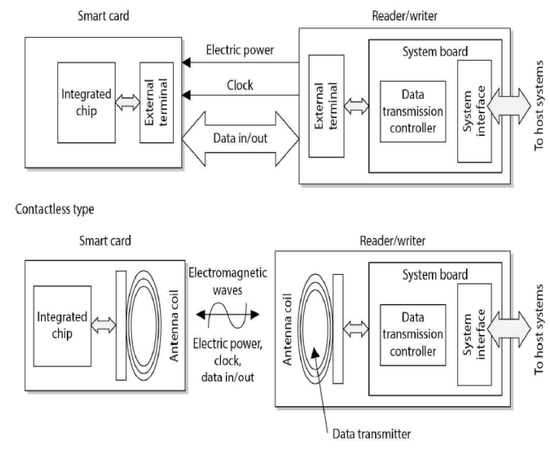
A passphrase is a sequence of characters that is longer than a password (thus a "phrase"). In many cases, the user is more likely to remember a passphrase than a password.

Memory Card

The main difference between memory cards and smart cards is their capacity to process information. A memory card holds information but cannot process information. A smart card holds information and has the necessary hardware and software to actually process that information.

Smart Card

Two general categories of smart cards are the contact and the contactless types. Contact smart card has a gold seal on the face of the card. The contactless smart card has an antenna wire that surrounds the perimeter of the card.



Asynchronous Token

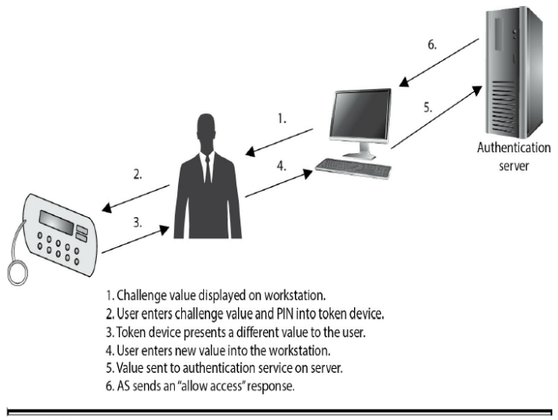


Figure 5-8 Authentication using an asynchronous token device includes a workstation, token device, and authentication service.

Non-Invasive Attack that can happen on Smart Card

Non-invasive attack is one in which the attacker watches how something works and how it reacts in different situations instead of trying to "invade" it with more intrusive measures.

Invasive Attack against Smart Card

A more intrusive smart card attack is called microprobing. Microprobing 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.

Authorization

The different access criteria can be enforced by roles, groups, location, time, and transaction types

As part of the Sarbanes-Oxley (SOX) regulations, managers have to review their employees' permissions to data on an annual basis

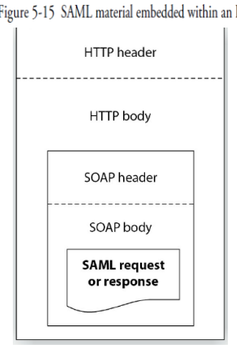
SSO increase security by eliminating a risk that user would write down his password on a piece of paper

Identity and Access Management

Concept of SOAP

Transmission of SAML data can take place over different protocol types, but a common one is Simple Object Access Protocol (SOAP) - SOAP is a specification that outlines how information pertaining to web services is exchanged in a structured manner

Figure 5-15 SAML material embedded within an HTTP message



Concept of XACML

Extensible Access Control Markup Language - is used to express security policies and access rights to assets provided through web services and other enterprise applications. XACML is both an access control policy language and a processing model that allows for policies to be interpreted and enforced in a standard manner

Concept of OpenID

OpenID is an open standard for user authentication by third parties - You have probably encountered OpenID if you've ever tried to access a website and were presented with the option to log in using your Google identity. It is a lot like SAML, except that the users' credentials are maintained not by their company but by a third party.

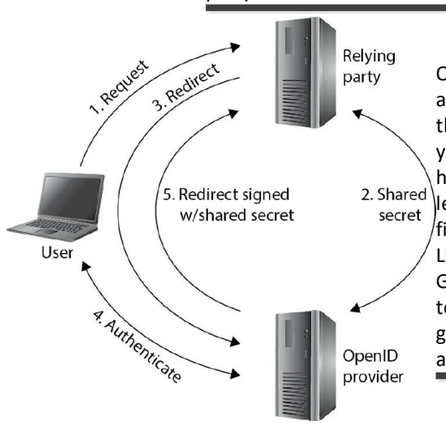


Figure 5-16 OpenID process flow

OAuth

OAuth is an open standard for authorization (not authentication) to third parties. The general idea is that this lets you authorize a website to use something that you control at a different website. For instance, if u 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. If you agree, you will next see a pop-up from Google asking whether you want to authorize LinkedIn to manage your contacts. If you agree to this, LinkedIn gains access to all your contacts until you rescind this authorization.

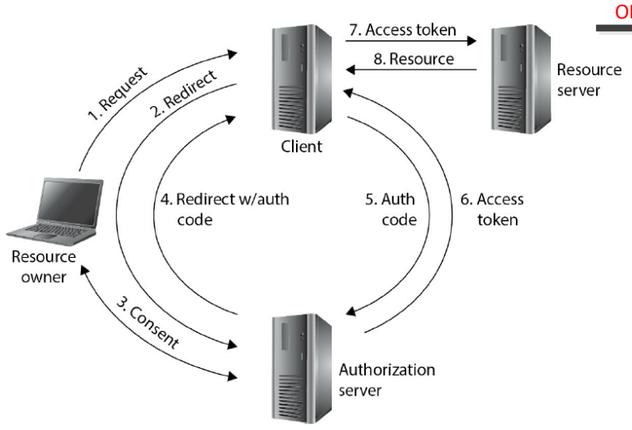


Figure 5-17 OAuth authorization steps

OpenID Connect

OpenID Connect (OIDC) is an authentication layer built on the OAuth 2.0 protocol

OIDC has 2 flows, read on page 952

Accounting

Accountability is tracked by recording user, system, and application activities

What should be audited & logged!

Today, more organizations are implementing security event management (SEM) systems, also called security information and event management (SIEM) systems. These products gather logs from various devices (servers, firewalls, routers, etc.) and attempt to correlate the log data and provide analysis capabilities

Deleting specific incriminating (criminal) data within audit logs is called scrubbing

Its confidentiality can be protected with encryption and access controls, if necessary, and it can be stored on writeonce media (CD-ROMs) to prevent loss or modification of the data.

Keylogger or Keypad Logging - If an attacker can successfully install a Trojan horse on a computer, the Trojan horse can install an application that captures data as it is typed into the keyboard.

System-level events:

- System performance
- Logon attempts (successful and unsuccessful)
- Logon ID
- Date and time of each logon attempt
- Lockouts of users and terminals
- Use of administration utilities
- Devices used
- Functions performed
- Requests to alter configuration files

Application-level events:

- Error messages
- Files opened and closed
- Modifications of files
- Security violations within applications

User-level events:

- Identification and authentication attempts
- Files, services, and resources used
- Commands initiated
- Security violations

Session Management

So, a session, in the context of information systems security, can exist between a user and an information system or between two information systems (e.g., two running programs)

Session termination can happen due to 3 reasons — Timeout duration, inactivity or some anomaly data

Digital Identity

Is not simply a username, it is actually made up of attributes, entitlements, and traits

A federated identity is a portable identity, and its associated entitlements, that can be used across business boundaries. It allows a user to be authenticated across multiple IT systems and enterprises.

Web Portal concept - Portals combine web services (web-based functions) from several different entities and present them in one central website.

Concept of Portlets - A web portal is made up of portlets, which are pluggable user-interface software components that present information from other systems

Markup Language - is a way to structure text and data sets, and it dictates how these will be viewed and used.

The use of a standard markup language also allows for interoperability.

As Internet grows, HTML was not enough - This is the reason that Extensible Markup Language (XML) was developed. XML is a universal and foundational standard that provides a structure for other independent markup languages to be built from and still allow for interoperability. There are different flavors of XML that are used for specific purposes but still interoperable because based on standard XML

Service Provisioning Markup Language (SPML) allows for the exchange of provisioning data between applications, which could reside in one organization or many and also user management

Security Assertion Markup Language (SAML) – XML standard that allows the exchange of authentication and authorization data to be shared between security domains.

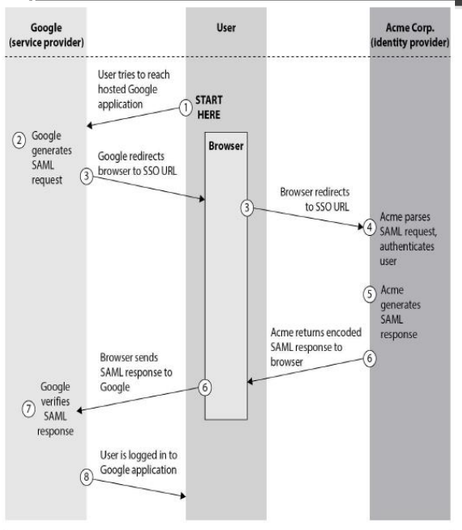


Figure 5-14 SAML authentication

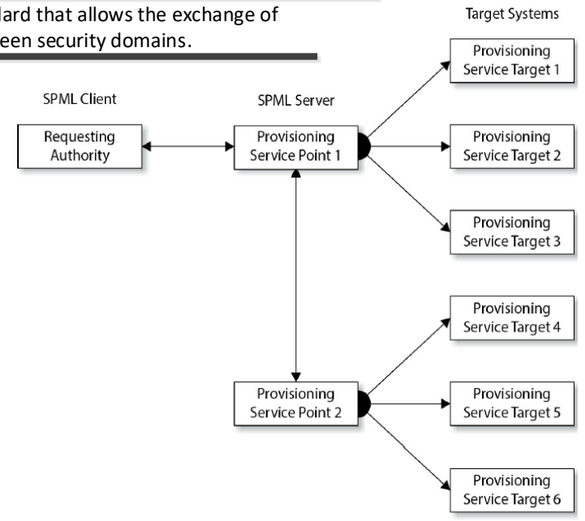


Figure 5-13 SPML provisioning steps

Identity and Access Management

Access Control Techniques/Technologies

Constrained user interfaces restrict users' access abilities by not allowing them to request certain functions or information, or to have access to specific system resources. Three major types of constrained user interfaces exist: menus and shells, database views, and physically constrained interfaces. Details page 967

Remote Authentication Dial-In User Service (RADIUS) is a network protocol that provides client/server authentication and authorization, and audits remote users

Because RADIUS is an open protocol, it can be used in different types of implementations. The format of configurations and user credentials can be held in LDAP servers, various databases, or text files

TACACS has been through three generations: TACACS, Extended TACACS (XTACACS), and TACACS+.

TACACS uses fixed passwords for authentication, while TACACS+ allows users to employ dynamic (one-time) passwords, which provides more protection.

TACACS+ provides basically the same functionality as RADIUS with a few differences in some of its characteristics

Diameter is a protocol developed to build upon the functionality of RADIUS and overcome many of its limitations

Diameter is another AAA protocol that provides the same type of functionality as RADIUS and TACACS+ but also provides more flexibility and capabilities

Diameter consists of two portions

base protocol, which provides the secure communication among Diameter entities, feature discovery, and version negotiation

Extensions, which are built on top of the base protocol to allow various technologies to use Diameter for authentication

Access Control Matrix

is a table of subjects and objects indicating what actions individual subjects can take upon individual objects

A capability table specifies the access rights a certain subject possesses pertaining to specific objects. A capability table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL

Controlling Physical and Logical Access

Administrative, Physical and Technical Controls

Access Control Best Practices – list on page 990

Unauthorized Disclosure of Information

Object reuse issues pertain to reassigning to a subject media that previously contained one or more objects. Meaning that before a new subject starts using an object, any residual data must be cleared

Method to deal with Electrical Emanations

Tempest Standard/Faraday Cage, but it is expensive

Inexpensive method are White Noise (random) and control zone (built with walls that don't transfer radiation)

Access Control Monitoring (who is accessing secretely?)

IDS

Detecting an unauthorized use of, or attack upon, a infrastructure

3 common components of IDS are; sensors, analyzers, and administrator interfaces

Sensors collect traffic and user activity data and send it to an analyzer that alerts administrator interface if found fishy

IDSs come in two main types: network-based, which monitor network communications, and host-based, which can analyze the activity within a particular computer system

Knowledge is accumulated by the IDS vendors about specific attacks and how they are carried out. Each identified attack has a signature. Signature Based IDS looks for these signature!

State Based IDS – good read on page 996, check and compare state of system, state change means that "data" is entered in empty variable field of program that is running the OS/Application

Statistical Anomaly–Based IDS, do not use predefined signatures, but rather are put in a learning mode to build a profile of an environment's "normal" activities by continually sampling. After this profile is built, all future traffic and activities are compared to it. It can detect "zero-day" attacks as this appear as "not normal". Issue is this IDS generates lots of False Positives (unnecessary alarm)

Once an IDS discovers an attack, several things can happen, depending upon the capabilities of the IDS and the policy assigned to it. The IDS can send an alert to a console to tell the right individuals an attack is being carried out, send an e-mail or text to the individual assigned to respond to such activities, kill the connection of the detected attack, or reconfigure a router or firewall to try to stop any further similar attacks. A modifiable response condition might include anything from blocking a specific IP address to redirecting or blocking a certain type of activity.

Integrating Identity as a Service

An on-premise (or on-premises) IdM system is one in which all needed resources remain under your physical control. A scenario in which an on-premise IdM solution makes sense is when you have to manage identities for systems that are not directly connected to the Internet.

Identity as a Service (IDaaS) is a type of Software as a Service (SaaS) offering that is normally configured to provide SSO, federated IdM, and password management services. Great service but regulatory compliant and data exposed to cloud are issues

Access Control Mechanism

There are five main types of access control models: discretionary, mandatory, role based, rule based, and attribute based.

A system that uses **discretionary access control (DAC)** enables the owner of the resource to specify which subjects can access specific resources.

The most common implementation of DAC is through ACLs,

Owner of the Resource is a USER in this case (USER who has created the resource)

Because USER can decide at its discretion who can access files, a risk is that USER allows access also to Malware without checking/authenticating and malware can harm the file/system

In a **mandatory access control (MAC)** model, users do not have the discretion of determining who can access objects, a user cannot install software, change file permissions, add new users, etc

The MAC model is much more structured and strict than the DAC model and is based on a security label system. Users are given a security clearance (secret, top secret, confidential, and so on), and data is classified in the same way.

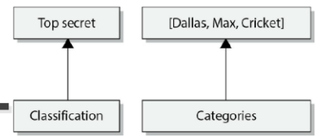
A company cannot simply choose to turn on either DAC or MAC. It has to purchase an operating system that has been specifically designed to enforce MAC rules. DAC systems do not understand security labels, classifications, or clearances, and thus cannot be used in institutions that require this type of structure for access control. A publicly released MAC system is SE Linux, developed by the NSA and Secure Computing.

Traffic Classification and Categories

The categories portion of the label enforces need-to-know rules. Just because someone has a top-secret clearance does not mean she now has access to all top-secret information

A **role-based access control (RBAC)** model uses a centrally administrated set of controls

The RBAC approach simplifies access control administration by allowing permissions to be managed in terms of user job roles



An RBAC model is the best system for a company that has high employee turnover. If John, who is mapped to the Contractor role, leaves the company, then Chrissy, his replacement, can be easily mapped to this role.

Details of RBAC if require are on page-963

Rule Based Access Control - Rule-based access control uses specific rules that indicate what can and cannot happen between a subject and an object. This access control model is built on top of traditional RBAC and is thus commonly called RB-RBAC to disambiguate the otherwise overloaded RBAC acronym. It is based on the simple concept of "if X then Y" programming rules, which can be used to provide finer-grained access control to resources. Rule-based access control is not necessarily identity-based. The DAC model is identity based. Rule-based access controls simplify this by setting a rule that will affect all users across the board—no matter what their identity is.

Attribute-based access control (ABAC) uses attributes of any part of a system to define allowable access. These attributes can belong to belong to subjects, objects, actions, or contexts

	RADIUS	TACACS+
Packet delivery	UDP	TCP
Packet encryption	Encrypts only the password from the RADIUS client to the server.	Encrypts all traffic between the client and server.
AAA support	Combines authentication and authorization services.	Uses the AAA architecture, separating authentication, authorization, and auditing.
Multiprotocol support	Works over PPP connections.	Supports other protocols, such as AppleTalk, NetBIOS, and IPX.
Responses	Uses single-challenge response when authenticating a user, which is used for all AAA activities.	Uses multiple-challenge response for each of the AAA processes. Each AAA activity must be authenticated.

Table 5-1 Specific Differences Between These Two AAA Protocols

Access Control Models

The main characteristics of the five different access control models are important to understand.

- DAC Data owners decide who has access to resources, and ACLs are used to enforce these access decisions.
- MAC Operating systems enforce the system's security policy through the use of security labels.
- RBAC Access decisions are based on each subject's role and/or functional position.
- RB-RBAC Adds on to RBAC by imposing rules that further restrict access decisions.
- ABAC Access decisions are based on attributes of any component of or action on the system.

Identity and Access Management

IDS Types Summary on Page 1001 is fantastic!

IPS

The traditional IDS only detects that something bad may be taking place and sends an alert. The goal of an IPS is to detect this activity and not allow the traffic to gain access to the target in the first place,

Sniffers

a general term for programs or devices able to examine traffic on a LAN segment

A sniffer is just a tool that can capture network traffic. If it has the capability of understanding and interpreting individual protocols and their associated data, this type of tool is referred to as a protocol analyzer

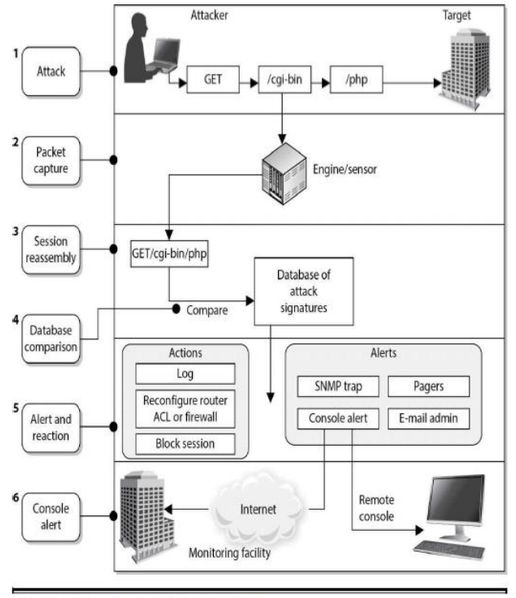


Figure 5-26 The basic architecture of a NIDS

Vulnerability Scanning Recap

Vulnerability scanners provide the following capabilities:

- The identification of active hosts on the network
- The identification of active and vulnerable services (ports) on hosts
- The identification of applications and banner grabbing
- The identification of operating systems
- The identification of vulnerabilities associated with discovered operating systems and applications
- The identification of misconfigured settings
- Test for compliance with host applications' usage/security policies
- The establishment of a foundation for penetration testing

Test Type	Frequency	Benefits
Network scanning	Continuously to quarterly	• Enumerates the network structure and determines the set of active hosts and associated software • Identifies unauthorized hosts connected to a network • Identifies open ports • Identifies unauthorized services
War dialing	Annually	Detects unauthorized modems and prevents unauthorized access to a protected network
War driving	Continuously to weekly	Detects unauthorized wireless access points and prevents unauthorized access to a protected network
Virus detectors	Weekly or as required	Detects and deletes viruses before successful installation on the system
Log reviews	Daily for critical systems	Validates that the system is operating according to policy
Password cracking	Continuously to same frequency as expiration policy	• Verifies the policy is effective in producing passwords that are difficult to break • Verifies that users select passwords compliant with the organization's security policy
Vulnerability scanning	Quarterly or bimonthly (more often for high-risk systems), or whenever the vulnerability database is updated	• Enumerates the network structure and determines the set of active hosts and associated software • Identifies a target set of computers to focus vulnerability analysis • Identifies potential vulnerabilities on the target set • Validates operating systems and major applications are up-to-date with security patches and software versions
Penetration testing	Annually	• Determines how vulnerable an organization's network is to penetration and the level of damage that can be incurred • Tests the IT staff's response to perceived security incidents and their knowledge and implementation of the organization's security policy and the system's security requirements
Integrity checkers	Monthly and in case of a suspicious event	Detects unauthorized file modifications

Vulnerability and Penetration Testing: What Color Is Your Box?

Vulnerability testing and penetration testing come in boxes of at least three colors: black, white, and gray. The color, of course, is metaphorical, but security professionals need to be aware of the three types. None is clearly superior to the others in all situations, so it is up to us to choose the right approach for our purposes.

- *Black box testing* treats the system being tested as completely opaque. This means that the tester has no *a priori* knowledge of the internal design or features of the system. All knowledge will come to the tester only through the assessment itself. This approach simulates an external attacker best and may yield insights into information leaks that can give an adversary better information on attack vectors. The disadvantage of black box testing is that it will probably not cover all of the internal controls since some of them are unlikely to be discovered in the course of the audit. Another issue is that, with no knowledge of the innards of the system, the test team may inadvertently target a subsystem that is critical to daily operations.

White box testing affords the auditor complete knowledge of the inner workings of the system even before the first scan is performed. This approach allows the test team to target specific internal controls and features and should yield a more complete assessment of the system. The downside is that white box testing may not be representative of the behaviors of an external attacker, though it may be a more accurate depiction of an insider threat.

Gray box testing meets somewhere between the other two approaches. Some, but not all, information on the internal workings is provided to the test team. This helps guide their tactics toward areas we want to have thoroughly tested, while also allowing for a degree of realism in terms of discovering other features of the system. This approach mitigates the issues with both white and black box testing.

Security Assessment

establishing a clear set of goals is probably the most important step of planning a security audit

These are called compliance audits and must be performed by external parties.

Test coverage is a measure of how much of a system is examined by a specific test (or group of tests), which is typically expressed as a percentage. For example, if you are developing a software system with 1,000 lines of code and your suite of unit tests executes 800 of those, then you would have 80 percent test coverage

When performing a penetration test, the team goes through a five-step process:
1. Discovery Footprinting and gathering information about the target
2. Enumeration Performing port scans and resource identification methods
3. Vulnerability mapping Identifying vulnerabilities in identified systems and resources
4. Exploitation Attempting to gain unauthorized access by exploiting vulnerabilities
5. Report to management Delivering to management documentation of test findings along with suggested countermeasures

Information System Security Audit Process

1. Determine the goals, because everything else hinges on this.
2. Involve the right business unit leaders to ensure the needs of the business are identified and addressed.
3. Determine the scope, because not everything can be tested.
4. Choose the audit team, which may consist of internal or external personnel, depending on the goals, scope, budget, and available expertise.
5. Plan the audit to ensure all goals are met on time and on budget.
6. Conduct the audit while sticking to the plan and documenting any deviations therefrom.
7. Document the results, because the wealth of information generated is both valuable and volatile.
8. Communicate the results to the right leaders in order to achieve and sustain a strong security posture.

Conducting Internal Audits

Here are some best practices to get the most bang out of internal audits that you conduct:

- Mark your calendars Nothing takes the wind out of your audit's sails quicker than not having all key personnel and resources available. Book them early.
- Prepare the auditors Rehearse the process with the auditors so everyone is on the same sheet of music. Ensure everyone knows the relevant policies and procedures.
- Document everything Consider having note-takers follow the auditors around documenting everything they do and observe.
- Make the report easy to read Keep in mind that you will have at least two audiences: managers and technical personnel. Make the report easy to read for both.

Conducting and Facilitating External Audits

It would be pretty unusual for you to conduct an external audit on a contractor. Instead, you would normally ask them to perform an internal audit (scoped in accordance with the contract) or else bring in a third-party auditor (described in the next section). Regardless, here are some tips to consider whether you are on the giving or receiving end of the deal:

- Learn the contract An external audit, by definition, is scoped to include only the contractual obligations of an organization. Be sure the audit doesn't get out of control.
- Schedule in- and out-briefs Schedule an in-brief to occur right before the audit starts to bring all stakeholders together. Schedule an out-brief to occur immediately after the audit is complete to give the audited organization a chance to address any misconceptions or errors.
- Travel in pairs Ensure the organization being audited has someone accompanying each team of auditors. This will make things go smoother and help avoid misunderstandings.
- Keep it friendly The whole goal of this process is to engender trust.

Facilitating Third-Party Audits

Your organization will typically pay for the third party to audit you, but if you're doing the audit for compliance or contractual reasons, the auditor won't be working for you. The job of a third-party auditor is to certify (using their own reputation) that you are meeting whatever standards are in scope. Regardless, the following are useful tips:

- Know the requirements Go through the audit requirements line by line to ensure you know exactly what the third-party auditor will be looking at. Call the auditor if you have any questions.
- Pre-audit Conduct your own internal audit using the same list of requirements to minimize the number of surprises.
- Lock in schedules Ensure the right staff will be available when the auditors show up, even if there's only a small chance they'll be needed.
- Get organized The audit team will likely need access to a large and diverse set of resources, so make sure you have them all assembled in one place and organized.
- Keep the boss informed A third-party audit, by definition, is an important event for the organization, and we all know that bad news doesn't get better with time. Be sure to keep the senior managers informed, especially of any potential deficiency areas.

Vulnerability Test vs. Penetration Test

A vulnerability assessment identifies a wide range of vulnerabilities in the environment. This is commonly carried out through a scanning tool. The idea is to identify any vulnerabilities that *potentially* could be used to compromise the security of our systems. By contrast, in a penetration test, the security professional exploits one or more vulnerabilities to prove to the customer (or your boss) that a hacker can *actually* gain access to company resources.

Security Assessment

Auditing of Administrative Controls

Account Management is very important task. Lease privilege and need to know should lead!

The AUP is a useful first line of defense, because it documents when each user was made aware of what is and is not acceptable use of computers (and other resources) at work

we must ensure that the account of someone who is not present to use it is suspended until that person returns or the term of our retention policy is met.

Backup Data

we need to periodically test it to ensure that the backups will work as promised when we need them.

Types of Data considered for backup

- User Data Files, Databases, Mailbox Data

Fortunately, all major database management systems (DBMSs) include one or more means to back up their databases. The challenge is in ensuring that the backup will be sufficient to reconstitute the databases if necessary

Testing Data Backups

- *Develop scenarios* that capture specific sets of events that are representative of the threats facing the organization.
- *Develop a plan* that tests all the mission-critical data backups in each of the scenarios.
- *Leverage automation* to minimize the effort required by the auditors and ensure tests happen periodically.
- *Minimize impact on business* processes of the data backup test plan so that it can be executed regularly.
- *Ensure coverage* so that every system is tested, though not necessarily in the same test.
- *Document the results* so you know what is working and what needs to be worked on.
- *Fix or improve* any issues you documented.

BCP and Disaster Recovery Assessment

The maintenance of the BCP should be incorporated into change management procedures. That way, any changes in the environment are reflected in the plan itself

The first exercises should not include all employees, but rather a small representative sample of the organization. This allows both the planners and the participants to refine the plan. It also allows each part of the organization to learn its roles and responsibilities. Then, larger drills can take place so overall operations will not be negatively affected.

Different Types of Test Drills to assess BCP/DRP

- Checklist Test: Copies of the DRP or BCP are distributed to the different departments and functional areas for review to check everything is listed
- Structured Walk-Through Test: Representatives from departments go through BCP step by step ensuring items are detailed enough with no missing element
- Tabletop Exercises: May be between Chiefs or Departments. Key purpose is to go through a created scenario and see how BCP addresses that scenario
- Simulation Test: Disaster is simulated for a specific case and teams participate to see how they act
- Parallel Test: A particular IT system is commissioned off-site/alternate site and then its performance is compared to same system at real/original site
- Full-Interruption Test: Operational Site is fully interrupted and operations moved to alternate site. Has huge impact on business

Keeping BCP/DRP Updated/Maintained

One of the simplest and most cost-effective and process-efficient ways to keep a plan up-to- date is to incorporate it within the change management process of the organization.

Synthetic Transactions

Many of our information systems operate on the basis of transactions. A user (typically a person) initiates a transaction that could be anything from a request for a given web page to a wire transfer of half a million dollars to an account in Switzerland. This transaction is processed by any number of other servers and results in whatever action the requestor wanted. This is considered a real transaction. Now suppose that a transaction is not generated by a person but by a script. This is considered a synthetic transaction.

Preventing Log Tampering

Log files are often among the first artifacts that attackers will use to attempt to hide their actions. Knowing this, it is up to us as security professionals to do what we can to make it infeasible, or at least very difficult, for attackers to successfully tamper with our log files. The following are the top five steps we can take to raise the bar for the bad folks:

- Remote logging When attackers compromise a device, they often gain sufficient privileges to modify or erase the log files on that device. 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 Some high-security environments use one-way (or simplex) communications between the reporting devices and the central log repository. This is easily accomplished by severing the "receive" pairs on an Ethernet cable. The term *data diode* is sometimes used to refer to this approach to physically ensuring a one-way path.
- Replication It is never a good idea to keep a single copy of such an important resource as the consolidated log entries. By making multiple copies and keeping them in different locations, you make it harder for attackers to alter the log files, particularly if at least one of the locations is not accessible from the network (e.g., a removable device).
- Write-once media If one of the locations to which you back up your log files can be written to only once, you make it impossible for attackers to tamper with that copy of the data. Of course, they can still try to physically steal the media, but now you force them to move into the physical domain, which many attackers (particularly ones overseas) will not do.
- Cryptographic hash chaining A powerful technique for ensuring events that are modified or deleted are easily noticed is to use cryptographic hash chaining. In this technique, each event is appended the cryptographic hash (e.g., SHA-256) of the preceding event. This creates a chain that can attest to the completeness and the integrity of every event in it.

Misuse Case Testing

- Use Case: Use cases are structured scenarios that are commonly used to describe required functionality in an information system
- Misuse Case: A misuse case is a use case that includes threat actors and the tasks they want to perform on the system

The idea behind misuse case testing is to ensure we have effectively addressed each of the risks we identified and decided to mitigate during our risk management process and that are applicable to the system under consideration

Code Review – Review process of software/application/program code. We are now getting to inner working of software

Defensive programming is a best practice that all software development operations should adopt. In a nutshell, it means that as you develop or review the code, you are constantly looking for opportunities for things to go badly. Perhaps the best example of defensive programming is the practice of treating all inputs, whether they come from a keyboard, a file, or the network, as untrusted until proven otherwise

A Code Review Process

1. Identify the code to be reviewed (usually a specific function or file).
2. The team leader organizes the inspection and makes sure everyone has access to the correct version of the source code, along with all supporting artifacts.
3. Everyone prepares for inspection by reading through the code and making notes.
4. All the obvious errors are collated offline (not in a meeting) so they don't have to be discussed during the inspection meeting (which would be a waste of time).
5. If everyone agrees the code is ready for inspection, then the meeting goes ahead.
6. The team leader displays the code (with line numbers) via an overhead projector so everyone can read through it. Everyone discusses bugs, design issues, and anything else that comes up about the code. A scribe (not the author of the code) writes everything down.
7. At the end of the meeting, everyone agrees on a "disposition" for the code:
   - Passed: Code is good to go
   - Passed with rework: Code is good so long as small changes are fixed
   - Reinspect: Fix problems and have another inspection
8. After the meeting, the author fixes any mistakes and checks in the new version.
9. If the disposition of the code in step 7 was passed with rework, the team leader checks off the bugs that the scribe wrote down and makes sure they're all fixed.
10. If the disposition of the code in step 7 was reinspect, the team leader goes back to step 2 and starts over again.

Interface Testing

At its essence, an interface is an exchange point for data between systems and/or users. You can see this in your computer's network interface card (NIC), which is the exchange point for data between your computer (a system) and the local area network (another system). Another example of an interface is an application programming interface (API), a set of points at which a software system (e.g., the application) exchanges information with another software system (e.g., the libraries).

interface testing is a special case of something called integration testing, which is the assessment of how different parts of a system interact with each other

Security Assessment

Security Training and Security Awareness Training

Security training is the process of teaching a skill or set of skills that will allow people to perform specific functions better. Security awareness training, on the other hand, is the process of exposing people to security issues so that they may be able to recognize them and better respond to them. Security training is typically provided to security personnel, while security awareness training should be provided to every member of the organization.

Attacks that can be mitigated using Security Awareness Training

Pretexting is a form of social engineering, typically practiced in person or over the phone, in which the attacker invents a believable scenario in an effort to persuade the target to violate a security policy. A common example is a call received from (allegedly) customer service or fraud prevention at a bank in which the attacker tries to get the target to reveal account numbers, personal identification numbers (PINs), passwords, or similarly valuable information.

Testing the degree to which our users are aware of data protection requirements and best practices can best be done by using tags in our files' metadata. The information classification labels we discussed in Chapter 2 become an effective means of tracking where our data is

Key Performance Indicators (KPI)

Measurement how well our security controls are doing?

ISO 27004, titled Information Security Metrics Implementation, outlines a process by which to measure the performance of security controls and processes

KPI relevant definitions and steps to implement good KPI posture is on page 1084-1085. Read it!

Key Risk Indicators (KRIs)

While KPIs tell us where we are today with regard to our goals, key risk indicators (KRIs) tell us where we are today in relation to our risk appetite. They measure how risky an activity is so that the leadership can make informed decisions about that activity, all the while taking into account potential resource losses

Reporting your assessment

Report "effectively" meaning understandable by management about business impact/chance of loss

You can think of analyzing results as a three-step process to determine the following: What?, So what?, and Now what?

Technical Reporting/Report Writing

One of an important aspect is Executive Summary – include financial benefit in executive summary – to get that benefit consider following approaches to evaluate asset cost

The cost approach simply looks at the cost of acquiring or replacing the asset. This is the approach we oftentimes take to valuating our IT assets (minus information, of course

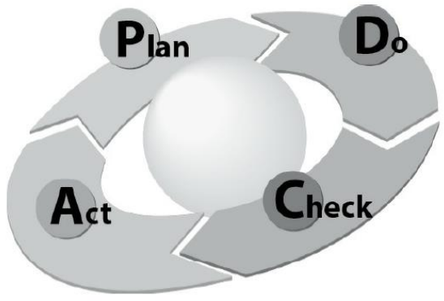
The income approach considers the expected contribution of the asset to the firm's revenue stream. See example on page 1090

The market approach is based on determining how much other firms are paying for a similar asset in the marketplace

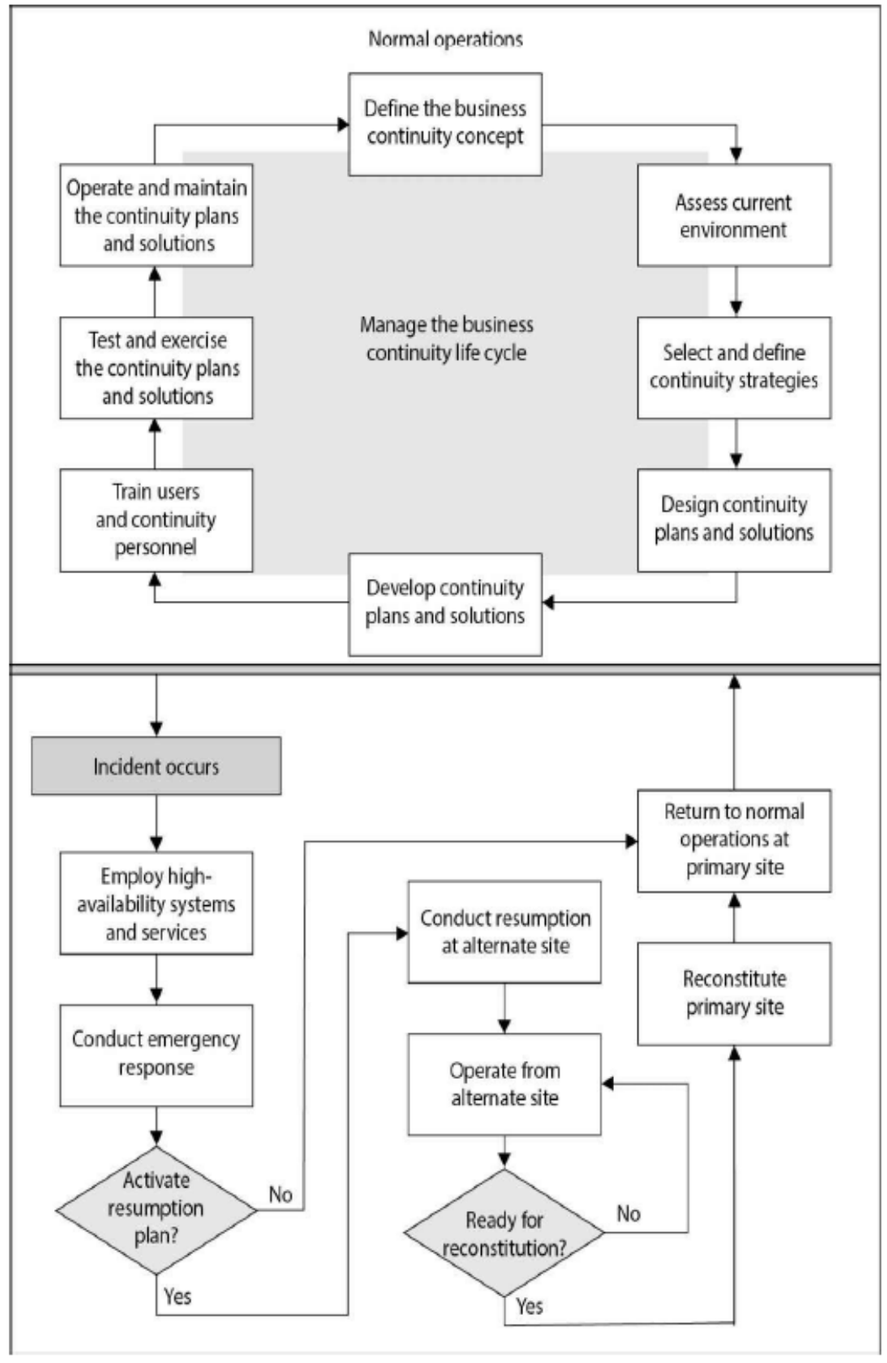
Management Review

Finally Management Review – it follows ISO 9000 series standard (Plan-Do-Check-Act) Loop

Plan (define strategy), Do (implement), Check (if implemented properly, audit/report), Act (modify/review strategy)



BCP Life Cycle – very well depicted



Security Operations

In short, security operations encompasses all the activities required to ensure the security of information systems. It is the culmination of most of what we've discussed in the book thus far

Security operations is all about ensuring that people, applications, equipment, and the overall environment are properly and adequately secured

A large part of operational security includes ensuring that the physical and environmental concerns are adequately addressed, such as temperature and humidity controls, media reuse, disposal, and destruction of media containing sensitive information

Administrative Management/Controls

Separation of duties, therefore, is a preventive measure that requires collusion to occur in order for someone to commit an act that is against policy

Organizations should create a complete list of roles used within their environment, with each role's associated tasks and responsibilities. This should then be used by data owners and security personnel when determining who should have access to specific resources and the type of access

Organizational Role	Core Responsibilities
Control Group	Obtains and validates information obtained from analysts, administrators, and users and passes it on to various user groups.
Systems Analyst	Designs data flow of systems based on operational and user requirements.
Application Programmer	Develops and maintains production software.
Help Desk/Support	Resolves end-user and system technical or operations problems.
IT Engineer	Performs the day-to-day operational duties on systems and applications.
Database Administrator	Creates new database tables and manages the database.
Network Administrator	Installs and maintains the local area network/wide area network (LAN/WAN) environment.
Security Administrator	Defines, configures, and maintains the security mechanisms protecting the organization.
Tape Librarian	Receives, records, releases, and protects system and application files backed up on media such as tapes or disks.
Quality Assurance	Can consist of both Quality Assurance (QA) and Quality Control (QC). QA ensures that activities meet the prescribed standards regarding supporting documentation and nomenclature. QC ensures that the activities, services, equipment, and personnel operate within the accepted standards.

Table 7-1 Roles and Associated Tasks

Job rotation means that, over time, more than one person fulfills the tasks of one position within the company. Can also helps identify fraudulent activities, and therefore can be considered a detective type of control

Security and Network Personnel

The security administrator should not report to the network administrator because their responsibilities have different focuses. 2 roles are different and can have conflict of interest

Accountability

A privileged account is one with elevated rights. When we hear the term, we usually think of system administrators, but it is important to consider that a lot of times privileges are gradually attached to user accounts for legitimate reasons, but never reviewed to see if they're still needed

Physical Security

Should be implemented by using a layered approach

Access control points can be identified and classified as external, main, and secondary entrances

Locks are inexpensive access control mechanisms that are widely accepted and used. They are considered delaying devices to intruders

To the curious mind or a determined thief, a lock can be considered a little puzzle to solve, not a deterrent

Figure 7-5 An electronic combination lock

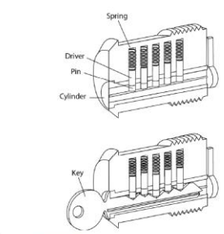


Figure 7-4 Tumbler lock

ure 7-2 A warded lock

Cipher locks, also known as programmable locks, are keyless and use keypads to control access into an area or facility

Some cipher locks require all users to know and use the same combination, which does not allow for any individual accountability. Some of the more sophisticated cipher locks permit specific codes to be assigned to unique individuals. This provides more accountability, because each individual is responsible for keeping his access code secret, and entry and exit activities can be logged and tracked. These are usually referred to as smart locks, because they are designed to allow only authorized individuals access at certain doors at certain times

Administrative Responsibilities It is important for a company not only to choose the right type of lock for the right purpose, but also to follow proper maintenance and procedures. Keys should be assigned by facility management, and this assignment should be documented. Procedures should be written out detailing how keys are to be assigned, inventoried, and destroyed when necessary, and what should happen if and when keys are lost.

Lock Strengths

Basically, three grades of locks are available:

- Grade 1 Commercial and industrial use
- Grade 2 Heavy-duty residential/light-duty commercial
- Grade 3 Residential/consumer

The cylinders within the locks fall into three main categories:

- Low security No pick or drill resistance provided (can fall within any of the three grades of locks)
- Medium security A degree of pick-resistance protection provided (uses tighter and more complex keyways [notch combination]; can fall within any of the three grades of locks)
- High security Pick-resistance protection through many different mechanisms (only used in grade 1 and 2 locks)

Lock Exploitation Techniques

Raking. To circumvent a pin tumbler lock, a lock pick is pushed to the back of the lock and quickly slid out while providing upward pressure

Lock bumping is a tactic that intruders can use to force the pins in a tumbler lock to their open position by using a special key called a bump key

Personnel Access Control

If the card is a memory card, then the reader just pulls information from it and makes an access decision. If the card is a smart card, the individual may be required to enter a PIN or password, which the reader compares against the information held within the card or in an authentication server

External Boundary Protection Mechanisms

System sensing access control readers, also called transponders, recognize the presence of an approaching object within a specific area. This type of system does not require the user to swipe the card through the reader. The reader sends out interrogating signals and obtains the access code from the card without the user having to do anything

Perimeter security controls can be natural (hills, rivers) or manmade (fencing, lighting, gates)

Fences work as "first line of defense" mechanisms

Gates basically have four distinct classifications (read on page 1125), These classifications and guidelines are developed by Underwriters Laboratory (UL), a nonprofit organization that tests, inspects, and classifies electronic devices, fire protection equipment, and specific construction materials

Critical areas need to have illumination that reaches at least eight feet with the illumination of two foot-candles. Foot-candle is a unit of measure of the intensity of light

An array of lights that provides an even amount of illumination across an area is usually referred to as continuous lighting

You probably are familiar with the special home lighting gadgets that turn certain lights on and off at predetermined times, giving the illusion to potential burglars that a house is occupied even when the residents are away. Companies can use a similar technology, which is referred to as standby lighting

Responsive area illumination takes place when an IDS detects suspicious activities and turns on the lights within a specific area

CCTV is a physical security control

Attackers can try to "replay" video on CCTV while doing attack, observer would assume that the recording is live, however, it is just a replay

Most of the CCTV cameras in use today employ light-sensitive chips called chargedcoupled devices (CCDs). The CCD is an electrical circuit that receives input light from the lens and converts it into an electronic signal, which is then displayed on the monitor

Two main types of lenses are used in CCTV: fixed focal length and zoom (varifocal). The focal length of a lens defines its effectiveness in viewing objects from a horizontal and vertical view

Short focal length lenses provide wider-angle views, while long focal length lenses provide a narrower view

The optical zoom lenses provide flexibility by allowing the viewer to change the field of view while maintaining the same number of pixels in the resulting image, which makes it much more detailed. Digital Zoom is different, it only zooms the existing image with fixed focal length, only expands the image with low dpi

The depth of field refers to the portion of the environment that is in focus when shown on the monitor. The depth of field varies depending upon the size of the lens opening, the distance of the object being focused on, and the focal length of the lens

Iris control amount of light enters in the lens

Security Operations

Trusted Recovery

An operating system's response to a type of failure can be classified as one of the following:

System Reboot - takes place after the system shuts itself down in a controlled manner in response to a kernel failure. If the system finds inconsistent data structures or if there is not enough space in some critical tables, a system reboot may take place

An emergency system restart takes place after a system failure happens in an uncontrolled manner. This could be a kernel or media failure caused by lower-privileged user processes attempting to access memory segments that are restricted. The system sees this as an insecure activity that it cannot properly recover from without rebooting

A system cold start takes place when an unexpected kernel or media failure happens and the regular recovery procedure cannot recover the system to a more consistent state. The system, kernel, and user objects may remain in an inconsistent state while the system attempts to recover itself, and intervention may be required by the user or administrator to restore the system.

Atomic Transactions are those that do not leave any gap between input provided and output received. That level of transaction stops TOC/TOU (Time of Check and Time of Use atttack)

A best practice for managing and securing workstations is to develop a standard hardened image, called a Gold Master (GM)

Locked-down systems (systems that are fully protected by disabling any unwanted services or applications) are referred to as bastion hosts (secure computers)

Remote Systems Administration

To gain the benefits of remote access without taking on unacceptable risks, remote administration needs to take place securely. The following are just a few of the guidelines to use:

- For best security, require a virtual private network (VPN) connection protected by two-factor authentication for any internal system access from an external (e.g., Internet) host.
- Commands and data should not take place in cleartext (i.e., they should be encrypted), even if using a VPN to remotely connect to the network. For example, Secure Shell (SSH) should be used.
- Strong authentication should be in place for any administration activities.
- Truly critical systems should be administered locally instead of remotely.
- Only a small number of administrators should be able to carry out this remote functionality.

Network and Resource Availability

Fault-tolerant technologies keep information available against not only individual storage device faults but even against whole system failures. Fault tolerance is among the most expensive possible solutions, and is justified only for the most mission critical information

MTBF implies that the device or component is repairable. If it isn't, then we use the term mean time to failure (MTTF)

For an unplanned reboot, the MTTR is the amount of time between the failure of the system and the point in time when it has rebooted its operating system

RAID (Redundant Array of Disk Drives)

When data is written across all drives, the technique of striping is used

Control data is also spread across each disk—this is called parity—so that if one disk fails, the other disks can work together and restore its data

Various levels of RAID dictate the type of activity that will take place within the RAID system. Some levels deal only with performance issues, while other levels deal with performance and fault tolerance

RAID Level	Activity	Name
0	Data striped over several drives. No redundancy or parity is involved. If one volume fails, the entire volume can be unusable. It is used for performance only.	Striping
1	Mirroring of drives. Data is written to two drives at once. If one drive fails, the other drive has the exact same data available.	Mirroring
2	Data striping over all drives at the bit level. Parity data is created with a hamming code, which identifies any errors. This level specifies that up to 39 disks can be used: 32 for storage and 7 for error recovery data. This is not used in production today.	Hamming code parity
3	Data striping over all drives and parity data held on one drive. If a drive fails, it can be reconstructed from the parity drive.	Byte-level parity
4	Same as level 3, except parity is created at the block level instead of the byte level.	Block-level parity
5	Data is written in disk sector units to all drives. Parity is written to all drives also, which ensures there is no single point of failure.	Interleave parity
6	Similar to level 5 but with added fault tolerance, which is a second set of parity data written to all drives.	Second parity data (or double parity)
10	Data is simultaneously mirrored and striped across several drives and can support multiple drive failures.	Striping and mirroring

Table 7-2 Different RAID Levels

SAN

Drawing from the local area network (LAN), wide area network (WAN), and metropolitan area network (MAN) nomenclature, a storage area network (SAN) consists of numerous storage devices linked together by a high-speed private network and storage-specific switches. This creates a "fabric" that allows users to attach to and interact in a transparent mode

Clustering

is a fault-tolerant server technology that is similar to redundant servers, except each server takes part in processing services that are requested. A server cluster is a group of servers that are viewed logically as one server to users and can be managed as a single logical system

Hierarchical Storage Management

Hierarchical storage management (HSM) provides continuous online backup functionality. It combines 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 devices that vary in speed and cost. The faster media holds the files that are accessed more often, and the seldom-used files are stored on the slower devices, or nearline devices. "Stub" is data that is left behind as a reference for those files that are seldom accessed and once accessed, "stub" guides them from where to get those files, hence quick in response and still saving capacity on drives that require frequent access!

IDS

A passive infrared (PIR) system identifies the changes of heat waves in an area it is configured to monitor. If the particles' temperature within the air rises, it could be an indication of the presence of an intruder, so an alarm is sounded

A proximity detector, or capacitance detector, emits a measurable magnetic field. The detector monitors this magnetic field, and an alarm sounds if the field is disrupted

Fail-Safe on right means that "when fail, fail safely without hurting others☺ equipment/devices

Intrusion Detection Systems Characteristics

IDSs are very valuable controls to use in every physical security program, but several issues need to be understood before implementing them:

- They are expensive and require human intervention to respond to the alarms.
- They require a redundant power supply and emergency backup power.
- They can be linked to a centralized security system.
- They should have a fail-safe configuration, which defaults to "activated."
- They should detect, and be resistant to, tampering.

How to control software provisioning/ tracking in an organization

Application whitelisting, only approved software will be allowed!

Use Gold Master, standard image workstation or server that includes properly configured and authorized software

Enforcing the principle of least privilege

Automated Scanning

Media are whatever substances we use to convey or store information. This includes hard drives, optical discs, tapes, and even paper

Tracking what software is installed on which systems, and for which users, is an important part of software asset management

Configuration management (CM) is the process of establishing and maintaining consistent baselines on all of our systems

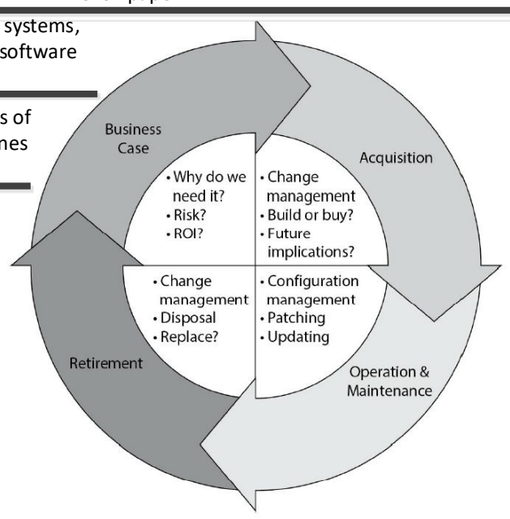
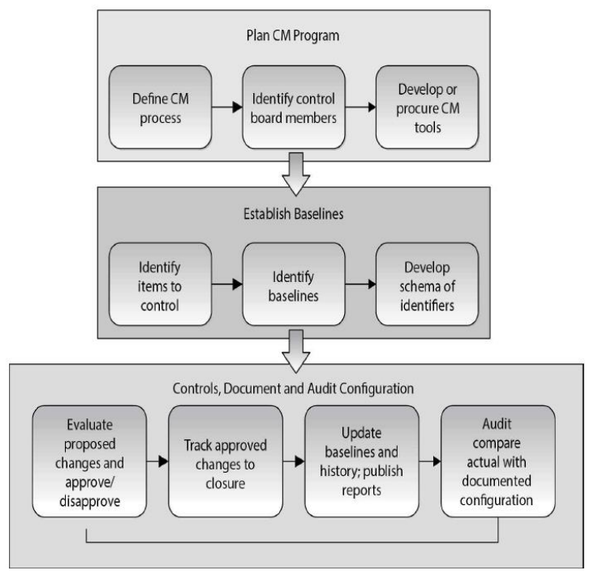


Figure 7-10 Asset management life cycle

Change Management Flow



Configuration Management vs. Change Management

Change management, which we discuss in Chapter 8, is a *business* process aimed at deliberately regulating the changing nature of business activities such as projects. It is concerned with issues such as changing the features in a system being developed or changing the manner in which remote workers connect to the internal network. While IT and security personnel are involved in change management, they are usually not in charge of it.

Configuration management is an *operational* process aimed at ensuring that controls are configured correctly and are responsive to the current threat and operational environments. Continuing our earlier two examples, configuration management would deal with how to configure the software system so that the new features are integrated with existing controls or, failing that, how to modify that controls so that they maintain the required security while allowing the new feature.

As an information security professional, you would likely lead in configuration management, but simply participate in change management processes.

Which of the following has incorrect RAID level mappings?
i. 0 - Data striped over several drives. No redundancy or parity is involved
ii. 1 - Mirroring of drives
iii. 2 - Data striping over all drives at the bit level.
iv. 3 - Data striping over all drives and parity data held on one drive

- None of them
- All of them
- iii
- iv

Incorrect

Incorrect.
RAID 0 - Data striped over several drives. No redundancy or parity is involved.
RAID 1 - Mirroring of drives. Data are written to two drives at once.
RAID 2 - Data striping over all drives at the bit level.
RAID 3 - Data striping over all drives and parity data held on one drive.

Next Question

Sue needs to identify a storage system technology that reduces both wear on the drives and also reduces power consumption. Which of the following technologies is the best fit for these types of requirements?

- RAIT
- RAID
- MAID
- TAT

Incorrect

Incorrect. Massive array of inactive disks is a technology that uses a large group of hard disk drives, hundreds or even thousands, with only those drives that are needed actively spinning at any given time. MAID is a storage system solution that reduces both wear on the drives and also reduces power consumption. Because only specific disks spin at a given time, what is not in use is literally a massive array of idle disks, which also means the system produces less heat than other large storage systems.

Next Question

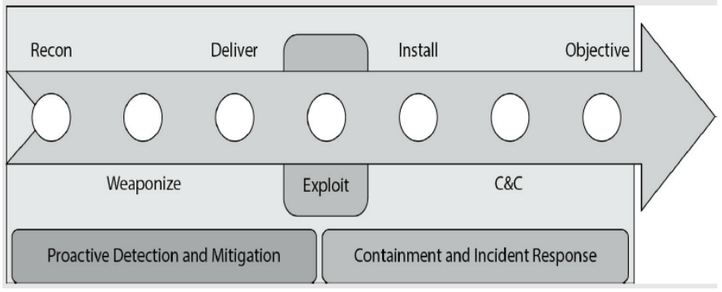
How attackers attack?

The Cyber Kill Chain

Even as we think about how best to manage incidents, it is helpful to consider a model for the attacker's behaviors. In their seminal 2011 paper titled "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Hutchins, Cloppert, and Amin describe a seven-stage intrusion model that has become an industry standard. Their seven stages are described here:

1. Reconnaissance The adversary has developed an interest in your organization as a target and begins a deliberate information-gathering effort to find vulnerabilities.
2. Weaponization Armed with detailed-enough information, the adversary determines the best way into your systems and begins preparing and testing the weapons to be used against you.
3. Delivery In this phase, the cyber weapon is delivered into your system. In over 95 percent of the published cases, this delivery happens via e-mail and usually in the form of a link to a malicious website.
4. Exploitation The malicious software is executing on a CPU within your network. This may have launched when the target user clicked a link, opened an attachment, visited a website, or plugged in a USB thumb drive. It could also (in somewhat rare cases) be the result of a remote exploit. One way or another, the attacker's software is now running in your systems.
5. Installation Most malicious software is delivered in stages. First, there is the exploit that compromised the system in the prior step. Then, some other software is installed in the target system to ensure persistence, ideally with a good measure of stealth.
6. Command and Control (C&C) Once the first two stages of the software (exploit and persistence) have been executed, most malware will "phone home" to the attackers to let them know the attack was successful and to request updates and instructions.
7. Actions on the Objective Finally, the malware is ready to do whatever it is it was designed to do. Perhaps the intent is to steal intellectual property and send it to an overseas server. Or perhaps this particular effort is an early phase in a grander attack, so the malware will pivot off the compromised system. Whatever the case, the attacker has won at this point.

As you can probably imagine, the earlier in the kill chain we identify the attack, the greater our odds are of preventing the adversaries from achieving their objectives. This is a critical concept in this model: if you can thwart the attack before stage four (exploitation), you stand a better chance of winning. Early detection, then, is the key to success.



Types of Investigation are;
1. Administrative (someone broke AUP)
2. Criminal (someone perpetrate a crime)
3. Civil (someone boke a law)
4. Regulatory (regulatory authority can ask enterprise to make them ready for investigation)

The next crucial piece is to keep **a proper chain of custody** of the evidence. Because evidence from these types of crimes can be very volatile and easily dismissed from court because of improper handling, it is important to follow very strict and organized procedures when collecting and tagging evidence in every single case—no exceptions!

Different Types of Assessments an Investigator Can Perform

There are four general types of assessments performed by investigators.

Network analysis
- Traffic analysis
- Log analysis
- Path tracing

Media analysis
- Disk imaging
- Timeline analysis (modify, access, create times)
- Registry analysis
- Slack space analysis
- Shadow volume analysis

Software analysis
- Reverse engineering
- Malicious code review
- Exploit review

Hardware/embedded device analysis
- Dedicated appliance attack points
- Firmware and dedicated memory inspections
- Embedded operating systems, virtualized software, and hypervisor analysis

For Forensic investigation, all data, bit level and even hard drive sector level should be retrieved so that proper investigation can be completed, this can be done using specific forensic tool such as Forensic Toolkit (FTK), EnCase Forensic

Evidence Life Cycle;
Collection and identification
- Storage, preservation, and transportation
- Presentation in court
- Return of the evidence to the victim or own

It is important that evidence be relevant, complete, sufficient, and reliable

Security Operations

How to respond to attack?
- Detect
- Think about response
  - Think how to mitigate? You may mitigate by attracting attacker to Honeypot or Honeynet and get some time in the meanwhile to investigate further, involve legal here because honeynets and honeypots can introduce liability issues
- Report it
- recovery
  - Remediate - Another aspect of remediation is the identification of your indicators of attack (IOA) that can be used in the future to detect this attack in real time (i.e., as it is happening) as well as indicators of compromise (IOC), which tell you when an attack has been successful and your security has been compromised.
  - Computer Forensics and Collection of Evidence
    - In some situations, it is best to remove the system from the network, dump the contents of the memory, power down the system, and make a sound image of the attacked system and perform forensic analysis on this copy
    - Within the United States, there is the Scientific Working Group on Digital Evidence (SWGDE), which aims to ensure consistency across the forensic community. Read there rules on page 1203
    - Investigators can perform different type of analysis

Contingency meaning "a future event or circumstance which is possible but cannot be predicted with certainty"

Pervasive meaning "(especially of an unwelcome influence or physical effect) spreading widely throughout an area or a group of people"

- Contingency management defines what should take place during and after an incident
  - BCP addresses how to keep the organization in business after a disaster takes place. It is about the survivability of the organization and making sure that critical functions can still take place even after a disaster. Contingency plans address how to deal with small incidents that do not qualify as disasters, as in power outages, server failures, a down communication link to the Internet, or the corruption of software.

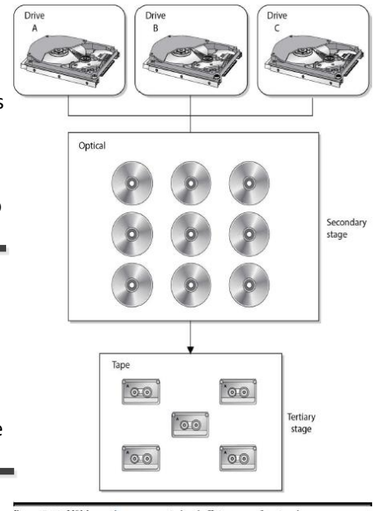
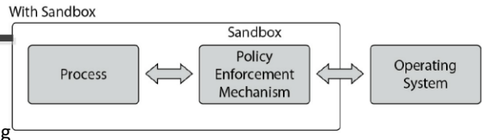


Figure 7-12 HSM provides an economical and efficient way of storing data.

- Pervasive Controls are those that are highly used & recommended
  - Continuous Monitoring
  - Intrusion Detection and Prevention
    - The options include host-based intrusion detection systems (HIDSs), network intrusion detection systems (NIDSs), and wireless intrusion detection systems (WIDSs). Each may operate in detection or prevention mode depending on the specific product and how it is employed
  - Whitelisting and Blacklisting
  - Antimalware
  - Vulnerabilities are usually discovered by security researchers who notify vendors and give them some time (at least two weeks) to work on a patch before the researchers make their findings public. This is known as responsible disclosure
  - Red Team Concept - A red team is a group of trusted individuals whose job is to look at something from an adversary's perspective. The term red team exercise is oftentimes used synonymously with penetration test.
    In reality, a red team exercise can apply to any aspect of an organization (people, processes, facilities, products, ideas, information systems), whereas a penetration test is usually concerned with facilities and/or information systems only
  - Human Vulnerability Assessment Steps
    - Open-source intelligence (OSINT) use open source to get info about target, assess the info and the execute the attack to get sensitive info
  - Sand Boxing
    - A sandbox is an application execution environment that isolates the executing code from the operating system to prevent security violations
  - HonetNet (like Honeypot)
    - A honeynet is an entire network that is meant to be compromised
  - Honey Clients
    - honeyclients are synthetic applications meant to allow an attacker to conduct a client-side attack while also allowing the friendly analysts an opportunity to observe the techniques being used by their adversaries



  - Managed Security Service Providers
    - MSSPs typically offer a variety of services ranging from point solutions to taking over the installation, operation, and maintenance of all technical (and some cases physical) security controls. (Sorry, you still have to provide policies and many administrative controls.)

  - The Incident Management Process
    - There are many incident management models, but all share some basic characteristics. They all require that we identify the event, analyze it to determine the appropriate counteractions, correct the problem(s), and, finally, keep the event from happening again. (ISC)2 has broken out these four basic actions and prescribes seven phases in the incident management process: detect, respond, mitigate, report, recover, remediate, and learn
      - Events and Incident, small difference
        - An event is any occurrence that can be observed, verified, and documented, whereas an incident is one or more related events that negatively affect the company and/or impact its security posture

Enticement (is legal meaning that entice attacker to attack and he genuinely then attack with bad intention) and Entrapment (is illegal meaning that entice user to use some function/download files but the user doesn't intend to attack)

End Users Consideration

The first issue pertaining to users is how they will be notified of the disaster and who will tell them where to go and when. A tree structure of managers can be developed so that once a disaster hits, the person at the top of the tree calls two managers, and they in turn call three managers, and so on until all managers are notified. The BCP committee identified the most critical functions of the company during the analysis stage, and the employees who carry out those functions must be put back to work first

In the context of security, due care means that a company did all it could have reasonably done, under the circumstances, to prevent security breaches, and also took reasonable steps to ensure that if a security breach did take place, proper controls or countermeasures were in place to mitigate the damages. In short, due care means that a company practiced common sense and prudent management and acted responsibly. Due diligence means that the company properly investigated all of its possible weaknesses and vulnerabilities

Fault tolerance and resiliency are oftentimes used synonymously, though, in reality, they mean subtly different things. Fault tolerance means that when a fault happens, there's a system in place (a backup or redundant one) to ensure services remain uninterrupted. Resiliency means that the system continues to function, albeit in a degraded fashion, when a fault is encountered.

Redundancy, fault tolerance, resiliency, and failover capal
increase the reliability of a system or network, where relia
the probability that a system performs the necessary func
a specified period under defined conditions

Due Care vs. Due Diligence

Due diligence is the act of gathering the necessary information so the best decision-making activities can take place. Before a company purchases another company, it should carry out due diligence activities so that the purchasing company does not have any "surprises" down the road. The purchasing company should investigate all relevant aspects of the past, present, and predictable future of the business of the target company. If this does not take place and the purchase of the new company hurts the original company financially or legally, the decision makers could be found liable (responsible) and negligent by the shareholders.

In information security, similar data gathering should take place so that there are no "surprises" down the road and the risks are fully understood before they are accepted. If a financial company is going to provide online banking functionality to its customers, the company needs to fully understand all the risks this service entails for the company. Website hacking will increase, account fraud will increase, database attacks will increase, social engineering attacks will increase, etc. While this company is offering its customers a new service, it is also making itself a juicier target for attackers and lawyers. The company needs to carry out due diligence to understand all these risks before offering this new service so that the company can make the best business decisions. If it doesn't implement proper countermeasures, the company opens itself up to potential criminal

Great explanation of MTD, RTO and WRT

The recovery time objective (RTO) is the maximum time period within which a business process must be restored to a designated service level after a disaster to avoid unacceptable consequences associated with a break in business continuity. The RTO value is smaller than the MTD value, because the MTD value represents the time after which an inability to recover significant operations will mean severe and perhaps irreparable damage to the organization's reputation or bottom line. The RTO assumes that there is a period of acceptable downtime. This means that a company can be out of production for a certain period of time (RTO) and still get back on its feet. But if the company cannot get production up and running within the MTD window, the company is sinking too fast to properly recover. The work recovery time (WRT) is the remainder of the overall MTD value after the RTO has passed. RTO usually deals with getting the infrastructure and systems back up and running, and WRT deals with restoring data, testing processes, and then making everything "live" for production purposes.

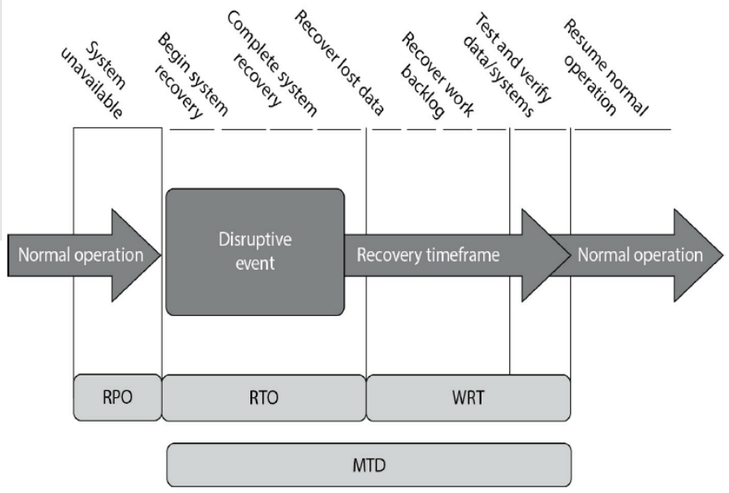


Figure 7-16 Metrics used for disaster recovery

So, how do we know which data has changed and needs to be backed up without having to look at every file's modification date? This is accomplished by an archive bit.

A differential process backs up the files that have been modified since the last full backup. When the data needs to be restored, the full backup is laid down first, and then the most recent differential backup is put down on top of it. Most companies choose to combine a full backup with a differential or incremental backup. The differential process does not change the archive bit value.

An incremental process backs up all the files that have changed since the last full or incremental backup and sets the archive bit to 0.

Electronic vaulting makes copies of files as they are modified and periodically transmits them to an offsite backup site. The transmission does not happen in real time, but is carried out in batches. So, a company can choose to have all files that have been changed sent to the backup facility every hour, day, week, or month. Electronic vaulting is a method of transferring bulk information to offsite facilities for backup purposes.

Remote journaling is another method of transmitting data offsite, but this usually only includes moving the journal or transaction logs to the offsite facility, not the actual files. These logs contain the deltas (changes) that have taken place to the individual files. If and when data is corrupted and needs to be restored, the bank can retrieve these logs, which are used to rebuild the lost data. Journaling is efficient for database recovery, where only the reapplication of a series of changes to individual records is required to resynchronize the database.

Remote journaling takes place in real time and transmits only the file deltas. Electronic vaulting takes place in batches and moves the entire file that has been updated.

Disk shadowing is used to ensure the availability of data and to provide a fault-tolerant solution by duplicating hardware and maintaining more than one copy of the information.

If only disk mirroring is used, then each disk would have a corresponding mirrored disk that contains the exact same information.

A software escrow, in which a third party holds the source code, backups of the compiled code, manuals, and other supporting materials. A contract between the software vendor, customer, and third party outlines who can do what, and when, with the source code.

The BCP should also include backup solutions for the following:

- Network and computer equipment
- Voice and data communications resources
- Human resources
- Transportation of equipment and personnel
- Environment issues (HVAC)

Security Operations

BCP Terms for disaster

Hot Site Advantages:

- Ready within hours for operation
- Highly available
- Usually used for short-term solutions, but available for longer stays
- Annual testing available

Hot Site Disadvantages:

- Very expensive
- Limited on hardware and software choices

Warm and Cold Site Advantages:

- Less expensive
- Available for longer timeframes because of the reduced costs
- Practical for proprietary hardware or software use

Warm and Cold Site Disadvantages:

- Operational testing not usually available
- Resources for operations not immediately available

EXAM TIP A hot site is a subscription service. A redundant site, in contrast, is a site owned and maintained by the company, meaning the company does not pay anyone else for the site. A redundant site might be "hot" in nature, meaning it is ready for production quickly. However, the CISSP exam differentiates between a hot site (a subscription service) and a redundant site (owned by the company).

Disruptions, in BCP terms, are of three main types: nondisasters, disasters, and catastrophes

A nondisaster is a disruption in service that has significant but limited impact on the conduct of business processes at a facility. The solution could include hardware, software, or file restoration. A disaster is an event that causes the entire facility to be unusable for a day or longer. This usually requires the use of an alternate processing facility and restoration of software and data from offsite copies. The alternate site must be available to the company until its main facility is repaired and usable. A catastrophe is a major disruption that destroys the facility altogether. This requires both a short-term solution, which would be an offsite facility, and a long-term solution, which may require rebuilding the original facility

Hot Site, Warm Site and Cold Site services are generally provided by, Service Bureau, a company that has additional space and capacity to provide applications and services such as call centers.

Contingency Company also provides services during disaster time. They provide basic services such as backup telecom service

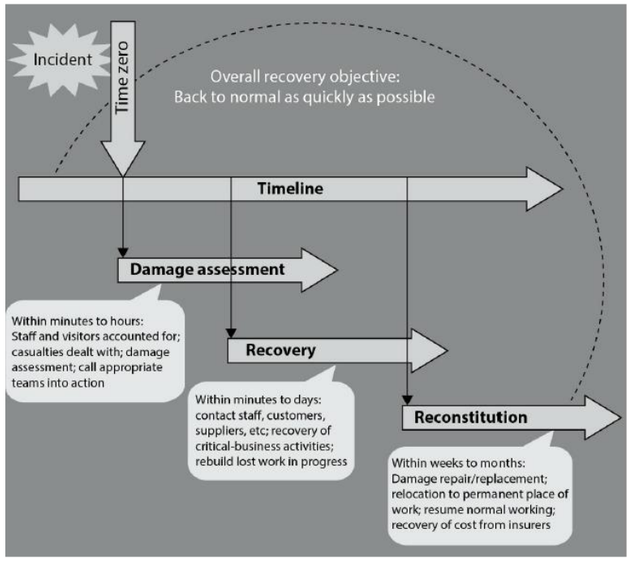
Offsite Location

When choosing a backup facility, it should be far enough away from the original site so that one disaster does not take out both locations. In other words, it is not logical to have the backup site only a few miles away if the company is concerned about tornado damage, because the backup site could also be affected or destroyed. There is a rule of thumb that suggests that alternate facilities should be, at a bare minimum, at least 5 miles away from the primary site, while 15 miles is recommended for most low-to-medium critical environments, and 50 to 200 miles is recommended for critical operations to give maximum protection in cases of regional disasters.

Assessment after Disaster

A role, or a team, needs to be created to carry out a damage assessment once a disaster has taken place. The assessment procedures should be properly documented and include the
following steps:

- Determine the cause of the disaster.
- Determine the potential for further damage.
- Identify the affected business functions and areas.
- Identify the level of functionality for the critical resources.
- Identify the resources that must be replaced immediately.
- Estimate how long it will take to bring critical functions back online.
- If it will take longer than the previously estimated MTD values to restore operations, then a disaster should be declared and the BCP should be put into action.



Insurance

Different types of insurance policies can be purchased by companies, cyber insurance being one of them. Cyber insurance is a new type of coverage that insures losses caused by denial-of-service attacks, malware damages, hackers, electronic theft, privacy-related lawsuits, and more.

A company could also choose to purchase a business interruption insurance policy. With this type of policy, if the company is out of business for a certain length of time, the insurance company will pay for specified expenses and lost earnings

Studies have shown that 65 percent of businesses that lose computing capabilities for over one week are never able to recover and subsequently go out of business

Proposed Teams for DR

The DR coordinator needs to define several different teams that should be properly trained and available if a disaster hits. Which types of teams an organization needs depends upon the organization. The following are some examples of teams that a company may need to construct:

- Damage assessment team
- Recovery team
- Relocation team
- Restoration team
- Salvage team
- Security team

The restoration team should be responsible for getting the alternate site into a working and functioning environment, and the salvage team should be responsible for starting the recovery of the original site.

Occupant Emergency Plan (OEP), plan focus on Personal Safety and guides what to should be done by facility occupants in case of emergency

COOP (Continuity of operations) focuses on restoring an organization's (usually a headquarters element) essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. This term is commonly used by the U.S. government to denote BCP.

Due Care vs. Due Diligence

Due diligence is the act of gathering the necessary information so the best decision-making activities can take place. Before a company purchases another company, it should carry out due diligence activities so that the purchasing company does not have any "surprises" down the road. The purchasing company should investigate all relevant aspects of the past, present, and predictable future of the business of the target company. If this does not take place and the purchase of the new company hurts the original company financially or legally, the decision makers could be found liable (responsible) and negligent by the shareholders.

In information security, similar data gathering should take place so that there are no "surprises" down the road and the risks are fully understood before they are accepted. If a financial company is going to provide online banking functionality to its customers, the company needs to fully understand all the risks this service entails for the company. Website hacking will increase, account fraud will increase, database attacks will increase, social engineering attacks will increase, etc. While this company is offering its customers a new service, it is also making itself a juicier target for attackers and lawyers. The company needs to carry out due diligence to understand all these risks before offering this new service so that the company can make the best business decisions. If it doesn't implement proper countermeasures, the company opens itself up to potential criminal charges, civil suits, regulatory fines, loss of market share, and more.

Due care pertains to acting responsibly and "doing the right thing." It is a legal term that defines the standards of performance that can be expected, either by contract or by implication, in the execution of a particular task. Due care ensures that a minimal level of protection is in place in accordance with the best practice in the industry.

If a company does not have sufficient security policies, necessary countermeasures, and proper security awareness training in place, it is not practicing due care and can be found negligent. If a financial institution that offers online banking does not implement TLS for account transactions, for example, it is not practicing due care.

Many times due diligence (data gathering) has to be performed so that proper due care (prudent actions) can take place.

For example, let's say company A and company B have constructed an extranet. Company A does not put in controls to detect and deal with viruses. Company A gets infected with a destructive virus and it is spread to company B through the extranet. The virus corrupts critical data and causes a massive disruption to company B's production. Therefore, company B can sue company A for being negligent. Both companies need to make sure they are doing their part to ensure that their activities, or the lack of them, will not negatively affect another company, which is referred to as downstream liability

EXAM TIP Proximate cause is an act or omission that naturally and directly produces a consequence. It is the superficial or obvious cause for an occurrence. It refers to a cause that leads directly, or in an unbroken sequence, to a particular result. It can be seen as an element of negligence in a court of law.

Procurement Process

Before purchasing any product or service, the organization's security requirements need to be fully understood so that they can be expressed and integrated into the procurement process. Procurement is not just purchasing something, but includes the activities and processes involved with defining requirements, evaluating vendors, contract negotiation, purchasing, and receiving the needed solution. While procurement is an activity an organization carries out to properly identify, solicit, and select vendors for products and services, vendor management is an activity that involves developing and monitoring vendor relationships after the contracts are in place. A vendor management governing process needs to be set up, which includes performance metrics, SLAs, scheduled meetings, a reporting structure, and someone who is directly responsible

B.

A pseudoflaw is a false vulnerability in a system that may attract an attacker. A honeynet is a network of multiple honeypots that creates a more sophisticated environment for intruders to explore. A darknet is a segment of unused network address space that should have no network activity and, therefore, may be easily used to monitor for illicit activity. A warning banner is a legal tool used to notify intruders that they are not authorized to access a system.

A disaster is any event that can disrupt normal IT operations and can be either natural or manmade. Hacking and terrorism are examples of manmade disasters, while flooding and fire are examples of natural disasters.

The checklist review is the least disruptive type of disaster recovery test. During a checklist review, team members each review the contents of their disaster recovery checklists on their own and suggest any necessary changes. During a tabletop exercise, team members come together and walk through a scenario without making any changes to information systems. During a parallel test, the team actually activates the disaster recovery site for testing, but the primary site remains operational. During a full interruption test, the team takes down the primary site and confirms that the disaster recovery site is capable of handling regular operations. The full interruption test is the most thorough test but also the most disruptive.

Entitlement refers to the privileges granted to users when an account is first provisioned.

1. So, while controls are critical to our systems' security, they need to be considered in the context of overall software quality

2. The controls can be preventive, detective, or corrective. While security controls can be administrative and physical in nature, the controls used within software are usually more technical in nature.

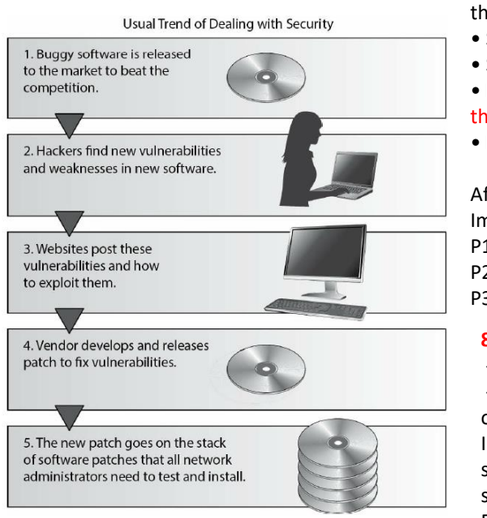


Figure 8-1 The usual trend of software being released to the market and how security is dealt with

3. NetBIOS services, which have few, if any, security controls, can be enabled to permit sharing resources in Windows environments. Other services, such as File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), and older versions of the Simple Network Management Protocol (SNMP), have no real safety measures in place. Some of these services (as well as others) are enabled by default, so when an administrator installs an operating system and does not check these services to properly restrict or disable them, they are available for attackers to uncover and use.

4. There have been several software development life cycle (SDLC) models developed over the years, which we will cover later in this section, but the crux of each model deals with the following phases:

- Requirements gathering Determine why to create this software, what the software will do, and for whom the software will be created
- Design Deals with how the software will accomplish the goals identified, which are encapsulated into a functional design
- Development Programming software code to meet specifications laid out in the design phase and integrating that code with existing systems and/or libraries
- Testing Verifying and validating software to ensure that the software works as planned and that goals are met
- Operations and maintenance Deploying the software and then ensuring that it is properly configured, patched, and monitored

5. Project management is an important part of product development, and security management is an important part of project management.

6. If a software product is being developed for a specific customer, it is common for a Statement of Work (SOW) to be developed, which describes the product and customer requirements.

7. Requirements Gathering Phase

Following items should be accomplished in this phase:

- Security requirements
- Security risk assessment
- Privacy risk assessment (what private data this software will process)
- Risk-level acceptance.

After a privacy risk assessment, a Privacy Impact Rating can be assigned;
P1, High Privacy Risk
P2, Moderate Privacy Risk
P3, Low Privacy Risk

8. Design Phase

- Maps theory to reality
- Software requirements concludes to 3 types of software behavior;

Informational model – what information software will process (example process virus signatures)
Functional model – what function expected (example scan a hard drive)
Behavioral model – how should behave if change happens (if virus detected, then scan a hard drive)

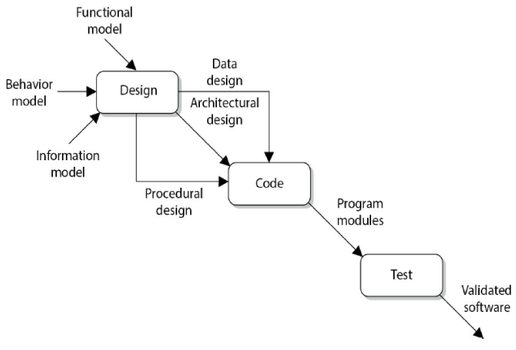


Figure 8-2 Information from three models can go into the design.

From a security point of view, the following items should also be accomplished in this phase:

- Attack surface analysis
- Threat modeling

It is common for software development teams to develop threat trees. See on page 1296!

9. Development Phase

Computer-aided software engineering (CASE) to assist coders. Every items should be properly documented in this phase. There are identified 25 top ten security vulnerabilities items (page 1299 list). A particularly important area of scrutiny is input validation. Security has to be addressed at each phase of SDLC, with this phase being one of the most critical.

Static analysis is a technique meant to help identify software defects or security policy violations using automated tools (can never reveal logical errors and design flaws, and therefore must be used in conjunction with manual code review) , while code review is by humans.

10. Testing Phase - test-driven development is an approach to test module by module - and tends to result in much higher-quality code - meant to simulate a range of inputs to which the code may be exposed. Testing technique called Fuzzer or Fuzzing - used to discover flaws and vulnerabilities in software by sending large amounts of malformed, unexpected, or random data to the target program in order to trigger failures.

- Beta testing can be carried out by various potential customers and agencies. Then the product is formally released to the market or customer

11. Operations and Maintenance Phase

Once the software code is developed and properly tested, it is released so that it can be implemented within the intended production environment.

- Verification vs. Validation

Verification determines if the product accurately represents and meets the specifications. After all, a product can be developed that does not match the original specifications, so this step ensures the specifications are being properly met. It answers the question: Did we build the **product right**?

Validation determines if the product provides the necessary solution for the intended real-world problem. In large projects, it is easy to lose sight of the overall goal. This exercise ensures that the main goal of the project is met. It answers the question: Did we build the **right product**?

12. **Summary of SDLC & Security**

The main phases of a software development life cycle are shown here with some specific security tasks.

Requirements gathering:
- Security risk assessment
- Privacy risk assessment
- Risk-level acceptance
- Informational, functional, and behavioral requirements

Design:
- Attack surface analysis
- Threat modeling

Development:
- Automated CASE tools
- Static analysis

Testing:
- Dynamic analysis
- Fuzzing
- Manual testing
- Unit, integration, acceptance, and regression testing

Operations and maintenance:
- Final security review

13. Software Development Methodologies

- **Waterfall Methodology** – very rigid, all requirements gathered in beginning and testing done at the end of project, hence not flexible, not suitable for large projects
- V-shaped methodology – better than waterfall – still rigid but recommends test after every phase – not flexible and recommended for dynamic requirements
- **Prototyping** – idea that creates a prototype and then built software on top of it – so it is more practical in approach – but no security consideration!!
- **Incremental Methodology** – its like multiple waterfalls, one after one another – repetitive – until final product is in hand – better then earlier approach!
- **Spiral Methodology** – its an iterative approach of understanding requirement, then risk analysis, then development and test and then goes through again if requirement or scope changes, until final product is delivered
- **Rapid Application Development** - methodology 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 – benefit is that if requirements keep on changing – they can be adjusted by delivering prototypes quickly
- **Agile Method** – promotes flexibility – rather than rigid process following – it tries to breakdown tasks into smaller segment and deliver those segments quickly – rather than following bureaucratic long approach – definition from book "The Agile methodology 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.

Agile (Scrum is part of agile) and RAD involves customer closely & hence customer does not get any surprises at the end – things remains within budget and expectation. Extreme Programming (another method of Agile) is a development methodology that takes code reviews to the extreme - continuous reviews are accomplished using an approach called pair programming, in which one programmer dictates the code to her partner, who then types it.

14. Summary of all methodologies

Waterfall Very rigid, sequential approach that requires each phase to complete before the next one can begin. Difficult to integrate changes. Inflexible methodology.
- V-shaped Emphasizes verification and validation at each phase and testing to take place throughout the project, not just at the end.
- Prototyping Creating a sample or model of the code for proof-of-concept purposes.
- Incremental Multiple development cycles are carried out on a piece of software throughout its development stages. Each phase provides a usable version of software.
- Spiral Iterative approach that emphasizes risk analysis per iteration. Allows for customer feedback to be integrated through a flexible evolutionary approach.
- Rapid Application Development Combines prototyping and iterative development procedures with the goal of accelerating the software development process.
- Agile Iterative and incremental development processes that encourage team-based collaboration. Flexibility and adaptability are used instead of a strict process structure.

15. DevOps(Development + Operations) when development and IT Ops team work in harmony. Good for orgenization!

16. Capability Maturity Model Integration - is a comprehensive, integrated set of guidelines for developing products and software - describes procedures, principles, and practices that underlie software development process maturity – its ultimate goal is process improvement - five maturity levels of the CMMI model are – Initial (Level-1), Repeatable (Level-2), Defined (Level-3), Managed (Level-4), Optimized (Level-5) – its scale that measures maturity of process – page 1321 AIO

17. Change Management – is Management Process and Change Control is part of Change Management - Change management is a systematic approach to deliberately regulating the changing nature of projects - Change control is the process of controlling the specific changes that take place during the life cycle of a system and documenting the necessary change control activities

18. Security of Software Development Environment – 3 key points to secure - the development platforms, the code repositories, and the software configurations. 1st is Development Platforms - secure the devices and environment on which our software engineers practice, separate them from production (VLAN and if remote users, connect with VPN). 2nd is code repository - place where code is saved by developers until tested – connect to repositories using SSH or secure connectivity medium – put that on Intranet for even secure approach. 3rd Software configuration – tool called SCM (software configuration management (SCM) manages these changes in a proper manner – its actually a versioning tool that keep changes of code in an updated version – synchronized.

19. The customer oftentimes gets compiled code instead of source code. Compiled code is code that has been put through a compiler and is unreadable to humans.

20. Secure Coding – meaning best practices and methods to ensure that our produced codes are secure – OWASP Project has 10 top attacks on codes (page 1328 good read) and Top 10 secure practice on page 1329 by Carnegie Melon Uni – they all focus on ensuring – input validation, simpler code lines, default deny and follow structured approach

21. Programming Languages
The following lists the basic software programming language generations:
• Generation one Machine language
• Generation two Assembly language
• Generation three High-level language
• Generation four Very high-level language
• Generation five Natural language

Higher the level, more abstract the language is, meaning concentrating more on programming features rather than computer intricacies.
Definitions/Concepts;
Assemblers - tools that convert assembly language source code into machine code
Compilers - tools that convert high-level language statements into the necessary machine-level format (.exe, .dll, etc.) for specific processors to understand. The compiler transforms instructions from a source language (high-level) to a target language (machine)
- If a programming language is considered "interpreted," then a tool called an interpreter does the last step of transforming high-level code to machine-level code. For example, applications that are developed to work in a .NET environment are translated into an intermediate, platform-independent format
- Garbage collection is an automated way for software to carry out part of its memory management tasks. A garbage collector identifies blocks of memory that were once allocated but are no longer in use and deallocates the blocks and marks them as free. It also gathers scattered blocks of free memory and combines them into larger blocks. It helps provide a more stable environment and does not waste precious memory

22. Object Oriented and Non-Object Oriented Languages
Object and Class Definition - OOP works with classes and objects. A real-world object, such as a table, is a member (or an instance) of a larger class of objects called "furniture." These attributes apply if a chair, table, or loveseat object is generated, also referred to as instantiated (example page 1336)

Object-oriented design	Procedural design
• Similar object classes • Common interfaces • Common usage • Code reuse—inheritance • Defers implementation and algorithm decisions	• Algorithm centered—forces early implementation and algorithm decisions • Exposes more details • Difficult to extend • Difficult to maintain

23. Definitions related to OOP;
- A method is the functionality or procedure an object can carry out
- The objects encapsulate the attribute values, which means this information is packaged under one name and can be reused as one entity by other objects
- Objects need to be able to communicate with each other, and this happens by using messages that are sent to the receiving object's API
- An object can have a shared portion and a private portion. The shared portion is the interface (API) that enables it to interact with other components
- The private portion of an object is how it actually works and performs the requested operations
- Data hiding is provided by encapsulation, which protects an object's private data from outside access
- The objects can be catalogued in a library
- **Polymorphism** comes from the Greek, meaning "having multiple forms , takes place when different objects respond to the same command, input, or message in different ways. Two objects can receive the same input and have different outputs.

24. Data Modeling; Data modeling considers data independently of both the way the data is processed and the components that process the data. A data model follows an input value from beginning to end and verifies that the output is correct

24. Data Structures; set of data that are either sits alone or combined in hierarchical structure – its like is a representation of the logical relationship between elements of data

Cohesion and Coupling in OOP

25. Cohesion - Cohesion reflects how many different types of tasks a module can carry out. If a module
carries out only one task (i.e., subtraction) or tasks that are very similar (i.e., subtract, add, multiply), it is described as having high cohesion, which is a good thing. The higher the cohesion, the easier it is to update or modify and not affect other modules that interact with it.

Coupling is a measurement that indicates how much interaction one module requires to carry out its tasks. If a module has low (loose) coupling, this means the module does not need to communicate with many other modules to carry out its job. High (tight) coupling means a module depends upon many other modules to carry out its tasks. Low coupling is more desirable because the modules are easier to understand and easier to reuse

26. Distributed Computing – method where services are connected through heterogeneous network and request are made through Remote Procedure Calls (RPC). Distributed Computing Environment (DCE) is a standard developed by the Open Software Foundation (OSF), also called Open Group. Following sections are about Distributed Computing

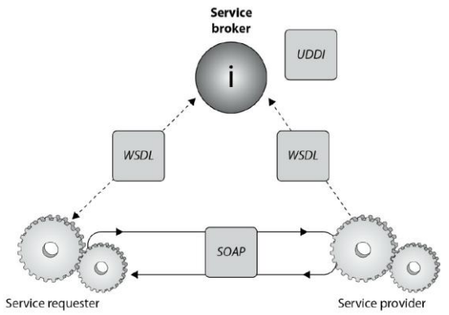
27. Common Object Request Broker Architecture (CORBA) - a standard that defines how 2 objects at diffferent platforms communicate together - (CORBA) is an open object-oriented standard architecture developed by the Object Management Group (OMG) –
The CORBA model provides standards to build a complete distributed environment. It contains two main parts: system-oriented components (object request brokers [ORBs] and object services) and application-oriented components (application objects and common facilities).

28. Component Object Model (COM) & Distributed COM (DCOM) – protocols/standards that allow objects to communicate in different systems

29. .NET Framework is Distributed Computing, only based on Microsoft Platform. Code written in any language is compiled with "platform neutral" Common Intermediate Language (CIL) and then transformed

30. Java Platform, Enterprise Edition is also Distributed Computing Environment based on Java language. It also used CORBA for inter-platform communication

31. Services Oriented Architecture (SOA) - standardized access to the most needed services to many different applications at one time. Has 3 main components;
- WSDL (Web Services Description Language (WSDL) - provides a machine-readable description of the specific operations provided by the service – acts as broker between request and server
- UDDI (Universal Description, Discovery and Integration) - is an XML-based registry that lists available services
- SOAP - The consumer then requests and accesses the service using SOAP, which is an XML-based protocol that is used to exchange messages between a requester and provider of a web service



32. Beauty of SOAP - SOAP is an XML-based protocol that encodes messages in a web service environment - request for an application comes from one computer (client) and is transmitted over a web-based environment (i.e., Internet) to another computer (server). While there are various distributed computing technologies, SOAP makes it easy by using XML and HTTP, which are already standard web formats

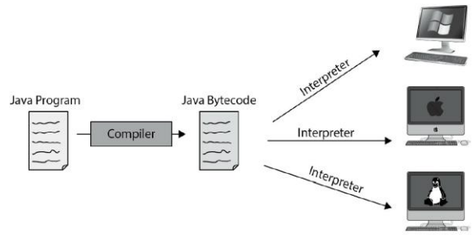
33. Summary of DCE
DCE Initial – Unix Based
DCE Non-Windows – CORBA
DCE Windows – DCOM and the .NET
DCE Web Based – SOA + SOAP
DCE Java Based – Java EE

Each of these has the same basic goal, which is to allow a client application component on one computer to be able to communicate with a server application on another computer. The biggest difference between these models pertains to the environment the applications will be working within: Unix, Windows, heterogeneous, or web-based.

34. Mobile Code – a code that traverse network and executes at remote
1st – Java Applet (small Java program) – browser may download from website – and then Java Virtual Machine on a local system executes it within safe environment (Sand Box) – risk is that hackers can bypass sandbox
2nd – ActiveX – similar to Java – but Windows based – risk is ActiveX installs directly on hard drive and unlike Java that has Sandbox, ActiveX executes on OS – far greater reach than Java then!

SIDE NOTE: Beauty of Java and Compiler & Interpreter
- Java code produces "bytecode" independent of platform – then Interpreter – change that bytecode to machine code for execution on any particular machine.

Compiler – transform code to executable code
Interpreter – interpret compiled code for specific OS



35. Specific Threats for Web Environment
1st Web Administration – manage device through web – limit access to certain users/ IP add – also may use Out of Band, not web at least
2nd Authentication/Access Control – hackers can hack password – always use safe websites, SSL/TLS
3rd Input Validation – attackers can enter rogue info, invalid strings. SQL injection and XSS Cross Site Scripting are these attacks!
4th Parameter Validation – checks the expected value that is entered in web page.

Difference between Input Validation & Parameter validation is – Input Validation checks if user entered correct value, Parameter Validation checks if user has input value where web server was not expecting anything to be entered!

5th Session Management – hackers can manipulate session ID to gain access to web – encrypt conversation between web and client

36. Data Base Management and Models
1st Relational Model – Data is shown as rows and columns – cell represents intersection of rows and columns – most used model
2nd Hierarchical Data Model – tree structure – (page 1380), not widely used
3rd Networked Database Model – like hierarchical but values are fully connected for quicker search (page 1382)
4th Object Oriented Model – Data values are define as Objects and its types – dynamic in nature – helps in querying data quickly
NOTE: SQL is data query language – when user trying to access data from database, it is using SQL

37. Object Relational Database Management System – simply – relational database is given front end, based on Objects – user needs to get info out of data is managed by Objects (vary in nature)

39. Data Dictionary is metadata for Database. Meaning that when applications access database, Database Management Software, checks with Data Dictionary to process

40. Ensuring Data Integrity in Databases – Integrity is confidence that data is TRUE!
3 types of data integrity;
Semantic – ensures data type integrity
Referential – ensures data reference integrity from one table to another
Entity – ensures data's location in database is correct

41. In order to ensure this integrity – database adopts following actions;
A) rollback – data can be rolled back
B) save point – data can be saved automatically
C) Commit – once committed, changes will take affect

42. Database Security Issues
2 key issues – Aggregation (user can get info about components and can deduce info about whole), Inference (Outcome of Aggregation is Inference, meaning the what user will deduce from aggregation is Inference)
Following techniques to mitigate these risks;
1st Content Based Access – user can access based on its approval for content
2nd Context Based Access – user can access based on user's previous activities and record, it checks why user wants to access?
3rd Partitioning – divide info such as it is distributed safely
4th Noise/Disturbance – add noise/ garbage in data to divert hacker/user attention
5th Polyinstantiation – meaning create 2 instances (views) for same object/ info – one view for Top Secret and 2nd view for Unclassified to deceive them

43. Online Transaction Processing (OLTP) – simply it is database server clustering providing fault tolerance, redundancy and consistency in transaction – meaning state of database is not final/closed until all servers in cluster are unified and agreed. For OLTP to process, 4 validations must be completed;
1) Atomicity(A) – divide transactions into atom (pieces) and then process)
2) Consistence© - make sure databases are consistent
3)Isolation(I) – unit transactions must run in isolation and update results so all DBs are unified
4)Durability(D) – make sure changes remains durable, changes commit once only all servers are updated

44. Data Warehouse, Data Mining And Big Data – if required read explanation on page 1399-1400

Incorrect. The correct definition mapping is below;
- Record - A collection of related data items.
- File - A collection of records of the same type.
- Primary key - Columns that make each row unique.
- View - A virtual relation defined by the database administrator

Correct. SQL (Structured Query Language) is a standard interactive and programming language for getting information from and updating a database. Although SQL is both an ANSI and an ISO standard, many database products support SQL with proprietary extensions to the standard language. Queries take the form of a command language that lets you select, insert, update, find out the location of data, and so forth. There is also a programming interface.

Incorrect. Prototype systems can provide significant time and cost savings

Incorrect. The number of rows in the relation is referred to as the cardinality and the number of columns is the degree.

Database Programming Interfaces
Data is useless if you can't access it and use it. Applications need to be able to obtain and interact with the information stored in databases. They also need some type of interface and communication mechanism. The following sections address some of these interface languages.
Open Database Connectivity (ODBC) An API that allows an application to communicate with a database, either locally or remotely. The application sends requests to the ODBC API. ODBC tracks down the necessary database-specific driver for the database to carry out the translation, which in turn translates the requests into the database commands that a specific database will understand.
Object Linking and Embedding Database (OLE DB) Separates data into components that run as middleware on a client or server. It provides a low-level interface to link information across different databases and provides access to data no matter where it is located or how it is formatted.
The following are some characteristics of an OLE DB:
• It's a replacement for ODBC, extending its feature set to support a wider variety of Non-relational databases, such as object databases and spreadsheets that do not necessarily implement SQL.
• A set of COM-based interfaces provides applications with uniform access to data stored in diverse data sources (see Figure 8-36).
• Because it is COM-based, OLE DB is limited to being used by Microsoft Windows–based client tools.
• A developer accesses OLE DB services through ActiveX Data Objects (ADO).
• It allows different applications to access different types and sources of data.

ActiveX Data Objects (ADO) An API that allows applications to access back-end database systems. It is a set of ODBC interfaces that exposes the functionality of data sources through accessible objects. ADO uses the OLE DB interface to connect with the database, and can be developed with many different scripting languages. It is commonly used in web applications and other client/server applications. The following are some characteristics of ADO:
• It's a high-level data access programming interface to an underlying data access technology (such as OLE DB).
• It's a set of COM objects for accessing data sources, not just database access.
• It allows a developer to write programs that access data without knowing how the database is implemented.
• SQL commands are not required to access a database when using ADO.
Java Database Connectivity (JDBC) An API that allows a Java application to communicate with a database. The application can bridge through ODBC or directly to the database. The following are some characteristics of JDBC:

It is an API that provides the same functionality as ODBC but is specifically designed for use by Java database applications.
• It has database-independent connectivity between the Java platform and a wide range of databases.
• It is a Java API that enables Java programs to execute SQL statements.

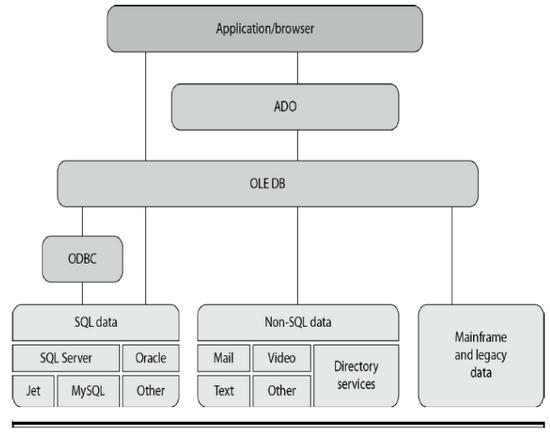


Figure 8-36 OLE DB provides an interface to allow applications to communicate with different data sources.

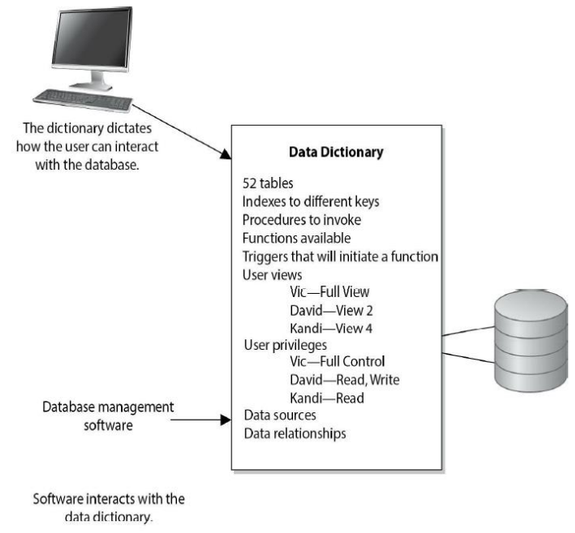


Figure 8-37 The data dictionary is a centralized program that contains information about a database.