Security +
Core Security Concepts

Author: Joseph Lee
Email: joseph@ripplesoftware.ca
Mobile: 778-725-3206

General Security Terms

IT Security Governance
- Specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated
- Essentially governance defines who is responsible for adhering to the laws, regulations, standards, and overall risk tolerance of policies

IT Security Management
- Making decisions to mitigate risks

Personally Identifiable Information (PII)
- Data that could potentially be used to identify a particular person
- Examples include a full name, Social Security number, driver's license number, bank account number, passport number, and email address

Personal Heath Information (PHI)
- Health information about an individual that identifies the specific individual

Use case
- A goal the organization wants to achieve
- A use case contains the following elements:
  - **Actors** – People involved
  - **Preconditions** – A set of conditions in place before the start of a processes
  - **Trigger** – An event that occurs to start a processes
  - **Post condition** – A set of events that happen after the trigger
  - **Normal flow** – A list of steps that occur as a result of the trigger
  - **Alternate flow** – A list of special conditions that will cause a change to the normal work flow

CIA
- These are critical principles to IT security
  - **Confidentiality**
    - Only provide access to the person you wish to have access
  - **Integrity**
    - Ensure the data has not changed from it’s original form
  - **Availability**
    - Ensuring uptime of the data / service

AAA

- These are critical principles of access security
  - **Authentication**
    - Correctly identifying the user / person
  - **Authorization**
    - Determining what the user / person should have access to
  - **Accounting (auditing)**
    - Keeping logs of authentication attempts and authorization given

Non-repudiation

- Ability to prove that that transition took place and mitigates the ability for someone to deny participation

Least privilege

- Example of technical control
- Users are only granted the rights and permissions needed to perform assigned tasks, but not more

Defence in Depth (layered security)

- Practices of implementing layers of protection

Control diversity

- Having various different methods of threat mitigation

Vendor diversity

- Ensuring diversity in your supply chain and software vendors
- This prevents being in a bad position if a single vendor fails to mitigate a particular threat and also if the vendor stops supporting their products

Redundancy

- Adds duplication to critical system components and networks and provides **fault tolerance**
- **Disk redundancy** with **RAID**
- **Server redundancy** with **failover clusters**
- **Power redundancy** with adding **generators** and / or **UPS**
- **Physical site redundancy** with **hot**, **warm**, and **cold sites**

Fault Tolerance

- Ability for a system to maintain performance during a security event through self-healing or redundancy

SPOF Single Point of Failure

- A component within a system that can cause the entire system to fail if the component fails
- **SPOF** can be mitigated using **fault tolerance** and such as **redundancy**
- Some common forms of redundancy include:
  - **Hard-disks** can use **RAID** to prevent a single disk failure from taking a

server down and provide data redundancy to reduce changes of data loss
    - **Failover servers** can replace a server if it fails, and a **server farm** can be actively acting as a **load balancer** while also providing redundancy
    - **Power** UPS or generators can provide backup power in the case of electrical failure
    - **Regular backups** of **important company data** or **configuration files** can provide redundancy for lost files or corrupted system configurations
    - **Site redundancy** can provide alternative sites at various stages of readiness (labelled hot, warm, cold) where a company can move operations in the case of fire, flood, or other natural disaster such as earthquake
- **Cooling systems** increase the stability of hardware and can increase **availability** to greatly reduce the likeliness of SPOF from failing

Physical Security Controls

Permitter
- Fences, walls, barricades, signage, security guards, video surveillance, barbed-wire, watch-towers, alarms, bollards

Buildings
- Guards, locked-doors, mantraps, lighting, signage, alarms

Secure work areas
- Restricted areas for classified or restricted tasks, escorts, multiple person policy

Hardware
- Cable locks
- Rack-mount/ cabinet locks
- Access panel locks
- Safes
- CCTV

Air-gap
- Removing cables that plug a system into a network
- Theoretically, this computer is 100% impervious to network attacks

Signage
- Signage can be a deterrent
- Signage can decrease the likeliness of user-mistakes

Locks
- Cipher locks (buttons with a code)
- Penetration testing locks to evaluate their resistance
- Access card / proximity cards / smart-cards
- Biometrics (retina-scanner, facial recognition, fingerprinting)

Environmental Controls

- **HVAC**
- **Hot and Cold Aisles**
  - Regulate heat to increase longevity and performance of hardware
  - Ensures efficiency that heat from one device is not spilling onto another device
  - Optimize the costs of cooling a server room / data center
- **Fire suppression**
  - Remote heat
  - Remove oxygen
  - Remove fuel
  - Disrupt chain reaction (CO2)
  - **Fire Extinguisher Classifications**
    - **Class A -** Foam or water based used for Combustibles (wood, paper)
    - **Class B -** CO2 and powder based used for flammable liquids (gasoline, oil)
    - **Class C -** CO2 based used for electrical (electrical equipment)
    - **Class D -** Powder based, used for combustible metals (sodium, magnesium)
- **Flood pumps**
- **Monitoring systems**

Shielding

- EMI Electro Magnetic Interference
- RFI Radio Frequency Interference
- Protected cabling **CAT 5e, CAT 6e** comes in **STP / UTP** (Shielded or Unshielded twisted pair cables)
- Fibre Optic is not susceptible to **EMI** and **RFI**

Faraday Cage

- Room that prevents RF signals from exiting and entering

Asset management

- The process of tracking valuable assets through their life-cycles, and ensuring that purchases go through a review and approval process.
- Track devices through their purchase to end-of-life
- **Architecture design and weaknesses**
- **System sprawl and undocumented assets**
  - The organization has more systems that it needs
- **Resource constraints vs security constraints**
  - Organizations need to balance between the need for security and the available resources