Security +
Hardware Security

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

General Terms

BIOS Basic Input / Output System
- A physical microchip includes software with instructions for the computer to start, run some basic checks, locates the boot sector, the operating system

UEFI Unified Extensible Firmware Interface
- Newer version of BIOS

UAV unmanned arial vehicle
- Flying drones can be autonomous or human controlled

UPS Uninterrupted Power Source
- An alternate or power generator in case of grid power failure
- Uninterruptible power supply keeps systems running on battery during power failure

Backups
- Data backups to prevent data loss in case of corruption, deletion, application failure, or human error

HVAC (heating ventilation air conditioning)
- Cooling systems keep hardware within recommended operating temperatures and reduce likeliness of system failure
- HVAC system's primary benefit is to **increase availability**
- Also HVAC system can be vulnerable to attacks since they have **embedded systems** in them

General Security Concepts

Server redundancy
- Using failover clusters (redundant servers that become operational when mail server fails)

Load balancing
- Used to balance the data request load in order to **increase availability**

Site redundancy
- **Hot site** available 24/7

- **Warm site** between hot/warm site
- **Cold site** can be prepared when needed

Electrical Security Threats

ESD Electrostatic discharge
- Wrist-straps and anti-static bags can prevent electrostatic from damaging computer parts

EMP Electromagnetic Pulse
- Short burst of electromagnetic energy can come from wide assortment of sources and cause damage to computer equipment

EMI Electromagnetic Interference
- Comes from sources like motors, power lines, lights, and can interfere with network signals
- Using shielded cable and faraday cages may become necessary when building physical network infrastructure in areas that have high EMI

Network Security Hardware Devices

RAS Remote access server
- A type of server that provides a suite of services to remotely connected users over a network or the Internet
- It operates as a **remote gateway** or **central server** that connects remote users with an organization's internal local area network (LAN)

Bastion host
- A high security server maintained to protect systems on the LAN from outside attack via access over a public facing IP
- Often hosts only a single application and includes HIDS or HIPS
- Usually a server that provides access to **highly sensitive** data, for example, a **VPN** that provides access to an internal network
- Instances that sit within your public subnet and are typically accessed using **SSH** or **RDP**

Network Tap
- A device that you can insert on a network path to capture and analyze packets

SED Self Encrypting Drive
- A HDD or SSD with an **embedded controller** to encrypt the drive’s contents
- The drive appears the same as a normal hard-drive but can be configured to erase its contents when connected to an untrusted system

UTM Unified Threat Management Device

- Hardware security appliance that operates in the **DMZ** and provides services:
  - Virus protection
  - Non-transparent proxy (modifies and inspects data)
  - Network Intrusion Detection System NIDS
  - Firewall
  - Anti-spam protection (mail-gateway)
  - DDOS mitigation
  - Content inspection

TPM Trusted Platform Module

- Works with system boot firmware (such as UEFI) to provide baseline of security and trust
- Keeps hard-drives locked until the system completes a verification and authentication process
- Supports the **secure boot** and **remote attestation / (attestation)** processes
- Comes with a unique RSA private key burned into it which is used for asymmetric encryption
- TPM provides **hardware root of trust** which ensures low-level security during system boot

HSM Hardware Security Module

- A security device that can generate, manage and **store cryptographic keys** and perform CPU intensive cryptographic processes more efficiently than standard hardware
- **High-performance HSMs** are **network attached external devices**
- Lower-performance HSM devices are expansion cards or plug into computer ports

RAID Redundant Array of Inexpensive Disks

- **RAID-0 (stripping)**
  - Writing data across 2 or more drives for performance increase
- **RAID-1 (mirroring)**
  - Writing data to 2 or more drives at the same time for redundancy
- **RAID-5**
  - 3 or more drives that use **parity to ensure redundancy** as well as **performance increase**
- **RAID-6**
  - Requires minimum of **4 or more disks** that use **double distributed parity** and can allow 2 drives to fail and still operate
- **RAID-10 (or 1+0)**
  - Combination of RAID-0 and RAID-1 (A stripe of two mirrored arrays)
- **RAID-01 (or 0+1)**
  - Similar to RAID 10 (A mirror of two striped arrays)

Failover Cluster / High availability cluster / distributive allocation

- Increases availability

- **Active - Passive**
  - One sever is active and the other is waiting for failure to be used
- **Active - Active**
  - Both servers in the cluster are actively being used unless one server is non-functional or requires maintenance
- **Scalability**
  - Refers to the ability to serve more clients
  - Adding additional hardware resources can increase availability
- **Load balancer**
  - For high availability (typically in the DMZ)
  - Load balancers can direct traffic using round-robin or by detecting load on servers
  - **Round-robin**
    - Requests to a server are rotated through a list of servers in the server farm
  - **Affinity / Session affinity / Sticky session**
    - Matches the session to a sever and continues to direct traffic from that session to a single particular server
  - **Elasticity**
    - Ability to scale up and down depending on need

Access Control Hardware

SMAP Supervisor Mode Access Prevention

- A feature of some CPU implementations
- Allows supervisor mode programs to optionally set user-space memory mappings so that access to those mappings from supervisor mode will cause a trap
- Makes it harder for malicious programs to "trick" the kernel into using instructions or data from a user-space program
- Supervisor code usually has full read and write access to user-space memory mappings
- Privilege escalation exploits, which operate by causing the kernel to access user-space memory when it did not intend to