Willian Prado
05/09/2025

11.1 What is air gap?

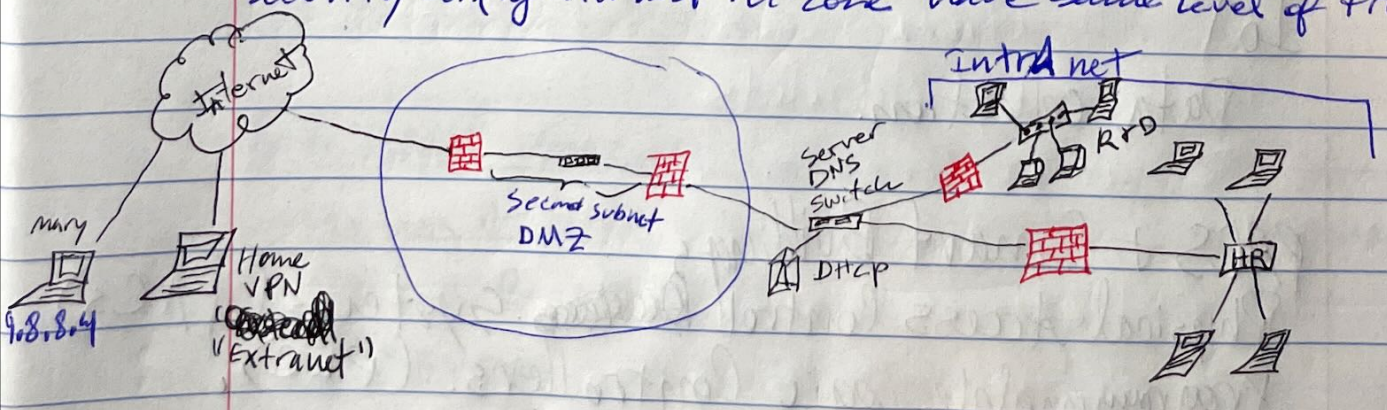
YTB AIR GAP is a security measure that involves physically separating a computer or network to prevent it from making connections to other devices. Air gap can protect critical data from attacks like malware & ransomware.

YTB. What is DMZ? A DMZ, or demilitarized zone, is used to help improve the security of an organization's network by segregating devices, such as computers & servers, on the opposite sides of a firewall.

sunny YTB Honeynet & DMZ

Zone-Based Security
- Ensure traffic flows securely btw zones.
- control access; minimize risk.

Zone - area where all host in network have the same security config. All host in zone have same level of trust.



Triple homed - firewall/router appliance w/ three or more NICs. NIC placement:
- interface for public (internet) zone
- " " private (LAN) zone
- " " perimeter zone

achieve same configuration as screened subnet.

William Prado
05-09-2075

YTB-Sunny Sunny YTB - Protecting your network part 1 - IDS, IPS, Honeynet, DMZ, proxy.

IDS & IPS - IDS stands for Intrusion-detection system.
IPS stands for Intrusion Prevention System.

TODO: Dion exam-practice exam.

11.2 Internet of things.

EEPROM - electrically Erasable Programmable Read-Only memory. is a type of non-volatile memory used in computers & embedded systems.

Consumer Devices
Consumer-grade smart devices
hub - control system
smart devices.

IoT
Data collection.

PACS & Smart Buildings
Physical Access Control Systems (PACs)
Programmable logic Controllers. (PLC).
- CPU
- RAM
- I/O
- power supply
- programming

Industrial Devices.
" Embedded Systems.
" Control " (ICS).

william Frado
05-09-2025.

Industrial Devices
Supervisory Control + Data Acquisition.

IoT Networks
Operational Technology (OT) networks.
Cellular networks
- Narrowband - IoT (NB) IoT
- LTE Machine Type Communication (LTE-M)
- Z-wave
- zigbee
- segmentation
- Regular Audits
- Employee training.

Managing IoT Security Risks
- consumer-Graded smart devices
- smart buildings
- ICS/SCADA

11.3 Physical Security
Badges + Site Security Entry Systems
Access Control
- Keypad (cipher lock)
- Key fob
- Badge Reader
- Proximity card
- Biometric
- Access Control Vestibule

William Prado
05/09/2025

mantrap
turnstile

Locks & Secure Entry Systems
II & Badge Readers
- Electronic locks.
- Badge Reader.
- Biometric locks.

Rack System locks
- Secure Cabinets & Enclosures
- Colocation Cages

Physical Security for Server Systems
- Rack System Locks
- Secure Cabinets & Enclosures
- Colocation Cages
- Locking Cabinets
- smart lockers

Detection-Based Devices
- security Guards
- Camera-Based Surveillance Systems.
- Camera specifications
  - resolution
  - focal length
  - Lux

William Prado
05-09-2025

Camera-Based Surveillance Systems
Camera models

Detection-Based Devices
Camera-Based Surveillance Systems
Camera lenses.
Fixed lenses.

Camera-Based Surveillance Systems.
- Detection Based Controls
- surveillance Applications

Camera Types
- Fixed Cameras
- PTZ (PAN-Tilt-Zoom) cameras
- CCTV Network Integration

Alarm + Tamper Detection
Alarm types.
- circuit/tamper detection
- motion detection
- alarms for rack systems + chassis intrusion
- protecting Distribution System (PDS).

Geolocation
- GPS (Global Positioning System)
- IPS (Indoor " ")

Geofencing
- Application
- Mobile Device Management (MDM)

Summary:
- Perimeter Defense - utilize firewalls/proxy servers in screened subnets.
- Internal Zone Protection - Implement firewall for internal zones/hosts.
- Intrusion Detection/Prevention - Deploys IDS/IPS behind firewalls.
- IoT Management - Develop a strategy for segmented network zone.
- Site Access Control - Access + implement access control measures.