IT Perimeter Security

Rajendra Hegadi

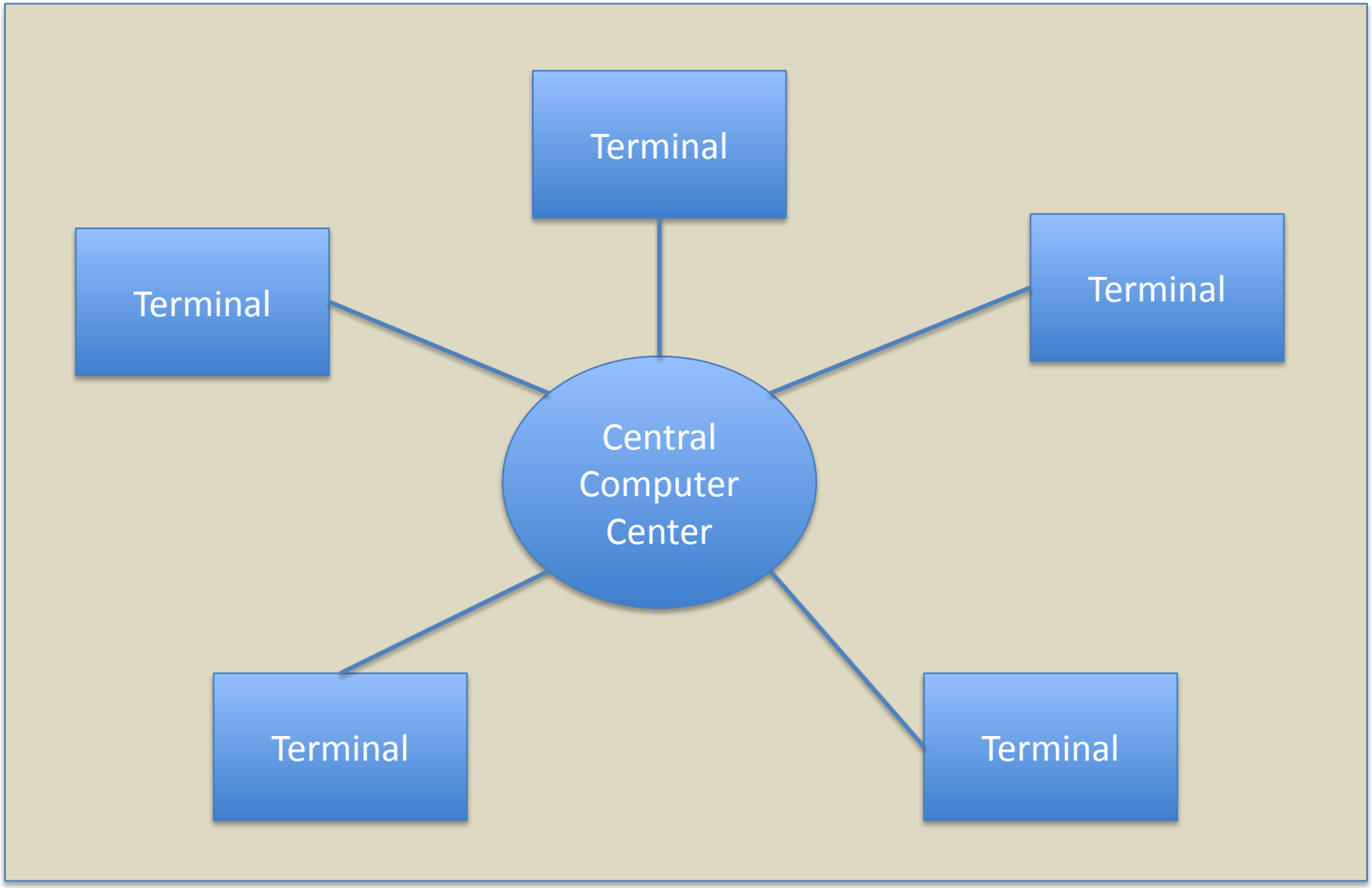
rajendrahegadi@iiitdwd.ac.in

Traditional vs. modern perimeter security

Perimeter was well defined ,
Security enforced on a physical level

Computers in 1980s-90s

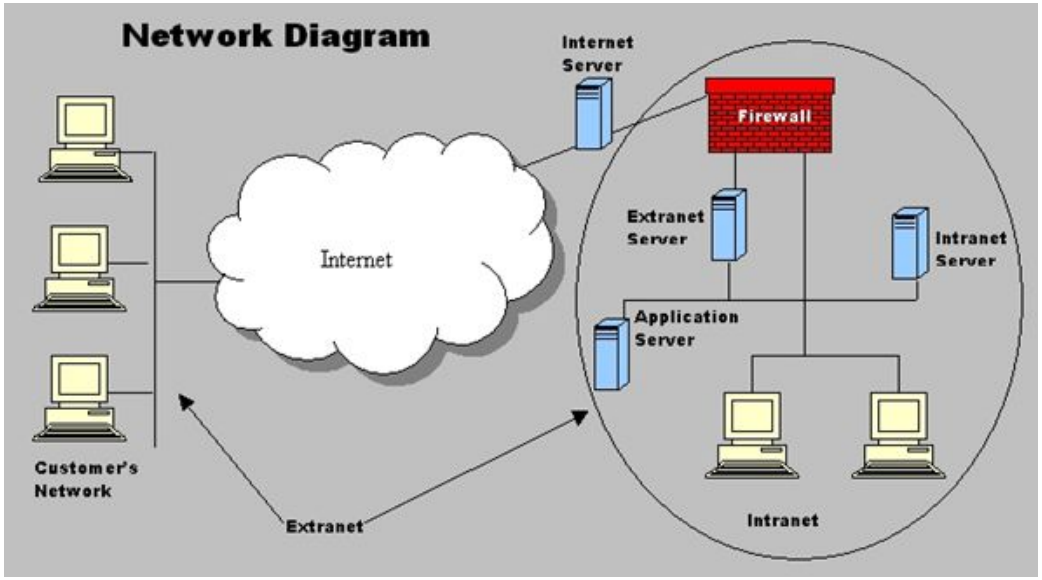
Traditional vs. modern perimeter security



Traditional vs. modern perimeter security

Modern computer networking

Devices
-Router
-Switches
-Access points
- Laptop
- Smart phones
- Wearable Devices
- IoT Devises



Applications
-Web applications
-OTT platform
-Social Media content
-File transfer applications

" The perimeter is now becoming fuzzy. Any sort of computing device may become the perimeter itself and these devices in many cases are mobile"

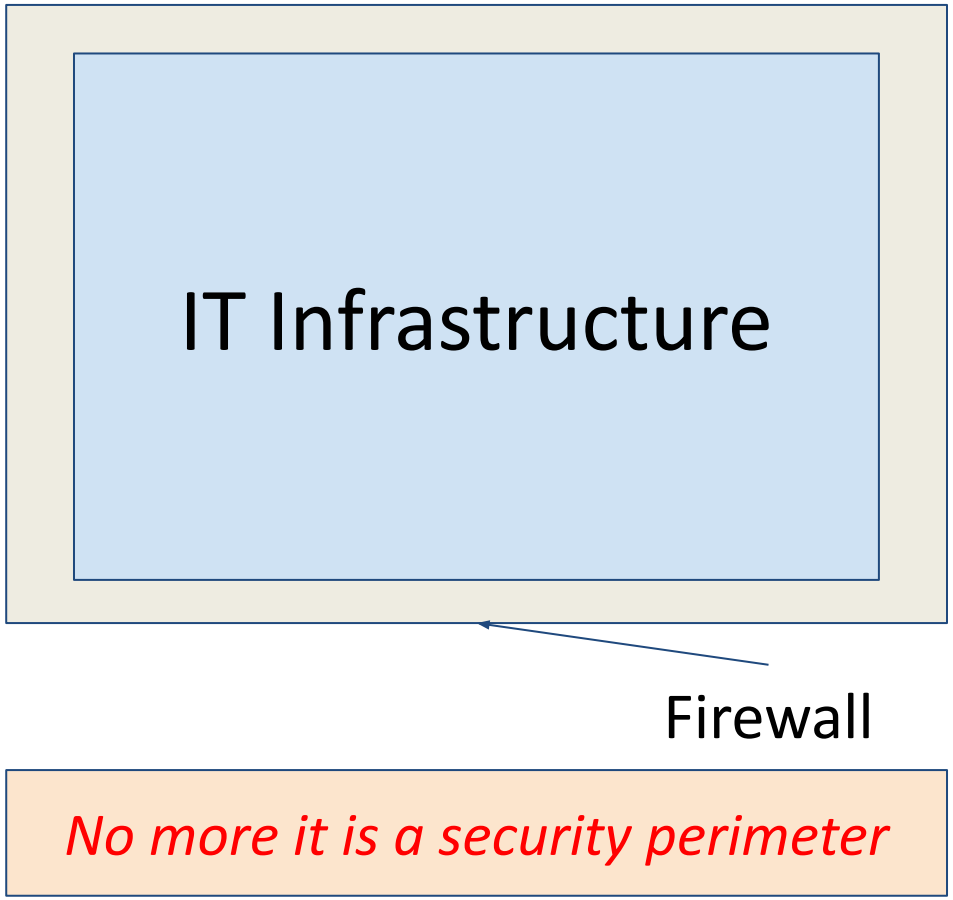
IT Network Perimeter (ITNP)

- Physical Network perimeter has vanished
- ITNP - *A Dynamic changing barrier (Not a static barrier)that must be redefined and protected*
- *So, it a System perimeter (SP)*

IT Network Perimeter (ITNP)

Devices

- A computer
- *Number of computers*
- *Small network of computers*
- *Now network of everything*
- *IP everywhere*



IT Network Perimeter (ITNP)

-Perimeter is becoming more and more defined by each node on the network

-Network protocols allow applications and data to traverse through the firewall and run on local machines

-Devices that break traditional perimeter security

- Applications
- *Mobile Devices*
- *IP-Enabled devices*
- *Devices keep moving from internal to external and vice-versa*
- *Wireless access points*
- *Direct internet access from devices*

IT Network Perimeter (ITNP)

Analysis Tools

-**Passive Monitoring tools** (Internet scanner and network scanner)

- Don’t scan all the time, scan only when invoked / schedule
- Discovering devices connected to network and What these devices can do
- Scan Vulnerabilities of the network devices(Configuration)
- Scan-Desktops, servers, routers, switches, firewalls, security devices, etc.
- Analyses - configurations, patch levels, OS, installed apps- to find the vulnerabilities

Passive Monitoring Tools

- https://www.advanced-ip-scanner.com/
- https://angryip.org/
- https://www.10-strike.com/network-scanner/

IT Network Perimeter (ITNP)

Analysis Tools

-**Active Monitoring tools -(Anomaly detection)**

- Scan network all the time
- Monitor traffic pattern , communications and transmitted data
- Detect unhealthy traffic patterns, security threats,
- Anomaly detection tools- noncompliant activities, abnormal network performance
- Detect- worm propagation and policy breaches

https://www.predictiveanalyticstoday.com/top-anomaly-detection-software/

Active Monitoring tools -(Anomaly detection)

- Critical asset management by keeping track of change management
- Identify and take action against malicious content, illegal access, insider misuse, and other security incidents
- These tools- help to reduce harmful activities
- Evaluate logs continuously and consistently

Network Zoning

- Each host is now perimeter
- Identify the network zones
- Define data and asset classification

Network Zoning

- Key concept- creating security zones on the network infrastructure
- Firewall- necessary but not sufficient
- All areas of n/w must be part of perimeter
- All nodes must act as perimeter

Network Zoning

- Uncontrolled zone- Internet outside the controlled network - Decentralized
- Controlled Internet - Inside the network
- Restricted zone- Production, Mgt

- Various types of mobility and rules restrictions
- Ex: Access restriction to Central VPN solution
- Restriction on traffic (Specific port)
- Security configuration in devices
- Re-addressing the packets using NAT at Firewall

Classification

- Today's IT Perimeter security is not Infrastructure security, also data security
- Classification
  - User
  - Data
  - Hardware
  - Communication
- Classification effort - which determines *When*, *Where* and *How* - the protection level should be Increased or decreased dynamically

Classification

User classification

- Based on the role of the individual
- Strict- Identity management

Data Classification

- Security and privacy of classified data
- File and File content security
- Proper backup mechanism
- Following standards - PDPA 2023

Classification

Hardware classification

- Tangible asset classification
- Zero trust architecture for every mobile devices whenever moves out of the security perimeter

Communication classification

- Traffic classification
- Placing IDS and IPS
- Decision on encrypted traffic

Perimeter security

The various components of Endpoint Security are:

FW (Firewall)

– The firewall module operates reactively.

– User impact can be high if this component is not centrally managed.

IPS (Intrusion prevention system)

– The IPS system protects against all known vulnerabilities and exploits.

– The user impact is low.

– It stops the attack.

BOEP (Buffer Overflow Exploit Prevention)

– BOEP protects against known and unknown buffer overflow exploits.

– These exploits represent the majority of attacks.

AC (Application control)

– AC is based on configuration.

– AC potentially protects against all known and unknown attacks.

– User impact can be high if this component is not centrally managed.

Who defines the perimeter?

Security

- *An attacker doesn't go through security, but around it.*
- Their goal is to find and exploit the weakest link.
- *Put your defenses in layers.*
- *It's a bad idea to rely on "security through obscurity."*
- *Keep it simple.*
- *Don't give a person or a program any more privileges than those necessary to do the job.*
- *Programming is hard.*
- *Security should be an integral part of the original design.*

Security

- *If you do not run a program, it does not matter if it has security holes.- Fail safe*
- *A program or protocol is insecure until proven secure.*
- *Security is a trade-off with convenience.*
- *Don't underestimate the value of your assets.*

References

1. “Understanding IT Perimeter Security”, Axel Buecker, Per Andreas, Scott Paisley., IBM Red books. 2008.
2. “Firewalls and Internet Security, Second Edition, Repelling the Wily Hacker”, William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin.,Addison-Wesley, 2023.