Course Instructor:
Anwar Haque

Lecture #11
Dept. of Computer Sc, Western University
Chapter 8 roadmap

8.1 What is network security?
8.2 Principles of cryptography
8.3 Message integrity
8.4 Securing e-mail
8.5 Securing TCP connections: SSL
8.6 Network layer security: IPsec
8.7 Securing wireless LANs
8.8 Operational security: IDS / IPS
Various Network Attacks

- Malware: Virus, Worm, Trojan Horse, Spyware, Adware, Rootkits, Sniffers, Botnets, Ransomware

- Reasons behind attacks:
  - Financial
  - Spying
  - Political
  - Industrial / Personal rivalry

- DoS / DDoS
IDS and IPS systems

IDS sensors

internal network

Proxy Server

Firewall

Internet

HoneyNet

Demilitarized zone

Web server

FTP server

DNS server
IDS and IPS

- IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems)
- IDS: Intrusion Detection System
  - Deep Packet Inspection: look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)
  - Examine correlation among multiple packets
    - Port scanning
    - Network mapping
    - DoS attack

Slide info source: https://www.youtube.com/watch?v=cMH4yGE73iQ
IDS and IPS

- IDS is a passive system
  - Identifies malicious traffic and raises flag to IPS
    - Inspection and Investigation
      - Analyzes suspicious packets and activities
      - Signature based inspection
      - Statistical-anomaly based inspection
  - IPS is an active system and takes necessary action
    - Put the traffic into quarantine
    - Simply drop the traffic
    - Log and reporting to network admin

Slide info source: https://www.youtube.com/watch?v=cMH4yGE73iQ
IDS and IPS

- IDS and IPS can be on separate devices, or combined into one device or could also be deployed in other network devices / routers / firewalls

Slide info source: https://www.youtube.com/watch?v=cMH4yGE73iQ
IDS and IPS systems

Internet

Demilitarized zone

firewall

Proxy Server

HoneyNet

IDS sensors

internal network

Web server

FTP server

DNS server

Internal network

IDS and IPS systems
Firewalls

**firewall**

isolates organization’s internal net from larger Internet, allowing some packets to pass, blocking others

administered network

trusted “good guys”

firewall

public Internet

untrusted “bad guys”
Firewalls: why prevent denial of service attacks:

- Traffic flooding: attacker establishes many bogus TCP connections, no resources left for “real” connections

prevent illegal modification/access of internal data

- e.g., attacker replaces CIA’s homepage with something else

allow only authorized access to inside network

- set of authenticated users/hosts

types of firewalls:

- stateless packet filters

- stateful packet filters
Firewalls: Stateless

❖ Port Filtering:
  ▪ Also known as port blocking
  ▪ Port number is associated to a certain application
  ▪ port 80: webpages; port 25: emails; port 21: FTP
  ▪ Denying certain applications by opening or closing application specific port/s
  ▪ What does it mean blocking port 21 for inbound traffic?

Slide info source: https://www.youtube.com/watch?v=RV2QznoyEBU
Firewalls: Stateless

❖ MAC Filtering:
  - Media Access Control (MAC) ID: Unique ID of a network interface card or port
  - MAC is static and never changes
  - Blocking traffic to and from a specific MAC address means blocking a specific device in the Internet

❖ IP Filtering:
  - Filter incoming or outgoing traffic by IP address
  - Block or restrict incoming or outgoing traffic from a specific IP address or a range of IP addresses

Slide info source: https://www.youtube.com/watch?v=RV2QznoyEBU
Firewalls: Stateless

❖ Content Filtering:
  ▪ Also known as Information filtering
  ▪ Similar to parental control
  ▪ Inspect specific signature in the IP packets (packet stream) and blocks the content accordingly

❖ All the above four filtering techniques are stateless filtering
  ▪ Each packet is examined independently and no relation with prior packets that may have passed through the firewall

Slide info source: https://www.youtube.com/watch?v=RV2QznoyEBU
Firewalls: Stateful

❖ Dynamic / Stateful Filtering:
  - Decision is not based on one individual packet but based on the packet trace / packet flow
  - It checks multiple items in the packet such as IP address, port number, contents, authentication etc. and then in relevance to the previous packet flow it takes a accept of reject decision

Slide info source: https://www.youtube.com/watch?v=RV2QznoyEBU
Honeynet

- Intentionally deployed in the network by the ISP or any network management systems
- Includes real network devices / routers / systems
  - These devices are called honeypots and they look real and legitimate
- Honeynet works as a trap for intruders:
  - Hackers can be attracted to it, and launch attacks and gain access to data or whatever they want from that Honeynet
  - Hackers’ activities are monitored carefully, their attack methods and strategies are studied
  - This info is valuable to the network operators for protecting their networks

Slide info source: https://www.youtube.com/watch?v=FihkG72z7MQ&t=282s
DMZ

❖ Some contents are intended for heavy public use such as company’s web servers
❖ These less vulnerable network points are usually put under lightweight IDS and IPS such that they can be accessed at all time by the public compare to company’s other data resources and systems that must be heavily protected by strong security systems
❖ This lightweight network systems is known as DMZ

Slide info source: https://www.youtube.com/watch?v=FihkG72z7MQ&t=282s
Proxy Server

- Proxy server acts as a Gateway between Intranet and Internet that provides:
  - Acts as an agent on behalf of its clients
    - Security and privacy protection through Network Address Translation (NAT)
  - Four Functions:
    - Acts as a content delivery cache
    - Control Inbound and Outbound traffic
    - Block malicious traffic
    - Block targeted sites

Slide info source: https://www.youtube.com/watch?v=f-oCTcf5k_0
Proxy Server

- Keep track of all incoming and outgoing traffic
- It can bypass the firewall
  - Gives an user access to a network that is prohibited by the intranet’s firewall

Slide info source: https://www.youtube.com/watch?v=f-oCTcf5k_0
Proxy Server: bypassing Firewall

AS 1234

internal network

IDS sensors

Proxy Server

firewall

Internet

Restricted Server for AS 1234
Network Security (summary)

basic techniques......

▪ Confidentiality / cryptography (symmetric and public)
▪ end-point authentication

.... used in many different security scenarios

▪ secure email
▪ secure transport (SSL)
▪ IP sec
▪ 802.11

operational security: IDS / IPS