NETWORK MODELS: VULNERABILITIES AND CONTROLS CONT.

Lecture 9a

COMPSCI 726

Network Defence and Countermeasures

Muhammad **Rizwan** Asghar

August 5, 2021

DATA LINK LAYER

- It defines higher level structure of data (frames) between directly connected nodes

- It also specifies the physical address structure

DATA LINK LAYER: SUB-LAYERS

- It can be divided into two sub-layers
  - Logical Link Control (LLC)
    - It provides a common interface
    - It manages flow control
    - Issues requests for transmission of data suffered with errors
  - Media Access Control (MAC)
    - Appends physical address to a frame

DATA LINK LAYER: VULNERABILITIES

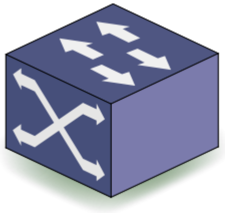
- MAC address spoofing
  - A node claims the identity of other node

- In case of wireless, access to unauthorised parties
  - Wireless access points with lax of default security settings

DATA LINK LAYER: CONTROLS

- MAC address filtering
  - Identifying nodes by address
- Wireless applications must be carefully evaluated for unauthorised exposure
- Built-in encryption, authentication, and MAC filtering may be applied to secure networks

NETWORK LAYER



- It decides how to route data from senders to receivers
- Translation of network addresses into physical counterparts
- Its addressing is used by applications to identify resources
  - Using DNS resolution to map a hostname to an address or group of addresses
- No built-in means to authenticate source addresses

NETWORK LAYER: VULNERABILITIES

- Route spoofing
  - Propagation of false network topology
- IP address spoofing
  - False source addressing on malicious packets

NETWORK LAYER: CONTROLS

- Route policy controls
  - Use strict anti-spoofing and router filters
- ARP/broadcast monitoring software
- Firewall protection
- Encryption and authentication technologies, such as IPSec, can be used to more reliably identify the source of IP communications

TRANSPORT LAYER

- It is concerned with the transmission of data streams into lower layers
- Transport protocols may be designed for high reliability
- Transport protocols may implement flow control, quality of service, and other data stream controls to meet their transmission needs
- It is purely a logical layer, where multiple data conversations from or to a single host are multiplexed
- It defines port addresses for services (processes)

TRANSPORT LAYER: VULNERABILITIES

- Mishandling of undefined, poorly-defined, or illegal conditions
- Differences in transport protocol implementation

TRANSPORT LAYER: CONTROLS

- Strict firewall rules
- Stateful inspection at firewall layer, preventing out-of-service packets, illegal flags, and other phony packet profiles from entering

SESSION LAYER

- It is concerned with the organisation of data communications into logical flows
- This layer focuses on establishment of identity
- Sets terms of communication
  - Decides which node will communicate first
  - Decides how long a node can communicate
- Failed attempts could be logged

SESSION LAYER: VULNERABILITIES

- Weak or non-standard authentication mechanisms
- Passing of session credentials such as user ID and password in cleartext
- Session ID may be subject to spoofing and hijack
- Information leakage based on failed authentication attempts
- Unlimited failed sessions lead to brute-forcing attacks

SESSION LAYER: CONTROLS

- Secure password exchange
- Accounts have specific expirations for credentials and authorisation
- Protect session ID information via random cryptographic means
- Limit failed session attempts via timing mechanism

PRESENTATION LAYER

- The presentation layer deals with the organisation of data passed from the application layer into the network

- Standardisation of data formats
  - Encoding, compression, and byte order

- An obscure layer, usually hidden deep in the implementation of applications and operating systems

PRESENTATION LAYER: VULNERABILITIES

- Poor handling of unexpected input can lead to application crashes
- Use of externally supplied input in control contexts may allow information leakage
- Cryptographic flaws may be exploited to circumvent privacy protections

PRESENTATION LAYER: CONTROLS

- Careful specification and checking of received input coming into applications or library function
- Separation of user input and program control functions
  - Input should be sanitised
- Careful and continuous review of cryptography solutions to deal with current security emerging threats

APPLICATION LAYER

- It ensures process-to-process communication over the network
- Applications should also implement their own security controls
- Lower layers cannot help if vulnerabilities lie within the application
- Many host-based firewall systems also include the means to control the access of applications to the network

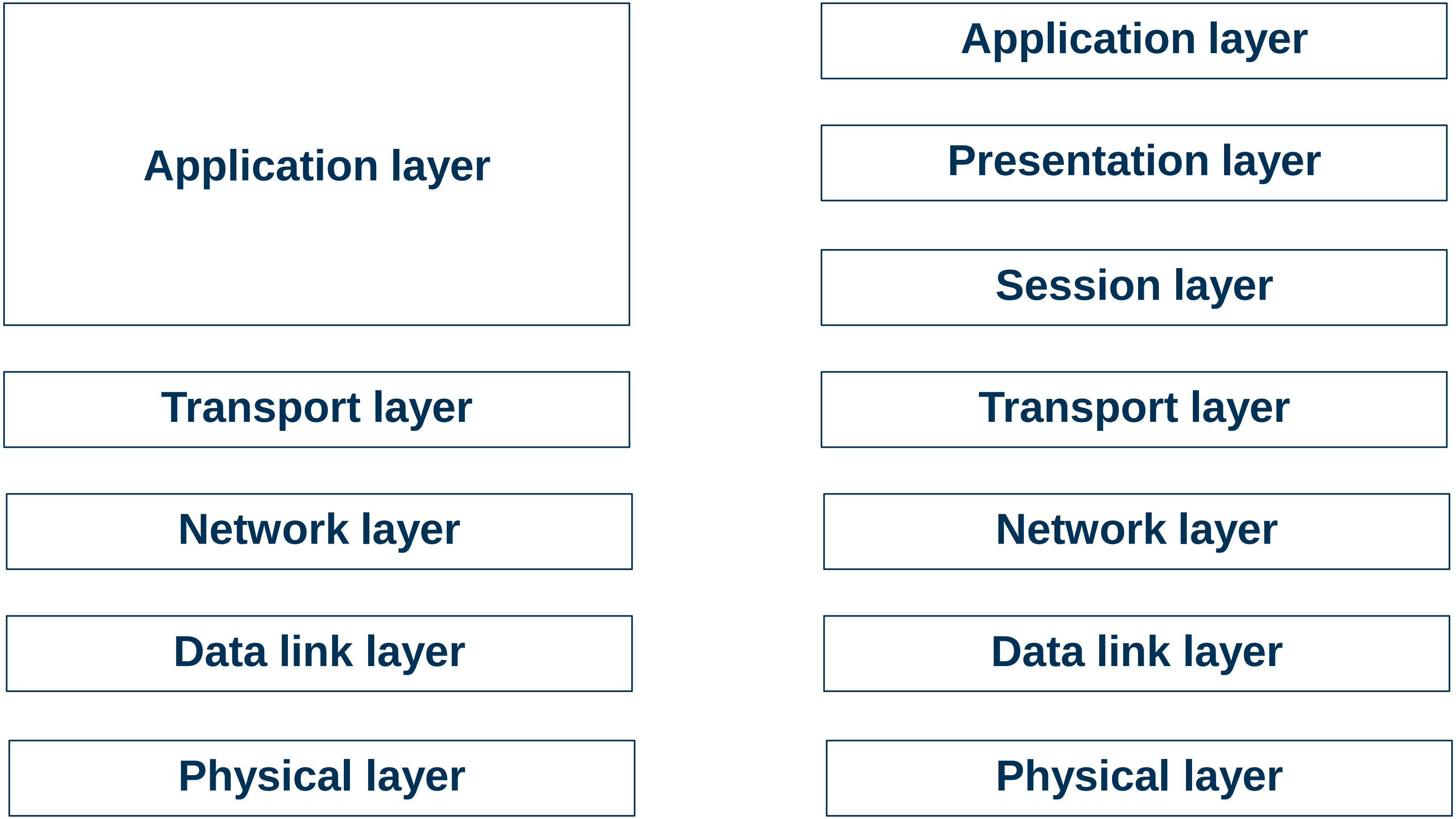
APPLICATION LAYER: VULNERABILITIES

- Backdoors and application design flaws bypass standard security controls
- Program logic flaws
- Inadequate security controls for “all-or-nothing” approach, resulting in either excessive or insufficient access
- User input is a significant threat
  - User may provide unexpected input into the application environment
- Applications with weak or no authentication are prime targets

APPLICATION LAYER: CONTROLS

- Application level access controls to define and enforce access to application resources
  - Control must be detailed and flexible
- Use of encryption to protect data
- Testing and review of application code and functionality
- Some host-based firewall systems can regulate traffic by application, preventing unauthorised use of the network

TCP/IP MODEL VS OSI MODEL



Application layer	Application layer
	Presentation layer
	Session layer
Transport layer	Transport layer
Network layer	Network layer
Data link layer	Data link layer
Physical layer	Physical layer

TCP/IP MODEL AND PROTOCOLS

Application layer	FTP, SMTP, HTTP, Telnet, SSL/TLS, SSH, DNS, BGP
Transport layer	TCP, UDP, RSVP
Network layer	IPv4, IPv6, IPSec, ICMP
Data link layer	Ethernet, Token ring, ARP, ATM, IEEE 802.11
Physical layer	DSL, USB

NETWORK TROUBLESHOOTING TOOLS

- ipconfig (or ifconfig for *nix users)
- ping
- tracert (or traceroute for *nix users)
- tcpdump (for *nix users)

RESOURCES

- Reed, Damon. "Applying the OSI seven layer network model to information security." SANS GIAC GSEC Practical Assignment Version 1.4 b Option One (2003). Link: http://www.sans.org/reading-room/whitepapers/protocols/applying-osi-layer-network-model-information-security-1309

- Read Chapter 1 of
  Network Defense and Countermeasures: Principles and Practices
  Second Edition
  William (Chuck) Easttom
  ISBN-13: 978-0789750945

Questions?

Thanks for your attention!