Lesson 5
Security Tomography and Layer Attack Models

Computational Tomography

- A computing method of producing a three-dimensional picture of the internal structures of an object
- Observation and recording of the differences in effects on passage of energy waves impinging on those structures

Computational Security Tomography

- Identifying the network vulnerabilities
- Used in computational security in complex set of networks
- Needed for the design of efficient attack strategies

Security Tomography

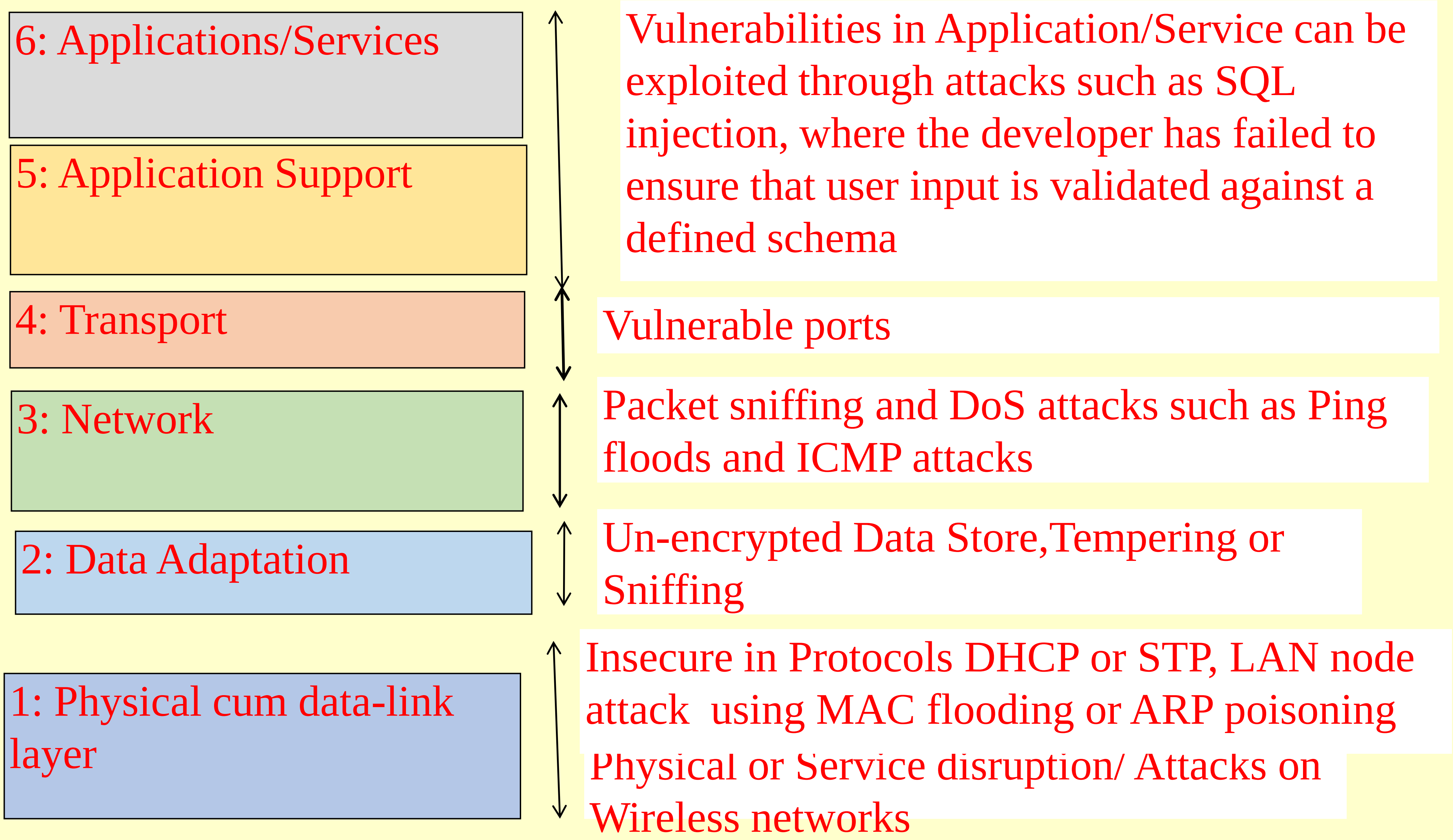
- Means finding attack vulnerable sections/subsections
- Observations for behaviours using a finite number of objects or threats in a complex set of subsystems

Network Tomography

- Refers to study of vulnerabilities and security aspects for network monitoring in a complex system
- WSNs
- RFIDs networks
- IoT networks
- Allocating resources and ensuring the network reliability and security

Layered attacker model

- Gives possible attacks on the layers



6: Applications/Services 5: Application Support	Vulnerabilities in Application/Service can be exploited through attacks such as SQL injection, where the developer has failed to ensure that user input is validated against a defined schema
4: Transport	Vulnerable ports
3: Network	Packet sniffing and DoS attacks such as Ping floods and ICMP attacks
2: Data Adaptation	Un-encrypted Data Store,Tempering or Sniffing
1: Physical cum data-link layer	Insecure in Protocols DHCP or STP, LAN node attack using MAC flooding or ARP poisoning Physical or Service disruption/ Attacks on Wireless networks

Fig. 10.4 Layered Attacker Model and possible attacks in IoT/M2M

Layer 1 Attacks Solution

- Depends on the devices used
- For example, link level provisioning of security
- Uses—BT LE link level AES-CCM 128 authenticated encryption algorithm for confidentiality and authentication, and
- ZigBee at link level security using AES-CCM-128.

Layer 2 Attacks Solution

- Programming the network switches to prevent internal node attacks during use of DHCP or Spanning Tree Protocol (STP)
- Additional controls:

1. ARP inspection,
2. Disabling unused ports and
3. Enforcing effective security on VLAN’s (Virtual LAN) to prevent VLAN hopping.

Layer 2 Attacks Solution

- Provisions for MAS for security, root key data store, and devices and data authentication in LWM2M OMA specification for device gateway to Internet

Layer 3 Attacks Solution

- Use of temper resistant router
- Use of packet filtering
- A firewall for controlling routing messages and packets data between layers 3 and 4 for reducing the risks.

Layer 4 Attacks Solution

- Port scanning method to Identify the vulnerable port
- Effective firewall configuring and opening of network ports and locking down ports only to those required

Layer 4 Attacks Solution

- DTLS between layers 5 and 4
- The DTLS three types of security services: integrity, authentication and confidentiality.
- Inclusion of SASL (Simple Authentication and Security Layer) for security when using the XMPP protocol.

Layer 5 and 6 Attacks Solution

- Results of poor coding practices of Application programmer
- Use HTTPS communication link for Web applications/services can use.

HTTPS

- Content privacy domain header:
- Allows use of digital signatures and encryption, various encryption options
- Server-client negotiations
- Cryptographic scheme is a Property assigned for the link
- Specific algorithm is the Value assigned
- Direction specification done: One-way or two-way security

CISO Suggested Layered Framework Solutions

- Layers 1–6: Role-based security
- Layers 1–4 Anti-temper and detection-based security
- Layers 1–6: Data protection and confidentiality
- Layers 1–6: IP protection

Summary

We learnt

- Network tomography help in observing each network sections and subsections
- Security tomography finding the attack vulnerable sections/subsections on observations for behaviours using a finite number of objects or threats in a complex set of subsystems

Summary

We learnt

- Layers 1 to 6 attacks
- HTTPS
- CISCO security solutions framework

End of Lesson 5 on
Security Tomography and Layer Attack Models