1. Data Encapsulation and De-Encapsulation

a. Describe how data is encapsulated before transmission from the application layer to the physical layer using the OSI model.

The OSI model has entities known as Protocol Data Units (PDUs). Each layer of the OSI model has one of these and uses it to encapsulate data passed to it from the layer above. An application will generate a message containing data that needs to be sent. The message will be encapsulated within an application-layer protocol's header (it is contained in its data field, typically). As we go down the OSI model, we find that each PDU from an upper layer is contained within the data field of the following layer's PDU. The application message is passed to the presentation layer via layer interface services. The data is encapsulated in the presentation layer PDU and passed to the session layer. This process continues through the transport layer's datagrams, the network layer's packets, to the link layer's frames until the frame is passed along a transmission medium using the physical layer's services.

Each layer uses its own services to pass an encapsulated piece of data to pass it to the layer below it.

b. Describe how a packet is de-encapsulated in order to reveal the data in a packet from the physical layer to the application layer using the OSI model.

In reverse order to encapsulation, the physical layer receives a signal from the link, converts it to bit data and passes it to the data link layer. Here, the data link layer checks for any errors in the signal, evaluates the sender's MAC address and passes the payload of the frame (the packet) to the network layer. The process of processing the data unit at each level and passing the payload to the next layer is called decapsulation. The application layer finally receives the payload of the presentation layer (in the OSI model) as a message which is then managed by the application layer protocol.

c. Evaluate some of the security challenges at each layer of the OSI model.

Each layer of the OSI model poses security challenges. At the physical layer, one of the main issues nowadays is that wireless networks rely on broadcast radio waves. Radio waves can be manipulated and broadcast by many people and types of devices and can lead to signal jamming as well as spying [1, 2]. To counteract this, there are various jamming devices that can counter jamming activity. But more to the point, there is an emerging field of end-to-end authentication on the physical layer [3] that aims to ensure transmission is secure, without the need for encryption at higher levels.

In this vein, encryption is a powerful tool used at each layer of the OSI model (including the data link and physical layers [4, 5], but is classically used in the presentation layer [6]. This technique is used to ensure that, if any data is intercepted by a malicious user, that data is illegible or nonsensical to that user. To this end, encryption uses an algorithm to encrypt and decrypt data at the sending and receiving end of the transmission. A security issue found at the data link layer of the Internet is ARP spoofing, which can be used to intercept, modify or stop data transmission in a local area network. This can be counteracted using packet filtering [7].

2. Discussion Based on Socket Programming with UDP: Identify and explain the major security implications of using the UDP protocol for data exchange.

a. Consider the following:

- How can these security challenges be addressed? Highlight an example of a network protocol that can be used to resolve these issues and their trade-offs
- Identify some services that make use of the UDP transport protocol and discuss why it is used instead of TCP

The User Datagram Protocol is used in the TCP/IP stack's transport layer. It is a barebones, unreliable connectionless protocol that encapsulates an application layer message in its payload. The header of a UDP datagram contains the source port number, destination port number, length, and checksum fields.

UDP does not offer security services like encryption. As such, it relies on upper- and lower-layer protocols to provide security over the network. For example, the IPsec suite extends the standard IP protocol to provide encryption services on the Internet layer. IPSec uses the Advanced Encryption Standard (AES) to encrypt an IP datagram and its header before sending it over a network [8]. Another workaround for the issue of encryption is to use a secure protocol based on UDP like QUIC (RFC 9000 [9]). This protocol works in the transport layer and aims to obsolete TCP by providing the security and reliability benefits of TCP to the speedy UDP protocol. An issue with using QUIC these days is that a lot of servers are actively refusing packets sent using QUIC because it is stateless, making it difficult to secure server-side. A discussion can be found here

Aside from lack of encryption, UDP also lacks the handshaking mechanism or session management that are present in TCP. Because of this, it is easy for a malicious user to pose as either the client or server during UDP communication – this is known as spoofing. Spoofing is a type of attack that can be overcome using IP packet filtering, a technique that is able to identify malicious IP packets sent from fraudulent hosts.

For all its security concerns, UDP sees a lot of use in real time applications. Interactive videoconferencing relies on fast communication between two hosts and will typically be sending and receiving UDP segments for both video and audio channels with millisecond frequency. Because TCP requires extra round trips for handshaking and has a larger header size that requires more parsing and processing, it is slower. The end user does not necessarily require reliable packet transport if they can piece together an image or words in their heads, but they do require real-time delivery of data in order for a conversation to be carried out. The same applies to internet telephony applications like WhatsApp calls and iMessage calls.

References

[1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, ‘Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey’, *IEEE Commun. Surv. Tutor.*, vol. 16, no. 3, pp. 1550–1573, 2014, doi: 10.1109/SURV.2014.012314.00178.

[2] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, ‘A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends’, *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016, doi: 10.1109/JPROC.2016.2558521.

[3] X. Wang, P. Hao, and L. Hanzo, ‘Physical-layer authentication for wireless security enhancement: current challenges and future developments’, *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, Jun. 2016, doi: 10.1109/MCOM.2016.7498103.

[4] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, ‘Design of an OFDM Physical Layer Encryption Scheme’, *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2114–2127, Mar. 2017, doi: 10.1109/TVT.2016.2571264.

[5] D. S. Ene, I. N. Davies, G. F. Lenu, and I. B. Cookey, ‘Implementing ECC on Data Link Layer of the OSI Reference Model’. arXiv, Sep. 25, 2021. doi: 10.48550/arXiv.2109.12403.

[6] A. Lombardo, E. Merelli, and S. Palazzo, ‘Implementation of encryption services in the OSI upper layers’, in *[1988] Proceedings. Computer Networking Symposium*, 1988, pp. 107–111. doi: 10.1109/CNS.1988.4986.

[7] C. Manusankar, S. Karthik, and T. Rajendran, ‘Intrusion Detection System with packet filtering for IP Spoofing’, in *2010 International Conference on Communication and Computational Intelligence (INCOCCI)*, Dec. 2010, pp. 563–567. Accessed: May 27, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5738791

[8] ‘What is IPSec? - IPSec Protocol Explained - AWS’, Amazon Web Services, Inc. Accessed: May 27, 2024. [Online]. Available: https://aws.amazon.com/what-is/ipsec/

[9] J. Iyengar and M. Thomson, ‘QUIC: A UDP-Based Multiplexed and Secure Transport’, Internet Engineering Task Force, Request for Comments RFC 9000, May 2021. doi: 10.17487/RFC9000.