Dan Otieno.
CPE 459 – Spring '24.
MITM Lab

# Man-in-the-Middle (MITM) Attack

## 1 Post Exercise Report

1.1 (30 points) Submit a video showing the effects of each one of your attacks (3.1, 4.1, and 4.2) on the HMI and the PLC (breadboard).

- **Submitted zip file in Canvas.**

1.2 (30 points) Submit all your Ettercap filters.

- **Submitted in the same zip file as videos ("filters&vids.zip").**

1.3 (20 points) In *Exercise 6: DoS*, the HMI was able to respond when performing SYN flood; however, the HMI does not respond when conducting a MITM DoS on 3.1. Explain why this is the case. Compare and contrast these attacks.

- **SYN Flood Attack: A SYN flood attack exploits the TCP three-way handshake process by sending a wave of TCP SYN packets to the target system, without completing the handshake. While the system's connection queue is flooded, its resources are exhausted, rendering it unable to accept legitimate connection requests. While a SYN flood attack overwhelms the targeted system with half-open connections, leading to a denial of service for legitimate users trying to establish connections, it remains operational to some extent and can potentially respond to incoming requests, with significant delay. Therefore, the system may experience degraded performance or temporary unavailability due to the SYN flood attack, but it can still manage to respond to incoming requests, albeit slowly.**
- **MitM Attack: A MitM DoS attack involves intercepting communication between two parties and disrupting the flow of data, typically achieved by intercepting packets and dropping them, altering their content, or by impersonating one of the parties. In general, the attacker's goal is to disrupt communication between the victim and the legitimate server, rendering the service inaccessible to the victim. Unlike SYN flood attacks, where the targeted system can still respond to incoming requests, a MitM DoS attack aims to prevent communication altogether between the victim and the legitimate server. Therefore, the victim may not receive any response from the targeted server, leading to a complete denial of service.**

Dan Otieno.
CPE 459 – Spring '24.
MITM Lab

1.4 (20 points) What are some countermeasures to prevent MITM attacks? Explain.

- **Encryption: End-to-end encryption using strong cryptographic protocols such as SSL/TLS for web traffic, SSH for remote access, and VPNs for securing network communication. Encryption keeps content unreadable from the attacker's perspective even if communication is intercepted.**
- **Certificate Pinning: Certificate pinning is used to ensure that communication occurs only with trusted servers whose digital certificates have been pre-approved. Attackers are prevented from impersonating legitimate servers using fraudulent certificates.**
- **Public Key Infrastructure (PKI): A PKI can be employed to manage digital certificates and to enable secure authentication of communication endpoints. This ensures that identities of parties involved in a communication are verified, and unauthorized entities may be detected.**
- **Regular Security Audits: Regular security audits and vulnerability assessments can be conducted to identify and address potential weaknesses in the network infrastructure, thus proactively helping in detecting and mitigating MitM attack vectors.**
- **Network Segmentation: Segmented networks restrict access and minimize the attack surface. Use of firewalls, VLANs, and access control lists (ACLs) help isolate sensitive systems and limit the impact of MitM attacks.**
- **Mutual Authentication: Mutual authentication involves parties authenticating each other before establishing a connection, such that both the client and server are legitimate entities, mitigating the risk of MitM attacks.**
- **Security Awareness Training: Employees and users must be educated about the risks of MitM attacks and best practices for securely accessing and transmitting sensitive information.**

## Cited Sources:

- **Ferguson, Niels, and Bruce Schneier. "Practical Cryptography." Wiley, 2003.**
- **Balfanz, Dirk, et al. "The SSL/TLS Handshake Protocol: An Overview." IETF, 2006.**
- **Adams, Carlisle, and Steve Lloyd. "Understanding PKI: Concepts, Standards, and Deployment Considerations." Addison-Wesley Professional, 2003.**
- **Bejtlich, Richard. "The Practice of Network Security Monitoring." No Starch Press, 2013.**

- **Zhu, Y., & Hu, H. (2014). "Research on mutual authentication mechanism based on TLS/SSL protocol." 2014 IEEE Workshop on Advanced Research and Technology in Industry Applications (WARTIA).**
- **Northcutt, Stephen, et al. "Network Intrusion Detection: An Analysts' Handbook." New Riders, 2012.**
- **Cole, Eric. "Cybersecurity for Executives: A Practical Guide." Wiley, 2014.**