H E A D Q U A R T E R S
ARMED FORCES OF THE PHILIPPINES CYBER COMMAND
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN 2025-08

Man-in-the-Middle (MITM) Attacks: Silent Interceptors in Cyberspace

Overview

MITM attacks present a critical cybersecurity threat in military networks by intercepting and potentially altering sensitive communications between parties without their knowledge. These attacks allow adversaries to covertly eavesdrop, steal classified information, or manipulate command and control data flows, posing risks to operational security and mission integrity.

A MITM attack occurs when a hostile actor positions themselves between two communicating parties such as personnel, systems, or networks intercepting data exchanged without detection. The attacker may also alter communications, leading to misinformation or unauthorized actions. Typical phases include interception of the communication channel, often through compromised Wi-Fi, IP or DNS spoofing, or ARP poisoning, followed by decryption of intercepted data for exploitation.

The AFP's reliance on secure, real-time communications for strategic commands, intelligence sharing, and operational coordination makes MITM attacks exceptionally dangerous. Adversaries exploiting weak points in military communication infrastructure can redirect or manipulate commands, breach classified networks, or conduct espionage. Historical incidents, such as interception and compromise of sensitive NATO documents due to insecure channels, highlight threats from MITM attacks in defense environments.

Common Techniques Used in MITM attacks are:

- IP Spoofing and DNS Spoofing to mislead communication endpoints.
- Exploiting unsecure Wi-Fi networks.
- Hijacking encrypted sessions via SSL/TLS vulnerabilities.
- Phishing and social engineering to gain access credentials for email or command systems

Recommendations

Following are the recommendations to prevent MITM attacks to AFP networks:

- Employ end-to-end encryption on all communication channels.
- Use multi-factor authentication and strict access controls on communication networks.
- Conduct continuous network monitoring and anomaly detection to identify unusual interception activity.
- Educate personnel on recognizing phishing attempts and secure handling of access credentials.
- Validate the security configuration of Wi-Fi connections before operational use.

Conclusion

MITM attacks undermine military communication integrity by allowing adversaries to stealthily intercept, alter, or disrupt critical information exchanges. Protecting military networks requires a layered cybersecurity strategy focused on encryption, vigilant monitoring, and personnel training to guard against these covert intrusions.

Stay alert, stay safe, protect every military communication.

References:

a. *https://sosafe-awareness.com/glossary/man-in-the-middle-attack/*
b. *https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/man-in-the-middle-mitm-attack/*
c. *https://www.ibm.com/think/topics/man-in-the-middle*