The Man in the Middle

Devante Metoyer

University of Arizona

CYBV 326: Introductory Methods of Network Analysis

Jonathan Martinez

April 20th, 2024

Wireless Network Attacks and Mitigation Strategies

Wireless and mobile networks, while facilitating global connectivity, are susceptible to specific security attacks. Two prevalent attacks include the Man-in-the-Middle Attack and the Wi-Fi Eavesdropping. The Man-in-the-Middle Attack occurs when an attacker intercepts communication between two unsuspecting parties. In wireless networks, this is often implemented via rogue Wi-Fi access points that appear legitimate but are controlled by the attacker. Once a user connects to such a network, the attacker can monitor and manipulate traffic. Mitigation involves using strong, end-to-end encryption protocols like HTTPS, ensuring all data remains encrypted and unintelligible to the interceptor. Wi-Fi Eavesdropping involves listening to unsecured wireless communications to capture sensitive data such as passwords and credit card numbers. This attack exploits the lack of encryption on many wireless networks. Implementing strong Wi-Fi Protected Access II (WPA2) or WPA3 encryption standards can significantly hinder eavesdroppers by encrypting the data transmitted over airwaves, thus upholding the confidentiality principle where "only the sender and intended receiver should be able to understand the contents of the transmitted message" (Kurose & Ross, 2021, p. 608).

For both attacks, employing Virtual Private Networks (VPNs) can provide an additional layer of security by encrypting data before it even reaches the Wi-Fi network, thus securing the user’s data across potentially insecure networks. Regular security training for users to recognize and avoid suspicious networks is also essential in mitigating these threats.

Insights from VoIP and QoS

In multimedia networking, particularly in Voice over Internet Protocol and Quality of Service frameworks, there are significant vulnerabilities that can compromise the integrity and

availability of services. Two notable vulnerabilities include Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks targeting VoIP networks, and the exploitation of QoS to prioritize malicious traffic.

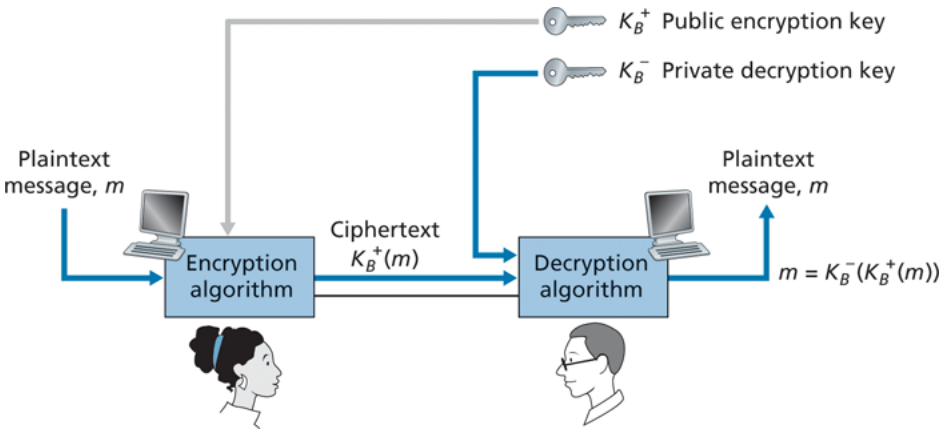
Firstly, VoIP services are susceptible to DoS and DDoS attacks due to their reliance on internet protocols and real-time communication requirements. An example is the flooding of VoIP servers with SIP (Session Initiation Protocol) messages, which overwhelms the server and prevents legitimate users from accessing the service. Such attacks can be launched using methods like INVITE, REGISTER, and BYE, effectively exhausting the server resources (Nazih et al., 2021).

Secondly, the manipulation of QoS, which is designed to prioritize internet traffic to ensure the quality of service, presents another vulnerability. Attackers can exploit QoS rules to prioritize their traffic, which can degrade the service for legitimate users and disrupt critical communications. This type of attack not only affects the efficiency of network performance but also compromises data integrity.

To mitigate these vulnerabilities, it is essential to employ robust security measures such as deep packet inspection, proper configuration and management of QoS settings, and real-time monitoring of network traffic. Employing advanced intrusion detection systems that utilize deep learning algorithms, such as Convolutional Neural Networks (CNNs), to detect and prevent attacks on VoIP systems is also crucial. These systems are designed to identify malicious activities with high accuracy and reduce detection times, thus maintaining the stability and security of multimedia services (Nazih et al., 2021).

Diffie-Hellman Key Exchange Process

The Diffie-Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel. This process is fundamental in many protocols, including those that establish secure communications over the Internet. Here's a step-by-step breakdown of the Diffie-Hellman key exchange process (Kurose & Ross, 2021, p. 619):



1. Agreement on Parameters: Alice and Bob agree on a large prime number p and a base g, which are public values.
2. Private Keys: Both Alice and Bob independently generate their private keys, a and b respectively, which are kept secret.
3. Public Keys: Alice computes her public key by calculating $\boldsymbol{A = g^a}$ mod p and sends A to Bob. Similarly, Bob computes his public key $B = g^b$ mod p and sends it to Alice.
4. Compute Shared Secret: Upon receiving Bob's public key B, Alice computes the shared secret key as $s = B^a$ mod p. Similarly, Bob computes $s = A^b$ mod p. Due to the properties of modular arithmetic, both calculations result in the same shared secret.

The security of the Diffie-Hellman exchange lies in the difficulty of deriving the private keys from the public keys, a problem known as the discrete logarithm problem, which is computationally infeasible to solve efficiently for large primes. This key exchange method does

not authenticate the parties involved, which means it is vulnerable to man-in-the-middle attacks unless combined with other security protocols that can provide authentication.

Client side Server side

In the realm of cybersecurity, both client-side and server-side attacks pose significant risks. On the client-side, Cross-Site Scripting (XSS) is a prevalent threat. This occurs when attackers inject malicious scripts into otherwise benign and trusted websites. Once the user visits the compromised website, the malicious script is executed in the user's browser, potentially leading to data theft or unauthorized actions on behalf of the user. Clients can mitigate XSS attacks by enabling features like Content Security Policy (CSP) that helps in specifying which dynamic resources are trusted, thus preventing the browser from executing unauthorized scripts.

For the server-side, a common threat is Distributed Denial of Service (DDoS) attacks, which can bring down a server by overwhelming it with traffic. These attacks can be mitigated through various strategies, including the deployment of specialized DDoS mitigation hardware or services that can filter out malicious traffic and scaling server resources to handle unexpected loads. Additionally, implementing network security measures like firewalls and intrusion detection systems can help in recognizing and blocking attack patterns.

Both XSS and DDoS attacks exploit different vulnerabilities, but the end goal is often the same—to disrupt normal operations and compromise data integrity. While XSS targets users to execute malicious scripts, DDoS directly aims at the service availability of servers. Continuous monitoring, regular updates to software, and strict security protocols are fundamental in protecting both clients and servers from these attacks (Klepper, 2022).

The 3 Mech Web

To establish a secure connection with a web server, three key mechanisms are commonly employed:

HTTPS (Hypertext Transfer Protocol Secure): HTTPS is the foundational protocol for secure communications over the internet. It encrypts data transferred between a user's browser and a website to protect sensitive information, utilizing Transport Layer Security (TLS) or its predecessor, Secure Sockets Layer (SSL). Websites using HTTPS display a padlock icon in the browser's address bar, indicating that the connection is secure and that the website's identity has been authenticated with a TLS/SSL certificate. HTTPS uses port 443, differentiating it from HTTP which uses port 80(Kurose & Ross, 2021, p. 96)..

TLS (Transport Layer Security): TLS is an encryption protocol that ensures the security of data transmitted over a network by using asymmetric public key infrastructure. This involves two keys: a public key that anyone can use to encrypt messages to the server, and a private key that the server uses to decrypt messages encrypted with the public key. The TLS handshake is the process by which the client and server establish a secure connection, including the negotiation of encryption algorithms and the exchange of key information.

SSH (Secure Shell Protocol): For secure remote administration, SSH is used to encrypt the connection between a client and a server, safeguarding login credentials and other sensitive data exchanged during the session. SSH employs asymmetric encryption for authenticating the remote user and symmetric encryption to maintain the confidentiality and integrity of the data. Changing the default SSH port from 22 to a random port number between 1024 and 32767 is a common security practice to avoid unauthorized access.

Conclusion

In summary, wireless networks face security challenges like Man-in-the-Middle and Wi-Fi Eavesdropping, mitigated through encryption standards such as WPA2/WPA3 and secure protocols like HTTPS and VPNs. Multimedia networking and web server connections rely on technologies like TLS and SSH for safe data transmission, combating vulnerabilities from DoS/DDoS attacks and unauthorized access. Continuous updates and user education on security best practices are key to safeguarding network integrity amidst evolving cyber threats.

References

Kurose, J., & Ross, K. (2021). *Computer Networking: Eighth Edition*. O'Reilly.

Nazih, W., Hifny, Y., Elkilani, W., & Abdelkader, T. (2021). *Fast Detection of Distributed Denial of Service Attacks in VoIP Networks Using Convolutional Neural Networks.* International Journal of Intelligent Computing and Information Sciences, 20(2), 125-138. https://journals.ekb.eg/article_145903_b799822fbdffddf56178d1dbd887abac.pdf.

Klepper, M. (2022). *Top 12 client-side security threats.* AT&T. https://cybersecurity.att.com/blogs/security-essentials/top-12-client-side-security-threats.