Wireless LAN Threats

Mobile Computing Presentation

- Atharva Sankhe (TE Comps B 96)
- Anil Sawant (TE Comps B 97)

Introduction to Wireless LAN Threats

Wireless LAN (Local Area Network) connections are vulnerable to various security threats.

Piggybacking: Definition and Examples

Security Risk

Piggybacking poses serious security risks by enabling unauthorized access to networks, potentially resulting in data breaches, malware distribution, network congestion, legal liabilities, and reputational damage.

Preventive Measures

Implementing robust security protocols, including strong authentication, encryption, access controls, and user education, can help prevent piggybacking and mitigate associated risks. Regular security audits and updates to patch vulnerabilities are essential.

Cracking Attack: How it Works and Its Impact

Process

In a cracking attack, attackers systematically attempt to exploit security vulnerabilities, such as weak passwords or software flaws, to gain unauthorized access to a system or network.

Impact

It gains unauthorized access to a system or network, potentially leading to data breaches, financial losses, reputational damage, personal privacy breaches, and identity theft.

Evil Twin Attack: Explanation and Prevention Measures

Deceptive Networks

Deceptive networks involve creating fake network environments to lure attackers away from critical systems or to gather intelligence on their tactics and techniques. It is also known as honeypots or decoy systems.

Mitigation Techniques

Mitigation techniques for deceptive networks encompass segmentation, monitoring, dynamic environments, early warning systems, intelligence sharing, diverse tactics, security control integration, and regular evaluation, ensuring robust cybersecurity defense.

Wireless Sniffing: Techniques and Risks

Method

Wireless sniffing involves capturing and analyzing data packets from wireless networks using specialized tools, with techniques including passive observation and active probing.

Risks

The risks associated with wireless sniffing include unauthorized data interception, eavesdropping, credential theft, and network reconnaissance, posing significant threats to data confidentiality, integrity, and privacy.

Mobile Computing and Its Vulnerability to Wireless LAN Threats

Mobile Devices

Mobile devices, relying on wireless LANs, face vulnerabilities like eavesdropping and unauthorized access, highlighting the crucial need for robust encryption and authentication measures to protect sensitive data and user privacy.

Remote Access

Remote access to mobile devices introduces vulnerabilities such as intercepted data transmission and unauthorized control access, emphasizing the need for strong encryption and authentication measures to safeguard data integrity and user privacy.

Mitigation Strategies for Wireless LAN Threats

Encryption

Implement strong encryption protocols, such as WPA3, to secure wireless communications.

Intrusion Detection Systems (IDS)

Deploy proactive IDS to detect and prevent unauthorized access to wireless networks.

Regular Audits

Conduct frequent network audits and security checks to identify and mitigate potential vulnerabilities.

Conclusion and Key Takeaways

1

Awareness

Awareness of wireless LAN threats is essential for proactive mitigation and safeguarding sensitive data on mobile devices.

2

Continuous Improvement

Regularly update security protocols to adapt to evolving wireless network threats.

3

Education and Training

equip individuals with knowledge and skills to effectively mitigate risks such as eavesdropping and unauthorized access, bolstering overall security readiness.

Thank You!