Assignment 3: Research on Wireless Network Security

Name: Abdulmajeed Aldawish

ID:431109432

Course: COE 351

Delivery 1: Wireless Connectivity Types:

1. Wi-Fi (Wireless Fidelity):

Wi-Fi provides wireless radio wave connectivity through which devices get connected to the internet or the local area network without cable connection. Wi-Fi runs primarily on the frequency band 2.4 GHz and 5 GHz.

Applications: Laptops, tablets, smart TVs, routers, mobile phones, and Internet of Things devices.

2. Bluetooth:

Overview: Bluetooth creates a near-field connection among devices by conveying signals over UHF radio waves. Bluetooth will generally have a range of about 10 meters.

Applied to: Wireless headsets, smartwatches, game controllers, fitness trackers, and computer accessories.

3. 3rd, 4th and 5G Cellular Networks:

Overview: Cellular networks use cellular towers to offer wireless communication over an extensive area and keep devices in contact even if they are mobile.

Used by: Handsets, in-vehicle GPS, pocket hotspots, and wearables.

Deliverable 2: Common Problems in Wireless Networks

1. Illegal Network Use

Problem: Such open or insecure Wi-Fi networks are available for malicious users or hackers.

Solution: This could lead to bandwidth abuse, data loss, or malware download.

Example: A cyber thief steals customers' usernames by using the open link in a coffee shop.

2. Interference by Wireless
Problem: The microwave appliances and the nearby networks disrupt the signal.
Consequence: It causes connection loss or unstable speeds, which degrade the performance.
Situation: Baby monitor causes consistent drops from a home router.

3. Network Performance Degradation:
Slower network speeds may be caused by network
traffic congestion, inadequate bandwidth, or old equipment.
Problem: Remote work, gaming, and streaming have too many slow speeds.
Context: Multiple remote workers lead to lag on video calls as well as slow downloading

Deliverable 3: Security Threats and Vulnerabilities

1. Eavesdropping Attacks

- **Role:** Attackers sniff wireless traffic in the clear to gain valuable information.
- **Risk:** Confidential information such as bank account numbers or personal emails becomes exposed.
- **Real-World Example:** Attackers use programs such as **Wireshark** to spy on users who log in to open Wi-Fi at hotels.

2. Man-in-the-Middle (MitM) Intrusion

- **Role:** The attacker invisibly directs or manipulates communication between two users.
- **Risk:** The victims might inadvertently reveal passwords or confidential information to the attacker.
- **Real-World Example:** A public airport Wi-Fi access point that pretends to be a legitimate one in order to pilfer user data.

3. Brute-Force Credential Cracking

- **Functionality:** Router password cracked by automated software attempting many combinations.
- **Vulnerability:** Complete network and device access will be granted to the attackers upon cracking.
- **Real-World Example:** Hackers remotely reset home networks via weak admin passwords on routers

Deliverable 4: Solutions to Wireless Network Problems

1. WPA3 Secure the Network

Solution: Provides device-to-device encryption as well as individual authentication at a per-device-level.

Efficiency: Avoids password guessing attack as well as data sniffing.

Implementation: Firmware update the routers and enable WPA3 via the router settings.

2. Interference Avoidance through Environment Optimization

Solution: Position the router in the middle of the room and ideally away from interference-generating devices.

Efficiency: Avoids packet loss as well as signal degradation.

Tools: Utilize Wi-Fi channel scanners to look for less busy channels.

3. Traffic Control Optimization and Hardware Upgrade

Solution: Upgrade the older routers with newer routers of higher throughputs and improved QoS capability.

Efficiency: Eliminates bottlenecks and optimizes bandwidth utilization.

Equipment: Wi-Fi 6 enabled routers, bandwidth control tools, and usage policy.

Deliverable 5: Wireless Network Security Checklist

1. Enable the newest encryption standard (WPA3) on your router for more secure data.
2. Hard code non-default usernames and passwords on all default accounts simultaneously.
3. Perform regular firmware upgrades to close network device security vulnerabilities.
4. Change Wi-Fi passwords frequently and never give them to strangers.
5. Position your router firmly and turn off unnecessary ports and services.

References

1. Cisco Systems. (2023). Introduction to Wireless Network Security. Retrieved from https://www.cisco.com

2. Kaspersky. (2024). Securing Wireless Networks. Retrieved from https://www.kaspersky.com

3. Norton LifeLock. (2024). Types of Cyber Threats. Retrieved from https://us.norton.com

4. Network World. (2023). Demystifying Wi-Fi 6 and Future Standards. Retrieved from https://www.networkworld.com