Computer Security – Week 11

1. Home Network Security Audit

I checked the security of my home Wi-Fi network. The router is using WPA2 encryption for protection. The SSID (network name) is visible to everyone, which means anyone nearby can see it. WPS (Wi-Fi Protected Setup) is currently enabled, and the firmware version of the router is v1.0.4.

After checking, I found a few weaknesses. First, WPA2 is secure, but WPA3 would offer stronger protection. Second, keeping the SSID visible makes it easier for attackers to try connecting. Third, having WPS enabled can allow hackers to guess the PIN and get access to the network.

To make the network safer, I would:
1. Update the router's firmware to the latest version.
2. Turn off WPS to block PIN-based attacks.
3. Hide the SSID or rename it to something that doesn't reveal my identity.
4. Use WPA3 security if supported.
5. Change the default admin password to a strong one.
6. Check connected devices regularly and remove unknown ones.

Following these steps will make my home Wi-Fi much more secure and harder for attackers to break into.

2. Research: The Future of Wireless Security – 5G Security

5G is the newest generation of mobile network technology. It offers faster internet speeds, lower delay (latency), and better support for many connected devices like smart cars, smart homes, and Internet of Things (IoT) systems. Because of these features, 5G is used in areas like autonomous driving, remote healthcare, smart cities, and industrial automation.

However, 5G also brings new security challenges. Since it connects millions of devices, attackers can target weak IoT devices to launch DDoS attacks. The virtualization of 5G networks also makes it easier for hackers to attack the network core. Another risk is data interception, especially if encryption is not properly used.

To protect 5G networks, several security measures are recommended:
1. Use end-to-end encryption for all communications.
2. Strong authentication for users and devices.
3. Regular software updates to patch vulnerabilities.
4. Network slicing security, ensuring that one compromised slice doesn't affect others.
5. AI-based monitoring to detect and stop attacks in real-time.

Overall, 5G offers huge benefits, but it must be protected with strong security measures to keep data and users safe in the future.