key considerations for ensuring wireless network security include:

- Wireless network security is essential to protect the confidentiality, integrity, and availability of data transmitted over wireless networks.

1. Encryption: Implementing strong encryption protocols such as WPA3 (Wi-Fi Protected Access 3) or WPA2 with AES (Advanced Encryption Standard) can help secure wireless communications and prevent unauthorized access to data.

2. Secure Authentication: Enforcing strong authentication mechanisms such as WPA3-Personal or WPA3-Enterprise can help verify the identity of users and devices connecting to the wireless network.

3. Network Segmentation: Segmenting wireless networks into separate VLANs (Virtual Local Area Networks) can help contain security breaches and limit the impact of potential attacks.

4. Intrusion Detection and Prevention Systems: Deploying intrusion detection and prevention systems can help monitor wireless network traffic for suspicious activities and block potential threats in real-time.

5. Regular Security Audits: Conducting regular security audits and assessments of wireless networks can help identify vulnerabilities, misconfigurations, and potential security risks that need to be addressed.

- By implementing these best practices and staying informed about emerging threats and security trends, organizations can enhance the security posture of their wireless networks and protect sensitive data from unauthorized access or malicious activities.

Vulnerabilities in Wireless Networks

- Confidentiality
- Integrity
- Availability
- Unauthorized WiFi access
- WiFi protocol weaknesses
  - Picking up the beacon
  - SSID in all frames
  - Association issues

Failed Countermeasure: WEP

- Wired equivalent privacy, or WEP, was designed at the same time as the original 802.11 WiFi standards as the mechanism for securing those communications
- Weaknesses in WEP were first identified in 2001, four years after release
- More weaknesses were discovered over the course of years, until any WEP-encrypted communication could be cracked in a matter of minutes

How WEP Works

- Client and access point (AP) have a pre-shared key
- AP sends a random number to the client, which the client then encrypts using the key and returns to the AP
- The AP decrypts the number using the key and checks that it's the same number to authenticate the client
- Once the client is authenticated, the AP and client communicate using messages encrypted with the key

WEP Weaknesses

- Weak encryption key
  - WEP allows to be either 64- or 128-bit, but 24 of those bits are reserved for initialization vectors (IV), thus reducing effective key size to 40 or 140 bits
  - Keys were either alphanumeric or hex phrases that users typed in and were therefore vulnerable to dictionary attacks
- Static key
  - Since the key was just a value the user typed in at the client and AP, and since users rarely changed those keys, one key would be used for many months of communications
- Weak encryption process
  - A 40-bit key can be brute forced easily. Flaws that were eventually discovered in the RC4 encryption algorithm WEP uses made the 104-bit keys easy to crack as well

WEP Weaknesses (cont.)

- Weak encryption algorithm
  - WEP used RC4 in a strange way (always a bad sign), which resulted in a flaw that allowed attackers to decrypt large portions of any WEP communication
- IV collisions
  - There were only 16 million possible values of IV, which, in practice, is not that many to cycle through for cracking. Also, they were not as randomly selected as they should have been, with some values being much more common than others
- Faulty integrity check
  - WEP messages included a checksum to identify transmission errors but did not use one that could address malicious modification
- No authentication
  - Any client that knows the AP's SSID and MAC address is assumed to be legitimate

WPA (WiFi Protected Access)

- WPA was designed in 2003 as a replacement for WEP and was quickly followed in 2004 by WPA2, the algorithm that remains the standard today
- Non-static encryption key
  - WPA uses a hierarchy of keys: New keys are generated for confidentiality and integrity of each session, and the encryption key is automatically changed on each packet
  - This way, the keys that are most important are used in very few places and indirect ways, protecting them from disclosure
- Authentication
  - WPA allows authentication by password, token, or certificate

WPA (cont.)

- Strong encryption
  - WPA adds support for AES, a much more reliably strong encryption algorithm
- Integrity protection
  - WPA includes a 64-bit cryptographic integrity check
- Session initiation
  - WPA sessions begin with authentication and a four-way handshake that results in separate keys for encryption and integrity on both ends
- While there are some attacks against WPA, they are either of very limited effectiveness or require weak passwords