Discussion Questions & Answers

Exploring Wi-Fi Security Protocols – WPA2 vs WPA3

Group Members:

Arunima Negi (30281210), Huma Naiman (30303242), Karanveer Singh (30282286),
Pradip Ghimire (30303867)

Questions:

1. Why is Enterprise mode considered more secure than PSK mode in WPA2?
2. What is the Password Element (PE) in WPA3's SAE handshake? What algorithm is used in the derivation of the Password Element? What makes it non-reversible, and what type of attacks does this non-reversibility protect against?
3. Should mitigation of KRACK vulnerabilities focus more on patch deployment at the device level or protocol redesign at the standards level?

Answers:

1. Enterprise mode in WPA2 offers more security than PSK mode because the 802.1X protocol is used to authenticate users individually, with distinct credentials for each person, so that every individual connecting to the network must enter their own username and password. This, in turn, renders the entire network much more resistant to being compromised by an attacker because guessing or stealing one individual's credentials doesn't provide access to all the devices. In PSK mode, all the users and devices in the network share the same password i.e. when that password is compromised or broken, all the devices in the network are instantly compromised, and the resulting reset and reconfiguration take all the devices off the air for an extensive period. Enterprise mode offers centralized management, instantaneous revocation of individual user's privileges, and individual user audit logging, so this mode, by far, is the gold standard in organizations where security of the data and keeping people accountable are essential.

2. The Password Element (PE) in WPA3's Simultaneous Authentication of Equals (SAE) handshake is a valid group element on the chosen elliptic curve or finite field that both peers derive by converting the plaintext password through the hunting-and-pecking algorithm. This ensures that the mapping from password to group element is deterministic yet computationally infeasible to reverse.

   The Password Element is non-reversible due to three factors-

   - *Hash functions are one way:* The process uses hash functions, which scramble data in a way that can't be unscrambled. They are one-way cryptographic functions that convert input data into a fixed size output (hash) in an irreversible manner.

- *Multiple inputs mixed together:* The Password Element is created from the password + MAC addresses + a counter. Even if someone had the Password Element, they wouldn't know which counter value was used, making it even harder to work backward.
- *Elliptic curve math is hard to reverse:* Elliptic curve math is computationally hard to reverse due to the Elliptic Curve Discrete Logarithm Problem, making it practically impossible to derive the original values from a resulting curve point.

This non-reversibility protects against offline dictionary attacks. During the WPA3 handshake, devices exchange information based on the Password Element, not the password itself. Even if an attacker captures all this information, they can't work backward to find the password. They can't test password guesses offline because they'd need to interact with the actual network to check if their guess produces the right Password Element.

3. Mitigating KRACK should focus on both patching and protocol redesign, but in practice, device-level patching is the immediate priority. Updating clients and access points closes the WPA2 key reinstallation flaw exploited in KRACK and is critical to protect existing infrastructure. However, long-term security requires protocol redesign—as implemented in WPA3, which eliminates the vulnerable four-way handshake and introduces stronger key exchange methods such as SAE, preventing replay or key reinstallation attacks. In short: patching defends today's networks, while protocol redesign secures future ones.