Paper: Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2

Summary:

The paper performs key reinstallation attack that abuses design or implementation flaws in cryptographic protocols used by the 4-way handshake in protected WiFi networks. These include both WPA and WPA-2-certified products. It does so by manipulating and replaying handshake messages, thus reinstalling a key that’s already being used. The attack also breaks PeerKey, group key, and Fast BSS Transition handshake. The impact on these is dependent on handshake under attack and data-confidentiality protocols being used. It ranges from decrypting arbitrary packets, injecting arbitrary packets to replaying group-addressed frames. All of this is achieved without the session key being leaked.

Strengths:

1. The paper provides a very detailed analysis of the vulnerabilities of WPA2 and how to abuse each of those scenarios. It also covers the attack against a range of devices and operating systems, including Android, Linux, Windows, and macOS.
2. The paper mentions 2 countermeasures: 1.: Checking if a key that’s already in use, is being installed then the entity implementing data confidentiality protocol shouldn’t reset associated nonces and replay counter. 2.: Assuring particular key is installed only once. This implies that the client should reply to a retransmitted message 3 but shouldn’t reinstall the session key.
3. The key reinstallation attack proposed by the paper goes to prove that formally proven secure protocols might not guarantee security in reality. The paper validates the security proofs and shows how the attack is successful while satisfying the formal security criteria shown by the protocol.

Weakness:

1. The paper doesn’t talk about how practical the attacks are in real-world scenarios. Technical aspects like the feasibility of the attack, time taken for performing the MiTM, and reinstallation of keys are left out. Even though the attacks mentioned are technically very feasible, a real-world demonstration would give valuable information on how long and complex it is to perform the attack. It mainly relies on laboratory experiments and simulations, and does not provide evidence of widespread or real-world exploitation.
2. Scope of impact is limited to talking about authentication and key exchange process of WPA., While an attacker may be able to intercept or manipulate Wi-Fi traffic through key reinstallation attacks, they would still need to decrypt the data to obtain any sensitive information. There’s no discussion around this aspect.