Wi-Fi Security Protocols for Mobile Devices

Industry Trends and Needs

As mobile devices see increased usage by the general public every year and more of the world becomes connected to the internet, the issue of network security has become increasingly critical for all parties involved in the development, production, and use of mobile devices. In particular, apps that require entering sensitive information, such as banking apps, online stores, and medical record apps, are especially vulnerable to attacks focused on stealing personal data. One of the most common vectors of attack is through connections to Wi-Fi networks, as almost all modern mobile devices can connect to the internet through Wi-Fi and the prevalence of less secure public Wi-Fi networks provides attackers with a convenient method of intercepting network communications.

Current Solutions

In response to the need for robust network security, there have been several protocols developed by the Institute of Electrical and Electronics Engineers (IEEE) to address these concerns. The first one that saw widespread use was known as the Wired Equivalent Privacy protocol (WEP), which was ratified in 1997 and was largely based on the RC4 stream cipher [1]. However, security researchers discovered major flaws in the RC4 cipher in 2001 and WEP was quickly deprecated as a result [1]. Subsequently, the IEEE developed a series of network security protocols that successively improved the security of mobile devices: WPA, WPA2, and WPA3. WPA has been largely phased out due to vulnerabilities discovered in its message integrity code, while WPA2 and WPA3 continue to be used to this day [2]. These two serve as the primary network security protocol for most Wi-Fi networks today.

Analysis

WPA2 is the most commonly used network security protocol due to its relative safety and its ease of use. However, within the past decade, several security flaws have been found within WPA2, most notably key reinstallation attacks which target the process of generating new session keys through a 4-handshake system that was previously thought to be secure [2]. WPA3 has been proposed as a solution to these vulnerabilities in WPA2; however, the process of upgrading devices to this new security standard has difficult as many older devices cannot support WPA3 (even if the local network routers can) and there remain security flaws within the protocol (i.e. a group of researchers discovered in 2019 that the Dragonfly handshake key exchange method used in WPA3 could be easily broken by attackers to gain access to any network using WPA3) [4]. As a result, WPA2 continues to be widely used due to its convenience from backward compatibility and the issues that continue to arise with WPA3.

Proposal

One solution to the vulnerability of WPA2 to various attacks is to create an intrusion detection system (IDS) that can detect and stop attacks in real time, without the need to immediately alter the encryption algorithms used [3]. Although many such solutions have been proposed for WPA3, there is less discussion on these types of security measures for WPA2. Therefore, I propose that an IDS using a machine learning model that can learn to recognize network attacks in real-time should be included in the WPA2 protocol as an additional layer of security. Although this solution has been proposed for WPA3, including an IDS in WPA2 as well would be much more impactful since the majority of mobile devices around the world still use WPA2 security and thus would not be dependent on waiting for WPA3 to become widely available [3].

References

[1] Fluhrer, S.R., Mantin, I., & Shamir, A. (2001). Weaknesses in the Key Scheduling Algorithm of RC4. ACM Symposium on Applied Computing. https://www.cs.cornell.edu/people/egs/615/rc4_ksaproc.pdf

[2] Huang, J., Seberry, J., Susilo, W., Bunder, M. (2005). Security Analysis of Michael: The IEEE 802.11i Message Integrity Code. In: Enokido, T., Yan, L., Xiao, B., Kim, D., Dai, Y., Yang, L.T. (eds) Embedded and Ubiquitous Computing – EUC 2005 Workshops. EUC 2005. Lecture Notes in Computer Science, vol 3823. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11596042_44

[3] Kohlios CP, Hayajneh T. A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. Electronics. 2018; 7(11):284. https://doi.org/10.3390/electronics7110284

[4] Mathy Vanhoef, & Eyal Ronen. (2019). Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. https://eprint.iacr.org/2019/383