WPA3 Wi-Fi Security

Andrew Price

The progression of wireless technology over the years has been steadily evolving, and with it, so has wireless hacking. The number of per user wireless devices is increasing every day, and most of these devices contain personal identifiable information (PII). The IEEE[1] is responsible for the wireless standards (802.11) and setting the standards to secure the wireless medium. Since 1997 when wired equivalent privacy (WEP) was implemented, hackers have constantly identified vulnerabilities in wireless security technologies. With new security technologies being released, hackers consistently find new vulnerabilities. A Hackers sole purpose is to find vulnerabilities in technologies so they can obtain the encrypted information whether it be for personal benefit, political benefit, or any other type of benefit that would, in-turn, damage the hacked individual. Wireless security has been the focus of many companies that manufacture wireless devices because the customers information is considered a liability, and any exploit could lead to unwarranted consequences. Is the increase in wireless devices a basis for increasing wireless security? Is the most recent security standard as secure as we think it is? What is the next step in wireless security?

Devices that are wireless capable have become the new norm, and the number of wireless devices has been steadily increasing based on a few factors. The first factor is that devices that once needed to have an ethernet port, such as a laptop, no longer have them because they come with a wireless adapter installed. If any wired connection is needed, many vendors offer an

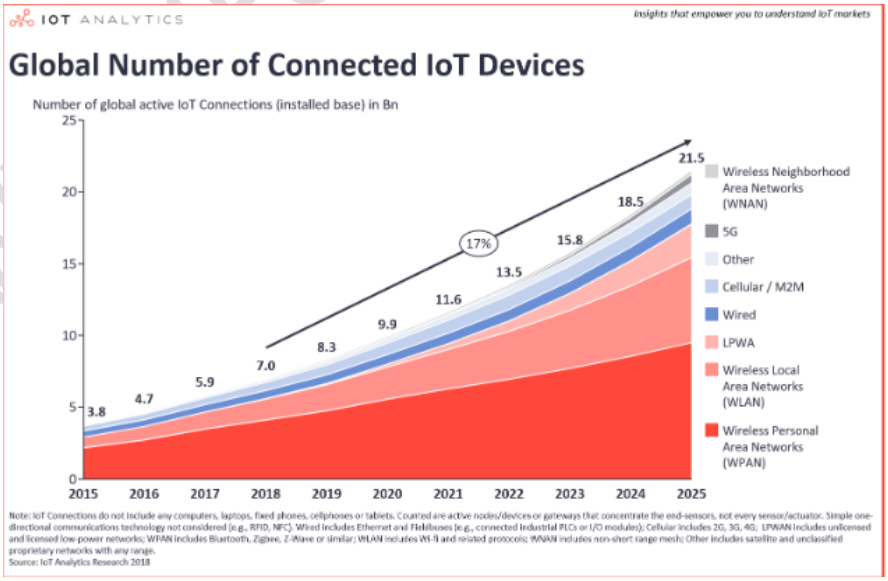
[1] Institute of Electrical and Electronics Engineers develop and maintain standards for the computer and electronics industry

WWW.INFOSECWRITERS.COM

external USB-to-ethernet adapter that still provide the users with a wired option if needed, such as initializing a SOHO router configuration.

Another leading factor to the increase of wireless devices is that wireless users are starting at a much younger age; some even as young as 3 years old. When going out in public, the number of children seen holding a smartphone, tablet, or Chromebook to keep their kids entertained while the parent gets their errands completed. Some companies have released tablets geared specifically for kids that only contain kid friendly applications and limited video access. This factor has significantly increased over the years

The last factor, and the most impacting, is the rise of the Internet of Things (IoT). IoT essentially enabling a device to be managed via the internet. Take for example the Google Nest which allows an end user to connect remotely or wirelessly and change the temperature of their home. An analytics study was conducted in 2018 by IOT Analytics to forecast the increase in IoT devices over the next 5 years:



WWW.ESSAYWRITERS.COM

While the IoT does include wired devices, wireless is also accounted for and becoming more common. With all these factors contributing to the growing wireless trend, end users have one major concern – security.

With the vulnerabilities introduced to WEP, the Wi-Fi Alliance introduced an enhanced security protocol in 2003 – WPA. WPA has two modes: WPA-personal and WPA-enterprise. WPA-personal utilizes a PSK and is deployed in home and small office deployments. WPA-enterprise is geared towards larger corporations and utilizes authentication protocols such as 802.1x and EAP. The key used in WPA is a bit size of 256, a size doubled that of the keys used in WEP. Hackers were able to exploit vulnerabilities in WPA which led to the enhanced version WPA2 that superseded WPA in 2006. Because of older devices that were still in use, WPA2 had to have some backwards compatibility so older devices could connect to the new protocol. WPA2 supports WEP, TKIP, and AES[2]. WPA2 has been a successful wireless security protocol since its induction – until now.

Hackers will spend any amount of time to try and exploit a protocol to gain sensitive information. An article written in 2017 by Dan Goodin talks about a serious weakness in the WPA2 protocol called key reinstallation attacks (KRACK). Goodin gives brief description of the attack in the article:

> "Researchers have disclosed a serious weakness in the WPA2 protocol that allows attackers within range of vulnerable devices or access point to intercept passwords, e-

[2] Wired Equivalency Protocol, Temporal Key Infrastructure Protocol, and Advanced Encryption Standard are encryption protocols that work together with WPA/WPA2

WWW.INFOSECWRITERS.COM

> mails, and other data presumed to be encrypted, and in some cases, to inject ransomware or other malicious content into a website a client is visiting."

But, how exactly does it work? KRACK will force the device into reinstalling an all-zero encryption key instead of the real key, and the attacker can use other software to force the destination site to downgrade an HTTPS connection to HTTP, and thus be able to see the information in the packets.

Another weakness of WPA2 is in the WPA2 enterprise protocol suite. The enterprise is, of course, geared towards an enterprise wireless network. The main issue at hand lies with the 802.1x[3] authentication of the wireless network. In 802.1x, the AP acts as the supplicant to an authentication server (usually a RADIUS[4] server), and the authentication server allows the user on to the network based on its backend configuration. When this is not configured correctly it serves as a weakness and allows an evil twin scenario. The reason this is detrimental is because the supplicant will have already sent credentials to the evil twin for authentication, and the hacker now has user credentials. Even though this is not a direct weakness of WPA2, the fact that the protocol relies on a third party for authentication proves a weakness. Alberto Bartoli, et al., mention a *secure by default design* in their article, "configuration should not require specific technical understanding and it should require only the insertion of a few short pieces of textual information." While WPA2 has had its run of being the dominant and stable wireless protocol, the weaknesses and exploits have led the Wi-Fi alliance to focus on enhancing wireless security even further, addressing all concerns and leaning towards a *secure by default* design – WPA3.

WWW.INFOSECWRITERS.COM

[3] 802.1x is an industry standard port-based authentication protocol where users are authenticated before being granted access on the network

[4] Remote Authentication Dial-in User Service

WPA3 was announced by the Wi-Fi- Alliance in 2018 as being the next security standard. As with many other introductions of new protocols, newly released devices would still need to support older technologies while WPA3 is still in its beta release. Companies that sell wireless products such as Cisco, Ruckus, and Aruba are in the process of implementing WPA3 capable chips in their devices and testing the capabilities. But what enhancements have been applied to WPA3 from its predecessor WPA2?

Like its predecessors WPA3 also has two suites, personal and enterprise, and there are fundamental changes on how the new renditions of each operate. WPA3-personal is, of course, geared towards home and personal Wi-Fi and utilizes a new technology called Simultaneous Authentication of Equals (SAE) that will replace the use of a PSK. But how exactly does SAE work?

The way that SAE works is by both devices (AP and end device) proving to each other that they have a key. A PSK is used as the seed to produce a master key (PMK) which will then be shared between the two devices. Once this has been done, the requesting device will then be allowed on the network. During this whole process it is encrypted from the beginning, so once the device sends a beacon join request it is encrypted.

The Wi-Fi Alliance organization has released a document on WPA3-personal security considerations and provides a good example on the increased benefit of WPA3 security:

> "To illustrate the benefits that WPA3-Personal affords, consider a password selected randomly from 5,000 possible passwords. The attacker knows this but does not know which password was randomly chosen. With WPA2-Personal an attacker could determine the password through an off-line dictionary attack with a probability of success of 1.

WWW.INFOSECWRITERS.COM

> With WPA3-personal, the attacker must launch repeated active attacks, guessing a different password each time. The probability of success of the WPA3-Personal attack would only reach 0.5 after 2,500 active attacks. It should be possible to detect such an attack on WPA3-Personal long before the probability of success becomes high."

Detecting an attack is highly pertinent and many actions can be taken once an attack has been identified such as password expiration. The AP would temporarily deactivate the password thus preventing the attacker from progressing any further. Also, when users initially connect to the WPA3 device, before entering a password, the communication between the two devices will be encrypted, thus making it harder for attackers to identify devices.

With IoT on the rise, connecting these devices to the network can be a pain because most of them do not have screens. The Wi-Fi Alliance has rolled out Wi-Fi certified Easy Connect, and this will be utilized to secure the initialization and configuration of IoT devices and allow them to connect to a WPA3 secured network. The website hosted by howtogeek mentions that a new feature will be used for screenless IoT devices, "WPA3 includes a feature that promises to "simplify" the process of configuring security for devices that have limited or no display interface." This will prove to make it easier for end users to securely connect their devices to their networks.

WPA3-enterprise will be getting an overhaul of minimum-security standards such as the use of 192-bit security mode that will provide key derivation and confirmation using a 384-bit HMAC with SHA384 and AES-256 will be used for authentication. With enterprise being geared towards larger corporations, user authentication will still rely on the backend protocol 802.1X and a RADIUS server.

WWW.INFOSECWRITERS.COM

WPA3 has been accepted as the next step towards increasing wireless security both in personal and enterprise networks. Hackers will constantly work to reveal vulnerabilities in emerging technologies, and WPA2 had a lengthy life span. The decision to migrate to WPA3 is for the best interest of the users, and with the growing numbers of wireless devices and security becoming more of a concern, the Wi-Fi Alliance has made the right decision on the move to WPA3.

WWW.INFOSECWRITERS.COM

References

Bartoli, Alberto, et al. “Enterprise Wi-Fi.” *Communications of the ACM*, vol. 62, no. 5, 2019, pp. 33–35., doi:10.1145/3319912. *

Goodin, Dan. *Serious Flaw in WPA2 Protocol Lets Attackers Intercept Passwords and Much More*. ARS Technica, 16 Oct. 2017, arstechnica.com/information-technology/2017/10/severe-flaw-in-wpa2-protocol-leaves-wi-fi-traffic-open-to-eavesdropping/.

Hoffman, Chris. “What Is WPA3, and When Will I Get It On My Wi-Fi?” *How*, How-To Geek, 21 Oct. 2018, www.howtogeek.com/339765/what-is-wpa3-and-when-will-i-get-it-on-my-wi-fi/.

Lueth, Knud Lasse. “State of the IoT 2018: Number of IoT Devices Now at 7B – Market Accelerating.” *IoT Analytics*, 8 Aug. 2018, iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/. *

WPA3 Security Considerations. *WPA3 Security Considerations*, Wi-Fi Alliance, 2019. https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Security_Considerations_201911.pdf

WWW.INFOSECWRITERS.COM

WWW.INFOSECWRITERS.COM