NATIONAL SECURITY AGENCY
CYBERSECURITY REPORT

WPA3 WILL ENHANCE WI-FI SECURITY

A TECHNICAL REPORT FROM THE NETWORK DEVICE VULNERABILITY SOLUTIONS SECTION

U/OO/173671-18 PP-18-0470

June 2018

DOCUMENT CHANGE HISTORY

25 May 2018	1	Original version

DISCLAIMER OF WARRENTIES AND ENDORSEMENT

The information and opinions contained in this document are provided “as is” and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes.

WPA3 WILL ENHANCE WI-FI SECURITY

CONTACT INFORMATION

Client Requirements and Inquiries or General Cybersecurity Inquiries

CYBERSECURITY REQUIREMENTS CENTER (CRC)

410-854-4200

Cybersecurity_Requests@nsa.gov

Table of Contents

1. INTRODUCTION

On January 8th 2018, the Wi-Fi alliance announced new enhancements to Wi-Fi Protected Access II (WPA2) security specification and a new WPA3 security specification. Enhancements to WPA2 will include improvements in authentication, encryption, and configuration requirements. WPA3 will build on the WPA2 enhancements and will offer enhanced protection for Wi-Fi networks that use password-based authentication, improved privacy on open networks, mitigations against denial-of-service attacks, and will deliver stronger cryptographic strengths that comply with Commercial National Security Algorithm (CNSA) requirements. WPA3 will also introduce a mechanism to provision Internet of Things (IoT) devices without or a limited user interface into the trusted network. WPA2 enhancements will be implemented before the end of 2018. WPA3 testing started in March 2018 and compliant products are expected to start appearing in commercial devices later in 2018. Over the next few years it is expected that WPA3 capable Access Points will be backward compatible with WPA2 client devices until WPA2 is phased out. The combination of WPA2 Enhancements and the introduction of WPA3 will improve Wi-Fi security.

2. WPA2 ENHANCED FEATURES

The WPA2 enhancements will introduce new requirements for protection from traffic-based Denial of Service (DoS) attacks, vulnerabilities introduced by bad security implementations and interoperability problems. The WPA2 enhancements include mandatory use of Protected Management Frames (PMF), more stringent validation of vendor security implementations, and improved consistency in network security configuration. These enhancements are important, as it will take a number of years for WPA3 to become commonplace.

IEEE 802.11w, the standard that describes PMF, was ratified in 2009 and has been broadly adopted in Wi-Fi devices but will be mandatory in WPA2 enhanced. Management frames are used for initiating and terminating Wi-Fi connections. Without PMF, management frames are transmitted unencrypted and their integrity is not verified. PMF ensures integrity of network management traffic. It provides protection against eavesdropping, replay and forging of management action frames. This protects against traffic-based DoS attacks that use forged deauthentication/disassociation frames to kick clients from a network and force them to authenticate again, a tactic which is used at the initial stage of some wireless attacks.

The 2018 update to WPA2 will require enhanced validation of vendor security implementations to reduce the potential for vulnerabilities due to network misconfiguration. Many wireless vulnerabilities are the result of poor implementation or misconfiguration, with misconfiguration being the most common cause. WPA2 enhancements will require additional tests on Wi-Fi certified devices to ensure implementation of best practices and the products yield expected behaviors.

The last WPA2 enhancement strives for better consistency in network security configuration by defining a set of secure cipher suites. The cipher suites ensure that all security components are of similar cryptographic strength. This will prevent an attacker from exploiting a configuration weakness.

3. NEW FEATURES INTRODUCED WITH WPA3

WPA3 will introduce several Wi-Fi security enhancements, including stronger cryptographic suites that align with CNSA requirements. WPA3 will also allow for individualized user encryption on public (Open) networks, and defend against dictionary/brute force password attacks on networks that rely on password based authentication. Along with WPA3, the Wi-Fi Alliance is also introducing a new on-boarding method intended to provision IoT “headless devices”, devices that have a limited or no user interface, in a simple and secure manner.

Wi-Fi devices have utilized AES with 128 bit keys for data protection for some time. Refer to Table 1 in Appendix A for a historical comparison of wireless security standards. WPA3 will mandate 256-bit encryption and use of CNSA approved cipher suites, including a set of compliant TLS cipher suites for EAP-TLS. Overall this would provide 192-bit security for Wi-Fi networks. Due to the number of available configuration options for WPA-Enterprise (e.g. key exchange, key strength, authentication and encryption), a clear set of requirements will improve the security of Wi-Fi deployments and ensure CNSA compliance.

WPA3 will introduce Opportunistic Wireless Encryption (OWE), which will replace unencrypted Open networks. OWE will provide individualized data encryption to users connecting to public open networks to protect against eavesdropping. On Open networks, an attacker connected to the network could read or even modify others’ traffic. HTTPS websites, to an extent, provide protection against eavesdropping on an Open network. OWE uses an unauthenticated Diffie-Hellman key exchange during association, resulting in a Pairwise Master Key (PMK) used to derive the session keys. There is no provisioning required and the encryption process is entirely transparent to users. The users would see and join the Wi-Fi network as they would an Open network. OWE is a big improvement over current open wireless networks.

In WPA3, a more resilient password-based authentication mechanism will replace Pre-Shared Key (PSK) mode. The new authentication method, Simultaneous Authentication of Equals (SAE), will protect against both active and passive brute force attacks that try to recover the password or the derived cryptographic keys even when weak passwords are chosen. WPA2-PSK is susceptible to these types of attacks. SAE will also limit the number of guesses an attacker can make. Currently they can guess at the rate of 400,000 possible passwords per second. The user experience will not change with SAE, as users will enter a password as they would with WPA2-PSK, but will be afforded additional security.

Finally, along with WPA3 the Wi-Fi Alliance will launch the Device Provisioning Protocol (DPP). DPP will work alongside WPA3 similarly to how WPS worked alongside WPA2. DPP will introduce a simple way to onboard “headless” IoT devices into the network, which will make provisioning of these devices more manageable and user friendly. Two devices will be involved with this process, the configurator and the enrollee. The configurator is typically a smart phone or tablet that is already part of the trusted network and can provision new devices. The enrollee will be authenticated and provisioned into the network through an initial bootstrapping process. The bootstrapping process is done through the following methods: scanning a QR code, negotiation of a trusted public key using a passphrase/code, NFC, or Bluetooth. DPP will allow for mutual authentication.

4. CONCLUSION

While WPA3 is expected to emerge at the end of 2018, full adoption will take a few years. According to the Wi-Fi Alliance, Wi-Fi Certified WPA3 capable devices will remain backward compatible with WPA2 for some time. The security enhancements in WPA2 will improve overall Wi-Fi security by addressing some of the immediate concerns regarding Wi-Fi security, resilience against DoS attacks, validation of Wi-Fi security implementations and consistency in security configurations. When WPA3 is adopted, the security improvements will allow Wi-Fi deployments requiring high security to comply with CNSA requirements as well as provide additional security to home and small business Wi-Fi users.

5. APPENDIX A – HISTORICAL COMPARISON OF ENCRYPTION AND AUTHENTICATION TYPES USED IN WI-FI

Standard	WEP	WPA	WPA2	WPA3
Release	1997	2003	2004	2018
Encryption	RC4	TKIP with RC4	AES-CCMP	AES-CCMP & AES-GCMP
Key Size(s)	64-bit and 128	128-bit	128-bit	128 and 256 bit
Cipher Type	Stream	Stream	Block	Block
Authentication	Open System & Shared Key	Pre-Shared Key (PSK) & 802.1x with EAP variant	Pre-Shared Key (PSK) & 802.1x with EAP variant	Simultaneous Authentication of Equals (SAE) & 802.1x with EAP variant