WPA3™ Security Considerations Overview

April 2019

Introduction

WPA3™-Personal provides next generation security for private Wi-Fi® networks based on a simple password credential. It raises the bar on security but does not completely prevent an external attack on a Wi-Fi network. This document covers several areas that deserve special mention, as well as recommended implementation considerations.

WPA3-Personal – Summary of Recommendations

- Passwords used with SAE must be extremely difficult to guess, and SAE implementations should limit authentication attempts when an implementation identifies an active attack. (see Password Strength)
- SAE AP implementations should handle SAE operations on non-privileged processing queues which, if overwhelmed, will not result in a failure of the entire BSS through CPU resource consumption. (see Denial of Service Protection)
- SAE implementations must use only suitable Diffie-Hellman groups. (see Suitable Diffie-Hellman Groups)
- SAE implementations should set the security parameter, k, to a value of at least forty (40) as per the recommendation in RFC 7664 “Dragonfly Key Exchange” for all ECC groups. (see Suitable Diffie-Hellman Groups)

SAE implementations should only offer a Diffie-Hellman group whose strength estimate is greater than or equal to the encryption cipher being offered. (see

- Diffie-Hellman Group Downgrade)
- SAE implementations must disable the use of MODP groups 22, 23, and 24 to prevent side-channel timing attacks. (see MODP Group Timing Side-Channels)
- SAE implementations must avoid differences in code execution that allow side channel information collection through the cache. (see Cache-Based Elliptic Curve Side-Channels)
- If WPA3-Personal Transition Mode is not suitable for a particular deployment, SAE and WPA2™-PSK should be deployed on separate networks (different SSIDs) with separate passwords. (see WPA3-Personal Transition Mode)

EAP-pwd – Summary of Recommendations

While EAP-pwd is not currently part of WPA3, this document covers several areas that deserve special mention, as well as recommended implementation considerations for those who choose to implement it.

- EAP-pwd implementations must use only suitable Diffie-Hellman groups. (see Suitable Diffie-Hellman Groups)
- EAP-pwd implementations should set the security parameter, k, to a value of at least forty (40) as per the recommendation in RFC 7664 “Dragonfly Key Exchange” for all ECC groups. (see Suitable Diffie-Hellman Groups)
- EAP-pwd implementations must disable the use of MODP groups 22, 23, and 24 to prevent side-channel timing attacks. (see MODP Group Timing Side-Channels)
- EAP-pwd implementations must avoid differences in code execution that allow side channel information collection through the cache. (see Cache-Based Elliptic Curve Side-Channels)

Security Considerations Detail

Password Strength

Recommendation:

Passwords used with SAE must be extremely difficult to guess, and SAE implementations should limit authentication attempts when an implementation identifies an active attack.

Summary:

WPA3-Personal replaces WPA2 Pre-Shared Key (WPA2-PSK) with Simultaneous Authentication of Equals (SAE). Unlike WPA2-PSK, SAE is resistant to off-line dictionary attacks. The only way for an attacker to learn a password is through repeated active attacks, each of which tests whether a single guess of the password is correct or not. Repeated authentication failures may indicate that such an active attack is underway, allowing implementations to respond appropriately, e.g. throttling authentication attempts and/or issuing alerts (e.g. SNMP trap, log message, etc.).

SAE resistance to off-line dictionary means that the onus for password security is not placed on users (as it is with WPA2-PSK). The requirement for exceedingly long, random passwords with mixed-case characters and special characters is no longer a valid requirement with SAE. This does not mean that passwords used with SAE can be weak or easily guessable (e.g. one from the list of "100 most popular Internet passwords") because an active attack is still possible. Passwords used with SAE must be extremely difficult to guess and the difficulty in guessing a password directly correlates to the security that SAE offers.

To illustrate the benefits that SAE affords without overselling it, 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-PSK an attacker could determine the password in a matter of seconds through an off-line dictionary attack with a probability of success of 1. With SAE, the attacker must launch repeated active attacks, guessing a different password each time. The probability of success of the SAE attack would only reach 0.5 after 2,500 active attacks. It should be possible to detect such an attack on SAE long before the probability of success becomes high.

It is recommended that implementations of SAE limit authentication attempts for a particular password (either identified with an SAE Password Identifier or not) when an active attack is identified. Implementations may temporarily disable a password after a series of unsuccessful authentication attempts. The determination of whether an attack is underway is implementation dependent. Note that the source MAC address used with failed authentication attempts is irrelevant and should not factor into the decision to disable or limit authentication for a particular password because an attacker can easily change the MAC address between attempts.

Denial of Service Protection

Recommendation:

SAE implementations should handle SAE operations on non-privileged processing queues which, even if overwhelmed, will not result in a failure of the entire BSS through CPU resource consumption.

Summary:

An access point (AP) will do a significant amount of cryptographic work upon receipt of the first message in an SAE handshake. This opens the opportunity to flood the AP with bogus messages from fake MAC addresses resulting in a denial of service attack.

To address this attack, SAE defines an *anti-clogging cookie* response in which the AP statelessly generates a string that is bound to the sender of the message when the AP detects it is under a denial of service attack. An AP may consider itself under a denial of service attack when the number of nascent connections, those in which the first message has been received but not the third message, reaches a threshold. The AP, when in a "cookie demanding" state, will not process the first SAE message unless that message contains a valid cookie bound to the MAC address of the sender.

This technique works against rudimentary and simple packet spraying attacks because the attacker is just sending random packets and not processing responses. Unfortunately, this technique does not work if the attacker chooses to receive the AP's cookie request and respond with the cookie from the same MAC address. Therefore, SAE does not afford adequate protection against more sophisticated denial of service attacks. SAE

implementations should handle SAE operations on non-privileged processing queues which, even if overwhelmed, will not result in a failure of the entire BSS through CPU resource consumption.

Suitable Diffie-Hellman Groups

Recommendation:

SAE and EAP-pwd implementations must use only suitable Diffie-Hellman groups.

SAE and EAP-pwd implementations should set the security parameter, k, to a value of at least forty (40) as per the recommendation in RFC 7664 “Dragonfly Key Exchange” for all ECC groups.

Summary:

SAE and EAP-pwd perform public key cryptography using named Diffie-Hellman groups. The IKEv1 (RFC 2409) group registry maintained by IANA maps the group’s complete domain parameter set to a reference number. Not all registered groups are suitable for use with SAE or EAP-pwd.

The rules used to evaluate the suitability of groups are:

1. No binary elliptic curve (EC2N) groups
2. No groups defined over a prime field (MODP) with a prime less than 3072 bits
3. No groups defined over a prime field (MODP) with a small sub-group of prime order
4. No elliptic curve group with a prime less than 256-bits

The following table indicates the suitability of each group in the registry. Groups marked “Unsuitable” must not be used with SAE or EAP-pwd.

Table 1: Diffie-Hellman Group Suitability

Group Number	Description	Suitability
1	768-bit MODP group	Unsuitable
2	1024-bit MODP group	Unsuitable
3	EC2N group on GP[2^155]	Unsuitable
4	EC2N group on GP[2^185]	Unsuitable
5	1536-bit MODP group	Unsuitable
6	Random EC2N group over GF[2^163]	Unsuitable
7	Koblitz EC2N group over GF[2^163]	Unsuitable
8	Random EC2N group over GF[2^163]	Unsuitable
9	Koblitz EC2N group over GF[2^163]	Unsuitable
10	Random EC2N group over GF[2^163]	Unsuitable
11	Koblitz EC2N group over GF[2^163]	Unsuitable
12	Random EC2N group over GF[2^163]	Unsuitable
13	Koblitz EC2N group over GF[2^163]	Unsuitable
14	2048-bit MODP group	Unsuitable
15	3072-bit MODP group	Suitable
16	4096-bit MODP group	Suitable
17	6144-bit MODP group	Suitable
18	8192-bit MODP group	Suitable
19	256-bit random ECP group (NIST)	Suitable (Mandatory)
20	384-bit random ECP group (NIST)	Suitable
21	512-bit random ECP group (NIST)	Suitable
22	1024-bit MODP group w/160-bit order	Unsuitable
23	2048-bit MODP group w/224-bit order	Unsuitable

Group Number	Description	Suitability
24	2048-bit MODP group w/256-bit order	Unsuitable
25	192-bit Random ECP group (NIST)	Unsuitable
26	224-bit Random ECP group (NIST)	Unsuitable
27	224-bit Random ECP group (Brainpool)	Unsuitable
28	256-bit Random ECP group (Brainpool)	Suitable
29	384-bit Random ECP group (Brainpool)	Suitable
30	512-bit Random ECP group (Brainpool)	Suitable

Diffie-Hellman Group Downgrade

Recommendation:

SAE implementations should only offer a Diffie-Hellman group whose strength estimate is greater than or equal to the strength estimate of the encryption cipher being offered.

Summary:

In SAE, the initiator chooses the group to use and includes the group number in the first message. The responder accepts the group or responds with a message containing an error code indicating group rejection if the responder does not want to use the group. If the group is rejected, the initiator chooses another group and tries again.

This technique opens the protocol to a downgrade attack where an attacker impersonates the AP and responds with a rejection of a stronger group until the STA offers a weak group and then lets the protocol proceed with the real AP.

SAE does not inherently protect against Diffie-Hellman Group Downgrade attacks, however they can be mitigated by not allowing weak groups and only allowing rejections to offer “upgraded” groups.

Suitable Diffie-Hellman groups for use with SAE all generate a key whose strength is appropriate for the default and mandatory-to-implement cipher, AES-CCM-128. While AES-CCM-256 and AES-GCM-256 ciphers may be used with SAE, SAE uses SHA256 for key derivation thereby mitigating, to some extent, the strength benefits afforded by different groups such as group 20 or group 21. SAE implementations should only offer a Diffie-Hellman group whose strength estimate is greater than or equal to the strength estimate of the encryption cipher being offered (see SP 800-57, Part 1 Rev 4, January 2016).

MODP Group Timing Side-Channels

Recommendation:

SAE and EAP-pwd implementations must disable the use of MODP groups 22, 23, and 24 to prevent side-channel timing attacks.

Summary:

The password element generation algorithm for MODP groups is affected by timing side-channels, and the obtained information can later be used to recover the password. MODP groups, 22, 23, and 24 have a small sub-group and are known to be weak; refer to "Measuring small sub-group attacks against Diffie-Hellman" by Valeta et al, 2017.

See Table 1: Diffie-Hellman Group Suitability in this document for group suitability with SAE and EAP-pwd.

Cache-Based Elliptic Curve Side-Channels

Recommendation:

SAE and EAP-pwd implementations must avoid differences in code execution that allow side channel information collection through the cache.

Two options exist:

1. Implement SAE and EAP-pwd in such a way to use constant time operations that use same memory access pattern regardless of the values derived from the password.
2. Reduce the visibility of side channel information, e.g. by preventing sharing of cache lines between processes. This may not be practical with existing hardware due to the potential performance drop.

Summary:

This vulnerability requires monitoring of cache access patterns on a compromised machine, one running the attacker's software. The obtained information can later be used to recover the password. The goal is to learn if the Quadratic Residue (QR) test in the first iteration of the hash to curve algorithm succeeded or not. This information can be used in the offline password partitioning attack to recover the target's password. The implementation of the hash to curve algorithm for ECC groups does include mitigations against side channel attacks. Those mitigations include performing extra dummy iterations on random data and blinding of the underlying cryptographic calculation of the quadratic residue test. Preventing the installation of malicious software may be an effective additional mitigation approach for some device categories.

WPA3-Personal Transition Mode

Recommendation:

If WPA3-Personal Transition Mode is not suitable for a particular deployment, SAE and WPA2-PSK should be deployed on separate networks (different SSIDs) with separate passwords.

Summary:

SAE is a new Wi-Fi authentication protocol, and it is not backwards compatible with any previous authentication protocol. Mandating that only SAE is used on a BSS would require every STA to support SAE in order to join the network. To prevent such a deployment "flag day", Wi-Fi Alliance defined WPA3-Personal Transition Mode (defined as WPA3-SAE Transition Mode in the Wi-Fi Alliance WPA3 Specification) to allow for gradual migration to an SAE network while maintaining interoperability with WPA2-PSK devices and without disruption to users.

This transition mode simply supports both SAE and WPA2-PSK on the same BSS (with the same SSID). WPA3-SAE Transition Mode uses the same password with both authentication protocols. This was done for ease-of-use and because it is not possible to make valid assumptions about user experience across diverse device types or the security awareness of users that would ensure a smooth roll-out. A trade-off is that the common password of a WPA3-SAE Transition Mode network can be determined by attacking WPA2-PSK using a simple offline dictionary attack. The WPA2-PSK attack could be performed passively on a legacy STA that only supports WPA2-PSK, or a more complex active downgrade attack could be performed on a STA that supports SAE.

The passive attack on a legacy WPA2-PSK only STA is the same as exists with legacy WPA2-PSK only networks. The active attack on an SAE STA is complex and gains the attacker little because of the possibility to run the simpler passive attack on legacy STAs. An attacker who determines the password can access the network simply by using WPA2-PSK, irrespective of SAE. In addition, even after this attack is successful and the attacker determines the password, the STAs that connect with SAE will still benefit from the forward-secrecy that SAE affords—that is, the traffic encryption keys will still remain unknown even if the password is known. This is not an attack against SAE.

If WPA3-SAE Transition Mode is not suitable for a particular deployment, SAE and WPA2-PSK should be deployed on separate networks (different SSIDs) with separate passwords/passphrases. In such a deployment, client devices must be reconfigured to support the SAE network when they are upgraded to support and use SAE. The full benefits of SAE are only available when *not* operating in WPA3-SAE Transition Mode. Once SAE availability reaches a sufficient level amongst client devices, network owners should disable WPA3-SAE Transition Mode to achieve the full benefits of SAE.

About Wi-Fi Alliance®

www.wi-fi.org

Wi-Fi Alliance® is the worldwide network of companies that brings you Wi-Fi®. Members of our collaboration forum come together from across the Wi-Fi ecosystem with the shared vision to connect everyone and everything, everywhere, while providing the best possible user experience. Since 2000, Wi-Fi Alliance has completed more than 45,000 Wi-Fi certifications. The Wi-Fi CERTIFIED™ seal of approval designates products with proven interoperability, backward compatibility, and the highest industry-standard security protections in place. Today, Wi-Fi carries more than half of the internet's traffic in an ever-expanding variety of applications. Wi-Fi Alliance continues to drive the adoption and evolution of Wi-Fi, which billions of people rely on every day.