PROJECT WYVERN: SECURITY AUDIT ON WPA3 SAE HANDSHAKE

(A Compressive Security Analysis)

Sydney A. Barreto

Master of Computer Application
Information Security Management Systems
Jain (Deemed-to-be University) Bangalore, India

Abstract: This paper features the latest Wi-Fi security standard WPA3 certification that provides several advantages over its predecessor WPA2. The focus here is the discovery of flaws on the latest WPA3 Handshake mechanism Simultaneous Authentication of Equals (SAE) handshake aka Dragonfly. This concept behind the vulnerabilities is as similar to password partitioning attacks that resemble a common dictionary attack that abuses the side-channel leaks, group negotiation and denial of service attacks. Here the focus is on the mechanism of both these methods of attacks and how to mitigate these attacks using backwards compatible methodologies.

I. Introduction

With the release of the new WPA3 certification by the Wi-Fi Alliance to better secure the Wi-Fi network came the discovery of new form of attacks that lead to the hold back of release. The new features added to WPA3 were not made public as it was for WPA2. This led to undiscovered flaws and missing critical functionalities. There is no clear understanding on how secure WPA3 is in this current situation. Jean Lancrenon and Marjan Škrobot in 2015 proves on how secure dragonfly is well equipped to handle the shortcoming of WPA2 while on the other hand Rene Struik. in 2013 updated in 2019 calls for review on the flaws of dragonfly related to password management policies. These issues are what question the security of WPA3.

WPA3 is certification and not a standard. It does not create any new security protocols but instead mandates existing protocols to all devices that can support the requirements. This means that supported devices can be WPA3 certified with the implementations of certain protocols in an interoperable manner. Even though WPA3 performs the best practices when it comes to security it is always necessary for the functionality and choice of protocols be open to the public to better increase the security.

In this paper we perform a security analysis in respect to the flaws of WPA3's Simultaneous Authentication of Equals (SAE) handshake. SAE was created to prevent dictionary attacks and shortcoming of WPA2 security. Analyzing the proofs and specification of WPA3 design to verify the side channel vulnerabilities in password encoding methods, group negotiation and denial of service attacks. At the same time find out ways to mitigate these vulnerabilities.

II. A Complete Picture of WPA3 Technology

WPA3 certificate was constructed for two different networks. The first one being the home network, this is where the authentication of the device takes place using a pre-shared password. The second one is enterprise networks. Here a higher level of device authentication is utilized such as a smartcard or certificates. The difference between both tyes is with the use of SAE in home networks and WP#-Enterprise in enterprise networks.

WPA3-Enterprise uses existing handshakes of cipher size of minimum 192 bits. It does not specify the length of the session key or the hash functions in use after authentication. WPA3-SAE home network uses Password Authenticated Key Exchange (PAKE) i.e. password-based authentication. Here the SAE handshake is more resistant to offline based dictionary attacks. The output result in communication is a Pairwise Master Key (PMK), which is a 4-way handshake and is not vulnerable to dictionary attacks because the complexity of the password PMK generated by SAE handshake have a higher entropy. In both networks Management Frame Protection (MFP) is mandatory. To understand the workings of how SAE handshake works then refer to the Wi-Fi Alliance. 2018 publication of WPA3 Specification Version 1.0. Retrieved 6 April 2019. This paper will be focusing on some of the attacks possible on breaking of the SAE handshake.

III. Breaking SAE's SIDE-CHANNEL

This part address on how side-channel defences of SAE overhead is being abused by using a denial of service attacks. This is achieved by bypassing the SAE's anti-clogging mechanism that prevents DoS attacks from happening.

3.1 Clogging Bypass Attack (Proof of Concept)

This proof of concept is where the attacker injects commit frames using spoofed MAC addresses, and reflects any cookie or anti clogging tokens it receives. Using some C programing code for it's performance on top of aircrack-ng, the tool can forge commit frames using any elliptic curve used by SAE. It is mandatory that the attacker accepts all the frames from the spoofed MAC addresses else the access point will loop the replies 8 times making it difficult for the attacker to inject commit frames to overload the target. Fortunately, with the instructions set by Mathy Vanhoef and Frank Piessens. 2014. Advanced Wi-Fi attacks using commodity hardware where the attacker replies to the virtual Wi-Fi interface Atheros chips force ACK is possible. This is the general idea of how the attack works. The clogging attacks can be enhanced by understanding how the access point generates the anti-clogging tokens. Note that all 802.11 standard recommends to generate their anti-clogging tokens by computing the hash secret values and the MAC address of the sender. Initially 802.11 standards keep a record of the number of handshakes that are open and close. This implies when the number of handshakes is above the trash hold, the secret value is not updated. That means that recycling old anti-clogging tokens is possible.

3.2 Countermeasures

To mitigate this form of attack, a low priority thread must be created and on it derivation of the password elements must be executing. This means that legitimate clients will not be able to connect during this attack but ensure that the access point is must more secure and that disruption of other services is eliminated. Also, MODP groups can be eliminated to prevent DoS attacks. Sam Scott, Nick Sullivan, and Christopher A. Wood. 2019. Hashing to Elliptic Curves. Internet-Draft draft-irtf-cfrg-hash-to-curve-03 recommends to use a stronger hashing algorithm.

3.3 Source Code: Side channel protected quadratic residue test (Sample)

```
static int is_quadratic_residue_blind(
struct sae_data *sae, const u8 *prime, size_t bits,
const struct crypto_bignum *qr,
const struct crypto_bignum *qnr,
const struct crypto_bignum *y_sqr)
{ struct crypto_bignum *r, *num;
int r_odd, check, res = -1;
/* Use the blinding technique to mask y_sqr while determining
* whether it is a quadratic residue modulo p to avoid leaking
* timing information while determining the Legendre symbol.
* v = y_sqr
* r = a random number between 1 and p-1, inclusive
* num = (v * r * r) modulo p
*/
r = get_rand_1_to_p_1(prime, sae->tmp->prime_len, bits, &r_odd);
if (r_odd) {
/* num = (num * qr) module p
* LGR(num, p) = 1 ==> quadratic residue */
if (crypto_bignum_mulmod(num, qr, sae->tmp->prime, num) < 0)
goto fail;
check = 1; } else {
/* num = (num * qnr) module p
* LGR(num, p) = -1 ==> quadratic residue */
if (crypto_bignum_mulmod(num, qnr, sae->tmp->prime, num) < 0)
goto fail;
check = -1; }
res = crypto_bignum_legendre(num, sae->tmp->prime);
res = re
```

IV. SAE’s Group Negotiating Attack

SAE handshake can run using various ECP or MODP mods. The “group description” part of IANA. 2018 gives a proper overview of all groups. 802.11 standard prioritize groups in a use-configuration order as per the IEEE Std 802.11. 2012. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. This specification provides the necessary standards and flexibility for negotiations but the mechanism that negotiates the choice of groups and curves during the SAE handshake is vulnerable to attack.

4.1 SAE Group Negotiation

When a client connects to the access point it chooses the group in the commit frame, along with a valid scaler s_i and an element E_i This continues to take place until the device select a curve that the access point supports. During this process there is no way for the access point to detect any form of interference. At this time the attacker can simply forge a commit frame that indicates the access point does not support the desire curve in the selected group.

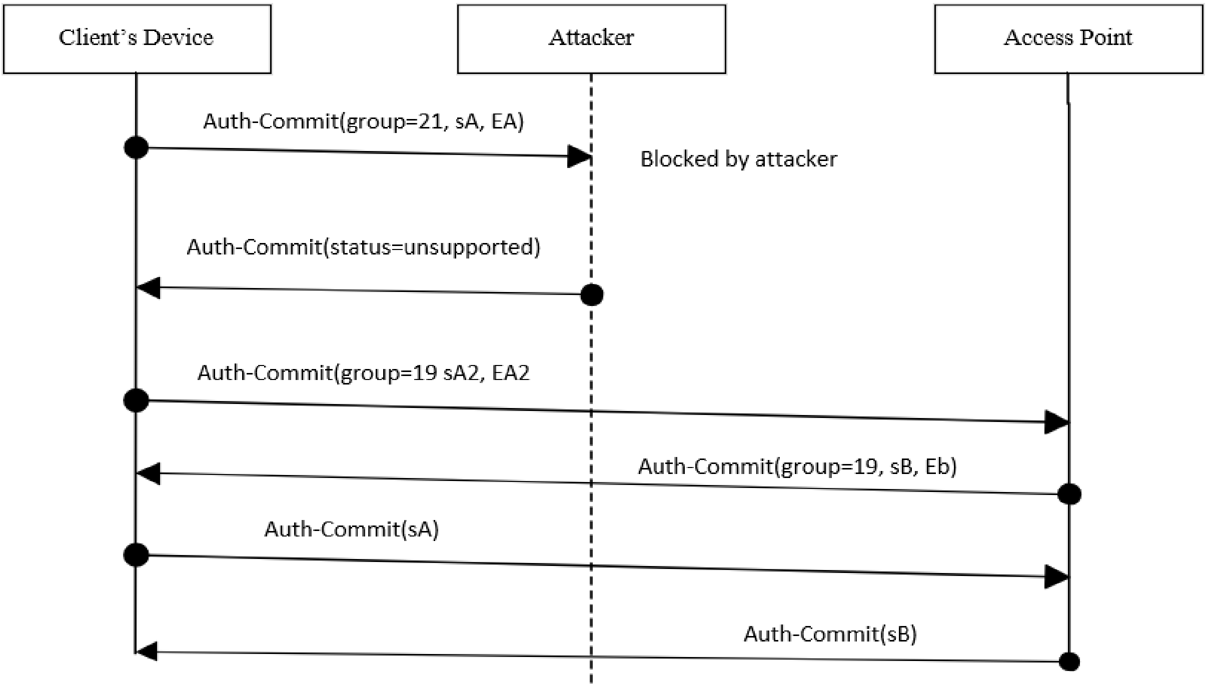
Client's Device
Attacker
Access Point
Auth-Commit(group=21, sA, EA)
Blocked by attacker
Auth-Commit(status=unsupported)
Auth-Commit(group=19 sA2, EA2
Auth-Commit(group=19, sB, Eb)
Auth-Commit(sA)
Auth-Commit(sB)

Fig 1 Downgrade attack against SAE's group selection. This is a form of man in the middle attack

Figure 1 illustrates the forces in downgrade using man in the middle type attack. In this scenario the client first constructs a commit frame of group 21. The attacker sitting in the middle of this exchange blocks the request from arriving to the access point (Stage 1). This is done by jamming the frame as discussed in Mathy Vanhoef and Frank Piessens. 2014. Advanced Wi-Fi attacks using commodity hardware or by forging channel-switch-announcements as mentioned in Mathy Vanhoef, Nehru Bhandaru, Thomas Derham, Ido Ouzieli, and Frank Piessens. 2018. Operating Channel Validation: Preventing Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks. In WiSec. The attacker then creates a forged commit frame that acts as a reply to the client's device informing the clients that the selected curve in the group are not supported. The Client in response will choose the second preferred frame which in the figure above is group 19. Note that this entire exchange is not cryptographically validated meaning that this attack was never detected.

4.2 Data and Sources of Data

To mitigate such an attack which is also vulnerable to dictionary attack, the clients should have a separate table containing a list of all supported groups in access points for a secure WPA-SAE. This is to be done after a successful connection to the access point allowing a faster and more secure handshake next time it tries to connect. This form of security is similar to SSH protocol and Strict-Transport-Security Header of HTTPS.

Another form of defense is also possible but that would require some form of modification to the clients or access points. The modification will allow both parties to create a separate network to hand over the keys or handshake negotiations. In principal keeping a list of all supported groups stored in the client's system is inefficient. In order to negate this the 4-way handshake should also include a bitmap of all groups. This will prevent any form of downgrade attacks by aborting the connections and trying again.

IV. Conclusion

With the possibilities of attacks on a newly introduced certification, WPA3 is not secure as it clams to be and should not be deployed prior to the patching of all discovered vulnerabilities. It is advisory that the WI-FI Alliance continue to create WPA3 in an open manner. A simple change in the algorithm and utilization of other service could simply mitigate the attacks mentioned in this paper.

References

[1] Jintai Ding, Saed Alsayigh, Jean Lancrenon, RV Saraswathy, and Michael Snook. 2017. Provably secure password authenticated key exchange based on RLWE for the post-quantum world. In Crypto Track at the RSA Conference. Springer, 183–204.

[2] Trevor Perrin. 2013. [TLS] Question regarding CFRG process. Retrieved 29 October 2018 from https://www.ietf.org/mail-archive/web/tls/current/msg10962. html.

[3] Trevor Perrin. 2013. [TLS] Review of Dragonfly PAKE. Retrieved 9 September 2018 from https://www.ietf.org/mail-archive/web/tls/current/msg10922.html.

[4] Mathy Vanhoef, Nehru Bhandaru, Thomas Derham, Ido Ouzieli, and Frank Piessens. 2018. Operating Channel Validation: Preventing Multi-Channel Manin-the-Middle Attacks Against Protected Wi-Fi Networks. In WiSec.

[5] IEEE Std 802.11. 2012. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Spec

[6] Kevin M. Igoe. 2012. [Cfrg] Status of DragonFly. Retrieved 8 November 2018 from https://www.ietf.org/mail-archive/web/cfrg/current/msg03258.html.