DRAGONBLOOD

Analysing WPA3's Dragonfly Handshake

(Submitted by: **SAYAN DAS, CSE/15/61**)

INTRODUCTION:

In the latest and secured protocol of WiFi Technology i.e., ***WPA3***(Wi-Fi Protected Access 3) vulnerability has been detected. Secure passwords of WPA3 enabled devices can be recovered through this vulnerability & also the wifi network can be hacked. Security researchers Mathy Vanhoef and Eyal Ronen discovered the vulnerability in WPA3 protocol named as **'DRAGONBLOOD'**. This allows hackers to steal the WiFi password from WPA3 enabled WiFi Network. Not only this but allows attackers to steal chat messages, card details and so on.

Currently, all modern Wi-Fi networks use WPA2 to protect transmitted data. However, because WPA2 is more than 14 years old, the Wi-Fi Alliance recently announced the new and more secure WPA3 protocol. One of the main advantages of WPA3 is that, thanks to its underlying Dragonfly handshake, it's near impossible to crack the password of a network. Unfortunately, we found that even with WPA3, an attacker within range of a victim can still recover the password of the network. This allows the adversary to steal sensitive information such as credit cards, password, emails, and so on, when the victim uses no extra layer of protection such as HTTPS.

The Dragonfly handshake, which forms the core of WPA3, is also used on certain Wi-Fi networks that require a username and password for access control. That is, Dragonfly is also used in the EAP-pwd(Extensible Authentication Protocol-PAssword) protocol. Unfortunately, attacks against WPA3 also work against EAP-pwd, meaning an adversary can even recover a user's password when EAP-pwd is used. Serious bugs in most products that implement EAP-pwd are also being discovered. These allow an adversary to impersonate any user, and thereby access the Wi-Fi network, without knowing the user's password. Although EAP-pwd is

used fairly infrequently, this still poses serious risks for many users, and illustrates the risks of incorrectly implementing Dragonfly.

DRAGONFLY HANDSHAKE:

The dragonfly handshake which in the Wi-Fi standard is better known as theSimultaneous Authentication of Equals (SAE) handshake is a key exchange using discrete logarithm cryptography that is authenticated using a passwordor passphrase. It is resistant to active attack, passive attack, and offline dictionary attack. WPA3 has perfect forward secrecy (which WPA2 lacks), and protects from offline brute force attacks.

FLAWS IN WPA3:

The design flaws discovered can be divided in two categories:

- Downgrade Attacks
- Side-Channel Leaks

The discovered flaws can be abused to recover the password of the Wi-Fi network, launch resource consumption attacks, and force devices into using weaker security groups. All attacks are against home networks (i.e. WPA3-Personal), where one password is shared among all users.

Discovered vulnerabilities in WPA3 are listed below:

1. Downgrade Attack against WPA3-Transtition mode leading to dictionary attacks**:**-

   In this mode a Wi-Fi network supports the usage both WPA3 and WPA2 with an identical password. An adversary can create a rogue network and force clients that support WPA3 into connecting using WPA2. The captured partial WPA2 handshake can be used to recover the password of the network (using brute-force or dictionary attacks). No man-in-the-middle position is required to perform this attack.

2. Security group downgrade attack against WPA3's Dragonfly handshake:-

   The victim can be forced to use a weak security group. The device that initiates the handshake (typically the client) sends a commit frame that includes the security group it wishes to use. If the AP(Access Point) does not

support this group, it responds with a decline message, forcing the client to send a commit frame using another group. This process continues until a security group is found that is supported by both sides. An attacker can impersonate an AP and forge decline messages to force clients into choosing a weak security group.

3. Side Channel Attack: This attack works against WPA3's Dragonfly handshake. This is further divided into two types:

    - Cache-Based Side-Channel Attack
    - Timing-based Side-Channel Attack

4. Resource consumption attack (i.e. denial of service) against WPA3's Dragonfly handshake:

    An attacker can overload Access Points (APs) by generating as little as 16 forged commit frames per second. This resource consumption attack causes a high CPU usage on the AP, drains its battery, prevents or delays other devices from connecting to the AP using WPA3, and may halt or slowdown other functionality of the AP as well.

TOOLS:

Tools are made to test for certain vulnerabilities.

- **Dragonslayer:** Performs invalid curve attacks against EAP-pwd clients and server. These attacks bypass authentication: an adversary only needs to possess a valid username.

    This tool is available on Github and is being tested on kali-linux.
    Link: *https://github.com/vanhoefm/dragonslayer*

- **Dragondrain:** This tool can be used to test wether, or to which extend, an Access Point is vulnerable to denial-of-service attacks against WPA3's SAE handshake.

    This tool is available on Github and is being tested on kali-linux.
    Link: *https://github.com/vanhoefm/dragondrain-and-time*

- **Dragontime:** This is an experimental tool to perform timing attacks against the SAE handshake if MODP group 22, 23, or 24 are supported. Note that most WPA3 implementations by default do not enable these groups.

- **Dragonforce:** This is an experimental tool which takes the information recovered from our timing or cache-based attacks, and performs a password partitioning attack. This is similar to a dictionary attack.

  This tool is available on Github and is being tested on kali-linux.
  Link: *https://github.com/vanhoefm/dragonforce*

REFERENCE:

✓ For more information visit: **https://wpa3.mathyvanhoef.com/**

*****