WPA3 Attack Flow in ADVISE

Antonio Osele, Marco Ruta

03/06/2023

Möbius Model-Based Environment for Validation of System Reliability, Availability, Security, and Performance

Contents

List of Figures

List of Tables

1 Introduction

In an increasingly interconnected world, ensuring the security of wireless networks is of paramount importance. The Wi-Fi Protected Access 3 (WPA3) protocol was introduced as an enhanced security measure to address vulnerabilities found in its predecessor, WPA2. However, it is crucial to comprehensively understand the attack flow within WPA3 to identify potential weaknesses and develop countermeasures effectively. In this project, we aim to **model the attack flow on WPA3-Personal using ADVISE** (Attack Dependency and Vulnerability Information System and Estimator) with the assistance of **Möbius**. The primary objective is to investigate the attractiveness of different attack paths based on various attacker profiles and goals, such as launching *Denial-of-Service (DoS)* attacks or *disclosing private information*.

Our project revolves around the concept of **attack flow**, which encapsulates the progression of attacks in a systematic manner. We adopted the *four-phase* structure of the WPA3 attack flow, wherein each phase comprises a *state* and a *set of potential attacks* that can be executed within that state. By leveraging Möbius, we developed an abstract representation of the attack flow, preserving the essential elements of state, phase, attack, and goals while simplifying the attack techniques.

The key objectives of this project are:

- **Analyzing Attack Paths**: we seek to explore and evaluate the various attack paths within the WPA3-Personal protocol. By modeling these paths in ADVISE, we can identify the most attractive routes for attackers based on their specific goals.
- **Assessing Attacker Profiles**: we consider different attacker profiles, taking into account their skills, knowledge, and motivations. By incorporating these profiles into our modeling, we can gain insights into how attacker characteristics influence the choice of attack paths.
- **Evaluate Social Engineering**: our project aims to investigate the feasibility of social engineering as possible attack vector to extended the attack surface of WPA 3. By integrating social engineering we added new paths on the original attack flow.

1.1 WPA3 Attack Flow

WPA3, the latest iteration of the Wi-Fi Protected Access protocol, introduces significant enhancements over its predecessor, WPA2. These improvements aim to address vulnerabilities and strengthen the security of wireless networks. Two key elements that differentiate WPA3 from WPA2 are the Dragonfly handshake and the introduction of protected management frames.

- **Dragonfly Handshake**: the Dragonfly handshake, also known as the Simultaneous Authentication of Equals (SAE), replaces the Pre-Shared Key (PSK) authentication method used in WPA2. It provides a more robust and secure key exchange protocol for establishing a secure connection between devices. The Dragonfly handshake utilizes the Elliptic Curve Diffie-Hellman (ECDH) protocol, which offers stronger cryptographic algorithms and resistance against offline dictionary attacks.
- **Protected Management Frames**: WPA3 introduces the concept of protected management frames, which adds an additional layer of security to management frames exchanged between the access point and connected devices. In WPA2, these management frames were transmitted in plain text, making them susceptible to various attacks.

By incorporating the Dragonfly handshake, WPA3 significantly reduces the risk of offline password cracking and enhances the security of Wi-Fi networks while protected management frames prevents attackers from intercepting and tampering with critical network management information, such as deauthentication or disassociation frames. As a result, WPA3 mitigates certain attack vectors that target the management frames in WPA2. It's important to note that while WPA3 offers improved security, it may still have its own set of vulnerabilities or attack vectors that need to be explored and understood. The attack flow targeting WPA3-Personal is illustrated in Figure 1, depicting the sequence of steps involved in compromising the security of WPA3-Personal networks. In the following chapter all the graph nodes will be furthermore explained.

Figure 1: WPA3 Attack Flow

1.2 ADVISE modeling

To summarize the creation of the ADVISE model from the original WPA3 attack flow we performed **Goals Reduction**, the original three goals are simplified to two mutually exclusive goals: *Denial of Service (DoS)* and *Sensitive Information* Disclosure. The concept of deception is considered as a means to achieve personal information disclosure. All the elements of the original graph are transformed in ADVISE Nodes as listed in Table 1.

ADVISE Node	**Name**	**Graph Objects**
Goal	Sensitive Information	Sensitive Information and Deception
Goal	DOS	Denial Of Service
Knowledge	SSID & MAC target network	Added
Knowledge	Key	Key Acquisition
Access	AP Hardware	Added
Access	MITM	Man in the Middle
Access	Network Access	Added
Access	Hijacking	Keyed Client Session Hijacking
Skill	Social Engineering	Added
Skill	AP Configuration	Added
Skill	Packet Forging	Added
Skill	Network Hacking	Added
Attack	Network scanning	Added
Attack	Password Capture	Added
Attack	Rogue AP	Rogue Access Point
Attack	Evil Twin	Evil Twin
Attack	Join Network	Join Network
Attack	Network Layer Attack	ARP Spoofing
Attack	Block Traffic Flow	Added
Attack	Application Layer Attack	DNS Spoofing or SSL Stripping

Table 1: ADVISE Nodes, Names, and Graph Objects

Several simplifications were made to condense multiple graph objects into single ADVISE nodes, allowing for a more streamlined representation of the steps between states. Additionally, new nodes were introduced to better capture the progression of the attack flow. All the relevant skill proficiencies were included in the model to facilitate the modeling of various attacks. Notably, a new attack called "password capture" was added to account for the specific action of acquiring the key via social engineering. These adjustments enhance the accuracy and comprehensiveness of the ADVISE model, enabling a more precise analysis of the WPA3 attack flow. The interpretation of the WPA3 attack flow phases in phases is listed below:

- **Phase 1**
  - *State*: the attacker does not have the key and access to the network and can perform all the attacks of this phase.
  - *Original Attack*: Rogue Access Point, requires scanning the network for obtaining the *SSID and MAC addresses knowledge*, having the necessary *AP hardware*, and having *AP configuration skills*. Results in acquiring the *key*.
  - *Added Attack*: Password capture, requires *social engineering skill*. Results in acquiring the *key*.
- **Phase 2**
  - *State*: the attacker now knows the *key*.
  - *Possible Attacks*: Join the network and move to the Joined Network state or Create an evil twin of the target network, requiring *AP configuration skills* and *AP hardware*. The Evil Twin attack results in achieving MITM position.
- **Phase 3**
  - *State*: the attacker has gained a Man-in-the-Middle (MITM) position via the evil twin or has simply joined the network in Phase 2.
  - *Possible Attacks*: Network layer attacks as ARP spoofing, requires *packet forging skill*.
- **Phase 4**
  - *State*: the attacker is still a Man-in-the-Middle (MITM) or is in Client Session Hijacking state.
  - *Possible Attacks*:
    - If the attacker is MITM he can perform Application layer attacks like SSL stripping or DNS spoofing to gain sensitive information. Both these attacks require *network hacking skills*. The attacker can also choose to cause a Denial of Service (DoS) by blocking the traffic.
    - If the attacker achieved Keyed Session Hijacking he can cause a Denial of Service (DoS).

These modifications and additions to the original WPA3 attack flow allow for a simplified representation of the attack states and possible actions within the ADVISE model represented in Figure 2. In the following section will be better explained how all the attacks of the model are characterized.

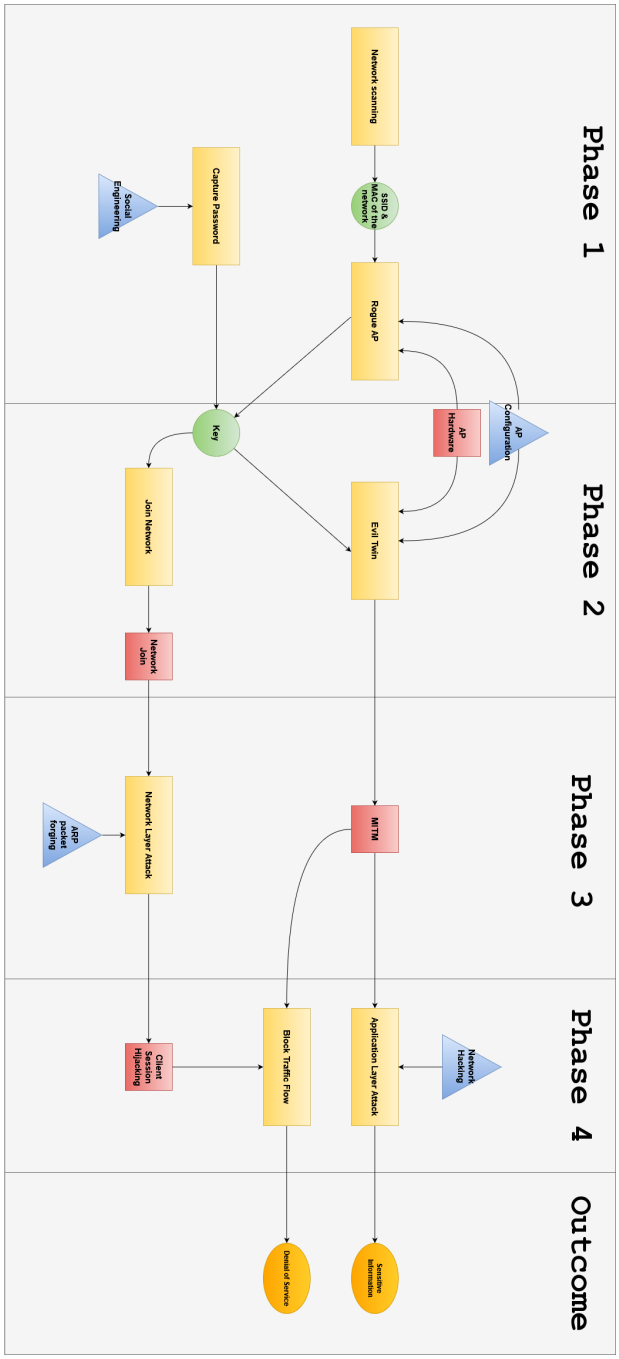

Figure 2: ADVISE Model

1.3 Attack Modeling

In our experiment setup we modeled the attack steps following the ADVISE characterization:

- The *attack cost* denotes the resource-intensive or complex nature of the attack, with higher values indicating greater costs.
- The *time* parameter represents the duration required to execute the attack, with higher values denoting longer durations.
- The *detectability* factor signifies the likelihood of the attack being detected by security measures or monitoring systems.

These weights and constants are reported in Table 2 and allow us to quantitatively assess on a scale (1,10) the attractiveness and feasibility of different attack paths within the ADVISE model.

Attack	Attack Cost	Time	Detectability Success	Detectability Failure
Network Scanning	0	2	0	0
Join Network	0	1	0	0
Password capture	6	10	0.1	0.5
Rogue AP	4	6	0.1	0.5
Evil Twin	6	8	0.2	0.7
Network Layer Attack	4	4	0.1	0.3
Block Traffic flow	3	2	0.5	0.1
Application Layer Attack	10	7	0.3	0.1

Table 2: Weights and Constants for Attacks in the ADVISE Model

The chosen weights for the attacks in the table are based on several factors and considerations. Here's a brief explanation of how each weight was determined:

- **Network Scanning**: this action is costless, requires minimal time, and is typically undetectable. Therefore, it has a weight of 0 in terms of attack cost and detectability.
- **Join Network**: similar to network scanning, joining a network with a known key is a costless action that requires a small amount of time and is generally undetectable.
- **Password capture**: involves retrieving the password via social engineering. It can be time-consuming and challenging, hence the higher cost of 6. The detectability differs depending on the outcome, with a higher detectability in case of failure (0.5) compared to success (0.1).
- **Rogue AP**: hosting a Rogue AP in a network requires some time and skills. It is considered a moderately complex attack, and thus, it has a weight of 4 for the attack cost.

- **Evil Twin**: the Evil Twin attack is an advanced version of the Rogue AP attack. It requires more skill and time to set up and configure properly. In case of failure, an evil twin AP is more likely to be detected due to incorrect configuration. Hence, it has a higher detectability in case of failure (0.7) compared to success (0.2).
- **Network Layer Attack**: network layer attacks, such as ARP spoofing, are relatively more mechanical and can be performed using specific tools. While they still require some skill, they are considered slightly less complex than application layer attacks. Hence, they have a lower attack cost of 4.
- **Block Traffic Flow**: this attack involves disrupting the traffic flow in one direction. Although it has a low attack cost (3), it has a higher detectability in case of success (0.5) because users will experience a Denial of Service situation.
- **Application Layer Attack**: these attacks target the application layer, such as SSL stripping and DNS spoofing. They are considered complex attacks that require significant skill and knowledge to execute effectively. Therefore, they have a higher attack cost of 10.

These weight assignments are based on the inherent characteristics of each attack type, including the required skills, time investment, and the detectability of the attack in different scenarios. They aim to provide a relative measure of the impact and feasibility of each attack within the WPA3 attack flow.

2 Attackers

In this chapter we'll present the various attacker profiles, with different skills and objectives, and their respective behavior when performing an attack. Every attacker had the following parameters:

- **Planning Horizon**: 5
- **Cost Weight**: 0.1
- **Detection Weight**: 0.1
- **Payoff Weight**: 0.8

In Table 3 instead we show an overview of each attacker, with their respective set of skills, accesses and goals.

Attacker	AP Config.	Net. Hacking	Packet Forging	Social Eng.	AP HW	DoS	Sensitive Info
Alice	0	0	10	10	0	1000	200
Bob	10	0	0	0	1	1000	200
Carl	10	10	0	10	1	1000	200
Dave	10	10	0	0	1	200	1000
Eve	10	10	0	10	1	200	1000
Frank	10	0	10	10	1	1000	200
Grace	0	0	0	0	1	1000	1000
Heidi	10	10	10	10	1	1000	1000

Table 3: Attacker Profiles

In Table 4 instead we show, for every attacker, the expected outcome of the experiment and the effective outcome that emerged from the simulation.

Attacker	Expected Outcome	Outcome
Alice	DoS via packet forging and social eng	DoS via packet forging and social eng
Bob	DoS via MITM and rogue AP	DoS via MITM and rogue AP
Carl	DoS via MITM and rogue AP || Social Eng	DoS via MITM social eng.
Dave	INFO via MITM and rogue AP	INFO via MITM and rogue AP
Eve	INFO via MITM and rogue AP || Social Eng	INFO via MITM and social eng.
Frank	DoS via MITM || Hijacking	DoS via Hijacking
Grace	Do nothing	Scan Network
Heidi	DoS || INFO	INFO via social eng.

Table 4: Attacker Expected Outcomes and Actual Outcomes

Let's now analyze in detail every attacker. Image 3 shows the possible paths an attacker can take.

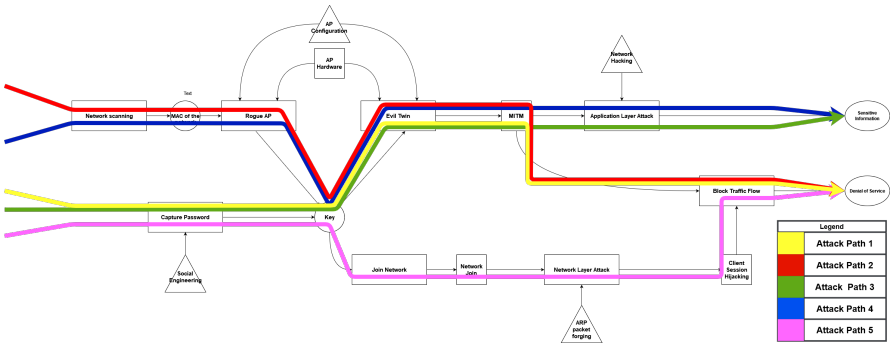

Figure 3: Attack paths

2.1 Alice

The first attacker is Alice, a charming black hat hacker on a budget that wants to block access to a government network. Her profile is the following:

- **Skills**: packet forging and social engineering;
- **Accesses**: None;
- **Goals**: DoS.

As expected, she's able to perform a DoS attack using Path 5, by choosing to gain the key via social engineering and blocking the traffic by hijacking the client session. The probability of achieving her goal is 72.9%.

2.2 Bob

The second attacker is Bob, an angry computer technician that wants to perform a DoS on his company's server to protest. His profile is the following:

- **Skills**: AP configuration;
- **Accesses**: AP Hardware;
- **Goals**: DoS.

As expected, he's able to perform a DoS attack using Path 2, by choosing to gain the key by setting up a rogue AP and blocking the traffic by becoming a Man in the Middle. The probability of achieving his goal is 64.8%.

2.3 Carl

The third attacker is Carl, a friendly professor of Network Security that wants to show his students how to perform a DoS on a network running WPA3. His profile is the following:

- **Skills**: AP configuration, network hacking and social engineering;
- **Accesses**: AP Hardware;
- **Goals**: DoS.

As expected, he's able to perform a DoS attack using Path 1. Being able to gain the key both with a rogue AP and social engineering, he chose the latter and then blocked the traffic by becoming a Man in the Middle. The probability of achieving his goal is 81.1%.

2.4 Dave

The fourth attacker is Dave, a student of Cybersecurity that likes to participate in hacking competitions and is trying to steal a flag inside a fictitious network. His profile is the following:

- **Skills**: AP configuration and network hacking;
- **Accesses**: AP Hardware;
- **Goals**: Sensitive Information.

As expected, he's able to steal sensitive information using Path 4, by choosing to gain the key by setting up a rogue AP and steal the information using an application layer attack. The probability of achieving his goal is 72%.

2.5 Eve

The fifth attacker is Eve, an IT System Engineer that really knows how to talk to people and wants to steal some personal information. Her profile is the following:

- **Skills**: AP configuration, network hacking and social engineering;
- **Accesses**: AP Hardware;
- **Goals**: Sensitive Information.

As expected, she's able to steal sensitive information using Path 3, by choosing to gain the key via social engineering and steal the information using an application layer attack. The probability of achieving her goal is 81.1%.

2.6 Frank

The sixth attacker is Frank, a web developer with no advanced knowledge of hacking that wants to test for vulnerabilities on his local network. His profile is the following:

- **Skills**: AP configuration, packet forging and social engineering;

- **Accesses**: AP Hardware;
- **Goals**: DoS.

As expected, he's able to perform a DoS attack using Path 5, and choose to block the traffic by hijacking the client session. The probability of achieving his goal is 72.9%.

2.7 Grace

The seventh attacker is Grace, an average girl with no particular abilities that watched Mr. Robot once and wants to imitate him. Her profile is the following:

- **Skills**: none;
- **Accesses**: AP Hardware;
- **Goals**: DoS and Sensitive Information.

As expected, she's not able to perform any attack since he has no skills, managing to only scan the network and get the SSID and MAC of the network. The probability of achieving her goal is 0%.

2.8 Heidi

The eighth and final attacker is Heidi, a world class hacker with great charisma that would like to steal credit card information from a bank but can settle to perform a DoS. Her profile is the following:

- **Skills**: AP configuration, network hacking, packet forging and social engineering;
- **Accesses**: AP Hardware;
- **Goals**: DoS and Sensitive Information.

Being skilled in everything and having every access and goal, she decides to take Path 3, by choosing to gain the key via social engineering and manages to steal sensitive information using an application layer attack. The probability of achieving her goal is 81.1%.

3 Conclusion

In conclusion, our analysis using Möbius to model the WPA3 attack flow and various attacker prototypes has provided valuable insights.

- **The prevalence of social engineering as a preferred attack method** emphasizes the importance of considering non-traditional attack paths when evaluating the security of a protocol like WPA3. By recognizing the potential impact of social engineering, security professionals can develop more comprehensive defense strategies that encompass both technical and human-centric aspects of cybersecurity.
- **The attackers' preference for gaining sensitive information over launching Denial of Service** attacks suggests that the potential value of the information obtained serves as a strong motivator. This finding underscores the necessity for robust measures to protect sensitive data within Wi-Fi networks.
- **Our analysis underscores the complexity and expertise required to execute successful attacks against WPA3**. The combination of specific skills, access, and knowledge necessary for each attack path highlights the formidable challenge faced by potential attackers.
- **Möbius has proven to be an invaluable tool in our analysis**. Its high level of abstraction enabled us to capture the essence of the WPA3 attack flow while maintaining a clear understanding of the overall landscape.

To sum up, our study utilizing Möbius to model the WPA3 attack flow has provided valuable insights into the potential vulnerabilities and complexities of the protocol. We have identified critical attack paths, emphasized the significance of social engineering as an attack vector, and highlighted the expertise required to exploit WPA3. These findings underscore the importance of user awareness, robust security measures, and a multi-faceted approach to network security.

In future work, a *finer representation of the attack steps*, encompassing substeps and more detailed associated time, skills, accesses, and knowledge, would enhance our understanding of the attack nature. Additionally, incorporating *new attack vector* (such as electromagnetic susceptibility to cause Denial of Service) would expand the evaluation of the WPA3 attack surface. Furthermore, further research can focus on *hardening the target network* with measures like firewalls and intrusion detection systems, enabling the study of how attackers navigate additional defenses. These avenues of exploration would contribute to a more comprehensive assessment of WPA3 and aid in fortifying network security.