The Future of Engineering Education
2024 Annual Conference & Exposition
Oregon Convention Center
Portland, OR . June 23 - 26, 2024
ASEE
Paper ID #44015

Development of WPA3-focused, Hands-on Lab Exercises at the Undergraduate Level

Dr. Emil H Salib, James Madison University

Professor in the College of Integrated Science & Engineering (CISE) at James Madison University (JMU). Current Teaching - Networking & Security, Introductory Programming and Cross Platform Mobile Application Development. Current Research - Private Cloud Computing

Development of WPA3 focused Hands-on Lab Exercises at the Undergraduate Level

Dr. Emil H. Salib, salibeh@jmu.edu,
College of Science and Engineering (CISE),
James Madison University (JMU), Harrisonburg, VA 22807

1 Introduction

The emergence of WPA3, a groundbreaking innovation in Wi-Fi security, presents both an opportunity and a challenge within the realm of wireless networking. The pressing need to upgrade the wireless networking and security curriculum in undergraduate IT programs is a priority. Equipping students with the latest knowledge in wireless networking and security is of utmost importance to our IT program at James Madison University, particularly considering the vulnerabilities that have tainted its predecessor, WPA2.

The first major challenge facing the educators in teaching WPA3 is the lack of cost-effective WPA3 Access Points (APs and wireless clients. For example, they may have to invest a significant amount of money to acquire brand-new devices since the vendors refused to provide a simple and cost-effective solution for upgrading their existing WPA2 APs and clients. The second major challenge, and more critical, is that the WPA3 security mode uses complex cryptographic algorithms. In teaching these algorithms, an educator is required to have access to information and data exchanged between the WPA3 APs and wireless clients. This data is not accessible using the native vendor AP and client firmware even for the brand new and expensive devices. Therefore, an alternative firmware solution is a must to allow the educators to develop practical WPA3 lab exercises that enable the students to gain a solid understanding of WPA3. The third major challenge is to find the hardware that can accept third-party alternate firmware that meet the needs described briefly in the second major challenge and will be explained in detail later in this paper.

In response to these challenges, we have embarked on a practical implementation of a WPA3 platform in the context of wireless networking and security IT education. In this paper, we describe the lessons learnt in the implementation of such an environment. Its objective is to enable educators to build hands-on lab exercises on WPA3 personal and enterprises security modes as well as to compare them with those of WPA2. The focus of this paper is to demonstrate that the custom WPA3 platform can enable an educator to create WPA3 lab instructions. These instructions should match the students' skills and be slightly above for new skills. For example they should be successfully able to set up the environment and perform the lab instructions and collect results for an entirely new topic, such as, WPA3 new authentication scheme.

Below are the details of our implementation and experimentation revolving around the creation of the custom solution that employs Raspberry Pi-based wireless access points (mainly for portability) and wireless clients as well as flashing alternate firmware such as OpenWrt onto inexpensive APs. These components have been customized and equipped to support not only WPA3 Personal but also the robust WPA3 Enterprise standard mode and the enhanced 192-bit higher security mode.

The structure of this paper is as follows: In Section 2, we present an overview of the project, encompassing the opportunity, objectives, and our proposed solution. Moving to Section 3, we provide an in-depth description of the requirements and the methodology adopted in crafting a flexible, easily flashed with alternate firmware and cost-effective platform. This platform serves as the foundation for the creation of new WPA3 lab exercises. Section 4 delves into the detailed implementation and configuration of the platform components, supporting the lab exercises centered around studying WPA2 & WPA3 personal and enterprise security modes. In Section 5, we provide brief descriptions of the concepts behind four (4) newly created and tested WPA3 lab exercises. Finally, Section 6 engages in a discussion, encompassing our students' observations, and suggestions for qualitative assessment of the lab instructions, the concepts they are based on, along with our conclusions and potential future steps.

2 Our Project

In this section, we outline the project's opportunity, goal, objectives, and the proposed solution. The overarching objective of this endeavor is to seamlessly integrate WPA3's wireless personal and enterprise security mode, as defined by [1], into our existing Information Technology (IT) undergraduate curriculum. Specifically tailored for juniors and seniors majoring in IT, the initiative anticipates that participating students will have successfully completed prerequisite courses, namely, ”Introduction to Telecommunications, Networking, and Security” and ”Advanced Networking for Information Technology.”

2.1 Project Opportunity

The introduction of WPA3 wireless security personal and enterprise modes has offered significant security enhancements over WPA2 [2]. However, it has presented us with a challenge regarding the best approach to updating our curriculum. The changes introduced in WPA3 are significant and require a new approach to studying WPA3 security algorithms. Here are some of the changes: (1) SAE/Dragonfly authentication algorithm [3] for WPA3-Personal in place of the Open Authentication adopted in WPA2-Personal, (2) WPA3 mandates the use of the Protected Management Frame (PMF) functionality [4], and (3) offers the 192-bit optional security mode in the WPA3-Enterprise environment. Additional challenge is the potential for incompatibility issues between the vendors implementation unless they all have gone through the Wi-Fi WPA3 certification [5].

2.2 Project Objectives

To fulfill the project's goal and bring the proposed solution to fruition, we have established the following key objectives: (1) Validate the seamless interoperability of the selected components to ensure the correct support of WPA3 security mode, (2) Design, implement, and deliver a set of hands-on lab exercises specifically targeting WPA3 security mode, encompassing both personal and enterprise settings that match the skills of senior IT students, (3) Demonstrate the distinctions between WPA3 and WPA2 security modes, (4) Conduct a qualitative assessment of the lab instructions and how effective they are in being exercised on the new platform, and (5) Formulate recommendations for potential enhancements, and future areas of work.

2.3 Project Proposed Solution

To meet the project objectives, we developed an affordable, customizable, and flexible solution comprising our own wireless access points (APs) and wireless stations (STAs)/clients. These tailored wireless components leverage open-source software, running seamlessly on cost-effective RPi-3B units [6]. These units are equipped with USB wireless adapters featuring chips that support WPA3 protocols and requirements, such as the TL-WN722N [7].

To underscore the significance of WPA3, it is crucial to provide students with the opportunity to compare it against its predecessor, WPA2. This necessitates configuring the designed platform effortlessly for both WPA2 and WPA3, aligning with Wi-Fi's adopted backward compatibility and support for a mixed WPA2/WPA3 operational environment.

3 Solution Components

In this section, we describe the design process we have undertaken to tackle the challenges outlined in Sections 1 & 2. Initially, we will outline the most critical requirements that the solution must fulfill. Subsequently, we will delve into the components selected to satisfy these specified requirements.

3.1 Requirements

From the outset, it was evident that our platform needed to possess the following attributes:

- Support for WPA3 security personal and enterprise modes.
- Provide security related data exchanged between the AP and wireless clients.
- Backward compatibility with WPA2, accommodating mixed WPA2 and WPA3 environment.
- Modularity and customizability.
- Adequate performance and availability.
- Capability to sniff IEEE 802.11 wireless frames.
- Cost-effectiveness.
- Integration with the wealth of programs and scripts available from the Wi-Fi community.
- Base itself on open source hardware and software.

Leveraging our prior experience with Raspberry Pi, we identified it as a crucial building block. Raspberry Pi, being a small portable single-board computer, aligns with open source hardware principles, proving both inexpensive and easily accessible.

In parallel, we recognized open source software, including hostapd, wpa supplicant, and FreeRADIUS, as essential packages enabling the creation of customizable Wi-Fi components such as APs, wireless clients, and authentication servers. The WPA supplicant, available across various operating systems, supports WPA2, and WPA3 (IEEE 802.11i / RSN). Its flexibility in build configuration facilitates easy selection of different feature combinations, suitable for desktops, laptops, and embedded systems.

In our exploration of existing developments, the OpenWrt [8] alternate firmware platform emerged as a valuable resource of pre-existing open source packages. We envisioned wireless devices flashable with OpenWrt as potential alternatives or collaborators with Raspberry Pi, emphasizing the significance of standards for competitiveness and innovation in implementing new capabilities, including WPA3.

To enable the sniffing of IEEE 802.11 wireless frames, we identified the iMac [9] as the optimal choice, despite its limitation in mobility. To mitigate this, we devised a solution—placing an iMac on a mobile cart (iMac-on-Wheel)—allowing students to sniff packets in configurations where multiple access points were spatially distributed.

In the following sections, we will offer brief descriptions of the components we have identified, showcasing how they align with and meet the previously mentioned requirements.

3.2 RPi-3B

This is the primary component upon which we heavily relied in constructing the platform for developing WPA3 lab exercises. The RPi-3B stands out for its ready availability and cost-effectiveness. However, its performance is contingent on the installed operating system (OS) and packages. Following our research and assessment, we opted to configure the RPi-3B with the Raspberry Pi OS (32-bit) Lite (Raspbian GNU/Linux 11 (bullseye)) [6] to ensure optimal performance.

Additionally, we discovered that the built-in wireless chip lacks support for WPA3 and Protected Management Frame (PMF) functionality. Fortunately, we found a solution by equipping the RPi-3B units with an external USB wireless adapter that supports WPA3 and PMF. The TP-Link TL-WN722N v1 USB wireless adapter [7] features a Qualcomm wireless chip (driver ath9k_htc version 5.25.61-v7, firmware 1.4), and we confirmed its compatibility with WPA3 and PMF. However, it restricts us to the use of the 2.4 GHz band. In our assessment, this limitation does not impede the effectiveness of wireless security algorithms, as they are not reliant on the operating frequency bands.

To convert an RPi-3B unit into an Access Point (AP), we utilized a bash script [10] designed to install essential packages such as hostapd release v2.9 and dnsmasq. Additionally, the script facilitates the creation of configuration files, namely hostapd.conf and dnsmasq.conf.

The Raspberry Pi OS (32-bit) Lite is equipped with the pre-installed wpa_supplicant release v2.9 [11], a crucial tool that we extensively leverage to create wireless clients with a diverse set of capabilities.

Converting an RPi-3B unit into a RADIUS-based Authentication Server required the installation of several packages, including FreeRADIUS (Version 3.0.21) [12], freeradius-utils (radtest), eapol_test (v2.9), and mariadb-server-10.0.

3.3 TP-Link Archer A7 v5

The Archer A7 [13] has been marketed as a high-speed IEEE 802.11ac Access Point (AP) with an extended range, making it an appealing option at a reasonable price point. However, in its original state with the factory firmware, this unit lacks support for the WPA3 security mode and the Protected Management Frame (PMF)/IEEE 802.11w feature.

Fortunately, owing to the Qualcomm chip QCA9560 embedded in this AP, we successfully flashed the unit with OpenWrt 22.03.2 [14], [15], thereby enabling these critical features. To further enhance wireless security options and introduce support for WPA3-Enterprise, also known as WPA3-Extensible Authentication Protocol (EAP) in the OpenWrt definition, we replaced the default OpenWrt wpad-basic-wolfssl package with the ”hostapd-openssl” package. This strategic adjustment ensures a more comprehensive and robust set of security capabilities on the Access Point.

4 Solution Implementation

In this section, we elaborate on the configuration process of the components outlined in Section 3, crucial for establishing our IEEE 802.11 wireless network that encompasses support for WPA2, WPA3-Personal, and WPA3-Enterprise wireless security modes.

4.1 WPA3-Personal and Enterprise Networks

Figures 1 and 2 illustrate the carefully designed and implemented configurations for establishing fully functional and adaptable wireless networks supporting WPA2, WPA3-Personal, and WPA3-Enterprise security modes. These network setups facilitated a comprehensive exploration of WPA3 wireless security algorithms across different security modes. Additionally, they served as the infrastructure for capturing IEEE 802.11 packets exchanged between the Stations (STAs) and Access Points (APs), and for recording detailed debug message logs from wpa_supplicant, hostapd, and FreeRADIUS. These logs play a crucial role in conducting in-depth functional analyses.

In Figures 1 and 2, the IEEE 802.11 sniffer was implemented using an iMac desktop running Wireshark, configured in monitoring/sniffing mode [9]. This setup allowed for the capture of IEEE 802.11 packets exchanged between the Stations (STA)/wireless clients (e.g., RPi-3B with wpa-rasp) and the Access Points (AP)/Wireless Access Points (e.g., RPi-3B with ap-rasp or TP-Link Archer A7 v5).

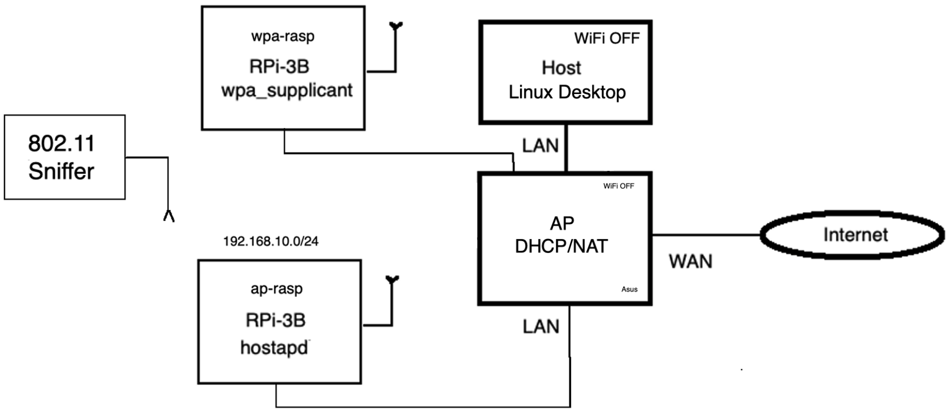

Figure 1: IEEE 802.11 WPA3-Personal Network Arrangement.

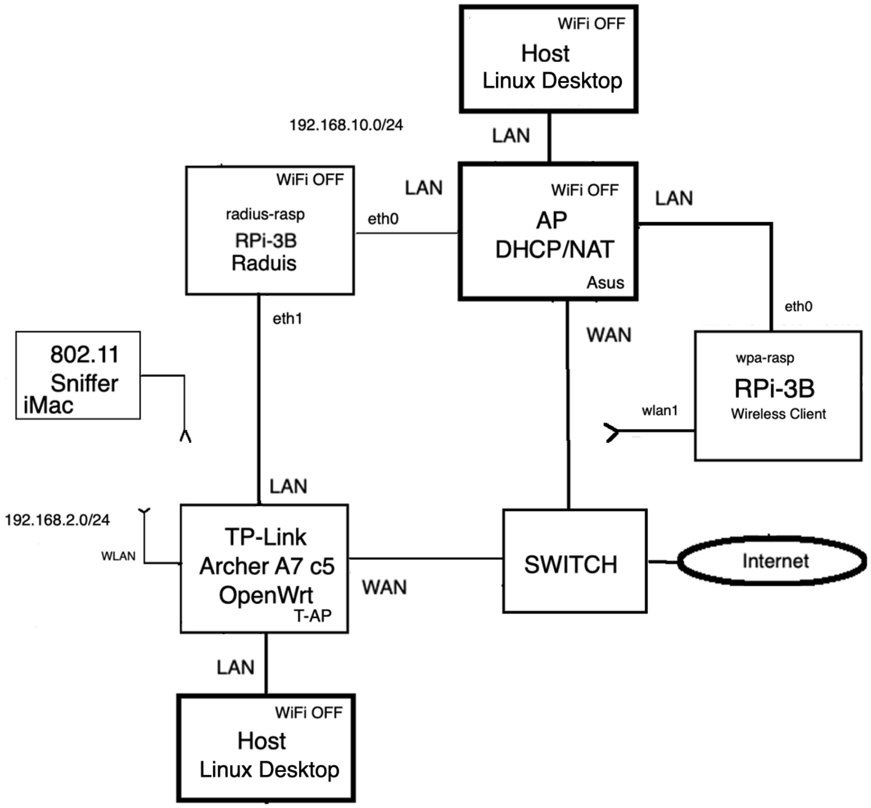

Figure 2: IEEE 802.11 WPA3-Enterprise Network Arrangement.

4.2 WPA2 and WPA3-Personal Security Mode Configurations

In this section, we present the configurations for the RPi-3B-based Access Point (AP) named ap-rasp and the Station/Wireless Client (STA) named wpa-rasp. Furthermore, we include the requisite commands to initiate both the WPA2 or WPA3 AP and STA, while displaying debug messages.

To enable the WPA3-Personal security mode, incorporating Simultaneous Authentication of Equals (SAE) and Protected Management Frame (PMF), the ap-rasp was configured based on the hostapd.conf example provided in Appendix A.1.1.

Similarly, to support the WPA3-Personal security mode, including SAE and PMF, the wpa-rasp was configured according to the wpa_supplicant.conf example given in Appendix A.1.2.

4.3 WPA2 and WPA3-Enterprise Security Mode Configurations

In this section, we provide details on the configuration of the TP-Link Archer A7 v5 Access Point with OpenWrt, the RPi-3B-based RADIUS server (radius-rasp) with eapol-ttls.conf, and the necessary command to test FreeRADIUS users and clients. Additionally, we present the configuration for the RPi-3B-based Station/Wireless Client (STA) named wpa-rasp along with the command required to bring up a WPA3 STA/Wireless Client, displaying debug messages including key data.

The TP-Link Archer A7 v5 serves as the WPA3-Enterprise Access Point, configured through the OpenWrt Luci interface. Refer to Figure 3 for the various WPA3 security mode options available.

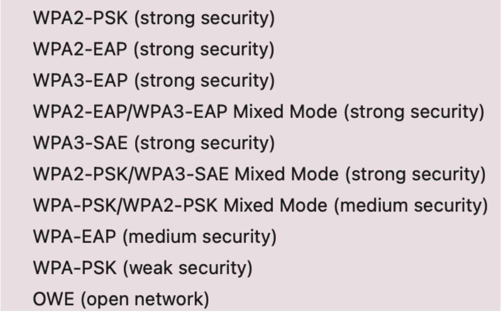
WPA2-PSK (strong security)
WPA2-EAP (strong security)
WPA3-EAP (strong security)
WPA2-EAP/WPA3-EAP Mixed Mode (strong security)
WPA3-SAE (strong security)
WPA2-PSK/WPA3-SAE Mixed Mode (strong security)
WPA-PSK/WPA2-PSK Mixed Mode (medium security)
WPA-EAP (medium security)
WPA-PSK (weak security)
OWE (open network)

Figure 3: WPA3 Enterprise options of TP-Link Archer A7 v5 flashed with OpenWrt.

For testing purposes, we established our own Certificate Authority (CA) and generated server certificates and private keys. Furthermore, we added multiple users (STAs/supplicants) and FreeRADIUS clients (AP/authenticators) to the radius-rasp server. To evaluate the radius server configurations, we utilized the eapol_test utility with various eapol configuration files, such as the one shown in Appendix B.1.1.

To support WPA2 and WPA3-Personal security modes, including Simultaneous Authentication of Equals (SAE) and Protected Management Frame (PMF), the wpa-rasp was configured according to the wpa_supplicant.conf example given in Appendix B.1.2.

5 Solution Results (Concepts of Lab Exercises)

In this section, we provide a brief description of the concepts we focused on in the development of the lab instructions of four (4) lab exercises using the platform described in Sections 3 & 4. Two exercises are on personal security mode. The other two are on the enterprise security mode.

Although these are aimed for the students to build new implementation and execution technical skills, they also provide them opportunities for analysis through comparison and answering analysis questions promoting the students to think critically and have deeper understanding of new security concepts. This is done through comparing the authentication utilized in WPA3 with that in WPA2. Also, the students are offered a unique opportunity to study new WPA3 features such as broadcast/multicast management frames. These and other concepts rely heavily on Wireshark 802.11 packet capturing, hostapd (custom AP) debug messages and wpa_supplicant (custom client) debug messages. The debug messages allow access to data not easily accessible through the use of vendor supplied firmware.

Here is a list of concepts we focused on in the development of the four (4) WPA3 lab exercises:

- The first major new concept introduced in WPA3 personal security authentication (discovery phase) is the ability to compute unique and unpredictable pairwise master key (PMK) for every client and for every session initiated by that client (see Section 12.4 in [3], [16]). This is unlike the WPA2 case where all clients and for all their sessions, the PMK is the same and predictable.
- The second major new concept in WPA3 personal security is the mechanism used by both the client and AP to compute independently the same PMK value without being ever communicated over the transmission path between them. But as important is the ability that each party can verify that the other has the same PMK value. Every time this method is exercised a unique PMK is created and verified independently by both the client and AP (see 12.4.5.5-12.4.5.6 in [3], [17]).
- The third major new concept in WPA3 personal and standard enterprise security modes is that the broadcast/multicast management frames are protected against forging using a new key known as Integrity Group Temporal Key (IGTK). The feature is mandatory under WPA3 and typically referred to as Protected Management Frames (PMF). Note that the frames are authenticated but not encrypted with that key. This key is created during the 4-way handshake key management phase and the broadcast/multicast management frames use a new algorithm known as Broadcast Integrity Protocol (BIP) (see Section 12.5.4 in [3]). It is also worth mentioning here that this feature has already been made available (optionally) under WPA2 security modes.
- The fourth major new concept is the optional WPA3 enterprise security enhanced mode. This is defined in the Wi-Fi Alliance [18] and is known as 192-bit mode. This optional mode employs 192-bit minimum-strength keys for the security protocols and cryptographic algorithms to enhance the protection of sensitive data.

6 Discussion, Conclusion & Next Steps

6.1 Discussion

The lab exercises content was created by one of the instructors and underwent testing by students during the Fall semesters of 2022 and 2023. The number of students in the FA22 and FA23 were 10 (5 groups) and 6 (3 groups), respectively. They are juniors and seniors. These are considered pilots to test the platform and the ability of the students to navigate the platform components and lab instructions.

Unfortunately the number of the groups is too small to provide viable sample size for meaningful statistical analysis. Therefore, we opted to survey them for qualitative assessment. Our major intent with this paper is to share with other educators the benefit of our experimentation in introducing WPA3 into the IT undergraduate curriculum. There are three key qualitative assessment questions built into the lab report template:

- Did you feel that you could do the steps and tasks in this lab exercise?
- Do you feel that you've acquired value in doing the steps and answering the analysis questions of this lab exercise?

- What are the barriers prevented you, if any, from investing time, energy or resources into the completion of the steps and answering the analysis questions of this lab exercise with high quality?

The typical group answer to the first question was that the students were able to execute the steps and the tasks. That is, the steps and tasks difficulties are not too high beyond their current skills. For the second question, the group answers were typically positive, that is, they felt that they gained value at least having to be introduced to a new topic such as WPA3. Note that the students were very excited to be learning about WPA3. The typical answer to the third question is that the lab is too long, too many questions, and they had schedule conflicts with other classes' assignments.

In addition to the three (3) questions covered above, the lab report template has two additional qualitative assessment questions. We asked the students to provide their specific observations of the lab instructions and analysis questions as well as their suggestions for improving the lab instructions.

Below are the observations and suggestions highlight provided by the students who actively engaged in performing and testing the WPA3 lab instructions.

Observations: Our students stated: (1) this was the most valuable lab we feel we have done thus far. The transition from WPA2 to WPA3 showed stark differences between the security of the two, (2) the value of this lab was the transition from WPA3-Personal and WPA2-Personal into WPA3-Enterprise as this is likely what we will be using and configuring in the workplace, (3) the value and impact of this lab is huge to us executing this lab because it deals with recent and up to date methods that we will be working with closely in the work field, and (4) we gained a lot of knowledge about how the WPA3 wireless security modes works compared to WPA2.

Suggestions: Our students provided the following suggestion for improvements: (1) While the overall content of the labs were considered appropriate, we (students) suggest trimming down the number of analysis questions for a more focused experience, and (2) we recommend to simplify the steps of configuring the environment, aiming to make it easier for us (students) to troubleshoot and resolve encountered problems.

6.2 Conclusion & Next Steps

We believe that the custom platform has proven to help overcome the challenges we faced as educators to introduce a number of new and unique WPA3 concepts into the IT undergraduate curriculum.

While the current lab exercises align with the project's objectives, we recognize the potential for further improvements in the following areas for future enhancements:

- Prepare and conduct quantitative assessment on the learning effectiveness of the WPA3 lab exercises.
- Provide in-depth characterization of the weakness and strength of the various WPA3 security algorithms.

Acknowledgment

The author would like to thank the College of Science and Engineering (CISE) and Computer Science Department at James Madison University (JMU) for their support throughout the development of the WPA3 platform, lab exercises and the creation of this paper. Special thanks are to the students in ISAT 465 class of the Fall of 2022 and IT 465 class of the Fall of 2023.

References

[1] "WPA3 Specifications." https://www.wi-fi.org/system/files/WPA3%20Specification%20v3.3.pdf, Retrieved: 2024-04-12.

[2] Morti, "WPA3 – Improving your WLAN security." https://wlan1nde.wordpress.com/2018/09/14/wpa3-improving-your-wlan-security/, Retrieved: 2024-04-12.

[3] "IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks–Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Redline," *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016) - Redline*, pp. 1–7524, 2020. Retrieved: 2024-04-12.

[4] "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 4: Protected Management Frames," *IEEE Std 802.11w-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, and IEEE Std 802.11y-2008)*, pp. 1–111, 2009. Retrieved: 2024-04-12.

[5] "Wi-Fi Alliance." https://www.wi-fi.org/discover-wi-fi/security, Retrieved: 2024-04-12.

[6] "Raspberry Pi OS." https://www.raspberrypi.com/software/operating-systems/#raspberry-pi-os-32-bit, Retrieved: 2024-04-12.

[7] "TP-LINK TL-WN722N v1.x." http://en.techinfodepot.shoutwiki.com/wiki/TP-LINK_TL-WN722N_v1.x, Retrieved: 2024-04-12.

[8] "Welcome to the OpenWrt Project." https://openwrt.org/, Retrieved: 2024-04-12.

[9] "How to capture 802.11 packets using Mac OS." https://community.cambiumnetworks.com/t/how-to-capture-802-11-packets-using-mac-os/78642, Retrieved: 2024-04-12.

[10] "Raspberry Pi Automated WiFi Access Point." https://github.com/arm358/Raspberry-Pi-Automated-WiFi-Access-Point, Retrieved: 2024-04-12.

[11] "Linux WPA2/WPA3/IEEE 802.1X Supplicant." https://w1.fi/wpa_supplicant/, Retrieved: 2024-04-12.

[12] "freeradius." https://freeradius.org/, Retrieved: 2024-04-12.

[13] "Archer A7 AC1750 Wireless Dual Band Gigabit Router." https://www.tp-link.com/us/home-networking/wifi-router/archer-a7/, Retrieved: 2024-04-12.

[14] "TP-Link Archer A7 v5." https://openwrt.org/toh/tp-link/archer_a7_v5, Retrieved: 2024-04-12.

[15] "How to unbrick TP Link Archer A7 v5 ." https://milankragujevic.com/restore-a-bricked-tp-link-router-with-tftp, Retrieved: 2024-04-12.

[16] M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the dragonfly handshake of wpa3 and eap-pwd," in *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 517–533, 2020. Retrieved: 2024-04-12.

[17] rdkcteam, “wpa_supplicant-2.9/src/common/sae.c).” https://github.com/rdkcteam/wpa_supplicant-2.9/blob/master/src/common/sae.c, Retrieved: 2024-04-12.

[18] “Discover Wi-Fi - Security.” https://www.wi-fi.org/discover-wi-fi/security/, Retrieved: 2024-04-12.

Appendix A Configurations for Section 4.2

A.1 Personal Mode

A.1.1 Personal Mode - ap-rasp - hostapd.conf

```
interface =wlan1
ssid=”<ssid_name>”
hw_mode=g
ieee80211n=1
channel=2
macaddr_acl=0
auth_algs =1
ignore_broadcast_ssid =0
wpa=2
wpa_passphrase=”<passphrase>”
wpa_key_mgmt=SAE
rsn_pairwise =CCMP
group_cipher=CCMP
wpa_group_rekey=120
ieee80211w=2
```

A.1.2 Personal Mode - wpa-rasp - wpa_supplicant.conf

```
network={
    ssid=”<ssid_name>”
    scan_ssid=1
    psk=”<preshared_key>”
    key_mgmt=SAE
    proto=RSN
    group=CCMP
    pairwise=CCMP
    ieee80211w=2
}
```

Appendix B Configurations for Section 4.3

B.1 Enterprise Mode

B.1.1 Enterprise Mode - radius-rasp - eapol-ttls.conf

```
network={
    eap=TTLS
    eapol_flags =0
    key_mgmt=WPA−EAP
    identity =”<supplicant_username?”
    password=”<supplicant_password>”
    ca_cert =”<path_to>/ca.pem”
    phase2=”autheap=MSCHAPV2”
}
```

B.1.2 Enterprise Mode - wpa-rasp -wpa_supplicant.conf

```
network={
    ssid =”<ssid_name>”
    scan_ssid =1
    proto=RSN
    pairwise =GCMP−256
    group=GCMP−256
    group_mgmt=BIP−GMAC−256
    ieee80211w=2
    eap=TTLS
    eapol_flags =0
    key_mgmt=WPA−EAP−SUITE−B−192
    identity =”<supplicant_username>”
    password=”<supplicant_password>”
    ca_cert =”<path_to>/ca.pem”
    phase2=”autheap=MSCHAPV2”
}
```