An Assessment and Study of Wi-Fi Security Through the Use of Wardriving in Caguas, Puerto Rico

Miguel A. Iglesias Santiago
Computer Engineering
Advisor: Alfredo Cruz, PhD
Polytechnic University of Puerto Rico
February, 2025

Abstract *— In this project, the current state of wireless security in Caguas, Puerto Rico, is analyzed using wardriving as the primary data acquisition method. Wardriving is a technique for scanning and collecting information from wireless access points while in motion and is widely used by security professionals/enthusiasts to evaluate WLAN systems. This project aims to assess the security configurations of publicly accessible IEEE 802.11 wireless networks and identify potential weaknesses. Data was collected through multiple wardriving audits, focusing on encryption protocols and access point configurations. The findings contribute to the broader understanding of wireless network security in Puerto Rico and suggest measures to strengthen protections in light of increasing internet usage.*

Key Terms *— Wireless, Wi-Fi, Security, Wardriving, Auditing*

INTRODUCTION

"Wardriving" involves scanning and collecting data, along with geolocating wireless access points while in motion. Originating in the early 2000s with the rise of IEEE 802.11 wireless networks, it can be performed using a computer, wireless network interface card, GPS device, and sometimes a vehicle[1]. As wireless networks proliferate, wardriving has gained interest as both a tool for evaluating WLAN security and a potential exploitation method. Unlike wired networks, which use physical media, wireless networks rely on electromagnetic waves, making them more vulnerable to intrusion if security best practices are not followed.

Based on the most recent data from the International Telecommunication Union for Puerto Rico in 2021, it was estimated that 85% percent of the population has access to the internet, a number that was approximately 45% in 2010, marking a growth of 89% over ten years[2]. Additionally, it was recorded that in 2021 there are approx. +670K fixed broadband subscribers on the island, with a 2018-2022 survey estimating that only 72% of households have a fixed internet subscription. This comes at a moment when the now outdated Wi-Fi Protected Access protocol or WPA2 is replaced with its next iteration, WPA3, to correct now well-known security vulnerabilities. This expected growth, newer versions of security protocols, and government telecommunications initiatives parallel that 25% of Puerto Ricans do not have a computing device, the lowest rate of device adoption in the United States[3]. The combination of expected growth in communications availability/use in the upcoming years following the historical trends and a population with a perceived low digital/cybersecurity literacy is a dangerous combination that can lead to a loss in all three security principles: confidentiality, integrity, and availability of these networks. For this reason, it is important to understand the current state of wireless networks and the magnitude of improper and/or outdated network configuration practices.

OVERVIEW OF IEEE 802.11

The IEEE 802.11 standard, better known as “Wi-Fi,” is a set of Local Area Network (LAN) technical standards that define the implementation of communications between a group of wireless networking devices within a limited area known as the range that exchanges data through radio communications and is known as the wireless local access network (WLAN).

The IEEE 802.11 standard was introduced in 1997 as the “802.11” or the “Wi-Fi 0” standard; it has gone through multiple name amendments that

each build upon its previous implementation to improve speed, security, and reliability as more significant requirements are needed as it represents one the world's most widely used wireless computer networking protocols. Figure 1 displays a chronological timeline for the release of standard amendments from its initial release to pending versions[4][5].

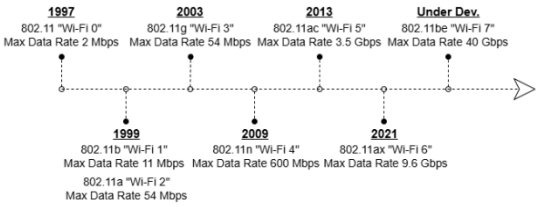

Figure 1
Timeline of Release of 802.11 Amendments

IEEE 802.11 Network Service Sets

The standard defines two primary modes of operation: Infrastructure mode and Ad-Hoc mode. As shown in Figure 2, the Infrastructure mode involves client devices (hosts) communicating through an Access Point (AP), which manages communication between clients and/or the Distribution System (DS). In contrast, Ad-Hoc mode enables direct communication between hosts without a base station or DS connection. Both modes form a Basic Service Set (BSS), the simplest network topology, identified by a shared Service Set Identifier (SSID). Ad-Hoc networks are specifically called Independent Basic Service Sets (IBSS)[4].

Other than the Basic Service Set (BSS), there is also the Extended Service Set (ESS). As illustrated in Figure 3, the ESS is a network topology formed by two or more BSS sharing a common SSID. This configuration allows networks to expand and scale, enabling hosts to transition seamlessly between APs within the ESS without communication disruption.

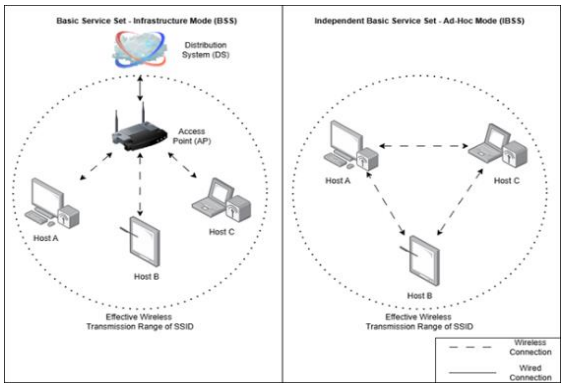

Figure 2
Example of Wi-Fi Communications Infrastructure Mode and Ad-Hoc Mode

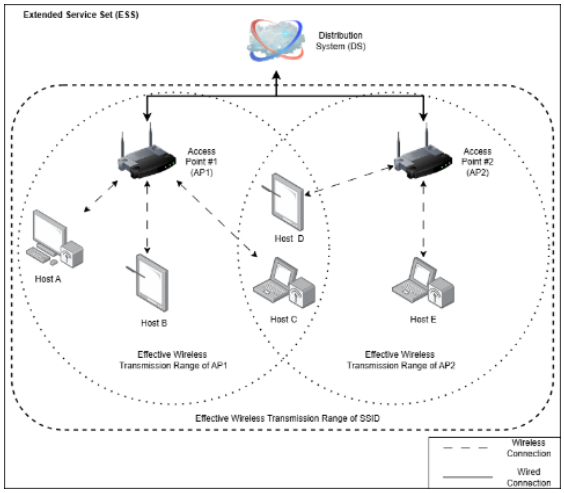

Figure 3
Example of Extended Service Set

Separate from the ESS, the Mesh Basic Service Set (MBSS) is another type of network topology. As shown in Figure 4, it consists of a series of interconnected Access Points (APs) called Mesh Points (MPs). MPs connect to each other and/or a Mesh Portal Point (MPP), which is wired to a Distribution System (DS). Each MP hosts a BSS and shares a common SSID with other MPs in the MBSS. Unlike the ESS, only the MPP in the MBSS is connected to the DS[4][5].

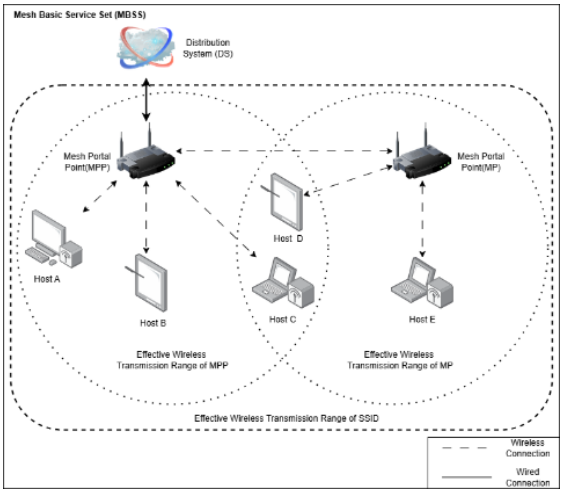

Figure 4
Example of Wi-Fi Communications Mesh Basic Service Set

At the hardware layer, 802.11 implementations use established frequency bands or channels. These bands reduce signal interference and network congestion by preventing overlapping transmissions. Currently, there are 48 channels in the 2.4GHz and 5GHz bands. With the introduction of Wi-Fi 6, the 6GHz band and a multi-band communication scheme were enabled, allowing for communication across multiple channels to improve efficiency[5][6].

802.11 Frame Types, Beacons And Association

When passively monitoring Wi-Fi traffic for wardriving purposes, the focus is on the framed data being transmitted. Certain details about the client and/or associated access points can be inferred by analyzing specific frames. Under the IEEE 802.11 standard, information is categorized into three frame types: management, data, and control.

- **Management frames:** These manage station or client connections and disconnections from wireless access points. Sub-types include beacon, probe, de-authentication, and authentication frames. Beacon and probe request frames are particularly valuable for wireless surveillance, as they carry unencrypted information about access points or previously connected networks.
- **Control frames:** These are used to regulate access to the radio frequency medium and for frame acknowledgment. They are generally encrypted and do not carry a payload, making them inaccessible for wardriving activities.
- **Data frames:** These frames carry data to higher network levels and are typically encrypted, making them inaccessible for wardriving activities[4].

During passive scanning, the process focuses on the initial stages of communication between an access point (AP) and a host or between hosts in ad-hoc mode. Both devices must confirm they are within transmission range and exchange parameters before authentication and communication, a process known as association. As illustrated in Figure 5, in the Basic Service Set (BSS) of IEEE 802.11, new devices listen to AP beacons containing information like SSID, data rates, and security settings. Active scanning, by contrast, involves broadcasting probes to elicit AP responses[7].

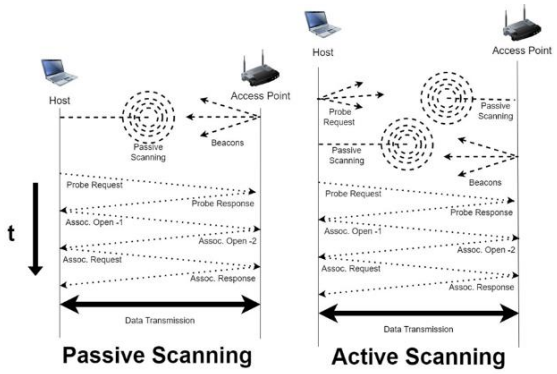

Figure 5
IEEE 802.11 Passive/Active Scanning Association Process

SECURITY SCHEMES

The need for integrated security and encryption is apparent. Most Wi-Fi networks are secured using a standardized configuration(security schemes) that provides a base level of security, reducing vulnerabilities and lessening the impact of successful attacks. As of the draft of this document, there are four principal “Wi-Fi” security schemes: WEP, WPA, WPA2, and WPA3.

- **WEP** (Wired Equivalent Privacy) was the first security protocol for wireless networks in 1999. Since its inception, significant security

weaknesses have been identified. These vulnerabilities are the use of initialization vectors (IVs) and the use of the RC4 stream cipher for encryption; with the development of upgraded computation capacity, these systems can be compromised via brute force cracking. WEP is considered obsolete and should not be used to secure wireless networks[8].

- **WPA** (Wi-Fi Protected Access Ver.1) was introduced in 2003 as a replacement for WEP. It was designed to address the vulnerabilities in WEP by introducing per-packet key mixing in the form of TKIP (Temporal Key Integrity Protocol), which dynamically generates a new 128-bit key for each packet of data and a WPA message integrity check (MIC) to prevent attackers from altering/resending data packets. WPA still used the RC4 cipher previously used in WEP. Over the years, its basis on the WEP security scheme vulnerabilities were identified; for this reason, WPA is no longer considered secure[9].
- **WPA2** (Wi-Fi Protected Access Ver2) Introduced in 2006, is an upgraded version of WPA. It replaced the RC4 cipher with AES encryption algorithm tied with the use of CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) method and provides a solution against a wide range of attacks, including brute force and replay attacks. In addition, WPA2 supports both personal pre-shared key and enterprise authentication methods, making it suitable for both home and business environments. In 2017 a vulnerability called KRACK was discovered; for this reason WPA2 is no longer considered completely secured, but is still widely deployed[10].
- **WPA3** (Wi-Fi Protected Access Ver3), released in 2018, is the latest and most secure wireless security protocol to date. It builds on the strengths of WPA2 while addressing some of its vulnerabilities. WPA3 uses GCMP-256, an encryption method stronger than WPA2's CCMP. One of the key improvements in WPA3 is the introduction of SAE, a secure key establishment protocol that replaces the WPA2 Pre-Shared Key (PSK) mode. SAE offers resistance against offline dictionary attacks by ensuring a more secure handshake, even when users choose weak passwords. Additionally, WPA3 includes forward secrecy, which prevents attackers from decrypting old traffic if they later discover the network's password. Some attacks that were found to be successful under WPA3 are such as some types of denial-of-service attacks and host side downgrade attacks. These are mostly mitigated in the protocol or are triggered via the use of WPA3's WPA2 backward compatibility features [11].

EVALUATION METHODOLOGY

A virtual machine running the latest stable release of Kali Linux, available from Offensive Security Ltd., was chosen to minimize compatibility issues. Kali Linux was selected because it is pre-installed with all necessary tools, requiring only configuration and testing before auditing. A virtual PC was used for the testing environment due to processor compatibility issues with the network interface card. An ALFA AWUS036AXML Wi-Fi 6 (802.11ax) Tri-band network interface card was used for multi-band monitoring, supporting 2.4 GHz, 5 GHz, and 6 GHz bands and ensuring compatibility with Kali Linux. As illustrated in Figure 6, a dual setup of externally mounted 9dBi tri-band antennas was used to reduce RF shielding caused by the vehicle's metal chassis and improve the antenna line of sight.

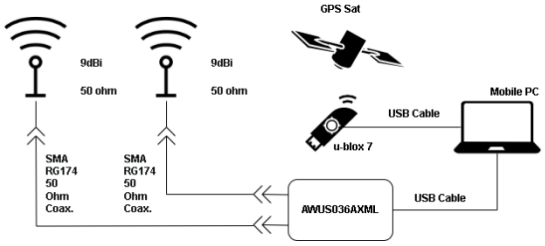

Figure 6
Collection System Wiring Diagram

GPS

A global positioning system module was required for collected data to be coupled with geo-spatial coordinates: a USB GPS receiver that can directly integrate with GPS service daemon "GPSd." The selected module was a u-blox 7 GNSS USB module that can provide up to a 10 Hz refresh rate with a positioning error of approx. 4 meters and uses GPS, GLONASS, QZSS, and SBAS systems to provide positioning information. Currently, it is only supported on Linux, OpenBSD, and NetBSD systems and can be directly integrated with Kismet for pairing positional data with collected information.

KISMET

Data collection was managed utilizing Kismet. This is an open-source network analyzer that can support applications such as an intrusion detection tool, wardriver, and packet capture tool for multiple wireless/wired protocols; it utilizes available RF sources to monitor and collect network traffic. As illustrated in Figure 7, Kismet permits the selection of RF sources and can be configured to monitor specific channels/bands.

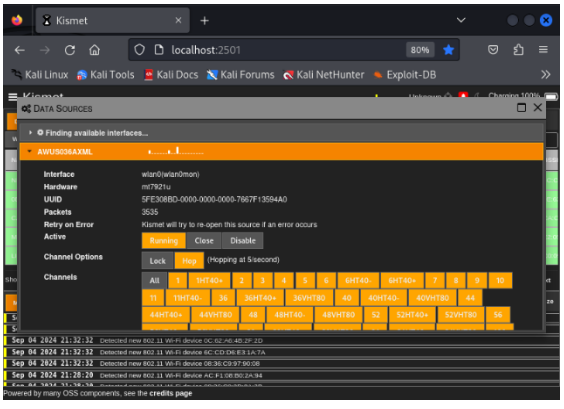

Figure 7
Configuration of Kismet Data Sources via Web Portal

The default output generated by Kismet's operation is a log file with the [.kismet] extension, which contains all the data gathered by Kismet, such as device information, packets, and GPS coordinates. Two file formats will be collected for this audit: [.kismet] and [.wiglecsv]. The [.kismet] log file can later be parsed into other formats using Kismet's native tools, while the [.wiglecsv] format allows for easier data analysis via Python. Table 1 provides the column structure and descriptions for the Kismet-generated [.wiglecsv] log file and collected parameters.

Table 1
CSV Structure of Kismet Generated [.wiglecsv] Log File

Field Name	Description
MAC	Media Access Control Address
SSID	Service Set Identifier
AuthMode	System capabilities (Security, Modes)
FirstSeen	First timestamp seen.
Channel	Integer channel value for the observed signal.
RSSI	Received Signal Strength Indicator
CurrentLatitude	Observed latitude
CurrentLongitude	Observed longitude
AltitudeMeters	Estimated position altitude
AccuracyMeters	Estimated position accuracy
Type	Signal Type (i.e. WIFI)

Area/Route Sample

The region selected for the study was Caguas, Puerto Rico, the fifth most populous municipality on the island (127,244 people), encompassing all three major population zones: Rural, Suburban, and Urban. The routes covered an estimated 27.66 km per iteration, ensuring coverage of all major zoning areas, as defined by the municipality's urban planning map: Rural General (R-G), Forest (B-Q), Intermediate Residential (R-I), High-Density Residential (R-A), and Urban Town Center. Two iterations per route were conducted to ensure accuracy, accounting for factors like vehicle speed, obstructions, and undetected access points. To minimize errors, transit speed was limited to 60 km/h (approx. 38 mph)[12].

Data Analysis Methods

The [*.wiglecsv] log file for each iteration is imported via the "pandas" Python library to a structured data frame that permits data manipulation/analysis. Entries are filtered to remove

devices that travel with auditor such as mobile device, or automobiles can continuously broadcast beacons that would be captured by Kismet. Entries are then grouped by MAC addresses as this will remove duplicate entries from dataset once formatted. The following entries are queried:

- Encryption Protocol Utilized (Count Per Configuration)
- Access Point Manufacturer (Count per device discovered.)
- 802.11 Channel Used (Count of Band Used/Channel/Frequency)
- Point Mapping of APs Discovered

Results from these queries are exported to separate [*.csv] files for further review and analysis.

RESULTS

A total of 13,981 APs were identified as part of wardriving activities, with an average linear density of 605.3 AP per km. Discovered APs were mapped utilizing "folium" Python library, APs points were color-coded as per their broadcasted security capabilities. From the generated AP mapping, it can be identified that rural routes such as PR#1 (Figure 7) and PR#788 (Figure 8), even though many access points were found along the route sections, showed some sections with scarce access point density; these sections correspond to less developed areas of county forest land. In comparison to PR#789 (Figure 9), Sub-Urban (Figure 10) and Urban (Figure 11) routes showed consistently higher access point densities throughout the wardrive. Additionally, interference from other devices appeared to be minimal in rural areas, while urban environments experienced higher levels of signal overlap and network congestion. Table 2 outlines several collected APs for each route and the calculated linear density for each route.

Table 2
Discovered AP and Linear Density

Route Name	# APs	Route Length [km]	Linear AP Density [#AP/km]
PR#1	1,148	8.82	130.2
PR788	1,321	7.11	185.8
PR789	1,327	2.35	564.7
Sub-Urban	3,982	4.23	941.4
Urban	6,203	5.15	1204.5
Total	13,981	27.66	-

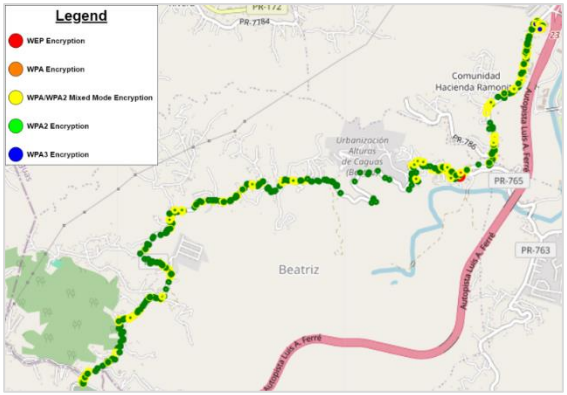

Figure 7
PR#1 Route – Access Point Mapping

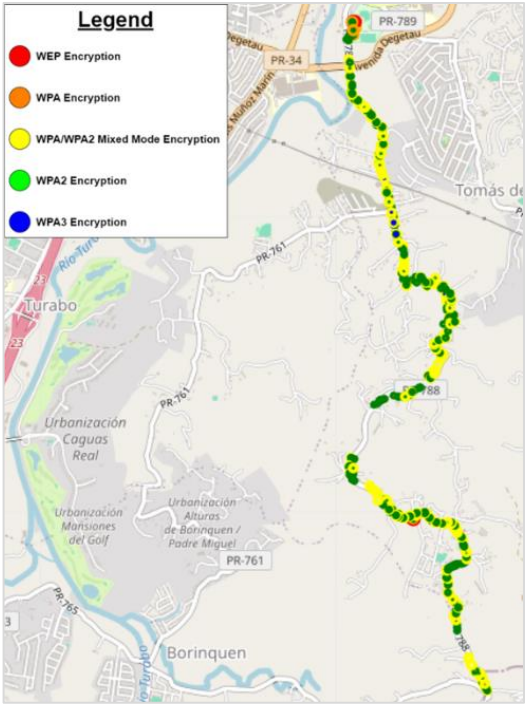

Figure 8
PR#788 Route – Access Point Mapping

Figure 9

PR#789 Route – Access Point Mapping

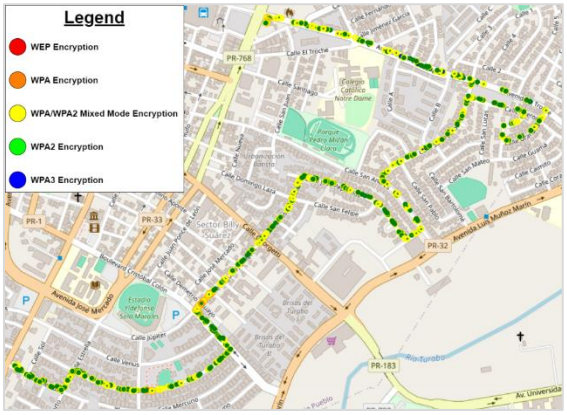

Figure 10

Sub-Urban Route – Access Point Mapping

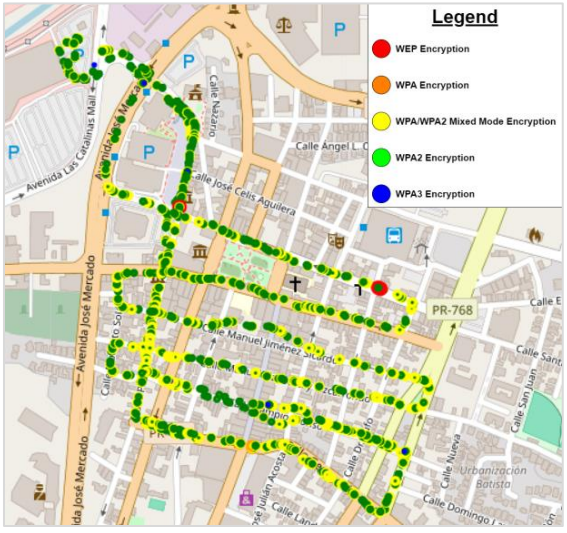

Figure 11

Urban Route – Access Point Mapping

Access Point Vendor Identification

The MAC addresses were analyzed from the collected beacon packets to identify the registered access point manufacturers. This analysis was conducted by extracting the first three bytes of the six-byte MAC address or the Organizational Unique Identifier (OUI) and comparing results with the publicly available OUI registration table (MA-L) published by IEEE Registration Authority. The analysis revealed that the predominant access point manufacturer was ARRIS Group, Inc., accounting for 19.19% of the total distribution of devices observed, indicating a strong presence of ARRIS devices. Technicolor Delivery Technologies Belgium NV was the second most prominent manufacturer, which comprised 8.39% of the total distribution. Table 5 outlines the top five manufacturers of discovered APs.

Table 5

Top 5 Access Points with Distribution Percentage

Access Point Vendor	%Dist
ARRIS Group, Inc.	19.19%
Technicolor Delivery Technologies Belgium NV	8.39%
NETGEAR	7.50%
SERNET (SUZHOU) TECHNOLOGIES CORPORATION	5.02%
Google, Inc.	3.68%

Identified AP Channel Distribution

Channel distribution was identified to be predominantly within the 2.4 GHz range; this corresponds to 90.42% of all access points broadcasting within the 2.4 GHz spectrum. This can signify the presence of older access points as 2.4GHz communications are typically used in older equipment and as 5GHz was more widely adopted from the introduction of the IEEE 802.11n standard that uses both 2.4GHz and 5Ghz frequency bands. Although the newer Wi-Fi 6 or 802.11n/ax standard does use the 2.4Ghz band for communication, it can be detected that especially for beacon packets collected in rural routes such as PR#1 and PR#788, the 5GHz bands were less present in comparison to the Sub-Urban and Urban routes.

Identified Encryption Protocol Distribution

Insecure encryption protocols were identified in all runs, including the outdated WEP (present to some degree in all runs) and the WPA protocol. The predominant encryption protocol observed across all runs was WPA2, with usage surpassing 60%. This indicates reliance on older access point technology, as certification requirements for Wi-Fi CERTIFIED™ devices mandate using the WPA3 encryption protocol for all newer devices after 1 July 2020 [13].

Overall, the use of the most recent WPA3 protocol was minimal, at 0.52% at its lowest (PR#1) and 4.90% at its highest (PR#789). This indicates that, at best, 95.10% of the detected access points were not compliant with the newest encryption standard. It was observed that a distribution of 22.52% of mixed modes of encryption was detected, with WPA-PSK-CCMP+TKIP and WPA2-PSK-CCMP+TKIP appearing at a low of 7.92% (Urban Route) and a high of 26.27% (PR#788 Route) with all distribution of 12.02%, second only to [WPA2-PSK-CCMP][WPA-AES].

Table 6
All Runs – Encryption Protocol Distribution

Encryption Protocol	%Dist
[WPA2-PSK-CCMP]	71.48%
[WPA-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP]	12.02%
[WPA-PSK-CCMP] [WPA2-PSK-CCMP]	10.49%
[WPA2-PSK-CCMP+TKIP]	2.75%
[WPA3-PSK-CCMP]	1.70%
[WPA3-UNKNOWN-CCMP]	0.69%
[WPA2-UNKNOWN-CCMP]	0.28%
[WPA2-OWE-CCMP]	0.18%
[WPA-PSK-CCMP]	0.14%
[WPA-PSK-CCMP+TKIP]	0.11%
[WEP]	0.08%
[WPA2-PSK-TKIP]	0.06%
[WPA-PSK-TKIP]	0.02%

CONCLUSION

From the findings discussed in previous sections, it can be inferred that the current state of IEEE 802.11 communications security in Caguas, Puerto Rico, is vulnerable to exploits. The analysis demonstrates that the systems detected employ outdated security measures during all trials. It is particularly surprising to find access points still using outdated encryption protocols like WEP and WPA, which are highly susceptible to attacks and have multiple known vulnerabilities. It was observed that 14.96% of networks identified can support TKIP as their encryption protocol and was most seen in beacons that advertised mixed mode operation for WPA2/WPA. These mixed modes are intended as backward compatibility features to allow connection with older devices. However, this leaves a large gap in security as network security will be the level of its least secure host. These observations come at a time when the outdated WPA2 is being replaced by its successor, WPA3, designed to address well-known security vulnerabilities, such as the KRACK attack. Although exploiting these vulnerabilities requires a considerable level of expertise, and patches can provide some protection, users are still at risk. It was noted in the analysis the low level of beacons advertising an access point using WPA3 encryption, 2.39% of overall detected access points for all runs and less than 3% individually for each route. This is concerning as this security scheme has been released/available since 2018, and newer devices after July 2020 mandate the use of the WPA3 encryption protocol. From the findings, it can be deduced that there is a gap in Wi-Fi security practices in Caguas, Puerto Rico, regardless of whether the location is urban or rural, which in turn reflects a gap in security awareness. This is an incremental problem that increases in magnitude as time and expanded use of wireless devices is/are increased, and newer versions of the IEEE 802.11 are pending release. Ideally, this can be addressed through direct educational campaigns aimed at informing users about the potential risks of hosting an unsecured access point and the dangers of

becoming a victim of cyber-attacks. Ultimately, the responsibility of having a secure wireless network is dependent on the end-user or network administrator. However, with the reality of the apparent low proliferation of information security knowledge, possible solutions may require intervention from internet service providers in the form of requiring routine equipment upgrades or changes in equipment default configurations. To ensure that the system can be at its least vulnerability, the following steps can be taken to secure a personal Wi-Fi network:

- Set the security protocol to WPA2 or WPA3 if available, as these provide better encryption than older methods like WEP/WPA.
- Do not use TKIP, including any security setting with TKIP in the name.
- Disable features that are not in use, such as WPS, WPA/WPA2 Mixed Modes.
- Change the AP default administrator credentials, such as login and password, to something unique and, ideally, randomly generated.
- Change the AP default/preconfigured SSID and PSK to be unique and, ideally, randomly generated. This strengthens the system against dictionary-based attacks and mitigates some vendor-specific vulnerabilities.
- Enable the router's firewall, restricting access only to known personal devices.
- Hide or avoid broadcasting your SSID, as this can help obscure your network from malicious scanners.
- Regularly update your router's firmware to ensure you have the latest security patches, which can help guard against new threats.
- Regularly monitor connected devices to detect any unauthorized access.

REFERENCES

[1] Kaspersky. (2023). *What is wardriving? Definition and explanation*. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-wardriving. [Accessed: August, 2024]

[2] World Bank. (August, 2024). *World Bank Open Data*. [Online]. Available: https://data.worldbank.org/country/puerto-rico. [Accessed: August, 2024]

[3] United States Census Bureau. (2023). *Census Bureau QuickFacts: Puerto Rico*. [Online]. Available: https://www.census.gov/quickfacts/fact/table/PR/PST045222

[4] M. S. Gast, *802.11 Wireless Networks*, 2nd ed. O'Reilly Media, 2005

[5] J. Henry, B. Hart, B. Gupta, and M. Smith, *Wi-Fi 7 in depth: Your guide to mastering Wi-Fi 7, the 802.11 be protocol, and their deployment*. Pearson Education, 2024. [E-book]

[6] National Institute of Standards and Technology (2007) *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*. Special Publication 800-97 [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-97.pdf

[7] Cisco. (2023). *802.11 association process explained. Cisco Meraki Documentation*. [Online]. Available: https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/802.11_Association_Process_Explained [Accessed: August 2024].

[8] C. P. Pfleeger, and S. L. Pfleeger, *Analyzing computer security: A threat.* Pearson Education International, 2012.

[9] J. Dion, *WiFi hacking: Wireless penetration testing for beginners*. Packt Publishing, 2024.

[10] C. P. Kohlios, and T. Hayajneh, "A comprehensive attack flow model and security analysis for Wi-Fi and WPA3." in *Electronics*, vol. 7, no 284. 2018 [Online]. Available: https://doi.org/10.3390/electronics7110284

[11] A. Halbouni, L. Y. Ong, and M. C. Leow, "Wireless security protocols WPA3: A systematic literature review." in *IEEE Access*, vol. 11. pp. 112438-112450, 2023 [Online] doi: 10.1109/ACCESS.2023.3322931.

[12] JP.PR.GOV (2007) *Mapa de Calificación Caguas*. [Online]. Available: https://jp.pr.gov/catalogo-de-calificacion/ [Accessed: August 2024]

[13] S. Orr, and T. Derham. (2020). *Wi-Fi Alliance® Wi-Fi® Security Roadmap and WPA3™ Updates*. [Online]. Available: https://www.wi-fi.org/system/files/202012_Wi-Fi_Security_Roadmap_and_WPA3_Updates.pdf