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

Author: Miguel A. Iglesias Santiago
Advisor: Dr. Alfredo Cruz
Electric & Computer Engineering and Computer Science

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, 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.

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 as a potential method for exploitation. 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 This comes at a moment when the now outdated Wi-Fi Protected Access protocol or WPA2 is replaced with its next iteration, WPA3, to correct now well-known security vulnerabilities[3].

Background

The IEEE 802.11 standard or 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 exchange 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 now known as “Wi-Fi 0” standard; it as gone thru multiple named amendments that each build upon its previous implementation to improve speed, security and reliability as greater requirements are needed as it represents one the world’s most widely used wireless computer networking protocols[4][5].

Problem

The combination of expected growth in communications availability/use in the upcoming years following historic trend and a population with a perceived low digital/cybersecurity literacy is a dangerous combination that can lead to a loss in all three security principals 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.

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 comes pre-installed with all necessary tools, requiring only configuration and testing before auditing. For multi-band monitoring, an ALFA AWUS036AXML Wi-Fi 6 (802.11ax) Tri-band network interface card was used, supporting 2.4 GHz, 5 GHz, and 6 GHz bands, and ensuring compatibility with Kali Linux. Figure 1 illustrates collection system wiring diagram.

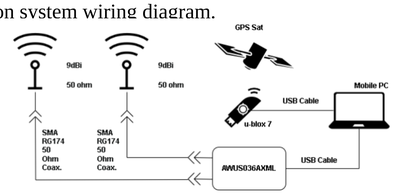

Figure 1 Collection System Wiring Diagram

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 a multiple of wireless/wired protocols, it utilizes available RF sources to monitor and collect network traffic. As illustrated on Figure 2 Kismet permits selection of RF sources and can be configured to monitor specific channels/bands.

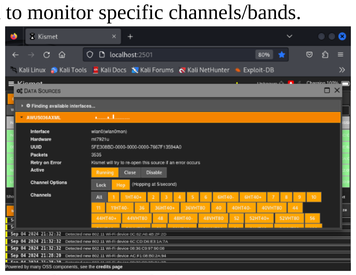

Figure 2 Configuration of Kismet Data Sources via Web Portal

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. To ensure accuracy, two iterations per route were conducted, accounting for factors like vehicle speed, obstructions, and undetected access points.

The [*.wiglecsv] log file for each iteration is imported via the use of the “pandas” python library to a structured data frames permits data manipulation/analysis. 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)

Results and Discussion

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 the PR#1 and PR#788, even though many access points were found along the route sections these showed some sections with scarce access point density; these sections correspond to less developed areas of county forest land. In comparison to PR#789, Sub-Urban and Urban 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 number of collected APs for each route and 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	1148	8.82	130.2
PR788	1321	7.11	185.8
PR789	1327	2.35	564.7
Sub-Urban	3982	4.23	941.4
Urban	6203	5.15	1204.5
Total	13981	27.66	-

In all runs, insecure encryption protocols were identified, 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 the use of the WPA3 encryption protocol for all newer devices after 1 July 2020 [6]. 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 a distribution of 22.52% of mixed modes of encryption were 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]. Figure 3 displays AP mapping for Urban Route.

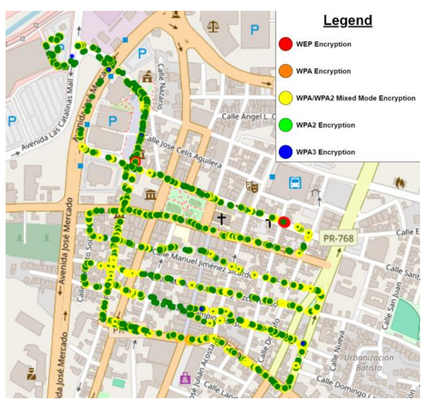

Figure 3 Urban Route – Access Point Mapping

Conclusions

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. 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.

Future Work

Future work may involve expanding data collection efforts to include additional geographic areas, as well as conducting comparative studies to enable a more comprehensive analysis.

Acknowledgements

I would like to thank my advisor, Dr. Cruz, for guidance and advice, as well as my family and friends for their support.

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] 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