Oct 20th, 1:25 PM - 1:50 PM

Hijacking Wireless Communications using WiFi Pineapple NANO as a Rogue Access Point

Shawn J. Witemyre
University of North Georgia, sjwite3948@ung.edu

Tamirat T. Abegaz
University of North Georgia, tamirat.abegaz@ung.edu

Bryson R. Payne
University of North Georgia, bryson.payne@ung.edu

Ash Mady
University of North Georgia, ash.mady@ung.edu

Abstract
Wireless access points are an effective solution for building scalable, flexible, mobile networks. The problem with these access points is often the lack of security. Users regularly connect to wireless access points without thinking about whether they are genuine or malicious. Moreover, users are not aware of the types of attacks that can come from "rogue" access points set up by attackers and what information can be captured by them. Attackers use this advantage to gain access to users' confidential information. The objective of this study is to examine the effectiveness of the WiFi Pineapple NANO used as a rogue access point (RAP) in tricking users to connect to it. As part of the preliminary study, a brief survey was provided to users who connected to the Pineapple to evaluate the reasons why users connect to RAPs. The result of the cybersecurity pilot study indicated that lack of awareness played an important role. Specifically, users unknowingly connect to rogue wireless access points that put at risk not only their devices, but the whole network. The information collected in this research could be used to better educate users on identifying possible RAPs and the dangers of connecting to them.

Location
KC 462

Disciplines
Information Security | Management Information Systems | Technology and Innovation

Comments
Addressing reviewer concerns:

There are several spelling, grammatical, and punctuation errors throughout the paper. Also, seems to have some issues with clarity and conciseness. Overall a good read and interesting topic. If areas are addressed it would be acceptable.
Thorough review with a number of minor changes, addressed some areas of clarity and conciseness in three sections. Also addressed concerns of second reviewer, but did not implement the table presenting the results or describe the experimental design more clearly, as this limited pilot is not representative of the final research setup.

INTRODUCTION

Wireless access points provide a cost-effective and easy-to-deploy solution for building a flexible, mobile, indoor-outdoor network. Current wireless communication standards, such as WiFi (IEEE 802.11n), enable engineers to build efficient and cost-effective wireless access points (Pradeepkumar et. al., 2017; Tzur et.al, 2015). However, a growing problem associated with wireless access points is the need to secure them. Often users connect to wireless access points without giving a second thought to whether the access point is genuine or an impostor. For instance, if the device is configured to automatically connect to a particular WiFi access point via a named SSID (service set identifier) that does not use encryption, then the device is imminently vulnerable to rogue access points (RAPs). Attackers use this advantage to launch attacks to gain access to users' confidential data.

For a RAP to work, the computer system or mobile device must connect to the RAP first. Such a connection generally requires user's intervention provided that the WiFi connection is not configured automatically. Switching off the auto-connect option in user devices will significantly reduce the RAP's available attack surface. Unfortunately, there is a trade-off between convenience and security. Users often prefer the convenience of automatically connecting to their preferred wireless networks. And many end-user devices, including PC and Mac laptops and most mobile phones, will remember the name of an access point and connect to it automatically whenever that network is present, unless the user specifically deletes that network's SSID from his or her device.

The objective of this research is to measure the effectiveness of tricking users into connecting to RAPs. Specifically, the research hopes to answer questions like: How are users fooled into connecting to rogue access points? And, what can network engineers do to better secure networks? In fact, regardless of how secure a network is, if a user account is compromised through a RAP, the entire organization's network is at risk. With a better understanding of why users connect to rogue wireless access points, network engineers can implement strategies that build safer and more secure networks.

In addition, this research seeks to uncover clues to better educate users on how to identify possible RAPs and the dangers of connecting to them. The research hopes to show how easy it is to set up RAPs, within minutes, and to intercept network communications with an intent to steal sensitive data, as a means of educating unwary users of the privacy dangers involved in insecure wireless networks.

BACKGROUND

Most studies conducted on the security of wireless access points focus on how to identify RAPs in the network and suggest ways to remove them (Agrawal & Tapaswi, 2015; Alotaibi & Elleithy, 2015, 2016; Anmulwar et. al, 2014). Very few published studies focus on how to protect networks from rogue wireless access points, with even less exploration of the reasons why users connect to RAPs (Zegzhda et. al, 2017, Zheng et. al., 2014). Currently, several devices capable of creating rogue WiFi APs are available on the market. Among the most widely used are Ubertooth One, Cape Networks, EyeQ, NetBeez, HackR, and WiFi Pineapple (Morrison et. al., 2017; Hill, 2013; Eric Geier, 2018). For this research, we will focus on WiFi Pineapple NANO because of its ease of use and cost-effectiveness.

The anatomy of the WiFi Pineapple is described in Figure 1. WiFi Pineapple NANO looks like a USB flash drive, which can easily be inserted into any computer or laptop to launch the attack. The device is developed by Hak5 LLC (Hak5, 2018). It contains a Micro SD storage expansion slot, a standard USB port, a high gain radio, and configurable status LED, among other features. It has several useful modules that enable penetration testers to launch various attacks on the clients connected to it. For instance, the PineApp module is used to conduct man-in-the-middle (MITM) and phishing attacks (Morrison et. al., 2017). Overall, this device can be set up as a rogue wireless access point within minutes, ready for attack.

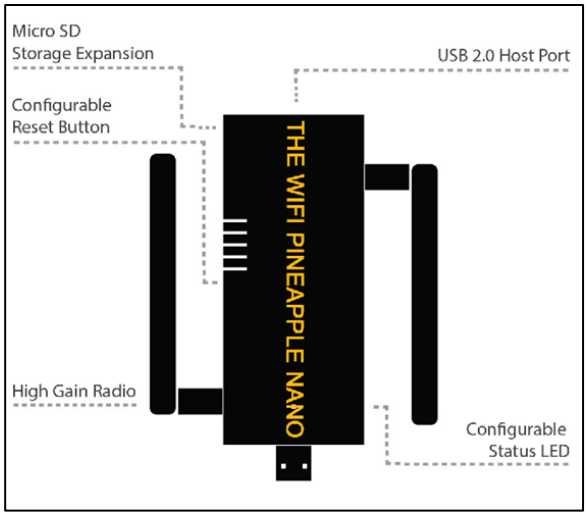


Figure 1: Anatomy of the WiFi Pineapple NANO (image adapted from https://www.wifipineapple.com/pages/nano)

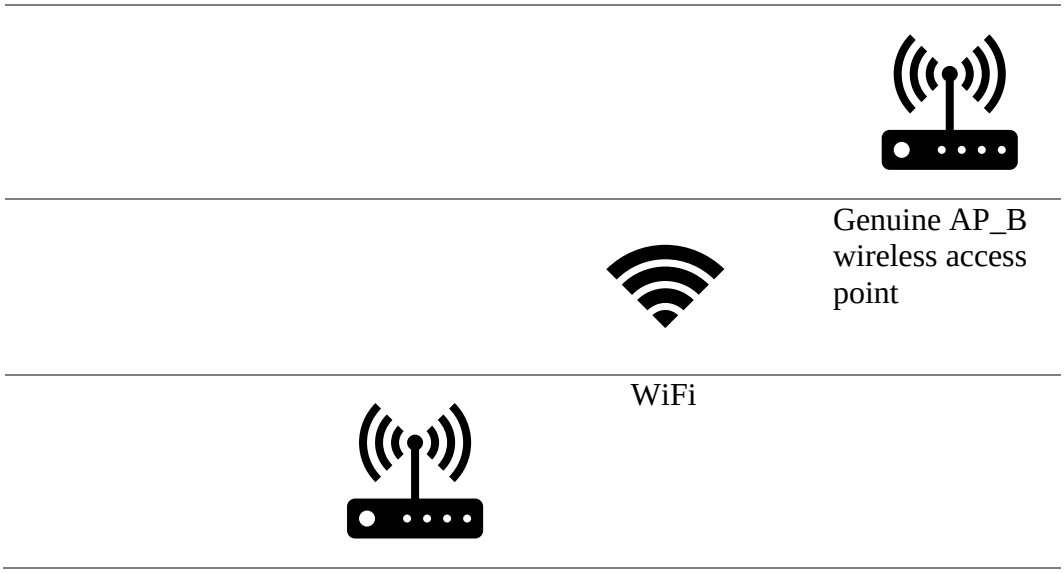
IMPLEMENTATION

First Phase

The first phase of the proposed design is to set up the rogue wireless access point on the WiFi Pineapple NANO. The rogue wireless access point was named “AP_B” (real network name redacted) to match a legitimate access point in a network controlled by one of the authors. This access point was set up in a home environment, specifically a multi-tenant rental shared by five college students, with frequent visitors. The point of this phase is to set up the rogue wireless access point in a way such that no users would suspect that the AP_B access point is a rogue access point.

Second Phase

The second phase of the proposed design was to trick users into connecting to the rogue wireless access point. As stated, the rogue wireless access point has a name similar to the genuine wireless access point. The WiFi Pineapple NANO user interface was used to modify the SSID of the rogue wireless access point to AP_B. Then, the interface was used to connect the rogue wireless access point to the internet through the genuine wireless access point.



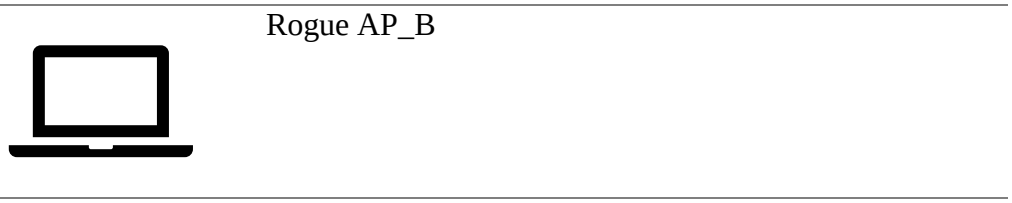


Figure 2: Tricking users into connecting to a rogue wireless access point

Phase Three

The third phase of the design was to count how many users connected to the rogue wireless access point and possibly find out why users connected to the RAP. The rogue wireless access point was connected to a test website that counts the number of connections made with it. Also, a link to a short survey was sent to the users who connected to the rogue access point to answer the following questions: Do you know what a rogue wireless access point is? Where you aware that this is a rogue wireless access point? Are you aware of the dangers of connecting to a rogue wireless access point? Do you check to see what wireless access points your devices connect to? Have you ever had any training or education about connecting to wireless access points?

Figure 3: Counting user connections to the rogue wireless access point and issuing a survey to users

Phase Four

The final phase in the proposed design was to disconnect the rogue wireless access point from the home network and collect the feedback from the survey. No malicious software was installed, and no user credentials were collected or compromised in this research, but users were educated on the WiFi Pineapple tool and how it could have been used to steal login information and other sensitive personal data, implant malicious code, and the like.

RESULTS

This study examined the effectiveness of the WiFi Pineapple NANO as a rogue access point (RAP) in tricking users to connect to it. Unfortunately, the study did not get IRB approval for use on campus, because there was no process in place for reviewing technology-based or information security projects, so a pilot study was conducted in the lead author's home with multiple college-age housemates. Of the pilot study that was conducted, five users connected to the rogue wireless access point. All five users filled out the survey that was provided after connection to the rogue wireless access point. The results of that survey are listed below. One of the five respondents answered "yes" to whether they knew "what a rogue wireless access point is." None of the five respondents answered "yes" to "were you aware that this is a rogue wireless access point." One of the five respondents answered "yes" to "are you aware of the dangers of connecting to a rogue wireless access point." Two of the five respondents answered "yes" to "do you check to see what wireless access point your devices connect to." Only one of the five respondents answered "yes" to "Have you had any training or education about connecting to wireless access points."

In the free-form section of the survey, users were "shocked" to discover that they had connected to a rogue wireless access point. Not only were they unaware of what a rogue wireless access point was, they were unaware of what a man-in-the-middle attack was. Users reported being "terrified" to discover the details of what type of information could be captured from man-in-the-middle attacks. Users said that they would be more careful when connecting to wireless access points in the future. With more knowledge about rogue wireless access points, users said they would be on the lookout for rogue wireless access points that had similar SSID names to genuine wireless access points.

This experiment conducted in the study has made users more aware of rogue wireless access points and the security vulnerabilities that can arise from connecting to them. After a basic understanding of what rogue wireless access points are and the dangers of connecting to them, it is hopeful that users will be more cautious when connecting to wireless access points in the future.

Finally, this experiment revealed how easily users are tricked into connecting to rogue wireless access points and how quickly and easily rogue wireless access points can be set up. With just a WiFi Pineapple NANO that costs under $100.00 and a USB power source, attackers can set up a rogue wireless access point within minutes. Attackers using a rogue wireless access point can implement a man-in-the-middle attack, phishing, and more. A WiFi man-in-the-middle attack can monitor a user's online activity, intercept login credentials, and even steal credit or debit card information. Only when users are armed with information on the dangers of RAP WiFi hijacking can they hope to defend themselves from RAPs.

CONCLUSIONS

The objective of this study was to examine the effectiveness of WiFi Pineapple NANO used as a rogue access point, (RAP) in tricking users to connect to it. As part of the preliminary study, a survey was provided to users who connected to the RAP to evaluate the reasons why users connect to RAPs. The result of the pilot study indicated that lack of awareness played an important role. Specifically, users unknowingly connect to rogue wireless access points that can put at risk not only their devices but the whole network. The information collected in this research could be used to better educate users on how to identify possible RAPs, as well as the dangers of connecting to them.

The researchers in this study believe that educating users on rogue wireless access points and the security and privacy risks of connecting to them could reduce the number of users connecting to rogue wireless access points. In the future, we plan to conduct a wider study on a university campus, as soon as the Institutional Review Board is equipped and able to process cybersecurity-focused research projects. We hope the information collected from a large-scale study would further improve the understanding of why users connect to rogue wireless access points. With a better understanding of why users connect to rogue wireless access points, network engineers can build safer and more secure networks.

REFERENCES

Agrawal, N., & Tapaswi, S. (2015). Wireless rogue access point detection using shadow honeynet. *Wireless Personal Communications*, 83(1), 551-570.

Alotaibi, B., & Elleithy, K. (2016). Rogue access point detection: Taxonomy, challenges, and future directions. *Wireless Personal Communications, 90*(3), 1261-1290.

Alotaibi, B., & Elleithy, K. (2015, May). An empirical fingerprint framework to detect Rogue Access Points. In *Systems, applications and technology conference (LISAT)*, 2015 IEEE Long Island (pp. 1-7). IEEE.

Anmulwar, S., Srivastava, S., Mahajan, S. P., Gupta, A. K., & Kumar, V. (2014, February). Rogue access point detection methods: A review. In *Information Communication and Embedded Systems (ICICES), 2014 International Conference on* (pp. 1-6). IEEE

Eric Geier, https://www.networkworld.com/article/3251664/lan-wan/review-5-top-hardware-based-WiFi-test-tools.html, accessed, August 13, 2018

Gupta, S., Chaudhari, B. S., & Chakrabarty, B. (2016, August). Vulnerable network analysis using wardriving and security intelligence. In *Inventive Computation Technologies (ICICT), International Conference on* (Vol. 3, pp. 1-5). IEEE.

Hak5, https://www.hak5.org/gear/wifi-pineapple/docs, accessed, August 13, 2018

Hill, R. (2013, August). Phantom network surveillance UAV/Drone. In DEFCON Conference.

Li, X., & Li, X. (2017, December). Rogue Access Points Detection Based on Theory of Semi-Supervised Learning. In *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage* (pp. 35-44). Springer, Cham

Morrison, L. P., Team, B., Nguyen, B., Kannan, S., Ray, N., & Lewin, G. C. (2017, April). AirChat: Ad hoc network monitoring with drones. In *Systems and Information Engineering Design Symposium (SIEDS)*, 2017 (pp. 38-43). IEEE.

Pradeepkumar, B., Talukdar, K., Choudhury, B., & Singh, P. K. (2017, September). Predicting external rogue access point in IEEE 802.11 b/g WLAN using RF signal strength. In *Advances in Computing, Communications and Informatics (ICACCI)*, 2017 International Conference on (pp. 1981-1986). IEEE.

Tzur, A., Amrani, O., & Wool, A. (2015). Direction Finding of rogue WiFi access points using an off-the-shelf MIMO–OFDM receiver. *Physical Communication, 17*, 149-164.

Zegzhda, D. P., Moskvin, D. A., & Dakhnovich, A. D. (2017). Protection of WiFi network users against rogue access points. *Automatic Control and Computer Sciences, 51*(8), 978-984.

Zheng, X., Wang, C., Chen, Y., & Yang, J. (2014, October). Accurate rogue access point localization leveraging fine-grained channel information. In *Communications and Network Security (CNS)*, 2014 IEEE Conference on (pp. 211-219). IEEE.