Zachary Munro

Computer System Security

Professor Ming Chow

30 April 2018

# Portable Hacking: Implementation, Risks, and Defense

## ABSTRACT

My project is the initial stages of a proof of concept for a mobile hacking device. It will combine some elements of packet sniffing and a modified Man in the Middle attack to gain access to someone's personal information. My portable hacking device will be built off of a Raspberry Pi 3, a 2.5A portable power supply, and a 3.5in LCD touch screen. The attack will be executed as follows: packet sniffing will allow me to find the victim's router's BSSID, then I send de-authentication messages to the router to bump the user off. Then a fake WiFi access point is created with the same name as the victim's original router, and their device will auto-connect to this new access point. From here, the possibilities are quite extensive and range from monitoring network traffic to tricking the victim into installing malware on their computer. The device now has nearly complete control over what the victim sees on the internet. If the victim's traffic is encrypted then it cannot be viewed directly, but it is possible to replace an https (encrypted) page with a similar looking http (unencrypted) page so that they are tricked into sending sensitive information in the clear to the device.

# INTRODUCTION

Portable hacking has been evolving to be more and more effective, and is becoming more threatening as other technologies advance. For instance, if a WiFi jammer needs to be very close to the router it is jamming, the jammer could be run from a raspberry pi, with a portable charger, and attached to a drone that is flown to the roof of a house that would otherwise be unreachable. After all, security cameras rarely are pointed straight up in the air.

In the early days of portable hacking, practices such as warwalking or wardriving were common, where the attacker would walk or drive around detecting wireless access points and looking for vulnerable ones to attack. The term originally comes from the 1983 movie *War Games* where the main character locates unprotected dial-up networks to hack into (Freeman). Other similar terms were created as well, such as warchalking, where cyber warfare enthusiasts would mark on sidewalks with chalk where vulnerable WiFi networks were reachable.

The tools and methods of attack have multiplied since those days but the principle is still the same: gain access to someone's WiFi and use it for malicious purposes. The Evil Twin attack that is used in this case study is designed to kick the victim off their router and onto the unsecured one. This works only if the network being attacked is not secured, the common security measure being WPA2 encryption, requiring a password to log onto the network.

The impacts of this attack are incredibly severe, and is not to be trivialized. It may seem like most networks are secured (your home and work likely are) but public coffee shops, libraries, and airports are all places where unsecured public networks make users vulnerable to these types of attacks, and defending against them is no trivial feat (Noman).

## TO THE COMMUNITY

The field of portable hacking is growing, and new, more powerful hardware is becoming more affordable and available for recreational hacking. The hardware used in this project could be bought for under $100, and the information needed to implement these techniques is not hard to locate online. Many popular websites such as null-byte.wonderhowto.com and lifehacker.com have articles explaining how to do similar projects to this on a low budget (OccupyTheWeb) (Klosowski). All the software that was used was free and openly available to the public.

The use of the internet by the general public and especially WiFi has grown more rapidly than knowledge of cybersecurity guidelines were able to be taught. Due to this, there exists a false sense of security among many people. I have had multiple people tell me “Why should I use a secure WiFi connection? No one is interested in what I am doing? I have $3 in my debit account, what are they going to steal?” I relate to this sentiment very strongly, but with these kind of attacks, it doesn’t necessarily have to be about taking information from you. If the attacker can trick you into installing malware on your computer then the whole game has changed; they can now use your computer’s processing power as part of a botnet or perform illegal cyber attacks FROM your computer, so that the blame cannot be traced back to them and instead falls on you. Identity theft is another all too real possibility, and is easy with the information the attacker could gather. You have more than just what is in your bank account to protect, and what has been mentioned here is only a fraction of what could be done to a victim of this attack.

The goal of this project is to show people how easily and discreetly severely malicious attacks can happen, and hopefully spread awareness that WiFi is not magic, but a tool that comes

with inherent risks and responsibilities. If the possibilities for attackers to steal your information in this way seems scary, that's because it is.

## DEFENSES

One of the easiest ways to defend against WiFi attacks like the one in this study is to make sure to use HTTPS encrypted web pages as much as possible when on public networks. HTTPS is the secure, encrypted version of HTTP (Hypertext Transfer Protocol) and is the protocol for the way that applications communicate over the internet. When your computer loads an HTTP web page, all the information on that page was sent in the clear, or unencrypted, over the network, and anyone who wanted to could see what it was. Similarly, if you enter your credit card information onto an HTTP page and hit "Send", that information is sent unencrypted over the network and can be seen by an attacker. With HTTPS, all your sensitive information that was entered on the page was securely encrypted before being sent over the network. This is not a perfect way to stop attackers but it does help.

One of the best ways to stop Evil Twin attacks is to turn off auto-connect to WiFi on your devices. Since auto-connect for WiFi is only based on the name of the network, it is easy for your devices to accidentally hook up to an unsecure network where your traffic can be monitored without you knowing. Never connect to networks that you don't know the legitimacy of.

One final method of preventing Evil Twin attacks, and just a general good practice to follow, it to use a Virtual Private Network (VPN). It encrypts all incoming and outgoing traffic by using an encryption algorithm with a key on both sides (Noman). There are many other benefits to using a VPN and different ways that someone can go about setting one up. They are

easy to use and, if set up properly, provide a greatly increased amount of security with only sacrificing a little internet speed. There is a reason that many enterprise companies require employees to use them.

Lastly, if you are wishing to defend against this happening on your own network, be sure to use a WPA or WPA2 encrypted network. This means that all users will need to provide a password, and possibly a username, in order to connect to the network. This prevents attackers from gaining easy access and monitoring network data, as they will first need to find out the credentials to get onto the network, so try not to leak them.

## SUMMARY

The goal of this project was to create a proof of concept of a portable hacking device that would perform a Evil Twin attack and possibly continue to maliciously exploit the victim. I was able to accomplish the first goal and get the victim kicked off their network, and connected to a fake network created by the device. With more time, I would have continued to complete a MitM attack which would then forward the victim's data to the user's router after passing through the device, most likely using Ettercap. The device would store the information that was sent or possibly export it to a database online. Incoming traffic to the user would be intercepted and the packets could be modified using Scapy. A request to go to gmail.com could be redirect to an HTTP version of the website that I fabricated where the victim would unknowingly enter their gmail credentials in which I would intercept, allowing me to gain access to their email account. As mentioned previously, the possibilities are extensive and range in maliciousness. This is only one path I could have taken with the project, and there is more to portable hacking than just WiFi

attacks. Things like bluetooth connections and airdrops are other avenues of attack that a portable hacking device could take advantage of. Don't be fooled into thinking cyber attacks are only done by a hermit in their basement on a supercomputer.

Portable hacking devices are a growing field and are popular projects for the casual hacker. They are easier to create than most people think and are more dangerous than most people are willing to believe. WiFi security needs to be taken seriously, and studies have shown that people are incredibly willing to hook up to vulnerable networks just so that they can get free WiFi for a few minutes (Noman). Evil Twin attacks and Man in the Middle attacks are especially scary since they are not noisy, and are hard to notice. Hacking is rarely what it is seen like in movies; you won't see a stream of number running down your screen like in the Matrix, or smoke coming out the back of your computer, and your anti-virus and malware don't make you impervious to any attack. Portable hacking devices can be much more complex and vary greatly in how they attack. This project was only a proof of concept to show the dangers that we need to protect ourselves against, but it is not a comprehensive examination of all of the dangers posed to us by these devices. At the end of the day, the best defense is to be informed, skeptical, and don't take risks with public access points.

SOURCES

---


“Wardriving: Unauthorized Access to Wi-Fi Networks.” *Information Systems Security* 15.1 (2006): 11–15. Web.

Noman, Sinan Ameen, et al. "Mitigating Evil Twin Attacks in Wireless 802.11 Networks at Jordan." *International Journal of Computer Science Issues (IJCSI)*14.1 (2017): 60-8. *ProQuest.* Web. 2 May 2018.

Web, Occupy The. “How to Hack Wi-Fi: Creating an Evil Twin Wireless Access Point to Eavesdrop on Data.” *NullByte*, WonderHowTo, 18 July 2013, null-byte.wonderhowto.com/how-to/hack-wi-fi-creating-evil-twin-wireless-access-point-eavesdrop-data-0147919/.

Klosowski, Thorin. “How to Build a Portable Hacking Station with a Raspberry Pi and Kali Linux.” *Lifehacker*, Lifehacker.com, 29 Oct. 2015, lifehacker.com/how-to-build-a-portable-hacking-station-with-a-raspberr-1739297918.

Jeremy Martin, "The art of casual WiFi Hacking", *CISSP-ISSAP*, 2009.

Modi, Vishwa, and Chandresh Parekh. "Detection & Analysis of Evil Twin Attack in Wireless Network." *International Journal of Advanced Research in Computer Science* 8.5 (2017)*ProQuest.* Web. 3 May 2018.