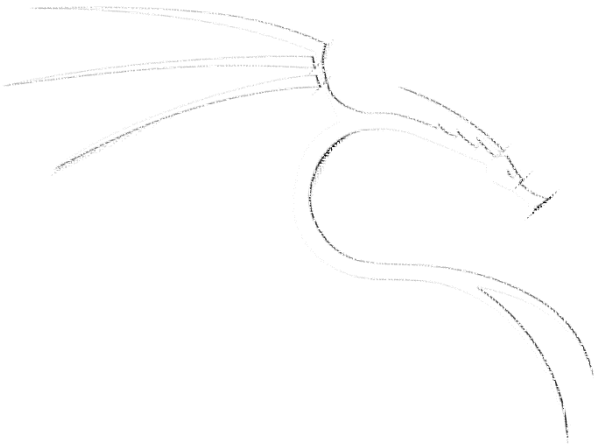
Asymmetric Manipulation of Network Authentication Protocols

Evil Twin Attack

Khir Henderson[1], Advisor: Kevin Kornegay[2]

[1, 2] Morgan State University, Baltimore, Maryland
[1, 2] Department of Electrical and Computer Engineering
[1] khhen2@morgan.edu, 443-509-5902



Student Signature	Date	Advisor Signature	Date

Contents

Abstract— **In the emerging era of "script kiddies", Internet of Things or IoT devices and an ever increasing ease of access to both; the very nature of our cyber security is at risk. This paper explores the entire gamut of manipulation of wireless network through the use of an evil twin attack. The project uses publicly available tools such as Kali Linux, and embedded systems adapted to use the internet such as the Zedboard to reveal important security flaws in Morgan State University's own public network authentication protocol as well as WiFi networks protocols as a whole. The results will prove how little money, processing power and even effort is needed to infiltrate the security of publicly operated networks no matter how large the size or security. This information is important because both proper security methods must be developed as well as educating the user base of public networks in order to reduce human errors which account for the number one cause of security flaws.**

Keywords—Cyber Security, Evil Twin Attack, Internet of Things, Scripting

I. INTRODUCTION

WiFi or WLAN defines any wireless local area network that is based on the Institute of Electrical and Electronics Engineers 802.11 standards. WiFi is less secure than other local area. These waves exist in the atmosphere or "free space", and because of this can be possibly used to for sabotage and espionage. The Internet of things (IoT) adds another accessible layer. This poses a threat to the security and safety of our cyber world. Today, technology exists that allows almost anyone to access and manipulate these signals without having to unencrypt the signal in anyway. This type of technology has been developed and fine-tuned at the corporate level, but as technology develops it is becoming easier and easier to access. This research suggests the exploration of technology that can be developed with portable tools and with low budget. Through the exploration of the uses of small time tools, such as portable USB transceivers we can define the risk our devices have in the future as technology develops, giving us ample time to develop protections against cyber espionage.

The following sections will briefly go over the tools and terms necessary to understanding the breadth of this project.

A. Penetration Testing

Penetration testing is an evaluation of security of an Information Technology (IT) system or infrastructure that attempts to exploit specific vulnerabilities that jeopardize the safety of the information and secure access to the system. Usually these tests exist in the form of a software attack that looks exploit security weaknesses in the OS, network protocol, user input security, or

anything that will allow the tester to exploit and disrupt the security and gain access to important information. James P. Anderson a leader of the formation of penetration testing describes the general attack sequence as:

- Determine feasibility of a particular set of attack vectors
- identify high-risk vulnerabilities from a combination of lower-risk vulnerabilities exploited in a particular sequence
- identify vulnerabilities that may be difficult to detect with automated network or application vulnerability scanning software
- assess the magnitude of potential business and operational impacts of successful attacks
- test the ability of network defenders to detect and respond to attacks
- provide evidence to support increased investments in ds security personnel and technology

Over the years as technology developed, more tools where created to address and test security flaws in newer security.

B. Kali Linux

Kali Linux is an open source Linux Distribution that is designed to provide tools for information security training and penetration testing services provided by Offensive security. The importance about this distribution is that it is preinstalled with over 600 penetration testing tools that include information gathering, vulnerability analysis, web attacks, exploitation tools forensics tools, stress testing, sniffing & spoofing, password attacks, maintaining access, reverse engineering, hardware hacking, and reporting tools. It is very surprising what one can do with this very light weight distribution alone.

The list of tools can be found at http://tools.kali.org/tools-listing.

Kali has a custom built kernel that is patched for wireless injection this is needed for wireless testing. Airmon and Aireplay are to important tools provided by the tool aircrack-ng., one of the more important tools in Network exploitation.

1) Aircrack-ng

Aircrack-ng is listed as an 802.11 WEP and WPA-PSK keys cracking program that can recover information once enough data packets have been captured. The package in itself is a suite of tools for wireless network audits. Aircrack-ng is capable of performing a variety of attacks such as Denial of Service, rouge access points, and evil twin attacks.

2) Airmon-ng

Airmon-ng, a tool compiled with aircrack-ng, is simply a script that enables monitor mode on wireless interfaces. This means the computer can now monitor all traffic received. Monitor mode is one of seven modes that 802.11 wireless cards can operate in. This script enables packet analysis without having to associate with an access point (AP) or ad hoc network. Monitor mode is limited to monitoring only a single channel at a time but aircrack-ng circumvents this limitation by scanning all channels and

compiling the results. This is done by sending by sending 128 packets total; 64 to the Access Point and 64 to the client itself for each deauth.

3) Aireplay-ng

Aireplay-ng generates traffic. This script that also exists as a script assembled with Aircrack-ng, is very important in this project because the packets sent are called disassociating packets used in deauthentication or deauth attacks. Deauthentication in this case is used to force clients to disconnect to the particular access point and require it to reconnect and authenticate.

Limitation: Deauthentication attacks even though are wireless access must be in a physically close proximity for the wireless card transmissions to reach the target computer. There needs to be enough transmit power for the packets to be reached and heard.

C. Scripting

Scripting or commonly called Bash (Bourne-Again SHell) or Shell scripts are computer programs ran by a UNIX based command line interpreter. In this case we are using Bash scripts for the root access terminal in Kali Linux. Bash scripts make the bulk of the tools used in Kali Linux and are essentially designed for user interaction. Bash Scripts are very robust, they are usually one file text documents that take up very little space and can be edited in any text editor.

D. Script Kiddies

A script kiddie is new term for people in programming culture that rely on premade exploit programs and scripts without truly understanding what they do. The "age of script kiddies" is very important because the technology and programming culture is continuing to grow. There is a growing number of easy to use, step- by step tutorials that allow many unknowledgeable people to use exploitation tools without truly understanding the repercussions. The programming culture is a very big deal and must be handled delicately. It is reported that the head of the C.I.A was hacked by a group of teenagers using methods commonly found online. One must be very wary of releasing a script because it can easily be used for unethical and nefarious methods even if it wasn't the main intention of the release of the exploit. Releasing exploits give script kiddies immense power with very little effort needed.

E. Internet of Things

The Internet of Things is composed of the trend of many internet connected devices and objects that are not traditionally connected like personal computers or devices. These "things" add another accessible manipulatable layer to the 802.11 network. These devices exist in many different forms from low end raspberry-pi's and Arduino's to dedicated access points to high-end embedded. In this case these devices can covertly be placed in the physical proximity of the network being exploited allowing ease

of use on an anonymous, uneasily trackable platform. Easily connected to a compatible USB Wifi card, these IoT devices hold low small profiles and can be hidden in everyday objects, and can last for long amounts of time with remote access to the network. The Raspberry Pi and the Zedboard are two IoT capable devices that both run will be focused on during this project.

1) Rasberry-Pi

The Raspberry-Pi is an easily accessible model for low end users, it can easily be equipped with a WiFi usb dongle, and run a live version of Kali Linux distro designed just for the Pi. This makes it a prime target for users interested in remotely targeting networks.

2) Zedboard

The Zedboard is characterized is an all-programmable system on chip or SOC. It is characterized as a high-end device with a Dual Core, 512 MB DDR3 and 256 MB of Flash memory, and is powered by 12 V. This device is more powerful and can be used for a short period of time to run multiple scripts at much and can be used to collect as much information as possible.

F. Public Network Security

Public WiFi security is very important, being on the same network as a potential exploiter is very dangerous. When a user uses a public network they must understand the implications of their choice. No matter what connecting to a public network is the least secure way?

G. Evil Twin Attack

An evil twin attack is the implementation of a rouge or unauthorized Wi-Fi access point that appears to be a legitimate one. In this case it is direct spoof of the network being exploited. This type of attack can be nearly undetectable if the user is not expecting an attack. An evil twin attack on a public network looks just like a hiccup in normal behavior which happens often with public networks which are normally seen as unreliable. It is difficult and costly to defend against Evil twin attacks because it requires both user education and mutual authentication practices.

H. Assymetric Attack

Asymmetric attacks or asymmetric warfare describes an attack where small income produces a large outcome. The income can range between energy spent, time spent, or resources, and the outcome can be described as the general effect of the attack. The main idea of asymmetric attacks is to have the largest effect while using minimal resources.

The following sections will describe the design and methods used to asymmetrically attack Morgan State University login authentication protocol for MSU-Wireless.

II. METHEDOLOGY

A. Materials

Since this is a cyber-attack resources are minimal. This attack runs through a single bash script. Kali Linux is used because it is already preconfigured for use with most of the necessary tools. An add-on script is added for initial setup and installation for tools needed by the script.

B. Design

This attack design was designed with asymmetric setup and operation in mind. This means that this attack is designed to use the limited amount of resources as possible. The exploit is based off a script called Linset. Linset is designed by a Spanish forum user of seguridadwireless.net which translates as Wireless Security. Linset is originally designed as an evil twin attack to capture and verify the password for WPA2 secured networks. Linset set up a rouge AP point and asked the user to input its network password through a vague and poorly set up web page. Linset essentially worked as follows

- Scan and select the network
- Capture handshake
- Create a web interface in temporary files
- Mount a rouge AP using FakeAP imitating the original AP
- Create a DHCP and DNS server to redirect all requests to Host
- Launch the web interface
- Deauthenticate all existing users on original network, and point them to the rouge AP
- Point to the web interface that asks user to enter in their password
- Verify entered password matches with captured WPA2 handshake
- Save password and disconnect server

This evil twin attack major flaw is that users never enter in their WPA password through a web interface. This surely would trigger even the casual of users that something “fishy” is going on. This alerts the user that there is something wrong with their network ruining the exploit and doesn’t prove to be a security threat. Evil Twin attacks will never work well in this manner for WPA passwords. Instead this attack modifies the premade script used for WPA2 hacking to do something entirely different.

Instead of hacking WPA2 for private networks this type of exploit works perfectly for public networks that require user authentication to gain access to the network. This means we can create an exact mirror copy of the login page where instead of

sending the username and password to the webserver it is saved to the DNS server and a text file on the host of the rouge AP. Since the webpage is identical it is nearly impossible to tell the difference between two login pages, especially if you are not expecting this type of attack.

The modified script works as follows:

- Scan and select the network
- Create a web interface in temporary files
- Mount a rouge AP using FakeAP imitating the original AP
- Create a DHCP and DNS server to redirect all requests to Host
- Launch the web interface
- Deauthenticate all existing users on original network, and point them to the rouge AP
- Point to the web interface that asks user to enter in their username and password
- Save password to text file and disconnect rouge AP

C. Implications of MSU-Wireless Network

The login page for MSU-Wireless is shown in figure 1, the page is simple and static, easy to duplicate simply by viewing the page source and copy and pasting. The only modification that is really needed is modifying the input values to save the input files to a text file. Since the MSU-wireless uses the same login information for practically all of its services, THE ENTIRE MORGAN NETWORK IS COMPROMISED at this point. As you can see there is no security or defense set up for this level of attack. This makes all further levels of security absolutely meaningless.

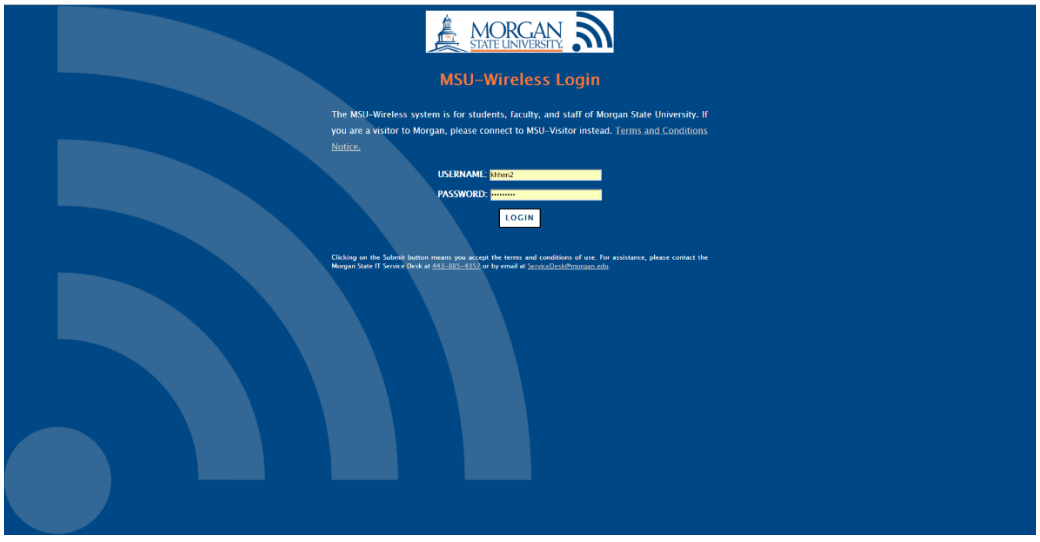


Figure 1: The login page for MSU-wireless

D. Spoofing credibility

The level of spoofing for this exploit can easily be designed to a level where the user inputs the username and password in the spoofed without question to about 90% by copying the page source of the code. The other 9% can be spoofed through meticulous tricks such as url spoofing, more layers of webpages such as spoofing the authentication redirects and ensuring the page source files are duplicated correctly. 99% of credibility because if someone was to compare the pages source code side by side, one could find the differences, but the likeliness of that happening is very low.

E. Skills Needed

In the "Age of Script kidding" it does take knowledge to design this type of attack, but not necessarily any skill to run or modify this attack. In order to design an evil twin attack needed here is a list of skills and knowledge that are needed by these attacks. This list of skills and knowledge used in order to modify the current script for this exploit.

- HTML
- CSS
- PHP
- JavaScript
- BASH shell
- DNS Web Server
- Linux command line
- Linux commands shell
- Objective coding logic
- Java
- Python

III. RESULTS

As designed, the script is able to easily obtain the SSID of any targeted network, spoof the SSID, and create a server containing the duplicated authentication page. The script also is designed to show the DNS server requests as well as the connected clients. As an added level of security the mac address is changed as well. After imputing user authentication data, which includes username and password. The script saves this information to a text file, and shutdown the server. From this point the user may find that they are not connected to the internet and may promptly try again, until they are connected.

A. Drawbacks

Certain drawbacks and limitations may affect the efficiency of the program. The first of the limitation is that physical access is required. This means that the access point must be in local range to both the user and the network. This also means

that the access point generally must exist in the same room as the target network and user. This may affect security by making it more difficult for the attacker to access the network covertly. A counter to this will be discussed in the later sections.

The second of the drawbacks is that most public networks that exist amongst large spatial areas, exist on multiple WiFi channels. This is an interesting phenomenon where you can see the same SSID multiple times. Normally the targets computer only shows the strongest network, but when the network is spoofed there may be multiple listings of the same network. This may alert the target user that something is awry. A simple fix to this is dynamically scanning the network, this is the same work around that aircrack-ng uses for its monitoring service.

B. Improvements

An improvement upon the design of the script would make the script very easy to read and to modify. The script could be improved to imitate up to 99% of the MSU-Wireless protocol. This includes the login procedure, error messages, and even the html website address. An added bonus is that the user information can actually be patched through to the real server so no lapse in connection is even noticed. The script could be modified to run automatically on any Linux device, this includes mobile, tablet and IOT applications. The script could be set up as a time scheduled application, and create an easily modifiable API for the attacker to easily modify for other unsecured network authentication sites. This unfortunately means it would be a prime target for Script Kiddies because all they would need to do is copy and paste a website's source code and change the input parameters.

IV. IOT APPLICATIONS

The Internet of Things adds another accessible layer to this attack. A user doesn't have to use a personal device such as a Linux enabled tablet, personal computer or laptop. Instead they can use an embedded system, which essentially means a small computer that is designed with a dedicated function in mind. Embedded systems can easily be adapted to access the wireless network with the inclusion of a wireless shield or USB wireless adapter. The two devices used in this project were the Zeboard and the raspberry pi.

The Raspberry-Pi is an easily accessible model for low end users, it can easily be equipped with a WiFi USB dongle, and run a live version of Kali Linux distro designed just for the Pi. This makes it a prime target for users interested in remotely targeting networks. The Raspberry-Pi is one of the most popular embedded systems, it has a lot of resources by means of user support and troubleshooting. Because of the devices popularity it already has a stable version of Kali Linux pre-built for the device and its kernel. This means it works well as "Plug-and-Play" device, term that means that there is minimal set up required. The device is cheap, and simple to use the perfect device for script kiddies.

The Zedboard is characterized is an all-programmable system on chip or SOC. It is characterized as a high-end device with a Dual Core, 512 MB DDR3 and 256 MB of Flash memory, and is powered by 12 V. This device is more powerful and can be used for a short period of time to run multiple scripts at much and can be used to collect as much information as possible. Setting up the Zedboard is a little more difficult than using the raspberry pi. The Zedboard does not have a pre-built installation to run Kali Linux a form of debian Linux that contains most of the necessary tools preinstalled. The script has to be modified to automated install the repositories' and applications needed to properly run the attack. This may take extra time and set up but once the Zedboard is properly set up persistently then that step is no longer needed. What is loses in ease of use it gains in power and function. The Zedboard is more capable of running more executions faster. It can also support higher power wireless cards.

IOT devices can be set up multiple ways covertly. They run on low power and can be powered by a battery pack for complete remote connectivity. It is easy to hide these internet connected embedded systems because they are so small. These devices can have a large effect with little effort.

V. IMPLICATIONS

There are many considerations and tradeoffs for this project. The implications of a program like this being released to the masses without proper counter measures and awareness could return disastrous results. In short the major impact of this project is that security authentications for semi-private logins authentication protocol must change in order to secure the network.

A. Economic

The economic implications could mean that public networks would have to spend money implementing more security layers for each network that chooses to increase their security, because public networks are so large securing the network may and changing the protocol may take large amounts of time, resources and money.

B. Environmental

The environmental impact for this project is low. Since this project exists entirely in the cyber realm it does not affect the environment as much. Although, because a lot of people use public network, there may be a switch from public wireless networks to tethered networks or fully private networks. This may increase electricity usage slightly, and also may take up physical space. There is very little environmental tradeoff with this project because the program exists entirely as software, and the energy used when running the script is minimal.

C. Sustainability

This project is sustainable because it exists as code. Code is easily adaptable as time changes, and it is very difficult to completely destroy once it is released to the public. A possible issue with this is that for anyone that intends for the program to "die off" or disappear it may be extremely difficult to make that happen.

D. Ethical

For Ethical hackers it is very difficult to release vulnerabilities without alerting criminals of current weaknesses. It is very important that that the ethical hacker releases security vulnerability in a way that minimizes any extra damage from its release. This can be achieved by contacting companies directly and encouraging immediate patches to network systems. A way this can be achieved better is along with finding the vulnerability is to add on countermeasures to the vulnerability. A tradeoff for releasing the program is the possibility that the program or the idea gets into the wrong hands. Ultimately ignorance is not a good solution because as technology develops, along with the openness of the internet this information will reach more and more eyes no matter what.

E. Social

Socially this project could and change how people view the internet, their information and safety. After viewing this project there should be a social movement towards awareness that normalizes proper security protocols and awareness that public networks are not safe. Awareness is the best counter measure for security breaches because a majority of security breaches happen because of a weakness in the user and not the network. In this case, the network is insecure and users must understand that. Socially people would be less likely to enter personal data, such as bank account information, or important passwords on public networks. They should understand that they are almost giving their information away.

F. Political

This attack could easily have political implications. Just recently the head of the CIA was hacked due to a vulnerability in his personal security protocols. He and the companies he allowed access to his personal information were too lax about their security protocols. This is a similar situation to the status of the security protocols here. Whether it is risking high profile politician's personal information or pushing for legislature to improve security of public networks this project has relatively large implications.

VI. CONCLUSION

The main take away from this project should be awareness of how easy this attack can be played out. This information is important because both proper security methods must be developed as well as educating the user base of public networks in order to reduce human errors which account for the number one cause of security flaws.

REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] K. Elissa, "Title of paper if known," unpublished.

[4] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[5] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[6] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[7] **http://www.ericgoldman.name/security/8-exploits-and-attacks/21-evil-twin-attack-explanation source**

ECE Senior Design Project Report Check-List

1. Have you discussed in detail the **economic** considerations and trade-offs involved in your design?

- ❑ Yes, On Page _____, Paragraph(s) _____.
- ❑ No. Briefly explain in the space below why you felt that such considerations were not relevant to your design.

---

2. Have you discussed in detail the **environmental** considerations and trade-offs involved in your design?

- ❑ Yes, On Page _____, Paragraph(s) _____.
- ❑ No. Briefly explain in the space below why you felt that such considerations were not relevant to your design.

---

3. Have you discussed in detail the **sustainability** considerations and trade-offs involved in your design?

- ❑ Yes, On Page _____, Paragraph(s) _____.
- ❑ No. Briefly explain in the space below why you felt that such considerations were not relevant to your design.

---

4. Have you discussed in detail the **manufacturability** considerations and trade-offs involved in your design?

- ❑ Yes, On Page _____, Paragraph(s) _____.
- ❑ No. Briefly explain in the space below why you felt that such considerations were not relevant to your design.

---

5. Have you discussed in detail the **ethical** considerations and trade-offs involved in your design?

- ❑ Yes, On Page _____, Paragraph(s) _____.
- ❑ No. Briefly explain in the space below why you felt that such considerations were not relevant to your design.

---

6. Have you discussed in detail the **health and safety** considerations and trade-offs involved in your design?

- ❑ Yes, On Page _____, Paragraph(s) _____.
- ❑ No. Briefly explain in the space below why you felt that such considerations were not relevant to your design.

7. Have you discussed in detail the **social** considerations and trade-offs involved in your design?

- ❑ Yes, On Page _____, Paragraph(s) _____.
- ❑ No. Briefly explain in the space below why you felt that such considerations were not relevant to your design.

---

8. Have you discussed in detail the **political** considerations and trade-offs involved in your design?

- ❑ Yes, On Page _____, Paragraph(s) _____.
- ❑ No. Briefly explain in the space below why you felt that such considerations were not relevant to your design.

Student Signature *Date*

Advisor Signature *Date*