ASEE'S VIRTUAL CONFERENCE

At Home with Engineering Education JUNE 22 - 26, 2020 #ASEEVC

Paper ID #28609

Credential Harvesting using Raspberry Pi

Dr. Tae-Hoon Kim, Purdue University Northwest
Dr. Ge Jin, Purdue University Northwest

Ge Jin, D.Sc, is currently an associate professor in the Department of Computer Information Technology and Graphics at the Purdue University Calumet. He teaches computer game development, computer graphics and animation, as well as computer information technology courses at the undergraduate and graduate levels. Prior to joining Purdue University Calumet, he was a postdoctoral research scientist at the George Washington University, Department of Computer Science. Professor Jin holds a B.S. in Computer Science from Peking University, China, and an M.S. in Computer Science from Seoul National University, South Korea. He earned his Doctor of Science degree in Computer Science with a concentration in computer graphics from the George Washington University. His research spans the fields of computer graphics, virtual reality, computer animation, medical visualization, and educational game development. He is a member of the ACM SIGGRAPH, ASEE, and International Society of Virtual Rehabilitation.

Dr. Michael Tu

Michael Tu, Ph.D. in Computer Science, associate professor of Computer Information Technology, Director of the Center for Cybersecurity , and the Point of Contact of the NSA/DHS Designated National Center of Academic Excellence in Cyber Defense Education at Purdue University Northwest. Dr. Tu's areas of expertise are information assurance, digital forensics, cybersecurity education, and cyber physics system security. His research has been supported by NSA and NSF and published over 40 peer reviewed papers in prestigious journals and peer reviewed conference proceedings. Dr. Tu has over 14 years of college teaching and research experiences in cybersecurity and digital forensics. Dr. Tu is a CISSP, Certified Ethical Hacker (CEH), & AccessData Computer Examiner (ACE).

Mr. Tianyang Guan, Purdue Northwest University

Credential Harvesting using Raspberry Pi

Abstract

Due to advances in digital technology, cyberattack grows faster than other crimes. According the cybersecurity statistics for 2020, Gartner forecasts the worldwide cybersecurity spending reaches up to $133.7 billion in 2022. As the growth of cyber threats, the practical cybersecurity education is gaining its importance. Hands-on experience through the lab exercise becomes crucial component because students tend to learn thing better when observing how practically it’s been applied in real system. The most common attacks are phishing and social engineering, which more than 60% of business experienced in 2018. Recently, the phishing attack in Wi-Fi, “Wifiphisher”, which utilizes automated phishing agent to public Wi-Fi to steal the credential information or infect victim’s device with malware, has been introduced. Here, we propose the “Phishing Wi-Fi” man-in-the-middle attack utilizing Wi-Fi, HTTP, and DNS for cybersecurity education. Since virtualization technology, commonly used in cybersecurity education, is not suitable for wireless lab exercise, we use Raspberry Pi, small and affordable computer, to build Wi-Fi Phishing lab. In this paper, we introduce the concept and guideline of the Phishing Wi-Fi attack using Raspberry Pi including building, delivery method, and countermeasures.

1 Introduction

Over the past decade, Internet became an essential component not only in human daily life but also in many different sectors including economy, industry, and etc. Such a growth of Internet is mainly due to technology advancement, such as mobile devices, wireless technology, Internet of Thing (IoT), and etc., and service development, such as social network, online banking and remote health system, online game, and etc. Currently, Industrial Internet of Thing (IIoT) is one of the driving forces of Industry 4.0, which enables the connection among factories to monitor and improve the system. However, connecting things to the Internet comes with great challenges such as security. According to Privacy Rights ClearingHouse (n.d.), the number of data breach incidents continuously increases. The total number of data breach incidents from 2005 to 2017 is more than 7,730. The victim of data breach includes not only private sector but also public sectors such as national infrastructure, corporations, financial, healthcare, and etc. [1,2]. Cyber-attacks are not limited in data breach, which results in business loss due to the damage on the trust level of the business from customer, partners, and stakeholders [3]. The consequences of cyber-attacks are not limited to financial loss. Attack on physical infrastructure such as power grid and power plant may cause more serious problem, for example, power blackout in Brazil, StuxNet worm, and etc. [4-6]. As the Internet dependency grows, the cyber-threats are also growing. In order to protect the system against the cyber threats, researchers focus on countermeasures, secure communications, intrusion detection, and etc. Another effort against cyber treats is education. According to Frost and Sullivan [7], a global shortage of 1.8 million cybersecurity professionals is projected by 2022. U.S. Bureau of Labor Statistics projected 37% of information security job growth from 2012 to 2022 and announced that more than 200,000 cybersecurity jobs in U.S. are not filled every year.

Education in cybersecurity draws more attention from K-12 to adult. Recently, U.S. Congress has urged to develop high-quality educators to cybersecurity education [8]. Many researchers studied teaching methodologies to maximize the student learning. One of the key components in engineering and science education is a laboratory-based course, which includes a practical hand-on exercise. Many academic institutes developed the laboratory-based courses to help students to accelerate their learning in different types of laboratories such as real, simulation, or online [9]. According to Findley, students learn 90% by practicing while 20% by reading [10]. Especially in cybersecurity education, hands-on exercises through the laboratory became an essential component of the course because it provides students with an opportunity to learn and observe how the concepts can be applied. Generally, the lab in cybersecurity education prefers virtualization technologies due to the cost restriction and ease of deployment and usage. Virtualization technology becomes an essential component in cybersecurity education because virtually isolated multiple systems can be created, modified, tested, and deleted easily with little or no additional cost. SEED labs, developed by Professor Du at Syracuse University [12], is the most popular security labs used in many Academic Institutes, which use virtual machine to emulate the Linux based computer system for security educations.

One of the most common cyber-attacks is a phishing attack, which mostly uses phone, email, malware, web application, and etc., to steal credential information (e.g., username and password) or money. There are various types of phishing attacks such as deceptive, malware-based, key and screen loggers, session hijacking, and etc. [13]. Even though phishing attack is one of continual threats, not many practical cybersecurity labs have been developed. In this paper, we introduce phishing attack in Wi-Fi environment including one of the important components in cybersecurity, adversarial thinking which inspires student to attack the system to learn how to protect the system [11]. Regarding on cybersecurity education, recently GenCyber funded by National Security Agency (NSA) introduced 6 Cybersecurity Concepts, Defense in Depth, Confidentiality, Integrity, Availability, Think Like an Adversary, and Keep in Simple. Our proposing Phishing Wi-Fi module can cover 3 out of 6 concepts, Defense in Depth, Confidentiality, and Think Like an Adversary.

Implementation of Wi-Fi phishing attack requires Wi-Fi capable device with several servers, web, DNS, and DHCP. However, virtualization technology cannot build such environment. Recently, affordable low-cost small computer, Raspberry Pi, has been introduced. Because of its small portable size and relatively high computing power with many available features, it is suitable for Wi-Fi phishing implementation. In this paper, we will introduce Wi-Fi phishing hands-on lab using Raspberry Pi.

The rest of paper is organized as follows. Section 2 introduces Raspberry Pi, current features, system specifications, and applications. Section 3 describes the structure and building procedure of phishing Wi-Fi attack module using Raspberry Pi. Learning topics and delivery method are discussed in Section 4. Finally, Section 5 concludes the paper.

2 Raspberry Pi

Raspberry Pi is a small computing device that can be adapted in many different field of area due to its portable small size with high performance computing. Besides, it includes other attractive features such as networking, I/O port, Wi-Fi, and etc. In this section, we will introduce Raspberry Pi in terms of specification, features, requirements, and its application fields.

2.1 Introducing Raspberry Pi

Raspberry Pi was developed by Raspberry Pi Foundation based in United Kingdom (UK) to help people to teach and learn basic Computer Science with low cost high-performance computer. Raspberry Pi is low cost, credit-card sized computer introduced in 2012 as shown in Figure 1.

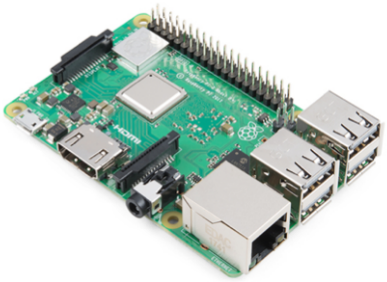


Figure 1. Raspberry Pi 3 B plus

Initially two models are developed, Model A and Model B in Raspberry Pi version 1. The difference of two models is different number of supporting USB ports and size of memory (i.e., 256 MB and 512 MB). Raspberry Pi has been upgraded with Model B and there are three versions. The most recent version, Raspberry Pi 3 Model B plus, has CPU of 1.4GHz 64-bit quad-core processor, built in dual-band wireless LAN, Bluetooth, faster Ethernet, 4 USB ports, and etc. Table 1 compares the specifications of different versions in Raspberry Pi model B.

Table 1. Specification comparison of different versions of Raspberry Pi model B

	Raspberry Pi 1 B	**Raspberry Pi 2 B**	**Raspberry Pi 3 B**	**Raspberry Pi 3 B+**
Released	Feb. 2012	Feb. 2015	Feb. 2016	Mar. 2018
CPU	700 MHz with single core	900 MHz with quad core	1.2 GHz with quad core	1.4 GHz with quad core
RAM	512 MB	1 GB	1 GB	1 GB
Storage	SDHC	Micro SDHC	Micro SDHC	Micro SDHC
USB ports	2	4	4	4
Wi-Fi	No built-in	No built-in	Built-in Wi-Fi	Built-in dual-band Wi-Fi

(Note: SDHC – Secure Digital High Capacity)

The price of Raspberry Pi is between $25 and $35 depending on the version and it comes with only a board. Additionally, it requires micro SD card to run OS, HDMI cable to display on monitor or TV, USB keyboard and mouse. Raspbian, Debian-based OS for Raspberry Pi, is provided as a default and several versions are available. Recently, other OS such as Ubuntu-mate is available. OS should be carefully selected, because each version of OS is suitable to specific version of Raspberry Pi. For example, Ubuntu-mate was built for Raspberry Pi model B. Depending on OS requirement, minimum of micro SD card size is 2 GB and portable external hard-drive can be used for additional storage through USB port. In addition, Raspberry Pi also includes GPIO (general purpose input and output) pins to connect with other electronic boards. Built-in Ethernet port allows up to 1 Gbps in latest version for Internet connection. Additional Ethernet ports can be added through USB ports. Wi-Fi is also available through built-in Wi-Fi supporting 802.11 b/g/n/ac in latest version while Wi-Fi dongle is used for the older versions.

2.2 Application areas of Raspberry Pi

Due to its small and portable size, relatively high computing power with many available features provided by its Linux-based Operating System (OS), Raspberry Pi is widely adapted and utilized in many different industry sectors such as health care, monitoring system, home automation, Internet of Things (IoT), and etc. [14-19]. Gupta and *et. al.* used Raspberry Pi to store and update the collected data from health monitoring system and alert the doctors. They used it as a database and web server to grant an access for authorized person [14]. In [15], Zhao and et. al. used Raspberry Pi as an aggregator of data from multiple wireless sensors. Wi-Fi for connection between wireless node and Raspberry Pi and client-server communication for data transfer from wireless node to Raspberry Pi were used in their project. Raspberry Pi application was extended to home automation and Rao and Uma built the home automation system using Raspberry Pi [16]. Raspberry Pi is located between router and home IoT devices to provide the updated data and remote control through Internet. Another application is surveillance system. Prasad and *et. al.* used it to collect and store the data from surveillance cameras and updated data can be seen at the smartphone through cellular network [17]. In education, Raspberry Pi is mostly used to teach programming who cannot afford a high-end computer. It is also often combined with Arduino to teach control education [22].

The performance of Raspberry Pi has been investigated by Maksimović and *et. al*, and it is shown as a perfect platform to interact with wide variety of external peripherals and access Internet using Wi-Fi, which makes it possible for remote communication [20]. In addition, several other advantages are discussed as following; small independent computer with Linux based with relatively high-speed CPU, expansion with external devices by supporting USB and Bluetooth capability, possible expansion with various electronic components via digital input and output, and etc. [20]. They also identified several features that are lack in Raspberry Pi, such as no real-time clock (RTC), diskless OS using micro-SD card, limited features from mini-Linux OS system, power consumption, and etc. [20,21]. These disadvantages may limit the usage and implementation in several applications.

3 Wi-Fi Phishing attack lab

Wi-Fi phishing attack lab requires one Raspberry Pi with two Wi-Fi adaptors and web, DNS, and DHCP servers. Each server also needs configuration to make this attack possible. In this section, we will introduce the lab scenario and setup with configurations.

3.1 Wi-Fi Phishing attack Scenario and setup

Free Wi-Fi is available in most of places in these days and most people like to use free Wi-Fi for their online activities including web surfing, online shopping, and etc. without doubting. This phishing utilizes the free Wi-Fi to find the victim. The basic idea of Wi-Fi phishing attack is to place the phishing Wi-Fi (i.e., Raspberry Pi) between public Wi-Fi and victims and provide normal Internet access to people. Phishing Wi-Fi will provide the normal Internet access to the people until victim. The architecture of Wi-Fi phishing attack is illustrated in Figure 2. Raspberry Pi will be configured to be a phishing Wi-Fi and it will connect to the public free Wi-Fi. Once it connects to the free Wi-Fi, it will start running new free Wi-Fi service as if it is part of the public free Wi-Fi to attract the victims. Victim will use it as a free Wi-Fi until he/she steps on the trap. Phishing Wi-Fi waits for victim to access designated well-known website such as Gmail, Facebook, LinkedIn, and etc. while forwards all traffic to the Internet. When victim accesses the designated website, phishing Wi-Fi redirects it to faked login webpage to harvest the credential information.

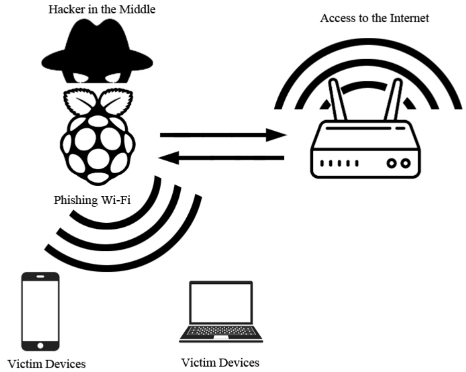


Figure 2. Wi-Fi Phishing attack scenario

3.2 Phishing Wi-Fi configuration

To build the phishing Wi-Fi, we used Raspberry Pi 3 model B+ with following specifications;

- SoC: Broadcome BCM2837B0 quad-core A53 (ARMv8) 64-bit @ 1.4GHz
- GPU: Broadcom Videocore-IV
- RAM: 1 GB LPDDR SDRAM
- Networking: 1 of Gigabit Ethernet and 1 of dual-band 802.11 b/g/n/ac Wi-Fi
- Bluetooth: Bluetooth 4.2 (BLE)
- Storage: Micro-SD
- GPIO: 40 pin GPIO header, populated
- Ports: 4 USB 2.0, HDMI, 3.5mm analogue audio-video jack, Camera Serial Interface (CSI), Display Serial Interface (DSI)
- Dimension: 82mm x 56mm x 19.5mm, 50g.
- OS: Raspbian (Debian based OS)

For the phishing Wi-Fi setup, two (2) wireless interfaces are required, one for the Internet to the public Wi-Fi and the other for the free Wi-Fi service to the victims. First, we need to configure it as a wireless hotspot with a public Wi-Fi connection, which requires packages such as udhcpd, udhcpc, dnsmasq, and hostapd. Udhcpd is to setup a Dynamic Host Configuration Protocol (DHCP) server to assign IP address for the PCs in internal network. Udhcpc is a DHCP client program to acquire IP address from existing DHCP server. The dnsmasq is to run the DHCP service. Next, access point host should be configured by editing “hostapd.conf” file. Since we are configuring for free Wi-Fi, authentication is not necessary. The path to the configured file should be set to DAEMON_CONF in “hostapd” file. Then, the access point is ready to start the service.

The next step here is to set up routing capability to forward the traffic between access point interface and wireless interface to the public Wi-Fi. For the first of all, IP forward should be enabled at “sysctl.conf” file. Then, add masquerade statement for the outbound traffic on wireless interface to the public Wi-Fi as shown below assuming wlan0 is wireless interface to the public Wi-Fi.

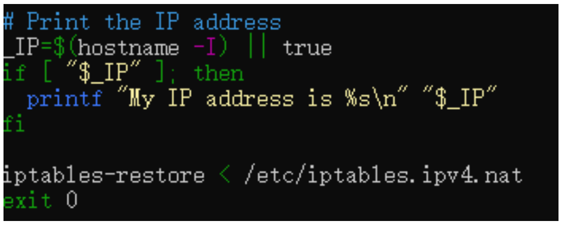
```
sudo iptables -t nat -A  POSTROUTING -o wlan0 -j MASQUERADE
```

Then, following set of commands will make it permanent

```
sudo sh -c "iptables-save > /etc/iptables.ipv4.nat"
sudo nano /etc/rc.local
```

Then, add following statement right before the “exit 0” as shown in Figure 3.

```
iptables-restore < /etc/iptables.ipv4.nat
```



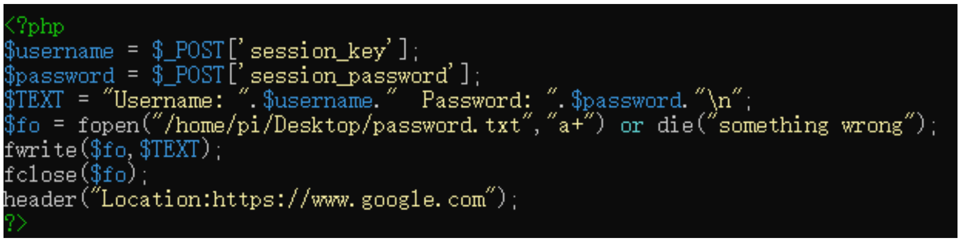
```
# Print the IP address
_IP=$(hostname -I) || true
if [ "$_IP" ]; then
  printf "My IP address is %s\n" "$_IP"
fi

iptables-restore < /etc/iptables.ipv4.nat
exit 0
```

Figure 3. Adding additional line at rc.local

Next step is setting DNS server, which will redirect designated website to faked one. DNS server requires installing two packages, apache2 for local server and bind9 for DNS. Since we configured dnsmasq, it has IP address conflict with bind9. It can be resolved by adding “bind-interface” line to “/etc/dnsmasq.conf” file. Once DNS server is installed, it will resolve the IP address from name address for all other website except target website. When target website name address is asked, it will resolve the IP address of its own to redirect it to the faked website built in phishing Wi-Fi.

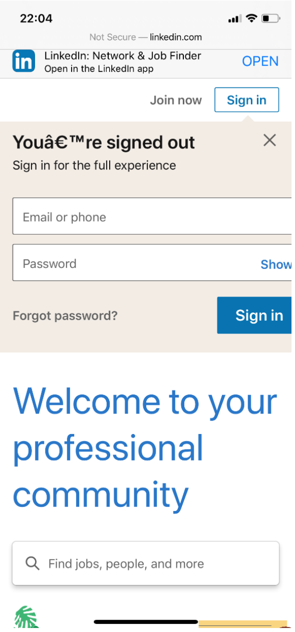
Final step is creating fake website, which will be installed in Raspberry Pi and wait for victim to access. Fake website can be created by copy the target website first page (i.e., index.html). In order to obtain the username and password, we need to write a short script to be run as an action in the webpage. Script is shown in Figure 4.



```
<?php
$username = $_POST['session_key'];
$password = $_POST['session_password'];
$TEXT = "Username: ".$username."  Password: ".$password."\n";
$fo = fopen("/home/pi/Desktop/password.txt","a+") or die("something wrong");
fwrite($fo,$TEXT);
fclose($fo);
header("Location:https://www.google.com");
?>
```

Figure 4. Script to obtain the credential information from faked webpage

Once every configuration is successfully completed, target webpage should be loaded from phishing Wi-Fi and asking for login as shown in Figure 5(a). Once victim login through this webpage, credential information will be stored in designated txt file in the phishing Wi-Fi as shown in Figure 6.

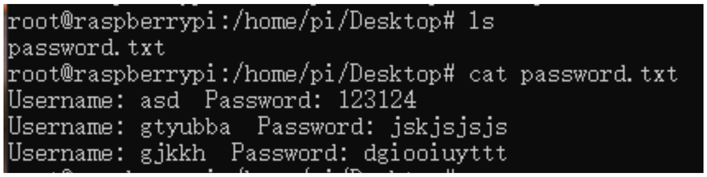


Youâ€™re signed out

Sign in for the full experience

Welcome to your professional community

Figure 5. Example of LinkedIn faked webpage



```
root@raspberrypi:/home/pi/Desktop# ls
password.txt
root@raspberrypi:/home/pi/Desktop# cat password.txt
Username: asd  Password: 123124
Username: gtyubba  Password: jskjsjsjs
Username: gjkkh  Password: dgiooiuyttt
```

Figure 6. Text file storing victim’s credential information

4 Discussion

The structure and building process of phishing Wi-Fi has been described in above. In this section, we will discuss how phishing Wi-Fi module can be delivered in class. First, we will introduce the topics that should be discussed with delivery method.

4.1 Learning topics

Before proceeding the phishing lab, students need set of knowledge about computer networking and data communication. Besides the fundamental knowledge, it requires several specific topics that student should know to understand the phishing Wi-Fi module. The topics are,

Wi-Fi network: this network uses wireless technology, which uses air as a physical medium to send the signal, which uses broadcasting mechanism. Due to this nature, wireless communication is vulnerable to eavesdropping attack. Therefore, Wi-Fi uses password not only to limit the user access but also to countermeasure this type of attack.

HTTP: HyperText Transfer Protocol (HTTP) is a server-client type application protocol used in World Wide Web, which defines the data transfer method and format. User application, such as web browser, sends a page information request to the web server and sever responses.

DNS: Domain Name System (DNS) is a hierarchical decentralized naming system to translate the name address to IP address used in Internet. IP address has been assigned to each server so that user can access through Internet. Since user prefers to remember the name instead of the number, all web servers are known as the name. Therefore, there needs a system for user to convert the name address to the number address (e.g., IP address).

These three topics should be discussed in advance to understand the phishing Wi-Fi module. Next, we will describe lab procedure and delivery method.

4.2 Delivery method

First, structure and data flow must be discussed. In Wi-Fi network, mobile device must connect to the access point (AP), which is directly connected to the Internet. For data communication, mobile device sends the message to AP first and AP forwards it to the Internet. When web server replies, AP will receive it and forward it to the mobile device. AP is working as a middle device between mobile user and Internet. At this moment, it is recommended to let students discuss how they could attack this type of network. Then, discuss man-in-the-middle attack concept. The middle device can be a vulnerable point of the network because all traffic passing through can be seen. Possible attack here is a sniffing attack, which finds the sensitive data from all by-passing data. However, this type of attack requires looking up the long list of collected traffic. Then, discuss the countermeasures for these types of attacks such as encryption.

The phishing Wi-Fi attack uses the DNS attack concept. Students need to understand the process when web application traffic flow. When user looks up the name address of the website, OS will consult DNS server to acquire the corresponding IP address. Then, web application contacts the web server for the webpage information using obtained IP address. After explaining DNS traffic flow, let students think and discuss how it would be used in attack. Then, explain phishing attack concept and process used in this paper.

In the available free public Wi-Fi area, phishing Wi-Fi device (i.e., Raspberry Pi) connects to the public Wi-Fi network and initiates the attack by starting the access point. Then, it waits until victim connects to the phishing device and it will pass all traffic as normal. When victim tries to access the website, phishing device will redirect the target website DNS traffic to its DNS server and reply back with its webserver IP address. Then, victim will be redirected to the faked webpage asking login information. After discussion, let student proceed the phishing Wi-Fi lab to understand the attack concept. Then, discuss about the vulnerabilities and possible risks of public Wi-Fi network.

4.3 Countermeasures

Avoiding phishing attack is not an easy job because there is no significant sign or evidence for non-expert user to recognize. Generally, end user training is considered to be a one of the strongest countermeasures against most of cyber-attacks. User should be aware of these types of attacks and carefully connect to public or private Wi-Fi because phishing attack is not only limited only to public are network, but it can be implemented in private network. First thing user needs to check is if it is password protected Wi-Fi. Even if it is password protected, it only countermeasures certain type of attach such as packet sniffing between mobile device and AP using encryption. Attacker may use same password and SSID and wait victim to take the bait. Using HTTPS, encryption version of HTTP, may highly avoid this type of phishing attack. So, user may need to check which HTTPS protocol is used in the web browser if it is supported by web service provider. For more protection, certificate pinning could be utilized since it let client web-browser store the webserver public key for short period of time. The most effective way is to check the IP address of webserver using "ping" webserver name address and "WHOIS IP Lookup Tool". This is the best way to check if correct IP address has been resolved for given name address. There are always other ways against cyber-attacks, and it is worth to let student discuss to find all other possible countermeasures.

5 Conclusions

With the growth of Internet use, cyber-crime also increases dramatically. The total number of data breach incidents, resulting in various losses, in recent years increases continuously. Due to the growth of cyber threat and shortage in cybersecurity professionals in US, education in cybersecurity becomes more important. As many researchers argue that the laboratory-based education maximizes the student learning, many academic institutes developed the laboratory-based courses such as SEED to help students to accelerate their learning. In this paper, we introduced Phishing Wi-Fi attack module utilizing public Wi-Fi and DNS concept. Low-cost affordable Raspberry Pi is used to implement phishing Wi-Fi attack module, which covers three out of six NSA Cybersecurity Concepts. This paper illustrated how to build the proposing phishing Wi-Fi attack and also introduced the delivery method.

Acknowledgements

This research was supported by NSA & NSF grant H98230-17-1-2006.

References

[1] E. Johnson and N. Willey, "Usability failures and healthcare data hemorrhages," *IEEE Security and Privacy,* vol 9, pp. 18-25, 2011.

[2] M. Tu and K. Spoa-Harty, "Data loss prevention management and control: inside activity monitoring, identification, and tracking in healthcare enterprise environments," *Journal of Digital Forensics, Security, and Law*. vol. 10, pp. 27-44, 2015.

[3] L. Trautman, “Cyberseurity: what about US policy?,” *Journal of Law, Technology and Policy*, vol. 2015, pp. 341, 2015. Available from: https://ssrn.com/abstract=2548561.

[4] Conti, Juan Pablo. "The day the samba stopped [power blackouts]." *Engineering & Technology* 5.4 (2010): 46-47.

[5] Farwell, James P., and Rafal Rohozinski. "Stuxnet and the future of cyber war." *Survival* 53.1 (2011): 23-40.

[6] Pasqualetti, Fabio, Florian Dörfler, and Francesco Bullo. "Attack detection and identification in cyber-physical systems." *IEEE transactions on automatic control* 58.11 (2013): 2715-2729.

[7] A Frost and Sullivan Executive Briefing, *Global Information Security Workforce Study*, 2017. Available from: https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf. [Accessed 27th August 2017].

[8] J. Cuny and J. Hamos, NICE cybersecurity in K-12 formal education, 2011. Available from: http://csrc.nist.gov/nice/Sept2011-workshop/presentations/Thursday/Thurs_Cuny_NICE_K-12_092211.pdf. [Accessed 25th August 2017].

[9] Ma, Jing, and Jeffrey V. Nickerson. “Hands-on, simulated, and remote laboratories: A comparative literature review.” *ACM Computing Surveys (CSUR)* 38.3 (2006): 7.

[10] M. Findley, “The relationship between student learning styles and motivation during educational video game play,” *International Journal of Online Pedagogy and Course Design*, vol. 1 (3), pp. 63-73, 2011.

[11] Schneider, Fred B. "Cybersecurity education in universities." *IEEE Security & Privacy* 11.4 (2013): 3-4.

[12] Hands-on Labs for Security Education (SEED labs), http://www.cis.syr.edu/~wedu/seed/

[13] Suganya, V. "A review on phishing attacks and various anti phishing techniques." *International Journal of Computer Applications* 139.1 (2016): 20-23.

[14] Gupta, M. Surya Deekshith, Vamsikrishna Patchava, and Virginia Menezes. “Healthcare based on IoT using Raspberry Pi.” *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*. IEEE, 2015.

[15] Zhao, Cheah Wai, Jayanand Jegatheesan, and Son Chee Loon. “Exploring iot application using raspberry pi.” *International Journal of Computer Networks and Applications* 2.1 (2015): 27-34.

[16] P. B. Rao and S.K. Uma, “Raspberry Pi Home Automation with Wireless Sensors using Smart Phone”, *International Journal of Computer Science and Mobile Computing*, *Vol. 4*, *Issue. 5*, May 2015.

[17] Prasad, Sanjana, et al. “Smart surveillance monitoring system using Raspberry Pi and PIR sensor.” *Int. J. Comput. Sci. Inf. Technol* 5.6 (2014): 7107-7109.

[18] Maksimović, Mirjana, et al. “Raspberry Pi as Internet of things hardware: performances and constraints.” *design issues* 3 (2014): 8.

[19] Ferdoush, Sheikh, and Xinrong Li. “Wireless sensor network system design using Raspberry Pi and Arduino for environmental monitoring applications.” *Procedia Computer Science* 34 (2014): 103-110.

[20] Vujovic, Vladimir, and Mirjana Maksimovic. “Raspberry Pi as a Wireless Sensor node: Performances and constraints.” *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on*. IEEE, 2014.

[21] M. Schmidt, “Raspberry Pi –A Quick Start Guide.” The Pragmatic Bookshelf, 2013.

[22] Sobota, Jaroslav, et al. "Raspberry Pi and Arduino boards in control education." *IFAC Proceedings Volumes* 46.17 (2013): 7-12.