Defense and Analysis of Hijacking User Login Credentials via Remote Code Execution and Raspberry PI

Patel Nishitkumar
Np05573@georgiasouthern.edu

Hayden Wimmer
Hayden.wimmer@gmail.com

Georgia Southern University
Statesboro, GA

Loreen Powell
lpowell@bloomu.edu
Bloomsburg University
Bloomsburg, PA

Abstract

Cyber-security is a rapidly growing concern for all organizations. Ransomware and Botnets are becoming pervasive across the internet. Management needs to understand how systems are compromised by attackers who implant payloads as ransomware and botnets. One such concern is physical access to machines by bad actors in the organization or mobile workstations working at offsite locations. Gaining physical access a bad actor can implant malware in the form of ransomware or a botnet which becomes an initial point of entry for assuming control over an organizations network. In this example, we illustrate the dangers of physical access and use a USB device to implant a payload via remote code execution. The remote code installs an application developed to mimic a Windows 10 login screen and populates the login screen with the username of the currently logged in user. Once the user logs in to this fake screen, the application logs the user's credentials, namely the username and plain text password, via an HTTP post to a remote command and control server. Following our demonstration, we discuss implications and countermeasures to aid management in improving security of the organization.

Keywords: Cyber-security, Raspberry Pi, Payloads

I. INTRODUCTION

As technology continues to advance, malicious information technology (IT) attacks also become more complex focusing on rich data (Christensen & Dannberg, 2019). Kavitha and Kavitha (2016), report that there were 360 million malware variants were released into the wild in 2016. The Universal Serial Bus (USB) is commonly recognized as a vector for malicious attacks. Thus, when a USB is maliciously used, it can deliver malware, steal critical data, and cause other malicious attacks which pose significant threats to computers and network systems (Muller, Zimmer & de Nittis, 2019). Today, USB attacks that target IT infrastructures are gaining popularity (Neugschwandtner et al., 2016).

One of typical security threat attributed to computer and network infrastructure includes the hijacking of user login credentials in Raspberry Pi systems (Chandreshekar et al., 2017). A recent literature work by Martin, Kargaard, and Sutherland (2019) analyzed this issue and offer

some significant perspectives regarding the development of Internet of Things (IoT) and its contributions in the hacking of login credential of such devices as Raspberry Pi systems. However, nobody has examined and documented the step-by-step process involved in such hackings. Emani, Glantz, Gamrat, and Hills (2019) explain that universities are beginning to explore and incorporate Raspberry Pi security learning projects into their IT courses and curriculum. They note that there is value to providing students with this type of hands-on experience.

The goal of this research is to document a novel process of how a successful remote code execution is carried out using Raspberry Pi Zero and a USB executable file. This study expands upon the implications of perspectives addressed in the literature by providing a better understanding about the vulnerabilities in preventing the hackings occurring with the Raspberry Pi. This work has practical implications for IT professional interested in gaining a comprehensive understanding of the attributes and process. As a result, this research will help IT professionals strengthen their systems and prevent malicious attacks attributed to computer systems and networks. Additionally, this work may serve as an applied resource for IT programs and faculty wishing to explore ongoing research to detect threats in Raspberry Pi devices. This research could be replicated at other institutions. The remainder of this paper is structured as follows: background/ literature review, methodology, results, and conclusion.

II. LITERATURE REVIEW

The mechanics used to hack Raspberry Pi remotely for the login credential payload require knowledge about innovations, security processes, protocols, and equipment that aid hackers to gain access into the systems. The main themes to consider in this regard include IoT, vulnerabilities of Raspberry Pi, and defense perspectives on how to prevent such hackings.

A. Internet of Things (IoT)

IoT is a major standpoint attributed to the growth of hijacking Raspberry Pi logins remotely. Martin, Kargaard and Sutherland (2018) implicated IoT as an essential factor towards the growth of login hijacking intrusions. Based on their perspectives, the manufacture and use of IoT over the past years has grown significantly vast. This development as a result, has led to an increase in the number of innovations in the field, both positive and negative. Ray (2018), analyzed similar perspectives, but with regard to the integrative innovations encompassing IoT. A common perspective shared by these literatures is the necessity of IoT devices in modern settings, which as a result, pose great security challenges. Accordingly, he argued that IoT implicate such attributes as economic benefits and efficiency, which renders their use across organization settings inevitable. Similarly, Martin et al. (2019) predicted that the value of the IoT would reach 7.1 trillion by the year 2020. Thus, it is evident that intrusion problem are likely to increase in the future.

With the number of IoT devices increasing and playing a more integrated role in our everyday lives, it is believed to have a played a significant role in the healthcare industry. Kaur and Jasuja (2017) proposed a system that would monitor pulse rate, body temperature of the person with sensors alongside with raspberry pi and IoT.

B. Vulnerabilities of the Raspberry Pi

A recent study by Al Saaidi et al. (2018) analyzed the functionality of the OpenSHH and security protocols that users can employ in securing the service of their Raspberry Pi. Specifically, they analyzed the functionality of the Debian v7.1 p2 systems, which they claimed is subject to vulnerabilities when installed in a Raspberry Pi 2. Their research established that SSH protocol exchange keys are points of weaknesses, especially when they allow multiple CRLF injections in the device. Because of this aspect of vulnerability, remote authenticated users can bypass the shell commands to extract significant payloads on command.

Neugschwandtner, Beitler and Kurmus (2018) analyzed the vulnerability in Raspberry Pi elaborating on the system's weaknesses from USB attack vectors. Particularly, they noted that USB attacks passively eavesdrop on communications by intercepting host devices without necessarily having a physical connection between the host and victim device. This intrusion aspect is crucial, as it constitutes the precise process of bypassing the Raspberry Pi protocols to access the login credentials of the victim device. They expressed concern that such intrusions are becoming more complex with the advancement of USB sticks.

Nissim, Yahalom and Elovici (2018) also explored USB-based intrusions. They noted that USB peripherals are vulnerable because they carry embedded malicious payloads deemed essential by hackers to launch attacks on victim devices. Because of such vulnerabilities, the setup of the P4wnP1 utilizes the USB functionalities to execute

the necessary protocols in hijacking the login credentials of a Raspberry Pi.

Equally relevant perspectives regard vulnerabilities of Raspberry Pi login hackings concerns ineffective security protocols. In particular, some device users use similar passwords and usernames in multiple accounts, which undermines the security of information stored within the devices. Recently, Ahmed et al. (2019) analyzed this security issue with regard to threats attributed to physical security. In their analysis, they suggested the relevance of incorporating multiple security level in ensuring data security. More so, they advocated that device users should utilize five levels of security that include among other, entering passwords on interactive GUI, facial recognitions, and speech pattern recognitions. Sharing similar perspective Radzi et al. (2020) suggested the essentiality of using safe password systems as facial recognitions in Raspberry Pi systems. In their evaluation, the authors warned that users who disregard effective password security protocols stand the chance of consistent network intrusion that might compromise the entire system the Raspberry is attached. Based on these perspectives, users should ensure that they use the most effective and reliable password protocols to safeguard their systems from intrusions and login hackings.

C. Defenses Against Raspberry Pi Vulnerability Points

Across most IT research analyzing the process of Raspberry Pi hackings, authors provide perspectives regarding how the device users may address intrusions. According to Martin et al. (2018), one of the best solutions is to use Internet honeypots. Accordingly, the mechanisms are necessary because of their capacity to identify IoT-related malware. Furthermore, they recommend using honeypot mechanism that uses a Cowrie framework or a fully interactive secure shell. They argue that this process has been successful in curbing the Mirai attack that targeted IoT devices and routers as slaves. Echoing these sentiments, Tripathi and Kumar (2018) analyzed how honeypot mechanisms can be incorporated in Raspberry Pi among other devices as essential defense mechanisms. In their argument, however, they noted the relevance of maintaining data integrity and incorruptibility within the system.

Alsaadi et al. (2018), in their solution segment, also offered relevant perspectives concerning the defenses against Raspberry-based intrusions. More so, among the various solutions proposed was addressing the Raspberry Pi remote access. According to the authors, the employment of PuTTY, which is a free license Windows SSH client server, can offer the best security solution. Similarly, O'Leary (2019) analyzed the employment of PuTTY noted that this tool allow for the creation of secure remote sessions when users intend to access the Raspberry Pi hardware over a network. Furthermore, he argued, with the mechanic's cryptography, the system benefits from an added protection layer against eavesdropping or hijacking attacks.

Another study by Yevdokymenko, Mohamed and Onwuakba (2017) examined the relevance of ethical hacking as a way of preventing system breaches through uncovered network areas. Specifically, they argued that through a successful penetration testing and information gathering, system users could put in place the correct patches as a way to reinforce their network defense.

Finally, Balooch (2017) shared similar perspectives purporting that ethical hacking is critical because it assumes hackers' point of view in determining the security protocols to put in place when preventing such breaches as the hijacking of login credentials.

III. METHODOLOGY

The goal of this study is to document the step-by-step process of how a successful remote code execution is carried out using Raspberry Pi Zero and a USB executable file. This study expands upon the implications of perspectives addressed in the literature by providing a documented understanding about the vulnerabilities in preventing the hackings occurring with the Raspberry Pi. Raspberry Pi is a low-cost, credit card-sized computer that connects to a computer monitor or TV using HDMI, and uses a standard keyboard and mouse. It can run a host of operating systems, such as Raspbian (Debian Linux), Android, Windows 10, IoT Core, etc.

In this section, we briefly explain how to set up a Raspberry Pi, installing P4wnP1 and remote connection to device. We demonstrated step-by-step how a successful remote code execution is being carried out using Raspberry Pi Zero and USB executable file. Raspberry Pi is a low-cost basic computer that plugs into a computer and runs on Linux. We developed our own version of P4wnP1 and use it to demonstrate how we can hijack user login credentials using remote code execution. An outline of the network is referred to in Fig. 1. For the setup, we used a Samsung

ISSN: 2167-1508
v13 n5302

Laptop (Attacker), Lenovo PC (Victim PC), 8GB USB, and raspberry pi zero.

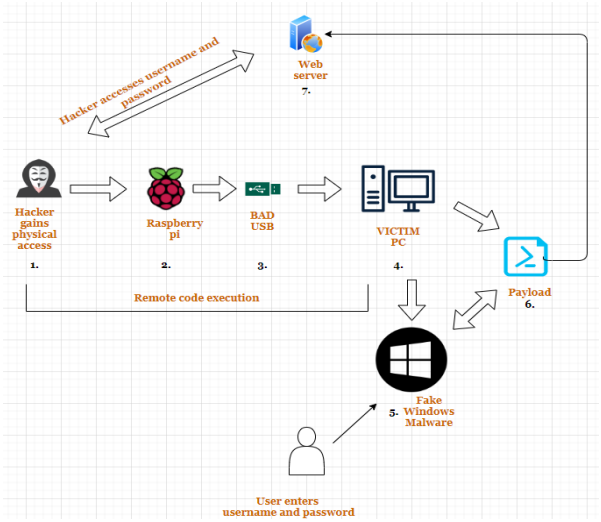

Figure 1: Configuration of the Network

A. Setting up Raspberry Pi

In order to get our raspberry pi setup as a USB device we needed: A long USB cable with power adaptor, Micro SD card, Power cable and Internet. We downloaded the latest version of Raspbian Stretch Lite to write the image onto a Micro SD card. We used angry IP scanner to find the IP address of the pi (172.24.0.1). Once we logged into the pi, we installed git and downloaded a clone of P4wnP1. P4wnP1 is a toolset that turns our pi into a WI-FI hotspot.

B. Installation and Testing the Connection

Figure 2 shows the code that we used to clone P4wnP1 from GitHub. After the install was completed, we then plugged the Raspberry Pi into the attacker machine and we were able to detect the Wi-Fi hotspot on the victim PC shown as "P4wnP1"

```
nishit@wimmlab:~$ mkdir ~/P4wnP1
nishit@wimmlab:~$ cd P4wnP1/
nishit@wimmlab:~/P4wnP1$ git clone https://github.com/mame82/P4wnP1
Cloning into 'P4wnP1'...
remote: Enumerating objects: 1413, done.
remote: Total 1413 (delta 0), reused 0 (delta 0), pack-reused 1413
Receiving objects: 100% (1413/1413), 2.74 MiB | 9.63 MiB/s, done.
Resolving deltas: 100% (851/851), done.
nishit@wimmlab:~/P4wnP1$ ./install.sh
```

Figure 2. Installation of P4wnP1

Figure 3 shows successful connection to PwnP1 Wi-Fi Hotspot. We connected to the Wi-Fi hotspot using the attacker machine. This allowed us to have connectivity to the raspberry pi so we could remotely login using PUTTY and execute commands.

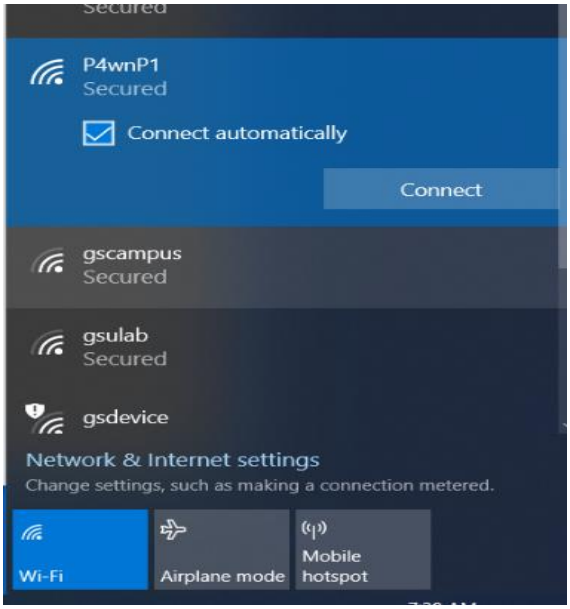

Figure 3. Successful installation of P4wnP1

C. Raspberry Pi Remote Access

We used PuTTY, a free open-source terminal licensed Windows SSH client server. It allows users to create a secure remote session access to Raspberry pi hardware over a network connection.

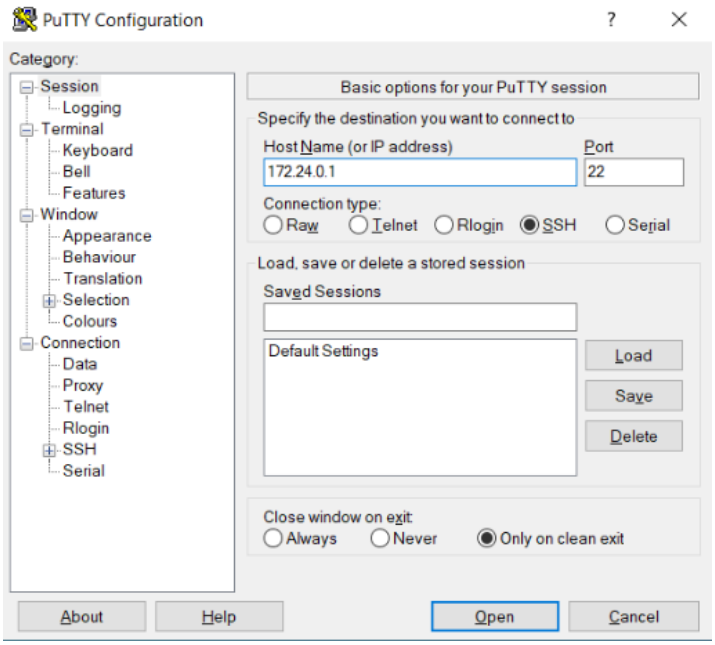

Figure 4. SSH connection to raspberry pi

SSH is a protocol for encrypted communications between computers that add protection against eavesdropping or hijacking attacks. We were successful in connecting the victim pc to the

P4wnP1 network, we then SSH into the raspberry pi as shown in figure 4.

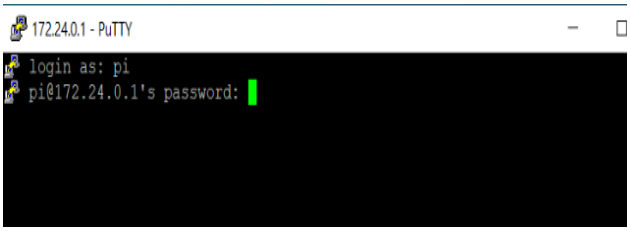

Figure 5. Successful Connection to the Pi

Figure 5 shows successful connection to the raspberry pi from the attacker pc. We were able to gain full access to the device. This will allow us to execute payload to the victim pc.

D. USB Loaded with exe File

We created a .NET application (fake windows lock screen) written in C#, all output is dumped into a HTTP request web server. We executed the application to create an .exe file, which was uploaded to a USB. The USB was plugged into victim pc to create a backdoor and hijack user login credentials.

E. Remote Code Execution

In order to do a remote code execution we wrote a USB Rubber Ducky Script. Figure 6 shows a simple scripting language that allows penetration testers to deploy payloads that mimic human keyboard input. The script will point to the USB drive E:\filename (SharpLocker).exe file.

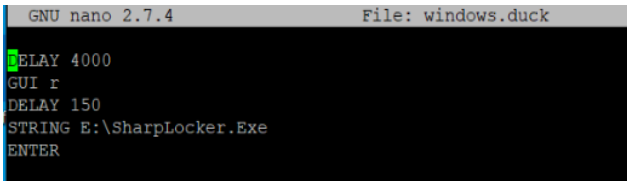

Figure 6. DuckyScript code

From the attacker pc, we executed SendDuckyScript injection to the victim pc, we chose option 14 (windows) as shown in Figure 7, this will execute a fake windows malware in victim pc and as soon as the victim enters the credentials we will hijack user login credentials on our web server.

Figure 8 shows a fake windows login screen pop up on the victim pc after the payload was executed. When the victim inputs the password, the password would be dumped into an external HTTP web server.

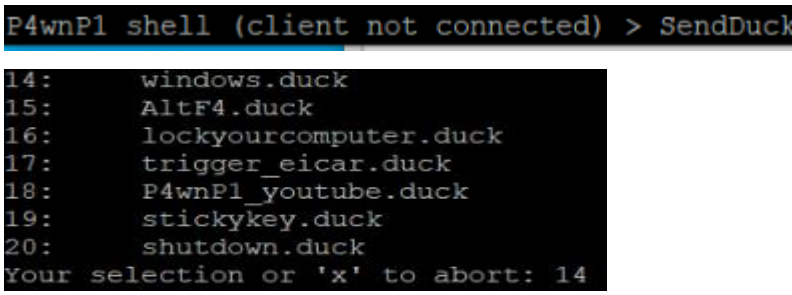

Figure 7. Choose option 14 to send to victim pc

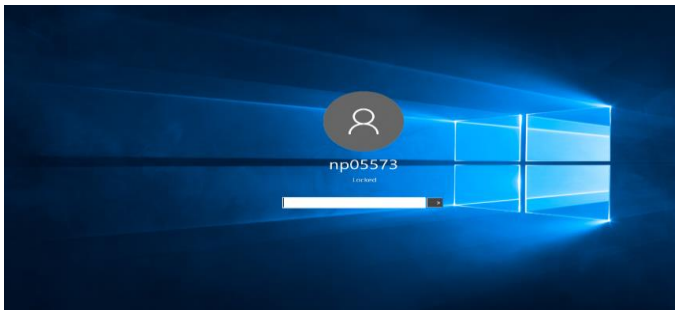

Figure 8. Fake Windows login screen on victim pc

IV. RESULTS

The results as shown in Fig 9, we were able to successfully hijack user login credentials on our web server once the user entered the password. By incorporating the functionalities P4wnP1 network, it was possible to connect the protocols to victim system and to launch the execution controls. Nonetheless, the most essential attribute of this setup was its capacity to provide relevant information from the malicious attack targeting the system. This attack opened a backdoor through which we were able to manipulate the whole system. Consequently, it was possible to create a fake windows lock screen through which the SendDuckScript was executed to eavesdrop on the credential input, which are consequently transferred as payloads to the USB infrastructure.

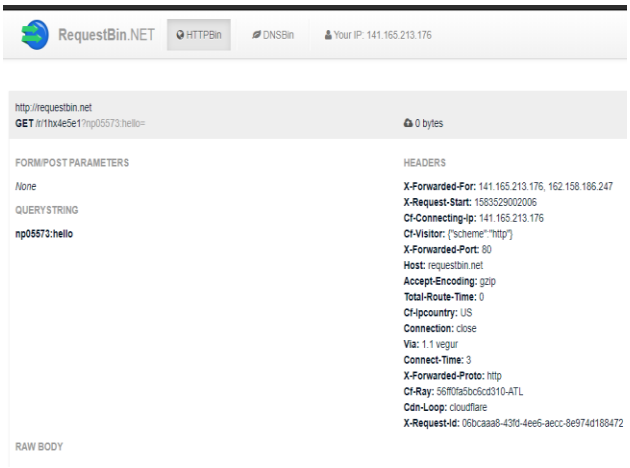

Fig 9. User login credentials hijacked

The countermeasures for mitigating Raspberry Pi hacking are in consideration with the strategies suggested in the Literature Review section. In brief, users can employ the honeypot mechanics that detect and prevent such intrusions. Second, the users can use such tools as PuTTY, which are client servers that offer security solutions. Last but not least, it is crucial to conduct ethical hacking, such as penetration testing, occasionally, which enable users to assume hackers' perspectives in order to secure their systems. Nonetheless, it is crucial to take precautionary measure that can prevent hackers from getting access and controlling network systems with sensitive information.

VI. CONCLUSION

In summary, the remote hijacking of login credentials through Raspberry Pi are attributable to certain vulnerabilities within network systems. Through the input of such frameworks as P4wnP1 network, hackers can exploit network weaknesses by executing attacks through USB mechanics. Based on the step-by-step procedure, it is evident that such attacks, leading to compromised login credentials can be problematic. Nonetheless, by employing such measures as employment of PuTTY and honeypot mechanics, network users can secure their systems. More so, ethical hackings can be potent solutions against network hackings.

VII. REFERENCES

Ahmed, S. U., Sabir, A., Ashraf, T., Ashraf, U., Sabir, S., & Qureshi, U. (2019, December). Security Lock with Effective Verification Traits. In *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)* (pp. 164-169). IEEE. DOI.101109/ICCIKE47802.2019.9004341

Alsaadi, H. H., Aldwairi, M., Al Taei, M., AlBuainain, M., & AlKubaisi, M. (2018, February). Penetration and security of OpenSSH remote secure shell service on Raspberry Pi 2. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1-5). IEEE. DOI: 10.1109/NTMS.2018.8328710

Apple Inc., Hewlett-Packard Inc., Intel Corporation, Microsoft Corporation, Renesas Corporation, STMicroelectronics, & Texas Instruments (2019).Universal Serial Bus 4 (USB4™) Specification.https://www.usb.org/document-library/usb4tm-specification

Baloch, R. (2017). Ethical hacking and penetration testing guide. (2nd ed.) New York, NY: CRC Press.

Chandreshekar, K., Clearly, G., Cox, O., Lau, H., Nahorney, B., Gorman, B., Wueest, C. (2017, April). Internet threat security Report . *Symantec*, *22*.

Christensen, L., & Dannberg, D. (2019). Ethical hacking of IoT devices: OBD-II dongles. http://www.diva-portal.org/smash/get/diva2:1333813/FULLTEXT01.pdf

Denney,K., Erdin, E., Babun,L., Uluagac. A. S.(2019). POSTER: Dynamically Detecting USB Attacks in Hardware (Extended Abstract). InWiSec '19: ACM Conference on Security and Privacy in Wireless and MobileNetworks, May 15–17, 2019, Miami, FL, USA.ACM, New York, NY, USA,2 pages. https://doi.org/10.1145/3317549.3326315

Emani, R., Glantz,E. J., Gamrat, C. & Hills, M. K. (2019). Using the Raspberry Pi in IT Education. In *Proceedings of the 20th SIGITE conference on Information technology education (SIGITE'19)*. Tacoma, WA, USA, 1 page. https://doi.org/10.1145/3344254

Kavitha, G., & Kavitha, R. (2016). An analysis to improve throughput of high-power hubs in mobile ad hoc network.

Martin, E. D., Kargaard, J., & Sutherland, I. (2019, June). Raspberry pi malware: An analysis of cyberattacks towards IoT devices.

In *2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 161-166). IEEE. DOI: 10.1109/DESSERT.2019.8770027

McDonald, G., Murchu, L. O., Doherty, S. & Chien, E. (2013).Stuxnet 0.5: The Missing Link. https://docs.broadcom.com/doc/stuxnet-missing-link-13-en

Mueller, T., Zimmer, E., & de Nittis. L. (2019). Using Context and Provenance to defend against USB-borne attacks. In 2019 Proceedingsof the 14th International Conference on Availability, Reliability and Security (ARES 2019) (ARES '19), Canterbury, United Kingdom. ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3339252.3339268

Neugschwandtner, M., Beitler, A., & Kurmus, A. (2016, April). A transparent defense against USB eavesdropping attacks. In *Proceedings of the 9th European Workshop on System Security* (pp. 1-6). DOI: 10.1145/2905760.2905765

Nissim, N., Yahalom, R., & Elovici, Y. (2017). USB-based attacks. *Computers & Security*, *70*, 675-688. DOI:10.1016/j.cose.2017.08.002

Nohl, K. & Lehl, J. (2014, August). BadUSB – On Accessories That TurnEvil. In Blackhat USA

O'Leary, M. (2019). Network Services. In Cyber Operations (pp. 649-720). Apress, Berkeley, CA. DOI:10.1007/978-1-4842-4294-0_13

Radzi, S. A., Alif, M. M. F., Athirah, Y. N., Jaafar, A. S., Norihan, A. H., & Saleha, M. S. (2020). IoT based facial recognition door access control home security system using raspberry pi. *International Journal of Power Electronics and Drive Systems*, *11*(1), 417. DOI:10.11591/ijpeds.v11.i1.pp417-424

Ray, P. P. (2018). A survey on Internet of Things architectures. *Journal of King Saud University-Computer and Information Sciences,* 30(3), 291-319. DOI:10.1016/j.jksuci.2016.10.003

Tian, Bates & Buttler (2015). Defending Against Malicious USB Firmware with GoodUSB. *ACM ACSAC '15 Conference*, December 07-11, 2015, Los Angeles, CA, USA https://adambates.org/documents/Bates_Acsac15.pdf

Tripathi, S., & Kumar, R. (2018, December). Raspberry Pi as an intrusion detection system, a honeypot and a packet analyzer. In *2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)* (pp. 80-85). IEEE. DOI: 10.1109/CTEMS.2018.8769135

Yevdokymenko, M., Mohamed, E., & Onwuakpa, P. (2017, October). Ethical hacking and penetration testing using raspberry PI. In *2017 4th International Scientific-Practical Conference Problems of Info communications. Science and Technology (PIC S&T)* (pp. 179-181). IEEE. DOI: 10.1109/INFOCOMMST.2017.8246375