# Potential Security Vulnerabilities in Raspberry Pi Devices with Mitigation Strategies

Briana Tolleson

# Potential Security Vulnerabilities in Raspberry Pi Devices with Mitigation Strategies

## 1. Abstract

For this research project I used a Raspberry Pi device and conducted online research to investigate potential security vulnerabilities along with mitigation strategies. I configured the Raspberry Pi by using the proper peripherals such as an HDMI cord, a microUSB adapter that provided 5V and at least 700mA of current, a TV monitor, PiSwitch, SD Card, keyboard, and mouse. I installed the Rasbian operating system (OS). The process to install the Rasbian took about 10 minutes to boot starting at 21:08 on 10/27/2023 and ending at 21:18. 1,513 megabytes (MB) was written to the SD card running at (2.5 MB/sec). On Sunday, November 26th, 2023, one of the peripherals seemed to have a circuit trip. I used an Apple USB-C cord and block to connect the PiSwitch to a laptop. This gave enough power for the Raspberry Pi to turn on using the same adapter as before. I referred to the Pi manual often for troubleshooting. The device has five indicator LEDs that provide statuses/feedback. Only two of my lights were turned on which where: ACT which lights up green when the SD card is accessed and PWR—which turns on red—signifying it is hooked up to 3.3V power. After booting up, I was able to get onto the desktop and open up LXTerminal and start entering Linux commands. Due to a lack of resources, I did not have a Wi-Fi dongle to enable network interface wirelessly or an ethernet cable to provide a wired connection.

## 2. Introduction

Raspberry Pi devices are single-board computers meaning they have all the features of a computer system on a single board, including network connectivity, storage, video output, input, Central Processing Unit (CPU), and memory. The Raspberry Pi came about in 2006 and was inspired by the British Broadcasting Corporation Microcomputer System (BBC Micro) (Capstick, 2023). It was invented in 2012. Eben Upton created the Raspberry Pi. His goal was to build a computer much cheaper than the BBC Micro. Raspberry Pi got its name following the trend of having computer manufacturers named by fruits. For example, before the Raspberry Pi, there were Apple, Acorns, and Apricot computers. Upton intended to make computers at an affordable cost for young students to learn how to program. Although these devices are pretty nifty there are potential security vulnerabilities involved with them. However, there are mitigation strategies that can be implemented. By exploring what others have published and examining the objective of each of their publication's context it is possible to understand the potential vulnerabilities and avoid security risks.

## 3. Literature Review

According to SEPIO Systems, the problem with Raspberry Pi is that it is a security risk. Some of the security challenges are known as PoisonTap, P4wnP1, Bypassing NAC, Advanced Persistent Threat (APT) attack, and Ventilators. Some of the risks of PoisonTap are that it can emulate an ethernet device over USB, it siphons and stores HTTP cookies, it installs web-based backdoors, and it can expose the system's internal router. P4wnP1 is a USB attack platform for the Raspberry Pi Zero. Some of the actions it can perform are mouse/keyboard emulation/HID covert channel – backdoor. HID over the channel – frontdoor, cookie harvesting, man-in-the-

middle attack, and the Raspberry Pi Zero W has a built-in Wi-Fi unit. It provides SSH access which allows an attacker to control various servers remotely. Using the Raspberry Pi, a genuine device can be spoofed allowing bypass for an attacker to have access to a device that has been authenticated. A hacker can have access to an organization's network. Some of the attacks that can occur are data breaches, malware installation, and even APT attacks (Sepio, 2023).

According to another recent publish dated July 24-26, 2023, "The study shows that the Raspberry Pi with Raspbian operating system (OS) is breached quicker than the Windows 10 operating system since it lacks a built-in software system to detect viruses or intrusions. The attacker takes 1 second to execute the Man In The Middle and backdoor attacks, whereas it takes 60 seconds for the Denial of Service (DoS) attack." (Arreaga, 2023)

There are a few Common Vulnerabilities and Exposures (CVEs) worth mentioning found in the Raspberry Pi. The first one is listed as CVE-2018-18068. It is described as, "The ARM-based hardware debugging feature on Raspberry Pi 3 module B+ and possibly other devices allows non-secure EL1 code to read/write any EL3 (the highest privilege level in ARMv8) memory/register via inter-processor debugging." Then there is CVE-2021-38545 which was detailed as, "Raspberry Pi 3 B+ and 4 B devices through 2021-08-09, in certain specific use cases in which the device supplies power to audio-output equipment, allow remote attackers to recover speech signals from an LED on the device, via a telescope and an electro-optical sensor, aka a "Glowworm" attack." Another vulnerability is listed as CVE-2021-38759. Its description states, "Raspberry Pi OS through 5.10 has the raspberry default password for the pi account. If not changed, attackers can gain administrator privileges." The CVE-2018-18068 max base score was rated 10/10 with a base severity of HIGH. The CVE-2021-38545 base score was rated at 4.3

and 5.9 and its base severity was rated as MEDIUM. Lastly, the CVE-2021-38759 had a base score of 10.0 and was rated as HIGH.

*Figure 1*

| **Security Vulnerabilities & Proposed Mitigation Strategies** | | | | |
|---|---|---|---|---|
| **Vulnerabilities:** | "Glowworm attack". | Hackers can gain administrator access due to not changing default password. | Lacks a built-in software system to detect viruses or intrusions. | Unauthorized access attempts. DoS attacks. |
| **Mitigation Strategies:** | The Glowworm attack can be blocked by placing a black tape over a device's power indicator LED or integrating a capacitor or an operational amplifier to eliminate the interference to power consumption while the speakers produce sound (Paganini, 2021). | Change default password immediately once logged into LXTerminal. | Download ClamAV which can detect a wide-variety of threats like Rasbian (Emmet, 2022). | Download UFW (uncomplicated firewall). |

## 4. Findings

Some mitigation strategies are as follows. Once the Rasbian operating system has been installed, make sure to change the default password that way hackers cannot gain administrator privileges. Another mitigation strategy would be to always keep the OS up to date as much as possible. When the OS is up to date it stops people from exploiting old bugs in software running on the device. Also, if running the OS Rasbian, set up a package called "unattended upgrades".

This package allows the user to have their system periodically update the package list and then upgrade the packages. Keeping the Raspberry Pi's SSH connection secure is also good. Some methods to do this by using a key authentication. "The keys act as a way of identifying yourself to the server." In addition, use USBGuard software which can help prevent rogue USB devices. Having a key authentication while being paired with a passphrase is a safer way of connecting to SSH. Adding two-factor authentication to SSH is another good method because an attacker will not be able to gain access without having to enter a code from the owner's app. Lastly, setting up a Firewall on the Raspberry Pi. Firewalls such as uncomplicated firewall (UFW) help protect the Raspberry Pi from port-based network attacks (Emmet, 2022).

## 4. Conclusion

Overall, Raspberry Pi is a good device to use with the proper amount of security. Just like now in any business or organization, security training is essential for quality assurance. Same applies here for utilization of this device. For the user to effectively gain benefit from the Raspberry Pi, certain methods need to be implemented to fulfill the three components of the CIA triad—confidentiality, integrity, and availability. If the user is using the Raspberry Pi to store important data, it is crucial that no other person has unauthorized access to it. It is important for the data in the Raspberry pi to not be altered due to malicious activity by an unauthorized user. Lastly, it reassuring to know that by using the Raspberry the data you store will always be available and accessible when needed by only authorized users.

## 5. References

DevicePlus Editorial. “The History of Raspberry Pi.” *The History of Raspberry Pi*, 13 Jan. 2023, www.deviceplus.com/raspberry-pi/the-history-of-raspberry-pi/#:~:text=coding%20and%20programming.-,Raspberry%20Pi%20origin%20story,Jack%20Lang%20and%20Alan%20Mycroft.

Capstick, Far. “History of Computing: The BBC Microcomputer.” *History of Computing: The BBC Microcomputer*, Parker Shaw, parkershaw.co.uk/blog/history-of-computing-the-bbc-microcomputer. Accessed 1 Dec. 2023.

“Raspberry Pi – a Friend or Foe? Cyber Physical Security ... - Sepio.” *Raspberry Pi – A Friend or Foe? Cyber Physical Security Challenges*, sepiocyber.com/wp-content/uploads/2020/07/Raspberry-Pi-Risks-Article-E-Book-12-2020.pdf. Accessed 1 Dec. 2023.

“CVE-2018-18068: Raspberry Pi 3 Module B+ ARM-Based Hardware Debugging ...” *RASPBERRY PI 3 MODULE B+ ARM-BASED HARDWARE DEBUGGING ACCESS CONTROL*, vuldb.com/?id.132972. Accessed 1 Dec. 2023.

“National Vulnerability Database.” *Nvd.Nist.Gov*, 4 Apr. 2019, nvd.nist.gov/vuln/detail/CVE-2018-18068.

“National Vulnerability Database.” *nvd.nist.gov*, 11 Aug. 2021, nvd.nist.gov/vuln/detail/CVE-2021-38545.

Paganini, Pierluigi. “Glowworm Attack Allows Sound Recovery via Device’s Power Indicator Led.” *Security Affairs*, 15 Aug. 2021, securityaffairs.com/121158/hacking/glowworm-attack-spy-conversations.html.

Emmet. “Set up UFW on Your Raspberry Pi.” *Pi My Life Up*, 29 Jan. 2022, pimylifeup.com/raspberry-pi-ufw/.

Emmet. “Setup Antivirus Software on Your Raspberry Pi.” *Pi My Life Up*, 29 Jan. 2022, pimylifeup.com/raspberry-pi-clamav/#:~:text=ClamAV%20is%20a%20popular%20free,malware%2C%20and%20other%20malicious%20threats.

Arreaga, Nestor X., et al. “Security Vulnerability Analysis for IOT Devices Raspberry Pi Using Pentest.” *Procedia Computer Science*, Elsevier, 10 Oct. 2023, www.sciencedirect.com/science/article/pii/S1877050923010785#abs0001.

“Confidentiality, Integrity, and Availability: The CIA Triad.” *Office of Information Security*, informationsecurity.wustl.edu/items/confidentiality-integrity-and-availability-the-cia-triad/#:~:text=The%20CIA%20Triad%E2%80%94Confidentiality%2C%20Integrity,to%20these%20three%20crucial%20components. Accessed 1 Dec. 2023.