PRINTSHOP: SERIAL PRINTER ENVIRONMENTS AND SECURITY

Research Proposal

Doctor of Philosophy

in

Cyber Operations

January 23, 2024

By

Micah Flack

Dissertation Chair:

Dr. Vaidyan Varghese

Dissertation Committee:

Dr. Yong Wang

Dr. Michael Ham

Beacom College of Computer and Cyber Sciences

TABLE OF CONTENTS

Introduction

1.1 Background

Serial printers are devices commonly used for instant reporting of system data for industrial control systems (ICS) and receipts for point-of-sale (POS) systems. These devices are connected to their host using Wi-Fi, bluetooth, ethernet, or USB; in some cases, serial RS232 is an option as well. The goal of this research is to assess what software and hardware protections are enabled, as well as, how configurable the serial printers are for further exploit research.

(a) Square POS (b) SurePOS

Figure 1.1: Comparison of common POS systems

Figure 1.1 shows us two similar looking point-of-sale systems, albeit one is much older looking. However, the operating system and required hardware is very different. Typically, unless you have the Square provided terminal, their software/client is installed onto an Android or iOS device and connected to a Square compatible card reader [1]. Whereas, the SurePoS, NCR, or other common EFTPoS system will run a proprietary OS based on Windows or Linux [2]. Furthermore, these PoS tend to require some form of printing receipts as record keeping for the business owner and customer. And these devices also vary in terms of processing capabilities and operating system.

For instance, a common thermal printer seen with PoS systems, integrated with fuel pumps, or other industrial control equipment, is the SNBC BTP-S80 thermal printer [3], [4]. There are multiple versions of the device with support for Bluetooth, USB only, or combination of USB/Serial/Ethernet. The bluetooth hardware is provided over an accessory 25-pin serial connection, with more I/O as a serial connection via RS232C connector and USB Type-B. It has driver support for various platforms: Android, iOS, Windows, Linux, and MacOS. The most interesting aspects are the processor, an Arm Cortex M4 clocked at 3.54MHz, and the operating system, a proprietary version of FreeRTOS. The system architecture is Armv7E-M with JTAG/SWD hardware debugging support [5], [6].

By default, the printer has enough headroom to process ESC/POS commands for printing paper and a webserver for debugging or general diagnostics. In theory, the uncompromised device could be flashed with modified firmware to act as a decoy and human-input-device (HID) against the host PoS. The viability of any vulnerabilities would likely be dependent upon supply chain attacks or physical bait-and-switch tactics [7].

1.2 Significance

According to the Federal Trade Commission (FTC), there were 37,932 reports of credit card fraud in 2012 and 87,451 reports in 2022. This marks an increase of credit card payment fraud by an estimated, 30.5%. By comparison, since 2020, there has been a 14.6% increase in credit card related fraud. Which does not include the millions of other fraud reports the FTC receives every year. In 2022 alone, there were around 5.1 million fraud, identity theft, and miscellaneous reports in total [8], [9]. The statistics for these reports stresses how crucial the security of payment systems are, both physical and online. And, the need to secure them grows every year.

1.3 Research Goals and Objectives

This research primarily focuses on physical POS systems or terminals and their hardware (serial accessories), rather than online solutions. For instance, not mobile payment apps like Venmo, CashApp, Zelle, or Paypal [10]. There are many reasons, but the types of systems being targeted varies greatly in terms of the hardware and software supported, as well as, how the transactions are handled with the payment processor. Presumably, the host-to-guest communication will not differ greatly between other environments (e.g., ICS). If the printers have demonstrable weaknesses with an Ubuntu host, that will fulfill the testing requirements.

The goal of this research is to further establish academic works in regards to embedded printer devices testing and security. This area is loosely documented within academia and only mentioned vaguely in relation to statistical reports or applied research using entirely different environments. For instance, most researchers limit their analysis of the environment to smartphones and the corresponding payment app, or detection systems for card skimmers [7]. Through this research we hope to apply gainful conclusions towards the development of an embedded environment for vulnerability assessment, penetration testing, and hardware-to-software interoperability against device hosts. Some examples of how the research could be applied in the future vary: BadUSB/BashBunny [11], JuiceShop [12], DVWA [13], or Webgoat [14]; no such work exists for embedded systems within the point-of-sale or serial printer context.

References

[1] J. Ondrus and K. Lyytinen, "Mobile Payments Market: Towards Another Clash of the Titans?" In *2011 10th International Conference on Mobile Business*, Jun. 2011, pp. 166–172. DOI: 10.1109/ICMB.2011.41. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6047067?casa_token=jp6ioVlqPjQAAAAA:L69Yx3rjP2tvbnS5zWF8-eMm8sUNjXR586jm2QV6hLH8T2MyuueyIFCeMDqjhNWtUh-_2ERWgQ (visited on 10/23/2023).

[2] S. T. Ebimobowei, Z. Enebraye Peter, and Y. Pual, "THE ROLE OF SOFTWARE IN A CASHLESS ECONOMY (CASE STUDY NIGERIA)," *International Journal of Research -GRANTHAALAYAH*, vol. 6, no. 1, pp. 177–186, Jan. 31, 2018, ISSN: 2350-0530, 2394-3629. DOI: 10.29121/granthaalayah.v6.i1.2018.1607. [Online]. Available: https://www.granthaalayahpublication.org/journals/index.php/granthaalayah/article/view/IJRG17_A11_812 (visited on 10/23/2023).

[3] "SNBC BTP-S80 Thermal Printer - Black Cabinet (USB/Serial/Ethernet)," CRS Inc. (), [Online]. Available: https://www.crs-usa.com/products/snbc-btp-s80-thermal-printer-black-(usb-serial-ethernet) (visited on 10/23/2023).

[4] "SNBC New Beiyang-Intelligent Micro-Super, Smart Express Cabinet, Barcode Label Printer, Ticket Printer_Electronics_Receipt/Log Printer, Barcode/Label Printer, Special Scanning Products, Mixed Print Scanning Products, Smart Express Cabinet, Smart Micro-Super_New Beiyang specializes in the development, production, sales and service of intelligent print identification and system integration products. It provides leading products and complete, one-stop application solutions for various industries around the world. It is the only core design in the industry in the country through independent innovation. Manufacturing technology and forming a large-scale production enterprise." (), [Online]. Available: https://www.snbc.com.cn/ (visited on 10/23/2023).

[5] "Cortex-M4." (), [Online]. Available: https://developer.arm.com/Processors/Cortex-M4 (visited on 10/23/2023).

[6] "FreeRTOS - Market leading RTOS (Real Time Operating System) for embedded systems with Internet of Things extensions," FreeRTOS. (), [Online]. Available: https://www.freertos.org/index.html (visited on 10/23/2023).

[7] N. Scaife, C. Peeters, and P. Traynor, "Fear the Reaper: Characterization and Fast Detection of Card Skimmers," presented at the 27th USENIX Security Symposium (USENIX Security 18), 2018, pp. 1–14, ISBN: 978-1-939133-04-5. [Online]. Available:

https://www.usenix.org/conference/usenixsecurity18/presentation/scaife (visited on 10/23/2023).

[8] "Consumer Sentinel Network Data Book for January - December 2011," Federal Trade Commission. (Oct. 22, 2023), [Online]. Available: https://www.ftc.gov/reports/consumer-sentinel-network-data-book-january-december-2011 (visited on 10/23/2023).

[9] C. FortheSentinel, "Consumer Sentinel Network Data Book 2022," 2022.

[10] Y. Wang, C. Hahn, and K. Sutrave, "Mobile payment security, threats, and challenges," in *2016 Second International Conference on Mobile and Secure Services (MobiSecServ)*, Feb. 2016, pp. 1–5. DOI: 10.1109/MOBISECSERV.2016.7440226.

[11] Hak5. "Bash Bunny," Hak5. (), [Online]. Available: https://shop.hak5.org/products/bash-bunny (visited on 10/23/2023).

[12] "OWASP Juice Shop — OWASP Foundation." (), [Online]. Available: https://owasp.org/www-project-juice-shop/ (visited on 10/23/2023).

[13] R. Wood, *DAMN VULNERABLE WEB APPLICATION*, Oct. 22, 2023. [Online]. Available: https://github.com/digininja/DVWA (visited on 10/23/2023).

[14] "OWASP WebGoat — OWASP Foundation." (), [Online]. Available: https://owasp.org/www-project-webgoat/ (visited on 10/23/2023).