DAKOTA STATE UNIVERSITY

PrintShop: Assessing OS and Capabilities of Serial Print Devices

Micah Flack

11/07/2023

Introduction

- Federal Trade Commission (FTC) reports:
  - 37,932 reports of credit card fraud in 2012
  - 87,451 reports in 2022.
    - 30.5% over the decade for reported credit card fraud.
  - Between 2020 and 2022 the increase was 14.6%
  - In 2022 alone, there were around 5.1 million fraud, identity theft, and miscellaneous reports in total.
- Critical to secure payment process and endpoints
  - Financial point-of-sale are not the only case (e.g., ICS, HMI, etc…)

Point of Sale (PoS) Systems with Serial Printers

Related Works

- R. Benadjila, M. Renard, P. Trebuchet, P. Thierry, and A. Michelizza, “Wookey : Usb devices strike back,” 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:199552896.
- W. D. Yu, D. Baheti, and J. Wai, “Real-Time Operating System Security,”
- Y. He, Z. Zou, K. Sun, et al., “RapidPatch: Firmware Hotpatching for Real- Time Embedded Devices,” presented at the 31st USENIX Security Symposium (USENIX Security 22), 2022, pp. 2225–2242, isbn: 978-1-939133-31-1. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/he-yi
- J. Tian, N. Scaife, D. Kumar, M. Bailey, A. Bates, and K. Butler, “SoK: ”Plug & Pray” Today – Understanding USB Insecurity in Versions 1 Through C,” in 2018 IEEE Symposium on Security and Privacy (SP), May 2018, pp. 1032–1047. doi: 16 10.1109/SP.2018.00037. Available: https://ieeexplore.ieee.org/document/8418652

Proposed Research - Objectives

- The goal of this research is to understand the hardware and software capabilities of serial print devices.
  - Can the hardware support adding unintended functionality at the application and physical layers?
  - And, with what we know about the USB standard and developing real time operating systems, can that functionality be used to create a dual purpose device?
- Research Q's are more specific

Proposed Research - Questions

- **RQ1**: What is the baseline or minimum hardware these devices are running?
- **RQ2**: What software is being used on these devices? OS, libraries...
- **RQ3**: Can the software/firmware be modified? FreeRTOS/ReconOS/VXWorks.
- **RQ4**: If so, how much can be modified in memory? Is manually reflashing possible?
- **RQ5**: Assuming reflashing is possible, can the original OS keep original functions and be used as a HID clone or hub?

The answers will be drawn from surveyed data (e.g., datasheets, technical specs, in-memory).

Methodology

- Research process has several parts:
  - Identify sample population (e.g., most popular and available printers)
  - Technical specification and datasheet gathering
    - Pull information regarding hardware, capabilties, and I/O
  - Hardware teardown and documentation
    - Take photos throughout process and identify hardware components
    - E.g., SNBC BTP-S80 has ARM Cortex M4, NXP LPC4078FET208
  - Using debug tools, gather firmware and bootloader information

Methodology - Approach

- Quantitative
- Cross sectional surveys
- Small sample of population specifications
  - Serial printer device
  - SoC/flash memory datasheets
- Best for gathering and comparing data in-time, not over long periods.

Specifications	
Max print speed	120mm (Two-Color), 150mm (Grayscale), 250mm (Mono)
Printing method	Direct Thermal
Paper roll type	9 x 7, 82.5 x 80 x 57.5mm
Bar code support	UPC-A, UPC-E, EAN8, EAN13, Code39, Code93, CODE128, CODABAR, ITF, PDF417, QR Code, Maxicode
Printer interpreter	ESC/POS
Interfaces	Serial+USB+Ethernet USB+Parallel USB+Serial USB+Bluetooth USB+WiFi USB Only
Supported OS	32-bit (Windows XP/2000/POSReady) 64bit (Windows XP/Server 2012) 32/64bit (Windows 10/8.1/8/7/Server 2008/Server 2003/Vista) Other (Linux/OPOS/BYJavaPOS Windows/BYJavaPOS Linux)
Development Kit	Android, iOS
Data Buffer	Receive Buffer RAM: 64KB RAM Bitmap: 128KB Flash Bitmap: 512KB
Power Supply	AC 100 ~ 240V, 50/60 Hz Adapter
Current/Power Usage	2.0A / 60W
Safety and EMI	FCC/UL

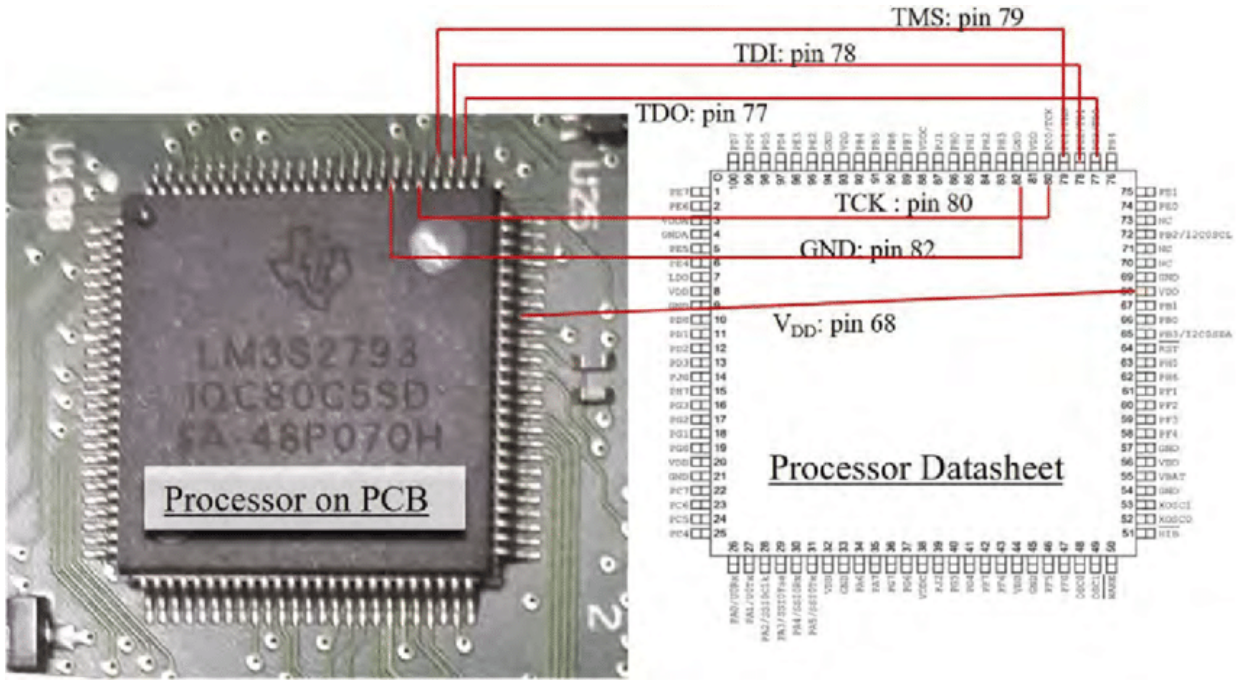
Example of Surveyed Device Specifications

Specifications	
Architecture	32-bit ARM
Platform	ARM Cortex-M3
Frequency	80-MHz, 100DMIPS performance
Memory	128KB single-cycle Flash memory 64KB single-cycle SRAM
Firmware	Internal ROM loaded with StellarisWare
Advanced Comm. Interfaces	UART, SSI, I2C, I2S, CAN
Debug Interfaces	JTAG, SWD
Package format	100-pin LQFP 108-ball pin BGA

Example of Surveyed SoC Datasheet

Specifications	
Single power supply operation	2.7 to 3.6V
Software Features	SPI Bus Compatible Serial Interface
Memory architecture	Uniform 64KB sectors 256 byte page size
Programming	Page programming (up to 256 bytes) Operations are page-by-page basis Accelerated mode via 9V W#/ACC pin Quad page programming
Erase commands	Bulk erase function Sector erase for 64KB sectors Sub-sector erase for 4KB and 8KB sectors
Protections	W#/ACC pin used with Status Register Bits to protect specified memory regions andconfigure parts as read-only One time programmable area for permanent and secure identification
Package format	16-pin SO 8-contact WSON 24-ball BGA, 5x5 pin config 24 ball BGA, 6x6 pin config

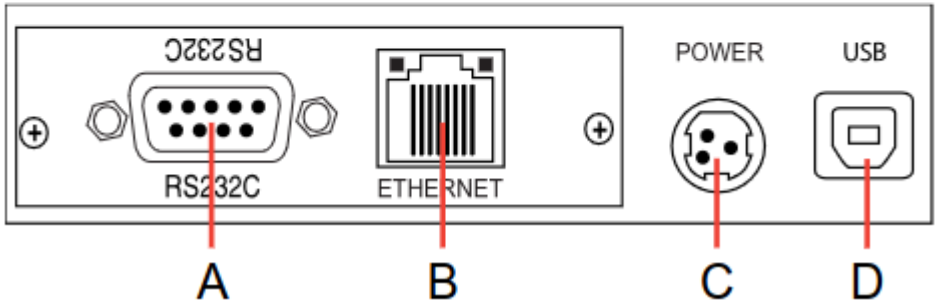
Example of Surveyed Memory Datasheet



Hardware Disassembly and Analysis

Ports and Connectivity

A Serial Port
B Ethernet Port
C DC 24V Power-In
D USB Port
E Cash Drawer Port



Example Serial Printer – SNBC BTP-S80

Task	Duration	Start Date	End Date
Review	7 days	06 Nov 23	13 Nov 23
Reread proposal paper	1 days	06 Nov 23	07 Nov 23
Review each related works	3 days	07 Nov 23	10 Nov 23
Take notes	1 day	10 Nov 23	11 Nov 23
Prepare work environment	2 day	11 Nov 23	13 Nov 23
Surveying	7 days	13 Nov 23	20 Nov 23
Gather list of most popular printers and acquire	4 days	14 Nov 23	17 Nov 23
Collect technical datasheets and specifications	2 days	18 Nov 23	19 Nov 23
Verify I/O and document before teardown	1 days	20 Nov 23	20 Nov 23
Disassembly	12 days	20 Nov 23	03 Dec 23
Disassemble each printer	3 days	20 Nov 23	22 Nov 23
Document interior/exterior of devices	1 days	23 Nov 23	23 Nov 23
Identify device components	3 days	24 Nov 23	26 Nov 23
Document interior/exterior of devices	3 days	27 Nov 23	29 Nov 23
Attempt hardware debug	1 days	30 Nov 23	30 Nov 23
Identify software/hardware protections	3 days	01 Dec 23	03 Dec 23
Writing	3 days	04 Dec 23	06 Dec 23

Research Timeline

Conclusion

Financial cybercrime is a growing concern as more criminals target those systems and their customers. Although, PoS systems are not a key component for those crimes it is important to secure them and investigate potential concerns before they do. The accessory devices that these systems use can be leveraged, specifically insecure or poorly designed printer devices.

Using the data surveyed through this research, we will be able to determine what security protections serial printer devices have. Either through the hardware compenents and the original firmware. Ultimately, knowing what limitations or obstacles there might will later help the development of a modified FreeRTOS/RTOS firmware as a BadUSB-like device; future design artifact research.