DAKOTA STATE UNIVERSITY

PrintShop: Assessing OS and Capabilities of Serial Print Devices

Micah Flack

12/07/2023

Conferences & Requirements

- IEEE Latex Format
  - https://www.ieee.org/conferences/publishing/templates.html
- Conference for paper submission
  - 37th IEEE Computer Security Foundations Symposium
    - https://www.ieee-security.org/TC/CSF2024/

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

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?

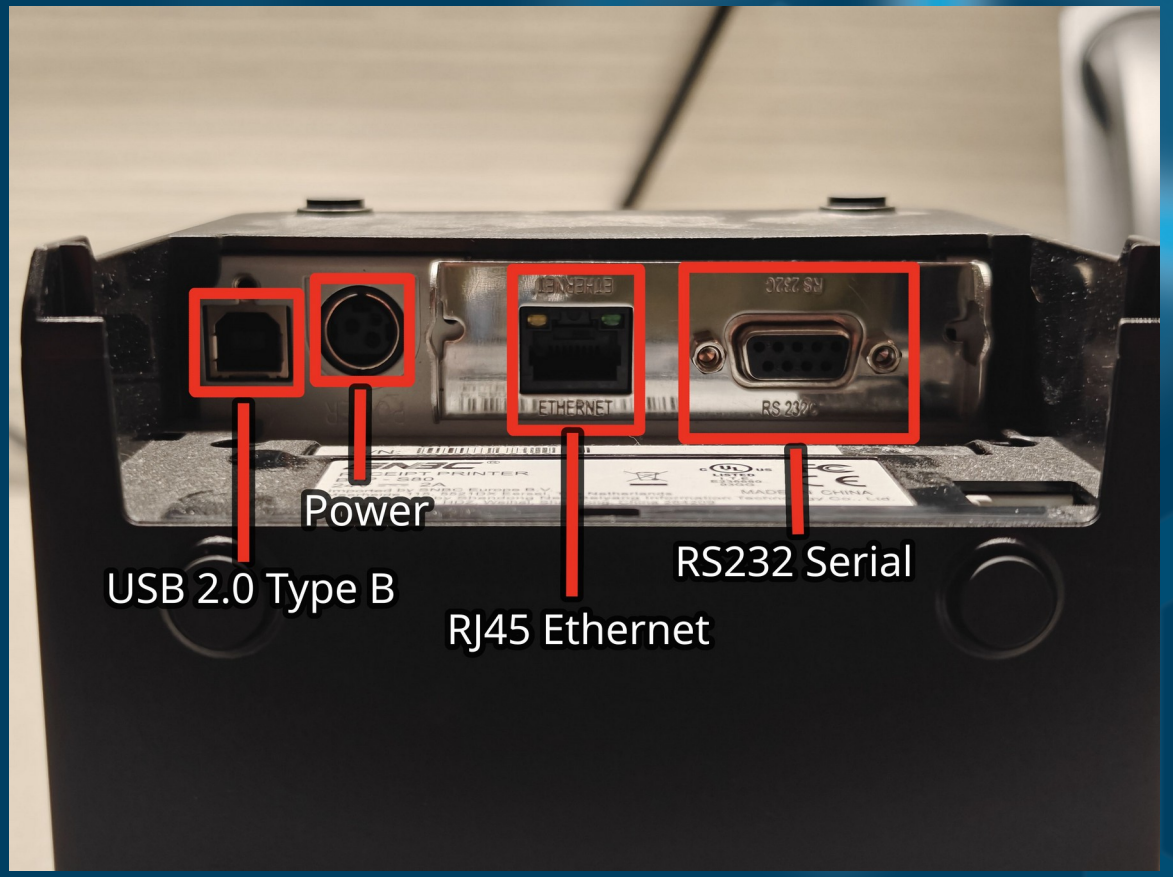
The answers will be drawn from surveyed data (e.g., datasheets, technical specs, in-memory).

Methodology

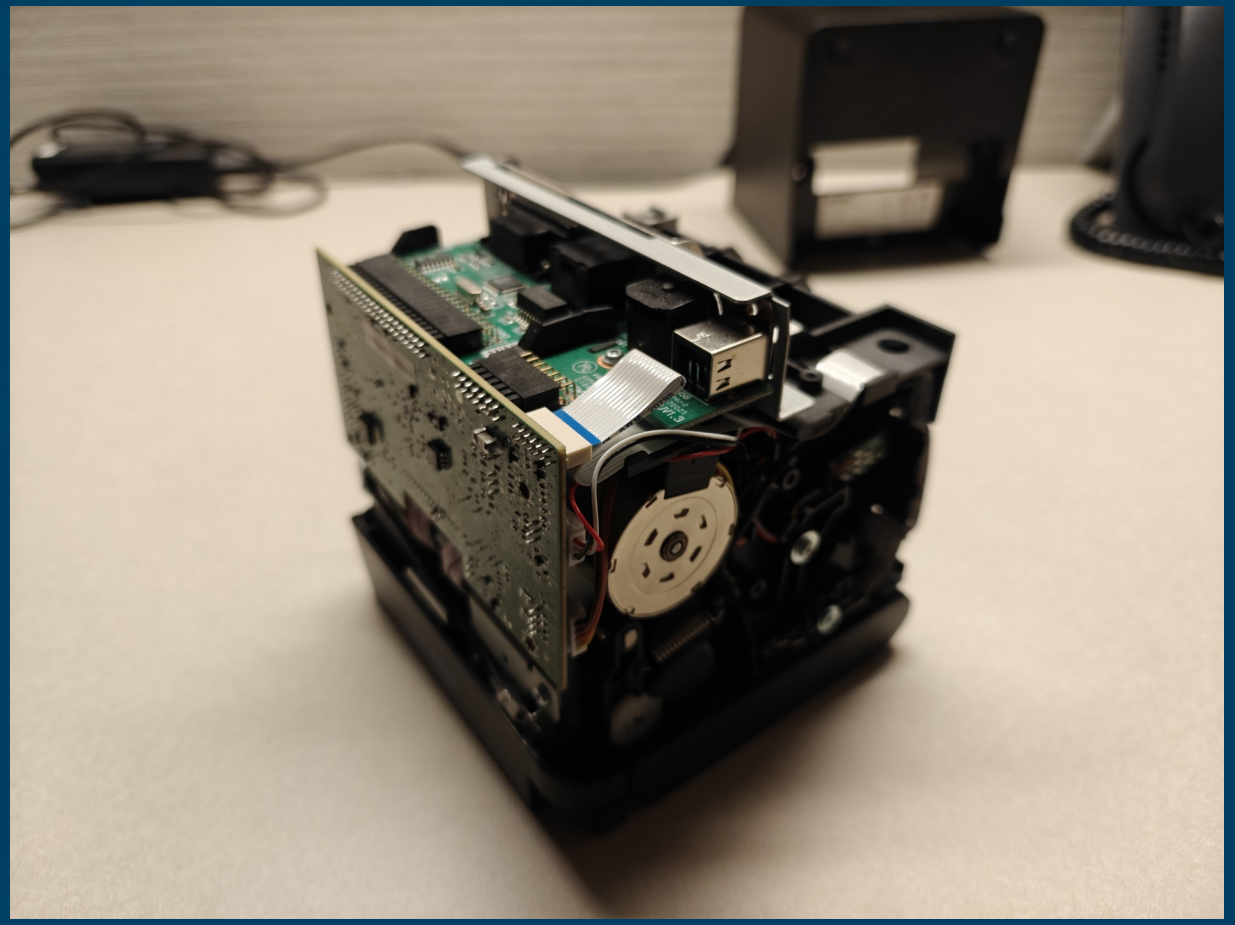
- Research process has several parts:
  - Identify sample population (e.g., most popular and available printers)
  - Technical specification and datasheet gathering
    - Pull information regarding hardware, capabilties, and I/O
  - Hardware teardown and documentation
    - Take photos throughout process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

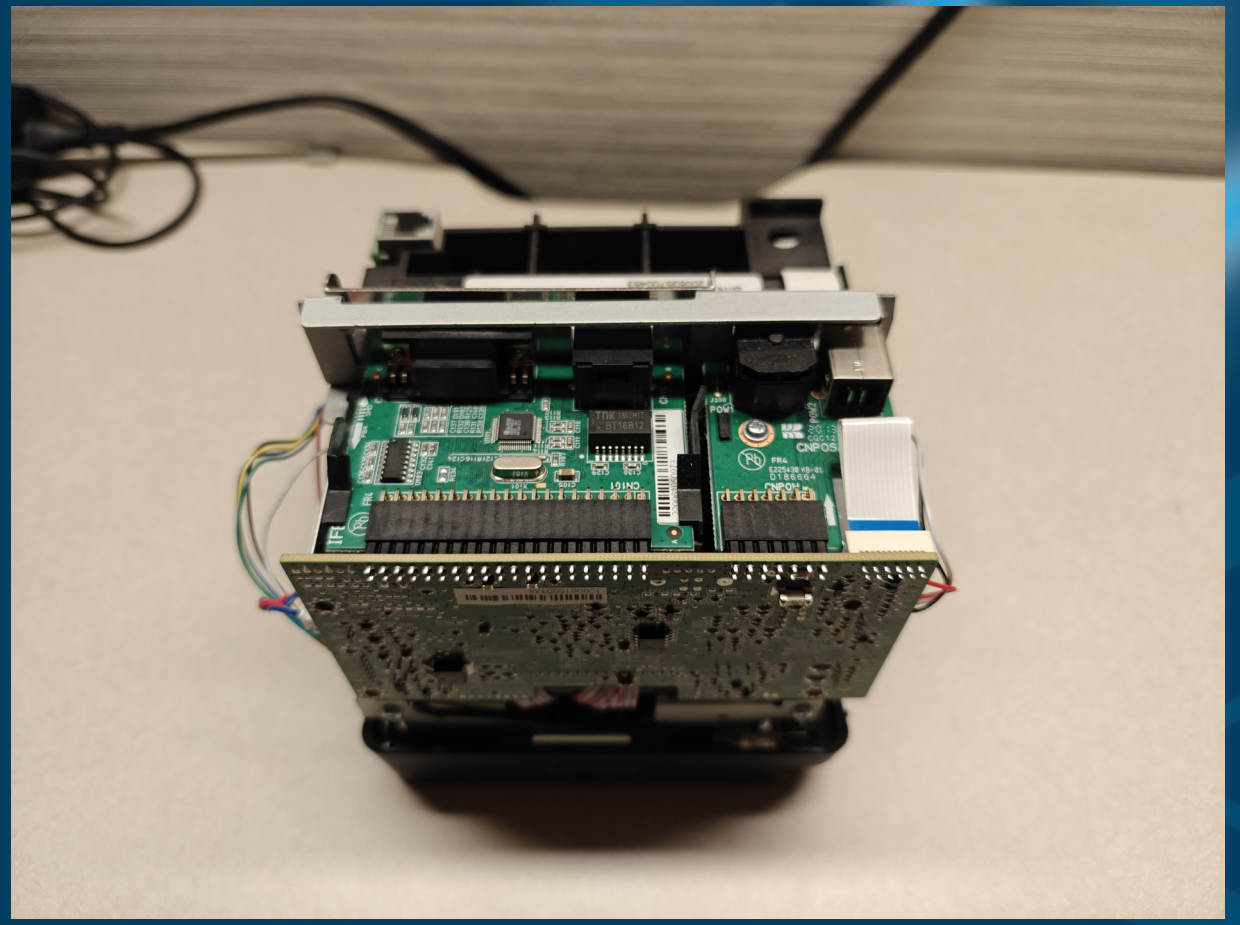
Methodology - Approach

- 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.

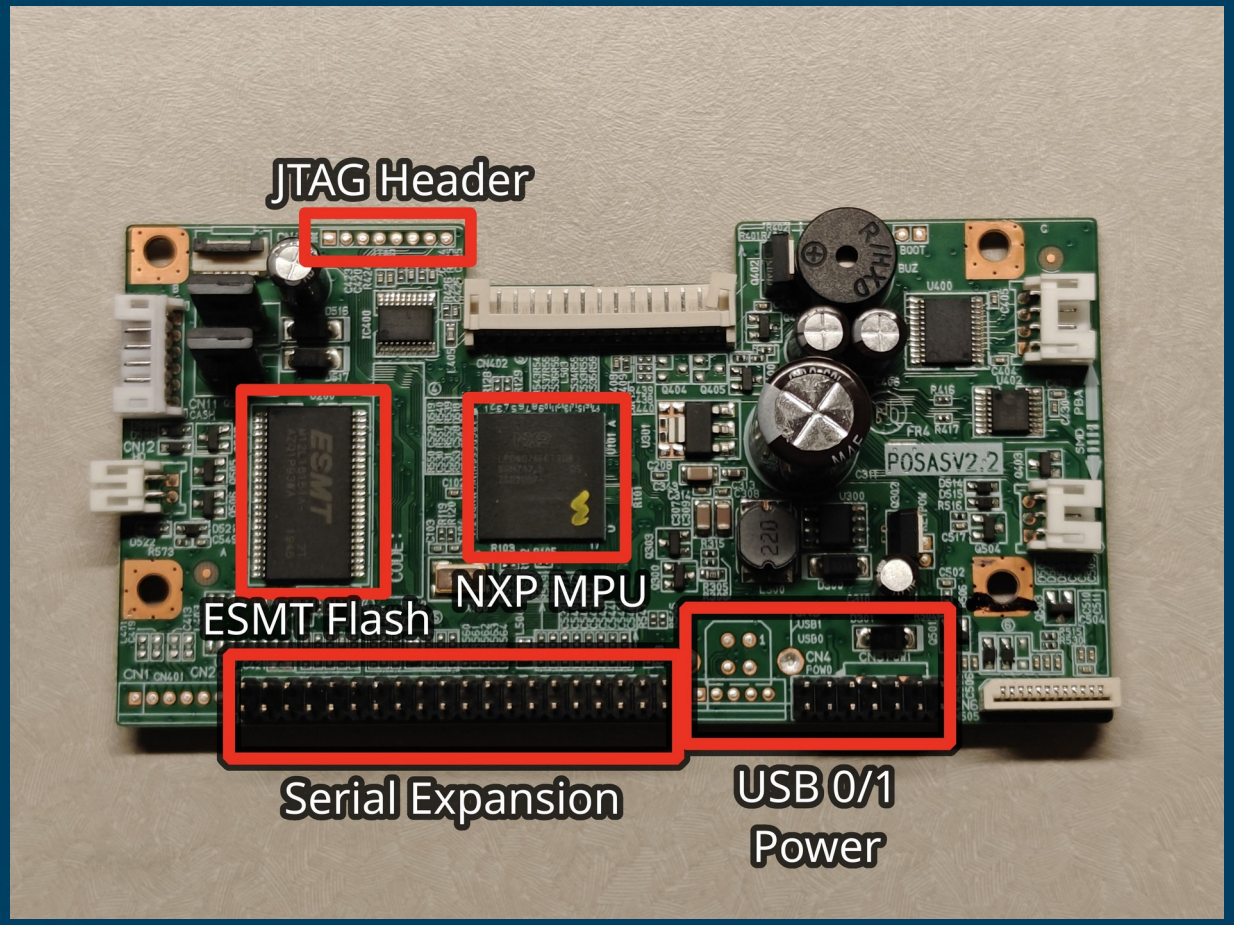


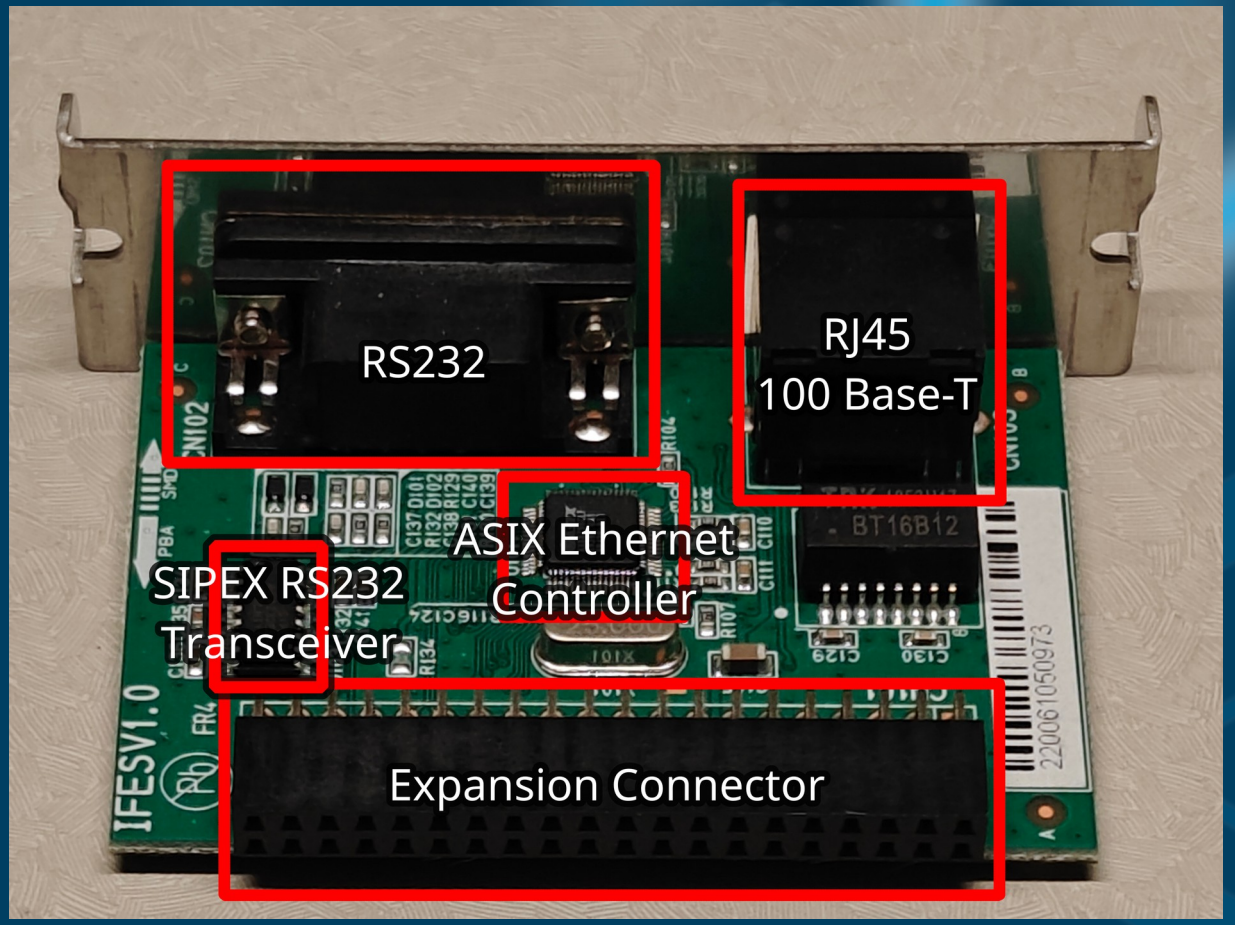
SNBC BTP-S80 (left) and labeled I/O (right)



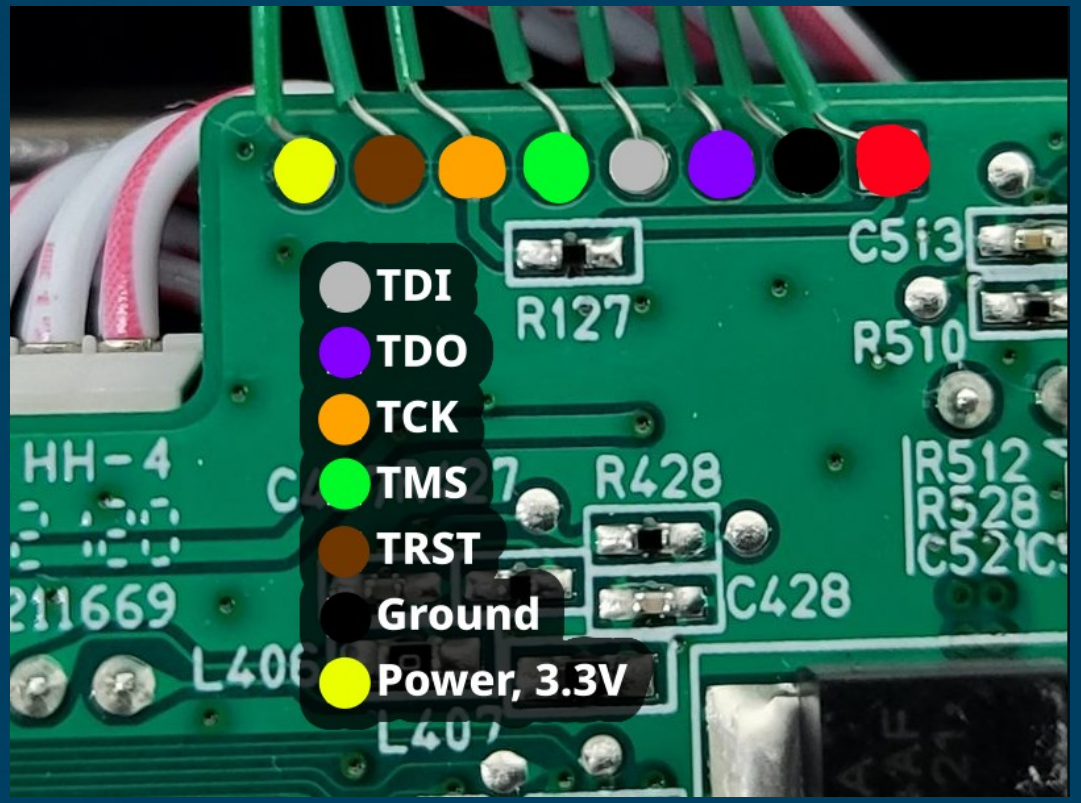


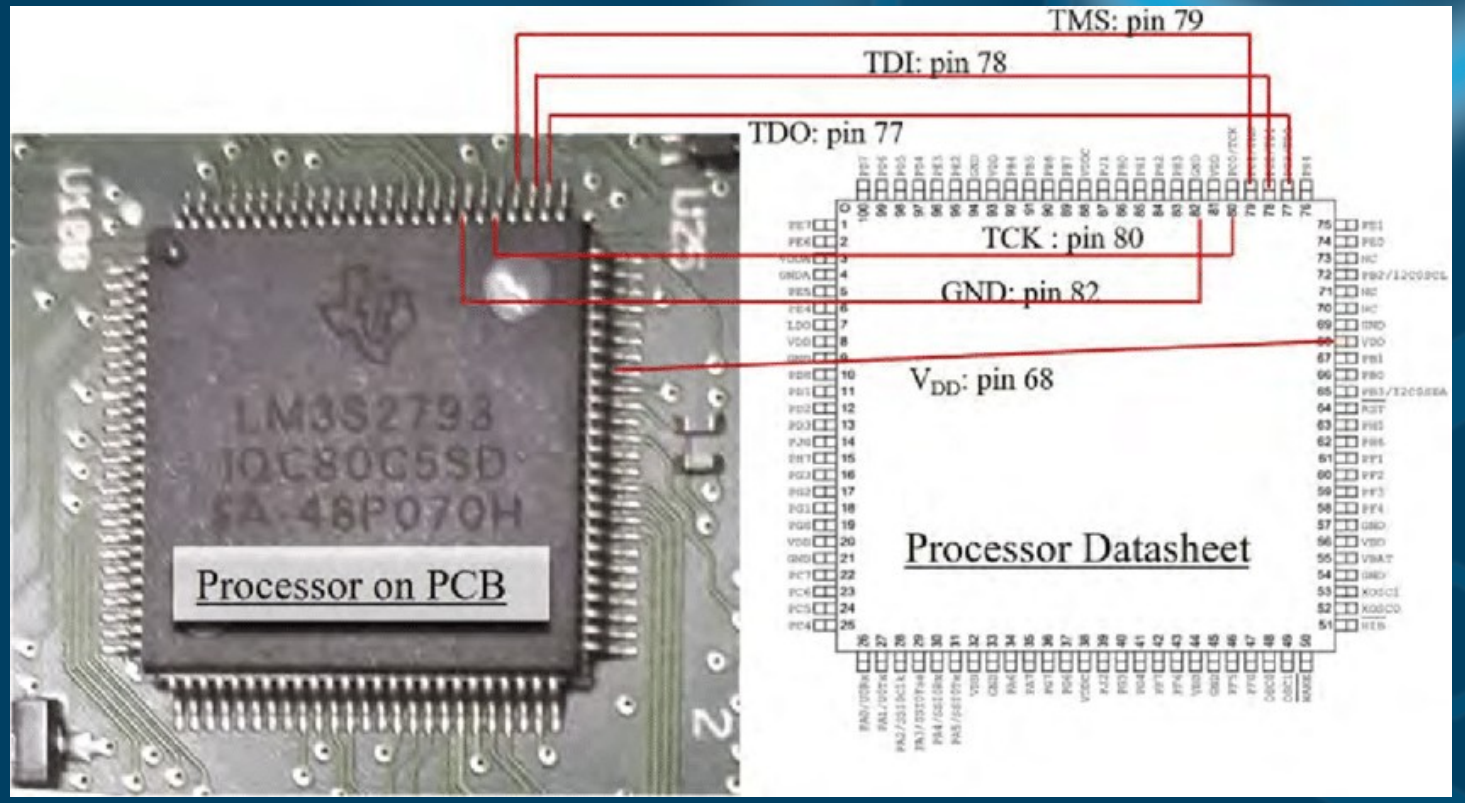
Inner chassis of the SNBC BTP-S80





SNBC BTP-S80 motherboard (left) and serial expansion (right)





Hardware Disassembly and Analysis

Technical Findings

Motherboard components:

- NXP 32-bit ARM Cortex-M4 MCU, LPC4078FET208
- ESMT DRAM, M12L16161A-7T

Serial expansion components:

- SIPEX RS-232 Transceiver, SP2209E
- ASIX Ethernet Controller, AX88796C

Firmware is stored within the EEPROM of the NXP LPC4078FET208

Technical Findings

Analysis into the recovered memory dump revealed:

- Operating system: RT-Thread RTOS
  - Version FV1.040.00
  - Indicators that firmware is shared across other products, SNBC BTP-2002NP
- Print interpreter: Epson ESC/POS
  - Version 7.00
- WebNET v1.0.0
  - Provides networking and webserver

Conclusion

In conclusion, the researcher was able to demonstrate four of the five objectives for the research.

We identified:

- Baselines of the hardware and operating system used by the serial printer
- The specific version of the operating system and supporting libraries

We demonstrated:

- That the manufacturers have enabled minimal security protections despite the hardware supporting them
- It is possible to reflash the memory utilizing the MCU hardware debug interfaces.

Future Research

Due to underestimating the time needed for delivery of the additional devices for the proposed sample population, only one device was assessed.

Although the SNBC BTP-S80 is a fairly common serial printer used across financial sectors as well as industrial control, the research would have been better represented with the cross-examination against several other devices.

Lastly, another goal of the research was to use the gathered data to support the proposal of future research into a design artifact for implementing BadUSB-like concepts on peripheral serial devices.