PrintShop: Serial Printer Environments and Security

March 19th, 2024

Micah Flack

> whoami

Cybersecurity Researcher @ Idaho National Laboratory (INL)

- Malware Analysis / Software & Hardware RE / Exploit Development (Embedded)

B.S. in Cyber Operations @ Dakota State University (DSU) in 2019

M.S. in Computer Science @ DSU in 2020

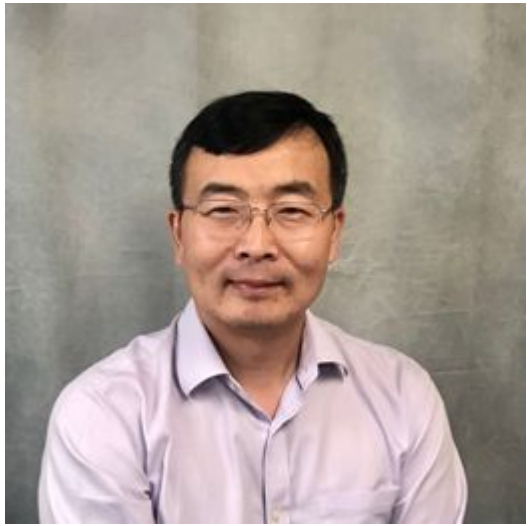
Enrolled for Ph.D. in Cyber Operations in 2021

https://micahflack.com/

Dissertation Committee

Dr. Varghese Vaidyan (Chair)

Dr. Michael Ham



Dr. Yong Wang

Presentation Structure

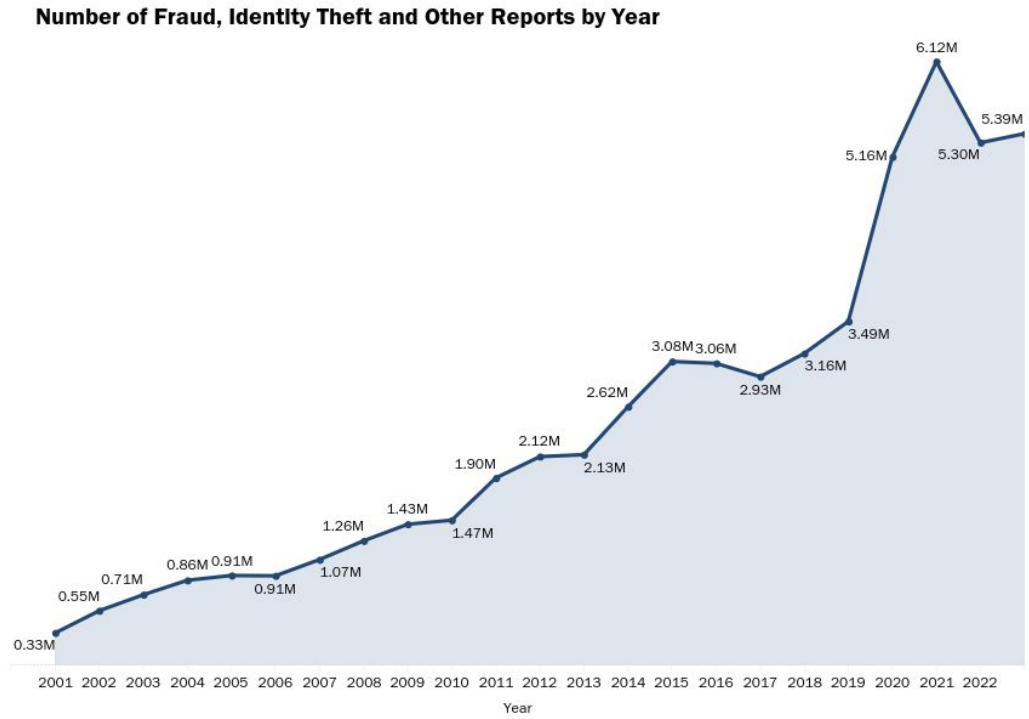
- Problem Statement
- Goals and Objectives
- Literature Review
- Methodology
- Novelty and Contributions
- Timeline

Problem Statement

Securing supply chains for critical infrastructure and any production environment is a growing concern (Roshanaei, 2021). Third-parties or nation state level attackers have been shown to target employees or infrastructure indirectly to gain access to their target's network (Makrakis, 2021; Goodin, 2023).

One of the devices being examined to aid this research is the SNBC BTP-S80, a USB/serial connected thermal printer. These devices are made with foreign software and hardware, and they are used “off-the-shelf” without any security review (Eggers, 2021). In some instances, the devices implement an MPU/MCU and an FPGA for I/O processing. There is potential at a firmware level for either component to manipulate data or be used maliciously (Rajkumar, 2021).

The proposed research aims to assess these devices for any risks and demonstrate that they could be used as a part of supply chain attacks.



Year	# of Reports
2001	325,519
2002	551,622
2003	713,657
2004	860,383
2005	909,314
2006	906,129
2007	1,070,447
2008	1,261,124
2009	1,428,977
2010	1,470,306
2011	1,898,543
2012	2,115,079
2013	2,134,565
2014	2,620,931
2015	3,080,378
2016	3,060,824
2017	2,926,167
2018	3,161,213
2019	3,485,938
2020	5,156,880
2021	6,122,341
2022	5,300,157
2023	5,392,028

Credit Cards and Loss Protection‡	Credit Cards and Loss Protection‡	74,885	1.22%	89,757	1.69%	101,427	1.88%

Federal Trade Commission, 2023

Goals and Objectives

- Q1: Can the hardware be reflashed with a modified firmware image (e.g., FreeRTOS, ReconOS, VxWorks)?
- Q2: Does the hardware and firmware have enough resources to support HID functionality on-top of printing?
- Q3: Besides HID cloning, what other threat areas are exposed (e.g., network stack, web management portal, memory protections)?

Literature Review

Spydruino is a working example of a programmable BadUSB attack using an Adruino to mimic the desired Human Input Device (HID) (Krystinos, 2019).

- Uses similar hardware and architecture to the serial printers
- Different software platform and does not use existing hardware
- Cannot mimic existing printer functionality and act as clone

The majority of attacks against PoS systems do not use the proposed delivery method (Scaife, 2018).

- Attacks limited to mobile device (not PoS systems)
- Already assume access for deployment of attacks (in-memory attacks)
- Target cards directly via skimming (PINs, NFC, magnetic stripe data)
- EMV cloning/pre-play attacks (Bond, 2014)

Literature Review - Cont'd

(Yu, 2019) introduces several common RTOS and discusses their security issues.

- There is a trade off where performance is the main criteria and security is not a priority.
- Depending on the MPU (microprocessor unit), the vendor has hardware protections like Intel SGX or Arm Trust Zone.
- Susceptible to code injection, cryptography inefficiency, unprotected shared memory, priority inversion, denial of service attacks, privilege escalation, and inter-process communication vulnerabilities.

Literature Review - Cont'd

There are instances where the user device is compromised by malware specifically for exfiltrating banking data or similar PCI, but further discourse is outside the scope of the proposed research (Darvish, 2018).

- Attacks target mobile devices (e.g., Android) and not the PoS systems (e.g., RTOS/Linux/Windows); additional platforms are outside of the proposed scope.

(Hizver, 2012) demonstrated a successful introspection-based memory scraping attack against nine commercial PoS applications.

- Targeted memory across multiple VMs within a shared virtualization platform (Xen Hypervisor)

Literature Review - Cont'd

BadUSB is a well-known and documented attack vector. One of the most popular hacker tools is built-on the concept (Thomas, 2021). However, there are some limitations:

- Precision of attacks is limited since scripts or effects are typically deployed blind. There is no knowledge of the user environment nor ability to interact with functional user interface mechanisms (e.g., a mouse clicking a button); the same goes for the proposed method.
- There are existing methods for limiting USB access from the host, such as GoodUSB (Tian, 2015); use of agents or monitoring software is left to the user/maintainer.
- Requires being physical present to attach another device; different delivery method

Literature Review - Cont'd

(Tian, 2018) describes several attacks at each of the applicable layers to USB standard:

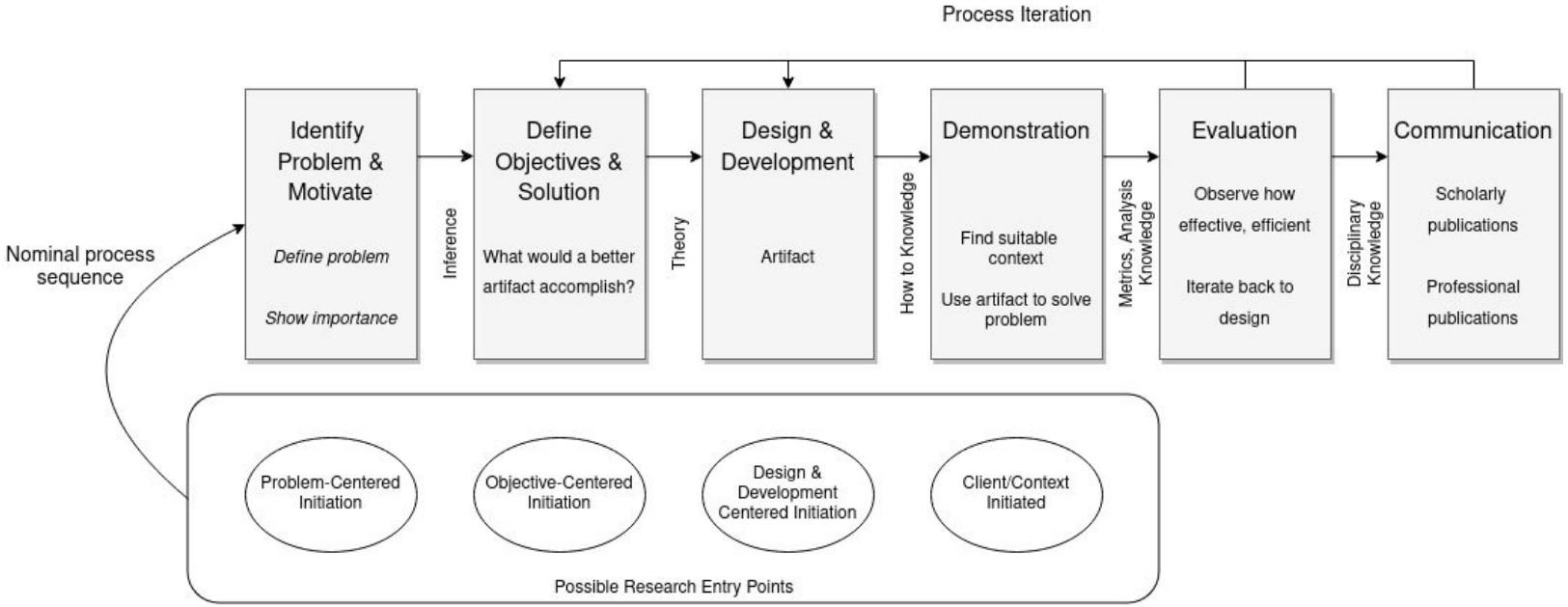
- Human, application, transport, and physical layer.
- Require some human element to deploy because attackers need to be within close proximity.
- Physical layer exposes the host or device to signal eavesdropping or side-channel attacks.
    - Require purpose built hardware to achieve (e.g., USB overvolting, TEMPEST) - usually not possible via changes to only firmware.

Methodology

For this research, the quantitative approach and case study research will be used (Babbie, 2017; Creswell, 2017) to create a design artifact.

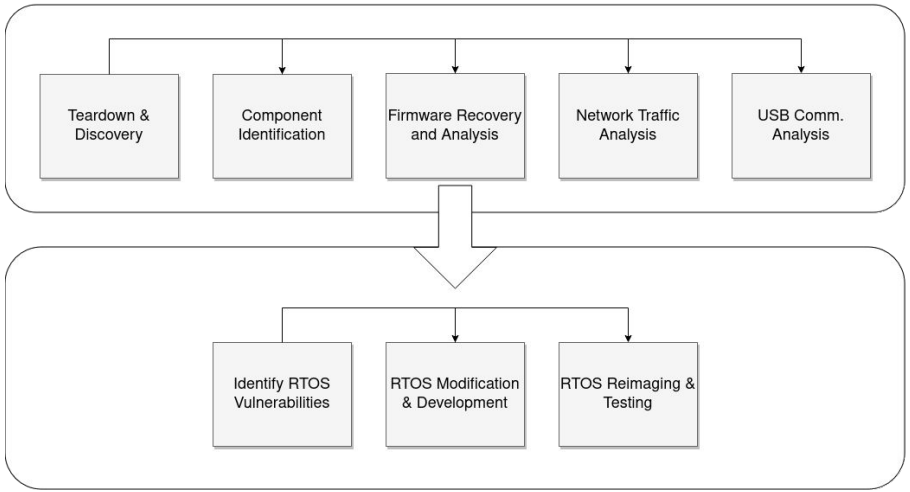
The goal being to gather and examine, point-in-time, data from a serial printer device as a common sample representative of the affected population.

By using quantitative survey research, it is possible to evaluate potential vulnerabilities for the attacks hypothesized, as well as, prototype a modified firmware image to use them against the host environment.



DSR Methodology, (Peffers et al. 2007)

Research Design



Research Design - Data Collection

The device is disassembled and documented at each step. Pictures are taken of each component, part numbers are identified, and technical datasheets are collected.

Process goes hand-in-hand with hardware assessment.

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

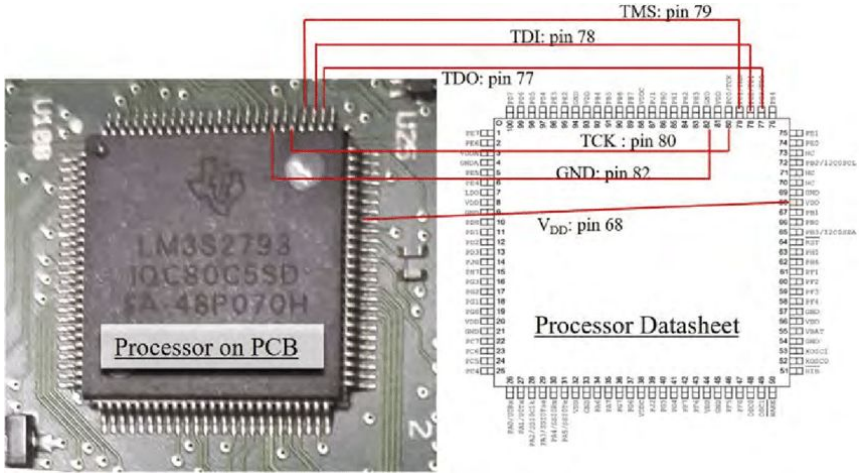
Research Design - Data Collection

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

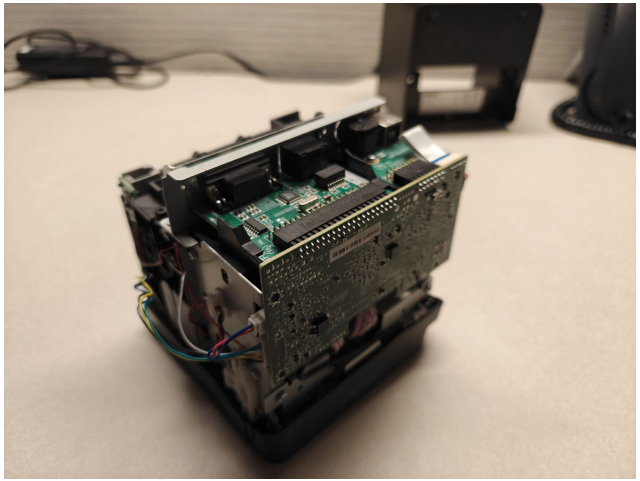
Research Design - Hardware Assessment

The device is disassembled and documented at each step. Pictures are taken of each component, part numbers are identified, and technical datasheets are collected.

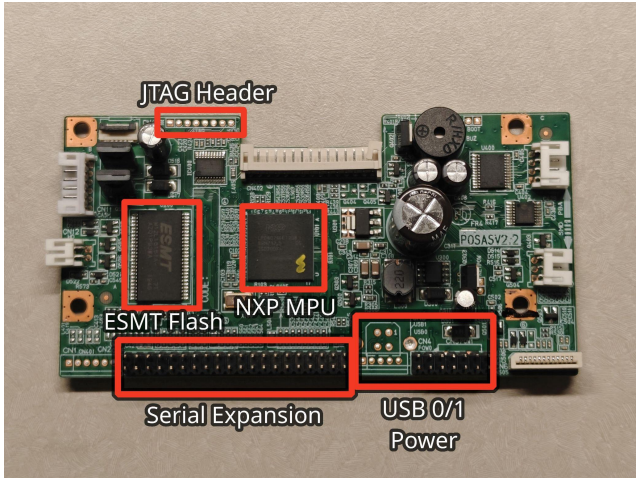
Using information from the prior step, component function is identified and any information needed to interface with the component is documented.

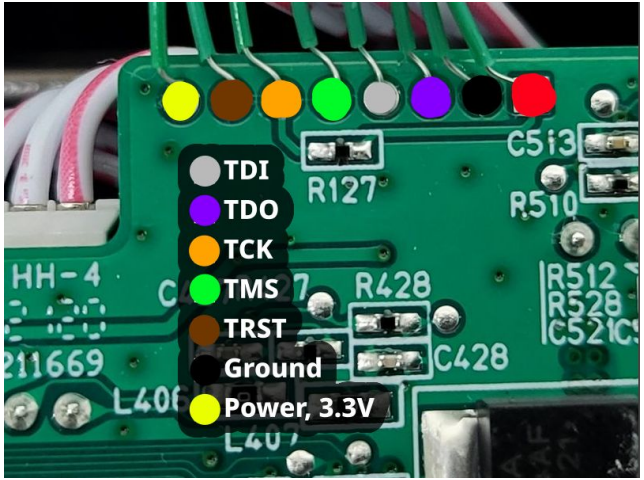


Research Design - Hardware Assessment



Research Design - Hardware Assessment





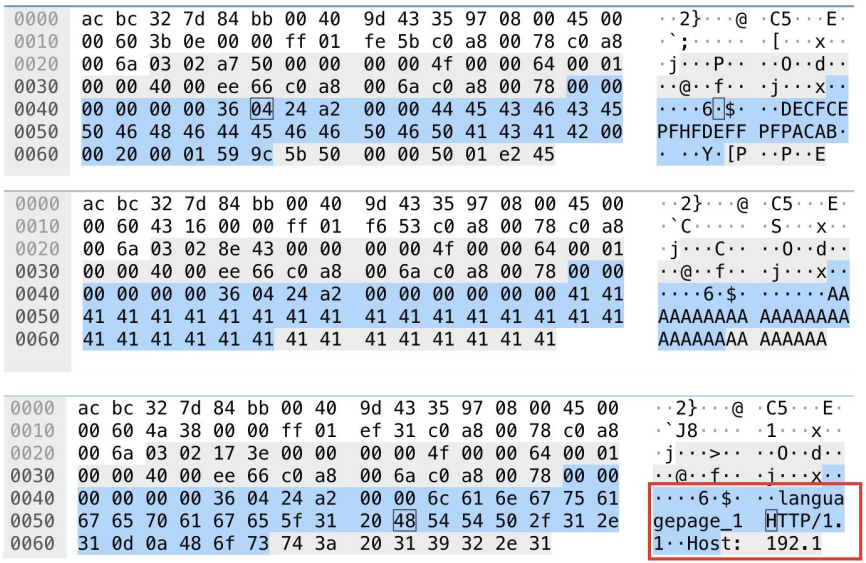
Research Design - Network Traffic Analysis

Any network traffic created during use is captured and analysed using software tools (e.g., WireShark).

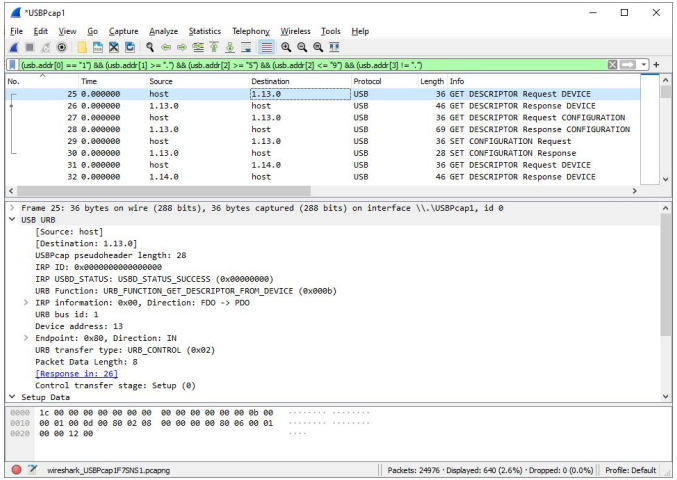
In conjunction with prior firmware analysis and identification of operating system libraries, communications are reviewed for potential vulnerabilities.

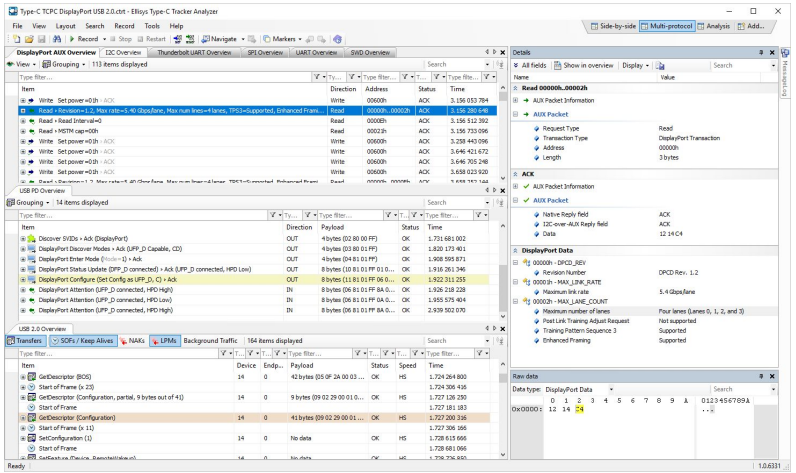
This is a possible area for remote code execution (RCE) if the management software is poorly implemented, (OWASP, 2024; Rajkumar, 2021).

Ripple20 is such an example (NVISO, 2020)



Research Design - USB Comm. Analysis





Research Design - Firmware Analysis

Using the technical datasheets, firmware is recovered and analyzed in a disassembler (e.g., Ghidra).

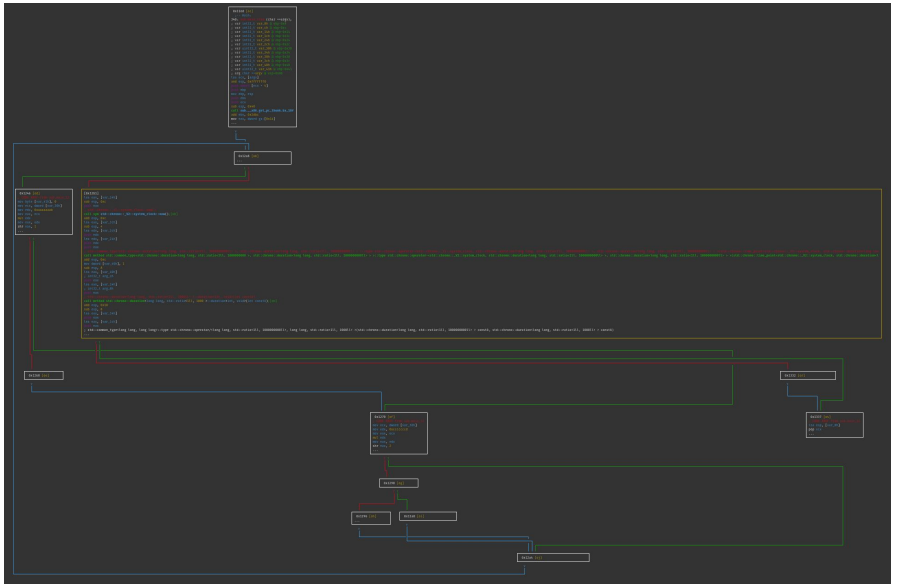
Libraries used by the operating system and their open source repositories are documented and collected at this stage.

Potential vulnerabilities can be identified within the firmware and libraries by comparison of source code or rebuilding the firmware with debug symbol information.

- RT-Thread: RTOS based operating system of the target printer
- WebNet: HTTP networking library
- Epson ESC/POS: Print interpreter library

Research Design - Firmware Analysis

```cpp
#include <iostream>
#include <chrono>

int main()
{

    int fizz = 0, buzz = 0, fizzbuzz = 0;

    bool isFizz = false;

    auto startTime = std::chrono::high_resolution_clock::now();

    for (unsigned int i = 1; i <= 4000000000; i++) {
        isFizz = false;

        if (i % 3 == 0) {
            isFizz = true;
            fizz++;
        }

        if (i % 5 == 0) {
            if (isFizz) {
                fizz--;
                fizzbuzz++;
            }
            else {
                buzz++;
            }
        }

    }

    auto endTime = std::chrono::high_resolution_clock::now();
    auto totalTime = endTime - startTime;

    printf("\t fizz : %d, buzz: %d, fizzbuzz: %d, duration %lld milliseconds\n",
           fizz, buzz, fizzbuzz, (totalTime / std::chrono::milliseconds(1)));

    return 0;
}
```

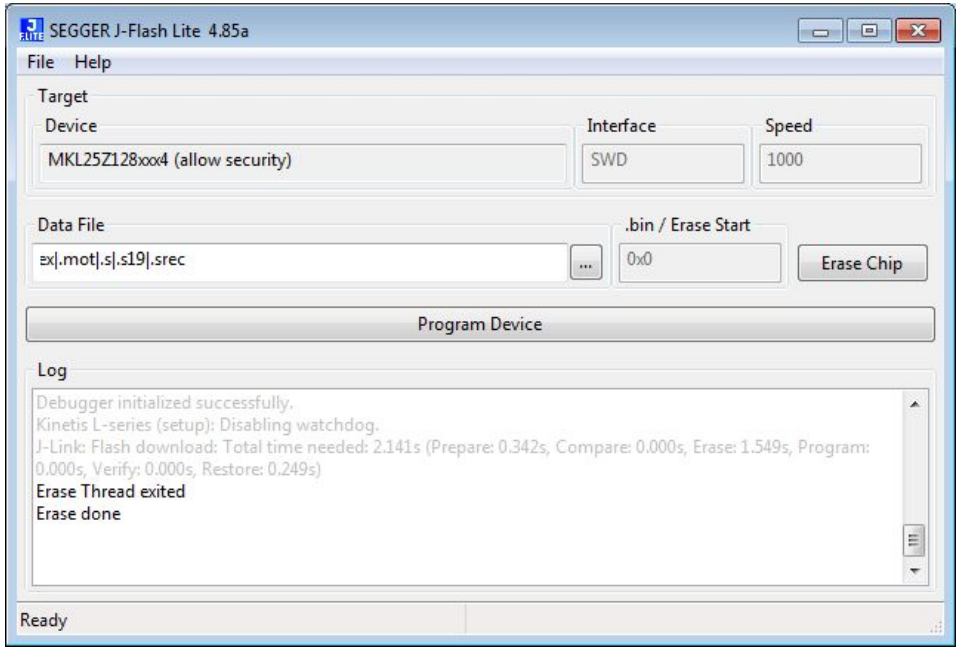


Research Design - Modify Firmware

Should analyses identify any exploitable vulnerabilities, further research is conducted to discover any public releases or proof of concepts (PoCs).

Open source RTOS firmware is modified to allow HID cloning while maintaining original print functionality. The attack vector is crucial step towards proving viability of supply chain attacks using the print devices.

Firmware is built and reimaged/reflashed onto the target device. Testing will include the verification of Epson ESC/POS commands interpreter operation and HID attack vector.



Novelty and Contributions

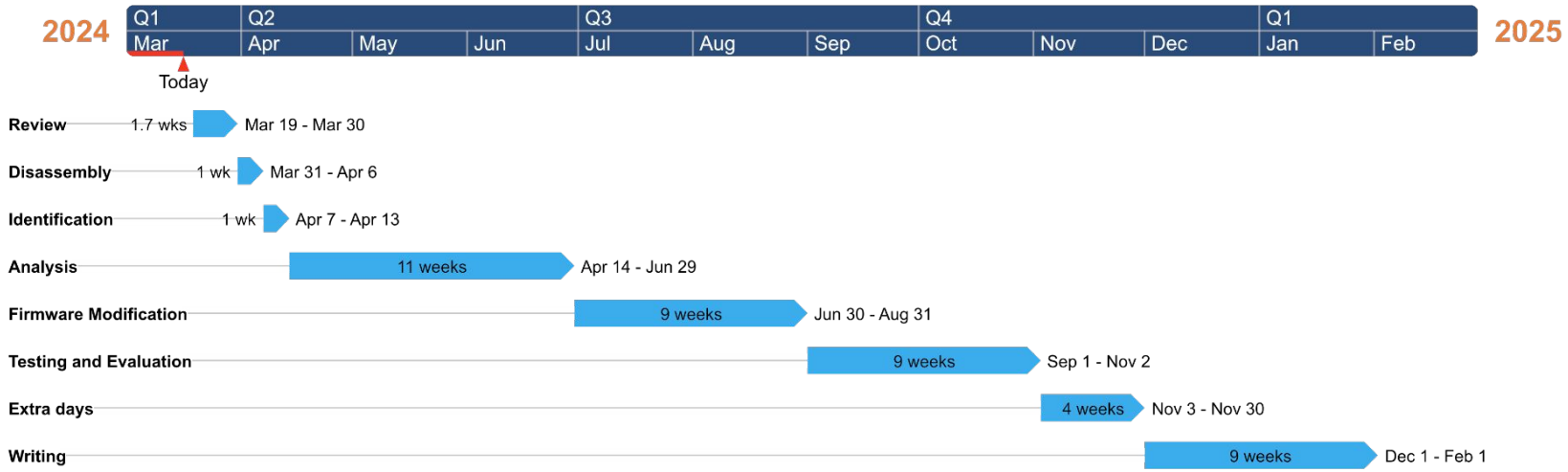
Contributions:

- Creation of design artifact (modified firmware) for testing auxiliary device attacks against host
  - Passing testing, there is potential to demonstrate and explore more attacks using the delivery method
- Demonstrating threat of supply chain attacks to PoS systems and similar environments
  - Uniquely, serial printer devices against Linux and Windows systems

Novelty:

- BadUSB/HID attacks are well documented and within the “known”
- But, the delivery method used and the target environment is a research gap
- If attacks are possible given the constraints of existing hardware and software functionality

Timeline


2024
Q1
Q2
Q3
Q4
Q1
2025
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Today
Review
1.7 wks
Mar 19 - Mar 30
Disassembly
1 wk
Mar 31 - Apr 6
Identification
1 wk
Apr 7 - Apr 13
Analysis
11 weeks
Apr 14 - Jun 29
Firmware Modification
9 weeks
Jun 30 - Aug 31
Testing and Evaluation
9 weeks
Sep 1 - Nov 2
Extra days
4 weeks
Nov 3 - Nov 30
Writing
9 weeks
Dec 1 - Feb 1

Audience - Q&A