PRINTSHOP: ASSESSING OS AND CAPABILITIES OF SERIAL PRINT DEVICES

Dissertation Proposal Outline

Doctor of Philosophy

in

Cyber Operations

September 15, 2023

By

Micah Flack

Dissertation Committee:

Dissertation chair

Dr. Someone Name

Dr. Another Person

...

Beacom College of Computer and Cyber Sciences

TABLE OF CONTENTS

Chapter 1

1.1 Introduction

Section Outline:

- Discuss why we are looking into serial printer devices
- Explain what platforms there are
- What are the current threats
- What will this information be used for?
- State the research questions and goals

1.2 Background

Section Outline:

- Further background on specific devices, manufacturers, platforms, and architectures
- Do these devices get hijacked often? Explain it: how, when, by what...
- Statistics on point-of-sale (PoS) systems involved in financial cybercrime
- Where are the majority of cybercrimes committed
- How does this involve serial printer devices?

- Maybe, include background info on the platforms (FreeRTOS/RTOS/Yocto)

- Introduce common methods used for researching these devices

Chapter 2

2.1 Literature Review

Section Outline:

- None of the papers to be used for this proposal have been decided yet.
- Once that has been decided, each paper will have it's own section/subsection.
- And, the papers will be reviewed based on their contributions.
- This section will also be useful for establishing what is current.

Chapter 3

Proposed Research

3.1 Research Objectives

Section Outline:

- The goal of the research is to get an idea of what the potential ”threat map” looks like.
- With the technical ”specs” for the hardware and OS, can we manipulate device capabilities?
- What capabilities can we extend or add?

3.2 Research Questions/Hypotheses

Section Outline:

- What is the baseline or minimum hardware these devices are running?
- What software is being used on these devices? OS, libraries...
- Can the software/firmware be modified?
- If so, how much can be modified? In memory? Reflashed?

- Given hardware baseline, what does that performance support? Intended functions plus a webserver?

3.3 Methodology

Likely, but not limited to the following:

- Gather recent research within the last 5-10 years for manufacturer/device shares of the market
- Gather technical sheets and specs for the most popular devices
- Take note of the hardware specs for each device as well as firmware used
- Create default/debug images of each popular devices' firmware - what is natively supported?
- Is there room to add functionality without crippling original function

Chapter 4

4.1 Significance

Section Outline:

- The research is significant because of the abundance of these devices.
- Proving that the devices can be used in this way could provide incentives for securing peripherals on PoS systems

Chapter 5

5.1 Timeline

Section Outline:

- Formal timeline broken down by months or quarters
- Provide expected actions and deliverables for each deadline
- Likely, Gantt chart with ”Agile” mindset

Chapter 6

6.1 Conclusion

Section Outline:

- Restate the research objectives, questions, what the research topic is and how this research will answer them.
- Briefly mention significance/impact in relation to the topic.
- Thank readers.

Self-Evaluation

Lockwood's three standards ratings:

- intellectually original [0 - 5] ... (4): I think the research goals and proposed research are novel in terms of their contributions and application of existing research. It's important to take research, see where it can be applied and then actually prove that it can be. With this project it is more than taking an exactly replicable idea and tossing it at an undocumented piece of hardware. It will require significant research and development time.

- technically substantial [0 - 5] ... (3): Again, the ideas are out there and have been used similarly. But they have not been used for this type of device nor type of platform. The exact definitions for how this differentiates from previous works could use some massaging to prevent confusion.

- socially constructive [0 - 5] ... (3): Similar to the second standard, finding the exact wording to stress the significance and utility of the work is required. Regardless, these devices are seen everywhere and not just on PoS systems. They can be found on critical infrastructure and industrial control systems or human-machine interfaces where paper reporting is used. Assessment and then creation of a proof-of-concept as future work would, in my eyes, be a novel contribution.