**Deliverable #1: Project Overview**

**Project: IoT Vulnerability Research Project**

**Participants:**

* Vikram Kher
* Varin Jaggi
* Tarik Wilkinson
* Patrick Kakooza
* Liza Moody
* Haoda Wang

**Introduction:**

This semester-long CSCI401 capstone project will consist of attempting to exploit security faults in a “LaView” device. As part of this project, the members will be actively involved in analyzing both the hardware and software components of the security camera. The ultimate goal of the project would be to learn how to maliciously alter the behavior of the camera. For example, one final goal might be to gain the ability to remotely reset its camera view or alter its image output.

**Estimated Timeline:**

**Deliverable 2 Due February 6, 2022**

For deliverable 2 we are going to focus on researching the “LaView” device we will be working with this semester.

1. **Hardware Teardown**
   1. During this phase we will be disassembling the device and examining the design of the device.
2. **Information Research**
   1. During this phase, we are going to identify ICs within the device’s PCB(s) on “DigiKey Electronics” and “Electronic Components Distributor.”

**Deliverable 3 Due February 20, 2022**

For deliverable 3, we will focus on analyzing the different hardware components found in the Laview security camera device. As part of this analysis will conduct a memory extraction procedure on the device.

1. **Hardware Analysis** 
   1. Using the information from the ICs listed, we will try to identify the functions of various ICs and the interconnect protocols used by them.
2. **Memory Extraction**
   1. If possible, we will attempt to extract the contents of the memory chip, which may provide a copy of the device’s firmware or running programs on the device.

**Deliverable 4 Due March 6, 2022**

1. **Firmware Analysis**
   1. The extracted memory may also provide a copy of the underlying firmware that the program uses, which we will try to reverse engineer the interconnect protocols.
2. **Header Inspection**
   1. The firmware may provide insight into how the device may be updated through header pins on the PCB. If possible, we will want to see if it is possible to flash new firmware onto this device or otherwise extract data from it.

**Deliverable 5 Due March 27, 2022**

1. **OS & File System Inspection**
   1. If we gain access to the storage, we will be able to extract a copy of the file system on the device, which may provide more insights into the device’s operation.
2. **Static Code Analysis**
   1. We will attempt to analyze the binaries used in the device through static analysis methods such as binary analysis and symbolic execution.

**Deliverable 6 Due April 10, 2022**

For deliverable 6, focus will be on analyzing network features on the security camera as well as analysis of the mobile app.

1. **Network Analysis & Protocol/Authentication Investigation**
   1. We will run the binary using knowledge gained in the previous week on a network testbed. This will let us analyze the network behaviour of the application
   2. Using traffic captured in the last week, we will attempt to reverse engineer the protocols used by the application when operating.
2. **Mobile App Analysis**
   1. We will use static analysis and network analysis methods on the app instead of the device.
3. **Data Flow Interpretation**
   1. Using the data captured from the last few weeks, we will attempt to summarize where and what data the device sends and receives.

**Deliverable 7 Due May 1, 2022**

1. **S/W Tools Development**
2. **Programming Analysis**
3. **Pre-existing PoC**
4. **Presentation**