Modelling Correct Operation of Webcams for Security Purposes

Blaine Billings and Xenia Mountrouidou

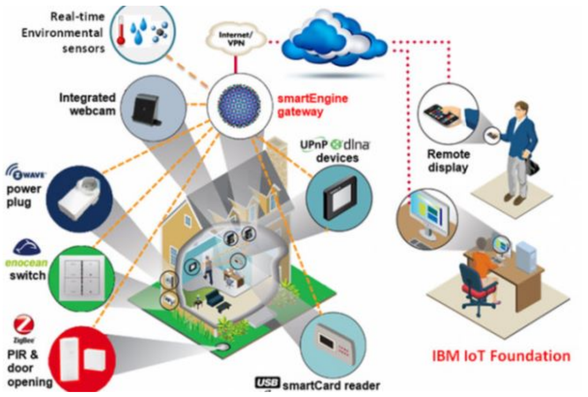
Department of Computer Science, College of Charleston, Charleston, SC

SIGCSE 2018, Baltimore, MD

NSF Award #1700254

Introduction

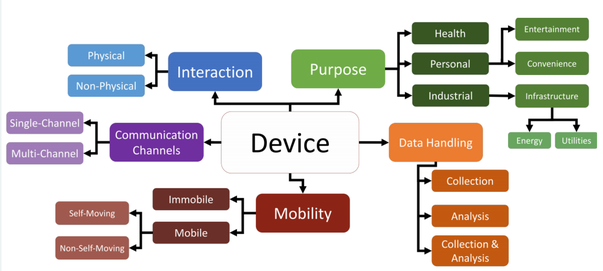
- **IoT vulnerabilities and attacks are increasing** with the rise of IoT in mainstream usage
- **IoT devices like webcams are often targeted** for malicious use, such as spam attacks, botnets, etc.
- **Being able to model correct behavior for a device** lets us better identify incorrect operation, i.e. attacks and even zero-day exploits



Modern Connected Devices of IoT
Picture Source: http://bit.ly/2EGqN0V

IoT Device Taxonomy

Classifications created for the IoT Taxonomy inspired the different characteristics for the separate Finite State Machines



Methodology and Verification

Foundation	Experimentation	Verification
• **Used IoT Taxonomy as a foundation** for identifying inherent characteristics of webcams • **What is at the core of a webcam**: sensing, acting, sending, and receiving – the basis for the four FSMs	• **Gained root telnet access** using web exploit to recover root password • **Simulated real-world scenarios** by characterizing webcam usage in different situations: home, enterprise, and infrastructure • **Ran repeatable experiments** from inside a compromised webcam in a closed environment • **Collected network traffic**, CPU and memory usage, and device process data	• **Arrived at data thresholds** to describe the states and transitions • **Derived correct operation model** to accurately and efficiently describe normal webcam behavior

State Definitions

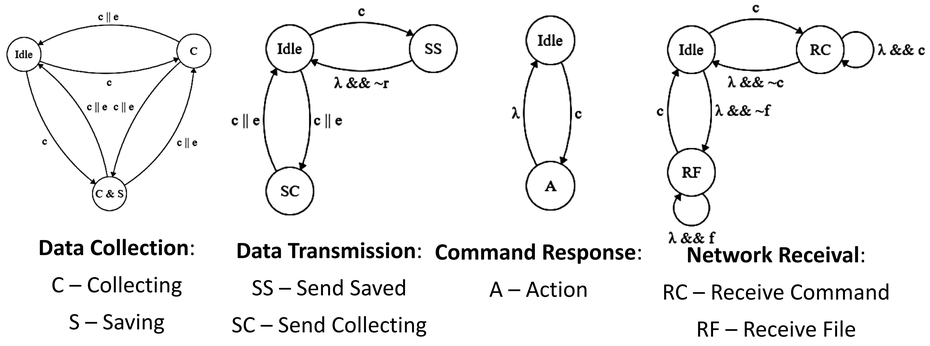
Data Vector – The Data Fields Which Characterize the Models
[Bytes In Per Second, Bytes Out Per Second, Frames Per Second, CPU Utilization, Memory Utilization, Actuator Indicator]

Idle – The device is performing no action related to the characteristic of the model in which it is idle

Data Collection	• Collecting & Not Saving – The device is collecting data from a sensor but not saving it in memory • Collecting & Saving – The device is collecting data from a sensor and saving it in memory
Data Transmission	• Send Collecting – The device is transmitting data it is collecting • Send Saved – The device is transmitting data that is saved in the system memory
Command Response	• Actions – The device is responding to an action received from outside the system
Network Receival	• Receive Files – The device is in the process of receiving a file • Receive Command – The device is in the process of receiving a command

The Finite State Machines

- **Data Collection** – Focuses on how the device collects data from its sensors and stores it in memory
- **Data Transmission** – Describes what the device sends out through the network
- **Command Response** – How the device responds to outside commands
- **Network Receival** – Used to characterize what the device receives from the network



Data Collection:
C – Collecting
S – Saving

Data Transmission:
SS – Send Saved
SC – Send Collecting

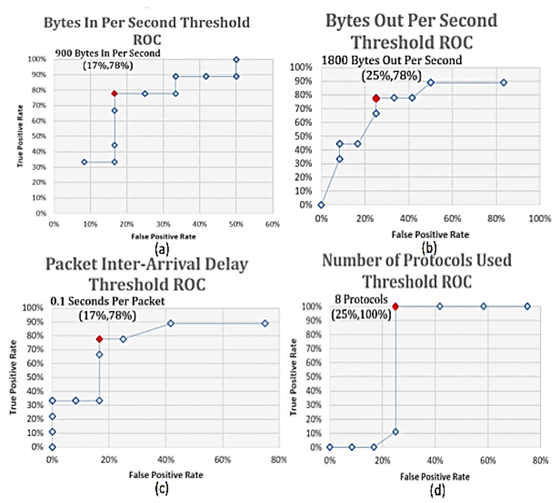
Command Response:
A – Action

Network Receival:
RC – Receive Command
RF – Receive File

c – Command; **e** – Event; **f** – File; **r** – Request; λ - End of Process

Results and Contribution

- **Collected data, and Receiver Operating Characteristic (ROC) curves** led to data thresholds for state definitions
- **An attack-independent behavior model** for characterizing normal operation of a webcam



- **Dual Usefulness:**

1. Can serve as the lone module for deriving **objective metrics for network security evaluation**

2. Can serve a part of a **behavioral Intrusion Detection System (IDS)** in order to detect intruders through anomaly analysis in deviations from regular operation