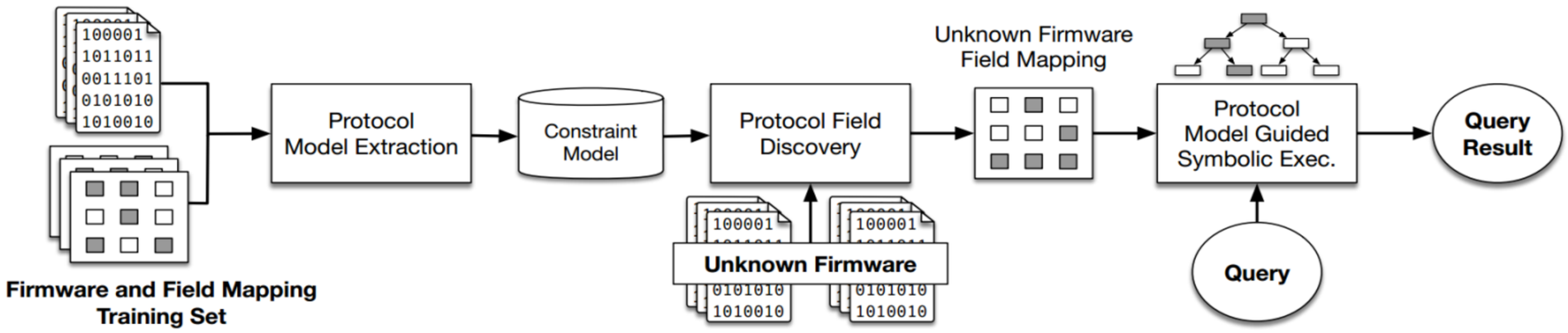
ProXray: Protocol Model Learning and Guided Firmware Analysis

PI: Kevin Butler, University of Florida, Co-PI: Tuba Yavuz, University of Florida

https://firmware-analysis.org/



Farhaan Fowze, Dave (Jing) Tian, Grant Hernandez, Kevin Butler, and Tuba Yavuz. ProXray: Protocol Model Learning and Guided Firmware Analysis. To appear in the IEEE Transactions on Software Engineering.

Problem Description

The number of Internet of Things (IoT) devices has reached 7 billion globally in 2018. Knowing whether these devices are safe and secure to use is becoming critical. IoT devices usually implement communication protocols such as USB and Bluetooth within firmware.

- Scalability issues in automated analysis of firmware.
- A lack of formal specifications of the protocols .
- Significant manual effort needed to reverse engineer the device firmware.

Scientific Impact

Automatically extracting and learning formal models of protocols can support automated reverse engineering and automated test generation.

Project Title: Domain Informed Techniques for Detecting and Defending Against Malicious Firmware

Award ID# : CNS-1815883

Approach

- Use symbolic execution to extract the protocol models and to perform guided analysis
- Constraints of the model are semantically checked against the constraints explored in the unknown firmware for reverse engineering

Broader Impact

- Improving security of peripheral devices by vetting how they utilize the underlying communication protocols that are not necessarily designed with security in mind.
- Reducing the attack surface of the IoT landscape by detecting vulnerabilities in the protocol stack implementations.
- Speedup in reaching protocol relevant targets during firmware analysis
  - up to 73.8 times speedup for USB firmware and at least an order of magnitude speedup for Bluetooth firmware
- Improved coverage of reaching protocol relevant parts of firmware during extraction
- Utilization of formal methods in embedded system security is demonstrated in PI Butler's Embedded Security course and Co-PI Yavuz's Automated HW/SW Verification course
- Public release of automatically generated protocol models