## STARSS: Domain Informed Techniques for Detecting and Defending Against Malicious Firmware (Pl: Kevin Butler)

Protocol

**Model Extraction** 

Firmware and Field Mapping

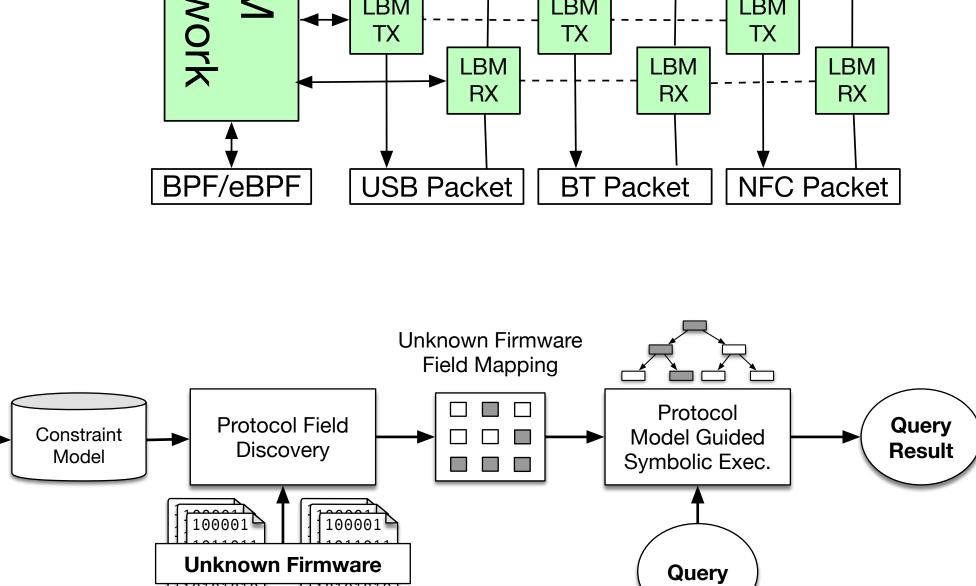
**Training Set** 



• **Hypothesis:** Understanding the communication protocols used by microcontroller firmware can ensure their safety and security and help protect computers from malicious devices.

## Major results:

- **LBM:** BPF-based protection framework for Linux defends against syntax and semantic attacks from USB, Bluetooth, NFC devices (Oakland 2019)
- ProXRay: Protocol model learning based on firmware analysis for automatic recognition of device functionality (IEEE Trans. Soft. Eng. 2020)



0101010

1010010

1010010

