Internet of Medical Things Security Research

Mike Cipolla ('20) and Justin Swirbul ('20)

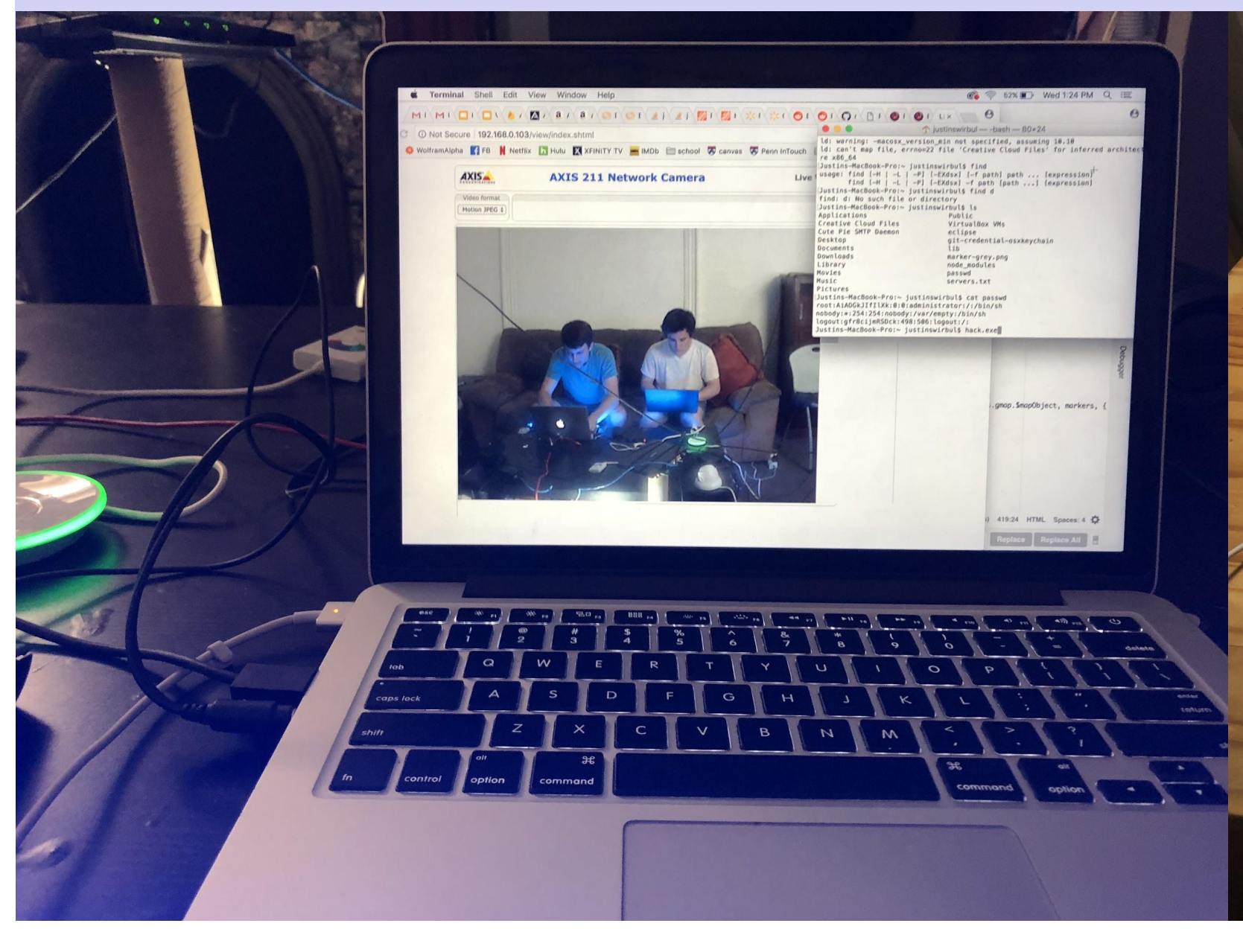
PRECISE Center, SEAS

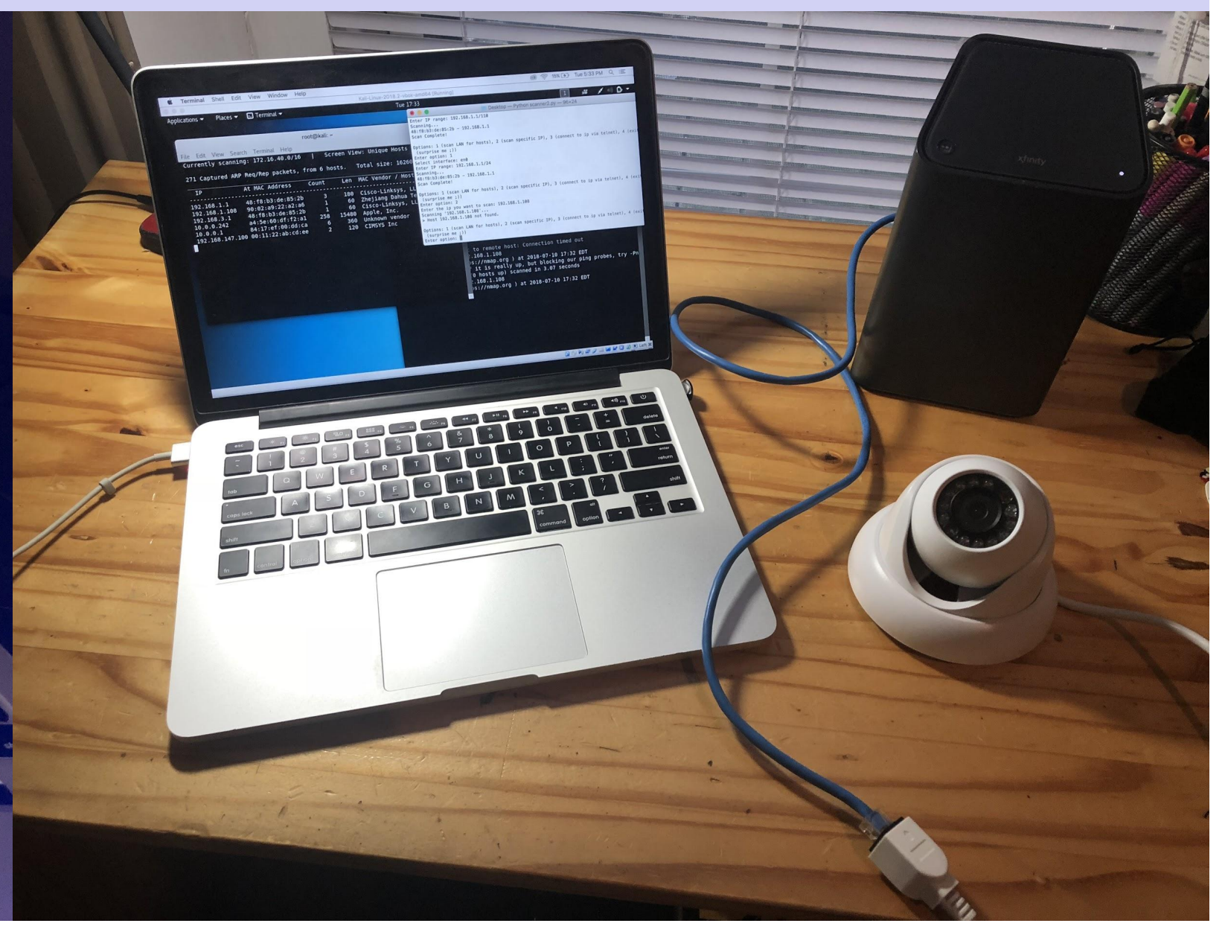
Motivation

- Healthcare has become one of the most targeted industry for cyber attacks, and important personal data and people's lives are at risk
- As IoT (Internet of Things), and specifically IoMT (Internet of Medical Things), devices become more prevalent, their security needs to be considered
  - These devices are not built with security in mind, and they are often cheaply made, resulting in many potential vulnerabilities
  - Mirai is an example of a large botnet that compromised insecure IoT devices

Clinical Need

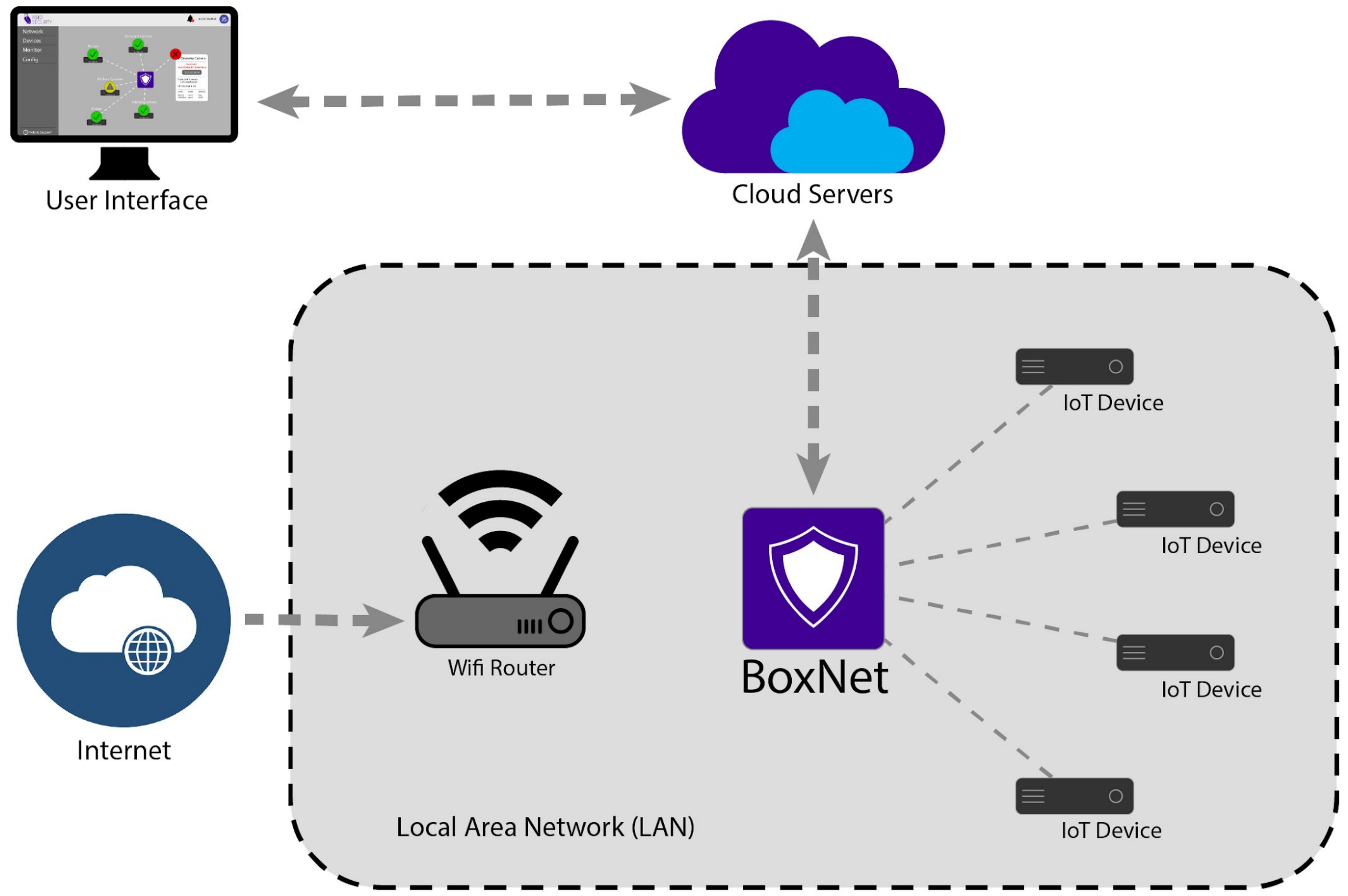
- Patient data privacy is extremely important, and laws like HIPAA set standards for the technical safeguards that covered healcare entities must put in place to secure individuals' "electronic protected health information".
- A third-party security solution allows continued use of potentially insecure devices (as similarly capable and secure alternatives often do not exist, and if they do they can be much more expensive)
- We performed security assessments of several IoMT devices (such as wireless glucometers and other PoC devices) to determine potential vulnerabilities and attack vectors

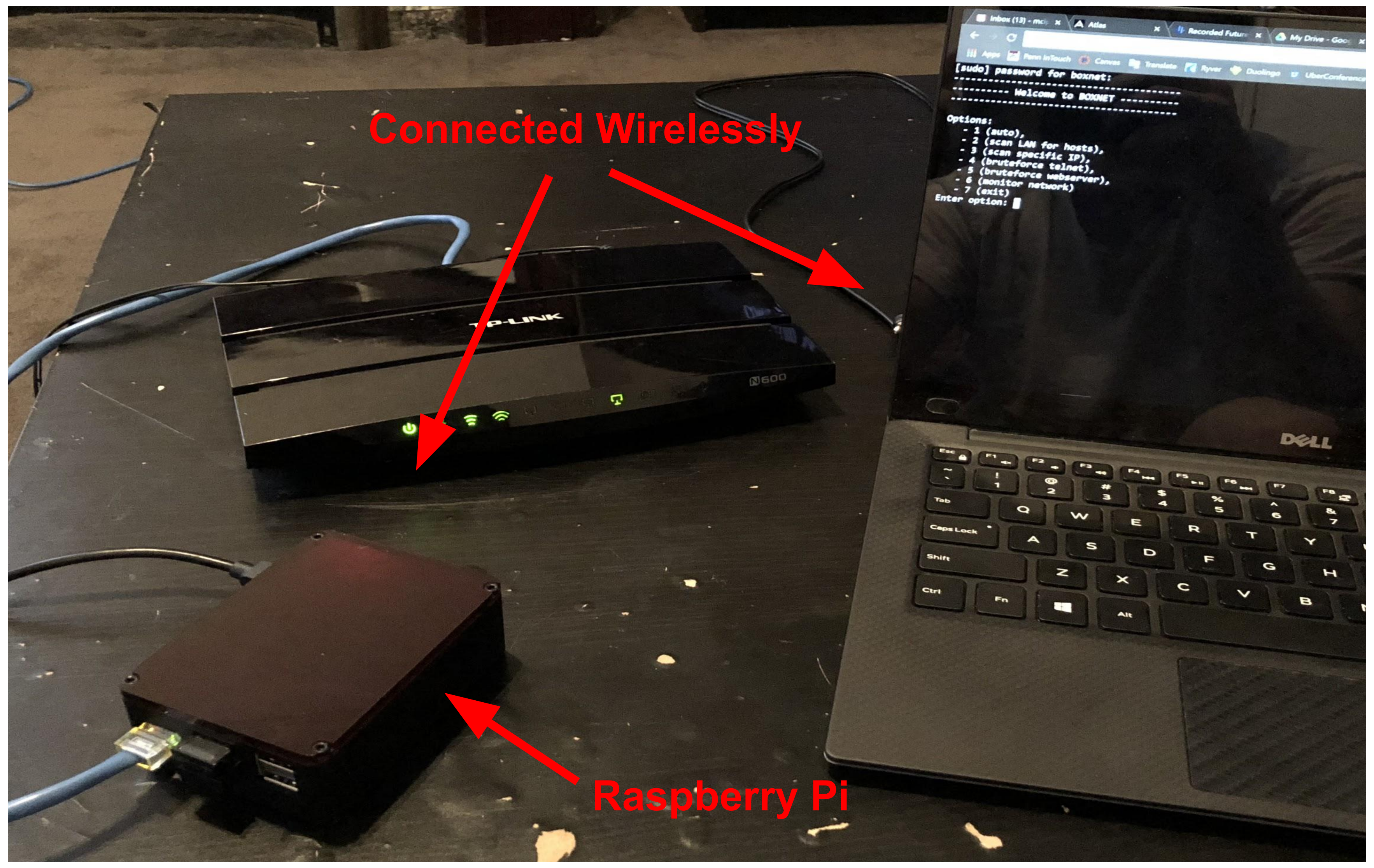




Application

BoxNet: An IoT security platform that autonomously secures vulnerable IoT devices and allows system administrators to visualize their network. It aims to lock down common vulnerabilities found in cheap IoT devices, which aren't built with security in mind.





Technical Approach

BoxNet is a small device that is plugged into a network to discover other devices on it, scan them for open ports/services, check for weak or default credentials, and then monitor the network for malicious traffic.

- Web server that allows control from any browser on the same network
- Device discovery via arp scan, then individually scan each device for open ports/services
- Check valid services (telnet, web server) with list of common default credentials, and then bruteforce weak credentials via hydra (a bruteforce login cracking tool)
- Monitor network traffic and check src/dst of packets against blacklist of malicious IPs, and log packet data in background

Future Work

- Create functionality for a payload that can be deployed on devices for further control and active monitoring
- Look into anomaly detection and other methods of analyzing network traffic and logged packets

Acknowledgment

Prof. James Weimer & Prof. Insup Lee, PRECISE Center, SEAS, Penn Medicine, PURM