The Mon(IoT)r Lab (pronounced “Monitor Lab”)

David Choffnes, Daniel J. Dubois, Jingjing Ren

THE LAB

- **The Mon(IoT)r Lab is a first-of-its-kind “living lab”** for measuring the privacy leaked by IoT devices, conducting controlled experiments, and IRB-approved user studies.
- The Lab consists of a “fishbowl” (glass walls) that encloses a space replete with smart devices from TVs to thermostats, fridges to fitbits, lights to locks.

WHAT WE DO

- We want to answer these questions:

  What personally identifiable information (PII) is being leaked from IoT devices?

  What can we do to mitigate privacy risks?

- Our methodology entails recording and analyzing network traffic generated by a variety of IoT devices that we have acquired for the Mon(IoT)r Lab.

HANDS-ON APPROACH

- We test and analyze **real IoT devices** behavior in experiments run by our team.
- We also conduct **uncontrolled experiments** where we allow consenting participants to use the Lab as a lounge to interact with its IoT devices naturally.
- Finally, we offer an **interactive component** that allows researchers and Lab visitors to visualize, understand, and control the information exposed by IoT devices in real-time.

METHODOLOGY

- **Tools.** Smart router, man-in-the-middle and TLS interception, Machine Learning, traffic fingerprinting.
- **Analysis.**
  Input: all exchanged traffic.
  Output: PII sent; type, destination, and legitimacy of exchanged traffic.
- **Control.** Obfuscate or block PII leaks and traffic that do not look legitimate (e.g., audio streams from idle IoT devices).

VISION

- **Privacy Awareness**
  The public will be aware of IoT privacy issues and will have the means to protect themselves.
- **Crowdsourced Detection**
  Share the list of leaking devices to help the community find new leaks.
- **Analyze Privacy Trends**
  Reveal IoT privacy trends by type, vendor, platform, price, etc.

Want to know more?

Visit https://moniotr.ccs.neu.edu

Northeastern University
Cybersecurity and Privacy Institute