A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic
Noah Apthorpe, Dillon Reisman, Nick Feamster
Computer Science Department & Center for Information Technology Policy, Princeton University

Abstract

- Internet-of-things (IoT) devices for “smart” homes are rapidly growing in popularity
- Many IoT devices have always-on sensors that constantly monitor users’ home environments and transmit sensor readings to the cloud
- Encrypting communications between devices and cloud servers does not preserve privacy
- A network observer can identify smart home devices and infer sensitive user behaviors from Internet traffic rates alone
- A combination of firewalling, tunneling, shaping and injecting network traffic could protect privacy if properly implemented

Threat Model

- Passive network observer
  - E.g., an Internet service provider (ISP) or Wi-Fi eavesdropper
  - Can record network traffic
  - Can obtain and analyze IoT devices for supervised inference
- Packet contents encrypted
- Metadata available
  - IP & transport layer packet headers
  - DNS queries
  - Send/receive rates

3 Step Privacy Attack

1) Separate traffic into individual device flows
2) Identify device generating each flow
3) Infer user behaviors from traffic rate changes leveraging known device function

IoT devices reveal private user behavior in network traffic rates

**Proposed Solutions**

- **Firewall devices** to prevent adversary from collecting traffic rate data
  - Difficult to determine which encrypted flows are essential for device function and which can be safely blocked
- **Generating effective firewall rules** would require manufacturer support
- **Tunnel traffic** through VPN to prevent adversary from separating flows from individual devices
  - Pushes problem to VPN exit point
  - Ineffective vs Wi-Fi eavesdropper
- **Shape traffic** to prevent accurate behavior inference
  - Less time-sensitive devices can delay cloud updates
- **Inject traffic** mimicking user behaviors to reduce adversary’s confidence in behavior inferences

**Data Collection**

- Laboratory smart home with several commercially-available IoT devices
  - Recorded network traffic using customized Raspberry Pi Wi-Fi access point

**Proposed Solutions**

- **Firewall devices** to prevent adversary from collecting traffic rate data
  - Difficult to determine which encrypted flows are essential for device function and which can be safely blocked
- **Generating effective firewall rules** would require manufacturer support
- **Tunnel traffic** through VPN to prevent adversary from separating flows from individual devices
  - Pushes problem to VPN exit point
  - Ineffective vs Wi-Fi eavesdropper
- **Shape traffic** to prevent accurate behavior inference
  - Less time-sensitive devices can delay cloud updates
- **Inject traffic** mimicking user behaviors to reduce adversary’s confidence in behavior inferences

**Acknowledgements**

This research was funded by the Department of Defense through the National Defense Science & Engineering Graduate Fellowship (NDSEG) Program, a Google Faculty Research Award, and the National Science Foundation.