Poster: A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic

Noah Apthorpe, Dillon Reisman, Nick Feamster
Computer Science Department, Princeton University
apthorpe@cs.princeton.edu, dreisman@princeton.edu, feamster@cs.princeton.edu

***Abstract*—The increasing popularity of specialized Internet-connected devices and appliances, dubbed the Internet-of-Things (IoT), promises both new conveniences and new privacy concerns. Unlike traditional web browsers, many IoT devices have always-on sensors that constantly monitor fine-grained details of users' physical environments and influence the devices' network communications. Passive network observers, such as Internet service providers, could potentially analyze IoT network traffic to infer sensitive details about users. Here, we examine several commercially-available IoT smart home devices and find that their network traffic rates reveal potentially sensitive user interactions even when the traffic is encrypted. These results suggest technical approaches for protecting IoT device owner privacy and indicate that IoT-specific concerns must be considered in the ongoing policy debate around ISP data collection and usage.**

I. Introduction

Concerns over the abilities of network observers have led regulators to institute new rules on ISP data collection and usage [1]. Some opponents argue that stronger regulation is unnecessary, because the increasing pervasiveness of encryption prevents ISPs from observing sensitive data in traffic content [2]. Privacy advocates, however, argue that metadata and traffic patterns can reveal sensitive information even when traffic content is unavailable [3]. Research detailing privacy vulnerabilities of encrypted traffic and metadata from IoT devices can help inform future regulation as IoT devices become more prevalent.

For this work, we set up a smart home laboratory with the following commercially-available IoT devices: a Sense sleep monitor, a Nest Cam Indoor security camera, an Amcrest Wi-Fi Video Security Camera, a Belkin WeMo switch, a TP-Link Smart Plug, an Orvibo Wi-Fi Smart Outlet, and an Amazon Echo. Analyzing network traffic from these devices suggests a three step privacy attack that would allow a passive network observer to identify IoT devices inside a smart home and infer user behavior from device traffic rates *even when the traffic is encrypted*. We implemented this attack and demonstrated its effectiveness against all tested IoT devices.

We are currently working to develop solutions to protect users from IoT device traffic rate privacy vulnerabilities. While additional research is needed, the case studies we have performed motivate several possible components of a general solution, including firewalling devices, tunneling traffic, shaping traffic, and injecting traffic.

NDSS '16, 21-24 February 2016, San Diego, CA, USA

http://dx.doi.org/10.14722/ndss.2016.23xxx

II. Threat Model

We assume a passive network observer threat model with capabilities similar to an ISP. Specifically, an adversary in this model can observe and record network traffic from the last-mile connection to a smart home. The traffic is assumed to be encrypted, so the adversary cannot read its contents. Only packet header information and traffic rate metadata is available. The adversary can also obtain and analyze their own IoT devices to generate training data for supervised inference.

Additional threat models, such as a passive Wi-Fi eavesdropper are also relevant to the smart home context. An eavesdropper on a WPA2-secured Wi-Fi network would have access to different information than an ISP (device MAC addresses and radio information but no IP or transport layer headers). However, the three step privacy attack we describe is still effective.

III. Three Step Privacy Attack

A passive network observer can identify smart home IoT devices and infer user behavior with the following three step privacy attack.

A. Separate traffic into individual device flows

An adversary first divides recorded network traffic into flows corresponding to individual devices. Even when the home gateway router acts as a NAT, it is still possible to separate network traffic into individual device flows using the IP addresses of the cloud servers communicating with the devices. In cases where multiple devices send to the same server IP, the TCP port number rewritten by the NAT allows for flow separation. While the devices we studied often communicate with multiple server IPs, we discovered that an adversary typically only needs to identify a single flow that encodes the device state.

B. Identify device generating each flow

The adversary next identifies what IoT device is most likely responsible for each flow. Knowing what devices a user owns can itself be a serious privacy violation. For example, a user might not want an ISP knowing they own an IoT blood sugar monitor or pacemaker.

DNS queries associated with each flow often contain the device manufacturer name or other identifier, allowing easy device identification. Among the devices we tested, the Nest Cam queried domains from dropcam.com (the predecessor to the Nest Cam), while the Sense sleep monitor queried domains from hello.is (the company that makes the Sense).

An adversary without access to or without informative DNS queries can identify devices with traffic rate information alone. We show that simple supervised machine learning (k-nearest neighbors) on features extracted from traffic rates is sufficient to identify all tested IoT devices.

C. *Infer user behaviors from traffic rate changes*

Once an adversary identifies traffic flows for a particular device, one or more of the flows are likely to encode device state. Simply plotting send/receive rates of the flows (bytes per second) revealed correlations to potentially private user interactions for each device we tested (Figure 1). For example, traffic from the Sense sleep monitor revealed a user's sleeping patterns. Traffic from the Nest Cam revealed when a user is actively monitoring the camera feed or when the camera detects motion in its field of view. Traffic from the WeMo switch revealed when a physical appliance in a smart home is turned on or off.

Even without learning such specific correlations prior to traffic analysis, an adversary can still infer user behaviors from traffic variations if they have identified the device and know its limited purpose. For example, the Sense sleep monitor is both easily identified from DNS queries and has a limited purpose. A traffic spike from the monitor in the late evening, for instance, likely corresponds to when a user goes to sleep.

IV. Proposed Solutions

Our results suggest the following approaches to protect smart home IoT devices from traffic rate privacy threats:

Firewalling smart home IoT devices could prevent an adversary from collecting traffic rate data. However, it is difficult to determine which encrypted flows are essential for device function and which can be safely blocked. Generating effective firewall rules or allowing selective blocking of encrypted traffic would require manufacturer support.

Tunneling IoT device traffic through a VPN could prevent an adversary from separating traffic flows from individual devices, provided they do not have access to traffic from the VPN exit point.

Shaping IoT device traffic could prevent accurate behavior inference. For example, devices without time-sensitive dependencies on cloud services could delay network communications, removing direct correlations between traffic rates and user behaviors.

Injecting IoT device traffic that mimics user behaviors could reduce an adversary's confidence in behavior inferences. This would require a model of typical interaction patterns but could be implemented on a third-party hub in addition to on the protected devices themselves.

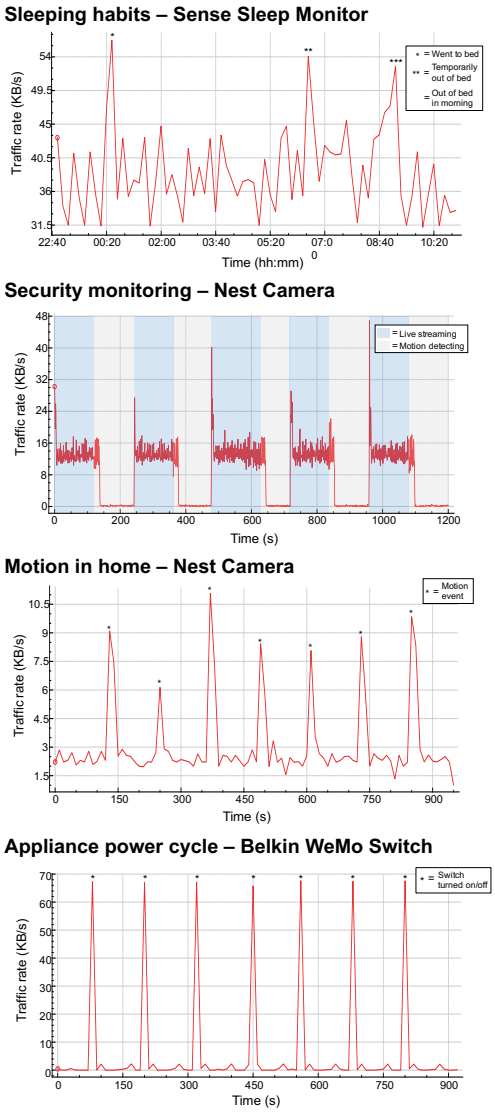

Fig. 1. Network traffic rates of selected flows from commercially-available IoT devices reveal user behaviors.

V. Citation

This poster abstract was drawn from the following workshop publication and additional unpublished results:

N. Apthorpe, D. Reisman, and N. Feamster. "A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic." *Workshop on Data and Algorithmic Transparency*. 2016. http://datworkshop.org/papers/dat16-final37.pdf

References

[1] Federal Communications Commission, "FCC adopts broadband consumer privacy rules," https://www.fcc.gov/document/fcc-adopts-broadband-consumer-privacy-rules, 2016.

[2] P. Swire, J. Hemmings, and A. Kirkland, "Online privacy and ISPs," The Institute for Information Security & Privacy. http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf, 2016.

[3] E. Falcon, T. Lee, and J. Gillula, "Comments of the electronic frontier foundation before the federal communications commission (docket no. 16-106)," Electronic Frontier Foundation. https://www.eff.org/files/2016/05/27/efffcc-privacy-comments.pdf, 2016.