FIAT: Frictionless Authentication of IoT Traffic

Yunming Xiao[1*], Matteo Varvello[2]
[1]Northwestern University, [2]Nokia Bell Labs

Introduction

The average US household currently hosts more than 10 Internet of Things (IoT) devices. Many research papers[1, 2] have demonstrated critical security concerns of the IoT, often due to lack of best practices like partial usage of HTTPS, or old ciphers. Even when best security practices are implemented, the IoT is still vulnerable to many attacks. Intruders can penetrate the home WiFi and directly control some IoT devices. They can compromise the account associated with an IoT device, mostly relying on username and password, or of third-party services like IFTTT. They can also compromise the devices where IoT apps run, i.e., mostly mobile phones.

The goal of this work is to build a frictionless authentication mechanism for legacy IoT devices. Our rationale is that IoT traffic is highly predictable, due to being mostly driven by software, e.g., to report at constant rate temperature readings from a smart thermostat, and less frequently triggered by routines set by the user, e.g., "turn on the heat each night at 6pm", or by a user via manual input, e.g., increase the thermostat temperature from its companion app. **Predictable traffic** can be learned and automatically authorized. **Unpredictable traffic**, when legitimate, is associated with some physical interaction between the user and a controlling device. We thus plan to automatically validate unpredictable traffic leveraging sensor data from the device used to control an IoT device, e.g., accelerometer and gyroscope on a mobile phone.

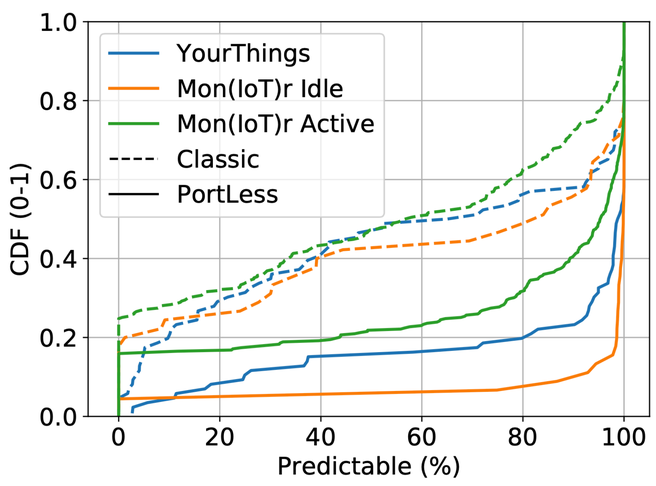

Figure 1. CDFs of the percentage of predictable traffic. Classic: < ip_src, ip_dst, port_src, port_dst, proto, size >; PortLess: < ip_src, ip_dst, proto, size >.

Is IoT Traffic Predictable?

Method. For each packet, we record arrival timestamp, size, source and destination IPs, transport protocol (TCP/UDP), and source and destination ports. We then store each packet in a bucket identified by the tuple above minus the arrival timestamp. We then compute the inter-arrival times between packets from the same bucket considering the last two received packets. If the computed inter-arrival time matches any previously computed inter-arrival times for this bucket, then all packets associated with this inter-arrival time (previous or future) are considered predictable.

Results. For YourThings[1] dataset, **Figure 1** shows that 80% of traffic for 80% of devices is predictable, assuming the PortLess definition of a flow. For Mon(IoT)r[3] dataset, the predictability of idle traffic is high, e.g., up to 90% of the traffic for 90% of the devices considering PortLess flows. In contrast, when there are active actions invoked, the IoT traffic predictability is reduced.

FIAT DESIGN

Client-Side App. FIAT's app keeps track of IoT apps running on a device. Each time one of these apps is used to trigger an action (e.g., turn on a light), it collects device's sensor data. The sensor data, e.g., gyroscope and accelerometer, along with OS information on which app is in the foreground, is encrypted and sent to the IoT proxy. This key is agreed offline between FIAT's app and IoT proxy at pairing. The human verification data is sent to the IoT proxy via a fast channel so that it can be informed of the human activity before that the corresponding manual traffic (triggered by a user interacting with the IoT app) is intercepted.

Server-side Proxy. The first task of FIAT's IoT proxy is to intercept IoT traffic via ARP spoofing and perform a predictability analysis. This analysis allows to identify and permit predictable IoT traffic (both control and automated). Note that the predictability analysis is learned for every device and there is no cross-device knowledge transfer. When unpredictable traffic is detected, it is labeled as suspicious and requires further validation.

The second task of FIAT's IoT proxy is to communicate with FIAT's app to verify human activity associated with manual traffic. Previous study zkSENSE[4] has shown the validity of machine learning technique to humanness verification. We assume IoT proxy and app are paired, e.g., by scanning a QR code at setup.

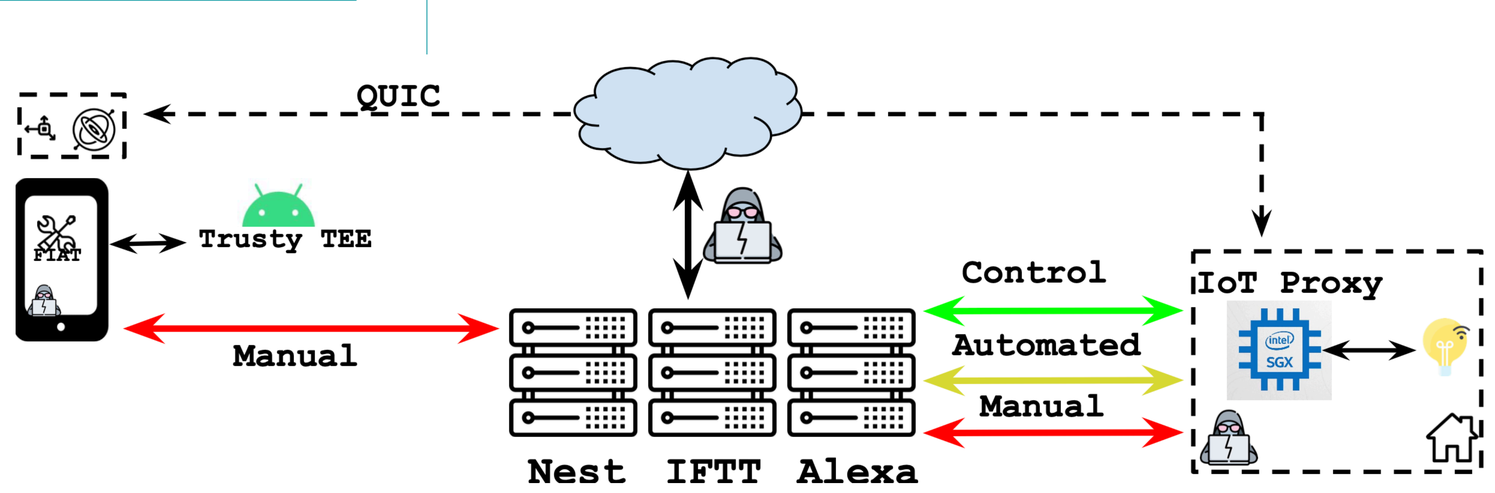

Figure 2. Graphical view of FIAT's architecture

Threat Model. We assume a computationally bounded attacker who can compromise any IoT account of the user. We assume an attacker who can control the home network, e.g., by breaking WiFi security, and can inject, drop, and modify (unencrypted) packets, but cannot break cryptographic primitives[5]. We also assume the attacker can compromise any of the devices associated with FIAT. However, we assume the attacker has no access to the device's OS level. Further, the attacker cannot hack into Trusted Execution Environments (TEEs).

Future Work

We plan to build a testbed including various IoT devices and collect data when performing controlled operations. This data will allow further analysis on the predictability of IoT traffic, especially focusing on the how to effectively distinguish between automated and manual traffic. Next, we will build a prototype of FIAT to verify its functionality and performance.

Note

*This work was done during the internship at Nokia Bell Labs

Contact

Emails:
yunming.xiao@u.northwestern.edu,
matteo.varvello@nokia.com,
Website:
https://yunmingxiao.github.io/projectsfolder/fiat/

References

1. Alrawi, Omar, et al. "Sok: Security evaluation of home-based iot deployments." 2019 IEEE symposium on security and privacy (sp). IEEE, 2019.
2. Fernandes, Earlence, et al. "Decoupled-ifttt: Constraining privilege in trigger-action platforms for the internet of things." arXiv preprint arXiv:1707.00405 (2017).
3. Ren, Jingjing, et al. "Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach." Proceedings of the Internet Measurement Conference. 2019.
4. Querejeta-Azurmendi, Iñigo, et al. "ZKSENSE: A Friction-less Privacy-Preserving Human Attestation Mechanism for Mobile Devices." Proceedings on Privacy Enhancing Technologies 2021.4 (2021): 6-29.
5. Dolev, Danny, and Andrew Yao. "On the security of public key protocols." IEEE Transactions on information theory 29.2 (1983): 198-208.