Poster: FIAT: Frictionless Authentication of IoT Traffic

Yunming Xiao*
Northwestern University
yunming.xiao@u.northwestern.edu

Matteo Varvello
Nokia Bell Labs
matteo.varvello@nokia.com

ACM Reference format:
Yunming Xiao and Matteo Varvello. 2021. Poster: FIAT: Frictionless Authentication of IoT Traffic. In *Proceedings of CoNEXT '21, Virtual Event, Germany, December 7–10, 2021,* 2 pages.
DOI: TBA

1 INTRODUCTION

The average US household currently hosts more than 10 Internet of Things (IoT) devices [2]. Many research papers [5, 8] have demonstrated critical security concerns of the IoT, often due to lack of best practices like partial usage of HTTP, 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 [4]. They can also compromise the devices where IoT apps run, *i.e.,* mostly mobile phones [1].

The above security concerns could be mitigated via *two-factor authentication* (2FA), as commonly done for online banking. With 2FA, the user is often required to validate her identity via, for instance, an SMS received on a mobile phone. Unfortunately, requiring a user to constantly validate her interactions with IoT devices is cumbersome, and unlikely to be accepted by users – which is why it is not used.

The goal of this work is to build a *frictionless* IoT authentication mechanism. Our rationale is that IoT traffic is highly *predictable*, due to being mostly caused 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.

Our first contribution is a quantification of the predictability of IoT traffic by analyzing public datasets. The analysis of public datasets shows that 80-90% of the IoT traffic (from hundred of devices) is indeed predictable. The second contribution of this work is the design of *FIAT*, a frictionless authentication mechanism for IoT traffic. FIAT is designed to improve the security of legacy IoT devices with minimal user input for authentication.

*This work was completed during the internship at Nokia Bell Labs.

CoNEXT '21, Virtual Event, Germany

DOI: TBA

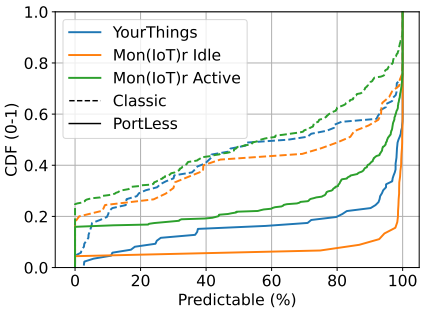

Figure 1: CDFs of the percentage of predictable traffic.

2 IS IOT TRAFFIC PREDICTABLE?

Previous studies [6, 9] have shown that IoT traffic has unique patterns which allow accurate passive IoT device identification. However, to the best of our knowledge, no previous study has yet quantified how *predictable* this traffic is, *i.e.,* how often such unique patterns repeat over time.

To answer this question, we explore two large and publicly available datasets: YourThings [5] and Mon(IoT)r [11]. YourThings dataset includes the network traffic collected from 65 IoT devices in the time span of 10 days. Mon(IoT)r dataset separates the idle and active (when manual action is executed) traffic from 104 IoT devices and 16 *controller* devices.

To investigate the *predictability* of IoT traffic, we proceed as follows. First, we record the timestamps of packets sent/received by the IoT device. Given that some IoT devices may communicate with the same destination regularly but with different port numbers as time goes by, we adopt a "PortLess" 3-tuple definition of TCP/UDP flows, compared to "Classic" 5-tuple. Next, we compute the time *interval* between packets for each flow. If all intervals identified for a flow appear repeatably, we consider the flow as *predictable*.

Figure 1 shows CDFs of the percentage of predictable traffic across devices. For YourThings dataset, Figure 1 shows that more than 80% of the traffic for 80% of the devices is predictable, assuming the PortLess definition of a flow. For Mon(IoT)r 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.

3 FIAT DESIGN

This Section describes the design of FIAT, a frictionless authentication mechanism for IoT traffic. FIAT aims at improving the security of IoT devices without disrupting their functioning, *i.e.,* with no impact on their current traffic or requiring annoying user action validation. FIAT automatically learns *control* and *automated* traffic, thanks to its demonstrated predictability, and leverages humanness verification to handle the unpredictable *manual* traffic. In the following, we first describe our threat model, and then proceed with the description of FIAT and its components.

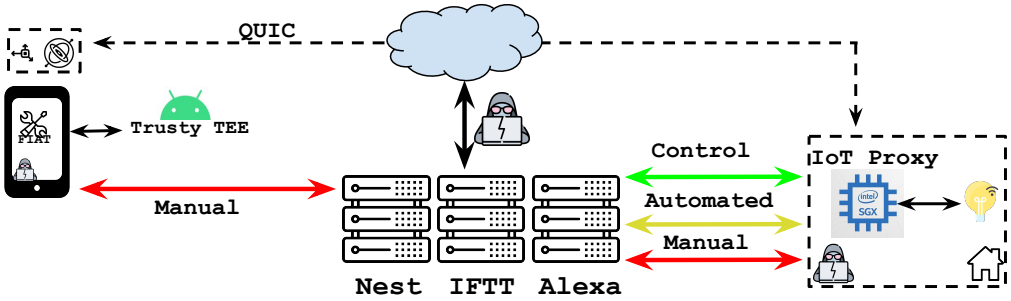

Figure 2: Graphical view of FIAT's architecture.

Figure 2 visualizes the main components of FIAT. On the left end-side, the figure shows an Android device running FIAT's client-side component, a user-space application that leverages the device's Trusted Execution Environments (TEEs) as a hardware-backed secure keystore [3]. In the following, we simply refer to it as FIAT's app. The center of the figure shows the IoT traffic, distinguishing between control, automated, and manual. The figure further shows some *new* traffic (carried over QUIC) originated by FIAT's app; this traffic carries a proof of human interaction linked with an IoT app. The right end-side of the figure shows instead a typical home network, with a smart bulb and FIAT's server-side component. This is a *secure* IoT proxy, e.g., implemented over SGX, which intercepts all IoT traffic and also receives the traffic carrying the human input validation. The figure further shows potential attackers as per our threat model: *remote* attackers who have access to the user's IoT account and/or the user-space of the device, and *local* attackers who have penetrated the home WiFi.

Threat Model – We assume a computationally bounded attacker who can compromise any IoT account of the user.We further assume an attacker who can control the home network, e.g., by breaking WiFi security, and can inject, drop, reroute, and modify (unencrypted) packets, but cannot break cryptographic primitives [7]. 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.Finally, we assume attackers cannot hack into Trusted Execution Environments (TEEs).

Client-Side App – FIAT's app monitors human interaction with any IoT app, and *quickly* and *securely* inform the IoT proxy of this interaction. This allows the IoT proxy to verify the validity of *manual* IoT traffic, e.g., that the traffic requesting to turn on a smart light is associated with the user physically interacting with the mobile app of the smart light.

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 with a key obtained by the TEE's keystore 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. To achieve fast channel between the FIAT's app and proxy, QUIC is the perfect tool with 0-RTT or 1-RTT connection establishment.

Server-Side IoT Proxy – The first task of FIAT's IoT proxy is to intercept IoT traffic via ARP spoofing and perform a similar analysis to the one presented in Section 2. 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 [10] has shown the validity of machine learning technique to humanness verification, where the inputs are 48 features extracted from the gyroscope and accelerometer and a 9-layer decision tree has the best performance. In addition, we assume that IoT proxy and FIAT's app are paired *locally*, by scanning a QR code on the proxy at setup.

4 FUTURE WORK

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

REFERENCES

[1] Automation script, 2019. https://github.com/NEU-SNS/intl-iot/blob/master/moniotr/auto_experiments/auto_app.sh.
[2] Average number of connected devices residents have access to in U.S. households in 2020, by device, 2020. https://www.statista.com/statistics/1107206/average-number-of-connected-devices-us-house.
[3] Data Encryption on Android with Jetpack Security, 2021. https://android-developers.googleblog.com/2020/02/data-encryption-on-android-with-jetpack.html.
[4] IFTTT helps every thing work better together, 2021. https://ifttt.com/.
[5] Alrawi, O., Lever, C., Antonakakis, M., and Monrose, F. Sok: Security evaluation of home-based iot deployments. In *2019 IEEE symposium on security and privacy (sp)* (2019), IEEE, pp. 1362–1380.
[6] Apthorpe, N., Reisman, D., and Feamster, N. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *arXiv preprint arXiv:1705.06805* (2017).
[7] Dolev, D., and Yao, A. On the security of public key protocols. *IEEE Transactions on information theory 29*, 2 (1983), 198–208.
[8] Fernandes, E., Rahmati, A., Jung, J., and Prakash, A. Decoupled-ifttt: Constraining privilege in trigger-action platforms for the internet of things. *arXiv preprint arXiv:1707.00405* (2017).
[9] Meidan, Y., Bohadana, M., Shabtai, A., Guarnizo, J. D., Ochoa, M., Tippenhauer, N. O., and Elovici, Y. Profiliot: a machine learning approach for iot device identification based on network traffic analysis. In *Proceedings of the symposium on applied computing* (2017), pp. 506–509.
[10] Querejeta-Azurmendi, I., Papadopoulos, P., Varvello, M., Nappa, A., Zhang, J., and Livshits, B. zksense: A friction-less privacy-preserving humanattestation mechanism for mobile devices. *Proc. of the Privacy Enhancing Technologies Symposium* (2021).
[11] Ren, J., Dubois, D. J., Choffnes, D., Mandalari, A. M., Kolcun, R., and Haddadi, H. Information Exposure for Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach. In *Proc. of the Internet Measurement Conference (IMC)* (2019).