Poster: Defining Actionable Rules for Verifying IoT Security

Kayla E Ibrahim*, Suryadipta Majumdar*, Daniel Bastos† and Anoop Singhal‡
*Information Security and Digital Forensics, University at Albany - SUNY, USA, Email: {keibrahim,smajumdar}@albany.edu
†British Telecom Research Lab, UK, Email: daniel.bastos@bt.com
‡Computer Security Division, National Institute of Standards and Technology, USA, Email: anoop.singhal@nist.gov

***Abstract*—The Internet of Things (IoT) is being widely adopted in recent years. Security, however, has lagged behind, as evidenced by the increasing number of attacks that use IoT devices (e.g., an arson that uses a smart oven, burglary via a smart lock). Therefore, the transparency and accountability of those devices very often become questionable. To that end, formally verifying the system state of those devices against desirable security rules might be a promising solution. However, there is a significant gap between the high-level IoT security recommendations (e.g., NISTIR 8228, NISTIR 8259, OWASP IoT Security Guidance, ENISA Good Practices for Security of IoT, and UK Code of Practice for Consumer IoT Security), and the low-level IoT system data (e.g., sensor data, logs, configurations). This poster aims to bridge this gap by designing an automated technique to define actionable security rules based on those recommendations and enable the security verification of IoT systems.**

***Index Terms*—IoT, security rules, verification**

I. Introduction

The wide-spread adoption of IoT devices is evident in recent years (with the projections of 75.44 billion devices worldwide by 2025 [11]). Most of those devices, however, are reported to suffer from various security threats due to their implementation flaws and misconfigurations [1], [9], [14]; which often question the accountability and transparency of those devices [1], [7]. To address this concern, verifying the system states of IoT devices against a set of security rules might be a promising solution.

However, the existing security standards, e.g., National Institute of Standards and Technology Internal Reports (NISTIR 8228 [7] and NISTIR 8259 [8]), Open Web Application Security Project (OWASP) IoT Security Guidance [10], UK Code of Practice for Consumer IoT Security [6], and European Union Agency for Cybersecurity (ENISA) Good Practices for Security of IoT [5] are intended more for high-level guidelines than for verifying IoT security. For instance, the recommendation *"ensure proper authentication mechanisms"* from OWASP [10] needs to be instantiated to actionable rules, such as *"no smart door opening without PIN"*.

The existing security solutions (e.g., [2]–[4], [14]) in IoT provide an ad-hoc list of rules for various security solutions, such as, application monitoring, intrusion detection, and access control. However, none of these works develops a generic approach to automatically define actionable rules for verifying IoT device security.

This work targets to overcome this limitation of the existing works, and designs a framework to automatically define actionable security rules for IoT. To this end, we first investigate the existing IoT security standards and identify their limitations in verifying IoT security. Then, we present the design and high-level steps of our proposed framework. Finally, we conclude the current status of this work in progress.

II. Challenges in Defining Actionable Security Rules

We investigate several IoT security standards (e.g., NISTIR 8259 [8], OWASP IoT Security Guidance [10], UK code of practice [6], and ENISA good practices [5]), and identify the following challenges in defining security rules from those standards, as they are not specifically designed for this purpose.

- The recommendations in those standards are too high-level and do not include any system specific information; therefore, for deriving actionable security rules, it is essential to obtain the in-depth system knowledge, and and interpret those recommendations in the context of that system knowledge.
- To verify those recommendations using formal tools requires significant effort including interpreting high-level recommendations to low-level security rules, and preparing these rules (e.g., identifying their data sources, and converting them into formal languages) for security verification.

This work aims to bridge this gap and outline the actionable security rules for verification.

III. Threat Model

We assume that IoT devices may have implementation flaws, misconfigurations, and vulnerabilities that could potentially be exploited by malicious entities to violate security rules. To conduct the verification process, our work relies on a remote server or a local hub/gateway. The communication between the devices and our verification server is secure, using their supported end-to-end encryption mechanisms, e.g., Transport Layer Security (TLS). The privacy threats involved with the data sharing of IoT devices are beyond the scope of this research and will be handled in future research through a privacy-friendly verification technique.

IV. Approach Overview

Fig. 1 shows the high-level design of our proposed solution.

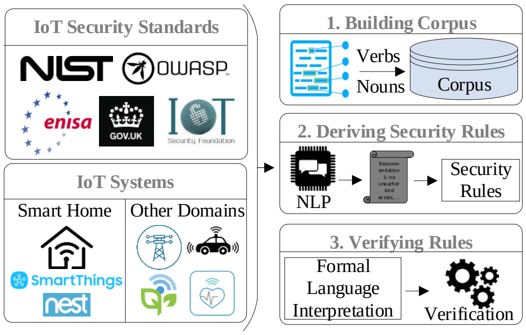

Fig. 1. An overview of our proposed approach

Step 1: Building a Corpus from Security Standards. To build a corpus from the existing IoT security standards, we first parse the contents (i.e., the sections that cover the security guidelines) of those document files. Second, we build a corpus with the relevant terms (i.e., which mainly include the nouns and verbs as those two parts of speech mainly indicate the main message of a recommendation).

Step 2: Deriving Actionable Security Rules. To derive actionable rules, we first extract the key recommendations of those standards by applying several text analytics techniques, such as, term frequency-inverse document frequency (TF-IDF), and natural language processing (NLP) techniques, such as, sentiment analysis [12]. Second, we interpret those key recommendations, apply them in the context of IoT devices, and define actionable security rules for specific cases.

Step 3: Verifying Security Rules. To verify these security rules for actual IoT devices, we translate the actionable security rules into a formal language (e.g., constraint satisfaction problem), collect supporting data for each rule from our smart home testbed, and verify those rules. For verification, we leverage formal verification techniques, e.g., Boolean satisfiability problem (SAT) [13], as it is well-known for its expressiveness, provable security and rigorous results.

V. Preliminary Results

The proposed approach is implemented in a smart home testbed and evaluated for two sample security rules. Fig. 2 shows the total time required for separately verifying the *no unauthorized door opening* and *no image capturing in toilet* security rules. We can easily observe that the execution time is not a linear function of the number of smart homes to be verified. Additionally, our results (not reported here due to space constraint) show that verifying more security rules would not lead to a significant increase in the execution time.

VI. Challenges and Next Steps

While the results of our preliminary experiments indicate the potentiality of leveraging formal tools in IoT security verification, different challenges need to be considered in the next steps of the project. Firstly, the current verification is performed in a remote server, which relies on data sharing and ignores its privacy concerns. Secondly, the Step 2 in Section IV is currently performed manually. Thirdly, there might be domain-specific challenges while adapting our approach in other IoT domains. In the next step, we will explore the feasibility of conducting (fully or partially) the local verification in a hub or gateway; which may require simplifying the workload by developing an incremental approach. Also, we will investigate existing NLP techniques and build an automated technique for Step 2. Finally, we will explore the challenges in applying our approach in other IoT domains.

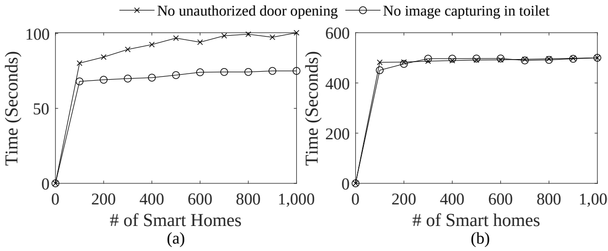

Fig. 2. Total time required to verify two sample security rules, by varying the number of smart appliances to (a) five and (b) 15 in each home.

Disclaimer. This paper is not subject to copyright in the United States. Commercial products are identified in order to adequately specify certain procedures. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the identified products are necessarily the best available for the purpose.

References

[1] Omar Alrawi, Chaz Lever, Manos Antonakakis, and Fabian Monrose. SoK: Security evaluation of home-based IoT deployments. In *IEEE S&P*, 2019.

[2] Simon Birnbach, Simon Eberz, and Ivan Martinovic. Peeves: Physical event verification in smart homes. In *ACM CCS*, 2019.

[3] Z Berkay Celik, Patrick McDaniel, Gang Tan, Leonardo Babun, and A Selcuk Uluagac. Verifying internet of things safety and security in physical spaces. *IEEE Security & Privacy*, 17(5):30–37, 2019.

[4] Z Berkay Celik, Gang Tan, and Patrick D McDaniel. IoTGuard: Dynamic enforcement of security and safety policy in commodity IoT. In *NDSS*, 2019.

[5] ENISA. Good Practices for Security of IoT - Secure Software Development Lifecycle, 2019. Available at: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1.

[6] The UK Government. Code of Practice for consumer IoT security, 2019. Available at: https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security.

[7] NIST. Considerations for managing internet of things (IoT) cybersecurity and privacy risks, 2019. Available at: https://csrc.nist.gov/publications/detail/nistir/8228/final.

[8] NIST. Recommendations for IoT device manufacturers: Foundational activities and core device cybersecurity capability baseline, 2020. Available at: https://csrc.nist.gov/publications/detail/nistir/8259/draft.

[9] Sukhvir Notra, Muhammad Siddiqi, Hassan Habibi Gharakheili, Vijay Sivaraman, and Roksana Boreli. An experimental study of security and privacy risks with emerging household appliances. In *IEEE CNS*, 2014.

[10] Open Web Application Security Project (OWASP). IoT security guidance, 2019. Available at: https://www.owasp.org/index.php/IoT_Security_Guidance.

[11] Statista. Smart home- United States, Statista market forecast, 2019.

[12] Maite Taboada, Julian Brooke, Milan Tofiloski, Kimberly Voll, and Manfred Stede. Lexicon-based methods for sentiment analysis. *Computational linguistics*, 37(2), 2011.

[13] Naoyuki Tamura and Mutsunori Banbara. Sugar: A CSP to SAT translator based on order encoding. In *Proceedings of the Second International CSP Solver Competition*, 2008.

[14] Qi Wang, Wajih Ul Hassan, Adam Bates, and Carl Gunter. Fear and logging in the internet of things. In *NDSS*, 2018.