COPSEC: Compliance-Oriented IoT Security and Privacy Evaluation Framework

Gianluca Anselmi*, Anna Maria Mandalari*, Sara Lazzaro§, Vincenzo De Angelis§
University College London*   Mediterranea University of Reggio Calabria§
{gianluca.anselmi.22, a.mandalari}@ucl.ac.uk, {sara.lazzaro, vincenzo.deangelis}@unirc.it

ABSTRACT

A rising number of Internet of Things (IoT) security and privacy threats have been documented over the last few years. However, IoT devices' domain designs are out-of-date and do not take into consideration the changing dangers associated with them. In this paper, we present COPSEC, a novel framework for evaluating whether IoT devices are compliant with security guidelines and privacy regulations. We extract metrics from existing guidelines and regulations and test them on a set of devices by performing hundreds of automated experiments. Our results indicate not only that these devices are not compliant with basic security guidelines, but also that their data collection operations may introduce privacy risks for the users that adopt them.

ACM Reference Format:
Gianluca Anselmi*, Anna Maria Mandalari*, Sara Lazzaro§, Vincenzo De Angelis§. 2023. COPSEC: Compliance-Oriented IoT Security and Privacy Evaluation Framework. In *The 29th Annual International Conference on Mobile Computing and Networking (ACM MobiCom '23), October 2–6, 2023, Madrid, Spain.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3570361.3615747

1 INTRODUCTION

The number of Internet of Things (IoT) devices has increased significantly in the last few years. They can be used in different contexts, from a common user who owns a consumer device, to far more complex environments such as hospitals. Differently from a computer or a mobile phone, these devices are constantly on and connected to their network, making them vulnerable to both security and privacy risks.

Security guidelines, such as ENISA and NIST [1, 2], have been released for improving IoT design practice, but, at the moment, they are not mandatory and it is not clear whether IoT devices are compliant with them. Furthermore, privacy regulations exist, such as GDPR [3] in the EU or CCPA [4] in California. However, there is a lack of understanding of how and whether IoT devices comply with these regulations.

We propose COPSEC, a framework for auditing the compliance of IoT devices with security guidelines and privacy regulations. Its aim is to automatically probe IoT devices and produce a certification. By extracting information from the privacy policies and comparing them with the behavior of the devices, and by defining metrics to test security guidelines, we perform an initial investigation of this compliance.

We address the following research questions (RQ):

RQ1. Is it possible to create a framework for benchmarking security and privacy on IoT devices? At the moment, there is no framework to check whether IoT devices are adhering to security guidelines and privacy regulations. Our goal is to create a methodology for auditing them automatically.

RQ2. What are the metrics for practically implementing IoT cybersecurity guidelines? In order to measure the compliance of IoT devices with security guidelines, it is necessary to extract metrics from each guideline. Every metric is tested on the devices through dedicated experiments.

RQ3. Is it possible to measure privacy regulations? Similarly to security guidelines, we also create metrics from privacy regulations, such as GDPR. By doing this, we determine whether IoT manufacturers respect such regulations. Differently from security guidelines, privacy regulations are mandatory in some countries.

2 COMPARISON WITH THE STATE OF THE ART

Due to the rapid growth of the IoT ecosystem, researchers have proposed different methods for analysing and validating the behaviour of IoT devices [5–8]. However, the state-of-the-art works all focus on specific aspects and do not propose any framework to obtain a comprehensive certification of the devices' security and privacy behavior. Conversely, there are active programs promoted by international agencies and standardisation bodies trying to fill this gap [1, 2].

In this direction, some attempts of certification frameworks tailored to the IoT context are available in the literature. See [9], for an extensive overview of recent proposals.

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike International 4.0 License.
ACM MobiCom '23, October 2–6, 2023, Madrid, Spain
© 2023 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9990-6/23/10.
https://doi.org/10.1145/3570361.3615747

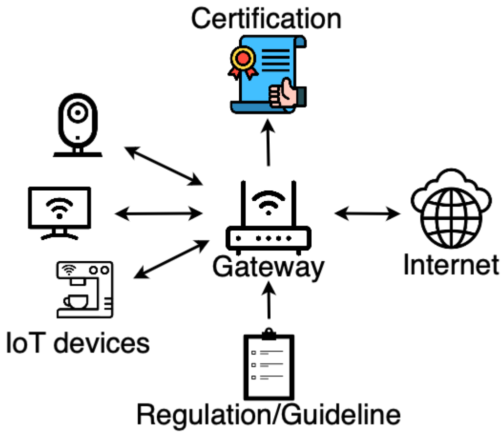

Figure 1: COPSEC Overview.

However, they are focused on certification processes performed by vendors, so that a certain degree of trust should be placed on them. To overcome this issue there is the need of a general framework for independent-third-parties (possibly final users) certifications of IoT devices.

As indicated in [10], it is crucial to have a robust open-source framework as automated as possible and not tailored for only a specific device. Therefore, assessing in a comprehensive manner whether IoT products comply with regulatory requirements is an open problem. This is mainly due to the heterogeneity of the IoT devices [11] and the dynamicity of IoT context [9]. Given this, a black-box testing methodology is the only effective way to address the above challenges.

The above overview makes it evident that a new framework is needed, in order to implement a scalable and trustworthy verification approach for IoT devices.

3 SYSTEM DESIGN

Figure 1 shows our system design. COPSEC runs on the gateway, we convert the input regulations and guidelines as measurable metrics and test them on IoT devices through *compliance scripts*. The output is a certification that states the compliance. We collect all the network traffic from the devices and we analyse it against the guidelines/regulations.

Our testbed is composed of: (*i*) a gateway, connected to the Internet, that provides IP connectivity to IoT devices and is able to capture all the network traffic, (*ii*) more than 200 medical and consumer IoT devices connected to the gateway, (*iii*) a suite of *compliance scripts* that perform automatic experiments for testing against security guidelines and privacy regulations running on the gateway.

We conduct idle and controlled experiments to analyse the devices under different conditions. Our initial results are generated through idle experiments, with no particular functionality executed on the devices. We also consider the network traffic generated during the device pairing with its respective app (configuration traffic).

4 METHODOLOGY AND RESULTS

In this preliminary work, we consider 10 consumer IoT devices from different categories (speakers, doorbells, cameras, appliances) and test them against the following two security guidelines reported in [1] and one article of GDPR.

4.1 Security Guidelines and Privacy Regulation

- **GP-TM-50**: Ensure only necessary ports are exposed and available.
- **GP-OP-04**: Use proven solutions, i.e. well known communications protocols and cryptographic algorithms, recognized by the scientific community, etc.
- **Art.32 (a)**: "... the controller and the processor shall implement... encryption of personal data"

4.2 GP-TM-50: Unnecessary Ports

Methodology. The procedure consists in the use of the *nmap* [12] to perform port scanning. Specifically, we scan the entire range of ports (from 0 to 65535). After detecting the open ports, we analyze the traffic exchanged by devices during idle activity for a period of 1 month. Then, we derive the subset of the open ports not actually used by the devices. **Result.** Table 1 (column 2) shows that 6 over 10 devices present at least a port not used during the idle activity. Further experiments will be conducted by triggering specific functions of the devices and analyzing the unused open ports. This behaviour is not compliant with the ENISA security guideline GP-TM-50 [1].

4.3 GP-OP-04: Standard Protocols

Methodology. We focus on checking the adoption of standard communication protocols by the IoT devices.

To test the compliance with the guideline, we proceed as follows. As a reference, we consider the list of well-known and registered ports assigned by IANA [13]. By examining the traffic in idle mode, we identify all the flows exchanged through ports not present in the above list. Through this procedure, we obtain the number of unrecognized protocols for each device. To get a complete view, we also detect the number of recognized protocols adopted by each IoT device. This number is obtained by simply counting the number of distinct ports known to be associated to standard protocols. **Result.** Results (Table 1, columns 3-4) show that 6 devices are not compliant with the guideline since they exchange traffic by leveraging at least one non-standard protocol during the idle activity. We expect that further violation of this guideline can be observed by triggering specific functions of the devices. We want to observe that this procedure does not present any false positive results. However it may result in some false negative result (unrecognized protocols identified as recognized). This happens when the devices use some well-known or registered ports of IANA to exchange data

Device	# of Unused Open Ports	# of Unrecognized Protocols	# of Recognized Protocols	Compliant with GDPR Art. 32 (a)
Bose Speaker	11	0	7	✓
Echo Dot 5	5	3	9	✓
Furbo Dog Camera	0	1	6	✓
Google Nest Cam	3	1	6	✓
Govee lights	0	0	5	✓
Ring Video Doorbell	0	2	6	✓
Sensibo Sky Sensor	0	0	2	✓
SimpliSafe Cam	1	0	3	✓
Sonos One	5	1	8	X
WeeKett Kettle	1	2	2	✓

Table 1: Results of devices compliance.

through not standard protocols. As future work, we will refine the methodology to address this limitation by checking packet headers.

4.4 Art.32 (a): Encryption of Personal Data

Methodology. We define a list of personal data (according to the directives issued by GDPR) that a device might send. This list includes data related to the accounts created during the configuration of the devices (e.g., name, surname, home address, telephone number, email address ecc.), the devices' IP, MAC addresses and identifiers.

Moreover, we include in the list some keywords related to the activity of users that may reveal private information (the state of devices, the values they capture, etc.).

COPSEC is able to detect the above keywords in the traffic sent in plain text by the device.

Result. Our analysis shows that the Sonos One device sends a firmware update request in plain text embedding in it the MAC address. This represents a violation of the GDPR directives, since MAC addresses are included in the category of "online identifiers". As future work we plan to apply the above methodology to the traffic exchanged in the local network by the devices.

5 CONCLUSION

This paper introduces COPSEC, a framework for automatically auditing the compliance of IoT devices with security guidelines and privacy regulations. Our idle experiments show a not compliant behaviour with two ENISA security guidelines (GP-TM-50 and GP-OP-04) and with the GDPR directives (Art. 32 (a)). Therefore, our initial results highlight the need of performing more experiments and testing more guidelines and regulations.

As future work, we plan to test more devices, make the framework open-source and running in a real smart gateway in order to produce open-source IoT certifications. Our aim is to bridge the knowledge and methodological gap that exists between stakeholders and the technical community, also producing knowledge for informing regulatory organizations.

REFERENCES

[1] European Union Agency for Cybersecurity (ENISA). Baseline security recommendations for iot, 2021. Accessed: June 14, 2023.

[2] NIST. Cybersecurity for iot program, 2021. Accessed: June 14, 2023.

[3] European Commission. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), 2016.

[4] California State Legislature. California consumer privacy act (ccpa), 2018. Accessed: June 30, 2023.

[5] Jingjing Ren, Daniel J. Dubois, David Choffnes, Anna Maria Mandalari, Roman Kolcun, and Hamed Haddadi. Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach. In *Proceedings of the Internet Measurement Conference*, IMC '19, page 267–279, New York, NY, USA, 2019. Association for Computing Machinery.

[6] Hyunji Chung, Michaela Iorga, Jeffrey Voas, and Sangjin Lee. "alexa, can i trust you?". *Computer*, 50(9):100–104, jan 2017.

[7] Noah Apthorpe, Danny Huang, Dillon Reisman, Arvind Narayanan, and Nick Feamster. Keeping the smart home private with smart(er) iot traffic shaping. *Proceedings on Privacy Enhancing Technologies*, 2019:128–148, 07 2019.

[8] Danny Yuxing Huang, Noah Apthorpe, Frank Li, Gunes Acar, and Nick Feamster. Iot inspector: Crowdsourcing labeled network traffic from smart home devices at scale. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 4(2), jun 2020.

[9] André Cirne, Patrícia R. Sousa, João S. Resende, and Luís Antunes. Iot security certifications: Challenges and potential approaches. *Comput. Secur.*, 116(C), may 2022.

[10] Sara N. Matheu, José L. Hernández-Ramos, Antonio F. Skarmeta, and Gianmarco Baldini. A survey of cybersecurity certification for the internet of things. *ACM Comput. Surv.*, 53(6), dec 2020.

[11] Gianmarco Baldini, Antonio Skarmeta, Elizabeta Fourneret, Ricardo Neisse, Bruno Legeard, and Franck Le Gall. Security certification and labelling in internet of things. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pages 627–632. IEEE, 2016.

[12] Gordon Fyodor Lyon. *Nmap network scanning: The official Nmap project guide to network discovery and security scanning.* Insecure. Com LLC (US), 2008.

[13] IANA. Service name and Transport Protocol Port Number Registry Internet Assigned Numbers Authority. https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml, 2023. Accessed: August 12, 2023.