Empowering End-Users in the Specification of Security Rules

Bernardo Breve[a], Vincenzo Deufemia[a]

[a]University of Salerno, 84084 Fisciano(SA), Italy

Abstract

With the rapid growth of Internet-of-Things (IoT) devices, especially in the context of smart homes, end-user programming is becoming increasingly common to easily create new functionalities by connecting IoT devices and online services using simple rules, such as *event-condition-action* (ECA) rules. Unfortunately, IoT devices and platforms are vulnerable under security terms, and the possible countermeasures to security threats are completely hidden to end-users. This position paper presents the idea of involving end-users in the management of security risks. In particular, we describe how existing ECA rules could be expanded to deal with security aspects, and possible strategies to support end-users in the definition and customization of security rules.

Keywords

End-user programming, Security rules, Internet of Things (IoT)

1. Introduction

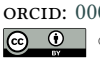
Internet-of-Things (IoT) platforms and devices are being widely used in industrial and domestic contexts. The platforms facilitate the interoperability between different smart devices and cloud services, providing end-users with tools to easily program their interaction by means of simple conditional rules [1, 2].

IoT platforms provide privileged access to a user's online services and physical devices, making them an attractive target for attackers. If they are compromised, both data and devices belonging to a large number of users can be arbitrarily manipulated by the attackers to cause damage. For example, the violation of an IFTTT rule allows an attacker to access sensitive information, such as user locations, fitness information, the content of private files, or private feed from social networks.

Most attempts to date in IoT security aim to improve perimeter defenses that harden the IoT infrastructure against attacks using firewalls [3], intrusion detection [4], access control policies [5], and software patches [6], or to execute the actions in decentralized fashion [7]. Unfortunately, end-users have a low-level awareness of security threats and usage of security measures. Most of the users have little o no technical knowledge of the gravity of what a

EMPATHY: Empowering People in Dealing with Internet of Things Ecosystems. Workshop co-located with AVI 2020, Island of Ischia, Italy

EMAIL: bbreve@unisa.it (B. Breve); deufemia@unisa.it (V. Deufemia)
URL: https://docenti.unisa.it/vincenzo.deufemia (V. Deufemia)
ORCID: 0000-0002-6711-3590 (V. Deufemia)



security violation could represent. The security of an IoT platform can be improved involving end-users in the security control and increasing their awareness of security risks [8].

This position paper presents the idea of involving end-users in the management of security aspects. In particular, we describe how existing ECA rules could be expanded to deal with security aspects, and possible strategies to support end-users in the definition and customization of security rules.

2. Specification of Security Rules

ECA rules represent a programming paradigm for the specification of a particular type of behavior in active systems [1]. For instance, an ECA rule can define how a certain IoT device should react at an external event generated by a sensor, an on-line service, or another IoT device. In the following, we describe how these rules can be enhanced to allow end-users to define countermeasures to security threats. For example, an end-user might want to define an ECA rule for turning off an IP camera installed in its smart home when an intrusion is detected. Also, in response to an external intrusion, s/he might want to temporally disable all internet connectivity from all the devices within the environment. By doing so, s/he prevents the intruder from spreading his/her control over the other IoT devices, waiting for reviewing the whole network, looking for some security flaws.

These rules require a Local Monitoring Service (LMS) that would oversee the network, providing the triggers for such security events. In particular, the LMS analyzes all the interconnected devices notifying any security threat happening in the smart environment. In fact, these types of events cannot be recorded by the IoT devices themselves, since IoT devices are commonly known to lack in performances, so it would be really difficult for them to perform monitoring tasks alongside the operations they have been initially designed for. Moreover, the majority of IoT devices are embedded systems, which means that their software capabilities are not meant to be expanded or modified by others.

Another important topic to discuss is the actual possibility for an end-user to understand the risks related to the security threats, and to autonomously decide of defining rules aimed at protecting the environment. In fact, the end-users' limited technical knowledge makes it hard for them to define behaviors for realizing security barriers. Thus, a valuable strategy for guiding users into this task would be to suggest rules that have been considered particularly suitable for defending the environment, perhaps by suggesting rules that have already been defined and deployed by other users. Rules could be stored in centralized repositories which can be organized and evaluated both automatically and manually [9].

To provide these suggestions in the most comfortable way, two types of strategies could be applied. A set of security rules could be provided directly from the environment once the IoT device is recognized, e.g., an IP camera, which basic functionalities are known, and generalized over different types of brands and models. In this way, end-users can comfortably decide what rules best suits the device installed in the smart environment. Alternatively, security rules could be organized based on their defense capabilities against certain types of attacks. For example, the environment might notify the end-user with all the security rules that could protect the IoT device against external intrusions. In this way, users can enable all the rules available for each

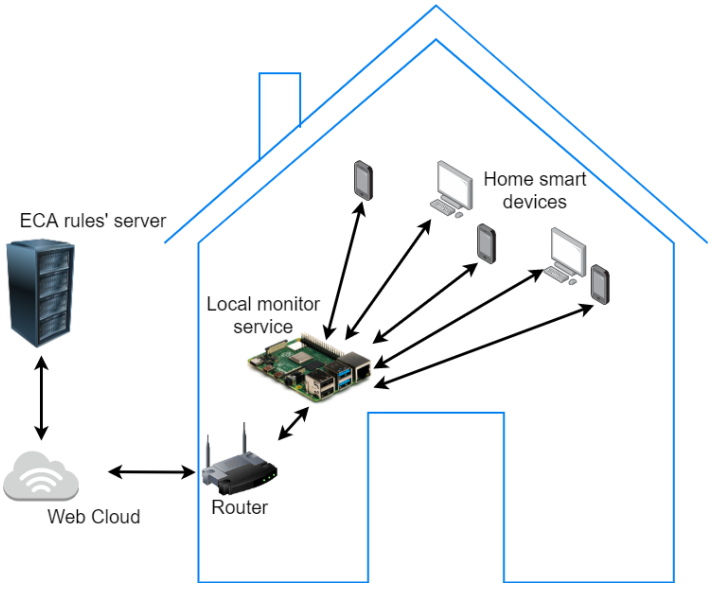


Figure 1: An LMS-based architecture for executing security rules.

device without having to singularly define each behavior from scratch.

The development of the proposed approach relies on the implementation of a LMS able to identify any network anomalies that might be associated with some ECA rule events. This service can be executed on single-board computers (SBCs), among which the most famous on the market appears to be the Raspberry Pi.

Figure 1 shows a simple schema of the architecture describing the logic of analysis and communication between the LMS and the server responsible for storing and triggering the ECA rules. The LMS acts as an intermediary between the smart devices and the router analyzing any network packets exchanged from/to the home smart devices. When the LMS identifies some anomalies in the network traffic, it will gather all the information about the anomalies and pack them all in a certain event. This event is sent to the ECA rules' server, which will verify whether there exist any ECA rules having that event as a trigger condition. Thus, the retrieved rules are triggered and the corresponding actions are executed.

At the workshop, we will discuss how the security rules could be specified by end-users and the challenges to be addressed for increasing the awareness of security threats.

Acknowledgments

This work has been supported by the Italian Ministry of Education, University and Research (MIUR) under grant PRIN 2017 "EMPATHY: Empowering People in deAling with internet of THings ecosYstems" (Progetti di Rilevante Interesse Nazionale – Bando 2017, Grant 2017MX9T7H).

References

[1] G. Desolda, C. Ardito, M. Matera, Empowering end users to customize their smart environments: Model, composition paradigms, and domain-specific tools, ACM Trans. Comput.-Hum. Interact. 24 (2017). doi:10.1145/3057859.

[2] G. Ghiani, M. Manca, F. Paternò, C. Santoro, Personalization of context-dependent applications through trigger-action rules, ACM Trans. Comput.-Hum. Interact. 24 (2017). doi:10.1145/3057861.

[3] S. Kubler, K. Främling, A. Buda, A standardized approach to deal with firewall and mobility policies in the IoT, Pervasive and Mobile Computing 20 (2015) 100 – 114. doi:https://doi.org/10.1016/j.pmcj.2014.09.005.

[4] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, S. C. de Alvarenga, A survey of intrusion detection in internet of things, Journal of Network and Computer Applications 84 (2017) 25 – 37. doi:https://doi.org/10.1016/j.jnca.2017.02.009.

[5] W. He, M. Golla, R. Padhi, J. Ofek, M. Dürmuth, E. Fernandes, B. Ur, Rethinking access control and authentication for the home internet of things (IoT), in: Proceedings of the 27th USENIX Conference on Security Symposium, SEC'18, USENIX Association, USA, 2018, p. 255–272.

[6] O. Leiba, R. Bitton, Y. Yitzchak, A. Nadler, D. Kashi, A. Shabtai, IoTPatchPool: Incentivized delivery network of IoT software updates based on proofs-of-distribution, Pervasive and Mobile Computing 58 (2019) 101019. doi:https://doi.org/10.1016/j.pmcj.2019.04.010.

[7] E. Fernandes, A. Rahmati, J. Jung, A. Prakash, Decentralized action integrity for trigger-action IoT platforms, in: Proceedings of the 22nd Network and Distributed Security Symposium (NDSS 2018), 2018.

[8] U. H. R. Xavier, B. P. Pati, Study of internet security threats among home users, in: Proceedings of the Fourth International Conference on Computational Aspects of Social Networks (CASoN), 2012, pp. 217–221.

[9] O. Alrawi, C. Lever, M. Antonakakis, F. Monrose, SoK: Security evaluation of home-based IoT deployments, in: Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), 2019, pp. 1362–1380.