

Enabling End-Users to Specify Security Rules with the EFESTO-5W Platform

Bernardo Breve¹, Francesco Greco², Giuseppe Desolda², Maristella Matera³ and Vincenzo Deufemia¹

¹University of Salerno, Fisciano SA 84084, Italy

²University of Bari Aldo Moro, Bari BA 70121, Italy

³Politecnico di Milano, Milano MI 20133, Italy

Abstract

Given the spread of the Internet of Things (IoT) technology, end-users have begun raising the need for configuring their smart environments. Task Automation Systems (TASs) recently emerged as tools to simplify the definition of trigger-action rules for personalizing the behavior of such devices. However, such tools do not take into account a typical aspect of IoT technologies, i.e., the security and privacy threats to which the smart devices are exposed to. This position paper describes how TASs can be extended to support end-users in the specification of trigger-action rules addressing security and privacy threats.

Keywords

End-User Development, Internet of Things, Cyber Security

1. Introduction

In the last years, the Internet of Things (IoT) fostered the development of the so-called smart objects, which are digital devices embedding sensors and/or actuators, connected to the Internet, and that communicate among them creating ecosystems of heterogeneous and distributed services [1]. Given the spread of such technology, end-users began raising the need for configuring their smart environments. Task Automation Systems (TASs) recently emerged as tools to support non-technical users in defining the personalized behavior of smart objects. Such tools provide visual simplified mechanisms that help users in performing trigger-action programming by defining Event-Condition-Action (ECA) rules that specify smart objects' behavior. With TASs, the users can therefore take advantage of their smart objects by creating synchronizations that accommodate their every day and contextual needs.

Despite their unquestionable benefits TASs still neglect an important aspect in the IoT landscape, i.e., security and privacy issues. Indeed, smart objects represent an attractive target for attackers, who might violate smart environments for manipulating data and stealing personal


EMPATY: Empowering People in Dealing with Internet of Things Ecosystems. Workshop co-located with INTERACT 2021, August 30, 2021, Bari, Italy

✉ bbreve@unisa.it (B. Breve); francesco.greco@uniba.it (F. Greco); giuseppe.desolda@uniba.it (G. Desolda); maristella.matera@polimi.it (M. Matera); deufemia@unisa.it (V. Deufemia)

🆔 0000-0002-3898-7512 (B. Breve); 0000-0003-2730-7697 (F. Greco); 0000-0001-9894-2116 (G. Desolda); 0000-0003-0552-8624 (M. Matera); 0000-0002-6711-3590 (V. Deufemia)



© 2021 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

information [2]. This problem is amplified when end-users, who are not provided with sufficient skills in security and privacy, put in communication their devices by using TASs. In addition, they underestimate the importance of these aspects in defending their smart environments, thus they neglect countermeasures that might protect the security of their smart devices [3].

This position paper describes an ongoing work that aims to support end-users in defending their smart environment. To this aim, we designed and evaluated a visual paradigm for TASs that facilitates the end-users in understanding and controlling security and privacy threats. This paper reports some technical details on how TASs can implement the proposed solution.

2. Extending TAS capabilities for managing security and privacy aspects

In order to include security and privacy management capabilities in TASs, we focused on EFESTO-5W, a TAS that provides visual mechanisms to create ECA rules characterized by multiple events/actions and temporal and spatial constraints on events and actions [4, 5]. We extended the EFESTO-5W visual paradigm and its functionalities so that end-users could manage security and privacy threats of a smart environment. The seed of this research is a smart object called Intrusion Defender (ID), which monitors the network traffic of a private area network (PAN) to detect attacks against smart devices. The proposed visual paradigm facilitates end-users to leverage the monitor capabilities of the ID through the definition of ECA rules like “**IF** the ID detects a virus in the IP camera **THEN** turn off the IP camera”. It is worth remarking that the visual mechanisms and the functionalities described in this paper, despite have been designed and tested for EFESTO-5W, can be applied to any TAS.

3. Intrusion Defender architecture

The ID is built on top of Snort¹ [6], a Network Intrusion Detection System that monitors all packets traveling from/to the PAN to detect attacks and suspect activities. Any anomalous pattern in the network traffic is identified and associated by the ID with a known security or privacy threatening event.

According to our proposal, it runs on a Raspberry Pi board that must be installed inside the PAN the users want to protect. The ID monitors the PAN traffic and eventually sends messages to the EFESTO-5W remote server when an attack is detected (see Figure 1).

Through the TAS, like EFESTO-5W in our case, users are given the possibility to trigger a rule according to 6 different security and privacy threatening events, each one associated with a specific attack the ID can detect. These events are the results of the previous study that addressed two main challenges. First, since the ID natively detects several attacks (35 in the current implementation), this high number can overload the users with too much information. Second, the detected attacks refer to technical cybersecurity concepts (e.g., DDoS, man in the middle, etc.), which are too complex for lay users. To address the first challenge, we performed a card sorting study with 11 IT and cybersecurity experts to group the 35 attacks detected

¹<https://www.snort.org/>

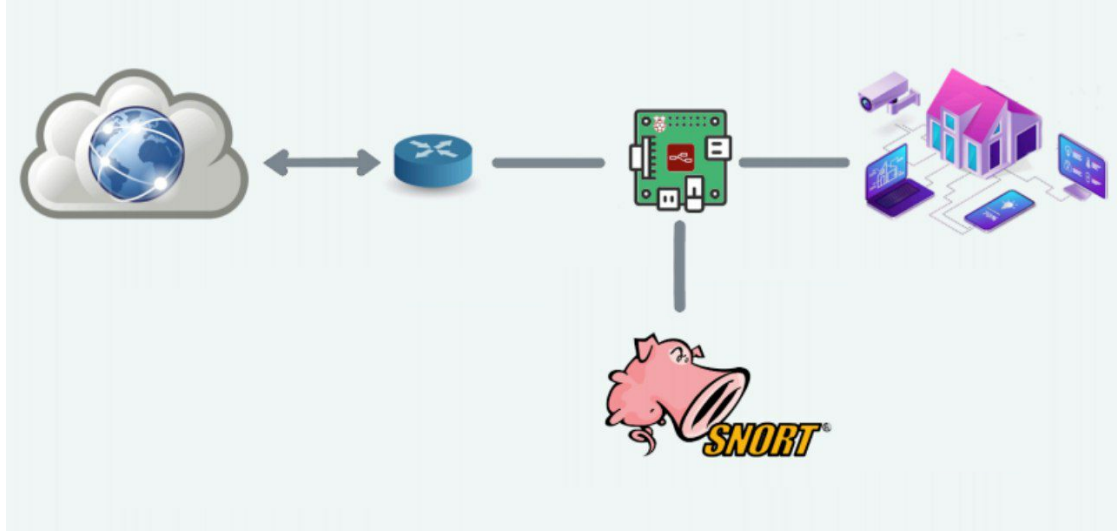


Figure 1: Architecture of a LAN which includes Snort (at the bottom) and the Raspberry Pi device (at the center).

by Snort according to their similarity [7]. This activity led to the definition of 6 groups of attacks. To solve the second challenge, and in particular to expose the ID events in a simple way within TASSs, we purposely designed 6 event messages, one for each group of attacks, in order to simplify the meaning of the attacks to non-technical users. The resulting ID events are:

1. *Someone is attacking one of your smart devices. This has the goal to make the device collapse;*
2. *A virus has infected one of your smart devices. This virus can compromise your device and your privacy (e.g., steal your files and passwords);*
3. *A non-authorized user has accessed one of your devices (or is trying to). If not stopped, this user may damage your device and steal your private data;*
4. *Someone is trying to steal your private data on one of your smart devices. This can threaten your privacy (e.g., pictures/video stolen);*
5. *Someone is looking for vulnerabilities in your network. This event might reveal an incoming attack;*
6. *Suspicious activity is going on against your network. Someone could be trying to attack and access your network.*

End-users can thus define an ECA rule using these ID events according to the threat they want to manage, and one or more actions in response to it. Figure 2 shows an example of an ECA rule configured with EFESTO-5W. This rule is triggered when the ID detects a virus in the Hallway camera, and reacts by turning off the attacked camera.

Every time a user defines an ECA rule in EFESTO-5W, a JSON file describing the rule is created according to the Node-RED syntax, since Node-RED is used in EFESTO-5W as rule engine [8]. Each rule of EFESTO-5W is, thus, represented as a Node-RED "flow" (i.e., a set of nodes which describe the rule). An EFESTO-5W rule, containing as event the ID smart object,

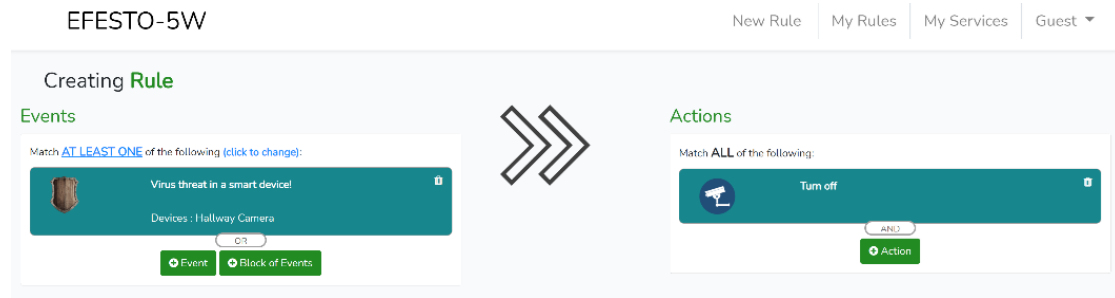


Figure 2: An example of ECA rule in response to a security threat created in EFESTO-5W.

translates to a Node-RED flow, in which the ID event is represented by an MQTT node listening on a specific port (in our configuration it is port 18883).

If the ID device detects an attack, it sends the attack details to the MQTT broker; the latter, in turn, notifies the MQTT node of the Node-RED flow (which represents the rule in EFESTO-5W). Then, the node checks if this attack is the one defined by the user in the rule. For example, to check if the triggered event of the ID is “*Someone is attacking one of your smart devices...*”, in the node there is the following code:

```
1 msg.payload = JSON.parse(msg.payload)[0]['sig_classname'];
2 if (msg.payload == 'system-call-detect' || msg.payload == 'denial-of-service' || msg.payload ==
    'successful-dos' || msg.payload == 'attempted-dos' || msg.payload == 'misc-attack')
    return msg;
```

Listing 1: Javascript code for checking the *DOS* class

In this code, the *msg.payload* includes the details of the attack received through the MQTT broker. To verify whether the attack is the one defined in the rule event, the *classname* attribute of the payload is compared with all the labels representing the ID event. Indeed, as we already explained above, the ID device can detect 35 attacks but they were grouped in 6 events, each one including similar attacks whose name is reported in a label. If the attack detected by the ID device is the same of one of the labels related to the event specified in the rule, the rule is triggered. This architecture is general enough to be implemented in every TAS. Of course, while in EFESTO-5W the ID device is represented by a Node-RED node, in other TASs it must be coded according to the specific solutions adopted to develop the tool, but the MQTT guarantees a strong decoupling between the ID device and the specific TAS.

4. Conclusions

In this position paper, we presented a solution to help users defend their smart environment thanks to the use of a specific smart device, the Intrusion Defender, whose monitor capabilities can be leveraged by using a TAS. In addition, we also reported some technical details about the integration of TASs and the ID device.

As future works, we are going to refine the 6 events provided by the ID device, according to the results of the study presented in [7]. In addition, we are empowering the entire solution offering, on demands, more powerful and low-level mechanisms to deeply control the ID device, for example, giving to IT and security experts the possibility to create ECA rules including one or more attacks selected from all the 35 attacks the ID device can detect.

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] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, *Computer networks* 54 (2010) 2787–2805.
- [2] M. Galluscio, N. Neshenko, E. Bou-Harb, Y. Huang, N. Ghani, J. Crichigno, G. Kaddoum, A first empirical look on internet-scale exploitations of iot devices, in: *Proceedings of IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)*, IEEE, 2017, pp. 1–7.
- [3] A. Alqhatani, H. R. Lipford, “there is nothing that i need to keep secret”: Sharing practices and concerns of wearable fitness data, in: *Proceedings of Fifteenth Symposium on Usable Privacy and Security (SOUPS’19)*, 2019.
- [4] G. Desolda, C. Ardito, M. Matera, End-user development for the internet of things: Efesto and the 5w composition paradigm, in: *International Rapid Mashup Challenge*, Springer, 2016, pp. 74–93.
- [5] G. Desolda, C. Ardito, M. Matera, Empowering end users to customize their smart environments: model, composition paradigms, and domain-specific tools, *ACM Transactions on Computer-Human Interaction (TOCHI)* 24 (2017) 1–52.
- [6] M. Roesch, Snort - lightweight intrusion detection for networks, in: *Proceedings of the 13th USENIX Conference on System Administration, LISA ’99*, USENIX Association, USA, 1999, p. 229–238.
- [7] B. Breve, G. Desolda, V. Deufemia, F. Greco, M. Matera, An end-user development approach to secure smart environments, in: D. Fogli, D. Tetteroo, B. R. Barricelli, S. Borsci, P. Markopoulos, G. A. Papadopoulos (Eds.), *End-User Development*, Springer International Publishing, Cham, 2021, pp. 36–52.
- [8] G. Desolda, F. Greco, Integrating the node-red server in an iot platform for ECA rules management, in: G. Desolda, V. Deufemia, C. Gena, M. Matera, F. Paternò, B. Treccani (Eds.), *Proceedings of the 1st International Workshop on Empowering People in Dealing with Internet of Things Ecosystems co-located with International Conference on Advanced Visual Interfaces (AVI 2020)*, Online / Island of Ischia, Italy, September 29, 2020, volume 2702 of *CEUR Workshop Proceedings*, CEUR-WS.org, 2020, pp. 45–48.