Task Automation Systems to Secure Smart Environments

Fabrizio Balducci[1], Bernardo Breve[2], Giuseppe Desolda[1], Francesco Greco[1], Vincenzo Deufemia[2]

[1] *Computer Science Department, University of Bari Aldo Moro, Italy*
[2] *Computer Science Department, University of Salerno, Italy*

Abstract

Task automation systems (TAS) allow users to customize the behaviour of their smart devices according to their daily and personal needs. However, they do not address the security and privacy threats that can arise from the use and composition of smart devices. To democratize cybersecurity in smart environments, TASs should enable both experts and novices to protect their devices from external threats. This paper reports a study that investigated the mental models of cybersecurity novices and experts when defining security policies using the trigger-action paradigm provided by TAS. The results of this study guided the design of prototype solutions that extend a TAS, called EFESTO-5W, to allow both experts and lay users to define the security policies for IoT devices.

Keywords

Task Automation Systems; Trigger-Action Programming; Cybersecurity policies;

Introduction

Smart environments are becoming increasingly popular thanks to the Internet of Things (IoT) technology, which enables various smart devices to interact with each other and with their users. These devices, which consist of sensors and actuators, can carry out tasks autonomously, making it easier for users to access smart features such as automatic lighting and camera recording. However, not all users possess the technical knowledge to customize IoT devices to their needs, which can go beyond the native features of each device. Task Automation Systems (TAS) have been proposed to simplify the definition of interoperability mechanisms between smart devices using Trigger-Action Programming (TAP), which facilitates the visual definition of Event-Condition-Action (ECA) rules.

Despite their ease of use, IoT devices and TAS are vulnerable to security and privacy threats, making them attractive targets for malicious individuals. This is especially concerning for end-users without expertise in cybersecurity, who are unaware of the vulnerabilities to which smart environments are exposed and are not motivated to protect their devices from external threats. In some cases, end-users themselves may inadvertently create vulnerabilities through the automation they define using TAS.

To address these limitations, we recently conducted a study [5] to explore the mental models of cybersecurity novices and experts to understand how they would define ECA rules to specify cybersecurity policies for smart environments. The survey involved 32 participants (18 experts, 14 novices), and the results were evaluated through a thematic analysis. The five lessons learned provided the seed for the design of a prototype of a TAS that helps users define security policies for their smart homes.

IS-EUD 2023: 9th International Symposium on End-User Development, 6-8 June 2023, Cagliari, Italy
EMAIL: fabrizio.balducci@uniba.it (A. 1); bbreve@unisa.it (A. 2); giuseppe.desolda@uniba.it (A. 3); francesco.greco@uniba.it (A. 4); deufemia@unisa.it (A. 5)
ORCID: 0000-0003-1174-4323 (A. 1); 0000-0002-3898-7512 (A. 2); 0000-0001-9894-2116 (A. 3); 0000-0003-2730-7697 (A. 4); 0000-0002-6711-3590 (A.5)

Method

This section reports a summary of the study detailed in [5], which aims to address the following research question: *How does the mental model of novices and experts translate into EUD solutions for the cybersecurity of smart environments?* The goal was to explore the mental models of cybersecurity experts and novices in defining security countermeasures for smart environments using TAP programming, to understand how their mental models differ and what TAP solutions should be provided to each group. The authors conducted a questionnaire study and an inductive thematic analysis of the qualitative data obtained from the participants' responses.

The study recruited 32 Italian participants (7 female, 25 male) with an average age of 28.0 years. The majority of participants had at least a high school diploma, with 68.75% having a bachelor's degree and 18.75% having a master's degree. Approximately half of the participants were classified as cybersecurity experts based on a questionnaire, with the remaining participants classified as novices. The novices reported medium IT experience and frequent use of IoT devices, while the experts reported high IT experience and frequent use of IoT devices.

The study consisted of an online survey carried out on an online platform purposely built for the study. The platform included a privacy policy and demographic questionnaire, followed by the US Cybersecurity Knowledge questionnaire [7] to measure participants' knowledge about cybersecurity concepts. Participants were then introduced to the basic concepts of IoT devices, TAP programming, and ECA rules through a scenario involving Alexa. Finally, participants were asked to complete 6 attack tasks (9 in the case of experts) designed by the authors. The study procedure was validated by 4 experts and 4 novices and took approximately 22 minutes per participant. The US Cybersecurity Knowledge questionnaire was used to distinguish novices and expert users. This questionnaire consists of 13 questions that focus on key concepts and basic building blocks that cybersecurity experts consider critical for protecting users online. It was integrated into the platform and used to administer additional tasks to those participants who scored 8/10 or higher and were identified as cybersecurity experts.

The results of the thematic analysis led to the identification of five themes, which have been distilled in the form of five lessons learned, which are summarized in the following for the sake of clarity:

1. *Alert the user by default*: A TAS should communicate attack information promptly and by default, with the ability to customize notifications based on urgency and preferences.
2. *Compensate for missing information in rules*: Auto-completion technology should be used to help users define rules in the most natural way possible, including the use of artificial intelligence (AI) approaches to enhance capabilities and support end-user development (EUD).
3. *Enable the creation of complex rules, even for novices*: TAS systems should allow users to define optional parameters, conditions, multiple events and actions, and generic rules that work for any device on their network.
4. *Abstract security triggers should be available also to experts*: even though experts can benefit from having the possibility to define granular events (by allowing the definition of parameters to constrain the events of the rules), EUD systems should include abstract events by default, also for expert users.
5. *Assist novices in choosing less drastic solutions*: EUD systems should suggest alternatives to drastic actions to protect users more efficiently and without loss of functionality.

These lessons learned can drive the design of TAS that allow users to manage the security of their smart environments. In the next section, we will show how we applied them to design a prototype of a TAS for defining cybersecurity policies by visually defining ECA rules.

A prototype of TAS to define cybersecurity policies for IoT devices

In order to propose a solution that implements the results of the study reported in the previous section, we designed a prototype of TAS that allows novice and expert users to define cybersecurity policies in smart environments. The proposed solution extends and refines the one already presented in [4]: the overall idea revolves around the Intrusion Defender (ID), a smart object that monitors the network traffic of a Private Area Network (PAN) to detect anomalous events that could result from

cyber-attacks. Specifically, the ID is built on top of Snort, an open-source network intrusion detection system that monitors network traffic packets going to and from all smart objects in the smart environment. By analyzing the signatures contained in a database of attack-signature pairs, Snort can identify intrusions and generate an event reporting key information about the attack. All events generated are stored in a database. To effectively defend an intelligent environment against external cyber-attacks, Snort is configured to monitor the network locally, within the PAN. This is because it is not possible to remotely monitor the exchange of packets between intelligent devices in a PAN from outside the network. Therefore, the ID is implemented as a smart object that acts as an intermediary in the communication between the smart devices and the router. The ID intercepts and analyses network traffic for possible network intrusions, enabling real-time detection of cyber-attacks and taking the necessary measures to mitigate them.

In the previous version presented in [4], the users could define cybersecurity policies by using EFESTO-5W, a TAS that supports the visual creation of ECA rules automating IoT devices [6]. Specifically, EFESTO-5W was initially extended to create ECA rules in the form "I*F the ID detects the attack X then switch off the attacked device*", with 6 different ID triggering events implemented in the EFESTO-5W platform [3]: 1) *Someone is trying to collapse a smart device down*, 2) *Virus threat in a smart device*, 3) *A hacker is breaking in a smart device*, 4) *There's a danger of data theft from a smart device*, 5) *A suspicious event has occurred in your network*, 6) *Threats coming from outside your network*.

Based on the lessons learned emerged from the study, we implemented in EFESTO-5W the following new features:

1. When the user selects a security-related ID event, an action to send a notification to the default device for such communications (chosen a priori by the user, e.g., Amazon Alexa, email, etc.) is automatically created in the actions available for that device. This action is editable to redefine the message and/or the device (lesson 1 – Alert the user by default).
2. When the user selects a security event by specifying a smart object, an action suggestion for the device concerning the event appears in the actions: in EFESTO-5W it could be an action that is completed up to the "which" (the device or service), and it remains to select the "what", i.e. the action/event (lesson 2 - Compensate for missing information in rules).
3. Advanced features reserved for users who consider themself cybersecurity experts are available (e.g., "*A specific port is scanned*"); specifically, advanced events/actions are available only to expert users who register to EFESTO-5W as experts or that, over time, increase their skills and update/upgrade their profile to expert. Nonetheless, expert users should also have access to abstract security triggers (lesson 4 - Abstract security triggers should be available also to experts), as those presented in [3].
4. Specific risky actions (such as turning off the router, a device, or performing a factory reset) are labeled with a warning triangle icon and a brief description of the consequences so that the users are aware of the potential risks associated with that action. Moreover, the system suggests a list of less drastic actions for the selected one: e.g., if the user defines "Turn off the security cameras", the system presents a tooltip with a suggested alternative action like "Disconnect the security cameras from the Internet" (lesson 5 - Assist novices in choosing less drastic solutions).

It is worth mentioning that lesson 3 (Allow the creation of complex rules even for novices) is available in EFESTO-5W since it is already possible to join with AND and OR conditions multiple triggering events. **Figure 1** shows an example of a security rule in EFESTO-5W to protect the user's smart TV against malware. Once the user selects the security event of Intrusion Defender (on the left), two actions are created automatically (on the right): an action to notify the user about the attack via their default communication channel (lesson 1), and a draft action for the smart TV that must be completed by the user (lesson 2). ***Figure 2*** shows how an expert user can define granular rules by selecting more advanced events and actions (lesson 4). Here the system reacts to the user choosing a risky action ("Turn off router") by showing alternative, less risky, actions in a popover (lesson 5).

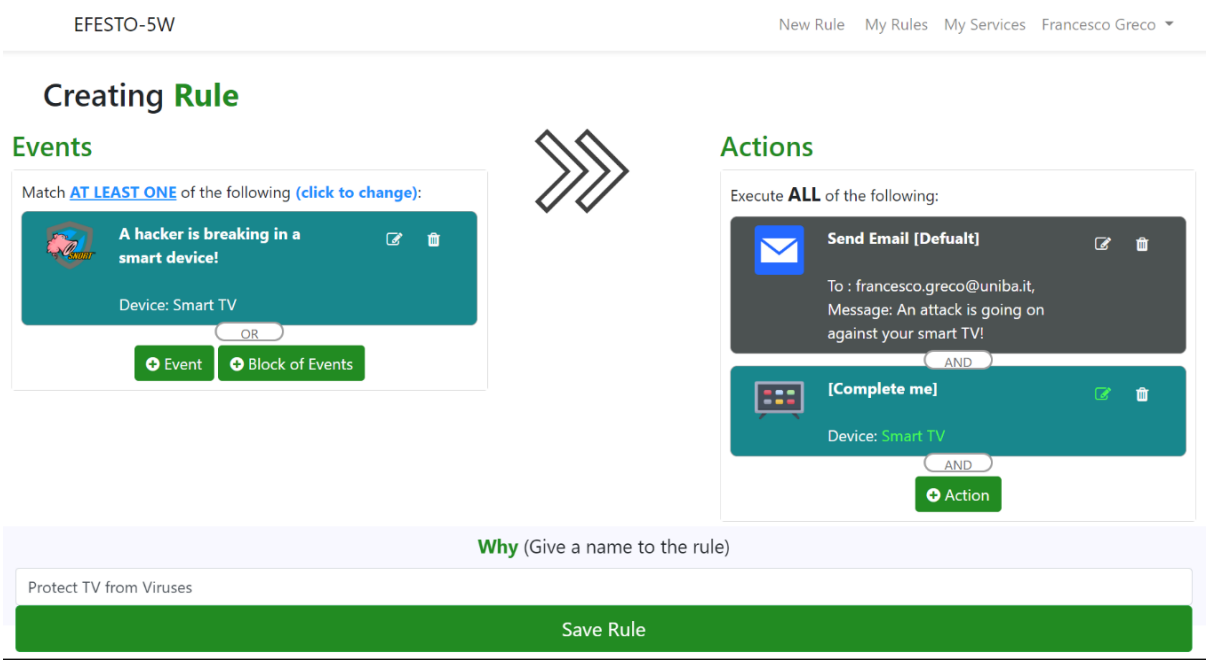

Figure 1: Implementation of lesson 1 (*Alert the user by default*) and lesson 2 (*Compensate for missing information in rules*) in the EFESTO-5W prototype. Lesson 3 (*Enable the creation of complex rules, even for novices*) is also implemented, as users can define granular rules with many events and actions.

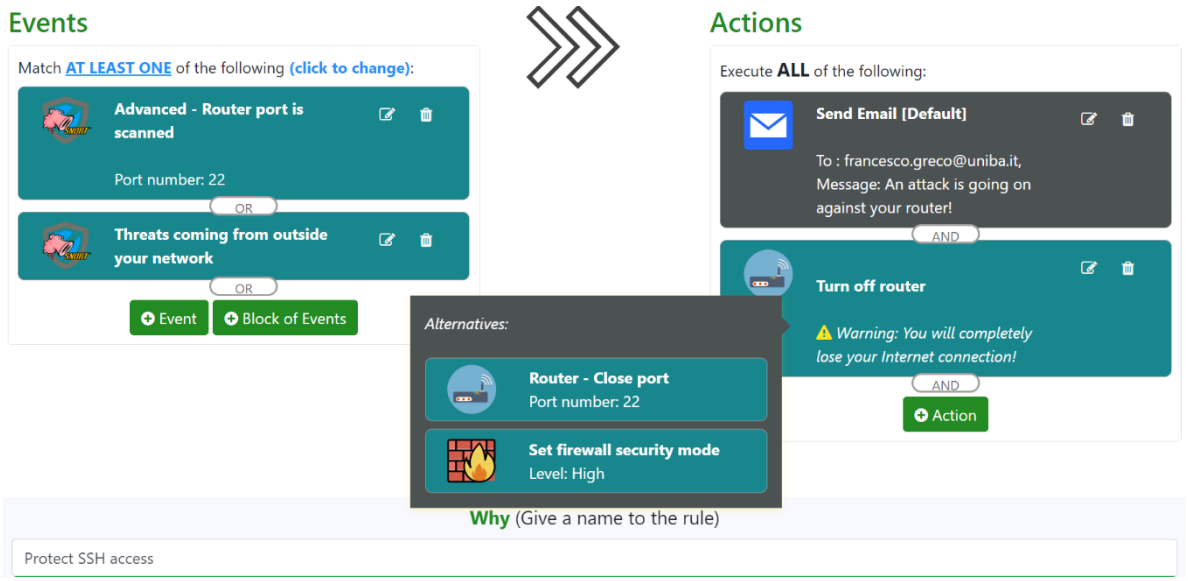

Figure 2. Implementation of lesson 4 (*Abstract security triggers should be available also to experts*) and lesson 5 (*Assist novices in choosing less drastic solutions*) in the EFESTO-5W prototype.

Conclusion and future work

In this paper, we present a prototype of an enhanced version of EFESTO-5W, a TAS that allows users to define security rules for their smart environment. The design of this prototype follows the results of a previous study that investigated the mental models of novice and expert users when securing their smart homes [5]. In particular, we proposed an implementation of the resulting lessons learned to support both novice and expert users in rule definition by matching their mental models. As future work, we planned to extend the functionalities presented in this workshop with further features that can give users more control over the defense of their cyberspace, also thanks to the use of semantic abstractions that can simplify the definition of ECA rules [1, 2].

Acknowledgements

This work is partially supported by the Italian Ministry of University and Research (MIUR) under grant PRIN 2017 “EMPATHY: Empowering People in dAling with internet of Things ecosYstems” and with the co-funding of the European union - Next Generation EU: NRRP Initiative, Mission 4, Component 2, Investment 1.3 – Partnerships extended to universities, research centres, companies and research D.D. MUR n. 341 del 5.03.2022 – Next Generation EU (PE0000014 - "Security and Rights In the CyberSpace - SERICS" - CUP: H93C22000620001).

The research of Francesco Greco is funded by a PhD fellowship within the framework of the Italian “D.M. n. 352, April 9, 2022”- under the National Recovery and Resilience Plan, Mission 4, Component 2, Investment 3.3 - PhD Project “Investigating XAI techniques to help user defend from phishing attacks”, co-supported by “Auriga S.p.A.” (CUP H91I22000410007).

Fabrizio Balducci acknowledges the support by the REsearch For INnovation (REFIN) grant, CUP:H94I20000410008 cod.F517D521 POR Puglia FESR FSE 2014-2020 “Gestione di oggetti intelligenti per migliorare le esperienze di visita di siti di interesse culturale”.

References

[1] Ardito, C., Desolda, G., Lanzilotti, R., Malizia, A. and Matera, M. (2020). Analysing trade-offs in frameworks for the design of smart environments. *Behaviour & Information Technology*, 39(1), 47-71.

[2] Ardito, C., Desolda, G., Lanzilotti, R., Malizia, A., Matera, M., Buono, P. and Piccinno, A. (2020). User-defined semantics for the design of IoT systems enabling smart interactive experiences. *Personal and Ubiquitous Computing*, 24(6), 781-796.

[3] Breve, B., Desolda, G., Deufemia, V., Greco, F. and Matera, M. (2021). Enabling End-Users to Specify Security Rules with the EFESTO-5W Platform. In *Proc. of the International Workshop “EMPATHY: Empowering People in Dealing with Internet of Things Ecosystems” co-located with INTERACT 2021 (Enabling End-Users to Specify Security Rules with the EFESTO-5W Platform)*. CEUR Workshop Proceedings.

[4] Breve, B., Desolda, G., Deufemia, V., Greco, F. and Matera, M. (2021). An end-user development approach to secure smart environments. In *Proc. of the End-User Development: 8th International Symposium (IS-EUD '21)*. Springer International Publishing, LNCS, 36-52.

[5] Breve, B., Desolda, G., Greco, F. and Deufemia, V. (2023). Democratizing Cybersecurity in Smart Environments: Investigating the Mental Models of Novices and Experts. *9th International Symposium on End User Development (IS-EUD '21)*. Cagliari, Italy.

[6] Desolda, G., Ardito, C. and Matera, M. (2017). End-User Development for the Internet of Things: EFESTO and the 5W Composition Paradigm. In *Proc. of the Rapid Mashup Development Tools (End-User Development for the Internet of Things: EFESTO and the 5W Composition Paradigm)*. Springer International Publishing, 74-93.

[7] Olmstead, K. and Smith, A. 2017. U.S. Cybersecurity Knowledge- What the public knows about cybersecurity Pew Research Center.