Learning Cybersecurity in IoT-based Applications through a Capture the Flag Competition

Alexandre Oliveira Junior*, Gustavo Funchal*, Jonas Queiroz*, Jorge Loureiro*,
Tiago Pedrosa*, Javier Parra†, Paulo Leitao*
* Research Centre in Digitalization and Intelligent Robotics (CeDRI), Instituto Politecnico de Braganca,
Campus de Santa Apolonia, 5300-253 Braganca, Portugal,
Email: {alexandrejunior, gustavofunchal, jpqueiroz, jorge.loureiro, pedrosa, pleitao}@ipb.pt
† BISITE Research Group, University of Salamanca,
Edificio Multiusos I+D+i, 37007 Salamanca, Spain, Email: javierparra@usal.es

2022 IEEE 20th International Conference on Industrial Informatics (INDIN) | 978-1-7281-7568-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/INDIN51773.2022.9976079

***Abstract*—The Internet of Things (IoT) is one of the main foundations of Industry 4.0, providing widespread connectivity of systems and devices, which promotes significant benefits, such as improved performance, responsiveness, and reconfigurability. However, it also brings some security problems, which make these devices and systems vulnerable to cyberattacks, consequently demanding efficient learning and training initiatives to address the challenges regarding the qualification of undergraduate students and active professionals to design more secure systems, as well as to be more aware of cyberthreats during the management and use of them. With this in mind, this paper describes a Capture the Flag competition based on IoT cybersecurity. The participants' feedback and performance evaluation show that this type of hands-on competition strongly contributes to learning the importance of cybersecurity in IoT-based applications.**

***Index Terms*—Internet of Things, cybersecurity, education 4.0.**

I. Introduction

The Internet of Things (IoT) paradigm is transforming processes in different sectors of society, namely industry, agriculture, autonomous vehicles, and others. The evolution of small embedded systems and wireless technologies has enabled sensors and computing systems to be integrated into daily objects that can now interact in new ways with the physical world, on such a scale that over 75 billion devices will be connected to the Internet by 2025 [1]. However, the fast diffusion of IoT-based applications is equipollent to the need for developing cybersecurity-related solutions, as the wide variety of connected devices also implies a plethora of vulnerabilities that put the global IoT network infrastructure at risk and constantly subject to cyberattacks [2].

Current trends within IoT-based systems such as Industry 4.0 (I4.0), smart homes, smart grids, and others generate and trade large amounts of personal or business data, which are very attractive to hackers. Cyberattacks on IoT systems are intensified by unconscious user practices, for instance, not updating the devices' systems and using default or weak passwords, which are further enhanced by the lack of security policies in developing and using IoT applications and protocols. Moreover, IoT devices are characterized by constrained computing resources, making it challenging to incorporate computationally intensive security and privacy methods [3], [4].

Learning cybersecurity is a must for everybody, from information and communication technologies (ICT) students to professionals. Resulting from the digital transformations and potentialized by the Covid-19 pandemic, several people lacking cybersecurity experience and skills have been brought into the virtual world and exposed to its threats. Training strategies must be deployed for cybersecurity awareness at different educational levels, ensuring everyone has a basic understanding of digital threats. Simultaneously, higher education institutions need to incorporate in their curricula subjects and actions that deepen theoretically and practically the concepts involving cybersecurity in its different domains, such as IoT, ensuring the mastering of the skills needed to develop applications with improved cybersecurity infrastructures [5]. Companies also have to focus on upskilling and reskilling their workforce, conducting regular cybersecurity training actions to prevent or mitigate the effects of cyberattacks on their Industrial Internet of Things (IIoT) systems [6].

Cybersecurity competitions and hackathons are an effective approach to the diffusion of ICT security learning. At these events, the attendees can acquire and improve their competencies in programming and security by developing innovative solutions to real cybersecurity problems. Moreover, these competitions are suitable for participants to foster teamwork skills and even create interest in pursuing a career as a cybersecurity specialist. Additionally, they often attract companies seeking to create networks with promising and talented future professionals [7].

Given the urgent need for training and learning strategies to meet the increasing demand for highly qualified students and professionals in IoT cybersecurity, a Capture the Flag (CTF) competition has been developed. This paper presents the held competition, describing its methodology, the proposed challenges, and respective learning outcomes. The CTF was developed and implemented in the scope of the DISRUPTIVE project (disruptive.usal.es), which aims to promote the diffusion of disruptive ICT in the cross-border region of north Spain-Portugal. By analyzing the attendees' performance on the challenges and their feedback, it was possible to evaluate

the CTF as a cybersecurity learning strategy and the points that must be improved for future editions. As a result, this competition contributes to the training of attendees by hands-on solving of challenges that address concepts of real cybersecurity problems in IoT-based systems.

The remaining of this paper is organized as follows. Section II discusses aspects of cybersecurity education, and Section III presents the structure and the learning goals of the CTF competition. Section IV describes the implementation of the CTF and discusses the achieved results. Finally, Section V rounds up the paper with the conclusions and future work.

II. Cybersecurity Education

Digital trends are taking the global population on a new trajectory of digitization and interconnectivity that brings harsher and more worrying consequences, such as the occurrence of cyber incidents, which are increasingly frequent and harmful, even leading to the downtime of critical services and infrastructure [8]. These significant changes in the digitization era impose substantial challenges, particularly in qualifying the workforce to mitigate potential threats. According to a State of Cybersecurity 2022 report from ISACA [9], companies lack the desired levels of staff and skills to combat cyberthreats. Furthermore, 63% of these companies have reported unfilled cybersecurity positions, and 60% of companies struggle to retain qualified cybersecurity professionals.

The knowledge gap among cybersecurity professionals is also strongly correlated with the static nature of academia, which has difficulty preparing students to deal with the constantly evolving digital threats that emerge along with the advent of technology trends related to the IoT and IIoT. It is vital to develop learning strategies that address the general aspects of cybersecurity, especially considering the fields that educational institutions do not properly cover, such as critical information infrastructures and data collecting devices like embedded and other IoT-related systems [10].

More interactive, hands-on learning strategies and environments are being encouraged to supplement traditional learning methods because they allow students to apply what they learn under controlled conditions, resulting in better retention of the learnt theory [11]. Regarding this within IoT-based applications, some works present the use of commercial off-the-shelf IoT devices [12], while others consider complete IoT environments, like smart homes, to teach IoT cybersecurity [13], [14]. In this context, hackathons and competitions are being widely introduced to facilitate training cybersecurity awareness [15], encouraging peer-to-peer learning, increasing participants' enthusiasm for learning new skills, and offering a more immersive and interactive experience. For example, in [16] an online and immersive CTF challenge was developed consisting of basic tasks related to cyberattacks on IoT devices.

CTF is a competition where the participants need to capture a flag as proof of solving a given challenge. There are different styles of CTF, such as the Jeopardy, attack-defense, and mixed. The first one consists of a series of problems that must be solved, e.g., by finding and exploiting a vulnerability in a system. In the attack-defense CTFs, the participants must protect their host computers while searching, exploiting and attacking the host computers of other teams. The Mixed CTF is a combination of the previously two styles [17].

In this context, CTFs have been used as an effective tool for cybersecurity education [18], complementing theoretical knowledge and concepts with practical and real-world exercises and applications. In a CTF, the participants can think like hackers to exercise their cybersecurity skills that can be used to design more secure systems [19].

III. A CTF for Cybersecurity Education in IoT

A Jeopardy-style CTF was developed to address the lack of educational strategies that relate cybersecurity learning to IoT-based devices and systems and also provide a hands-on approach. Moreover, the proposed CTF follows a gamification strategy that lately has shown several benefits as an educational tool, e.g., improving the student's engagement in the learning activities. The competition comprises two components. The first one consists of a multi-choice quiz to evaluate the participants' general knowledge of IoT cybersecurity concepts. The second component incorporated hands-on hacking challenges covering different cybersecurity categories, as illustrated in Fig. 1 and detailed in Table I.

A. Exploiting a Smart Home IoT Network Vulnerabilities

The CTF was developed following a story where the narrative unfolds in a sequence of challenges that lead the hacker to get full access to a smart home control system from an old IoT device found in the trash.

This scenario was chosen given the wide adoption of home appliances with smart devices features that aims to monitor, control and automate a home (e.g., light bulbs and security cameras). In many cases, they are connected and managed

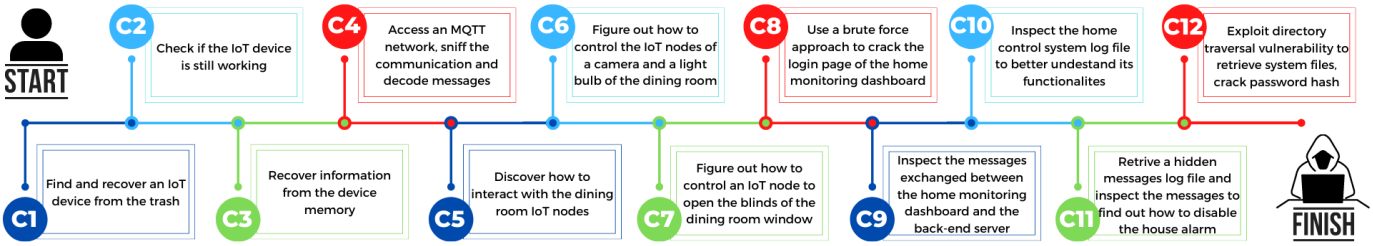


Fig. 1. Overview of the challenges developed for the IoT cybersecurity CTF.

TABLE I
LEARNING GOALS OF THE DESIGNED CHALLENGES

#	*Category*	*Learning goals*
C1	Reconnaissance, engineering	Disassemble and investigate an IoT device hardware components, and search for their specifications, in order to better understand the device features, including the microcontroller, operating system and communication protocols.
C2	Reconnaissance, engineering	Search for and use tools and procedures to connect to an IoT device through its input/output and communication interfaces.
C3	Firmware, engineering	Understand how to access and read binary code, how variables and program code are stored in microcontrollers, and how to identify and recover useful information, e.g., network and credentials from an IoT device memory.
C4	Cryptography, programming	Understand how the MQTT protocol works and how to implement a MQTT client, subscribe to topics and publish messages, as well as how to encode/decode the messages.
C5	Programming	Implement a MQTT client to sniff the messages in the IoT network and discover the connected devices and their message topics.
C6	Cryptography, programming	Understand the structure and format (e.g., JSON) used by the messages exchanged between the nodes, how to decode/encode the message content, and send messages to control an IoT device.
C7	Cryptography, programming	Implement and send encoded messages to control an IoT device.
C8	Web, cryptography	Exploit web login vulnerabilities (e.g., weak passwords and lack of mechanisms to prevent infinite login tries), searching for and using tools that can assist and automate these tasks (e.g., by performing brute force attacks to crack the password).
C9	Web	Understand the HTML elements, HTTP and web socket communication protocols, and discover how read and inspect the exchanged messages (e.g., by using the browser developer tools).
C10	Forensics	Use tools that support regex expressions to search in files (e.g., grep), analyzing their content to understand some functionalities of the system and possibly vulnerabilities (e.g., by analyzing the errors log).
C11	Forensics, web	Understand and exploit vulnerabilities related to the storage of files in endpoints, retrieving them to perform forensics analysis to find information to perform message replay attacks in order to control an IoT device.
C12	Web, linux, cryptography	Understand and exploit directory traversal vulnerabilities to get access to system files, and use tools to crack hashed passwords.

by a home automation system that may also include home assistant interfaces capable of recognizing voice commands, providing enhanced user experience and automation features. However, connecting heterogeneous devices (different sellers and protocols) can increase the networks' susceptibility to cyberattacks. For instance, gaining access to one vulnerable device in a home network can compromise the other devices and the whole home automation system.

In the CTF, an ESP8266 development board embedded with some sensors was used as the IoT device. It was loaded with a program mimicking a smart device connecting to the WiFi network to send telemetry data from its sensors. Besides that, this IoT node is part of a smart home control system that uses the Message Queuing Telemetry Transport (MQTT) communication protocol to interconnect the different nodes. Fig. 2 illustrates the structure of the components of this smart home control system.

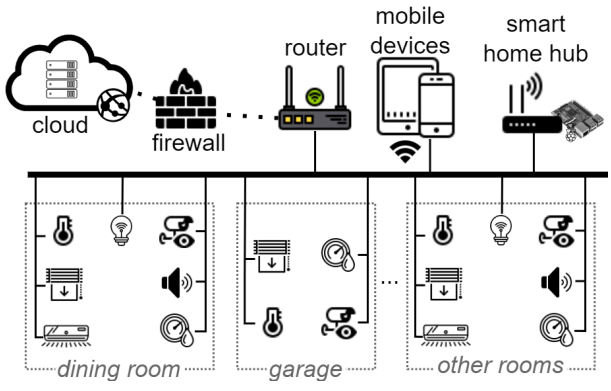


Fig. 2. Smart home IoT control system and network architecture.

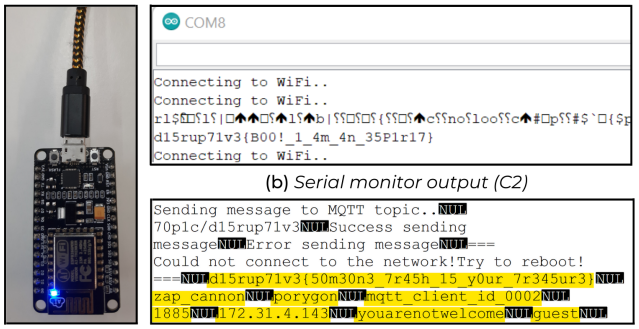
Each CTF challenge has specific learning goals as summarized in Table I. They are organized into three groups, according to their primary task, as described in the following:

- extract the credentials of the house WiFi and the home automation system network from the flash memory of the IoT device to access them (Section III-B);
- connect to the home automation system network, discover the IoT devices, and sniff their communication to control them (Section III-C);
- crack the login of the endpoint of the home control system to exploit its vulnerabilities and obtain root privileges (Section III-D).

B. Extract Information from the Physical IoT Device

This group comprises three challenges (C1, C2 and C3, see Table I), which the main objective is to develop the participants' general skills and abilities in search and identify the hardware components of the IoT device regarding the microcontroller and its physical communication interfaces. Additionally, these challenges aim to encourage the participants to search for and use tools and procedures to access and read the flash memory of the device, as well as interact with it through its physical communication interfaces. Fig. 3 illustrates the device used for the CTF (a), the information obtained when using a tool to monitor the output of its serial port (b), and the data recovered from its memory, highlighting the credentials of the WiFi and IoT network (c).

Although not a prerequisite, having experience in programming and developing IoT-based devices could help the participants solve these challenges faster, otherwise, an additional effort will be required to discover the related aspects. On the other hand, these challenges are facilitated by using a development board since the ESP8266 module has a lot of



(a) *ESP8266 (C1)* (b) *Serial monitor output (C2)* (c) *Data recovery from ESP8266 flash memory (C3)*

Fig. 3. CTF IoT device and information discovered in the first challenges.

easily accessible documentation and a built-in micro-USB port for communication. Note that some commercial IoT devices could be used to make this exercise even more challenging. For instance, since such devices leave some Input/Output pins for access and programming of the microcontroller, the participants would need to identify the correct pins in the circuit board and use specific electronic components and modules that would need to be wired. This would also require some electronic skills from the participants.

These challenges show the need for multidisciplinary teams to develop, maintain and hack IoT-based devices. They also warn about scenarios in which if somebody has access to a physical device, the use of passwords and other security policies can become meaningless. This illustrates that IoT devices must be properly disposed of from an end-user perspective.

C. Infiltrate the Home IoT Network and Control the Devices

This group comprises five challenges (C4, C5, C6, C7 and C11, see Table I) that aim to develop the participants' skills in general aspects of IoT-based applications, especially regarding the message protocols used by such devices.

The CTF smart home scenario was implemented using the MQTT message protocol, i.e., the IoT devices use this protocol to communicate with each other and the home control system. The MQTT comprises a publish-subscribe message protocol where a central node is responsible for managing a topic-based message structure and broker the connected clients. Each client can publish and subscribe to a set of message topics. All the messages published to a given topic are forwarded to the clients that subscribed to that topic.

Although the MQTT was used, other IoT-based protocols could also be used. Each of them has its features and capabilities, thus requiring specific skills for developing such applications and consequently hacking them.

Regardless of the specific aspects of implementation, these challenges require the participants to understand and develop skills on how the devices exchange messages and the related encoding protocols. They also illustrate that message content can be easily interpreted when sent as plain text, consequently enabling cyberattacks like man-in-the-middle, data tampering and eavesdropping. This is a reality for many IoT devices since they do not have enough computing resources to implement cryptography algorithms, but also, in some cases, they do not work with sensitive data that require encryption. In other cases, although the message is encoded, they are not hidden, for instance, files and images are usually sent encoded in Base64 that can be easily decoded since this algorithm is not meant to provide security.

It also illustrates that using cryptography algorithms makes messages practically impossible to decode without knowledge about the algorithms and keys used. On the other hand, even without knowing precisely the message's content but its context, the message can be resent, and if the system has related vulnerabilities, it can interpret it as a valid message. This approach is commonly used in message replay attacks that are also explored in these challenges. This challenge aims to provide an example for the IoT developers about the importance of considering approaches to validate the integrity of received messages, even if they are encrypted. For instance, send in the message content a timestamp that can be used to validate its lifespan.

D. Hack into the Home Control System and Get Full Access

This group comprises four challenges (C8, C9, C10 and C12, see Table I) that aim to develop the participants' skills in exploiting some basic Web applications vulnerabilities. In this CTF is considered the assumption that some of the IoT smart home control systems are designed to be deployed in constrained devices, called smart home hubs that may not receive updates, thus being susceptible to several vulnerabilities.

In this context, some vulnerabilities were exploited regarding default user ids, weak user passwords and a lack of mechanisms to prevent brute force login attempts. These challenges require the participants to understand and use tools that can assist in these tasks but also illustrate the importance of avoiding weak passwords and adopting different policies and mechanisms to force the end-users to change the default passwords and use more sophisticated ones, as well as mechanisms to prevent such kinds of attacks when developing these kinds of Web applications.

Another vulnerability explored in these challenges regards the access to system files, especially logs that may keep registered errors or messages. Such information can expose the system vulnerabilities or functionalities that intruders can exploit to design and perform attacks. These files and logs can be accessed through interfaces designed for debugging, and they should be disabled or hidden from system users or by mechanisms that prevent, e.g., directory traversal. This one is a severe vulnerability that can give access to unauthorized users of system files that may contain user credentials.

Regarding that, although the users' credentials are hashed in most cases, several tools can be used to break the hash code offline. In this context, these challenges require the participants to explore approaches and tools to retrieve these files and crack the hashed passwords. At the same time, they illustrate the importance of adopting good practices while developing such

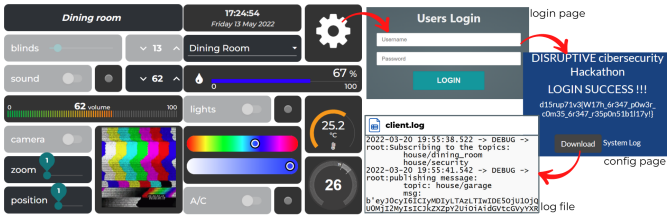


Fig. 4. The smart home dashboard (monitoring, user login and configuration pages) and the system log file.

Web applications as well as provide mechanisms to keep them up-to-date.

Fig. 4 illustrates the main user interfaces of the smart home dashboard developed for the CTF. The monitoring interface intends to help the participants to discover the existing devices and their message topics. The devices cannot be controlled, instead the participants need to access the configuration page that requires them to login. After cracking the password, the participants can download the system log file and retrieve other system files.

IV. CTF Implementation and Discussion

This CTF was designed to allow the participants to develop their cybersecurity skills, especially considering IoT-based applications. Although the challenges require hacking systems and devices, the knowledge acquired can be used to make them more secure. The participants were encouraged to engage as teams to stimulate knowledge exchange and brainstorm to solve the challenges. Two editions were held in 2022, in March at the University of Salamanca (Spain) and in May at the Polytechnic Institute of Bragança (Portugal), totalling 27 participants organized in 9 teams. The dissemination of the events was carried out through email and social media of the partners of the DISRUPTIVE project.

In order to manage the CTF's teams and challenges, an instance of the open-source CTFd platform (ctfd.io) was configured and deployed locally. The challenges were implemented with widely used IoT-based technologies (e.g. Node-RED) and deployed in individual dockerized containers for the teams in a virtual machine. The CTFd platform also provides several tools for monitoring the solution of the challenges that can be used to evaluate the participants' performance and, consequently, the difficulty of the challenges.

A. Participants Assessment

The CTF had a total duration of 9 hours. In the quiz component, the participants had to answer ten multiple-choice questions on general IoT cybersecurity topics, allowing them to obtain some points, which could provide an advantage to them in the overall score or even be spent to unlock hints of the challenges of the second component, which included the 12 challenges presented in section III.

Table II illustrates the participants' performance in resolving the challenges. It shows the minimum, average and maximum elapsed time throughout the competition in which the teams

TABLE II
Evaluation of the participants performance in the challenges.

#	*elapsed time (min/avg/max)*	*solved by*	*attempts*	*hints*
C1	0:06:46 / 0:30:01 / 0:50:04	9/9	31	1 [1/9]
C2	0:19:08 / 1:13:29 / 3:07:06	9/9	12	1 [1/9]
C3	0:38:58 / 2:08:30 / 3:35:09	9/9	13	2 [2/9]
C4	0:58:25 / 4:03:07 / 7:30:53	9/9	14	0 [0/9]
C5	1:41:21 / 4:29:56 / 7:28:45	6/9	15	3 [2/9]
C6	2:04:15 / 5:13:08 / 8:07:08	4/9	14	6 [3/9]
C7	4:31:31 / 5:36:35 / 7:26:09	4/9	12	4 [3/9]
C8	4:16:26 / 4:57:35 / 5:38:45	2/9	2	0 [0/9]
C9	2:14:31 / 2:59:17 / 3:44:03	2/9	2	0 [0/9]
C10	7:26:11	1/9	1	2 [1/9]
C11	–	0/9	5	5 [2/9]
C12	5:59:22	1/9	2	3 [1/9]

were able to complete each of the challenges. The observed elapsed times reflect that some challenges are only unlocked after submitting the right solution to others, according to the storyline (Fig. 1). The table also shows how many teams solved the challenges and the total number of attempts, i.e., how many answers were submitted to the CTFd system.

Note that challenges C1, C2, C3, and C4 were completed by all teams, with challenges C5, C6, and C7 having a reasonable success rate, being all the mentioned challenges related to basic hardware and IoT concepts. The remaining challenges, mostly related to Web application vulnerabilities, had a low rate of completeness, indicating a higher difficulty by the participants, who may lack experience in this topic and have a short amount of time left to spend on these challenges.

Another noticeable factor is that despite the difficulty found by the participants in solving some challenges, only a few hints were used by them. Table II shows the total number of hints used (each challenge has about three hints) and the number of hints used per team. This can be interpreted as the teams being afraid to spend points to get information that could help solve the challenge. In the next CTFs, some strategies can be adopted to incentive the use of hints, e.g., reduce their cost.

Overall, the learning outcomes of this CTF were a better understanding of the inherent vulnerabilities related to:

- IoT hardware devices (e.g., physical interfaces, memory);
- Communication protocols used by IoT applications;
- Smart home hub Web applications.

B. Participants Feedback

Fig. 5 presents a summary of the feedback given by the attendees in the CTF evaluation survey. A Likert scale is used to assess the level of agreement in different learning outcomes.

About 48% and 52% of the participants reported having poor or no backgrounds in IoT and cybersecurity, respectively. After participating in the competition, about 96% of them reported having fairly or significantly achieved the learning outcomes. The competition had a remarkable impact on the attendees, as 88% said to have found the field of IoT cybersecurity exciting, with 96% being extremely satisfied with participating. The utilization of challenges that involved real cybersecurity problems, supported by the narrative of hacking

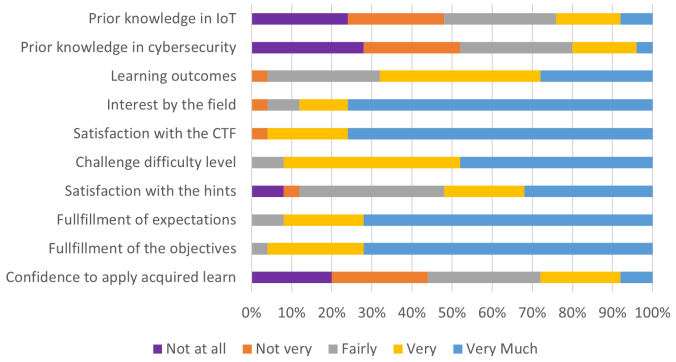


Fig. 5. Assessments of the participants' feedback.

the smart home system, were factors that contributed positively to the enjoyment and immersion of the participants in the CTF, also being helpful in the learning process.

While 92% of the participants consider the difficulty of the challenges proposed appropriate for the competition, they consider that they would have a better performance if the competition had a longer duration, and if the hints had provided more relevant information for solving the challenges, something also evidenced by the 52% satisfaction rate with the hints. 92% of the participants had their expectations with the competition met, with 96% considering that the proposed objectives were accomplished. Even in the short time of the competition, 28% of the participants felt more confident in applying the knowledge obtained in IoT cybersecurity to develop small applications. Regarding the development of future editions of the CTF, 84% of the participants reported being very interested in participating in a new edition of the competition with new and more advanced challenges.

V. Conclusions and Future Work

The fast adoption of IoT applications in our houses, farms, and industries has evinced the benefits of these technologies. However, training and qualifying students and professionals to develop and keep these applications secure from cyberattacks are crucial to ensure that these applications can continue to evolve. This paper discussed the design and implementation of a learning strategy based on a CTF that covers cybersecurity in IoT, addressing the lack of educational approaches related to these topics.

The CTF allowed the participants to develop their skills related to cybersecurity and IoT, driven by the competitive and immersive environment based on real cybersecurity problems. Moreover, this hands-on and gamification strategy improved the students' engagement compared to traditional approaches, as observed from their feedback and learning outcomes. Future work will be devoted to developing new CTF editions covering cybersecurity in IoT issues.

Acknowledgments

This work has been supported by the European Regional Development Fund (ERDF) through the Interreg Spain-Portugal V-A Program (POCTEP) under grant 0677_DISRUPTIVE_2_E (Intensifying the activity of Digital Innovation Hubs within the PocTep region to boost the development of disruptive and last generation ICTs through cross-border cooperation). This work has also been supported by FCT – Fundação para a Ciência e Tecnologia within the Project Scope UIDB/05757/2020.

References

[1] L. Babun, K. Denney, Z. B. Celik, P. McDaniel, and A. S. Uluagac, "A survey on IoT platforms: Communication, security, and privacy perspectives," *Computer Networks*, vol. 192, p. 108040, 2021.

[2] Y. Lu and L. D. Xu, "Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2103–2115, 2019.

[3] I. Lee, "Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management," *Future Internet*, vol. 12, no. 9, 2020.

[4] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and Security: Challenges and Solutions," *Applied Sciences*, vol. 10, no. 12, 2020.

[5] N. Ahmad, P. Laplante, J. Defranco, and M. H. Kassab, "A cybersecurity educated community," *IEEE Transactions on Emerging Topics in Computing*, pp. 1–1, 2021.

[6] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, "Cybersecurity awareness in the context of the industrial internet of things: A systematic literature review," *Computers in Industry*, vol. 137, p. 103614, 2022.

[7] M. Bashir, C. Wee, N. Memon, and B. Guo, "Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool," *Computers & Security*, vol. 65, pp. 153–165, 2017.

[8] W. E. Forum, "Global Cybersecurity Outlook 2022: Insight Report," https://www.weforum.org/reports/global-cybersecurity-outlook-2022, January 2022.

[9] ISACA, "State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources and Cyberoperations," https://www.isaca.org/go/state-of-cybersecurity-2022, January 2022.

[10] B. J. Blažič, "The cybersecurity labour shortage in europe: Moving to a new concept for education and training," *Technology in Society*, vol. 67, p. 101769, 2021.

[11] M. A. Khan, A. Merabet, S. Alkaabi, and H. E. Sayed, "Game-based learning platform to enhance cybersecurity education," *Education and Information Technologies*, jan 2022.

[12] T. Chothia and J. de Ruiter, "Learning from Others' mistakes: Penetration testing IoT devices in the classroom," in *2016 USENIX Workshop on Advances in Security Education (ASE 16)*. Austin, TX: USENIX Association, Aug. 2016.

[13] Z. Trabelsi, "Iot based smart home security education using a hands-on approach," in *2021 IEEE Global Engineering Education Conference (EDUCON)*, 2021, pp. 294–301.

[14] M. M. Yamin, B. Katt, E. Torseth, V. Gkioulos, and S. J. Kowalski, "Make it and break it: An iot smart home testbed case study," in *Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control*, ser. ISCSIC '18. NY, USA: ACM, 2018.

[15] A.-A. O. Affia, A. Nolte, and R. Matulevičius, "Integrating hackathons into an online cybersecurity course," *Creative Commons Attribution 4.0 International*, 2022.

[16] P. Legg, T. Higgs, P. Spruhan, J. White, and I. Johnson, ""Hacking an IoT Home": New opportunities for cyber security education combining remote learning with cyber-physical systems," in *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 2021, pp. 1–4.

[17] S. Kucek and M. Leitner, "An empirical survey of functions and configurations of open-source capture the flag (ctf) environments," *Journal of Network and Computer Applications*, vol. 151, p. 102470, 2020.

[18] K. Leune and S. J. Petrilli, "Using capture-the-flag to enhance the effectiveness of cybersecurity education," in *Proc. of the 18th Annual Conference on Information Technology Education*, ser. SIGITE '17. New York, NY, USA: ACM, 2017, p. 47–52.

[19] V. Švábenský, J. Vykopal, M. Cermak, and M. Laštovička, "Enhancing cybersecurity skills by creating serious games," ser. ITiCSE 2018. NY, USA: ACM, 2018, p. 194–199.