Teaching Hardware Security: Earnings of an Introduction proposed as an Escape Game

Florent Bruguier, Emmanuelle Lecointre, Béatrice Pradarelli, Loïc Dalmasso, Pascal Benoit, Lionel Torres

Teaching Hardware Security: Earnings of an Introduction proposed as an Escape Game

Florent Bruguier[1,2,3], Emmanuelle Lecointre[3] Beatrice Pradarelli[1,2], Loic Dalmasso[1,2], Pascal Benoit[1,2], and Lionel Torres[1,2]

[1] LIRMM, University of Montpellier, CNRS, 161 rue Ada, F-34095 Montpellier Cedex, France
[2] Pôle CNFM de Montpellier, University of Montpellier, 161 rue Ada, F-34095 Montpellier Cedex, France
[3] IUT de Nîmes, University of Montpellier, 8 Rue Jules Raimu, F-30907 Nîmes, France
first.last@lirmm.fr

Abstract. The Internet of Things (IoT) sees the appearance of ever more connected objects. In such a context, the security aspect of these objects is more relevant than ever. That's why we have developed several courses about hardware security. Traditional security courses often start with a catalog of definitions that can sometimes be boring for students and therefore counterproductive. This study describes an escape game used as a sequence to introduce several security concepts. This serious game could be adapted according to the degree level of the students. Results show a significant improvement in acquiring skills for the students who plays to the escape game. All the contents of this course are open sourced and could be freely available on request.

Keywords: Security, Data Security, Cryptography, Education, Hardware Security, Security Course, Serious Game, Escape Game.

1 Introduction

Nowadays, digital systems are everywhere. They are found in a wide range of applications, including communication systems, digital instruments, and consumer products. This is all the more true with the advent of the Internet of Things (IoT). They change users' habits and cater to the new needs of customers in various fields such as audio-visual, health, transport, and tourism ... By 2021, it is expected that there will be around 28 billion connected devices [1].

Nevertheless, this omnipresence increases the chances of user exposure to security issues. Smart fridge, smart cars, smart toys, or smart medical devices..., the number of hacked devices keeps going up [2] [3] [4]. Security breaches are easily exploitable since the users don't master technology and security aspects. For example, the use of personal information (birth date, place of residence...) as a password is still too common [5].

In this context, we have developed several courses about hardware security to educate students from high school to PhD degrees. All these courses rely on the SECNUM platform, a platform dedicated to hardware security evaluation [6]. This paper described a teaching sequence used as an introduction to different courses.

Since we address various audiences, we choose not to employ the purely transmissive method. Indeed, it keeps the audience in a passive posture and standardizes the pace of progress. Also, we hope that this sequence has a real impact on practices through an awareness of security risks. These 6 levers of the motivation described by Turner and Paris [7] are operated in the frame of the game and the simulation. It ensures commitment and the maintenance of attention needed for deep learning. Accordingly, we have chosen to experiment gamification methods to attract attention and maintain the commitment of target audiences.

This paper describes a teaching sequence allowing to introduce the key concepts of digital security. The main contribution consists of an escape game and the associated teaching materials which are open-sourced and freely available on request. The remainder of the paper is organized as follow. In section II, an overview of related works is offered. Then, principle, objectives and pedagogical issues of escape game courses are exposed. In the following section, our escape game is deeply described. Finally, outcomes are produced.

2 Related work and pedagogical issues

2.1 Related work

Several papers present different descriptions of hardware security courses.

First of all, Bossuet offers a description of two different labs about FPGA security [8]. These two labs are deeply depicted. The introduction course is done in the form of a 90 minutes lecture. In the same way, in [9], the authors present a full course dedicated to hardware security. The paper doesn't explain in details the way the course is done. More recently, Halak offers a full course on design and evaluation of secure chip [9]. This course seems to contain everything that must contain such a design course about hardware security. The students give good feedback. The same observation is done for [10]. The authors set forth a 3-day training course for PhD students. Once again, the theoretical contributions are done in a traditional way.

To sum up, all these contributions offer terminology and definition part on a classical way.

2.2 Pedagogical issues

We teach security since 2012 at different level from high school to PhD level in embedded systems / microelectronics. The table 1 offers evaluation of this course since 2015, year in which we have introduced the evaluation. With an average rating better than 4 out of 5, we could conclude the course has reached

the objective. Nevertheless, a redundant finding is often done by the students: the 3-hour sequence offered to expose terminology and cryptography principles asks for a lot of concentration efforts for the students. Indeed, their attention decreases significantly after 30 minutes if there is no change in their activity [11].

Table 1: PhD course rating on 5

PhD Course	2015	2016	2017	2018
Course structure	4.0	4.83	4.83	4.5
Content clarity	4.33	4.5	4.33	4.0
Used tools	4.33	4.33	4.33	4.5
Quality of materials	4.33	4.5	4.33	4.5
Instructor educational quality	4.33	4.5	4.67	4.67
Course understanding	4.5	4.5	4.5	4.67
Overall benefit of the course	4.33	4.33	4.83	4.67
Average	4.31	4.5	4.55	4.5

That's why we have decided to change this part of the course. We looked for a way to put the students in an active posture and we chose to experiment a new kind of serious game: the educational escape game [12].

3 Educational escape game

3.1 An educational vector

An escape game is a game in which a team must escape from a room in a given time. For this, it has to solve puzzles using hints hidden in the room. After beginning in the entertainment world, they are in full expansion in education world. The use of the game in class is part of what is called gamification, playfulness, or edutainment [13] [14]. As part of the latter, these are part of the category of serious games; the game becomes a learning tool.

The emotion and the positive stress generated lead the participant to the flow: a feeling of satisfaction and fullness in the realization of an activity for which all the attention is put on the task in progress [15]. All the ingredients of the video game are there to engage the participant via the storytelling or narrative frame in which they play the role of a hacker.

It's a simulated situation but with real challenges requiring periods of observation, choice and action to immediate feedback (stagnation / error-advancement / success). We aim for experiential learning through this device that allows a perceptual approach that is both abstract and concrete, and a knowledge integration that is based on both observation and action.

Thus, the sequence respects Kolb's theory of learning preferences based on constructivist theories [16]. It adapts to the different profiles and preferences of the participants since it is built in three stages. First, a phase of exchanges and

reflection in small groups or among peers on the practices of each one in terms of security. An active search for information on the basis of a questionnaire and information posters is also done. Then, the simulation of the game and finally the opportunity to reflect on the achievements during the debriefing on the experience lived: each enigma acting as a memory 'anchor' to ease the retrieval of the associated concepts of security.

Students are more receptive to the use of fun goals and to the concrete representations that are offered to them. The immersion and the pleasure of playing serve as a driving force for learning.

3.2 Importance of the scenario

Just like any teaching sequence, the scenario is essential to any escape game. It makes it possible to put the students pursue a quest or a challenge to solve in a limited and timed time.

To create the context for the development of new skills, the assimilation of new knowledge or the application of previously acquired knowledge, students will be offered to deal with riddles, puzzles or even experiences... The objective is to propose riddles as far as possible from classical exercises to ensure success. In the same way, the non-linearity scenario will allow the appearance of the collective intelligence [17]. Aside from the initial situation, the absence or almost absence of instructions is part of the format of an escape game. It is important not to limit students' imagination and reflection to the risk that the game will lose its interest.

3.3 Teacher posture

When designing an educational escape game, the teacher plays a leading role in planning and orchestrating the frame. Upstream, he organizes the playful experience to maximize the autonomy of the participants during the game. On the other hand, during the experience, he monitors the progress of the group and the time that elapses. He has also planned the possible dead ends in which the students could end up and has prepared 'boost' or 'help' elements for the groups strap up on a riddle.

The main difficulty will be to adapt the progress of each group to keep the sequence in the time allotted.

3.4 Debriefing

In order to ensure that students have fully integrated the concepts discussed during the game, it is important to focus on the debriefing sequence. This will allow students to put their finger on the skills and knowledge necessary to succeed but also to write them down. The teacher will take advantage of this to collect information for the improvement of the game.

4 Transposition to hardware security

4.1 Pedagogical goals

The objective is to offer a game allowing to develop the skills necessary to the understanding of the security of the digital world. The terminology and definition necessary to this course have to be introduced during this teaching sequence. First, it is needful to identify them:

- We first want to make students aware of social engineering. It is a question of carrying out a psychological manipulation in order to realize a swindle. For example, "a hacker will call up and imitate someone in a position of authority or relevance and gradually pull information out of the user" [18].
- Then, the concept of brute force attack has to be introduced. A brute force attack is the simplest method to find a secret key. It consists in testing all combinations of a secret key until the right one is found.
- The basic techniques of encryption / decryption must also be presented. We introduce the two most basic of them: : substitution and transposition ciphering. These two techniques are still used in modern cryptography algorithms. For example, the Advanced Encryption Standard, AES uses this kind of encryption schemes [19].
  A substitution cipher is a method of encryption. It consists in replacing a letter or a group of bits by another, according to a fixed system. For example, in Caesar cipher, an A is replaced by a D [20].
  Transposition-based encryption relies on inverting the position of letters in a message. One example of such a system is a Scytale, a tool consisting of a cylinder with a strip of leather wound around it. The leather is used to write the message and it is in theory impossible to retrieve it without the cylinder of good diameter [21].

Depending on the level of the students, other skills / knowledge will be involved:

- Students with little knowledge of the digital world and electronics will be confronted with the principles of operation of an electrical circuit and the principle of binary coding.
- More experienced students will have the opportunity to experiment with the joy of penetration testing [22]. The principle is to measure voltages directly on a digital circuit in order to extract sensitive information.
- Differential and correlative power analysis are also of interest. Such side-channel attacks allow deducing secret keys by analyzing power consumption from multiple cryptographic operations performed by a vulnerable device [23] [24].

4.2 Implementation

The proposed teaching sequence is divided into several stages. Unlike traditional escape game, our teaching sequence includes upstream and downstream phases

in addition to the real escape game phase. During the whole process, students are divided into groups of two or three. So that everyone can learn and experiment. The whole pedagogical material is duplicated for each group of students.

Upstream phase The upstream phase is divided into two stages.

First of all, an icebreaker is proposed. The students are asked to answer few quick questions. These questions about cryptography allow to facilitate exchanges towards learning in order to know each other better and to turn negative emotions into positive emotions.

Then, students are led to face different skills. For this, several posters describe the concepts exposed in subsection 4.1 and students have to explore them to answer multiple choice questions. This first contact with the notions to be learned allows activating the two first levels of Bloom's taxonomy: knowledge and comprehension [25].

Escape game phase The game phase will be broken down as follows.

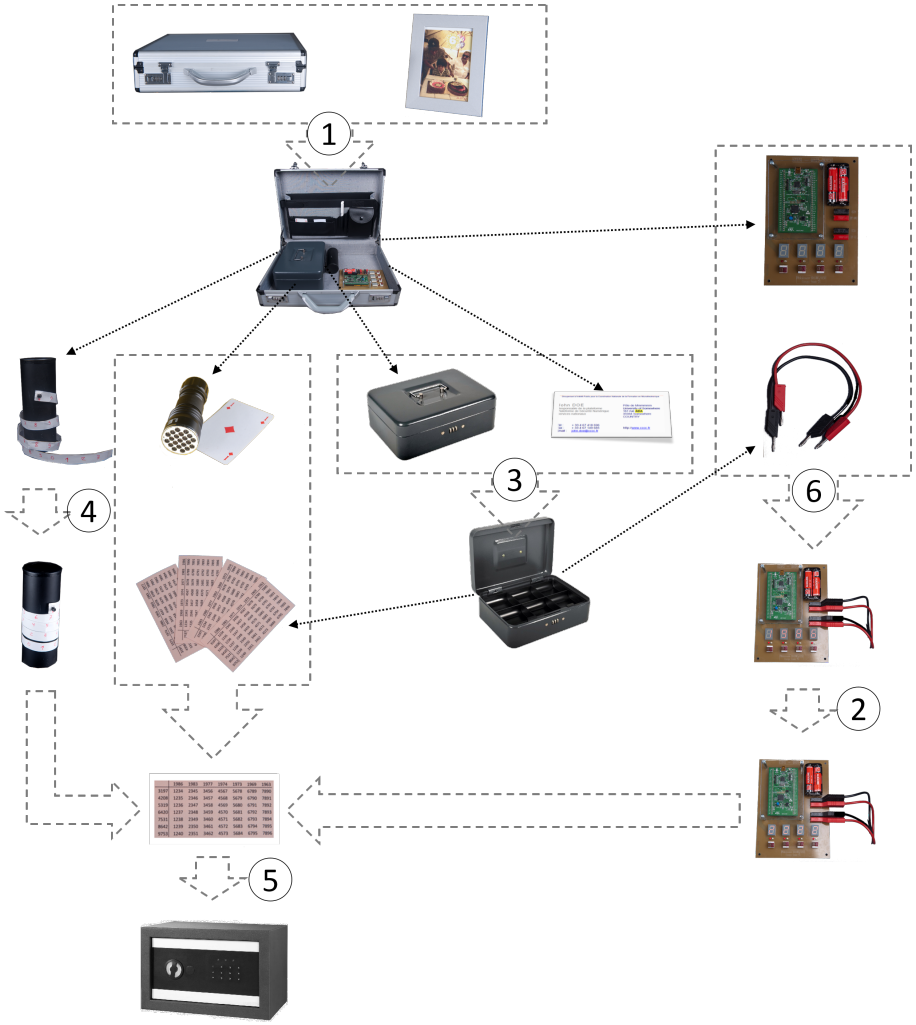
Principle First, the teacher explains the rules of the game. Then, students are divided into binomials or trinomials. Each group has several objects enabling to open a briefcase containing the code of a safe. More details will be given in the next paragraph. All the groups are in competition since there is only one safe to open. Once opened, depending on the time remaining, the other groups could continue to search the combination of the safe.

Gamification of knowledge Spoiler: If you want to confront the game without knowing all the tricks, please skip the following paragraph.

At the beginning, each team is in possession of one picture frame including a picture and a briefcase as depicted at the top of the Figure 1. Numbers in circles refer to the puzzle number shown in Table 2. The numbers are referred with a # for better comprehension.

As social engineering example, the birth date of the children on the photo is used as combination to open the briefcase (#1). Once opened, each group disposes of a "brute force" electronic card, a playing card, a "scytale" ribbon, a storage cylinder for an ultraviolet lamp, an ultraviolet lamp, a closed box, a business card, a notebook, and a pen. Using the substitution principle, each team could open the closed box using the business card address (#3). Two new objects are unlocked: two electric cables, four substitution tables. The cables power on the "brute force" card where the user has to test all the combinations to display another code (#6 and #2). The playing card and the ultraviolet lamp allow selecting one substitution table among the 4. The "scytale" ribbon and the storage cylinder illustrate the principle of transposition ciphering (#4). Finally, the codes deduced from the "brute force" electronic card and the "scytale" give the combination of the safe using the substitution card (#5). The safe is now opened.

Fig. 1: Logical path between the different puzzles of the escape game. The simplest version is depicted here.



Each skills / knowledge proposed above gives rise to an enigma proposed during the game as well as a possible associated boost that can be offered to students stuck during the game (Table 2).

In addition to the riddles above, extra puzzles are available and could be added to offer extra skills depending on the level of the students. Indeed, we propose to study two important skills of hardware security: penetration testing or *pentesting* and side-channel attacks. The first one could be introduced using a connected object which is disassembled to allow voltage measurement. The last

Table 2: Knowledge / skills and related puzzles

Puzzle number	Knowledge / skills	Puzzle	Boost / help
1	Social engineering	Using the date of birth found on the photo frame to open the briefcase	Presentation of the principle of social engineering
2	Brute force attack	Test all combinations to find the code used on the electronic board	Recall of the definition of brute force attack
3	Substitution encryption	Replacing letters of the address provide by the business card by their positions in the alphabet	Presentation of the code of Caesar
4	Transposition encryption	Winding a strip of paper around the ultraviolet lamp holder	Presentation of the principle of Scytale
5	Encryption using substitution boxes	Using the result from the electronic board and the transposition encryption as input of the substitution table	Principle of substitution boxes in the AES
6	Operation of an electronic device	Turning on the electronic board	Movie: "the seventh company" [26]
7	Binary coding	Using measured voltages on the connected object	Principle of voltage measurement
8	Pentesting	Voltage measurement on the connected object and conversion to decimal	Principle of penetration testing
9	DPA & CPA	Use of a specific application on Arduboy	Principle of the attack

one is presented with a short video game implemented on an Arduboy. These two elements could be easily added into the briefcase.

This phase of the sequence allows enhancing the skills of the students through application and analysis: the two-second levels of Bloom's taxonomy.

Downstream phase At the end of the game, the students have to fill an online multiple choice test. This test resumes all the different skills that were addressed during the game. This allows to settle them and to be sure they are mastered. The two last levels of Bloom's taxonomy are developed here. Moreover, at the end of the sequence, a correction of the multiple choice is offered and a discussion is proposed to be sure each student has correctly understand all notions.

4.3 Scenarisation

In order to guarantee maximum student involvement during the phase of the game, a simple scenario has been devised. The students were summoned to the first stage of recruitment as a new security expert of the National Security Agency of their country. For this test, they have to open a safe containing state secrets using all elements they find into the office of the boss of the agency. His office is almost empty except a briefcase and a photo of his son's birthday. By discovering the different enigmas presented in Table 2 as well as some additional challenges, the fastest student group will discover the combination of the safe and join the Agency.

5 Outcomes

5.1 Past courses

A preliminary version of this game met a great success during different courses given to students from high school to PhD students. The version proposed here was used during three different courses for students from high school and bachelor degree. We chose these three courses since they are followed by the students with the lowest level of study. If it works for them, it will for the other too and especially for the PhD ones. Even if it is too early to draw definite conclusions, the results are very positives.

5.2 Evaluation

In order to be able to properly evaluate what students have learned, we have chosen to make a double assessment. First, before the training sequence, we ask them if they know the different skills. Finally, after the downstream phase, we evaluate them a second time. The evaluation proposed here relates to three groups. Each one is composed of 15 students. Two groups are composed of students from high school and the other one is formed by students from bachelor level.

Figure 2 depicts the number of students confident with the different skills for the three groups. The Figure 3 shows the results of this evaluation. We can see that the progression is without appeal. Indeed, almost all students answer successfully to the evaluation. The few failures lie in the fact that students confuse substitution and transposition. This confusion shall be tackled in the next version of the upstream and downstream sessions thanks to a major focus on the differences between both concepts in the questionnaire.

Fig. 2: Number of students thinking of knowing the different skills for each group of 15 students

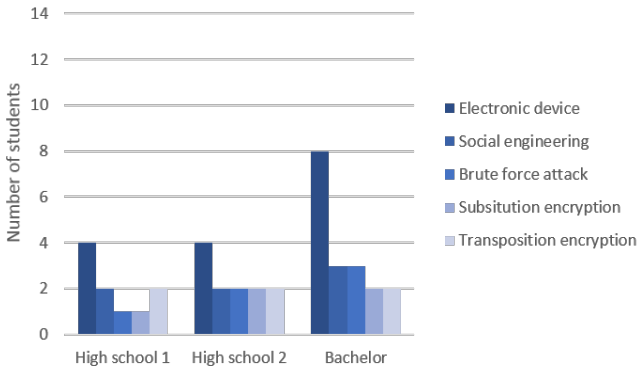
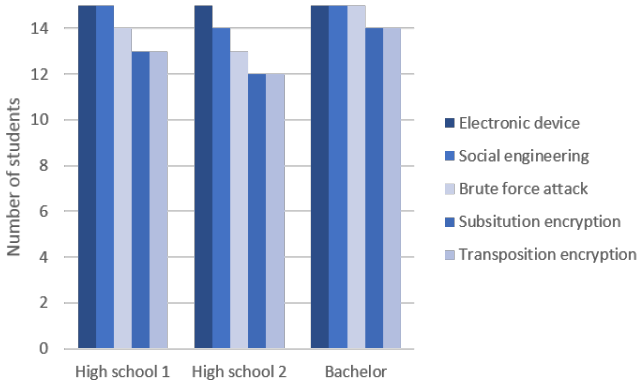


Fig. 3: Number of students having correctly answered for each skill



5.3 Feedback from the students

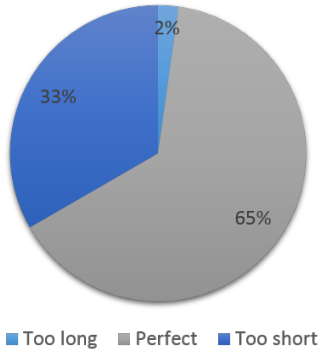
The table 3 depicts the average rating on different questions about the course. This sequence gave us very good student feedback. When students are asked if the escape game is a playful tool, they are unanimous and plebiscite of course the yes. The same answer is given when asked if the escape game is a good learning tool with a nuance. We still have work to convince all students of the opportunity to learn through play.

Table 3: Feedback from the students (rating on 5)

	High school 1	High school 2	Bachelor	Average
Is the escape game playful?	4.4	4.6	4.6	4.53
Is the escape game a learning tool?	3.8	4.33	4.6	4.04

Figures 4, 5, and 6 show other feelings of the students. The duration of the game is considered satisfactory even if some of them consider that the game is too short. The level of difficulty is also acceptable. Since the students are doing the game by groups of two or three, they were also ask is they are involved on all puzzle. The students are involved on almost all the puzzles. We are planning to tackle this in the next version of the game.

Fig. 4: How was the duration of the escape game phase?



6 Conclusion

This paper has exposed an introduction sequence for hardware cryptography courses. In order to increase the understanding and therefore the success of

Fig. 5: How was the difficulty of the escape game?

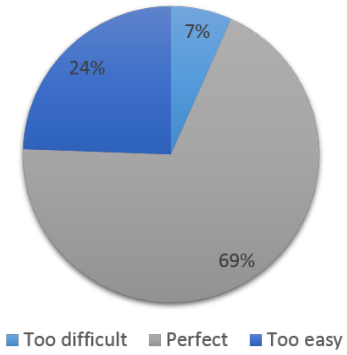
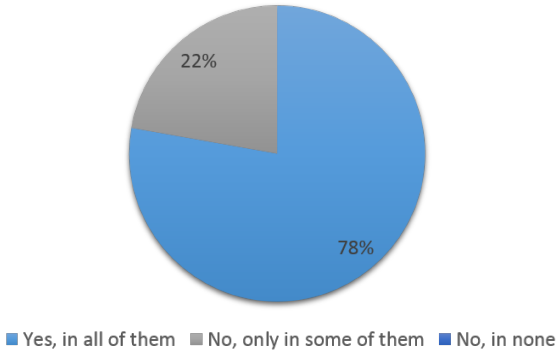


Fig. 6: Have you been involved in all the puzzles?



students, we offer an escape game. This serious game has the advantage to make the students actor of their apprenticeship. Therefore, naturally, it provides very good outcomes and will be integrated to all the hardware security courses we are given regardless of the students' level. Moreover, this course is open-sourced. Course materials could be sent on request.

7 Acknowledgment

The authors acknowledge the support of the French AgenceNationale de la Recherche (ANR), under grant ANR-11-IDFI-0017 (project IDEFI-FINMINA). They also acknowledge the Occitanie and the FEDER for they support to this project as well as the University of Montpellier and the I-site MUSE.

References

1. : Cellular networks for massive IoT. Technical report, Ericsson (01 2016)
2. Dagon, D., Martin, T., Starner, T.: Mobile phones as computing devices: The viruses are coming! IEEE Pervasive Computing **3**(4) (2004) 11–15
3. Wolf, M., Weimerskirch, A., Wollinger, T.: State of the art: Embedding security in vehicles. EURASIP Journal on Embedded Systems **2007**(1) (2007) 074706
4. Halperin, D., Heydt-Benjamin, T.S., Ransford, B., Clark, S.S., Defend, B., Morgan, W., Fu, K., Kohno, T., Maisel, W.H.: Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In: Security and Privacy, 2008. SP 2008. IEEE Symposium on, IEEE (2008) 129–142
5. Morris, R., Thompson, K.: Password security: A case history. Communications of the ACM **22**(11) (1979) 594–597
6. Bourrée, M., Bruguier, F., Barthe, L., Benoit, P., Maurine, P., Torres, L.: Secnum: an open characterizing platform for integrated circuits. In: European Workshop on Microelectronics Education. (2012)
7. Turner, J., Paris, S.G.: How literacy tasks influence children's motivation for literacy. The reading teacher **48**(8) (1995) 662–673
8. Bossuet, L.: Teaching fpga security. In: Field-Programmable Technology (FPT), 2013 International Conference on, IEEE (2013) 306–309
9. Halak, B.: Course on secure hardware design of silicon chips. IET Circuits, Devices & Systems **11**(4) (2017) 304–309
10. Bruguier, F., Benoit, P., Torres, L., Bossuet, L.: Hardware security: From concept to application. In: 2016 11th European Workshop on Microelectronics Education (EWME). (May 2016) 1–6
11. Mackworth, N.H.: The breakdown of vigilance during prolonged visual search. Quarterly Journal of Experimental Psychology **1**(1) (1948) 6–21
12. Annetta, L.A.: The "i's" have it: A framework for serious educational game design. Review of General Psychology **14**(2) (2010) 105
13. Deterding, S., Dixon, D., Khaled, R., Nacke, L.: From game design elements to gamefulness: defining gamification. In: Proceedings of the 15th international academic MindTrek conference: Envisioning future media environments, ACM (2011) 9–15
14. Deterding, S., Sicart, M., Nacke, L., O'Hara, K., Dixon, D.: Gamification. using game-design elements in non-gaming contexts. In: CHI'11 extended abstracts on human factors in computing systems, ACM (2011) 2425–2428
15. Csikszentmihalyi, M.: Flow and the psychology of discovery and invention. Harper-Perennial, New York **39** (1997)
16. Kolb, D.A.: Experiential learning: Experience as the source of learning and development. FT press (2014)
17. Lévy, P., Bononno, R.: Collective intelligence: Mankind's emerging world in cyberspace. Perseus books (1997)
18. Granger, S.: Social engineering fundamentals, part i: hacker tactics. Security Focus, December **18** (2001)
19. Daemen, J., Rijmen, V.: The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media (2013)
20. Goyal, K., Kinger, S.: Modified caesar cipher for better security enhancement. International Journal of Computer Applications **73**(3) (2013)
21. Kelly, T.: The spartan scytale. The Craft of the Ancient Historian: Essays' in honor of Chester G. Starr (1985) 141–169

22. Engebretson, P.: The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Elsevier (2013)
23. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Annual International Cryptology Conference, Springer (1999) 388–397
24. Brier, E., Clavier, C., Olivier, F.: Correlation power analysis with a leakage model. In: International workshop on cryptographic hardware and embedded systems, Springer (2004) 16–29
25. Bloom, B.: Bloom's taxonomy of educational objectives. Longman (1965)
26. : Mais où est donc passée la septième compagnie? (1973)