AMUSE : l'escape game pour s'évader en toute sécurité
Enseignement de la sécurité numérique sous forme d'un escape game

F. Bruguier[a,c], P. Benoit[b,c], L. Dalmasso[c], B. Pradarelli[b,c], E. Lecointre[a] et L. Torres[b,c]

[a] IUT de Nîmes et Pôle CNFM de Montpellier (PCM), Université de Montpellier, Montpellier, France

[b] Polytech Montpellier et Pôle CNFM de Montpellier (PCM), Université de Montpellier, Montpellier, France

[c]LIRMM, Université de Montpellier, CNRS, Montpellier, France

Contact email : florent.bruguier@umontpellier.fr

L'Internet des objets (IoT) voit l'apparition d'objets de plus en plus connectés. Dans un tel contexte, l'aspect sécurité de ces objets est plus important que jamais. C'est pourquoi nous avons développé plusieurs cours sur la sécurité matérielle. Les cours de sécurité traditionnels commencent souvent par un catalogue de définitions qui peuvent parfois être ennuyeuses pour les étudiants et donc contre-productives. Cette étude décrit un « *escape game* » utilisé comme séquence pour introduire plusieurs concepts de sécurité. Ce jeu sérieux pourrait être adapté au niveau de diplôme des étudiants.

Mots-clés : Sécurité, Enseignement, Cryptographie, Sécurité matérielle, Jeu sérieux, Gamification, *Escape Game*.

I. Introduction

De nos jours, nous utilisons de plus en plus de systèmes numériques. Ceci est d'autant plus vrai avec l'avènement de l'Internet des Objets (IoT). Ils modifient les habitudes des utilisateurs et répondent à des besoins nouveaux dans de nombreux domaines tels que l'audiovisuel, la santé, le tourisme ou encore les transports… Leur nombre est estimé aujourd'hui à 23 milliards et devrait être de plus de 75 milliards dans le monde en 2025 (1).

Néanmoins, cette omniprésence accroit les chances d'exposition des utilisateurs. Frigos, voitures, jouets ou dispositifs médicaux connectés…, les exemples d'objets ayant des failles ne cessent d'augmenter (2–4). Ces failles sont d'autant plus facilement exploitables que les utilisateurs des objets ne maitrisent pas les technologies et les rudiments de la sécurité numérique. Par exemple, l'utilisation d'informations personnelles (date de naissance, lieu de résidence…) pour sécuriser l'accès aux informations sensibles reste encore trop courant.

Dans ce contexte, le pôle CNFM de Montpellier a décidé de développer un programme de formation sur la sécurité numérique (5) autour de la plateforme SECNUM (6). Ce papier décrit une séquence de cours développée comme introduction aux différents cours. Il s'agit d'un jeu sérieux permettant d'introduire tous les concepts nécessaires à l'apprentissage de la sécurité numérique. Cette séquence est notamment développée dans le cadre du projet AMUSE : Academic Multi-Users Security game for Education, projet financé par l'I-site MUSE.

Puisque nous nous adressons à différents publics, nous avons choisi de ne pas utiliser la méthode purement transmissive lors de cette séquence. En effet, elle maintient le public dans une posture passive et normalise le rythme de progrès. Nous espérons également que cette séquence aura un impact réel sur les pratiques en prenant conscience des risques de sécurité. Les 6 leviers de la motivation décrits par Turner et Paris (7) sont exploités dans le cadre du jeu

Article publié par EDP Sciences et disponible sur le site https://www.j3ea.org ou https://doi.org/10.1051/j3ea/20191017

et de la simulation. Cela garantit l'engagement et le maintien de l'attention nécessaire à l'apprentissage en profondeur. En conséquence, nous avons choisi d'expérimenter des méthodes de gamification afin d'attirer l'attention et de maintenir l'engagement des publics cibles.

Cet article décrit une séquence d'enseignement permettant d'introduire les concepts clés de la sécurité numérique. La contribution principale consiste en un jeu d'évasion et le matériel pédagogique associé. Le reste du document est organisé comme suit. Dans la section II, un aperçu des travaux connexes est proposé. Ensuite, les principes, les objectifs et les problèmes pédagogiques du parcours de jeu d'évasion sont exposés. Dans la section suivante, notre jeu d'évasion est décrit en détail. Enfin, les résultats sont proposés.

II. Travaux connexes et questions pédagogiques

1. Travaux connexes

Plusieurs articles présentent des descriptions de cours sur la sécurité du matériel. Lilian Bossuet propose tout d'abord une description de deux travaux pratiques sur la sécurité des FPGA (8). Ceux-ci sont présentés en détails. Le cours d'introduction se déroule sous la forme d'une conférence de 90 minutes. De même, dans (9), les auteurs présentent un cours complet dédié à la sécurité matérielle. Le document n'explique pas en détail la façon dont le cours est fait. Plus récemment, Basel Halak propose un cours complet sur la conception et l'évaluation de la puce sécurisée (10). Ce cours semble contenir tout ce qui doit contenir un cours de conception sur la sécurité du matériel. Les étudiants font de bons commentaires. La même observation est faite pour (11). Les auteurs ont proposé une formation de trois jours aux doctorants. Encore une fois, les apports théoriques se font de manière traditionnelle.

2. Questions pédagogiques

Nous enseignons la sécurité depuis 2012 à différents niveaux du lycée au doctorat dans des cours de systèmes embarqués ou de microélectronique. Le tableau 1 présente l'évaluation de ce cours depuis 2015, année au cours de laquelle nous avons introduit l'évaluation. Avec une note moyenne supérieure à 4, nous pourrions conclure que le cours a atteint l'objectif. Néanmoins, les étudiants effectuent souvent une remarque redondante : la séquence initiale de trois heures proposée pour exposer les principes de terminologie et de cryptographie leurs demande beaucoup d'efforts de concentration. En effet, leur attention diminue significativement après 30 minutes s'il n'y a pas de changement dans le rythme du cours (12).

C'est pourquoi nous avons décidé de changer cette partie du cours. Nous avons cherché un moyen de mettre les élèves dans une posture active et nous avons choisi d'expérimenter un jeu sérieux : un « *escape game* » éducatif (13).

TABLEAU I: Retours sur les cours donnés aux doctorants (notes sur 5)

	Doctorants 2015	**Doctorants 2016**	**Doctorants 2017**	**Doctorants 2018**
Organisation du cours	4.0	4.83	4.83	4.5
Clarté du contenu	4.33	4.5	4.33	4.0
Qualité des outils utilisés	4.33	4.33	4.33	4.5
Qualité de la présentation	4.33	4.5	4.33	4.5
Qualité pédagogique de l'enseignant	4.33	4.5	4.67	4.67
Compréhension du cours	4.5	4.5	4.5	4.67
Bénéfice global du cours	4.33	4.33	4.83	4.67
Moyenne	4.31	4.5	4.55	4.5

III. L'escape game ?

1. Un vecteur de pédagogie

Un *escape game*[1] est un jeu dans lequel une équipe doit s'échapper d'une pièce en un temps impartit. Pour cela, il lui faudra résoudre des énigmes à l'aide d'indices cachés dans la pièce. Après avoir conquis les loisirs des français, ceux-ci sont en pleine expansion dans l'enseignement. L'utilisation du jeu en classe fait partie de ce que l'on appelle ludification, ou ludicisation, ou gamification (14). Dans le cadre de ce dernier, ceux-ci font partie de la catégorie des *serious games*[2]. Ils permettent de faciliter l'apprentissage en utilisation la pédagogie active. En effet, les étudiants se sont plus réceptifs à l'utilisation d'objectifs ludiques mais aussi grâce aux interactions entre élèves ou encore les représentations concrètes qui leurs sont offertes. L'immersion et le plaisir de jouer servent de moteur à l'apprentissage.

L'émotion et le stress positif générés conduisent le participant au flux : un sentiment de satisfaction et de plénitude dans la réalisation d'une activité pour laquelle toute l'attention est portée sur la tâche en cours (15). Tous les ingrédients du jeu vidéo sont réunis pour engager le participant via le cadre de narration ou de récit dans lequel il joue le rôle d'un hacker. C'est une situation simulée mais avec de réels défis qui nécessitent des périodes d'observation, de choix et d'action pour un retour immédiat (stagnation / progression des erreurs / succès). Nous visons l'apprentissage par l'expérience à travers ce dispositif qui permet une approche perceptuelle à la fois abstraite et concrète et une intégration des connaissances basées à la fois sur l'observation et l'action.

Ainsi, la séquence respecte la théorie de Kolb des préférences d'apprentissage basée sur les théories constructivistes (16). Il s'adapte aux différents profils et préférences des participants puisqu'il se construit en trois étapes. Tout d'abord, une phase d'échanges et de réflexion en petits groupes ou entre pairs sur les pratiques de chacun en matière de sécurité. Une recherche active d'informations sur la base d'un questionnaire et de posters est également effectuée. Ensuite, chaque groupe est confronté à « l'*escape game* » avant d'avoir la possibilité de réfléchir aux réalisations lors d'un debriefing sur l'expérience vécue avec pour «ancrage» de réflexion les énigmes à associer aux concepts de sécurité acquis.

Les élèves sont plus réceptifs à l'utilisation d'objectifs amusants et aux représentations concrètes qui leur sont proposées. L'immersion et le plaisir de jouer servent de moteur à l'apprentissage.

2. L'importance du scénario

Au même titre que toute séquence d'enseignement, le scénario est essentiel à tout *escape game*. Il permet de mettre les étudiants face à une quête ou un défi à résoudre en un temps limité et chronométré.

Afin de faire apprendre de nouvelles compétences ou connaissances ou de mettre en application celles qu'ils ont déjà acquises, les étudiants devront faire face à des énigmes, des devinettes ou encore des expériences… L'objectif est de proposer des énigmes les plus éloignées possibles des exercices classiques afin d'en assurer le succès. De la même manière, la non linéarité de celles-ci permettra de laisser la part belle à l'apparition de l'intelligence collective (17).

Mis à part la mise en situation initiale, l'absence ou quasi absence de consignes fait partie du format d'un *escape game*. Il est important de ne pas limiter l'imagination et la réflexion des étudiants au risque que le jeu perde de son intérêt (18).

[1] Jeu d'évasion en français

[2] Jeux sérieux en français

3. Rôle de l'enseignant

Tout comme dans chaque séquence d'enseignement, lors d'un *escape game* pédagogique, l'enseignant joue un rôle prépondérant. En effet, celui-ci est le maitre du jeu. C'est lui qui surveillera l'avancement du groupe et le temps qui s'écoule mais aussi qui donnera un coup de pouce aux groupes bloqués sur une énigme (19). La principale mission consistera à adapter l'avancement de chaque groupe afin de faire tenir la séquence dans le temps impartit.

4. Debriefing

Afin de garantir que les étudiants aient bien intégré les notions abordées lors du jeu, il est important de mettre l'accent sur la séquence de débriefing. Celle-ci permettra aux étudiants de mettre le doigt sur les compétences et connaissances nécessaires pour réussir mais aussi de poser par écrit celle-ci. L'enseignant en profitera pour récupérer des informations pour l'amélioration du jeu.

IV. Transposition à la sécurité matérielle

1. Objectifs pédagogiques

L'objectif étant de proposer un jeu permettant d'appréhender des compétences nécessaires à la compréhension de la sécurité du monde numérique, il est d'abord nécessaire de les identifier :

- Nous souhaitons tout d'abord sensibiliser les étudiants au social engineering[3]. Il s'agit de réaliser une manipulation psychologique afin de réaliser une escroquerie (20).
- Ensuite, le concept d'attaque par force brute doit être introduit. Une attaque par force brute consiste à tester la totalité des combinaisons d'un algorithme de chiffrement pour retrouver la clé secrète utilisée.
- Les techniques de bases du chiffrement/déchiffrement doivent aussi être présentées. Le chiffrement par substitution est une technique de chiffrement. Il consiste à remplacer dans un message une lettre ou un groupement de bits par une autre définie à l'avance. Par exemple, dans le chiffre de César, un A sera remplacé par un D (21). Le chiffrement par transposition repose sur l'inversion de la position de lettres dans un message. Un exemple de ce système de chiffrement est la Scytale utilisée par les grecs pour chiffrer des messages. A l'époque, un bandeau de cuir était enroulé autour d'un cylindre de bois avant d'y écrire un message dessus. Sans le bon diamètre, il n'était pas possible de déchiffrer le message à nouveau (22). Ces deux techniques sont associées dans la plupart des algorithmes de chiffrement modernes.
- Une autre manière de mettre en œuvre la substitution est l'utilisation de boites de substitution. Celles-ci seront également abordées.

En fonction du niveau des étudiants, d'autres compétences/connaissances seront mises en jeu :

- Les étudiants n'ayant que peu de connaissances du monde numérique et de l'électronique seront confrontés aux principes de fonctionnement d'un circuit électrique ainsi qu'au principe du codage binaire.
- Les étudiants plus expérimentés auront l'occasion de gouter aux joies du *pentesting*[4] (23). Le principe étant de venir mesurer des tensions directement sur un circuit numérique afin d'en extraire de l'information.
- Les méthodes d'analyses corrélatives et différentielles sont aussi abordées. Ces méthodes utilisées pour les attaques par canaux cachés permettent de retrouver la clé

[3] Ingénierie sociale en français

[4] Test de pénétration en français

de chiffrement d'un circuit cryptographique à partir de mesures de consommation (24-25).

2. Mise en œuvre

La séquence d'enseignement proposée est divisée en plusieurs étapes. Contrairement aux « *escape games* » traditionnels, notre séquence d'enseignement comprend des phases amont et aval en plus de la phase de jeu d'évasion réelle. Pendant tout le processus, les étudiants sont divisés en groupes de deux ou trois. Pour que tout le monde puisse apprendre et expérimenter, le matériel diffusé est dupliqué pour chaque groupe d'élèves.

Phase amont. La phase amont est divisée en deux étapes.

Tout d'abord, un brise-glace est proposé. Les étudiants sont invités à répondre à quelques questions rapides. Ces questions sur la cryptographie permettent de faciliter les échanges d'apprentissage pour créer une émulation dans chaque groupe et transformer les émotions négatives en émotions positives.

Ensuite, les étudiants sont amenés à faire face à des compétences différentes. Pour cela, plusieurs posters décrivent les concepts exposés dans la sous-section 4.1 et les étudiants doivent les consulter pour répondre à des questions à choix multiples. Ce premier contact avec les notions à apprendre permet d'activer les deux premiers niveaux de la taxonomie de Bloom : la connaissance et la compréhension (26).

Phase de jeu.

Principe. Tout d'abord, l'enseignant explique les règles du jeu. Ensuite, les étudiants sont divisés en binômes ou en trinômes. Chaque groupe dispose de plusieurs objets permettant d'ouvrir un porte-document contenant le code d'un coffre-fort. Plus de détails seront donnés dans le paragraphe suivant. Tous les groupes sont en concurrence puisqu'il n'y a qu'un seul coffre-fort à ouvrir. Une fois ouvert, les autres groupes peuvent continuer à rechercher le code du coffre-fort, en fonction du temps restant pour cette séquence.

Gamification de la connaissance. Spoiler : Si vous voulez affronter le jeu sans connaître toutes les astuces, veuillez sauter le paragraphe suivant.

Au début, chaque équipe est en possession d'un cadre photo comprenant une photo et une mallette, comme illustré en haut de la Figure 1. Les chiffres entourés d'un cercle désignent le numéro de l'énigme explicitée dans la Table 2. Comme exemple d'ingénierie sociale, la date de naissance des enfants sur la photo est utilisée comme code pour ouvrir le porte-document. Une fois la mallette ouverte, chaque groupe dispose d'une carte électronique « force brute », d'une carte à jouer, d'un ruban «Scytale», d'un cylindre de stockage pour la lampe à ultraviolets, d'une lampe à ultraviolets, d'une boîte fermée, d'une carte de visite, d'un cahier et d'un stylo. En utilisant le principe de substitution, chaque équipe peut ouvrir la boîte fermée en se servant de l'adresse de la carte de visite. Deux nouveaux objets sont déverrouillés : deux câbles électriques et quatre tables de substitution. Les câbles alimentent la carte « force brute » sur laquelle l'utilisateur doit tester toutes les combinaisons pour afficher un autre code. La carte à jouer et la lampe à ultraviolets permettent de sélectionner une table de substitution parmi les 4.

Le ruban "Scytale" et le cylindre de stockage illustrent le principe du chiffrement par transposition. Enfin, les codes déduits de la carte électronique « force brute » et de la « Scytale » donnent le code du coffre-fort en utilisant la carte de substitution. Le coffre-fort est maintenant ouvert.

Chacune des compétences / connaissances proposées ci-dessus donne lieu à une énigme proposée au cours du jeu ainsi qu'à un éventuel « coup de pouce » qui peut être offert aux étudiants bloqués pendant le jeu (table 2).

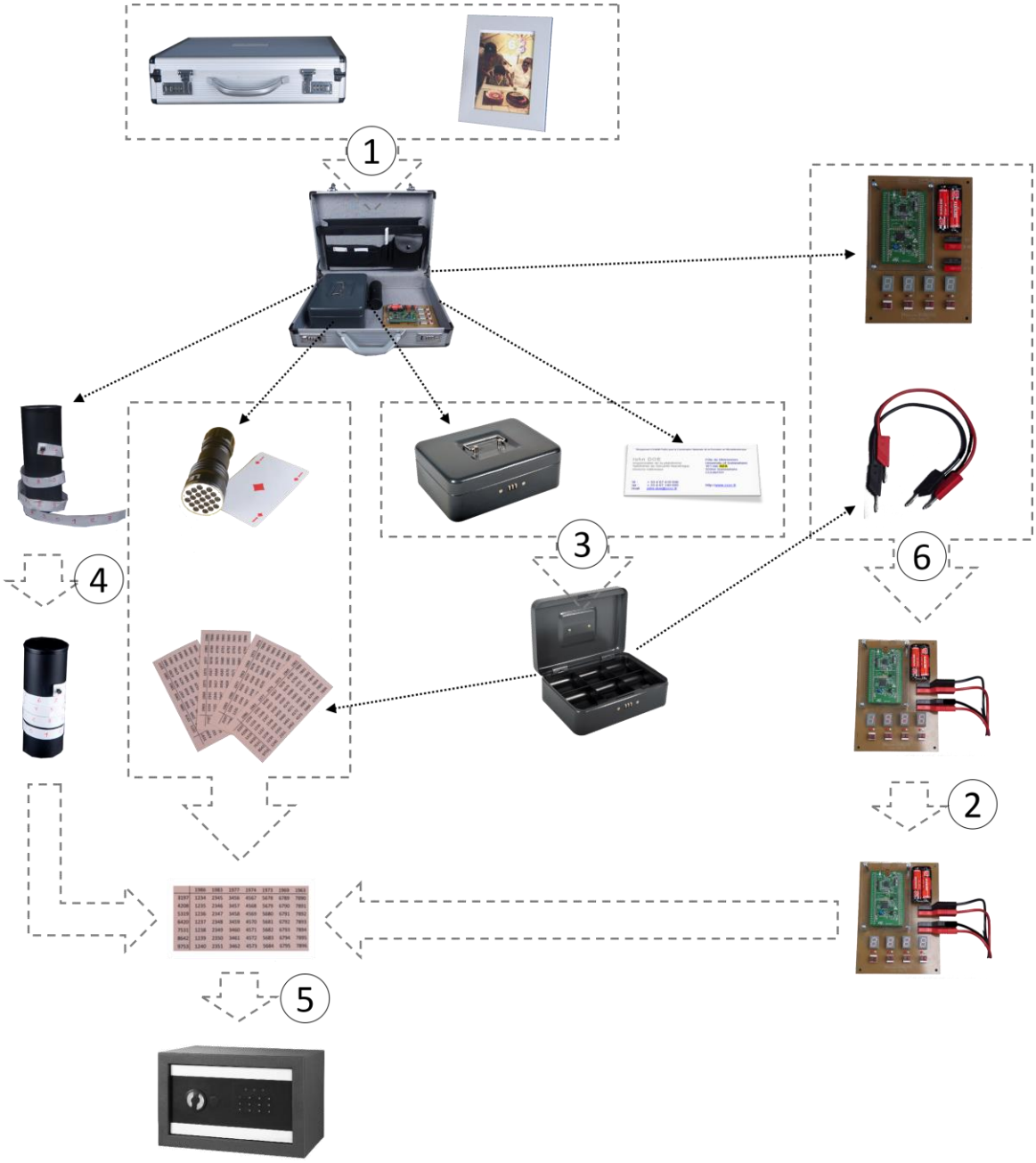

Figure 1: Enchainement logique des différentes énigmes de l'*escape game*. La version la plus simple est proposée dans cet exemple.

En plus des énigmes ci-dessus, des puzzles supplémentaires sont disponibles et peuvent être ajoutés pour offrir des compétences supplémentaires en fonction du niveau des élèves. En effet, nous proposons d'étudier deux compétences importantes de la sécurité matérielle : le test d'intrusion ou *pentesting* et les attaques par canaux cachés. Le premier pourrait être introduit en utilisant un objet connecté qui est démonté pour permettre la mesure de la tension. Le dernier est présenté avec un court jeu vidéo implémenté sur un Arduboy (27).

Cette phase de la séquence permet d'améliorer les compétences des étudiants grâce à l'application et à l'analyse : les troisième et quatrième phases de la taxonomie de Bloom.

Phase de débriefing. À la fin du jeu, les étudiants doivent remplir un questionnaire à choix multiples en ligne. Ce test reprend toutes les compétences qui ont été abordées au cours du jeu. Cela permet de fixer les connaissances et de vérifier qu'elles sont maîtrisées. Les deux derniers niveaux de la taxonomie de Bloom sont développés ici.

1. Scénarisation

Afin de garantir un maximum d'implication des étudiants lors de cette phase du jeu, un scénario simple a été imaginé. Les étudiants sont là pour la première étape de recrutement en tant que nouvel expert sécurité de l'Agence Nationale de Sécurité. Pour ce test, ils devront ouvrir un coffre-fort renfermant des secrets d'Etat. On va pour cela leur permettre de rentrer dans le bureau de Cyril Ainèfaime. Sur ce bureau, ils trouveront une mallette ainsi qu'un cadre photo ; photo présentant Cyril Ainèfaime lors de son dernier anniversaire.

En découvrant les différentes énigmes présentées dans la Table II ainsi que quelques défis complémentaires, le groupe d'étudiant le plus rapide découvrira la combinaison du coffre-fort.

V. Bilan

1. Sessions précédentes

Une version préliminaire de ce jeu a rencontré un vif succès lors de différents cours donnés aux étudiants du lycée au doctorat. La version proposée ici a été utilisée lors de deux cours différents pour les étudiants de lycée et de DUT. Même s'il est trop tôt pour tirer des conclusions définitives, les résultats sont très positifs.

TABLEAU II. Connaissances/compétences et énigmes associées.

Numéro d'énigme	Connaissances	Enigme	Coup de pouce
1	Social engineering	Utilisation de la date de naissance trouvée sur le cadre photo pour ouvrir la mallette	Présentation du principe
2	Attaque par force brute	Test de toutes les combinaisons pour trouver le code utilisé sur la carte électronique	Définition de l'attaque par force brute
3	Chiffrement par substitution	Remplacement de lettres par leurs positions dans l'alphabet	Présentation du code de César
4	Chiffrement par transposition	Enroulement d'une bande de papier autour du support de la lampe ultraviolet	Présentation du principe de la Scytale
5	Chiffrement à l'aide de boites de substitution	Utilisation du résultat issu de la carte électronique et de la transposition à l'aide d'une table de substitution	Principe des boites de substitution dans l'AES
6	Fonctionnement d'un circuit électronique	Mise sous tension de la carte électronique	Film la septième compagnie (28)
7	Codage binaire	Utilisation des tensions mesurées sur l'objet connecté	Principe de mesure de tension
8	Pentesting	Mesure de tension sur l'objet connecté puis conversion en décimal	Principe du pentesting
9	DPA & CPA	Utilisation d'une application spécifique sur Arduboy	Principe des attaques

2. Evaluation

Pour pouvoir évaluer correctement ce que les élèves ont appris, nous avons choisi de faire une double évaluation. Tout d'abord, avant la séquence d'entraînement, nous leur demandons s'ils ont acquis les différentes connaissances de base. Enfin, après la séquence d'entraînement, nous les évaluons.

L'évaluation proposée ici concerne deux groupes. Chacun est composé de 15 étudiants. Ils ont le niveau « lycée » pour le premier et « DUT GEII » pour le second. La figure 2 illustre le

nombre d'élèves confiants dans leurs propres compétences au sein de chacun des deux groupes. À la fin du jeu, les élèves sont invités à répondre à plusieurs questions. Cette enquête évalue le niveau d'acquisition des différentes compétences. La figure 3 montre les résultats de cette évaluation. Nous pouvons voir que la progression est sans appel. En effet, presque tous les étudiants répondent avec succès à l'évaluation. Les quelques échecs sont dus au fait que les étudiants confondent substitution et transposition.

3. Retours des étudiants

Cette séquence nous a donné de très bons retours d'étudiants. Lorsqu'on demande aux élèves si le jeu d'évasion est un outil ludique, ils sont unanimes et plébiscitent bien évidemment le « oui ». La même réponse est donnée lorsqu'on leur demande si le jeu d'évasion est un bon outil d'apprentissage.

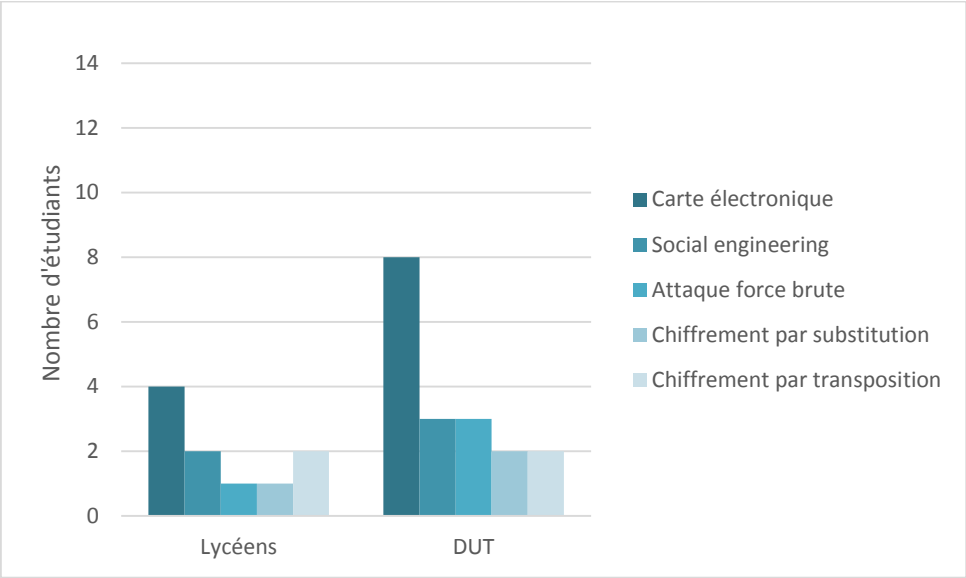

Figure 2: Nombre d'étudiants pensant connaitre les différentes connaissances avant la formation pour chaque groupe de 15 étudiants

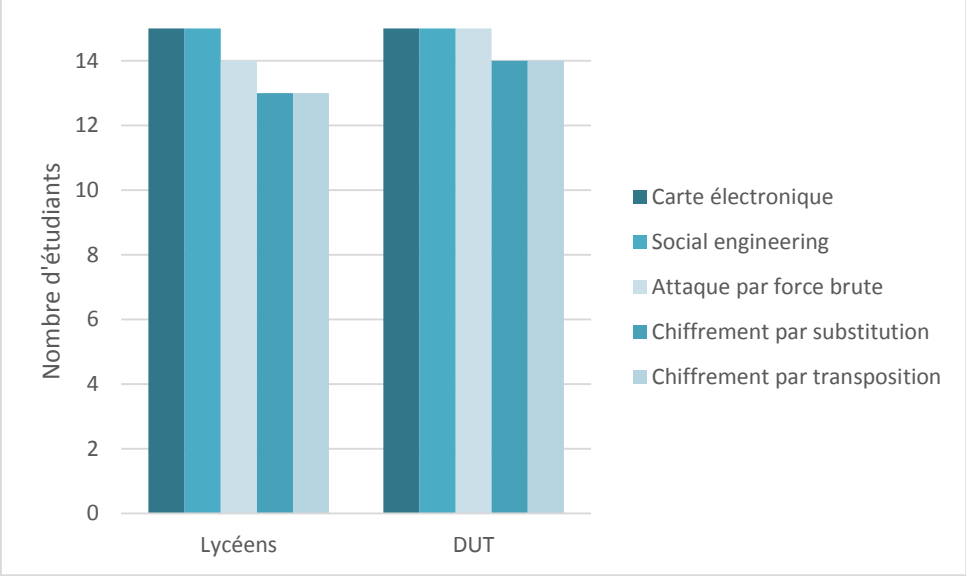

Figure 3: Nombre d'étudiants ayant correctement répondu après la formation pour chaque connaissance pour chaque groupe de 15 étudiants

VI. Conclusion

Ce papier présente un *escape game* sur la sécurité numérique. Il permet à travers le jeu de sensibiliser les étudiants aux notions nécessaires à appréhender le monde numérique de demain et sa sécurité. Ce jeu simple est facile d'accès et permet de renforcer l'intérêt des étudiants pour l'enseignement dispensé.

Naturellement, les résultats présentés sont positifs et nous renforcent dans l'idée d'utiliser des jeux d'évasion dans les séquences d'enseignement (29).

Une prochaine version est en réflexion avec notamment l'apprentissage du fonctionnement de la blockchain.

Remerciements

Les auteurs remercient l'Agence Nationale de la Recherche (ANR) pour le support apporté grâce au financement ANR-11-IDFI- 0017 (projet IDEFI-FINMINA) et ANR-16-IDEX-0006 (I-SITE MUSE, projet AMUSE) ainsi que la région Occitanie et l'Europe pour le financement apporté par le fonds FEDER et le fonds Région.

Références

1. https://fr.statista.com/statistiques/584481/internet-des-objets-nombre-d-appareils-connectes-dans-le-monde--2020/
2. D. Dagon, T. Martin, and T. Starner : "Mobile phones as computing devices: The viruses are coming!" *Pervasive Computing, IEEE*, **3**(4), pp. 11–15 (2004)
3. M. Wolf, A. Weimerskirch, and T. Wollinger : "State of the art: Embedding security in vehicles," *EURASIP Journal on Embedded Systems*, **2007** (1), pp. 1–16 (2007)
4. D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, *et al.*: "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Security and Privacy, 2008*. SP 2008. IEEE Symposium on. IEEE, pp. 129–142 (2008)
5. F. Bruguier, P. Benoit, L. Torres : "Enseignement de la sécurité numérique : De la sensibilisation à l'expertise", *J3eA2017*, 1004 (2017)
6. M. Bourrée, F. Bruguier, L. Barthe, *et al.* : "Secnum: an open characterizing platform for integrated circuits", *Proc. Euro. Work. Microelectronics Education*, Grenoble, France, 88-91 (2012)
7. J. Turner, S.G Paris, How literacy tasks influence children's motivation for literacy. *The reading teacher*, **48**(8), 662–673 (1995)
8 L. Bossuet, Teaching FPGA security. *Proc. International Conference in Field-Programmable Technology* (FPT), 306–309 (2013)
9 Koushanfar, Farinaz, and Miodrag Potkonjak. "Hardware security: preparing students for the next design frontier." *IEEE International Conference on Microelectronic Systems Education (MSE'07)*. IEEE (2007).
10 B. Halak, Course on secure hardware design of silicon chips. *IET Circuits, Devices & Systems* **11**(4), 304–309 (2017)
11 F. Bruguier, P. Benoit, L. Torres, and L. Bossuet. Hardware security: From concept to application. *In Proc. 11th European Workshop on Microelectronics Education (EWME)*. 1–6 (2016)
12 N.H Mackworth, The breakdown of vigilance during prolonged visual search. *Quarterly Journal of Experimental Psychology*, **1**(1), 6–21 (1948)
13 L.A. Annetta, The "I's" have it: A framework for serious educational game design. *Review of General Psychology* **14**(2) 105 (2010)
14. J. Alvarez, D. Djaouti, et O. Rampnoux, "Apprendre avec les serious games ? ", *Réseau Canopé*.
15. P. Nadam, M. Fenaert, A. Petit, "Créer SON énigme ", 2018, http://scape.enepe.fr/creer-son-enigme.html
16. D. Halperin, Th.S. Heydt-Benjamin, B. Ransford, S.S Clark, B. Defend, W. Morgan, K. Fu, Tadayoshi Kohno, and W.H Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. *IEEE Symposium on In Security and Privacy*, 129–142 (2008)
17. P. Lévy and R. Bononno, Collective intelligence: Mankind's emerging world in cyberspace. *Perseus books*, (1997)
18. P. Nadam, "Les contraintes d'un escape game en classe", http://scape.enepe.fr/les-contraintes-d-un-escape-game-en-classe.html (2017)

19. P. Nadam, M. Fenaert, A. Petit, "Édu Game Master, quand le prof se prend au jeu !", http://scape.enepe.fr/edugamemaster.html (2018)
20. S. Granger, Social engineering fundamentals, part I: hacker tactics. *Security Focus*, December 18 (2001).
21. K. Goyal and S. Kinger, Modified Caesar cipher for better security enhancement. *International Journal of Computer Applications* **73**(3) (2013)
22. T. Kelly, The Spartan Scytale. The Craft of the Ancient Historian: *Essays' in honor of Chester G. Starr* 141–169 (1985)
23. P. Engebretson, The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Elsevier (2013)
24. P. Kocher, J. Jaffe, and B. Jun, Differential power analysis. *In Annual International Cryptology Conference. Springer*, 388–397 (1999)
25. E. Brier, Ch. Clavier, and F. Olivier, Correlation power analysis with a leakage model. *In International workshop on cryptographic hardware and embedded systems. Springer*, 16–29 (2004)
26. BS Bloom, Bloom's taxonomy of educational objectives. *Longman* (1965)
27. Arduboy. https://arduboy.com/
28. Film : "La septième compagnie", Robert Lamoureux (1973)
29. Vidéo en ligne, AMUSE : https://www.youtube.com/watch?v=-weijQTu4Io (2019)