AMUSE : un escape game pour l'enseignement de la sécurité numérique

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

AMUSE : un escape game pour l'enseignement de la sécurité numérique

F. Bruguier[a,c], P. Benoit[b,c], L. Dalmasso[c], B. Pradarelli[b,c] 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

Le numérique est de plus en plus présent dans nos vies. La sécurité du monde numérique en est donc d'autant plus importante. Afin de sensibiliser et former les lycéens et étudiants à la sécurité numérique, le pôle CNFM de Montpellier a choisi de développer un escape game dans ce sens. Ce serious game est dispensé sous plusieurs formats en fonction du public visé : du lycéen au doctorant.

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. 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 en complément de ce programme. 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. La suite de l'article est organisée comme suit. Dans la section 2, le choix d'un escape game est justifié. S'en suit une description des principales notions proposées et leur transcription dans le jeu.

II. Escape game ?

Un vecteur de pédagogie

Un escape game1 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 [7]. Dans le cadre de ce dernier, ceux-ci font partie de la catégorie des serious games2. 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'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 [8]. De la même manière, la non linéarité de celles-ci permettra de laisser la part belle à l'apparition de l'intelligence collective [9].

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 [10].

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 [11]. La principale mission consistera à adapter l'avancement de chaque groupe afin de faire tenir la séquence dans le temps impartit.

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.

[1] Jeu d'évasion en français

[2] Jeux sérieux en français

III. Transposition à la sécurité matérielle

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.
- 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. Le chiffrement par transposition reposer sur l'inversion de la position de lettres dans un message. 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 boite de substitution. Celle-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]. Le principe étant de venir mesurer des tensions directement sur un circuit numérique afin d'en extraire de l'information.

Mise en œuvre

La séquence d'enseignement proposée se découpe en plusieurs phases.

Phase amont. Lors de celle-ci, les étudiants sont amenés à étudier plusieurs posters tout en complétant un QCM évoquant les différentes notions.

Phase de jeu. La phase de jeu sera décomposée comme suit. Tout d'abord, l'enseignant expose les règles du jeu. Les étudiants sont répartis en binômes ou trinômes. Chaque groupe dispose de matériel pour ouvrir une mallette contenant le code d'un coffre-fort. Plus de détails seront donnés dans la section suivante.

Phase de débriefing. Lors de cette phase, l'enseignant représentera les différentes phases du jeu en présentant les compétences/connaissances abordées.

Gamification des compétences/connaissances

Spoiler : Si vous souhaitez vous confronter au jeu sans en connaitre toutes les astuces… merci de ne pas lire la section qui suit.

Le jeu est constitué des objets suivants pour chaque groupe : un cadre photo, une mallette, une carte électronique « force brute », deux câbles électriques, une carte à jouer, quatre tables de substitution, un ruban « scytale », un cylindre de rangement pour lampe à ultraviolet, une lampe à ultraviolet, un carnet et un stylo. A cela s'ajoute un coffre-fort et un chronomètre permettant de stimuler les étudiants.

---

[3] Ingénierie sociale en français

[4] Test de pénétration en français

Chacun des compétences/connaissances proposées ci-dessus donne lieu à une énigme proposée lors du jeu ainsi qu'à un éventuel coup de pouce associé qui pourra être proposé aux étudiants bloqués lors du jeu (Tab. I.).

TABLEAU I. Connaissances/compétences et énigmes associées.

Connaissances / compétences	Enigme	Coup de pouce
Social engineering	Utilisation de la date de naissance trouvée sur le cadre photo pour ouvrir la mallette	Présentation du principe
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
Chiffrement par substitution	Remplacement de lettres par leurs positions dans l'alphabet	Présentation du code de César
Chiffrement par transposition	Enroulement d'une bande de papier autour du support de la lampe ultraviolet	Présentation du principe de la Scytale
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
Fonctionnement d'un circuit électronique	Mise sous tension de la carte électronique	Film la septième compagnie
Codage binaire	Utilisation des tensions mesurées sur l'objet connecté	Principe de mesure de tension
Pentesting	Mesure de tension sur l'objet connecté puis conversion en décimal	Principe du pentesting

A ces énigmes s'ajoutent d'autres énigmes n'ayant pas forcément de rapport avec la thématique enseignée même si certains arriveront toujours à trouver un lien. L'utilisation d'une lampe à ultraviolet et d'une carte à jouer permet notamment de choisir la bonne boite de substitution à utiliser.

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 disposent d'un voltmètre et d'une table de conversion binaire décimal (pour les étudiants novices) afin d'ouvrir un coffre-fort renfermant des secrets d'état. On va pour cela leur permettre de rentre 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 le tableau I ainsi que quelques défis complémentaires, le groupe d'étudiant le plus rapide découvrira la combinaison du coffre-fort.

Bilan

Une version préliminaire de ce jeu a rencontré un succès important lors de la fête de la science 2017 ainsi lors de son utilisation pour des cours à Polytech Montpellier. La nouvelle version proposée ici est déjà planifiée pour différents enseignements mais il est encore trop tôt pour tirer un bilan définitif.

IV. 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 et facile d'accès et permet de renforcer l'intérêt des étudiants pour l'enseignement dispensé. Une prochaine version est en réflexion avec notamment l'apprentissage du fonctionnement des chaines de blocs.

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) ainsi que la région Occitanie et l'Europe pour le financement apporté à travers le fond FEDER et le fond région. Enfin, les auteurs remercient également l'Université de Montpellier pour son soutien au travers de l'Isite MUSE et notamment du projet AMSUE.

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, vol. 3, no. 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, vol. 2007, no. 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, 2008, pp. 129–142.
5. F. Bruguier, P. Benoit, L. Torres : "Enseignement de la sécurité numérique : De la sensibilisation à l'expertise", - J3eA, 2017
6. Bourrée, M., Bruguier, F., Barthe, L., et al.: "Secnum: an open characterizing platform for integrated circuits", Euro. Work. Microelectronics Education, 2012, Grenoble, France, pp. 88-91.
7. Alvarez,J., Djaouti, D., et Rampnoux, O. : "Apprendre avec les serious games ? ", Réseau Canopé.
8. Nadam, P., Fenaert, M., Petit, A. : "Créer SON énigme ", 2018, http://scape.enepe.fr/creer-son-enigme.html
9. Nadam, P. : " Favoriser l'intelligence collective", 2018, http://scape.enepe.fr/intelligence-collective.html
10. Nadam, P. : "Les contraintes d'un escape game en classe", 2017, http://scape.enepe.fr/les-contraintes-d-un-escape-game-en-classe.html
11. Nadam, P., Fenaert, M., Petit, A. : " Édu Game Master, quand le prof se prend au jeu ! ", 2018, http://scape.enepe.fr/edugamemaster.html