

Retour sur le jeu sérieux : Initiation à la sécurité informatique des objets connectés

Olivier Fruchier, Philippe Egea, Faissal Bakali, Thierry Talbert
Olivier.Fruchier@univ-perp.fr

UFR SEE, Université de Perpignan Via Domitia, 52 Av. Paul Alduy, 66100 Perpignan:

RÉSUMÉ : Lors de la 13^{ème} édition du CETSIS, en 2018, nous avons présenté un jeu sérieux que nous avons mis en place [1]. Ce jeu sérieux a pour objectif de sensibiliser les étudiants à la sécurité informatique en utilisant des cartes raspberry pi. Nous avons conçu notre jeu sérieux sous la forme d'une enquête policière. Cette enquête conduit les étudiants tout au long du scénario et les amène à avancer dans la résolution des problèmes étape par étape. Le jeu sérieux a été testé grandeur nature avec un binôme d'étudiants de Licence 3 Informatique et de Licence 3 Électronique en février 2019. Dans cet article nous reviendrons sur la présentation du jeu, le déroulement des séances, le retour des étudiants et les améliorations que nous avons apportées au jeu.

Mots clés : Jeux sérieux, Piratage éthique (Ethical hacking), Électronique embarquée, Objets connectés, Transdisciplinarité, Porte dérobée (backdoor), Retour d'expérience.

1 INTRODUCTION

Dans la littérature, les jeux sérieux sont définis par Julien Alvarez, en effet, dans sa thèse il définit les jeux sérieux de la façon suivante : "Application informatique, dont l'objectif est de combiner à la fois des aspects sérieux tels, de manière non exhaustive, l'enseignement, l'apprentissage, la communication, ou encore l'information, avec des ressorts ludiques issus du jeu vidéo. Une telle association a donc pour but de s'écarter du simple divertissement." [2] L'apprentissage par le jeu conduit les étudiants à être actifs, leur niveau de concentration augmente et ils devraient apprendre davantage [3].

Il existe plusieurs types de Serious Games avec des règles et des scénarios parfois très complexes, conçus pour les besoins de différentes communautés (hackeurs, étudiants, militaires) [4]. Les jeux sérieux, ou d'une manière générale les jeux offrent un avantage incontestable, il s'agit du droit à l'erreur. Quel informaticien n'a pas lancé une compilation et exécution en espérant avoir le bon résultat ? Les jeux sérieux donnent le droit à l'erreur naturellement. Nous ne sommes pas là pour sanctionner, mais pour apprendre. De plus, une autre raison pour laquelle nous avons choisi de faire un jeu sérieux plutôt qu'une formation classique tient au fait que les jeux sérieux permettent aux étudiants de devenir acteurs de leur formation tout en captivant leur attention sur la discipline visée. Ce type de méthode permet également de redynamiser la formation tout en rendant le contenu plus facilement accessible et, enfin, elle déplace le rôle du formateur au rôle de facilitateur [5].

En outre, dans le domaine de l'apprentissage de la sécurité des systèmes d'information, l'enseignement est souvent difficile. Le domaine est immense et la théorie seule ne permet pas de sécuriser efficacement des systèmes. Le jeu semble être une solution intéressante d'apprentissage par la pratique [6].

L'organisation d'un exercice de Serious Game exige beaucoup de préparation. Il est également nécessaire de définir le public cible, les objectifs pédagogiques et le

contenu détaillé de l'exercice : scénario, règles du jeu, durée. Sa réalisation va demander la mise au point d'une plateforme technique ainsi qu'un ensemble d'éléments logistiques. L'équipe pédagogique doit définir quels savoirs techniques sont donnés aux étudiants et définir clairement les compétences à acquérir. À partir de cela, un scénario de jeu adéquat est construit [7].

Ici, notre jeu sérieux s'adresse à des étudiants de Licence 3 Électronique, Électrotechnique et Automatique (EEA) et de Licence 3 Administration Systèmes et réseaux (ADMISYS). La particularité consiste à mélanger des formations qui sont éloignées (enseignants différents, culture et méthodes de travail distinct) mais possédant des problématiques connexes (informatique industrielle et sécurité informatique, électronique embarquée). Le jeu, ainsi créé, a pour objectif de montrer aux étudiants qu'ils possèdent un domaine d'expertise et peuvent partager leurs connaissances avec des élèves d'un autre domaine.

Pour motiver les étudiants, il s'agira de résoudre une énigme réaliste dans laquelle une entreprise a perdu l'accès à ses données. Notre exercice d'hacking est une simulation qui placera des participants dans une situation réaliste. Ce cadre de réalisme sera ponctué tout le long du jeu par des traits d'humour pour ne pas perdre l'esprit ludique. Nous précisons aussi que dans notre cas nous avons voulu utiliser la notion de Ethical Hacking ou piratage éthique pour donner un cadre de déontologie.

L'autre objectif de ce jeu est de faire progresser et de sensibiliser les étudiants au problème de la sécurité informatique [8]. Pour cela, un scénario basé sur des faits crédibles, abordant aussi bien des problématiques liées à la sécurisation des serveurs ou des interrogations légales sont présentés.

2 CONTEXTE PÉDAGOGIQUE

2.1 Origine du projet

La licence 3 Électronique, Électrotechnique et Automatique (EEA) vise à former des étudiants dans le domaine de la physique appliquée. Tournée vers les

sciences et techniques de l'ingénieur, elle s'appuie sur des bases théoriques et pratiques dont les objectifs principaux sont de former des étudiants en physique et physique appliquée par l'acquisition de connaissances solides tant théoriques qu'expérimentales en électronique, énergie électrique, automatique, matériaux, procédés et physique.

La licence 3 professionnelle Administrateur de Systèmes ADMISYS propose une formation pluridisciplinaire en informatique axée sur les systèmes d'exploitation et les réseaux.

Ces deux licences sont des domaines différents avec des débouchés bien distincts. Cependant, l'essor des technologies dans l'embarqué et l'augmentation de la puissance de calculs des systèmes embarqués demandent aux EEA plus de compétences en informatique et aux informaticiens plus de compétences dans le domaine de l'électronique. Les terminaux mobiles, tels que les smartphones où les enceintes intelligentes en sont un parfait exemple. Malgré tout, nous faisons le constat que les étudiants d'informatique et d'électronique sont réticents à sortir de leurs domaines. Un des objectifs de ce jeu est de décloisonner ces deux disciplines et d'amener à travailler ensemble des étudiants dans des domaines professionnels très proches. Le Tableau 1 ci-dessous résume les connaissances et compétences que nous aimerions croisées dans le cadre de notre jeu sérieux.

Connaissances et compétences en :	
Informatique	Électronique
Systèmes d'exploitation	Base de l'électronique Capteurs RFID Protocole de communication SPI Codage ASCII Hexa Câblage d'un circuit électronique
Commande du système d'exploitation	
Droit informatique	
Porte dérobée (backdoor)	
Base de données	
Programmation python	
HTML, PhP, MySQL	

Tableau 1 - Connaissances et compétences des licences à mettre en commun.

Lors du développement de notre projet de *freecooling*, qui a été présenté au CETSIS 2017 [9], nous avons constaté l'intérêt de travailler avec des compétences de domaines connexes tels que l'électronique et l'informatique. Lors de ce projet nous avons fait intervenir des stagiaires issus de la licence EEA et des stagiaires issus de la licence ADMISYS et nous avons constaté un cloisonnement intellectuel de nos étudiants : les électroniciens étaient très réticents à aborder toute programmation (même simpliste) et les informaticiens très frileux dès qu'il s'agit d'interagir avec des réseaux de capteurs ou d'actionneurs. Ce constat nous a amené à nous tourner vers la pédagogie innovante.

Ce projet a pu être réalisé avec les compétences des deux domaines, et nous a montré que les connaissances seules ne suffisent pas. Les jeux sérieux présentent donc de nombreux intérêts pour les étudiants. Ils associent une pédagogie didactique, apportent un enrichissement humain au niveau de la communication, permettent de croiser des connaissances interdisciplinaires et, enfin, d'utiliser les ressorts du jeu

2.2 Objectifs pédagogiques

Associer des populations d'étudiants permet d'établir des scénarios de travail réalistes. Mélanger des disciplines permet aux étudiants de s'aider au travers de leurs connaissances propres et de développer de l'entraide. Le scénario que nous proposons permet aux étudiants d'appréhender les notions suivantes :

- câblage de circuit électronique ;
- branchement d'un capteur RFID ;
- protocole de bus de communication ;
- codage ASCII ;
- système d'exploitation Linux ;
- commandes SHELL Unix ;
- bases de données ;
- notions de programmation en Python, PhP, Mysql, HTML ;
- notions de droit en informatique, de piratage éthique.

Nous avons écrit un scénario permettant d'intégrer toutes ces notions. Par ailleurs, le jeu active des compétences personnelles comme la capacité à travailler en équipe et à prendre des décisions avec des informations limite dans une période de temps contrainte. À la fin du jeu, les étudiants des deux formations devront obtenir des compétences dans les deux domaines de chaque licence.

3 LE JEU

3.1 Origine

L'idée de base est partie d'une machine personnelle qui avait été piratée pour faire du minage de cryptomonnaie. Nous avons pu réaliser une analyse *post-mortem* de cette machine qui s'est révélée une mine d'information. Comment les pirates ont-ils obtenu un login et mot de passe ? Comment ont-ils fait pour lancer un programme qui se relance automatiquement tout en restant discret ? Ainsi, le scénario a commencé à prendre forme. Nous avons par la suite décidé d'ajouter des faiblesses propres aux lectures de données RFID et d'introduire des notions d'électronique. Un autre facteur déterminant a été d'utiliser des boîtiers Raspberry. Ces boîtiers complets et peu onéreux sont parfaits pour mettre en place un scénario réaliste : système d'exploitation Linux, bus de communication pour intégrer des lecteurs RFID, Serveur Web intégré, langage Python... Enfin une machine complète capable de connecter des objets électroniques et de se connecter à Internet. La structure physique prend forme : un Raspberry client, un Raspberry Serveur, un lecteur RFID, des badges RFID, des plaques de connectique, des fils de cuivre vont constituer le matériel du jeu sérieux. La structure générale se met en place. Celle-ci nous permet alors d'évaluer le budget.

3.2 Budget

Sans compter le coût humain, pour 24 Raspberry avec carte SD intégrées, 20 plaques de connectique, des boîtes de fils de cuivre, 20 lecteurs de badge RFID, nous avons dépensé environ 1 400€. Cette somme a été répartie sur les deux licences.

3.3 Dramatisation

Pour le bon fonctionnement du jeu, il est important de mettre les étudiants dans un contexte ludique et dramatique. Nous avons conçu notre scénario sous la forme d'une enquête policière. Cette enquête conduit les étudiants tout au long du scénario et les amène à avancer dans la résolution des problèmes. Le nom des personnages doit être révélateur du scénario et les orienter sur la culpabilité des personnages. Chaque personnage a un nom révélateur au sens d'une pièce de théâtre de vaudeville.

3.4 Scénario

Le scénario est sûrement la chose la plus difficile à réaliser, car il doit tenir compte des objectifs pédagogiques, d'une cohérence d'ensemble et de l'esprit ludique. Nous vous délivrons ici le début du scénario pour donner une idée générale de l'esprit.

« Vous venez d'être recruté comme détective privé par Monsieur Bob Hésite, PDG de l'entreprise TestSol spécialisée en panneaux solaires thermiques et photovoltaïques. Pour votre couverture, vous êtes recruté comme spécialiste de l'informatique industrielle pour vos compétences dans l'électronique et l'informatique (Licence EEA + Licence Admisys). Monsieur Bob Hésite pense que vous mènerez à bien vos nouvelles missions et que vous démontrerez toutes vos capacités décrites dans votre Curriculum Vitae, tant en espionnage, qu'en expertise d'informatique industrielle. Ainsi, votre première mission est de reprendre le travail de Madame Bidouille connue pour son esprit remarquable et son charme. Elle est partie subitement suite à une dispute très virulente avec un collègue de travail. Votre responsable est Monsieur Joseph Vial connu pour son élégance et sa discrétion. Aussi il ignore la vraie raison de votre embauche. Comme première mission, Monsieur Vial vous demande de gérer le système d'ouverture et fermeture de l'entrepôt de SolarTest situé à quelques centaines de mètres. Ce système fonctionne avec des badges RFID (Radio-Authentification) et permet l'entrée et la sortie de l'entrepôt de TestSol. Vous devez trouver qui a menacé Madame Bidouille et pourquoi elle est partie si rapidement. Monsieur Bob Hésite a remarqué des problèmes relationnels au niveau des responsables de l'entreprise. Le PDG Hésite vous a fourni ce document secret afin de remplir votre mission d'investigation... ».

Le scénario « document secret », disponible pour chaque étudiant comporte 23 pages sous format papier. Il est constitué d'aides techniques, de questions et d'actions à réaliser. Du fait du format papier, chaque

étudiant du binôme informatique/électronique peut facilement s'échanger le document. Nous envisageons éventuellement une version numérique sous format Web ou Moodle.

3.5 Organisation du jeu

Les deux Licences 3 EEA et ADMISYS sont composées habituellement de 25 étudiants chacune. La salle de TP peut accueillir 15 postes de travail double constitués d'un accès à Internet et d'une autre prise réseau permettant de mettre en réseau l'ensemble des machines du jeu sérieux. Nous constituerons 25 binômes constitués d'un étudiant EEA et d'un étudiant ADMISYS. Nous formerons alors deux groupes comprenant respectivement 12 et 13 binômes.

Chaque binôme aura accès à un ordinateur pour effectuer des recherches techniques sur Internet : configuration du Raspberry, comment connecter le lecteur RFID, aide sur les commandes Shell, etc. Il possède aussi un ordinateur léger de type Raspberry qu'il devra connecter au lecteur RFID. Le Raspberry aura un accès à Internet afin de réaliser des mises à jour. Les Raspberry Pi ont accès à la machine cible qui contiendra une base de données pour chaque étudiant. Ces bases de données seront différentes pour chaque groupe de travail afin de personnaliser les réponses et éviter les fuites entre les étudiants.

Plusieurs documents techniques accompagnent le scénario tel que la fiche technique du capteur RFID, le câblage d'un GPIO, le programme python pour la mise en fonctionnement du capteur RFID, etc. Nous fournissons un maximum d'informations nécessaires et suffisantes afin d'éviter que les étudiants perdent trop de temps avec les recherches sur la toile.

3.6 Déroulement des séances

La première séance débute par une présentation du document et une lecture du scénario général pendant 10 minutes. Ces 10 minutes permettent de faire rentrer les étudiants dans l'ambiance et de commencer le jeu sérieux. Devant eux les étudiants découvrent le matériel : Lecteur de badge, plaque de test, câbles de connexion, Raspberry, clavier, souris, alimentation électrique, écran, etc. Chaque groupe doit relier son Raspberry client au serveur Raspberry. Pour cela, il faut câbler le Raspberry client à une prise réseau de la table et s'approcher de l'armoire de brassage (en présence d'un organisateur) pour connecter la bonne prise au commutateur. Nous les informons du mode d'évaluation : la moitié de la note est obtenue lorsqu'ils réussissent la mission et l'autre moitié en répondant aux questions des missions. Nous distribuons deux jokere sous forme de deux post-its de couleurs leur donnant droit d'obtenir une aide des organisateurs. Les étudiants ressentent un léger stress au départ, et le jeu peut commencer (Figure 3).

Le jeu suit alors son cours sur les 3 séances. Nous sentons la pression monter au cours du temps et les étudiants se prennent au jeu, très sérieusement. La salle est relativement peu bruyante, car il n'y a que des commu-

nications entre les binômes. Les jokers sont peu utilisés, car les étudiants négocient pour ne pas avoir à les utiliser, tout le monde est dans le jeu. Les 3 organisateurs sont très sollicités au départ, et au fil des 9 heures, les étudiants deviennent autonomes. Le niveau du jeu semble convenir, ni trop facile, ni trop compliqué ; ce point est essentiel pour le bon déroulement du jeu. Les étudiants passent les étapes avec plus ou moins de difficultés et nous constatons que notre rôle de facilitateur est essentiel pour débloquer les étudiants : câble défectueux, plaques ayant des problèmes de connectiques, messages morses trop rapides. Les étudiants arrivent par des biais différents (ce qui nous étonne !) à récupérer la base de données du serveur et l'exploiter pour trouver qui est la coupable. Nous sommes ravis, car environ 80 % des étudiants arrivent à la fin du scénario et 50 % au moins ont trouvé les bonnes réponses.

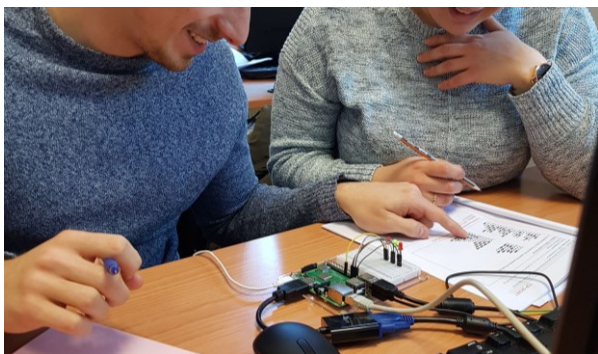


Figure 1 - Les étudiants en train de jouer

3.7 Évaluation des étudiants

L'évaluation n'est pas forcément de mise dans l'univers du jeu, néanmoins nous devons essayer de connaître l'impact de cet exercice sur l'apprentissage des étudiants. Nous demandons à chaque binôme d'étudiant un compte-rendu sous forme de questions ludiques. Ce compte-rendu rempli à la fin du jeu nous servira de base pour évaluer l'implication des étudiants dans le jeu.

Un travail dirigé quinze jours plus tard nous sert de marqueur afin d'évaluer l'impact du jeu sur les connaissances et compétences acquises, cette séance permettra aussi d'avoir un retour sur le déroulement du jeu (sous forme de dialogue direct avec les étudiants) afin améliorer le jeu au fil des années que ce soit du point de vue du scénario ou de celui du niveau attendu.

4 RETOUR D'EXPERIENCE

Le jeu s'est déroulé sur 3 séances de 3h et sur 3 jours consécutifs pour le groupe 1 et pour le groupe 2. La plus grosse difficulté a été de réinitialiser le jeu au niveau des Raspberry qui ont été modifiés par le premier groupe. Finalement nous avons dû implanter l'image d'origine sur chacune des cartes SD des Raspberry aussi bien pour les clients que pour les serveurs. Cette opération est assez laborieuse et demande du temps, environ 5 minutes par Raspberry. Pour améliorer cela, nous avons virtualisé les serveurs avec le logiciel de virtualisation Proxmox VE qui évite d'utiliser de vraies cartes Raspberry pour les serveurs. Nous ne pouvons pas virtualiser les clients, car nous souhaitons garder le Raspberry comme outil pratique.

Pour améliorer la correction et le côté ludique, nous envisageons de transformer le document papier contenant les questions et les réponses vers la plateforme numérique de travail Moodle de l'université [10]. Cet outil nous permettra de suivre en temps réel l'avancement et l'évaluation du travail pour chaque groupe.

Au niveau des étudiants, nous avons observé une forte adhésion, environ 80% des groupes sont arrivés à la fin du jeu. Nous avons été agréablement surpris que le mélange d'étudiants de promotions différentes qui ne se connaissent pas auparavant fonctionne très bien : l'ambiance est studieuse, de nombreux échanges entre les étudiants au sein du binôme sont riches et fructueux. Dans notre jeu, nous pouvons parler de succès quant à l'apprentissage entre pairs.

Nos formations sont dotées de conseils de perfectionnement qui permettent un retour direct des étudiants sur les matières enseignées. Ainsi, les étudiants ont, de manière unanime, plébiscité ce type de méthode pédagogique.

5 CONCLUSION

La conception et la réalisation du jeu sérieux nous ont amusés et enrichis. Mais est-il possible de réaliser l'ensemble des cours sous cette forme ? La réponse vient du temps consacré à la préparation et à la réalisation. Quatre-vingts heures de préparation sont nécessaires pour concevoir une heure de jeu. Mais est-ce pour autant inutile ? Bien sûr que non ! Réaliser un jeu avec les étudiants permet de briser les relations élèves-enseignants et d'entrer dans une relation d'égal à égal. Nous déplaçons le rôle de formateur à facilitateur. Nous espérons aussi que l'activité intrinsèque liée au jeu amène les étudiants à s'approprier le savoir et à l'utiliser de manière concrète. De plus ce type de formation peut facilement s'exporter vers d'autres licences EEA et informatiques.

Bibliographie

- [1] Olivier Fruchier, Philippe Egea, "Apprendre en jouant, c'est sérieux : Initiation à la sécurité informatique des objets", *CETIS 2018 - 13ème édition - Fès Maroc 29 - 31 Oct. 2018*.

- [2] Julian Alvarez. "Du jeu vidéo au Serious Game : approches culturelle, pragmatique et formelle. Multimédia", *Thèse de doctorat l'Université de Toulouse (UT3 Paul Sabatier), [cs.MM]. Université Toulouse, 2007. Français. (el-01240683)* .
- [3] Damien Djaouti, "Serious Game Design Considérations théoriques et techniques sur la création de jeux vidéo à vocation utilitaire", *Thèse de doctorat l'Université de Toulouse (UT3 Paul Sabatier), 2011, <http://thesesups.ups-tlse.fr/1458/1/2011TOU30229.pdf>*.
- [4] Jean Benoit, "Exercices de Sécurité Informatique", *Actes des Journées Réseaux de l'Enseignement et de la Recherche (JRES 2017), Nantes (France), Novembre 2017, <https://www.jres.org/fr/presentation?id=95>*.
- [5] Julian Alvarez, Damien Djaouti, Olivier Rampnoux, "Apprendre avec les Serious Games ?", *Édition Réseau Canopé, 2016, ISBN : 978-2-2400-4084-8*.
- [6] Olivier Levillain, Pascal Chour, "La sécurité du numérique dans les formations de l'enseignement supérieur", *Actes des Journées Réseaux de l'Enseignement et de la Recherche (JRES 2017), Nantes (France), Novembre 2017, <https://www.jres.org/fr/presentation?id=53>*.
- [7] Ames F. Knight, Simon Carley "Serious gaming technology in major incident triage training: a pragmatic controlled trial", *Thèse de doctorat l'Université de Toulouse (UT3 Paul Sabatier), Volume 81, Issue 9, 2010, Pages 1175-1179, ISSN 0300-9572*.
- [8] ACISSI, Collection Epsilon (Saint-Herblain), "Sécurité informatique - Ethical Hacking: Apprendre l'attaque pour mieux se défendre", *Editions ENI, 2009, ISBN : 2746051052, 9782746051058*.
- [9] Olivier Fruchier, Philippe Egea, "Mise en place d'un système de rafraîchissement d'un local informatique par ventilation hybride", *CETISIS 2017 - 12ème édition - - Le Mans 3-4 mai 2017*.
- [10] Thierry Talbert, Olivier Fruchier, F. T. "Retour sur 5 ans d'apprentissage par résolutions de problèmes et par projet", *Actes du 12ème Colloque sur l'Enseignement des Technologies et des Sciences de l'Information et des Systèmes (CESTIS 2017), Nantes (France), Novembre 2017*.