HAL open science

Retour d'expérience sur l'utilisation des challenges de sécurité durant un cours sur la sécurité des objets connectés

Christophe Tilmant, Jacques Laffont

To cite this version:

Christophe Tilmant, Jacques Laffont. Retour d'expérience sur l'utilisation des challenges de sécurité durant un cours sur la sécurité des objets connectés. RESSI (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information), Dec 2020, En ligne - cause COVID19, France. hal-03079060

HAL Id: hal-03079060

https://uca.hal.science/hal-03079060v1

Submitted on 17 Dec 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Retour d'expérience sur l'utilisation des challenges de sécurité durant un cours sur la sécurité des objets connectés

Christophe TILMANT[1], Jacques LAFFONT[2]
christophe.tilmant@uca.fr
(1) Université Clermont Auvergne, CNRS, SIGMA Clermont, Institut Pascal, F-63000 Clermont-Fd, France
(2) Université Clermont Auvergne, Polytech Clermont-Ferrand, F-63000 Clermont-Fd, France

RESUME : Dans le cadre de la mise en place d'un cours sur la sécurité des objets connectés, les enseignants ont utilisé une approche pédagogique différente pour aborder ce thème. Ce cours intervient au début d'une formation en informatique avec une spécialisation en sécurité informatique. Les enseignants ont décidé de mettre en œuvre une pédagogie par échec productif qui a démontré un intérêt certain comme un enseignement introductif tout en permettant une meilleure intégration des connaissances. Une approche classique de contrôle des connaissances n'était pas judicieuse, en effet les compétences acquises se basent sur du savoir-faire non formaté. Les étudiants changent alors de rôle et passent du côté de l'attaquant par des approches de piratage éthique pour exploiter des failles de sécurité où ils sont évalués par leurs résultats durant cet exercice que l'on appelle des challenges de sécurité. Afin de voir l'intérêt de cette pédagogie, les enseignants ont mis en place un dispositif d'évaluation de cette nouvelle approche d'enseignement dont les résultats sont présentés dans cet article.

Mots clés : objets connectés, sécurité, challenge de sécurité, pédagogie.

1 INTRODUCTION

Dans le cadre de leur formation d'ingénieur en informatique à l'ISIMA (http://www.isima.fr) des étudiants se forment aux objets connectés au niveau bac+4. En plus d'un cours en tronc commun sur ce thème, certains suivent également dans leur spécialisation « Réseaux et Sécurité Informatique » des travaux pratiques sur les problématiques liées à la sécurité des objets connectés.
Durant ces séances, différentes failles de sécurité sont mises en évidence et corrigées afin d'arriver à un système le plus durci possible. Les étudiants vont commencer par concevoir leur application, puis tenteront d'outrepasser les processus de sécurité mis en place (cf. *figure 1*). La stratégie pédagogique employée est l'échec productif (*Productive failure* [1, 2]). Dans cette approche de résolution, les apprenants sont confrontés à un problème complexe sans avoir étudié une solution spécifique. Les étudiants ne trouvent pas la solution directement et ils ont besoin régulièrement de monter en compétences par des formations directement liées au sujet pour avancer. Il a été montré que ce type d'approche à un intérêt dans un enseignement comme activité introductive. Dans notre cas, c'est un des premiers cours réalisé par les étudiants durant leur spécialisation en sécurité informatique et les objets connectés sont un magnifique terrain de jeu pour découvrir la chaine de sécurité.

L'évaluation des compétences acquises ne peut pas se faire par des approches classiques car les apprenants ont étudié la mise en pratique par l'exploitation des failles de sécurité. Ces techniques ne sont pas formatées mais se basent beaucoup sur une bonne culture scientifique, du bon sens, de la logique et des compétences informatiques.
Les enseignants ont donc décidé de mettre en place une évaluation des compétences acquises par l'utilisation de challenge de sécurité : durant une séance de 2h les étudiants doivent résoudre des défis afin de pirater l'objet connecté des professeurs. Ces challenges ont aussi un double intérêt car une bonne compréhension des notions d'attaques par les failles est nécessaire pour mettre en place des correctifs (*ethical hacking*). Cette forme d'évaluation a démontré une adhésion des apprenants par l'utilisation des approches de *serious game*.
Afin d'évaluer l'intérêt pédagogique de ce type d'approche pour contrôler l'acquisition des compétences acquises par les apprenants, les enseignants ont mis en place un dispositif d'évaluation de celle-ci.
Cette démarche d'amélioration continue est soutenue et encouragée par l'université Clermont Auvergne (tutelle de la composante d'enseignement) via le programme Learn'in Auvergne (https://cap2025.fr/formation/learn-in-auvergne/). Ce programme transverse du projet CAP 20-25 a pour objectif d'accompagner la transformation des pratiques pédagogiques en fournissant un ensemble de services.

Figure 1 : Organisation pédagogique du cours basé sur le durcissement d'un objet connecté.

Pour appuyer l'accompagnement de ces transformations pédagogiques, des appels à projet sont régulièrement proposés et le travail présenté dans cet article a été retenu en janvier 2019.
Cet article va d'abord présenter dans le paragraphe 2 le contenu de ce cours sur la sécurité des objets connectés, puis présentera l'innovation pédagogique qui réside dans la technique de modalité de contrôle des connaissances qui se base sur des challenges de sécurité. Le déroulé et l'outil développé pour réaliser ces challenges seront détaillés dans le paragraphe 3. Comme ce projet est dans une démarche d'amélioration continue l'évaluation de ce dispositif sera présenter dans le paragraphe 4 avant de proposer des perspectives possibles et de conclure.

2 CONTENU DU COURS : « SECURITE DES OBJETS CONNECTES »

2.1 Objectifs pédagogiques

L'un des intérêts de cet enseignement est de présenter la chaîne de sécurité ainsi que différentes attaques possibles. Il s'agit de sensibiliser les étudiants à une approche globale de la sécurité et à la nécessité de l'intégrer au plus tôt dans le cycle de conception. Différentes failles de sécurité sont mises en évidence et corrigées afin d'arriver à un système le plus durci possible à la fin des travaux pratiques (cf. *figure 1*).
Afin d'aborder ces différents points, la pédagogie employée se veut très pragmatique. Les étudiants vont commencer par concevoir leur application, puis tenteront d'outrepasser les processus de sécurité mis en place.
La stratégie pédagogique employée est l'échec productif (*Productive failure*) [1,2]. Dans cette approche de résolution de problèmes, les apprenants sont confrontés à un problème complexe sans avoir reçu de formation spécifique au préalable. Les étudiants sont confrontés à ne pas pouvoir trouver la solution directement et ils ont besoin régulièrement de monter en compétences. Les spécialistes des neurosciences ont démontré que le savoir se construit par l'erreur et confèrent à celle-ci, par voie de conséquence, une valeur positive plutôt que négative.

2.2 Organisation du cours

Cette formation est constituée de 10 séances de travaux pratiques de 4h en enseignement présentiel. Les séances sont organisées en plusieurs parties :

- la mise en place d'un objet connecté sans contraintes de sécurité informatique ;
- mise en évidence des failles de sécurité en mettant en défaut le système. Cela permet l'introduction de nouvelles connaissances au niveau de la sécurité informatique ;
- un durcissement du système en mettant en place des correctifs suite à des vulnérabilités détectées (ou plutôt mise en évidence).

De plus, des phases d'évaluation des étudiants complètent ce processus. Plusieurs QCM permettent de valider l'acquisition des connaissances par une approche de classe inversée et des séances de challenges de sécurité, où les étudiants se mettent à la place de l'attaquant et permettent d'évaluer le savoir-faire des apprenants.
Le contenu détaillé du cours avec les technologies employées et les failles misent en évidence sont présentées dans [3].

3 PEDAGOGIE ET MODALITES DE CONTROLE DES CONNAISSANCES DU COURS

La pédagogie est une série d'actions éducatives qui visent à provoquer des effets précis d'apprentissage.
L'objectif de ce cours est la montée en compétences sur la sécurité informatique par la mise en place d'un durcissement d'un système. Nous avons mis en place une stratégie d'échec productif où chaque durcissement peut est contourné en exploitant une nouvelle vulnérabilité. L'échec est mis en évidence par les enseignants en montrant régulièrement que le système n'est toujours par sûr. Ici, le savoir se construit par un pseudo-échec ou plutôt par une solution incomplète et comme le système devient de plus en plus dur à pirater cela confère par voie de conséquence une valeur positive plutôt que négative. Il faut noter que le terme « échec » ne signifie pas de faire échouer l'étudiant dans son développement, mais bien de situations d'apprentissages où l'apprenant ne réussit pas du premier coup. Cela permet aux apprenants de comprendre la difficulté du mécanisme et qu'ils reconnaissent qu'ils avaient une approche erronée, car incomplète.

3.1 Pédagogie inversée

Durant les séances de présentiel, on se concentre sur l'apprentissage du savoir-faire et les enseignants utilisent la classe inversée pour l'acquisition du savoir. Pour préparer la séance suivante, un ensemble de documents sont à lire et à étudier, mais également la mise en place de briques logicielles afin d'être le plus efficace durant la séance. Pour assurer le bon fonctionnement de cette approche, des QCM sont réalisés au début de chaque séance pour inviter les étudiants à s'investir dans cette démarche. En ce qui concerne l'outil pédagogique numérique, la plateforme pédagogique Moodle est utilisée afin de distribuer les documents, mais aussi pour rythmer les séances de cours.

3.2 Challenges de sécurité

Durant le cours, deux challenges de sécurité sont réalisés et qui permettent d'évaluer le savoir-faire des apprenants sur l'exploitation des failles de sécurité. Elles ont lieu à la cinquième et dixième séance de cours afin de valider les différents contenus du cours : une première partie sur des attaques du monde de l'embarquée et une deuxième sur les attaques sur le réseau.

3.2.1 Principe des séances des challenges

Le cadre de travail est bien défini pour éviter une dispersion des moyens employés par les apprenants. Les étudiants sont convoqués à une séance pour un challenge de

sécurité sans plus d'informations. En arrivant (*cf. figure 2*), ils découvrent le contenu de l'épreuve sur une page de la plateforme pédagogique Moodle (*cf. figure 3*).
Ils découvrent un contexte général, par exemple d'écouter le réseau afin de sortir des informations, mais aussi plusieurs défis à résoudre dans ce cadre global.

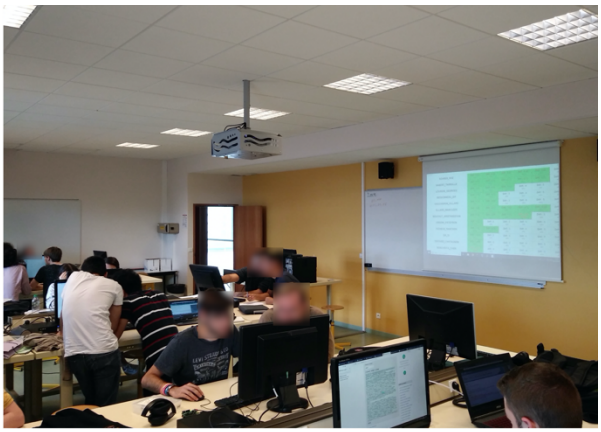


Figure 2 : Challenge de sécurité — Déroulé d'un challenge avec projection des résultats des défis

Déroulement du challenge :

Ce challenge est constitué de 5 défis.

Chaque défi vous octroie des points additionnés de points bonus dès qu'il est résolu.

Chaque défi vous apporte 2 points. Les points bonus sont calculés comme en fonction de votre rang. Le premier à avoir validé le défi emporte 3 points, le deuxième : 3.(1-1/N), et de façon générale pour le groupe de rang i le bonus sera : 3.(1-(i-1)/N).

Chaque groupe ayant réalisé le défi aura donc un bonus, par contre la valeur du bonus dépendra du nombre de personnes ayant validé le défi (sauf pour le premier groupe).

Le temps pris en compte est le temps depuis le début du challenge, puis le temps depuis la validation du défi précédent.

Objectif :

Pour chaque défi, vous devez allumer la LED2 d'un IOT.

Pour allumer la LED2, il faut qu'un message ayant un payload correct soit reçu sur un topic de cette forme :

- ISIMA/SECRET_ZZZ/CHALLENGE_2/DEFI_Y/GROUPE_NOMS_ETUDIANTS/LEDS/LED2
  - ZZZ est à déterminer pendant le défi

Défi No 3

nfin un défi à la hauteur des compétences du service.

ios deux espions ont réussi à déterminer que le mot de passe utilisé était très court. Probablement 2 caractères uniquement.

e plus, une analyse poussée des touches du clavier semble montrer que seules les lettres de l'alphabet en majuscule ont été utilisées.

e payload lui semble être constitué des caractères suivants "ONF .0123456789".

e port du broker est 10803.

e document à rendre aura la forme suivante :

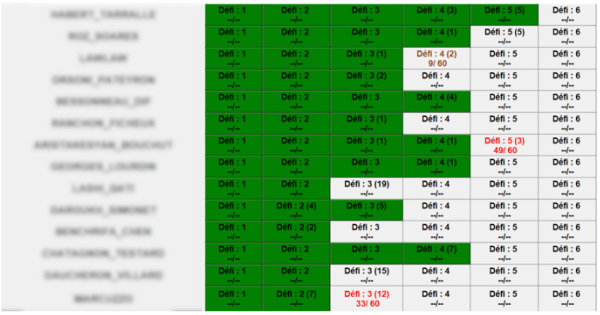
---------- Informations sur le Hack ----------

étailles succinctement dans cette partie votre analyse et la méthode utilisée

---------- Proof of Concept ----------

ode Python utilisé pour réaliser l'attaque.

Figure 3 : Challenge de sécurité —Utilisation de Moodle pour donner les directives et le cadre de travail.



Défi : 1 -/-	Défi : 2 -/-	Défi : 3 -/-	Défi : 4 (3) -/-	Défi : 5 (5) -/-	Défi : 6 -/-
Défi : 1 -/-	Défi : 2 -/-	Défi : 3 -/-	Défi : 4 (1) -/-	Défi : 5 (5) -/-	Défi : 6 -/-
Défi : 1 -/-	Défi : 2 -/-	Défi : 3 (1) -/-	Défi : 4 (2) 9/ 60	Défi : 5 -/-	Défi : 6 -/-
Défi : 1 -/-	Défi : 2 -/-	Défi : 3 (2) -/-	Défi : 4 -/-	Défi : 5 -/-	Défi : 6 -/-
Défi : 1 -/-	Défi : 2 -/-	Défi : 3 -/-	Défi : 4 (4) -/-	Défi : 5 -/-	Défi : 6 -/-
Défi : 1 -/-	Défi : 2 -/-	Défi : 3 (1) -/-	Défi : 4 -/-	Défi : 5 -/-	Défi : 6 -/-
Défi : 1 -/-	Défi : 2 -/-	Défi : 3 (1) -/-	Défi : 4 (1) -/-	Défi : 5 (3) 40/ 60	Défi : 6 -/-
Défi : 1 -/-	Défi : 2 -/-	Défi : 3 -/-	Défi : 4 (1) -/-	Défi : 5 -/-	Défi : 6 -/-
Défi : 1 -/-	Défi : 2 -/-	Défi : 3 (19) -/-	Défi : 4 -/-	Défi : 5 -/-	Défi : 6 -/-
Défi : 1 -/-	Défi : 2 (4) -/-	Défi : 3 (3) -/-	Défi : 4 -/-	Défi : 5 -/-	Défi : 6 -/-
Défi : 1 -/-	Défi : 2 (2) -/-	Défi : 3 -/-	Défi : 4 -/-	Défi : 5 -/-	Défi : 6 -/-
Défi : 1 -/-	Défi : 2 -/-	Défi : 3 -/-	Défi : 4 (7) -/-	Défi : 5 -/-	Défi : 6 -/-
Défi : 1 -/-	Défi : 2 -/-	Défi : 3 (15) -/-	Défi : 4 -/-	Défi : 5 -/-	Défi : 6 -/-
Défi : 1 -/-	Défi : 2 (7) -/-	Défi : 3 (12) 33/ 60	Défi : 4 -/-	Défi : 5 -/-	Défi : 6 -/-

Figure 4 : Challenge de sécurité — Visualisation en temps-réel des résultats des défis.

Il y a N défis à résoudre de difficulté croissante. La validation et le contrôle de la réussite des défis sont traités automatiquement par un script Python conçu par les enseignants et présent sur leur ordinateur. Celui-ci joue le rôle de l'objet à attaquer et c'est un oracle qui est capable de comprendre les différentes attaques pour vérifier leur réussite. Durant la séance, les résultats des apprenants sont diffusés en temps-réel par une projection via un vidéoprojecteur (cf. *figure 1* et *4*).
Afin de créer une émulation durant ces challenges de sécurité des points sont attribués si les défis sont réalisés, mais aussi des points suite à un classement des groupes par rapport au temps qu'ils ont mis pour réussir un défi.
Cette notation possède un double intérêt :

- la notation du « défi réussi » permet d'évaluer les compétences intrinsèques des apprenants ;
- la notation « temps mis » permet d'évaluer la réactivité (indispensable en sécurité informatique), mais surtout cela empêche la diffusion des résultats entre chaque groupe en créant une compétition saine.

Pour que ces challenges puissent se dérouler dans un cadre serein et éviter toute impasse pour les étudiants, des garde-fous sont mis en place :

- Du travail préparatoire est demandé avant la séance sur des thèmes particuliers pour que les étudiants possèdent des éléments de bases. En pratique cela prend la forme de plusieurs fonctions Python qui doivent réussir plusieurs tests unitaires ;
- Afin d'éviter des attaques « aléatoires » ou en brute force, une notion de *blacklist* est mise en place. Une mauvaise attaque, c'est-à-dire, qui n'a pas réussi va empêcher des attaques durant 60 secondes. Sur la figure 3, les groupes qui sont mis en liste noire peuvent le voir à travers le code couleur : le défi est écrit en rouge avec un compteur visible (cf. *figure 4*). Cette contrainte est assez proche du monde réel car il existe des contremesures classiques qui se basent sur un nombre d'accès maximal ;
- Durant la séance, les groupes peuvent demander des indices aux enseignants en contrepartie de points, cela prend la forme de feuille de papier avec des éléments pour les aider dans leur réflexion.

3.2.2 Outil informatique de gestion des challenges

Le bon déroulé de ces séances repose sur la gestion sans failles du traitement automatique du challenge. Un programme informatique, codé en Python, permet de le faire.
Il a été développé en programmation orientée objet en respectant le concept MVC (Modèle-Vue-Contrôleur) afin de garantir une bonne maintenabilité et maintenance à moyen terme.
Les fonctionnalités de ce programme sont les suivants :

- <u>Généralités</u>
  - Interface multiplateforme ;
  - Le logiciel devra permettre de réaliser des scénarios de tests *off line* pour tester et valider les challenges/défis.
- <u>Gestion du challenge</u>
  - La gestion doit permettre un import et un export de challenge (format JSON) ;
  - Configuration du challenge par le choix des défis avec la notation associée et une configuration via des métadonnées ;

- Un export de l'avancé du challenge (note intermédiaire) vers l'IHM pour alimenter un tableau dynamique.

– Gestion des défis
  - Création/Suppression/Modification d'un défi ;
  - Un défi aura en charge la gestion d'un serveur (un broker MQTT ⇔ cible de l'attaquant) ;
  - Il génère une « activité » : une publication MQTT sur le broker simulant un envoi d'information d'un IoT (cible de l'attaquant) ;
  - Un « moniteur » réalisera le rôle d'oracle et validera ou non une attaque des utilisateurs. Il échangera avec le challenge ces informations par le calcul de l'avancement ;
  - Le « moniteur » journalise ses activités dans un fichier (format texte) afin de retrouver l'ensemble des avancés en cas d'arrêt impromptu de l'application ;
  - La création d'un nouveau défi génèrera un squelette de code que l'enseignant devra compléter pour créer son propre défi ;
  - Les défis gèrent de façon fine et précise les exceptions pour garantir la fiabilité du code et la bonne gestion des raisons de rejet : *blacklist* ou information des utilisateurs.

– Affichage des résultats
  - Tableau dynamique : intégration des défis résolus, en cours de résolution ou temporairement inaccessible (dû à une mauvaise attaque).

Ce programme est fonctionnel et il est déjà utilisé en pratique mais doit être robuste et sécurisé. En effet, ce cours a lieu avec un public averti et il ne doit pas être l'attaque des étudiants pour valider automatiquement leur défi sans le faire.
Cette approche a aussi un autre intérêt où les notes sont connues et peuvent être diffusés dès la fin de la séance. Ce point est très apprécié par les étudiants.

4 DISPOSITIF D'ÉVALUATION

Dans le cadre d'un projet d'innovation pédagogique il est nécessaire de concevoir un dispositif d'évaluation afin de voir, avec le plus objectivité possible, si le projet a des effets bénéfiques pour les apprenants.
Cette démarche est un outil d'amélioration continue dans la démarche classique du cycle PCDA *(plan-do-check-act*). Ce type d'approche est en cohérence avec nos obligations internes : certification ISO 9001-2015 et l'accréditation CTI (ou HCERES), où l'évaluation des formations et des enseignements est une démarche normale pour améliorer notre offre de formation.

4.1 Analyse quantitative de l'impact pédagogique

Une première démarche pour évaluer l'impact pédagogique de cette approche est purement quantitative. Dans notre établissement, le retour des étudiants se réalise par un groupe de travail (commission pédagogique) où les représentants des étudiants (délégués) et les enseignants font le point sur la qualité des cours et les points d'améliorations des enseignements. Ce groupe de travail est l'organe qui permet d'alimenter notre indicateur qualité ISO 9001-2015 dans le processus « former les étudiants » pour juger de la qualité des cours.
Ce cours s'est déroulé sur deux années universitaires et le retour des étudiants a été enthousiaste avec une émulation autour de faire un « jeu ». Notre approche de *serious games* a vraiment fonctionné. Nous avons eu certains mauvais retours où, pour certains étudiants, ce type de séances a créé un énorme stress car la forme est très différente des séances de cours classiques. Ce point nous a interpellé et cela nous a permis de comprendre que ce type d'approche permet aussi de travailler des compétences transversales, comme le travail dans une ambiance stressante et urgente. Ces compétences peuvent être plus qu'indispensable dans le monde de la sécurité informatique.

4.2 Analyse qualitative de l'impact pédagogique

Dans une deuxième démarche nous avons souhaité mettre en place une analyse qualitative de ces séances de challenge de sécurité.
Une démarche classique avec un groupe témoin (étudiant qui n'auraient pas suivi les challenges de sécurité) et un groupe test (étudiants qui auraient reçu la formation normale) n'aurait pas été éthique. Une autre démarche possible aurait été de comparer les résultats en termes de compétences acquises avant la mise en place des challenge de sécurité. Cependant cette approche n'est pas possible car les challenges ont été mis en place dès la première année de ce cours.
Nous avons donc décidé de mettre en place une évaluation en proposant un questionnaire d'auto-évaluation pour les étudiants sur une promotion avant et après les challenges de sécurité.
L'objectif est d'évalué des compétences techniques mais aussi transversales comme la gestion du stress, une recherche rapide et efficace de l'information, le travail en équipe (ici des binômes) dans l'urgence, …

4.2.1 Questionnaire d'auto-évaluation

Nous avons proposé aux étudiants 9 questions (cf. annexe 1) qui se décomposent en 3 groupes :

- G1 = Q1 à Q3 : questions sur les connaissances techniques (information, sécurité, mathématiques);
- G2 = Q4 à Q6 : questions sur les compétences transverses (stress, équipe, collaboration)
- G3 = Q7 à Q9 : questions sur l'approche pédagogique (utilisation des challenges, généralisation, enthousiasme).

Pour le choix et la forme des questions nous nous sommes appuyés sur les travaux de Côté et *al.* [4].

4.2.2 Résultats

Avec un effectif de 26 étudiants nous avons eu un taux de réponse de 73,08 % pour le questionnaire avant le premier challenge et de 92,31 % pour le questionnaire après les challenges. Sur la figure 5, on peut retrouver

l'ensemble des résultats bruts pour toutes les questions avant les challenges (figure 5a) et après les challenges (figure 5b). Les descriptifs exacts des questions et les réponses possibles sont détaillés dans l'annexe 1. Sur la figure 6, l'évolution moyenne des réponses est représentée. Pour la réponse la plus positive, on a attribué une valeur de 100 % et une décroissante linéaire jusqu'à la réponse la plus négatif à 0%.

4.2.3 Discussions

On peut observer sur la figure 6b une évolution globale et positive des réponses des étudiants aux 3 groupes de questions. Les apprenants ont senti une amélioration sur leurs compétences techniques (G1) et transverses (G2). Le concept des challenges est une approche qu'ils souhaiteraient voir diffuser dans d'autres enseignements (G3).

Si l'on regarde en détail l'évolution par questions sur la figure 6a, on peut observer certaines variabilités.

En effet, sur la question Q2 (« l'utilisation d'outils informatiques en lien avec la sécurité ») l'évolution a baissé. Cela peut s'expliquer par le fait que les étudiants sont peut-être arrivés avec une idée fausse de la sécurité et plus particulièrement sur la difficulté de mise en place d'un mécanisme sécurisé et ils ont pris conscience de cette difficulté après les challenges.

Pour la question Q5 (« aisance à travailler en équipe ») il y a une stagnation du taux de réponse. Il est vrai que les étudiants réalisent les challenges en binôme et c'est un cadre de travail très courant pour des étudiants en bac+4, donc on comprend que cela ne leur a pas apporté de nouvelles compétences.

Néanmoins, il y a une évolution importante du taux de réponse sur la recherche pertinente d'informations (Q1), la même en place de raisonnement (Q3) et surtout, chose que les enseignants attendaient, de travailler dans un environnement stressant (Q4).

5 PERSPECTIVES

L'outil informatique qui a été développé, peut être utilisé pour d'autres approches.

Une généralisation vers une version *on-line* (web) pourra être intéressante pour que les apprenants puissent réviser en dehors des séances de cours sans avoir à manipuler le matériel.

On peut aussi utiliser cet outil pour animer des ateliers pour la communication de l'établissement comme des portes ouvertes pour mettre en place des séances de CTF (*Capture The Flag*).

Une dernière utilisation serait de l'utiliser durant des séances de formation continue afin de challenger les apprenants sur une séance de jeu, non pas pour noter les personnes, mais pour créer une émulation et rendre plus dynamique les séances.

6 CONCLUSION

Nous avons présenté dans cet article la mise en place d'un cours de sécurité des objets connectés dans une formation d'ingénieur en informatique (au niveau Bac+4), sur une spécialité « Réseaux et Sécurité Informatique » et plus particulièrement les modalités de contrôle de connaissances.

Cet enseignement introductif à la sécurité comporte différents aspects techniques et scientifiques : initiation à l'informatique embarquée et à ses contraintes, initiation à la chaîne de sécurité et à la sécurité des objets connectés.

Les enseignants ont choisi d'utiliser une pédagogie basée sur l'échec productif où régulièrement le système mis en place par les étudiants est mis en défaut par l'exploitation d'une faille de sécurité. Afin de cadrer l'intégration des connaissances, les enseignants ont utilisé le principe de la classe inversée pour structurer le contenu du cours et éviter de dériver vers « bricoler » une solution et avoir une approche plus scientifique. Afin d'inciter les étudiants à adhérer à la classe inversée, des évaluations régulières sont réalisées par l'utilisation des QCM et la mise en phase de deux challenges de sécurité. La notation particulière des challenges a permis d'obtenir une ambiance de compétition durant ses séances et a créé une adhésion des étudiants à cette évaluation.

Le dispositif d'évaluation de l'approche pédagogique a mis en évidence un sentiment de montée en compétences sur des thèmes transverses : recherche d'information et travailler dans un environnement stressant mais a aussi montré aux apprenants la difficulté de mise en place de processus sécurisé.

BIBLIOGRAPHIE

[1] Kapur M., "Productive failure", *Cognition and Instruction, Vol. 26, pp. 379–424, 2008.*

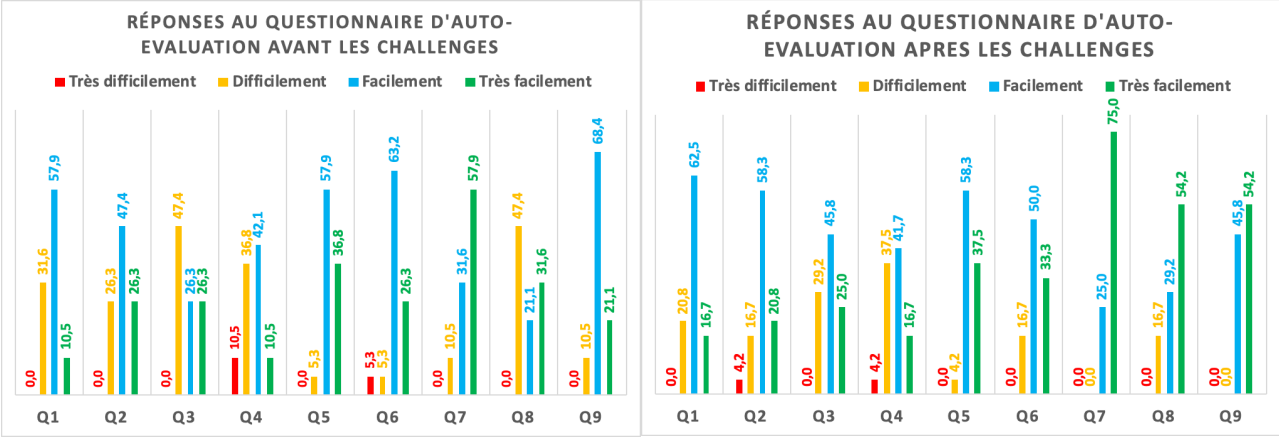
[2] Tawfik, Andrew A., Rong, Hui, & Choi, Ikseon. "Failing to learn: towards a unified design approach for failure-based learning", *Educational Technology Research and Development, Vol. 63 (6), pp. 975-994, 2015.*

[3] Tilmant C., Laffont J., "Pédagogie innovante pour l'enseignement de la sécurité des objets connectés", *Actes du 13ième Colloque de l'Enseignement des Technologies et des Sciences de l'Information et des Systèmes (CETSIS 2018), Fes, (Maroc), Octobre 2018, pp. 104 – 108.* https://cetsis2018.sciencesconf.org/conference/cetsis2018/livre_des_actes.pdf

[4] Côté R., Tardif J., "Élaboration d'une grille d'évaluation", *Atelier pédagogique à l'intention des enseignants universitaires. Québec : Groupe ECEM, 2011.* http://reseauconceptuel.umontreal.ca/rid=1MHHC8VF9-1BVD5FD-2VF3/ED0220a%20%C3%89laboration%20d%27une%20grille%20d%27%C3%A9valuation.pdf

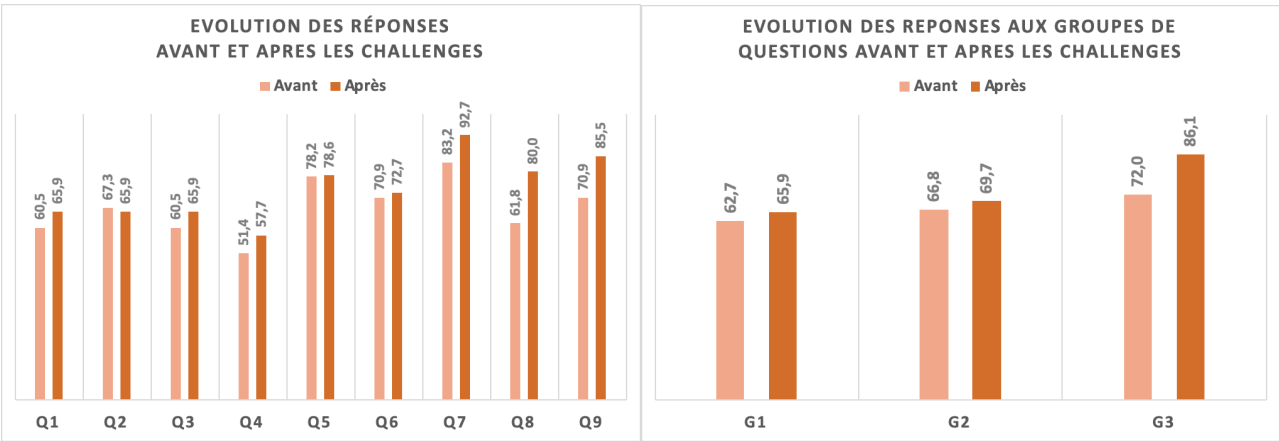
REMERCIEMENTS

Les auteurs remercient l'Agence nationale de la recherche du gouvernement français pour le soutien reçu dans le cadre du programme « Investissements d'Avenir » (16-IDEX-0001 CAP 20-25).



(a) (b)

Figure 5 : Taux de réponse en pourcentage des questionnaires d'auto-évaluation des apprenants avant (a) et après (b) les challenges. Les questions 1 à 9 (Q1 à Q9) ainsi que les valeurs de réponses sont décrites en annexe 1



(a) (b)

Figure 6 : Évolution du taux de réponse en pourcentage avant et après les challenges pour toutes les questions (a) et pour les groupes de questions (b).

ANNEXE 1 : QUESTIONS DE L'AUTO-EVALUATION

	Questions	Réponses possibles			
Q1	Comment évaluez-vous votre aisance à trouver facilement et rapidement des informations pertinentes ?	Très difficilement	Difficilement	Facilement	Très facilement
Q2	Comment évaluez-vous votre aisance à l'utilisation d'outils informatiques en lien avec la sécurité ?	Très difficilement	Difficilement	Facilement	Très facilement
Q3	Comment évaluez-vous votre aisance à mobiliser des raisonnements et des outils mathématiques ?	Très difficilement	Difficilement	Facilement	Très facilement
Q4	Comment évaluez-vous votre aisance à travailler efficacement dans un environnement stressant ?	Très difficilement	Difficilement	Facilement	Très facilement
Q5	Comment évaluez-vous votre aisance à travailler en équipe ?	Très difficilement	Difficilement	Facilement	Très facilement
Q6	Comment évaluez-vous votre aisance à répartir les tâches et à collaborer ?	Très difficilement	Difficilement	Facilement	Très facilement
Q7	Pensez-vous qu'une évaluation basée sur des challenges de sécurité est pertinente ?	Pas du tout	Un peu	Plutôt pertinent	Très pertinent
Q8	Pensez-vous que ce type d'évaluation soit intéressante dans le cadre d'autres enseignements ?	Pas du tout	Probablement pas	Plutôt	Tout à fait
Q9	Quel est votre sentiment sur l'évaluation par challenge de sécurité ?	Très négatif	Négatif	Positif	Très positif