Pédagogie innovante pour l'enseignement de la sécurité des objets connectés

Christophe Tilmant, Jacques Laffont

Pédagogie innovante pour l'enseignement de la sécurité des objets connectés

Christophe Tilmant [1], Jacques Laffont [2]
Christophe.tilmant@uca.fr, jacques.laffont@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

RÉSUMÉ : Dans le cadre de la mise en place d'un nouveau cours sur la sécurité des objets connectés, les enseignants ont utilisé une approche pédagogique différente pour aborder ce thème. Ce cours a lieu au début d'une formation en informatique avec une spécialisation en sécurité informatique. Les enseignants ont décidé de mettre en œuvre la pédagogie par échec productif qui a démontré un intérêt certain comme un enseignement introductif tout en permettant une meilleure intégration des connaissances. En complément et pour éviter une dispersion des étudiants pour résoudre les problèmes, les enseignants ont rajouté, entre autres, des évaluations sous forme de challenges de sécurité.

Mots clés : objets connectés, sécurité, échec productif, classe inversée, plateforme pédagogique Moodle.

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 (*Internet of Things* - IoT). L'objectif du cours en tronc commun est de permettre aux étudiants d'assimiler les bases de la technologie IoT et de se rendre compte de la pluralité des solutions possibles pour mettre en place des technologies connectées. Ces interventions sont réalisées par des intervenants extérieurs, experts du domaine et illustrent leurs cours par des cas industriels concrets.
Cet article s'intéresse aux travaux pratiques sur la sécurité des objets connectés correspondant à un volume horaire de 22 h (11x2 h) de formation en présentiel.
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.
De façon très classique, le fond de ce cours se base sur la présentation du principe de sécurité en profondeur avec un durcissement sur plusieurs niveaux :

- Au niveau réseau : en protégeant la sécurité physique du réseau utilisé ;
- Au niveau transport : utilisation de SSL en tenant compte du problème de déploiement de certificats côté client ;
- Au niveau applicatif : une authentification applicative simple, un chiffrement des données au niveau applicatif, le problème du cloisonnement entre utilisateurs ;
- Au niveau matériel : accès à la mémoire et au protocole de communication entre périphériques.

Le matériel et les logiciels utilisés sont volontairement classiques et « grand public ». Le système matériel est constitué d'une carte Genuino 101 pour la partie contrôle/commande et d'un module ESP8266 pour la communication WIFI (cf. figure 1). Les logiciels utilisés sont l'environnement de développement Arduino et le protocole MQTT.

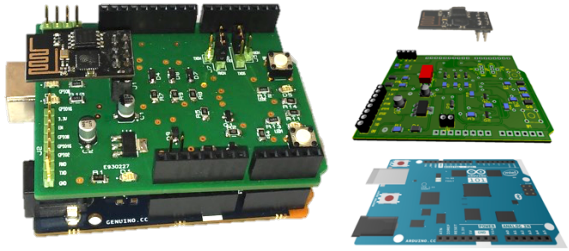

figure 1 : Matériel utilisé pour travailler sur la sécurité d'un objet connecté : carte Genuino 101 + carte fille intégrant des capteurs + ESP8266

À partir de cette base et à chaque séance de cours, les 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.
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 par des formations directement liées au sujet pour avancer.
Il a était 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. 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.

figure 2 : Organisation pédagogique du cours basé sur le durcissement d'un objet connecté

Un des inconvénients de cette approche est que certains étudiants pourraient se complaire à « bidouiller » sans réellement comprendre, c'est pour cela que les enseignants doivent bien organiser le cours avec des objectifs clairs et en proposant des activités d'évaluation obligeant les étudiants à intégrer les connaissances.
Une originalité de cet enseignement est son évaluation sous forme de challenges. Deux challenges de sécurité sont mis en place où les étudiants doivent pirater eux-mêmes des systèmes fournis. La notation est directement liée au nombre de challenge résolu, mais aussi à la vitesse de résolution.

2 ARCHITECTURE DU COURS

2.1 Organisation des séances

Cette formation est constituée de 11 séances de travaux pratiques de 2 h en enseignement présentiel. Les séances sont organisées en plusieurs parties (cf. figure 2) :

- 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 complètent ce processus. Plusieurs QCM permettent de valider l'acquisition de savoir par une approche de pédagogie inversée et des séances de challenges de sécurité, où les étudiants se mettent à la place de l'attaquant, permettent d'évaluer le savoir-faire des apprenants.

Voici le plan des 11 séances :

1- Introduction — Mise en place de la plateforme de développement sous Arduino ;
2- QCM —Introduction au protocole MQTT — Échange de messages avec un *broker* public ;
3- Mise en place de l'application IoT/MQTT sur Arduino ;
4- QCM —Chaîne de sécurité MQTT ;
5- Challenge de sécurité n° 1 ;
6- Camouflage des informations et authentification pour faire suite au débriefing du challenge 1 ;
7- QCM – Analyse réseau avec *tcpdump* et chiffrement ;
8- QCM – Chiffrement symétrique AES
9- Chiffrement du *payload* et mise en œuvre sur Arduino
10- Challenge de sécurité n° 2 ;
11- Mise en œuvre SSL et sécurité bas-niveau : utilisation du *sniffeur* de bus BusPirate.

2.2 Technologies employées

La partie communication utilise le protocole MQTT [3] qui utilise une architecture « publish/subscribe ». L'élément central de la communication est le *broker* MQTT responsable du relais entre les messages des émetteurs et les clients. Chaque client s'abonne via un message vers le *broker* : le « topic » qui permettra au broker de réémettre les messages reçus des producteurs de données vers les clients. Les clients et les producteurs n'ont ainsi pas à se connaitre, ne communiquant qu'au travers des topics.
L'organisation matérielle de ce cours est décomposée en deux parties (cf. figure 3). Chaque apprenant peut utiliser un objet connecté qui utilise un module Wifi afin d'utiliser le protocole MQTT. Le *broker* MQTT est mis en place par les enseignants à l'aide d'une machine virtuelle où la solution Mosquitto [3] est utilisée. Ce *broker* est aussi accessible de l'extérieur afin de récupérer les données pour un affichage graphique via un *dashboard*.

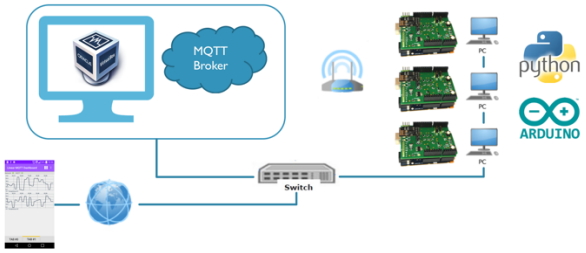

figure 3 : Organisation de la partie matérielle

Afin de réaliser ce cours, les apprenants doivent avoir des prérequis sur l'utilisation du langage Python et du langage C (afin d'aborder facilement le langage Arduino).

2.3 Évaluation du cours

L'évaluation de ce cours est décomposée en deux parties :

- Réalisation de 4 QCMs en début de cours afin de contrôler la bonne compréhension des concepts par les apprenants via l'approche de la pédagogie inversée. Ces QCM durent environ 5 minutes et sont corrigés automatiquement via la plateforme Moodle [5]. Cette correction en temps-réel permet aux enseignants de rebondir sur les points qui n'ont pas été compris par les étudiants et de prendre le temps nécessaire à une explication afin que les travaux pratiques puissent commencer sur de bonnes bases ;
- Réalisation de 2 challenges de sécurité qui permettent d'évaluer le savoir-faire des apprenants sur l'exploitation des failles de sécurité : une bonne compréhension de ces notions est nécessaire pour mettre en place des correctifs (*ethical hacking*).

Par la suivante nous allons détailler uniquement un des deux challenges de sécurité qui sont tous les deux très proches sur leur forme et sur leurs objectifs.

L'objectif du challenge est d'être capable d'allumer les LEDs de l'objet connecté du professeur en arrivant à trouver des failles de sécurité dans le système mis en place.

Le cadre de travail est bien défini pour éviter une dispersion des moyens employés par les apprenants. Ils sont invités à utiliser l'outil *tcpdump* [6] et à analyser les *payload* échangés entre la carte du professeur et le broker MQTT (cf. figure 4).

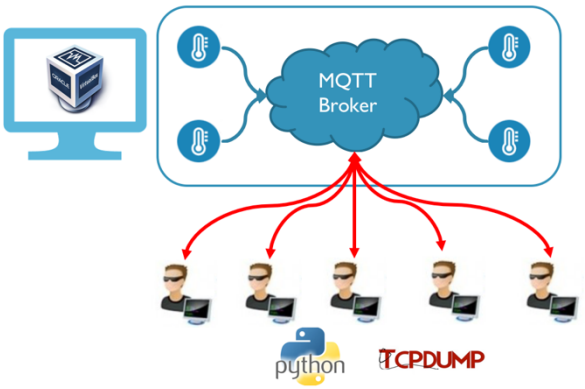

figure 4 : Challenge de sécurité — Cadre de travail. Les apprenants utilisent Python et tcpdump afin de trouver des failles de sécurité dans l'objet mis à disposition.

Ce challenge est décomposé par des défis qui sont valorisés par des points :

1. Récupération sur une communication non-sécurisée des paramètres d'authentification ;
2. Réussite par un simple rejet ;
3. Dix messages sont émis à tour de rôle : envoyer le bon ;
4. Chiffrement AES avec une clef de 2 bytes ;
5. Chiffrement AES avec une clef de 128 bits.

L'ensemble des éléments du challenge et des défis se retrouve sur une page du cours en ligne de la plateforme Moodle (cf. figure 5).

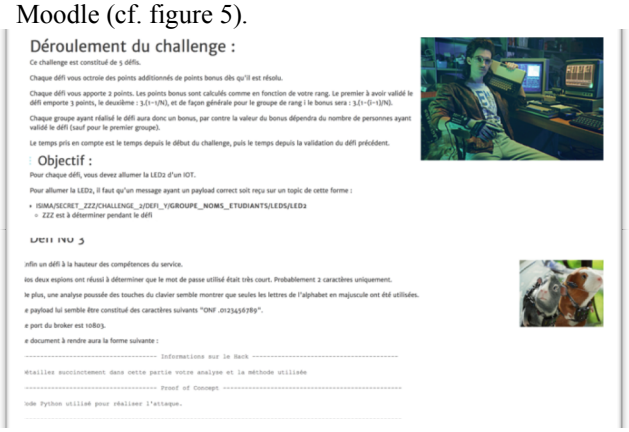

figure 5 : Challenge de sécurité — utilisation de Moodle pour donner les directives et cadre de travail.

La validation et le contrôle de la réussite des défis sont traités automatiquement par un script Python présent sur l'ordinateur des enseignants. Cela permet de diffuser en temps-réel les résultats des apprenants par une projection via un vidéoprojecteur (cf. figure 6).

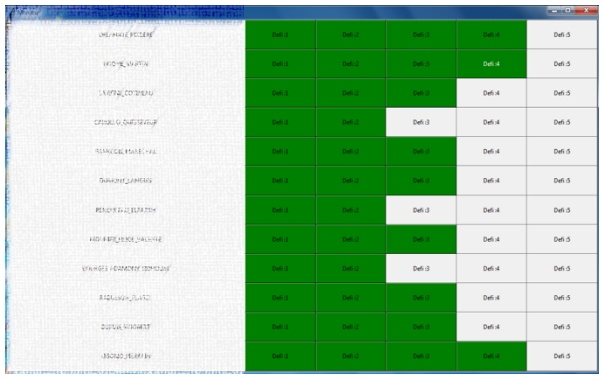

figure 6 : Challenge de sécurité — Visualisation en temps-réel des résultats des défis

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 ;
- 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.

2.4 Pédagogie employée

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.

Durant les séances de présentiel, on se concentre sur l'apprentissage du savoir-faire et les enseignants utilisent la pédagogie 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, les QCM sont ici pour pousser 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 rythmer les séances de cours.

3 RETOUR D'EXPERIENCE

La démarche d'évaluation des enseignements dans la structure où se déroule ce cours est réalisée par une réunion appelée « commission pédagogique » mise en place par le processus de la démarche qualité (ISO 9001-2015). Cette réunion rassemble les enseignants et les délégués des classes concernées. Les étudiants font remonter les avis sur les enseignements afin de participer à l'amélioration continue de la formation. Ce retour est un retour informel sous la forme d'un compte-rendu de ces avis.
Suite à la réalisation de ce cours (qui s'est déroulé qu'une seule fois pour l'instant), cette approche créée un réel enthousiasme dans l'implication des étudiants dans les challenges avec un bon esprit compétitif où les étudiants se challengent entre eux en oubliant la partie notation. Les premiers retours de ce cours sont très positifs : un réel enthousiasme des apprenants, un apprentissage basé sur le jeu où la correction des « erreurs » (failles de sécurité) est un moment d'apprentissage : *serious game*.

4 CONCLUSION

Nous avons présenté 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 ».
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 IoT.
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.
Les premiers retours informels sur cet enseignement sont très positifs avec un sentiment de montée en compétences.

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] MQTT community. MQTT homepage. http://mqtt.org/. Page d'accueil organisation MQTT.
[4] Eclipse Mosquitto —An open source MQTT broker, https://mosquitto.org. Page d'accueil Eclipse Mosquitto.
[5] Dominique Bouillet, Marie-Christine Monget. De l'usage des quiz dans Moodle : retours d'expériences et questions posées. MoodleMoot 2009 : 5e conférence annuelle des utilisateurs francophones de la plateforme Moodle d'apprentissage en ligne, Jun 2009, Lyon, France.
[6] Tcpdump.1. Tcpdump.org. 20 May 2004, http://www.tcpdump.org/tcpdump_man.html, Stevens, Richard W. TCP/IP Illustrated, Volume 1. Boston: Addison-Wesley, 1994.