Internet des objets connectés : Challenges de sécurité (SecIoT)

Porteur de projet	Christophe TILMANT
Établissement, composante, laboratoire	Institut d'Informatique - ISIMA
Date de début du projet (conception)	01/01/2019
Date de déploiement	01/09/2019
Mots clés	IoT, Sécurité, Challenges, Savoir-faire, Connaissances, Serious game, Evaluation

Résumé :

Dans le cadre de la formation à la sécurité informatique au sein de l'ISIMA (UCA), un cours en présentiel sur la sécurité des objets connectés (IoT) va être mis en place. Le projet vise à développer des situations fictives d'attaques informatiques que les étudiants devront parer le plus rapidement possible (jeu sérieux en groupe).

Descriptif global :

Une modalité de contrôle de connaissances "classique" (examen écrit ou compte rendu de TP par contrôle continu) n'est actuellement pas pertinente pour évaluer les compétences développées par les étudiants. En effet, les compétences en sécurité informatique s'appuient sur du savoir-faire (fondé sur de l'expérience et de l'intuition), une culture informatique en perpétuelle évolution et non sur des protocoles préétablis et/ou figés dans le temps.

Dans ce contexte, les challenges de sécurité sont des moyens efficaces pour contrôler les connaissances et compétences des étudiants à l'épreuve de situations authentiques d'attaques informatiques et qui ont fait leurs preuves (Hackathons).

Pour cela, des challenges de sécurité seront mis en place durant les séances d'évaluation en répondant à un cahier des charges bien défini. Les parcours d'attaque seront automatisés et gérés informatiquement (projection en temps-réel des attaques). Cette approche par "jeu" (serious game) créera une émulation auprès des étudiants.

Ce que LIA finance :

Des moyens humains : Un stagiaire pour une période de 4 mois et des heures complémentaires pour les enseignants impliqués dans le projet (120 éq.TD).
Soit un total de 7633€.