Projets pour l'enseignement de la sécurité

Julien Iguchi-Cartigny (julien.iguchi-cartigny@univ-lille1.fr) *

1 Projets

La présentation portera sur le retour d'expérience de plusieurs projets développés dans le Master CRYPTIS depuis 2005 et de projets en cours de développement.

Audits réels (depuis 2005) : plusieurs projets ont consisté à l'audit d'installation réelle de partenaires (laboratoires publics, entités de l'enseignement supérieur, start-ups, PME, etc.). Ce format permet d'offrir un environnement plus riche pour réaliser un audit (réseau ou web), mais demande par contre la mise en place de canaux de communication avec l'entité à auditer, de poser une base juridique, d'identifier le périmètre de l'audit et dans la mesure du possible d'isoler l'infrastructure cible. De plus, un travail d'explication avec l'entité auditée et les étudiants est nécessaire, notamment vis-à-vis des effets de bord potentiels durant l'audit (scan automatique surchargeant l'installation, risque de dysfonctionnements difficiles à identifier, etc.).

Écriture d'exploits (depuis 2009) : de nombreux enseignements se concentrent sur l'étude de failles déjà connues. Une approche développée par les cours dispensés par Frédéric Raynal est l'écriture d'exploits de failles connues (disponibles dans la base CVE) mais dont il n'existe aucun exploit public. Ce type de projet donne aux étudiant une bonne idée de la difficulté réelle d'exploitation de vulnérabilités (difficulté augmentant d'année en année), mais nécessite des collaborations extérieures et un canal de communication sûr durant l'identification des failles exploitables et durant l'évaluation de l'exploit.

Développement d'une salle réseau / serveur avec accès public à Internet : Il est très difficile pour les étudiants d'accéder à une vraie vision des problèmes de déploiement de système et de réseau sur Internet. De plus, il existe de nombreuses activités qui demandent un accès réel à Internet (étude du trafic entrant et sortant, filtrage, caractérisation des attaques externes en permanence, installation de *honeypot* pour la capture et l'analyse d'attaques réels). La disponibilité d'une telle installation est très difficile, au vu des restrictions appliquées par les universités ou écoles sur leur réseau interne. Les possibles pistes (réseau dédié et isolé hors des plages de l'entité hébergeante, déploiement dans le *cloud*) ainsi que les contraintes légales seront discutés.

"Eat your own dog food" : Ce projet s'articule autour des outils pour aider au développement sécurisé (test unitaire et fonctionnel, analyse statique, bibliothèque dédiée) et sur l'évaluation de logiciel. L'idée est de proposer un projet s'articulant autour d'un cycle de développement puis d'évaluation. Dans un premier temps, les étudiants développent une application basée sur une spécification d'un protocole accessible par le réseau. Puis une itération consiste à développer des tests fonctionnels et des outils de fuzzing pour évaluer la sécurité des premières implémentations et d'explorer les possibilités d'exploitation des failles trouvées. Ce développement en cycle permet de renforcer la sécurité du

*. Université de Lille 1

développement au fur et à mesure.

2 A propos du Master CRYPTIS

Le Master CRYPTIS (`www.cryptis.fr`) est un master de sécurité de l'information créé en 1986. D'abord orienté sur la cryptographie, il est accompagné depuis 2000 par un DESS puis Master de sécurité informatique. Les deux Masters sont adossés adossé aux équipe de recherche en cryptographie (PICC) et carte-à-puce (SSD) du laboratoire XLIM (`www.xlim.fr`).

Le Master propose aux deux parcours (mathématique et informatique) une approche pluri-disciplinaire avec un certain nombre de modules communs (cryptographie, carte à puce, certification) permettant l'ouverture de nouveaux débouchés aux deux parties. De plus, le master de sécurité informatique propose une formation pointue incluant de nombreux aspects de sécurité offensive et défensive (système, réseaux et web), avec la présence de nombreux intervenants extérieurs.

Depuis 25 ans, plus de 580 diplômés ont intégré les secteurs d'activités suivants :

— Conseil/service/intégration en sécurité de l'information
— Doctorat (cryptologie ou sécurité informatique)
— Ministères (Défense, Intérieur,...)
— Développement logiciels de confiance
— Administration sécurité système et réseaux
— Industrie des cartes à puces
— ...