Enseignement de la sécurité numérique : De la sensibilisation à l'expertise

F. Bruguier, P. Benoit, L. Torres

LIRMM et pôle CNFM de Montpellier, Université de Montpellier, Montpellier, France
Contact email : florent.bruguier@umontpellier.fr

Avec l'avènement de l'internet des objets, les dispositifs électroniques sont omniprésents dans nos vies. Cette omniprésence implique une augmentation des failles de sécurité (vol de données ou d'identité, prise de contrôle d'équipements sensibles…). Pour parer à ces vulnérabilités, deux méthodes complémentaires doivent être mises en place en parallèle. Il est nécessaire de sensibiliser les utilisateurs afin d'éviter les comportements à risque mais aussi de créer des objets plus sécurisés en formant les ingénieurs de demain à ces problématiques. Dans ce contexte, le pôle CNFM de Montpellier a mis en place un programme de formation en sécurité numérique. Ce programme est composé de 4 formations s'adressant à des étudiants du lycée au doctorat en passant par la formation continue. Ce papier présente ces 4 formations qui nous ont permis de former plus de 800 étudiants depuis 2014.

I. Introduction

De nos jours, nous utilisons de plus en plus de systèmes numériques. Ceci est d'autant plus vrai avec l'avènement des objets connectés. Ces objets nomades ou embarqués constituent ce que l'on appelle l'internet des objets[1]. Ils modifient les habitudes des utilisateurs et répondent à des besoins nouveaux dans de nombreux domaines tels que l'audiovisuel, la santé, le tourisme ou encore les transports… Leur nombre est estimé aujourd'hui à 15 milliards et devrait monter à plus de 25 milliards dans le monde en 2020 [1].

Néanmoins, cette omniprésence accroit les chances d'exposition des utilisateurs. Frigos, voitures, jouets ou dispositifs médicaux connectés…, les exemples d'objets ayant des failles ne cessent d'augmenter [2]–[4].

Les implémentations matérielles et logicielles de tels systèmes sont devenues leur principal talon d'Achille. En effet, l'analyse de paramètres physiques tels que la consommation électrique, les émissions électromagnétiques ou encore le temps d'exécution peuvent être utilisés pour les attaquer. Ces attaques, appelées attaques par canaux cachés, permettent en un minimum de temps et avec peu d'effort de découvrir les clés de chiffrement utilisées pour la sécurité de ces circuits.

Pour s'adapter à ce type de menaces, il est nécessaire d'éduquer les nouvelles générations d'utilisateurs. En effet, l'erreur humaine est une des plus grosses vulnérabilités d'un système et il est facile d'y remédier juste en changeant les habitudes. De plus, il est nécessaire de former les concepteurs et développeurs de tels objets. Ils doivent être au fait de l'importance de la sécurité mais aussi du fait qu'il faut penser la sécurité dès la phase

[1] Internet of things (IoT)

Article publié par EDP Sciences et disponible sur le site https://www.j3ea.org ou https://doi.org/10.1051/j3ea/20171004

initiale de conception d'un produit. Les objets doivent être « sécurisés à la conception » et non pas mis à jour à chaque découverte de faille…

Dans ce contexte, le pôle CNFM[2] de Montpellier a décidé de développer un programme de formation autour de la sécurité numérique. Ce papier décrit ce programme de formation. Il est constitué de 4 cours balayant des publics du lycée au doctorat en passant par la formation continue. La suite de l'article est organisée comme suit. Dans la section 2, une vue d'ensemble du programme est proposée. S'en suit une description des 3 principaux cours. Finalement les premiers résultats de ce programme de formation sont présentés.

II. Programme de formation

Afin de répondre à un manque d'offres de formation en sécurité numérique, nous avons décidé de développer un programme autour de cette thématique. L'objectif est d'offrir des connaissances en sécurité matérielle aux étudiants du lycée à la thèse. Il inclut également un module destiné aux ingénieurs en microélectronique souhaitant acquérir de nouvelles compétences. Quatre formations ont été développées et chacune d'entre elle s'adresse à une audience spécifique et possède ses propres objectifs pédagogiques (Tableau I).

TABLEAU I. Formations développées.

Formation	Public cible	Durée	Lieu
Sensibilisation	Lycéens / étudiants de Licence	1 heure	Sur site
Conférence spécialisée	Etudiants de Master	3 heures	Sur site
Stage technologique	Etudiants de Master / doctorants	3 jours	Montpellier
Formation continue	Ingénieurs microélectronique	2-3 jours	Montpellier

Les différentes formations seront détaillées dans les prochaines parties à l'exception de celle sur la formation continue. En effet, cette formation présente le même programme que le stage technologique. La principale différence est qu'en fonction des attentes du public, il est possible d'adapter le programme. Ce cours dédié à des ingénieurs micro-électroniciens leur permet d'améliorer leurs connaissances en cryptographie et sécurité. Certaine sessions spéciales sont aussi organisées pour les enseignants et enseignants chercheurs souhaitant étendre leur domaine de compétences.

III. Sensibilisation

Cette formation a pour objectifs de présenter les principes de la cryptographie. Elle cherche à rendre les étudiants conscients des problèmes de sécurité dans la vie de tous les jours mais aussi réaliser l'importance des mathématiques, des sciences physiques et de l'électronique pour résoudre ces problèmes. La possibilité d'utiliser les canaux cachés comme la consommation électrique ou les émissions électromagnétiques pour trouver la clé de chiffrement d'un système crypté est aussi introduit. Le Tableau II présente les différentes séquences constituant cette formation.

Cette formation peut être effectuée en lycée mais aussi dans n'importe quelle licence scientifique. Puisque les étudiants n'ont aucune expertise dans ce domaine, la principale crainte pédagogique est de ne pas proposer un contenu suffisamment abordable. La seconde est de garder les étudiants alertes tout au long du cours sachant que ce dernier ne fait pas partie intégrante de leur cursus. Ce cours peut être adapté pour introduire les concepts de

[2] Coordination Nationale de Formation en Microélectronique et nanotechnologies

la sécurité numérique à des professionnels. Ce cours dure une heure. Puisqu'il ne requiert pas de support particulier, ce cours peut être donné n'importe où par un de nos formateurs.

TABLEAU II. Programme de la formation « Sensibilisation »

Séquence	Résumé	Durée
Introduction	Exemples de failles de sécurité.	6 minutes
Code de César	Exemple didactique pour comprendre le code de César.	8 minutes
Recherche de clé secrète	Interaction avec les étudiants qui donnent leurs idées pour trouver une clé secrète codée avec le code de César.	9 minutes
Chiffre de Vigenère	Extension du code de César en vue d'améliorer sa sécurité.	6 minutes
Vidéo	Vidéo introduisant la machine Enigma. Transition vers la cryptographie moderne.	8 minutes
Cryptographie moderne	Concepts de substitution et transposition. Notion de clés publiques et privées [5]	5 minutes
Cartes de crédit	Principe des transactions et exemples de failles de sécurité [6]	9 minutes
Analyses par canaux cachés	Principe des analyses par consommation et émissions électromagnétiques	9 minutes

IV. Conférence spécialisée

L'audience de cette conférence de trois heures est composée d'étudiants de Master en microélectronique et de doctorants non-experts. Ce dernier permet aux étudiants de comprendre les challenges de la société digitale et plus particulièrement les dangers et contremesures de la sécurité numérique. Ce cours de trois heures peut être donné partout en France dans le sens où il ne requiert pas d'équipements spécifiques.

Plus en détails, ce cours est divisé en deux principales parties comme résumé dans le Tableau III. La première permet de faire une introduction générale des problématiques de la sécurité tout en montrant le fonctionnement d'algorithmes de chiffrement moderne. La seconde est plus spécifique et se focalise sur les attaques physiques. Les attaques par analyse de la consommation électrique et des émissions électromagnétiques sont abordées plus en détails.

TABLEAU III. Programme de la formation "conférence spécialisée".

Séquence	Résumé	Durée
Partie 1		
Introduction	Exemples de failles de sécurité	6 minutes
Définitions	Définitions : cryptologie, cryptographie, cryptanalyse. Concept de clé secrète	12 minutes
Challenges	Challenges du monde numérique et de sa sécurité	12 minutes
Histoire	Code de César, Chiffre de Vigenère, Scytale et machine Enigma	10 minutes

Cryptographie moderne	Concepts de substitution et de transposition. Notions de clés privées et publiques. Principes de Kerckhoffs [5]	15 minutes
DES [7]	Principes et faiblesses	14 minutes
AES [8]	Principes et avantages par rapport au DES	12 minutes
RSA [9]	Fonctionnement de cet algorithme asymétrique	9 minutes
Partie 2		
Attaques physiques	Tour d'horizon des attaques invasives, semi-invasives et non-invasives [10]	14 minutes
Consommation statique des circuits CMOS	Modèles de consommation des circuits CMOS	10 minutes
Attaques en consommation	Principe des attaques par analyse de la consommation (SPA, DPA, CPA) [11]	20 minutes
Attaques électromagnétiques	Principe des attaques par analyse des émissions électromagnétiques (DEMA et CEMA) [12]	12 minutes
Exemples d'attaques	Exemples d'attaques sur des mesures de consommation (carte à puce et FPGA)	15 minutes
Contremesures	Tour d'horizon des contremesures existantes	19 minutes

V. Stage technologique

Le stage technologique est un cours spécialisé. Il est dédié aux étudiants de Master et d'école d'ingénieurs en microélectronique et systèmes embarqués ainsi qu'aux doctorants non-spécialistes du domaine. En plus de permettre aux étudiants de comprendre les challenges de la société digitale, ce cours leur permet d'assimiler les principes des systèmes de chiffrement. Ils peuvent mettre en œuvre certaines attaques par canaux cachés mais aussi utiliser un équipement de mesure électromagnétique dédié [13]. Enfin, une étude des principales contremesures est réalisée.

Le principal défi pédagogique à relever lors de ce cours est que le programme est très chargé. Afin de maximiser les chances de faire passer le message, il est primordial de juger du niveau des étudiants dès le début mais aussi de vérifier qu'ils maitrisent bien les prérequis nécessaires pour comprendre les concepts introduits.

Ce cours est donné au sein des locaux du pôle CNFM de Montpellier dans le sens où il requiert des équipements spécifiques qui ne peuvent pas être facilement déplacés vers un autre lieu. La plateforme de sécurité numérique SECNUM fait partie de ces équipements [15].

Ce stage technologique est en général organisé sur trois jours consécutifs. Il est divisé en 6 cours et 2 séances de travaux pratiques pour un total de 21 heures de formation. Le tableau IV décrit le programme détaillé de la formation.

Le point fort de ce cours est de fournir très rapidement les concepts de base en cryptographie mais aussi des connaissances sur les implémentations matérielles et les failles potentielles de tels algorithmes. Il permet aussi de mettre en pratique les mécanismes d'attaques et de contremesures sur des systèmes réels.

TABLEAU I. Programme de la formation "stage technologique".

Séquence	Résumé	Durée
Cours 1	Introduction à la société digitale et cryptographie : terminologie, définitions, histoire et techniques de substitution et de transposition	120 minutes
Cours 2	Présentation d'algorithmes de chiffrement symétriques et asymétriques : théorie et exemples pratiques (DES, AES, RSA)	120 minutes
Cours 3	Tour d'horizon des attaques physiques, focus sur les attaques par canaux cachés et plus particulièrement celles par analyse de la consommation	210 minutes
Travaux pratiques 1	Attaque différentielle par analyse de la consommation sur une implémentation logicielle d'un AES fonctionnant sur une carte à puce	210 minutes
Cours 4	Analyse des émissions électromagnétiques : principe, avantages et faiblesses	120 minutes
Travaux pratiques 2	Attaque corrélative par analyse des émissions électromagnétiques d'un crypto-processeur AES	270 minutes
Cours 5	Métriques de succès d'attaques et exemples basés sur les expérimentations du TP2	90 minutes
Cours 6	Contremesures pour les crypto-systèmes logiciels et matériels	120 minutes

VI. Conclusion

Au cours des deux années passées, nous avons effectué 18 différentes interventions : 6 sensibilisations, 8 conférences spécialisées, 3 stages technologiques et 1 formation continue. Nous avons sensibilisé ou formé pas moins de 800 personnes pour un total de plus de 2200 heures de formation. Le bilan est d'autant plus positif si l'on regarde d'une part les retours très positifs des évaluations laissées par nos étudiants et d'autre part l'engagement et la motivation des enseignants qui suite à notre formation enseignent à leur tour cette discipline.

Remerciements

Les auteurs remercient l'Agence Nationale de la Recherche (ANR) pour le support apporté grâce au financement ANR-11-IDFI- 0017 (projet IDEFI-FINMINA), et le GIP-CNFM porteur du projet FINMINA et qui a également soutenu l'introduction de cette nouvelle thématique dans le réseau national.

Références

1. Lund, D., MacGillivray, C., Turner, V., *et al.* : "Worldwide and regional internet of things (iot) 2014-2020 forecast: A virtuous circle of proven value and demand," International Data Corporation (IDC), May 2014, pp. 1-29

2. D. Dagon, T. Martin, and T. Starner : “Mobile phones as computing devices: The viruses are coming!” Pervasive Computing, IEEE, vol. 3, no. 4, pp. 11–15, 2004.
3. M. Wolf, A. Weimerskirch, and T. Wollinger : “State of the art: Embedding security in vehicles,” EURASIP Journal on Embedded Systems, vol. 2007, no. 1, pp. 1–16, 2007.
4. D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, *et al.* : “Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses,” in Security and Privacy, 2008. SP 2008. IEEE Symposium on.IEEE, 2008, pp. 129–142.
5. Kerckhoffs, A. : “La cryptographie militaire, ” Journal des sciences militaires, 1883, 9, pp. 161-191
6. Pele, L. : “French banking smartcard cracked : the story!”, http://www.parodie.com/english/smartcard.htm consulté le 20 September 2016
7. FIPS : “Data encryption standard,” in FIPS PUB 46, Federal Information Processing Standards Publication, 1977, 46-2
8. FIPS : “Advanced encryption standard (aes),” Federal Information Processing Standards Publication, 2001, 197
9. Rivest, R., Shamir, A., Adleman, L. : “Cryptographic communications system and method”, US Patent 4,405,829, September 20 1983
10. Tehranipoor M.,Wang, C. : “Introduction to hardware security and trust,” (Springer Science & Business Media, 2011)
11. Kocher, P., Jaffe, J., Jun, B., *et al.* : “Introduction to differential power analysis”, Journal of Cryptographic Engineering, 2011, 1, (1), pp. 5-27
12. Ordas, T., Lisart, M., Sicard, E., *et al.* : “Near-field mapping system to scan in time domain the magnetic emissions of integrated circuits”, Int. Work. Power and Timing Modeling, Optimization and Simulation, Lisbon, Portugal, September 2008, pp. 229-236
13. Bourrée, M., Bruguier, F., Barthe, L., *et al.* : “Secnum: an open characterizing platform for integrated circuits”, Euro. Work. Microelectronics Education, 2012, Grenoble, France, pp. 88-91.