Sujets de TER 2017-2018

1 Sujets proposés par Emmanuel Fleury

Contact : emmanuel.fleury@u-bordeaux.fr

1.1 Implementation d'un AES Whitebox

Éric SAGELOLI, Guillaume WAFO-TAPA

La cryptographie "whitebox" suppose que l'attaquant a un contrôle total de la mémoire et de l'exécution du logiciel, pourtant on veut pouvoir livrer un logiciel permettant de chiffrer un message sans laisser fuiter la clef de chiffrement. Un certain nombre de méthodes existent, mais celle qui a donné lieu à une implémentation sérieuse s'appuie sur les articles de Chow et al. L'idée est de faire une implémentation aussi poussée que possible de ces idées.

En suivant l'article "A Tutorial on White-box AES" de James A. Muir, concevez un programme qui puisse générer le code C d'un AES Whitebox avec une clef cachée dedans. Puis, implémentez une des méthodes d'attaque permettant d'extraire la clef (méthode BGE ou autres).

1.2 Spectre et Meltdown

Vincent Fournier, Alexandre MARUITTE

1.3 Isomorphisme de graphes en temps quasi-polynomial

Le problème de trouver un isomorphisme de graphes est un problème que l'on peut rencontrer dans de nombreux cas d'applications pour identifier les similitudes entre deux programmes. Récemment (2015), László Babai a proposé un algorithme qui propose une solution en temps quasi-polynomial. La preuve de cet algorithme a nécessité encore un certain nombre d'allers et retours avant que la communauté scientifique soit vraiment convaincue de sa véracité. Néanmoins, le but de ce projet est de tester les différentes méthodes connues pour construire un isomorphisme de graphes (total ou partiel) et de tester (si possible) l'algorithme proposé par Babai. À minima, nous espérons essayer d'avancer un peu sur la compréhension du problème et de l'algorithme qui a été proposé.

Référence :

- Graph Isomorphism in Quasipolynomial Time László Babai, 2015. `https://arxiv.org/abs/1512.03547`

1.4 Heap-overflow Exploitation in 2017

Le but de ce projet est de dresser un panorama des failles touchant la Heap et des techniques d'exploitations qui marchent encore en 2017. Le groupe devra étudier les articles de référence et tester les différentes failles en les exploitants sur des systèmes Linux relativement récents (Debian/Ubuntu/...). Le but de ce projet est d'arriver à une synthèse des techniques qui marchent encore et une compréhension du fonctionnement du malloc d'une libc6 récente.

Références :

- Malloc Des-Maleficarum blackngel, 2009 `http://www.phrack.org/issues/66/10.html`
- Yet another free() exploitation technique huku, 2009 `http://www.phrack.org/issues/66/6.html`

- The House Of Lore : Reloaded (ptmalloc v2,v3 : Analysis & Corruption) blackngel, 2009 http://www.phrack.org/issues/67/8.html
- Advanced Doug lea's malloc exploits jp, 2003 http://www.phrack.org/issues/61/6.html
- Vudo - An object superstitiously believed to embody magical powers Michel "MaXX" Kaempf, 2001 http://www.phrack.org/issues/57/8.html
- Once upon a free() anonymous, 2001 http://www.phrack.org/issues/57/9.html
- Heap overflow using Malloc Maleficarum sploitF-U-N, 2015. https://sploitfun.wordpress.com/2015/03/04/heap-overflow-using-malloc-maleficarum/
- how2heap, shellphish, 2017. https://github.com/shellphish/how2heap

2 Sujets proposés par Olivier Brinon

Contact : olivier.brinon@math.u-bordeaux.fr

2.1 L'algorithme de Berlekamp

Il existe des algorithmes simples pour factoriser les polynômes à coefficients dans un corps fini. L'algorithme de Berlekamp (et ses raffinements) en est un. En travaillant un peu, on peut en déduire un algorithme de factorisation dans $\mathbf{Q}[X]$.

Référence :

- von zur Gathen, Gerhard, Modern computer algebra, Cambridge (2003), 786p.

2.2 L'algorithme AKS

EL HERICHI Hafsa, MARTY Yoan, VEILLAT Emma

Agrawal, Kayal et Saxena ont trouvé en 2002 un algorithme déterministe qui décide si un nombre entier est premier ou non en temps polynomial. Le but du TER est de comprendre cet algorithme (qui relève de l'arithmétique élémentaire) et de l'implémenter.

Références :

- Agrawal, Kayal, Saxena, Primes is in P, Annals of Math 160 (2004), 781-793.
- Morain, La primalité en temps polynomial, Séminaire Bourbaki, 55ème année, 2002-2003 no.917.

3 Sujets proposés par Jean-Marc Couveignes

Contact : Jean-Marc.Couveignes@math.u-bordeaux.fr

3.1 Fonctions de hachage, codes d'authentification, arithmétique rapide.

Sous certaines conditions, une fonction de hachage permet d'assurer l'intégrité de données : une modification de ces données invalide le certificat. On propose d'étudier cette question plus en détail. Si le temps le permet, on abordera la construction proposée par Wegman et Carter et le rôle joué la réduction modulo un entier ou un polynôme.

Références :

- Douglas Stinson, Cryptographie, théorie et pratique, chapitre 4, Vuibert.
- J. Lawrence Carter, Mark N. Wegman, Universal classes of hash functions, Journal of Computer and System Sciences 18 (1979), 143–154. ISSN 0022–0000. http://cr.yp.to/bib/1979/carter.html
- Daniel J. Bernstein. "Floating-point arithmetic and message authentication." http://cr.yp.to/antiforgery/hash127-20040918.pdf

3.2 Réduction de réseaux et cryptographie

COULAUD Jeremie, KINDOMBA Emmanuel

La réduction de réseaux est un outil puissant pour la cryptanalyse. On propose d'étudier les cryptosystèmes à base de sac-à-dos et leur attaque à l'aide de l'algorithme LLL de réduction de réseaux.

Références :

- The rise and fall of knapsack cryptosystems by Andrew Odlyzko, `http://www.dtc.umn.edu/~odlyzko/doc/arch/knapsack.survey.pdf`
- The Two Faces of Lattices in Cryptology by Phong Q. Nguyen and Jacques Stern Cryptography and Lattices – Proceedings of CALC '01 (March 29–30, 2001, Providence, Rhode Island, USA), J. Silverman (Ed.), vol. 2146 of Lecture Notes in Computer Science, Springer-Verlag.

4 Sujets proposés par Jean-Paul Cerri

Contact : Jean-Paul.Cerri@math.u-bordeaux.fr

4.1 Décodage des codes de Reed-Solomon

Victoire LANGLAIS, Lucas ROUX

Il existe plusieurs algorithmes de correction d'erreurs pour les codes de Reed-Solomon. L'objet de ce TER est d'étudier certains de ces algorithmes et de les comparer en théorie et en pratique.

4.2 Crible quadratique et variantes

Nathan Castets, Olivier Huge-Sou, Simon Montoya

Il s'agira d'étudier et d'implémenter la méthode dite du crible quadratique, mise au point par Carl Pomerance en 1981 et qui permet de factoriser de grands entiers. S'il n'est plus actuellement le plus performant, il a permis de battre quelques records (RSA-129, 1994). L'étude portera aussi sur quelques variantes du crible.

4.3 Casser un LFSR

Anatole DELABROUILLE et Maxime ROMÉAS

Il existe plusieurs algorithmes ayant pour but de retrouver, à partir de la connaissance de certains bits d'une suite engendrée par un LFSR, la relation qui a permis de générer cette suite. L'objet de ce TER est d'étudier certains de ces algorithmes et de les comparer. Il pourra se prolonger à l'étude de chiffrements plus complexes utilisant des LFSR et des attaques qu'ils peuvent subir.

5 Sujets proposés par Abdou Guermouche

Contact : abdou.guermouche@labri.fr

Étudier, comprendre en detail, voire implementer les attaques suivantes :

5.1 Same Origin Method Execution (SOME)

Brian Labaurie, Dhekra Mahmoud

`http://www.benhayak.com/2015/06/same-origin-method-execution-some.html`

5.2 Key Reinstallation Attacks : Breaking WPA2 by forcing nonce reuse

AIRD Kenneth, DUCRETTET Damien, GONZALEZ Boris

`https://www.krackattacks.com/`

6 Sujet proposé par Arnaud Jehanne

Contact : arnaud.jehanne@u-bordeaux.fr

Inspirés par le système C^* de T. Matsumoto et H. Imai, certains systèmes de chiffrements sont basés sur des polynômes multivariés. Le calcul de bases de Gröbner constitue un bon angle d'attaque de ses systèmes.
Il s'agit d'étudier et d'implémenter l'algorithme F4 de J.-C. Faugère, bien adapté à ce genre de calcul.

Référence :

- Faugère, J.-C. (June 1999). "A new efficient algorithm for computing Gröbner bases (F4)". Journal of Pure and Applied Algebra. 139 (1) : 61–88.

7 Sujets proposés par Guilhem Castagnos

Contact : guilhem.castagnos@math.u-bordeaux.fr

7.1 Attaques sur les primitives Elgamal et RSA

Messan Afangbom, Mohamed Hamza Harifi, Amina Kasmi

Il est bien connu que les primitives de chiffrement Elgamal et RSA, c'est à dire sans transformation préalable du message à chiffrer, ne peuvent atteindre les plus hauts niveaux de sécurité, par exemple ceux ou un adversaire a accès à un oracle de déchiffrement. En 2000, Boneh, Joux et Nguyen ont proposé des attaques sur ces primitives dans le cas spécifique où elles sont utilisées pour chiffrer un message court, par exemple une clef de session de cryptographie symétrique. Il s'agira d'étudier et de mettre en œuvre ces attaques.

Référence :

- Boneh, Joux et Nguyen, Why textbook ElGamal and RSA encryption are insecure, `http://www.ssi.gouv.fr/archive/fr/sciences/fichiers/lcr/bojong00.pdf`

7.2 Protocole d'interrogation anonyme de base de données

D'ordinaire, pour récupérer un champ d'une base de données, un client envoie une requête indiquant quel élément l'intéresse, puis la base lui renvoie cet élément. Quel élément a été consulté est une information que le client peut ne pas souhaiter divulguer y compris au serveur de base de données. Pour protéger l'anonymat de la requête, des protocoles, appelés protocoles PIR (*Private Information Retrieval*) ont été proposés. Il s'agira d'étudier et de mettre en œuvre une construction de protocole PIR utilisant des systèmes de chiffrement dits homomorphes additifs, comme le système de Paillier.

Références :

- Rafail Ostrovsky, William E. Skeith III, A Survey of Single-Database PIR : Techniques and Applications, `http://eprint.iacr.org/2007/059.pdf`
- Pascal Paillier, Public Key Cryptosystems based on Composite Degree Residue Classes, `http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.112.4035`
- Yan-Cheng Chang, Single Database Private Information Retrieval with Logarithmic Communication, `https://eprint.iacr.org/2004/036.pdf`

7.3 Algorithme ρ de Pollard pour le logarithme discret

Laure Bachelet, Xavier Maso, Charlotte Rance

Les systèmes cryptographiques basés sur le problème du logarithme discret tels que le chiffrement Elgamal ou la signature DSA peuvent utiliser un sous groupe multiplicatif d'ordre q premier d'un corps fini $\mathbf{F}_p$ avec p premier. Dans un tel cadre, la complexité de l'algorithme le plus performant pour le problème du logarithme discret, le calcul d'index, dépend de la taille de p. Pour l'algorithme ρ de Pollard, c'est la taille de q qui compte. Il s'agira d'étudier et d'implanter cet algorithme dans ce cadre. On pourra notamment s'intéresser à des méthodes récentes pour accélérer la méthode de Pollard.

Références :

- Jung Hee Cheon, Jin Hong, and Minkyu Kim, Speeding Up the Pollard Rho Method on Prime Fields, `http://www.math.snu.ac.kr/~jhcheon/publications/2008/TTDLP_A08_CheonHongKim.pdf`

7.4 Schéma de signature à seuil

Étant donné un groupe de personnes, un schéma de signature à seuil permet à n'importe quel sous-groupe, de taille supérieure à un seuil fixé, de générer une signature numérique pouvant être vérifiée par une personne quelconque. Il s'agira d'étudier et de mettre en œuvre un tel schéma, proposé par Shoup, utilisant la primitive RSA.

Référence :

- Practical Threshold Signatures, Victor Shoup,
  `https://www.iacr.org/archive/eurocrypt2000/1807/18070209-new.pdf`

8 Sujet proposé par Aurélien Esnard

Contact : aurelien.esnard@labri.fr

Attaque man-in-the-middle de HTTPS Simon Duret, Brendan Guevel, Amélie Risi

Le but de ce projet est d'effectuer un état de l'art des attaques HTTPS. En particulier, on se concentrera sur l'attaque SSLStrip dont on détaillera précisément le fonctionnement. En outre, il est demandé de réaliser une démonstration simplifiée de cette attaque en Python, à la manière d'un tutoriel pas à pas. Afin de mettre en place cette démo, un environnement réseau virtualisé sera mis à disposition des étudiants.

Référence :

- `https://moxie.org/software/sslstrip/`

9 Sujets proposés par Eric Balandreaud

Contact : eric.balandraud@math.u-bordeaux.fr

9.1 Décodage par ensemble d'information

Housni Ali

Il s'agit d'une méthode générique de décodage d'un code linéaire qui peut être assez efficace pour des longueurs qui restent raisonnables. Le principe est de « deviner » un ensemble de k coordonnées sans erreur. Si on y arrive, il suffit de réencoder pour trouver le mot de code correct et localiser les erreurs. Bien sûr, il faut essayer plusieurs fois avant de trouver un tel ensemble d'information, mais un calcul simple montre que si $k = n/2$, le nombre moyen de tentatives pour corriger t erreurs est 2^t, ce qui reste praticable pour t petit. Il s'agira d'implémenter ce décodage et de faire quelques expériences avec.

9.2 Décodage algébrique des codes de Reed-Solomon au-delà de la moitié de la distance minimale

Il s'agira de faire des expériences avec la stratégie de décodage développée dans l'article :

J. Nielsen, Power Decoding of Reed-Solomon Codes Revisited, `https://arxiv.org/abs/1311.1940`