Projets 2020

Sujets proposé par *Emmanuel Fleury.*

1. **Conception d'un outil d'aggrégation de traces d'exécution**
   Amélie Marotta et Aurélien Plet
   Avec l'appel système ptrace(), on peut simplement suivre l'exécution d'un programme instruction par instruction. L'idée derrière ce projet est de proposer un programme capable de fusionner (de manière pertinente) plusieurs traces d'exécution sous la forme d'un graphe de flot de contrôle (CFG).
   Il s'agit à la fois de programmer l'outil mais aussi de concevoir un modèle formel qui puisse représenter l'ensemble des traces exécutables collectées à travers plusieurs exécutions et proposer une vue du programme exécuté sous la forme d'un CFG partiel du programme à un niveau assembleur.
2. **Survol des techniques d'anti-fuzzing**
   Lucas Perez et Gwendal Tailliez
   Récemment des articles autour de l'anti-fuzzing sont apparus pour déjouer les techniques d'analyse par exécutions symboliques et exécutions concrètes. Le but du projet est de dresser un panorama de ces techniques et, éventuellement, de réaliser quelques preuves de concepts face à AFL (par exemple).
   (a) Fuzzification : Anti-Fuzzing Techniques, USENIX Security Symposium, 2019. https://www.usenix.org/conference/usenixsecurity19/presentation/jung
   (b) Introduction to Anti-Fuzzing : A Defence in Depth Aid, 2014. https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2014/january/introduction-to-anti-fuzzing-a-defence-in-depth-aid/
   (c) Escaping the Fuzz by David Göransson and Emil Edholm, 2016.
   http://publications.lib.chalmers.se/records/fulltext/238600/238600.pdf
   (d) How to Kill Symbolic Deobfuscation for Free ; or Unleashing the Potential of Path-Oriented Protections, 2019.
   https://arxiv.org/abs/1908.01549
   (e) Destroying `x86_64` instruction decoders with differential fuzzing
   https://blog.trailofbits.com/2019/10/31/destroying-x86_64-instruction-decoders-with-differential-fuzzing/

Sujets proposés par *Abdou Guermouche*

1. **Étude de la dernière attaque sur le protocole DNS : "FIRST-TRY" DNS CACHE POISONING WITH IPV4 AND IPV6 FRAGMENTATION**
   Gaël Jankowski et Nataël Couturier
   Il s'agit d'une attaque permettant de faire du man in the middle en empoisonnant les caches DNS. Elle est basée sur les mécanismes de fragmentation IPv6 et IPv4. De plus, il est possible avec cette attaque d'injecter du contenu malveillant même lorsque DNSSec est utilisé.
   Source :
   https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20presentations/DEFCON-27-Travis-Palmer-First-try-DNS-Cache-Poisoning-with-IPv4-and-IPv6-Fragmentation.pdf
2. **Étude du protocole WPA3 et des attaques visant la poignée de main**
   Bérenger Faurot, Émile Josso et Oren Nezer
   WPA3 est la dernière norme de sécurisation des réseaux sans fil. La norme a été publiée en Janvier 2018 et des travaux ont été publiés illustrant comment on pouvait attaquer ce nouveau protocole (les attaques se concentrant principalement sur la poignée de main).
   Source :
   https://papers.mathyvanhoef.com/dragonblood.pdf
3. **attaques Zombie Poodle et GoldenPoodle**
   Marie Durand et Louis Valette

Sujets proposés par *Guilhem Castagnos*

1. **Attaques à base de réduction de réseaux euclidiens sur RSA**
   Noémie Bossard et Thomas Rabaud
   Pour accélérer la signature RSA, on peut être tenté d'utiliser un petit exposant privé d. Cependant, Wiener a montré en 1990, que si on utilise un exposant $d < N^{0.25}$, où N est le module public, alors le système RSA peut être cassé. Par la suite, Boneh et Durfee ont montré par des attaques utilisant l'algorithme de réduction de réseaux LLL que le système n'est pas sûr dès que $d < N^{0.292}$.
   Il s'agira d'étudier et d'expérimenter de telles attaques. On pourra en particulier implanter l'attaque de Boneh Durfee en utilisant des méthodes de constructions de réseaux pour la cryptanalyse récemment proposée par May et Hermann.

   Références :
   — D. Boneh, G. Durfee, Cryptanalysis of RSA with Private Key d Less Than $N^{0.292}$, http://crypto.stanford.edu/~dabo/papers/lowRSAexp.ps

— M. Herrmann, A. May, Maximizing Small Root Bounds by Linearization and Applications to Small Secret Exponent RSA, http://www.cits.rub.de/imperia/md/content/may/paper/pkc10_rsa_unraveled.pdf

2. **Chiffrement fonctionnel pour le produit scalaire**

   Le chiffrement asymétrique classique offre un accès binaire à l'information à partir d'un chiffré : celui qui possède la clef secrète peut retrouver toute l'information sur le message clair m, et celui qui ne la possède pas est censé n'avoir aucune information sur m. Pour de nombreuses applications, il est nécessaire d'avoir un accès plus fin à l'information. Le chiffrement fonctionnel formalisé par Boneh, Sahai et Waters en 2011, permet à celui qui possède une clef secrète associée à une fonction f d'apprendre $f(m)$ à partir du chiffré de m, et aucun autre information sur m. Des constructions ont été proposées pour des fonctions f assez générales, mais elles sont en général peu efficaces, ou reposent sur des hypothèses peu standard. Aussi, plusieurs travaux récents se sont consacrés à produire des chiffrements fonctionnels efficaces pour des classes limitées de fonctions utiles pour les applications : m est maintenant un vecteur et on considère des fonctions $f_a : m \mapsto \langle a, m \rangle$.

   Il s'agira d'étudier des constructions de tels protocoles et les notions de sécurités associées.

   Références :

   — Boneh, Sahai, Waters. Functional Encryption : Definitions and Challenges, https://eprint.iacr.org/2010/543.pdf
   — Abdalla, Bourse, De Caro, Pointcheval. Simple functional encryption schemes for inner products, https://eprint.iacr.org/2015/017.pdf
   — Agrawal, Libert, Stehlé. Fully secure functional encryption for inner products, from standard assumptions, https://eprint.iacr.org/2015/608.pdf

3. **Cryptanalyse de l'AES à 5 tours**

   Agathe Houzelot et Clara Pernot

   Si aucune attaque concrète n'a été trouvée sur le chiffrement AES complet, de nombreuses ont été proposées sur l'AES réduit à 5 tours. On s'intéressera à ces attaques et notamment à une attaque très performante récemment proposée par Dunkelman, Keller, Ronen et Shamir. L'objectif du projet sera d'implanter ces attaques.

   Référence :

   — Orr Dunkelman, Nathan Keller, Eyal Ronen, Adi Shamir, The Retracing Boomerang Attack, http://eprint.iacr.org/2019/1154.pdf

4. **Variantes de Paillier à seuil sans *trusted dealer***

   Camille Mutschler et Aelith Saillard

   Le système de Paillier est un chiffrement à clef publique linéaire homomorphe. La clef publique de ce système est un module RSA N. Dans une variante à seuil de paramètre (t, n) la clef secrète est partagée entre n personnes de telle manière que

$t < n$ personnes n'apprennent rien mais $t + 1$ peuvent collaborer pour déchiffrer. Ceci a de nombreuses applications notamment pour du calcul multipartite sécurisé.

Des solutions efficaces ont été proposées pour construire de telles variantes de Paillier, mais elles supposent l'existence d'un *trusted dealer*, une tierce personne de confiance qui connaît la factorisation de N et génère les parts de la clef secrète. On s'intéressera à des solutions relativement efficaces sans *trusted dealer* et à leur implantation.

Référence :

— Veugen, Attema, Spini, An implementation of the Paillier crypto system with threshold decryption without a trusted dealer, http://eprint.iacr.org/2019/1136.pdf

5. **Verifiable delay function** Une *Verifiable delay function* est une fonction qui prend du temps à être évaluée (même en parallèle) mais dont la sortie peut-être vérifiée efficacement. De telles fonctions sont utiles par exemple pour fournir un générateur d'aléa public à partir d'une source pouvant être manipulée comme les cours de la bourse. Ces fonctions trouvent également une application dans certaines propositions de blockchain. On s'intéressera à des constructions récentes de telles fonctions.

   Références :

   — Boneh, Bünz, Fisch, A Survey of Two Verifiable Delay Functions, https://eprint.iacr.org/2018/712.pdf

   — Wesolowski, Efficient verifiable delay functions, http://eprint.iacr.org/2018/623.pdf

Sujets proposés par *Jean-Marc Couveignes*.

1. **Le crible quadratique et le crible algébrique.**

   On étudiera les principes généraux et quelques détails de cette grande famille d'algorithmes de factorisation des nombres entiers.

   Une implémentation d'une version simplifiée de l'un de ces cribles pourra illustrer cette étude.

   http://websites.math.leidenuniv.nl/algebra/sieving.pdf

2. **Compter les points sur une courbe elliptique.**

   Le groupe des points d'une courbe elliptique sur un corps fini est utile en cryptographie. Pour utiliser ce groupe il est nécessaire de connaître son cardinal.

   On étudiera quelques algorithmes pour ce faire et on proposera une implémentation.

   http://iml.univ-mrs.fr/~ritzenth/cours/point-counting-ec.pdf

Sujet proposé par *Jean-Paul Cerri*.

Étude et mise en œuvre de l'attaque de Bleichenbacher sur le procédé de padding PKCS# 1.

il s'agit d'une attaque maintenant célèbre, à chiffré choisi, où la réponse de l'oracle (ou en pratique du serveur) est 0 ou 1 (en pratique : message d'erreur ou absence de message d'erreur). L'attaque adaptative à chiffré choisi permet à terme de décrypter un cryptogramme cible.

Référence principale :

http://archiv.infsec.ethz.ch/education/fs08/secsem/Bleichenbacher98.pdf

Sujets proposés par *Gilles Zémor*.

1. **Wave : un procédé de signature basé sur les codes**
   Suzanne Lansade et Eva Palandjian

   Il est notoirement beaucoup plus délicat de réaliser un procédé de signature à base de codes que de faire du chiffrement. Le procédé Wave, qui vient d'obtenir le prix du meilleur article présenté à la conférence Asiacrypt 2019, propose une solution très originale et élégante à ce problème. Il s'agir d'étudier ce procédé et de réaliser quelques expériences d'implémentation.

   Référence (ne pas être effrayé par la longueur de la soumission, il n'est pas nécessaire de tout lire pour bien comprendre le procédé) :

   https://eprint.iacr.org/2018/996

2. **Le chiffrement à base de codes HQC**
   Pierre Lledo

   On s'interessera au chiffrement à base de codes HQC https://pqc-hqc.org/ Au cœur du système sont des codes de petits rendements destinés à corriger un nombre important d'erreurs. On tentera de tester une ou deux variantes de codes avec en vue l'application HQC.

3. **Le décodage de codes linéaires par paires localisatrices d'erreurs**
   Celian Banquet et Elie Bouscatié

   Le décodage par paires localisatrices d'erreurs est une méthode mise en évidence dans l'article cité ci-dessous qui a l'avantage d'unifier des algorithmes de décodage connus de plusieurs familles des codes. Récemment des méthodes de cryptanalyse de systèmes cryptographiques à clé publique basés sur les codes linéaires ont été développées avec succès.

   L'objet du projet est de comprendre théoriquement et par implémentation en quoi consiste ce décodage, puis de construire des exemples de codes pour lesquels ce décodage fonctionne. On pourra déboucher sur une proposition de système de chiffrement.

   Ruud Pellikan : *on decoding linear codes by error locating pairs*

   http://www.win.tue.nl/~ruudp/paper/15-ecp-preprint.pdf