Générateurs de nombres aléatoires – Tests et exploitation des vulnérabilités

RÉSUMÉ

Dans un monde numérique sans frontière où tout est connecté, l'information est accessible partout, à tout moment. Mais ce monde nous expose à de nouveaux risques : piratage, vol d'informations, rançonnage... La sécurité informatique s'impose alors dans tous les usages numériques sensibles, où l'emploi de la cryptographie est essentiel. Les clés secrètes ou privées des systèmes de chiffrement, de signature ou d'authentification doivent être choisies de manière parfaitement aléatoire. Les générateurs de nombres aléatoires ont de nombreuses applications dans des domaines très différents que ce soit les jeux de hasard, la simulation, la prise de décisions, mais aussi la sécurité informatique. Leur défaillance totale ou partielle met donc en péril la fonctionnalité du système dans son ensemble.
L'évaluation d'un générateur de nombres aléatoires nécessite d'une part de caractériser ses propriétés statistiques et d'autre part de vérifier sa résistance aux attaques. L'objectif de cette thèse est d'étudier et de proposer des méthodes pour évaluer la qualité de ces générateurs, de détecter les défauts observés en sortie et d'exploiter les vulnérabilités identifiées lors de l'utilisation de ces nombres qui in fine ne sont plus fiables et donc amènent à une cryptographie dégradée.

FORMATION NIVEAU MASTER RECOMMANDÉ

Master 2 Mathématiques/Cryptographie/Informatique/Statistiques

INFORMATIONS PRATIQUES

Lieu : CEA Grenoble, Département Systèmes (LETI) - CESTI
Le laboratoire CESTI (Centre d'Evaluation de la Sécurité des Technologies de l'Information) évalue la sécurité des cartes à puce dans le contexte de la certification de produits du schéma français piloté par l'ANSSI sous l'autorité du Premier Ministre. La certification permet d'attester qu'un produit atteint, à un instant donné, un niveau de sécurité représenté par les services de sécurité qu'il offre et sa résistance à un niveau d'attaques donné : en France, quel que soit le type d'évaluation, la certification s'appuie systématiquement, outre des vérifications de conformité, sur des tests de pénétration pour déterminer le niveau de sécurité réellement atteint par le produit. L'activité du CESTI consiste donc entre autres à tester des composants sécurisés afin d'étudier leurs vulnérabilités et de tester leur résistance aux attaques.

Conditions : l'autorisation d'accès aux locaux sera soumise aux résultats d'une enquête préliminaire de sécurité.

Date souhaitée pour le début de la thèse : 01/09/2020

PERSONNE À CONTACTER PAR LE CANDIDAT

Cécile DUMAS
CEA DRT/DSYS/SSSEC/CESTI
cecile.dumas@cea.fr

UNIVERSITÉ / ÉCOLE DOCTORALE

Université Grenoble Alpes
Mathématiques, Sciences et Technologies de l'Information, Informatique (MSTII)

DIRECTEUR DE THÈSE

Philippe ELBAZ-VINCENT
Université Grenoble Alpes - Institut Fourier - 100 rue des maths - 38610 Gières

SUJET DÉTAILLÉ

Les nombres aléatoires constituent la clé de voûte de la sécurité des systèmes. En effet, toute la sécurité des algorithmes et protocoles cryptographiques repose sur la qualité de ces nombres. Les propriétés d'uniformité et d'imprévisibilité sont essentielles pour garantir la confidentialité ou l'intégrité des données échangées ou stockées. Par exemple, il a été mis en évidence qu'il est possible de retrouver la clef de

signature de l'algorithme DSA si celui-ci utilise un nombre aléatoire d'entropie diminuée [1]. Pour les applications sensibles telles que la transaction bancaire ou la gestion de données personnelles stockées dans un passeport, il est nécessaire de générer des nombres aléatoires de grande qualité. D'autant plus que l'arrivée des algorithmes de cryptographie post-quantique devrait amplifier l'utilisation des générateurs d'aléa tout en conservant les contraintes de qualité et de sécurité.

Le Centre d'Évaluation de la Sécurité des Technologies de l'Information (CESTI) du CEA-Leti Grenoble mène ses activités dans le domaine de l'évaluation sécuritaire de systèmes électroniques. Dans ce contexte, les évaluateurs sont, entre autres, amenés à tester la résistance des mécanismes cryptographiques embarqués face aux attaques telles que les attaques par perturbation du composant [2] ou les attaques par observation des signaux compromettants émis par ce dernier [3].

Les nombres aléatoires utilisés dans ces mécanismes sont générés grâce à une brique matérielle appelée Physical True Random Number Generator (PTRNG). Le travail de l'évaluateur vis-à-vis du PTRNG, consiste d'une part à évaluer la qualité des nombres aléatoires, même en présence d'attaque, et d'autre part à valider la résistance des mécanismes cryptographiques basés sur ces nombres qui peuvent être de plus ou moins grande qualité.

La qualité des nombres aléatoires générés par un PTRNG n'est pas triviale à démontrer. Par le passé elle était validée à l'aide de nombreux tests statistiques [4,5], parfois redondants, insuffisants ou inadaptés [6]. De nos jours la tendance est de baser cette évaluation sur une modélisation du comportement statistique du PTRNG, telle que préconisée dans la méthodologie AIS31 [7,8] ou plus récemment par le NIST [9]. Cette modélisation, élaborée en parallèle de la conception du PTRNG, permet d'une part de définir des tests statistiques adaptés aux particularités physiques du générateur afin de détecter des anomalies pertinentes [10,11], et d'autre part de spécifier une fonction sur mesure de retraitement afin de corriger les défauts attendus [6,12].

Les objectifs de cette thèse concernent la définition de tests statistiques adaptés, la détection d'anomalies et les conséquences d'un point de vue cryptographique de l'utilisation de tels nombres aléatoires dégénérés :

- A partir de modélisations classiques de PTRNG [13], le doctorant sera amené à étudier les propriétés statistiques des nombres aléatoires générés, et de proposer de nouvelles méthodes de caractérisation afin d'aider un développeur à ajuster les paramètres de son PTRNG, puis de détecter les défauts qui pourraient se manifester au cours de la génération des aléas [14]. Pour cela, le doctorant s'appuiera sur des techniques statistiques existantes et au besoin pourra étendre ses recherches sur l'utilisation d'outils d'apprentissage automatique [15].
- Afin de seconder l'évaluateur dans la recherche de vulnérabilités, le doctorant examinera également les moyens de détecter les défauts statistiques des paramètres issus de nombres aléatoires. Ces anomalies peuvent provenir soit des nombres aléatoires eux-mêmes, car générés par un PTRNG imparfait, défectueux ou corrompu, soit d'erreurs de calcul suite à un bogue d'implémentation ou suite à une attaque par perturbation lors de l'exécution du programme de calcul du paramètre [16,17].
- Plus généralement, le doctorant pourra analyser les conséquences liées à l'utilisation de tels paramètres (ou nombres aléatoires) aux propriétés statistiques imparfaites, dans les mécanismes cryptographiques courants (génération de clé, signature (EC)DSA, passeport, IAS, etc.) [18] et plus particulièrement pour la nouvelle génération d'algorithmes post-quantiques.

Ces études mathématiques pourront être menées en parallèle ou à la suite les unes des autres. Elles seront essentiellement basées sur des simulations effectuées par le doctorant et des données obtenues dans le cadre des évaluations menées par le CESTI.

[1] P. Q. Nguyen, I. E. Shparlinski. The Insecurity of the Elliptic Curve Digital Signature Algorithm with Partially Known Nonces. Journal of Cryptology, volume 15, pp. 151-176, 2000.

[2] D. Boneh, R.A. DeMillo, R.J. Lipton. On the Importance of Checking Cryptographic Protocols for Faults. EUROCRYPT 1997, volume 1233, pp. 37–51. 1997.

[3] P. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. CRYPTO 1996.

[4] P. L'Ecuyer, R. Simard. TestU01: A C Library for Empirical Testing of Random Number Generators. ACM Transactions on Mathematical Software. 2007.

[5] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Tech. rep., NIST SP 800-22, Revision 1a. 2010.

[6] G. De Julis. Analyse d'accumulateurs d'entropie pour les générateurs aléatoires cryptographiques. Thèse de doctorat. Univ. Grenoble Alpes. 2014.

[7] W. Killmann, W. Schindler. A proposal for : Functionality classes for random number generators. Tech. Rep. 2, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2011.

[8] W. Schindler. Security Evaluation of Physical RNGs. Guest lecture at Workshop on Randomness and Arithmetics for Cryptography on Hardware (WRACH'19), April 16 2019.
https://wrach2019.lip6.fr/slides/wrach_2019_schindler_presentation_website.pdf

[9] M. S. Turan, E. Barker, J. Kelsey, K. A. McKay, M. L. Baish, M. Boyle. Recommendation for the entropy sources used for random bit generation. Tech. Rep. NIST SP 800-90b. 2018.

[10] M. Baudet, D. Lubicz, J. Micolod, A. Tassiaux. On the Security of Oscillator-Based Random Number Generators. Journal of Cryptology, pp. 1–28, 2010.

[11] D. Lubicz, N. Bochard. Towards an Oscillator Based TRNG with a Certified Entropy Rate. IEEE Transactions on Computers, vol. 64, pp. 1191–1200, 2015.

[12] P. Lacharme. Post-Processing Functions for a Biased Physical Random Number Generator. Fast Software Encryption, vol. 5086, pp. 334–342, 2008.

[13] K. Layat. Modélisation et validation des générateurs de nombres aléatoires cryptographiques pour les systèmes embarqués. Thèse de doctorat. Univ. Grenoble Alpes. 2015.

[14] V. Fischer, D. Lubicz. Embedded Evaluation of Randomness in Oscillator Based Elementary TRNG. Advanced Information Systems Engineering, vol. 7908, pp. 527–543. 2014.

[15] F. Ganji, S. Tajik, F. Fäßler, J-P. Seifert. Strong Machine Learning Attack against PUFs with No Mathematical Model, CHES 2016.

[16] M. Nemec, M. Sys, P. Svenda, D. Klinec, V. Matyas. The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli. ACM Conference on Computer and Communications Security. CCS 2017.

[17] K. Ryan. Return of the Hidden Number Problem – A Widespread and Novel Key Extraction Attack on ECDSA and DSA. CHES 2019.

[18] Timing sur l'aléa dans (EC)DSA : Minerva Group. https://minerva.crocs.fi.muni.cz