Vulnérabilités et évaluation des générateurs de nombres aléatoires des composants sécurisés

Référence	CYBERINSTITUTE-INT-20002
Description	La cryptographie embarquée sur les cartes à puce utilise amplement les nombres aléatoires afin d'obtenir des propriétés d'uniformité ou pour cacher de l'information. En pratique ces nombres sont issus d'une brique matérielle appelée TRNG (True Random Number Generator). La qualité des nombres aléatoires générés par un TRNG n'est pas évidente à démontrer, puisque toute séquence de bits a la même probabilité d'apparition. Depuis plusieurs années, de nombreuses batteries de tests statistiques ont été définies afin de décider si les séquences générées sont aléatoires ou non. Ces tests, appliqués massivement, sont parfois difficiles à exploiter car ils ne permettent pas toujours de caractériser le défaut observé et de qualifier précisément le générateur. Le Centre d'Évaluation de la Sécurité des Technologies de l'Information (CESTI) de Grenoble mène des activités dans le domaine de l'évaluation sécuritaire de systèmes électroniques, et plus particulièrement des TRNG embarqués sur carte à puce. Dans ce contexte, les évaluateurs sont amenés à tester la qualité du TRNG même en présence d'attaque, comme par exemple les attaques par perturbation de la puce. Le laboratoire a développé un outil comportant de nombreux tests statistiques classiques, qui permettent de valider le caractère aléatoire des nombres générés, mais ne répondent pas à toutes les questions liées à l'évaluation. Les objectifs de ce stage sont donc d'analyser les différents besoins de l'évaluateur et de définir d'autres tests statistiques qui répondent dans un premier temps aux questions suivantes : Comment détecter dans une séquence de bits l'effet d'une perturbation du composant ? Comment caractériser les défauts d'un générateur lorsque les tests montrent que les nombres générés ne sont pas aléatoires ? Le stage pourra débuter sur l'implantation et l'évaluation des tests statistiques étudiés dans les thèses de Guenaëlle De Julis (2014) et Kevin Layat (2015). Ensuite, le stagiaire pourra proposer d'autres idées afin d'investiguer de nouveaux tests qui répondent aux différents besoins de l'évaluateur. Pour cela il sera en contact avec l'équipe des évaluateurs du CESTI et s'appuiera sur la littérature existante. L'efficacité des tests sera validée sur des séquences de nombres aléatoires simulées ou réelles, obtenues dans le cadre des évaluations menées par le CESTI. Le candidat devra montrer des qualités d'autonomie et l'envie de découvrir de nouveaux domaines. Ce stage pourra éventuellement se poursuivre en thèse. <u>Contexte</u> Le Grenoble Alpes Cybersecurity Institute regroupe environ 150 chercheurs - experts en informatique, cryptographie, micro-électronique mais également en droit international, politique et économie - issus de 16 laboratoires de l'Univ. Grenoble Alpes et travaillant dans les domaines de la cybersécurité et de la protection de la vie privée. Ses principaux axes de recherche sont les éléments sécurisés à bas coût, les infrastructures critiques sécurisées et leur gestion en terme de cycle de vie, l'analyse de vulnérabilité et les défis globaux en termes d'analyse des risques et de validation des grands systèmes, incluant la résilience pratique dans l'industrie et la société. En prenant en compte l'impact sociétal de la cybersécurité, cette approche – dite holistique – permet d'intégrer la recherche fondamentale dans un contexte plus large, donc plus pertinent (https://cybersecurity.univ-grenoble-alpes.fr).
Prérequis	Le ou la candidat(e) doit avoir un profil de formation Bac+5 et pouvoir justifier de solides connaissances en statistiques. Par ailleurs, il ou elle devra impérativement lire couramment l'anglais scientifique.

Encadrant(s)	Cécile Dumas (CEA-LETI)
Candidature	Envoyer CV, lettre de motivation avec recommandation(s) de 1 ou 2 référents (dont responsable de la formation), relevés de notes de M1 (obligatoire) à cyberalps-contact@univ-grenoble-alpes.fr Pour plus d'information sur le stage, contacter cecile.dumas@cea.fr
Localisation	CEA-LETI (Grenoble)
Date de début	Février 2020
Durée	5 – 6 mois
Gratification	Selon réglementation en vigueur (env. 560€/mois). Possibilité de prise en charge partielle des frais de transport.