Offre de stage : Vulnérabilités et évaluation des générateurs de nombres aléatoires des composants sécurisés

Référence	CYBERINSTITUTE-INT-19005
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 seront produits soit de façon prédictible grâce à un algorithme déterministe amorcé par une graine (générateur pseudo-aléatoire), soit physiquement à l'aide d'une brique matérielle appelée TRNG (True Random Number Generator) ou encore via une méthode mixte où la graine d'un générateur pseudo-aléatoire provient d'un TRNG. 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 le générateur. Ils sont de plus souvent trop génériques pour déceler de petites anomalies. Par ailleurs, afin de s'assurer de la qualité des nombres générés, un développeur peut concevoir une modélisation statistique de la sortie du générateur et/ou ajouter une fonction de retraitement. Le Centre d'Évaluation de la Sécurité des Technologies de l'Information (CESTI) du CEA-LETI de Grenoble mène des activités dans le domaine de l'évaluation sécuritaire de systèmes électroniques, et plus particulièrement des générateurs de nombres aléatoires. Dans ce contexte, le laboratoire a développé un outil comportant de nombreux tests statistiques classiques, qui permettent de valider le caractère aléatoire des nombres générés. Malheureusement cet outil ne répond pas à toutes les questions liées à l'évaluation. En effet le métier d'évaluateur a beaucoup évolué ces dernières années ; il nécessite également d'étudier la conception du TRNG (et notamment sa fonction de retraitement) et d'analyser le modèle fourni par le développeur. Dans le cadre de ce stage pour Grenoble Alpes Cybersecurity Institute, les objectifs sont donc d'analyser quels sont les besoins de l'évaluateur et de définir d'autres tests statistiques qui répondent par exemple 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 ? - Comment vérifier que la modélisation fournie correspond bien aux sorties du générateur ? - Comment valider l'efficacité de la fonction de retraitement ? Dans un premier temps le stagiaire pourra implémenter et évaluer les tests statistiques étudiés dans les thèses de Guenaëlle De Julis (2014), Kevin Layat (2015) et Patrick Haddad (2015). Ensuite, il devra s'appuyer sur la littérature existante et faire preuve d'un esprit curieux et créatif afin d'apporter d'autres tests qui répondent aux différents besoins de l'évaluateur. 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.
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 recommandations de 2 référents (dont responsable de la formation), relevés de notes de M1 (obligatoire) et relevé de notes de M2 (si possible) 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 2019
Durée	5 à 6 mois
Gratification	Selon réglementation en vigueur (env. 560€/mois). Possibilité de prise en charge partielle des frais de transport.

financed by IDEX Université Grenoble Alpes