

Offre de stage de Master 2 en « Tatouage de logiciels »

Mots clés. Tatouages, Sécurité logicielle, cryptographie, cryptanalyse.

Contexte. Le tatouage numérique a pour objectif la protection des données contre la copie illégale ou de permettre de restreindre le cadre d'utilisation de ces données. Il est largement utilisé aujourd'hui sur des données multimédia mais peut aussi être utilisé sur d'autres types de données comme les logiciels. Les propriétés de sécurité demandées à ces schémas de tatouage sont variées comme la robustesse contre des attaques ou des transformations, en fonction du modèle de sécurité envisagé. En particulier, de tels tatouages doivent être résistants :

- aux attaques par soustraction (identification et suppression d'un tatouage)
- aux attaques par addition (un second tatouage est ajouté)
- aux attaques par collision (localisation d'un tatouage à partir de deux versions)

En fait, les travaux sur les tatouages de logiciels existent depuis une vingtaine d'années et peuvent se séparer en deux grandes catégories relativement étanches. D'un côté on trouve des solutions théoriques souvent éloignées du contexte applicatif logiciel, et d'un autre côté, on trouve des schémas créés pour ce contexte mais dont la sécurité est non prouvée, voir douteuse.

Objectifs. L'objectif de ce stage est de prendre en main cette problématique, dans un premier temps par un état de l'art sur les méthodes de tatouages existantes et les attaques de la littérature.

Une fois cet état de l'art réalisé, le ou la stagiaire proposera une implémentation d'un ou plusieurs schémas identifiés comme faible. Environnement de travail : Langage C / Linux.

Profil recherché : Master 2 en informatique ou école d'ingénieur, intéressé par la recherche en sécurité informatique. **Suite à ce stage de M2 une poursuite en doctorat est envisageable.**

Une première expérience dans la sécurité informatique (plateformes dédiées, CTF, hackathons,...), des connaissances dans les domaines de la sécurité, vérification logicielle ou de la cryptographie seront un atout pour la candidature mais ne sont pas obligatoires.

Lieu du stage : laboratoire GREYC, Université de Caen, Ensicaen, UMR CNRS 6072

Rémunération : environ 590 euros par mois

Candidature : Les candidatures doivent être envoyées aux encadrants du stage : patrick.lacharme@ensicaen.fr et matthieu.dien@unicaen.fr. Elles doivent inclure un CV détaillé, une courte lettre de motivation, les relevés de notes de Licence et du Master 1 et éventuellement une lettre de recommandation du responsable du master.

Les candidatures au stage doivent être envoyées dès que possible et seront évaluées au fil de l'eau. Le plus tôt sera le mieux, en particulier pour préparer une candidature à la poursuite en thèse.