

Analyse formelle de propriétés d'anonymat dans les protocoles de routage

Laboratoire, institution et université LSV, ENS de Cachan

Le stage sera localisé au LSV à Cachan.

Équipe ou projet dans le labo Équipe Secsi au LSV.

Nom et adresse électronique du directeur de stage

Stéphanie Delaune (LSV), delaine@lsv.ens-cachan.fr

Indemnisation Ce stage pourra être indemnisé. En particulier, ce stage a le support du projet ANR VIP (Programme JCJC) ¹.

Présentation générale du domaine. Pour transmettre un message entre deux points du réseau, les données sont transmises de nœuds voisins en nœuds voisins. Les protocoles de routage ont comme objectif d'établir une « route », c'est-à-dire un chemin entre deux points du réseau tel que chaque arête du chemin relie des nœuds voisins. La première étape d'une attaque consiste souvent à faire accepter à un nœud honnête des routes malhonnêtes qui, soit empêchent le nœud de communiquer avec une partie de ses correspondants, soit forcent les communications à passer par un nœud contrôlé par l'attaquant. Pour contrer ce type d'attaque, plusieurs protocoles de routage dits sécurisés ont été proposés [HPJ05, SKY05]. Dans ces protocoles, chaque nœud ajoute une information (signature, MACs, hachage, ...) de manière à empêcher un attaquant de modifier la route. Certains de ces protocoles, *e.g.* [SKY05], ont pour but d'établir ces routes d'une façon anonyme, et de préserver l'anonymat des participants lors de la transmission des données (*e.g.* Tor [DMS04]).

Objectifs du stage. L'objectif de ce stage est l'analyse de propriétés d'anonymat dans les protocoles de routage. Pour cela, il faudra tout d'abord comprendre le fonctionnement de ces protocoles de routage et étudier les différentes propriétés qu'ils ont pour but d'assurer (*e.g.* anonymity, pseudonymity, unlinkability, ...). À partir de là, et en s'inspirant des définitions existantes d'anonymat dans d'autres types d'applications (vote électronique [DKR09], protocoles RFID [ACRR10]), nous proposerons des définitions formelles pour ces différentes notions que nous validerons sur des études de cas.

Une fois ces définitions obtenues, nous chercherons à mettre au point des techniques *automatique* pour l'analyse de la sécurité des protocoles de routage sécurisés. Les techniques actuelles spécifiques aux protocoles de routage sont assez restrictives [ACD10]. En particulier, elles ne permettent pas d'analyser les propriétés du type anonymat.

1. <http://www.lsv.ens-cachan.fr/Projects/anr-vip/>

Compétences espérées. L'étudiant devra avoir de bonnes compétences en logique (déduction automatique, arbres, etc.) et un goût pour les preuves. Des connaissances en sécurité sont un plus mais ne sont pas requises car elles pourront être assimilées au cours du stage.

Références

- [ACD10] Mathilde Arnaud, Véronique Cortier, and Stéphanie Delaune. Modeling and verifying ad hoc routing protocols. In *Proceedings of the 23rd IEEE Computer Security Foundations Symposium (CSF'10)*, pages 59–74, Edinburgh, Scotland, UK, July 2010. IEEE Computer Society Press.
- [ACRR10] Myrto Arapinis, Tom Chothia, Eike Ritter, and Mark Ryan. Analysing unlinkability and anonymity using the applied pi calculus. In *Proc. of 23rd IEEE Computer Security Foundations Symposium*, 2010.
- [DKR09] Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. Verifying privacy-type properties of electronic voting protocols. *Journal of Computer Security*, 17(4) :435–487, July 2009.
- [DMS04] Roger Dingledine, Nick Mathewson, and Paul F. Syverson. Tor : The second-generation onion router. In *USENIX Security Symposium*, 2004.
- [HPJ05] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Ariadne : A secure on-demand routing protocol for ad hoc networks. *Wireless Networks*, 11 :21–38, 2005.
- [SKY05] R. Song, L. Korba, and G. Yee. Anondsr : Efficient anonymous dynamic source routing for mobile ad-hoc networks. In *Proceedings of the 2005 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2005)*, pages 32–42, Alexandria, Virginie, 2005.