DOR: Dynamic Onion Routing.
Vers un système de communications anonymes pair-à-pair

Mot-clés : Routage en onion, confidentialité, anonymat, système à large échelle

1 Contexte

Ces dernières années ont été marquées par de nombreux scandales de surveillance de masse très médiatisés[1]. Bien que le chiffrement des données puisse aider à contrer ces efforts de surveillance, il ne suffit pas à lui seul à protéger pleinement les utilisateurs qui souhaitent échanger des données à distance, car il n'empêche pas en soi le suivi des métadonnées telles que la localisation et l'activité d'un utilisateur, et révèle avec qui et quand un utilisateur a interagi. Les réseaux d'anonymat ont été proposés pour réduire le risque de surveillance en ligne. Ils cachent généralement l'identité de leurs utilisateurs en utilisant des réseaux mixtes ou un routage en oignon. Ces mécanismes transmettent les messages des utilisateurs par l'intermédiaire d'une série de relais qui effectuent des opérations cryptographiques à chaque saut, et finissent par masquer le lien entre les émetteurs et les récepteurs. Pour empêcher un adversaire d'intercepter suffisamment de trafic pour être capable de corréler les actions d'un utilisateur, les relais doivent être suffisamment nombreux, disponibles et répartis sur de nombreux systèmes autonomes. Dans l'exemple du réseau Tor, les relais, opérés volontairement, représentent environ 6000 nœuds à ce jour et servent 2 millions d'utilisateurs chaque jour.

Dans la recherche de garanties d'anonymat plus fortes, les systèmes de routage en oignon devraient augmenter le nombre de relais impliqués dans l'anonymisation des communications. Cela pourrait être réalisé en incluant dans le système de routage des nœuds moins stables tels que les appareils des utilisateurs (ordinateurs, tablette, smartphone). Cependant, en raison de leur volatilité, de l'hétérogénéité des ressources disponibles et de leur comportement potentiellement malveillant, ces dispositifs ne conviennent pas aux stratégies actuelles de routage en oignon et aux systèmes décentralisés.

2 Objectif

Le but de ce projet est de proposer et tester un nouveau système de routage en oignon entièrement distribué qui incorpore les appareils des utilisateurs. Il s'agit de concevoir et d'étudier des stratégies de routage en oignon efficaces et robustes qui correspondent mieux à la dernière vision du routage en oignon distribué : supporter des dispositifs volatiles avec des ressources hétérogènes. Pour cela, vous vous appuierez sur les techniques de routage en oignon existantes ainsi que sur des outils cryptograhiqies tel que le chiffrement de groupe, les chiffrements symétriques et asymétriques

Dans ce projet, il s'agira alors de:

- Partir d'une base de reflexions sur un protocole de routage en oignon distribué pair-à-pair
- Implémenter le protocole proposé.
- Évaluer la résistance aux attaques et la performance ce protocole via des simulations et des expérimentations.
- Implémenter un démonstrateur de la solution.

[1] https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

Profil recherché

Les taches techniques seront en lien avec: développement de systèmes distribués, développement d'un démonstrateur avec une interface utilisateur (applications Web, Android) et un backend. Il faudra aussi comprendre un esprit créatif pour imaginer et tester des solutions innovantes de routage en oignon. Esprit d'équipe, collaboration, curiosité, inventivité et débrouillardise dans les futures technologies seront de mise.

Contact

- Joachim Bruneau-Queyreix: jbruneauqueyreix@enseirb-matmeca.fr
- Laurent Réveillère: laurent.reveillere@u-bordeaux.fr