Sujet de Thèse : Architecture P2P pour Réseaux Sociaux Privés Virtuels

22 septembre 2011

1 Informations générales

TITRE : Architecture P2P pour Réseaux Sociaux Privés Virtuels.

EQUIPE/THEME : LSR / Comet.

DIRECTEURS : Damien Magoni.

THESES EN COURS au 1er octobre 2012 :

Vincent Autefage (20%).

Telesphore Tiendrebeogo (50%).

COURRIELS : magoni@labri.fr

MOTS-CLES : réseau social, protocoles de sécurité, distribution de clés, VPN.

DIRECTEURS HABILITES : Damien Magoni.

DESCRIPTION DU SUJET : cf. ci-dessous.

2 Description du sujet de thèse

L'explosion des réseaux sociaux a mis en lumière l'importance de leur usage dans les communications d'aujourd'hui mais aussi les failles de leur fonctionnement. En effet, les sociétés qui hébergent ces réseaux font face à une situation de conflit d'intérêt. D'un côté, elles s'engagent à respecter la vie privée de leurs utilisateurs et de l'autre, elles ne peuvent générer de l'argent que par la divulgation de ces mêmes informations confidentielles. Croire en leur vertu serait faire preuve d'une grande naïveté. De plus, il est pratiquement impossible de savoir si elles mettent correctement en application le droit à l'oubli numérique.

Ce constat fait apparaitre le besoin de nouveaux outils non marchands permettant aux internautes de créer des réseaux sociaux limités à des groupes restreints d'utilisateurs et contrôlés par eux-mêmes. Ces réseaux seraient donc privés et virtuels au sens où ils seraient déployés au dessus de l'Internet public à l'instar des VPNs. L'objectif de cette thèse est de définir une architecture P2P permettant la création et la gestion de tels réseaux sociaux privés virtuels en partant du concept des VPNs. Cette architecture de communication entre membres d'un groupe fermé d'utilisateurs devra pouvoir être configurable pour fournir un réseau virtuel sécurisé et contrôlé par ses membres. Elle s'inspirera éventuellement de la solution libre Diaspora ou des solutions commerciales SocialGo, Frenzy, Tuenti ou Chattertree. L'architecture devra fournir des services pour l'authentification des membres ainsi que pour l'intégrité et la confidentialité

du trafic interne au réseau social. Elle devra aussi être capable de gérer la distribution des clés publiques des utilisateurs en utilisant éventuellement une DHT.

Cette architecture devra être définie en tenant compte des contraintes de l'architecture existante de l'Internet (e.g. NAT, firewalls, proxies, etc) et en utilisant les algorithmes et les protocoles de sécurité existants. Les performances de cette architecture seront évaluées par simulation puis par prototypage dans un environnement virtualisé puis dans l'Internet.

3 Plan de la thèse

1. Etablir un état de l'art des technologies et des logiciels liés aux réseaux sociaux publics (e.g., Facebook, Twitter, Flickr, Linkedin, etc) et privés (e.g., Diaspora, SocialGo, Frenzy, Chattertree, etc). Décrire les technologies réseaux actuelles permettant de fournir des services d'authentification, de confidentialité, et d'intégrité utilisables par les réseaux sociaux. Les protocoles réseaux liés à la sécurité seront présentés (e.g. IPSec, SSL, TLS, SSH, PGP, GPG, etc). Présenter en détail les travaux de recherche en cours ayant des objectifs similaires à cette thèse et se positionner par rapport à ceux-ci.
2. Définir les fonctionnalités requises par cette architecture, les services à fournir aux utilisateurs ainsi que les briques élémentaires constituant cette architecture.
3. Implémenter cette architecture dans un logiciel.
4. Effectuer des analyses et des simulations pour quantifier les performances de ce logiciel en termes de consommation de ressources.
5. Comparer les fonctionnalités et les performances de cette architecture avec d'autres solutions existantes en utilisant leurs implémentations respectives.
6. Effectuer des tests fonctionnels et des évaluations de performances dans un environnement virtualisé.
7. Déployer et valider le logiciel dans un environnement réel qui sera l'Internet lui-même.

4 Références bibliographiques

– Identifying Similar Neighborhood Structures in Private Social Networks. Singh, L. ; Schramm, C. ; Data Mining Workshops (ICDMW), 2010 IEEE International Conference on Digital Object Identifier : 10.1109/ICDMW.2010.165 Publication Year : 2010 , Page(s) : 507 - 516.
– Design and Implementation of FAITH, An Experimental System to Intercept and Manipulate Online Social Informatics. Ruaylong Lee ; Nia, R. ; Hsu, J. ; Levitt, K.N. ; Rowe, J. ; Wu, S.F. ; Shaozhi Ye ; Advances in Social Networks Analysis and Mining (ASONAM), 2011 International Conference on Digital Object Identifier : 10.1109/ASONAM.2011.86 Publication Year : 2011 , Page(s) : 195 - 202.
– A more comprehensive activity analysis of standard online social networking functionalities. Memic, H. ; Joldic, A. ; Software Technology and Engineering (ICSTE), 2010 2nd International Conference on Volume : 2 Digital Object Identifier : 10.1109/ICSTE.2010.5608773 Publication Year : 2010 , Page(s) : V2-108 - V2-111.
– Generalizing terrorist social networks with K-nearest neighbor and edge betweeness for social network integration and privacy preservation. Xuning Tang ; Yang, Christopher C. ; Intelligence and Security Informatics (ISI), 2010 IEEE International Conference on

Digital Object Identifier : 10.1109/ISI.2010.5484776 Publication Year : 2010 , Page(s) : 49 - 54.

– Enabling Secure Secret Sharing in Distributed Online Social Networks. Le-Hung Vu ; Aberer, K. ; Buchegger, S. ; Datta, A. ; Computer Security Applications Conference, 2009. ACSAC '09. Annual Digital Object Identifier : 10.1109/ACSAC.2009.46 Publication Year : 2009 , Page(s) : 419 - 428.