STAC: Un outil pour vous aider à sécuriser vos applications

Gyrard Amelie (gyrard@eurecom.fr)*
Christian Bonnet (bonnet@eurecom.fr)*
Karima Boudaoud (karima@polytech.unice.fr) †

Résumé : L'application STAC que nous proposons dans cet article, emploie les technologies du Web Sémantique, plus particulièrement une ontologie, afin de décrire et classifier les principaux concepts de sécurité : attaques, propriétés de sécurité, mécanismes de sécurité (protocoles, outils, concepts cryptographiques), technologies et modèle OSI. Nous avons également conçu la base de connaissance associée. Une première version du prototype (http ://securitytoolbox.appspot.com/) offre une interface graphique avec les concepts référencés dans l'ontologie et la base de connaissance.

Mots Clés : Sécurité, ontologie, web sémantique, attaques, mécanismes de sécurité, cryptographie, application sécurisée

1 Introduction

Sécuriser une application ou un projet nécessite un temps considérable lorsqu'ils utilisent diverses technologies (base de données, langages de programmation, frameworks, outils d'administration réseau, protocole de communication réseau). Un même mécanisme de sécurité ne peut être employé pour sécuriser toutes les technologies : les protocoles de sécurité conçus pour les réseaux Wi-Fi ne peuvent pas être utilisés pour sécuriser les réseaux de capteurs ou une application e-commerce. Afin de décrire les principaux concepts de sécurité et leurs relations, nous avons crée notre propre ontologie de sécurité.

Plusieurs ontologies de sécurité ont été définies [DKF05, HSD07, KLK05], malheureusement aucune d'entre elles n'a pour objectif d'aider le développeur non expert en sécurité à concevoir des applications sécurisées. De plus, ces ontologies ne classifient pas les différentes attaques et mécanismes de sécurité selon les couches du modèle OSI, leurs avantages et inconvénients et le fait qu'elles ont été conçues pour des technologies spécifiques. Les auteurs [ZMB+08] définissent seulement les attaques dans les réseaux de capteurs, mais n'introduisent pas les mécanismes de sécurité pour contrecarrer ces attaques. Une autre ontologie [NB12] décrit la sécurité dans les réseaux cellulaires : 2G (GSM), 3G (UMTS), 4G (LTE) mais ne précise pas que ces mécanismes de sécurité ne peuvent pas être réutilisés pour sécuriser une autre technologie.

∗. Eurecom, Mobile Communication Department, 450 Route des Chappes, 06410 Biot, France Tel : 33 (0) 4 93 00 81 00

†. Laboratoire I3S-CNRS/UNSA Ecole Polytechnique de l'Université de Nice Sophia Antipolis 930 Route des Colles - BP 145- 06903 Sophia Antipolis Cedex, France. Tel : 33 (0) 4 92 96 51 72

2 L'application STAC (Sécurité Toolbox : Attaques et Contre-mesures)

Un `mécanisme de sécurité` est un protocole de sécurité, un outil ou un concept cryptographique (algorithmes de chiffrement, signatures digitales, fonctions de hachages, protocoles de gestion de clés, etc.). Chaque mécanisme de sécurité a ses avantages et ses inconvénients : un chiffrement asymétrique est utilisé pour l'échange des clés, mais est consommateur en terme de ressources pour le chiffrement, les algorithmes symétriques sont plutôt utilisés pour chiffrer un message. Les `propriétés de sécurité` représentent l'authentification, l'integrité, les contrôles d'accès, etc... Nous avons décrit que les mécanismes de sécurité satisfont ces propriétés de sécurité (e.g., les algorithmes de chiffrement satisfont la propriété de confidentialité, les signatures digitales assurent l'authentification). Les `attaques` sont contrecarrées par des mécanismes de sécurité spécifiques et sont classées selon les couches du modèle OSI. Les `technologies` sont les applications web/mobiles (langage de programmation, base de donnée, framework, système d'exploitation, cloud), les réseaux cellulaires (2G/GSM, 3G/UMTS, 4G/LTE), les réseaux de capteurs, le Wi-Fi, le bluetooth, le filiaire (Ethernet), etc... L'ontologie STAC définit de nombreuses restrictions telles que : les réseaux de capteurs ne peuvent être sécurisés que par les mécanismes de sécurité inventés pour les réseaux de capteurs. Notre base de connaissances de sécurité est conçue selon l'ontologie STAC.

3 Conclusion et travaux futurs

L'application STAC, l'ontologie et la base de connaissances définissent les principaux concepts de sécurité associés à diverses technologies. Une évolution de STAC est de proposer à l'utilisateur, plus précisément au développeur, une interface graphique plus conviviale et de lui suggérer les mécanismes de sécurité les plus adaptés pour sécuriser son application (un formulaire serait à remplir avec les technologies utilisées dans l'application à sécuriser).

Références

[DKF05] G. Denker, L. Kagal, and T. Finin. Security in the semantic web using owl. *Information Security Technical Report*, 10(1) :51–58, 2005.

[HSD07] A. Herzog, N. Shahmehri, and C. Duma. An ontology of information security. *International Journal of Information Security and Privacy (IJISP)*, 1(4) :1–23, 2007.

[KLK05] A. Kim, J. Luo, and M. Kang. Security ontology for annotating resources. *On the Move to Meaningful Internet Systems 2005 : CoopIS, DOA, and ODBASE*, pages 1483–1499, 2005.

[NB12] H. Neji and R. Bouallegue. Roadmap for establishing interoperability of heterogeneous cellular network technologies-3. *International Journal of Computer Applications*, 54(5) :17–27, 2012.

[ZMB+08] W. Znaidi, M. Minier, J.P. Babau, et al. An ontology for attacks in wireless sensor networks. 2008.