Architectures PKI et communications sécurisées

Jean-Guillaume Dumas*[1], Pascal Lafourcade*†[2], and Patrick Redon‡

[1]Laboratoire Jean Kuntzmann (LJK) – CNRS : UMR5224, Université Grenoble Alpes – Tour IRMA 51 rue des Mathématiques - 53 38041 GRENOBLE CEDEX 9, France

[2]Laboratoire d'Informatique, de Modélisation et d'optimisation des Systèmes (LIMOS) – Institut Français de Mécanique Avancée, Université Blaise Pascal - Clermont-Ferrand II, Université d'Auvergne - Clermont-Ferrand I, CNRS : UMR6158 – Bât ISIMA Campus des Cézeaux BP 10025 63173 AUBIERE cedex, France

Résumé

Compte-tenu de la croissance du nombre d'objets connectés, mais également de l'augmentation de cyber-attaques, la sécurité des communications est une nécessité. Enseigner la sécurité n'est pas facile. Faut-il présenter un catalogues d'attaques, qui sont souvent obsolètes une fois celles-ci découvertes, ou bien présenter des primitives et protocoles cryptographiques. Dans l'ouvrage "Architectures PKI et communications sécurisées", Dunod 2015, nous avons essayé de couvrir à la fois les aspects fondamentaux de l'organisation d'architectures à clefs publiques (PKI) et leur utilisation dans la sécurisation des communications internet de tous les jours. Il présente les solutions fondamentales déployées aujourd'hui, avec leurs forces, leurs faiblesses et leurs défauts. Il est illustré par plus de cent vingt figures et plus de cinquante exercices corrigés.

Cet ouvrage est organisé de manière à donner au lecteur un aperçu général de tout ce qui concerne la cryptographie à clef publique et plus particulièrement des infrastructures de gestion de clefs (IGC, " Public Key Infrastructure – PKI ") nécessaires à la mise en place de cette cryptographie.

Il présente ensuite un panorama des techniques et protocoles permettant de réaliser des communications sûres, de X.509 à bitcoin. Le livre traite également du Référentiel Général de Sécurité (RGS), référentiel émis par l'Agence

Nationale de la Sécurité des Systèmes d'Information (ANSSI). Les Autorités Administratives comme les Opérateurs d'Importance Vitale au travers de la loi de programmation militaire sont incités à protéger leurs systèmes d'information,

en particulier par l'emploi de produits de sécurité labellisés par l'ANSSI et de se conformer aux règles et recommandations émises par celle-ci. Le traitement d'un tel sujet dans un livre est aujourd'hui unique.

Enfin, nous avons souhaité apporter un point de vue pratique complémentaire aux aspects théoriques des premiers chapitres. À cette fin deux chapitres sont dédiés aux déploiements. Le premier décrit la mise en oeuvre d'outils

librement disponibles tels PGP, OpenCA ou OpenSSL, dans l'objectif de donner au lecteur un premier tutoriel et une connaissance pratique du domaine. Le second décrit le déploiement industriel d'infrastructures, suite à des retours d'expériences recueillis auprès d'entreprises ayant mis en oeuvre de telles architectures.

*Intervenant

†Auteur correspondant: pascal.lafourcade@udamail.fr

‡Auteur correspondant: patrick_redon@yahoo.fr

En français les ouvrages traitant de PKI sont très rares et datent en général d'une dizaine d'année alors que le sujet a beaucoup évolué, notamment avec la généralisation des applications mobiles. Même en anglais, deux ou trois
ouvrages sont parus récemment mais aucun ne traite des aspects théoriques conjointement avec leur mise en oeuvre pratique (aspects déploiement industriel, communications sécurisées, certification et évaluation suivant les critières
communs, référentiel de général de sécurité).

Cet ouvrage s'adresse à tous les Master 1 d'informatique et Mathématiques pour une introduction au domaine, aux Master 2 spécialisés, aux enseignants-chercheurs du domaine mais aussi aux industriels désireux de développer des solutions informatiques robustes.

Mots-Clés: PKI, Infrastructures de gestion de clefs, communications sécurisées