Série modulaire sur la

Sécurité informatique

Fascicule 0:

Introduction à la série et Contenu des fascicules

Guy Lépine et Frédéric Mailhot

Université de Sherbrooke

Avril 2022

Note : En vue d'alléger le texte, le masculin est utilisé pour désigner les femmes et les hommes.

Document fascicule00.pdf
Version 3.14, Avril 2022

Département de génie électrique et de génie informatique, Université de Sherbrooke.
Réalisé à l'aide de LaTeX et TeXstudio.

Série sur la sécurité informatique

Cette série a pour objectif l'introduction à la cryptographie et la sécurité informatique. Ce vaste domaine touche à la fois la théorie des nombres, les algorithmes et méthodes de chiffrement, les systèmes logiciels et matériels en lien avec la sécurité des systèmes numériques, les différents types d'authentification, le calcul de résumés, le calcul de nombres aléatoires, etc. Tous ces éléments sont utiles à un niveau ou à un autre pour protéger les systèmes numériques (ordinateurs, téléphones, tablettes, contrôleurs matériels et autres). Cette série touche à un éventail de techniques et d'algorithmes permettent à tous ces systèmes d'opérer de façon sécuritaire, en protégeant leur intégrité, leur opération, ainsi que l'accès à leurs données. La série est composée d'une série de fascicules, chacun touchant un aspect spécifique de la sécurité informatique. Comme le domaine de la sécurité informatique évolue très rapidement, le nombre de fascicules est appelé à augmenter, pour couvrir de nouveaux concepts ou techniques. En ce moment, la série comporte huit fascicules :

Fascicule 1: Introduction à la cryptographie (Frédéric Mailhot)

Fascicule 2: Grands nombres et calculs rapides (Frédéric Mailhot)

Fascicule 3: Télématique et sécurité (Guy Lépine)

Fascicule 4: Cyberattaques et contre-mesures (Guy Lépine et Frédéric Mailhot)

Fascicule 5: Calcul de résumés (hachage) (Frédéric Mailhot)

Fascicule 6: Nombres aléatoires et pseudo-aléatoires (Frédéric Mailhot)

Fascicule 7: Techniques d'authentification (Frédéric Mailhot)

Fascicule 8: Cryptographie quantique et impact classique (Frédéric Mailhot)

Le premier fascicule couvre à la fois les techniques d'encryptage symétrique (à clé unique) et les techniques à doubles clés (privées et publiques). Il existe de nombreuses méthodes distinctes pour chacune des deux techniques, et nous présenterons les plus connues. Nous introduirons certains concepts provenant de

la théorie des nombres dans cette partie, puisqu'ils sont à l'origine de la majorité des méthodes d'encryptage à clés publiques et privées. Nous discuterons des vulnérabilités de certaines des méthodes d'encryptage et des moyens de protection. En particulier, nous présenterons plusieurs algorithmes de factorisation, dont les performances nous indiquent la taille des clés publiques/privées à utiliser pour bien sécuriser les messages cryptés. La performance des calculs effectués étant primordiale pour une utilisation efficace des méthodes d'encryptage, nous terminerons cette partie par un chapitre sur les méthodes efficaces de calcul des très grands nombres.

Le deuxième fascicule couvre les grands nombres, leur représentation ainsi qu'un ensemble de techniques de calcul rapide.

Le troisième fascicule s'attarde aux protocoles utilisés pour sécuriser les messages dans les systèmes d'information modernes. Il existe de nombreux standards qui datent de l'époque des premiers réseaux d'ordinateurs des années 1970. Depuis 1994 et la croissance explosive de l'internet, de nombreux standards et protocoles ont été proposés et mis en place pour l'échange sécurisé d'information, l'authentification d'usagers, la signature électronique de documents, etc.

Le quatrième fascicule s'occupe des vulnérabilités des systèmes d'information. On y parle des vulnérabilités des systèmes d'exploitation, des problèmes liés aux liens réseau, des outils et méthodes utilisés par les gens qui tentent d'utiliser les systèmes d'autrui à mauvais escient, de même que des outils et techniques de protection.

Le cinquième fascicule touche le calcul des résumés, c'est-à-dire les techniques de hachage. On y retrouve les éléments importants de ces techniques dans un contexte de sécurité des systèmes.

Le sixième fascicule se concentre sur la génération de nombres aléatoires et pseudo-aléatoires. L'importance de ces nombres est d'abord mis en lumière, puis plusieurs techniques à la fois logicielles et matérielles de génération de ces nombres sont présentées.

Le septième fascicule touche les techniques d'authentification. Les techiques ususalles sont présentées, ainsi que des méthodes alternatives, les avantages et inconvénients de chacune étant expliqués.

Le huitième fascicule présente certaines méthodes d'encryptage basées sur les phénomènes quantiques. Cette technologie commence tout juste à être utilisable à l'extérieur des laboratoires de recherche, mais présentera des possibilités impressionnantes lorsqu'on pourra la mettre en oeuvre sur une grande échelle.

Cette série s'intéresse à deux aspects complémentaires des systèmes d'information modernes : la sécurité et l'encryptage. Il est habituel de retrouver des livres qui portent soit sur les techniques d'encryptage, leurs limites, et les mathématiques sous-jacentes, soit sur les vulnérabilités des systèmes d'information, les méthodes employées pour les utiliser, ainsi que les façons de les minimiser et de

les contrôler. Pourtant, quoiqu'il s'agisse de deux champs très distincts, ils ont une influence notable l'un sur l'autre. En effet, la cryptographie est à la base des méthodes modernes d'authentification et de sécurisation des transactions à distance, permettant la définition de protocoles de transfert où l'information n'est compréhensible que par les parties concernées. Cependant, la cryptographie n'est qu'un des éléments essentiels à la sécurité de l'information. En effet, les ordinateurs modernes sont inter-connectés par des réseaux rapides qui en facilitent l'accès. Cet accès rapide et simple aux ordinateurs permet maintenant à des individus ou organisations mal intentionnés d'utiliser les systèmes d'autrui et l'information qu'ils contiennent. La sécurisation d'un système procède donc autant des méthodes d'encryptage modernes que de la compréhension des vulnérabilités des systèmes réseautiques récents et des protocoles et techniques utilisés pour les protéger. Cette série a pour objectif de couvrir ces deux aspects complémentaires dans un ensemble de fascicules relativement indépendants qui permettent de bien appréhender le domaine.

Contexte et historique

Ce document a été écrit au départ comme support des cours GIF-630, puis GIF-380 (Encryptage et sécurité informatique), donnés sous forme d'APP (apprentissage par problème) depuis 2004 au département de génie électrique et informatique de l'université de Sherbrooke. À partir l'automne 2007, le texte a été significativement augmenté et est utilisé comme référence dans six cours gradués formant les modules de spécialisation touchant la sécurité informatique, offerts à la maîtrise et aussi au baccalauréat en génie informatique: GEI-760 (Techniques avancées de cryptographie), GEI-761 (Télématique et protocoles sécurisés), GEI-762 (Sécurité des systèmes informatiques), GEI-771 (Programmation sécuritéd), GEI-772 (Sécurité web) et GEI-773 (Introduction à l'investigation numérique). Ces sept cours forment une progression qui a pour objectif de familiariser les étudiants tant à la cryptographie qu'à la sécurité informatique dans son sens plus large. Au printemps 2021, il a été décidé de scinder le livre original en une série de fascicules indépendants, intégrant la couverture originale de la matière et un ensemble de sujets et méthodes connexes, le tout en permettant un accès facilité aux différents aspects de la sécurité informatique.

Remerciements

Je remercie tous les étudiants en génie informatique et électrique qui ont lu ces textes et ont indiqué des erreurs, omissions ou explications peu claires, souvent en proposant des solutions ou exposés alternatifs. En particulier, merci à Maxime Albert-Gauthier, Francis Beaulé, Arthur Carré, François Charron, Mathieu Chevalier, Jean-François Desjeans-Gauthier, Éloïse Dubé, Jean-Sébastien

Goupil, Jean-Philippe Jodoin, Mohamed Firas Kammoun, Derek Labadie, Alexandre Mathieu, Pierre-Étienne Messier, Édouard Murat, Simon Poirier et Francis Ruel. Je remercie aussi les chargés d'exercices qui ont pris la peine de lire ce document et ont proposé de nouvelles idées. À cet égard, un merci spécial va à Joël Tran. Je remercie mes collègues Ruben Gonzalez-Rubio et Bernard Beaulieu, qui ont fait d'excellents commentaires au sujet de la structure de ce texte. Les discussions portant sur la pédagogie, avec mes collègues Daniel Dalle et Noël Boutin, ont aussi eu un impact sur ce texte.

F.M.

Contenu des fascicules

Fascicule 1: Introduction à la cryptographie

Fascicule 2: Grands nombres et calculs rapides

Fascicule 3: Télématique et sécurité

Fascicule 4: Cyperattaques et contre-mesures

Fascicule 5: Calcul de résumés (hachage)

Fascicule 6: Nombres aléatoires et pseudo-aléatoires

Fascicule 7: Techniques d'authentification

Fascicule 8: Cryptographie quantique et impact classique