BIBLIOTHÈQUE UNIVERSITAIRE DE NIORT

NOUVEAUTÉS EN RAYON

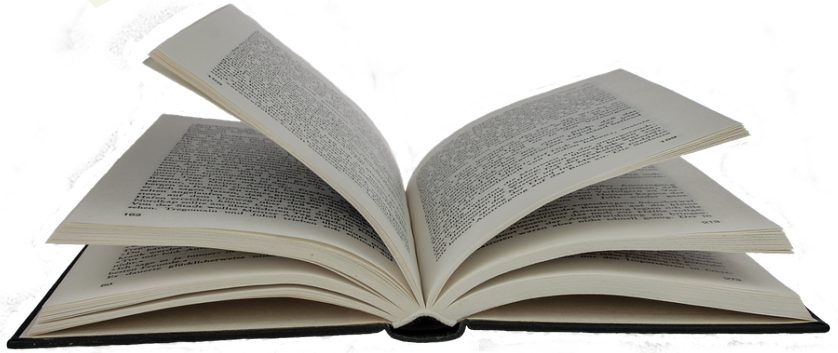
Juin 2021

SERVICE COMMUN DE DOCUMENTATION
Bibliothèques de l'Université de Poitiers

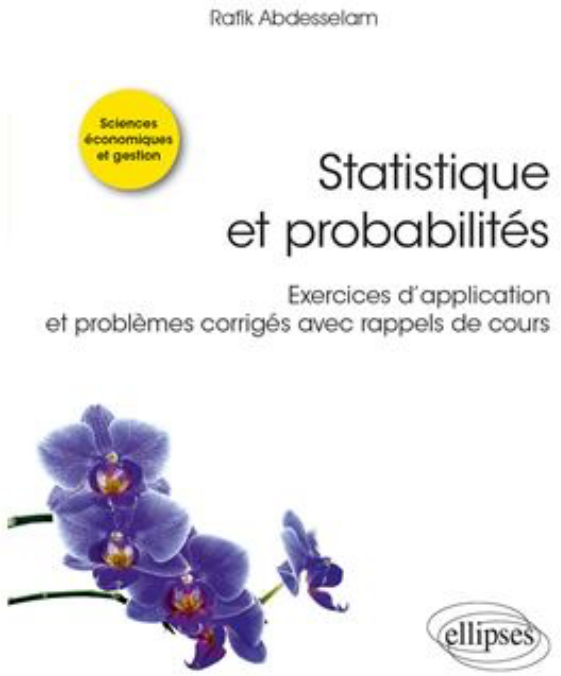
SOMMAIRE

Cliquez sur la discipline souhaitée, parcourez les pages pour découvrir nos nouveautés en rayon. Vous trouverez un lien à la fin de chaque discipline pour retourner au sommaire.

Bonne lecture ☺



Mathématiques et statistique :



Ce livre présente une synthèse rigoureuse de la théorie mathématique de la statistique et des probabilités. Sa présentation structurée avec une approche volontairement pratique facilite l'apprentissage et la compréhension. Il traite du calcul des probabilités et de modèles probabilistes et explique comment les appliquer à des problèmes bien concrets issus de la réalité. Tout en gardant une grande rigueur mathématique, il expose de façon claire et pédagogique les concepts de statistique et de probabilités.

Cote : 519.5 ABD

Réserver-le directement sur ODéBU en cliquant ici

Mathématiques et statistique :

La quantité de données collectées et stockées par les entreprises n'a jamais été aussi importante qu'aujourd'hui, entraînant un bond en avant de la statistique industrielle qui permet d'utiliser ces données dans le but de contrôler, fiabiliser et optimiser les procédés industriels.
Fruit de l'expérience d'un statisticien et d'une chercheuse, cet ouvrage à destination des ingénieurs détaille dans une première partie les quatre piliers de la statistique industrielle :

- l'analyse, l'évaluation et la maîtrise des systèmes de mesure ;
- la maîtrise statistique des procédés ;
- l'échantillonnage ;
- l'estimation.

Sept cas d'étude concrets issus de problèmes industriels dans des domaines aussi variés que la microélectronique, l'aéronautique, l'industrie pharmaceutique… viennent ensuite illustrer et développer la partie théorique pour apporter une approche terrain.

Cote : 519.5 BE

Réserver-le directement sur ODéBU+ en cliquant ici

Sécurité informatique :

Cet ouvrage est consacré à la sécurité des équipements informatiques : **les risques de hacking**, **virus**, **spams et autres malwares**, **et les solutions pour y remédier**. Cette nouvelle édition mise à jour et enrichie aborde notamment :

- les vulnérabilités des processeurs,
- la sécurité des nouveaux systèmes d'authentification,
- les nouvelles techniques d'attaque et de défense,
- la sécurité des réseaux sans fil,
- les institutions internationales et françaises de lutte contre le cybercrime,
- les méthodes d'évaluation du risque informatique en entreprise.

Un répertoire commenté d'adresses web incontournables en matière de sécurité complète l'ouvrage.

Cote : 005.8 PIL

Réserver-le directement sur ODéBU en cliquant ici

SERVICE COMMUN DE DOCUMENTATION
Bibliothèques de l'Université de Poitiers

Sécurité informatique :

En France, quelques chercheurs, souvent militaires, ont posé les bases de la réflexion cyberstratégique. Les spécialistes techniques du domaine, ingénieurs et techniciens cyber, possèdent également un savoir précieux. Il manquait une réflexion sur le niveau tactique, intermédiaire entre le stratégique et le technique. C'est l'objet de ce livre. A partir de trois modes tactiques de base — la sécurisation, la défense et l'offensif—, il est possible de concevoir une opération de cyberdéfense comme une opération classique avec ses missions et son organisation. La conduite des opérations du combat numérique soulève cependant de nombreuses questions : il s'agit d'analyser clairement ce que sont les premières briques tactiques du combat dans le cyberespace. La force, le cyberespace, l'arme, le tempo, la manoeuvre numérique, la mesure de l'efficacité, l'attribution, le ciblage, le renseignement... sont ainsi décrits pour mieux appréhender ce que peut être un combat dans le cyberespace. Finalement, la mission des militaires dans le cyberespace demeure une constante : combattre.

Cote : 005.8 LED

Réserver-le directement sur ODéBU+ en cliquant ici

SERVICE COMMUN DE DOCUMENTATION
Bibliothèques de l'Université de Poitiers

Sécurité informatique :

Ce livre sur la sécurité informatique (et le ethical hacking) s'adresse à tout informaticien sensibilisé au concept de la sécurité informatique mais novice ou débutant dans le domaine de la sécurité des systèmes d'information. Il a pour objectif d'initier le lecteur aux techniques des attaquants pour lui apprendre comment se défendre. Cette nouvelle édition tient compte de l'actualité en matière de sécurité informatique et voit l'apparition de deux nouveaux chapitres qui traitent de la sécurité des communications sans fil et du Black Market. L'ouvrage commence par une définition précise des différents types de hackers et de leurs objectifs. Les auteurs présentent la méthodologie d'une attaque et les moyens de repérer les failles par lesquelles s'insérer dans un système. Le chapitre sur le Social Engineering, ou manipulation sociale, illustre pourquoi les failles humaines représentent plus de 60% des attaques réussies. La prise d'empreintes, élément essentiel avant de lancer une attaque, est largement développée. Arrive le coeur du sujet avec les failles physiques, qui permettent un accès direct aux ordinateurs visés, ainsi que les failles réseaux et Wi-Fi, illustrées avec à chaque fois des propositions de contre-mesures. La sécurité sur le web est également traitée et les failles courantes identifiées à l'aide d'outils qui peuvent facilement être mis en place par le lecteur sur ses propres systèmes. L'objectif est toujours d'identifier les failles possibles pour ensuite mettre en place la stratégie de protection adaptée. Viennent ensuite les failles systèmes sous Windows ou Linux avec l'arrivée des nouvelles versions de ces systèmes et les failles applicatives introduisant quelques éléments pour se familiariser au langage assembleur et ainsi mieux comprendre les possibilités d'attaque. Suivent des chapitres sur le Forensic, les Box, omniprésentes dans nos maisons, les failles Hardware et le Black Market. Finalement les aspects juridiques sont traités dans un dernier chapitre qui intègre notamment les dispositions du Règlement européen sur la Protection des Données (RGPD/GDPR). Les auteurs de ce livre composent une équipe de personnes de conviction qui se donnent pour mission de rendre la sécurité informatique accessible à tous : "apprendre l'attaque pour mieux se défendre" est leur adage. Hackers blancs dans l'âme, ils ouvrent au lecteur les portes de la connaissance underground.

Cote : 005.8 SEC

Réserver-le directement sur ODéBU+ en cliquant ici

Sécurité informatique :

Ce livre décrit les techniques et la méthodologie utilisées par les professionnels de l'analyse de malwares (ou logiciels malveillants). Il s'adresse à des informaticiens passionnés de sécurité, à des professionnels dans le domaine de la sécurité informatique, qui souhaitent une approche opérationnelle et hautement technique. L'auteur commence par l'identification et la classification des malwares, il décrit ensuite les collectes rapportées par des investigations numériques légales (inforensiques) puis les analyse. Ces collectes comportent des images disque, des journaux d'évènements, mais aussi des images mémoire. Les outils et techniques permettant d'analyser ces données sont décrits avec de nombreux exemples. Après avoir identifié le malware, il convient de l'analyser. L'auteur explique le fonctionnement des outils de sandboxes et décrit des formats de fichier comme les documents PDF, Microsoft Office ou encore les binaires Windows. Afin de réaliser des analyses extrêmement techniques, le livre contient un chapitre entier sur le reverse engineering (ou rétro-ingénierie), l'auteur y explique les bases de l'assembleur (x86 et x64) et l'utilisation d'outils d'analyse statique tel que Ghidra et Radare2 ou de debuggers tels que Immunity Debugger et WinDBG. En complément sur ce sujet du reverse engineering, un chapitre explique les techniques d'obfuscation utilisées par les malwares, telles que l'obfuscation de chaînes de caractères ou l'utilisation de packers. L'auteur détaille les techniques permettant de dépacker des binaires packés. Deux chapitres sont dédiés à l'analyse de malwares sous systèmes mobiles : le système d'exploitation Android de Google et celui d'Apple : iOS. La dernière partie de ce livre parcourt les méthodes permettant d'éradiquer les malwares précédemment identifiés et analysés. Le livre est illustré d'exemples d'analyses de véritables malwares et les techniques présentées ont toutes été validées sur des cas réels. Tous les codes sources du livre sont en téléchargement sur le site www.editions-eni.fr. Paul RASCAGNERES, tout au long de sa carrière, a créé en Europe diverses équipes de réponses à incidents, il a également réalisé de nombreuses analyses de codes malveillants complexes pour un éditeur d'anti-virus. Il travaille aujourd'hui dans une équipe de Cyber Threat Intelligence, au sein de laquelle il a pour mission l'analyse de malwares lors d'incidents de sécurité ou lors de projets de recherche. Il participe également activement à la communauté anti-malware et est l'auteur de nombreuses publications. Conférencier à l'international (Europe, Asie, Amérique) sur l'analyse de malwares, il partage dans ce livre ses connaissances dans ce domaine de la sécurité.

Cote : 005.8 RAS

Réserver-le directement sur ODéBU+ en cliquant ici

N’hésitez pas à partager cette liste et à nous signaler des nouveaux ouvrages

Elena Razzoli
Médiatrice documentaire,
responsable acquisitions en risques, économie, informatique et statistiques

Bibliothèque du Pôle Universitaire de Niort
11, rue Archimède
79000 Niort
Tél. 05 49 24 99 96

Retour au sommaire