

Sécurité informatique

3^e édition

Principes et méthodes

Laurent Bloch

Christophe Wolfhugel

Préfaces de Christian Queinnec et d'Hervé Schauer

Avec la contribution de Nat Makarévitch

© Groupe Eyrolles, 2007, 2009, 2011, ISBN : 978-2-212-13233-5

EYROLLES



Table des matières

Avant-propos	1
PREMIÈRE PARTIE	
Principes de sécurité du système d'information	5
CHAPITRE I	
Premières notions de sécurité	7
Menaces, risques et vulnérabilités	7
Aspects techniques de la sécurité informatique	9
Définir risques et objets à protéger	10
Identifier et authentifier	11
Empêcher les intrusions	12
Concevoir la défense en profondeur	13
Aspects organisationnels de la sécurité	14
Abandonner les utilisateurs inexpérimentés aux requins?	14
Externalisation radicale et accès Web	16
Sauvegarder données et documents	17
Vérifier les dispositifs de sécurité	17
La nécessaire veille auprès des CERT	18
Organisation des CERT	18
Faut-il publier les failles de sécurité?	19
Le management de la sécurité	21

Les systèmes de management	21
Le système de management de la sécurité de l'information	22
Un modèle de maturité?	25
Critères communs	26
Faut-il adhérer aux normes de sécurité de l'information?	26
Un projet de certification de sécurité Open Source : OSSTMM	28
Législation financière et système d'information	29
Prolifération des systèmes de contrôle et d'audit	30
Sauvés par la régulation?	31
Brève critique de la sécurité financière	31
La sécurité procédurale n'est pas la solution	32
Richard Feynman à propos de la conduite de projet	36
 CHAPITRE 2	
Les différents volets de la protection du SI	39
L'indispensable sécurité physique	39
Protéger le principal : le système d'exploitation	41
Droits d'accès	42
Vérification des droits, imposition des protections	43
Gérer l'authentification	44
Séparation des privilèges	44
Identification et authentification	45
Le bon vieux mot de passe	47
Listes de contrôle d'accès	48
Le chiffrement asymétrique	49
Comprendre les failles et les attaques sur les logiciels	53
L'attaque par interposition (Man in the middle)	54
Vulnérabilité des cryptosystèmes	54
 CHAPITRE 3	
Malveillance informatique	57
Types de logiciels malveillants	57
Virus	58
Virus réticulaire (botnet)	59
Ver	62
Cheval de Troie	62

Porte dérobée	62
Bombe logique	62
Logiciel espion	62
Courrier électronique non sollicité (spam)	64
Attaques sur le Web et sur les données	65
Injection SQL	65
Cross-site scripting	66
Palimpsestes électroniques	67
Matériels de rebut	67
Lutte contre les malveillances informatiques	68
Antivirus	68
Les techniques de détection	70
Des virus blindés pour déjouer la détection	71
Quelques statistiques	73

DEUXIÈME PARTIE

Science de la sécurité informatique	75
--	-----------

CHAPITRE 4

La clé de vôte : le chiffrement	77
Chiffrement symétrique à clé secrète	78
Naissance de la cryptographie informatique : Alan Turing	79
Data Encryption Standard (DES)	80
Diffie et Hellman résolvent l'échange de clés	81
Le problème de l'échange de clés	81
Fondements mathématiques de l'algorithme Diffie-Hellman	82
Mise en œuvre de l'algorithme Diffie-Hellman	85
Le chiffrement asymétrique à clé publique	87
Évaluer la robustesse d'un cryptosystème	91
Robustesse du chiffrement symétrique	91
Robustesse du chiffrement asymétrique	92
Responsabilité de l'utilisateur de cryptosystème	92

CHAPITRE 5

Sécurité du système d'exploitation et des programmes	95
Un modèle de protection : Multics	95
Les dispositifs de protection de Multics	96
Protection des systèmes contemporains	98
Débordements de tampon	98
Attaques par débordement sur la pile	99
Débordement de tampon : exposé du cas général	102
Débordement de tampon et langage C	104
Sécurité par analyse du code	105
Analyses statiques et méthodes formelles	105
Méthode B	105
Perl en mode souillé	107
Séparation des privilèges dans le système	108
Architectures tripartites	109

CHAPITRE 6

Sécurité du réseau	111
Modèle en couches pour les réseaux	111
Application du modèle à un système de communication	112
Modèle ISO des réseaux informatiques	114
Une réalisation : TCP/IP	116
Les réseaux privés virtuels (VPN)	120
Principes du réseau privé virtuel	120
IPSec	121
Autres réseaux privés virtuels	123
Comparer les procédés de sécurité	124
Partager des fichiers à distance	125
Sécuriser un site en réseau	128
Segmentation	128
Filtrage	129
Pare-feu	131
Listes de contrôle d'accès pour le réseau	139
Les pare-feu personnels pour ordinateurs sous Windows	139
Le système de noms de domaines (DNS)	145
Fonctionnement du DNS	145

Un espace abstrait de noms de serveurs et de domaines	146
Autres niveaux de domaines	148
Conversations entre serveurs de noms	149
Sécurité du DNS	151
Traduction d'adresses (NAT)	153
Le principe du standard téléphonique d'hôtel	154
Adresses non routables	155
Accéder à l'Internet sans adresse routable	155
Réalizations	156
Une solution, quelques problèmes	158
Promiscuité sur un réseau local	160
Rappel sur les réseaux locaux	160
Réseaux locaux virtuels (VLAN)	162
Sécurité du réseau de campus : VLAN ou VPN?	163
Réseaux sans fil et sécurité	164
Types de réseaux sans fil	165
Vulnérabilités des réseaux sans fil 802.11	166
CHAPITRE 7	
Identités, annuaires, habilitations	173
Qu'est-ce que l'identité dans un monde numérique?	173
Problématique de l'identification	173
Trois types d'usage des identifiants	174
Vers un système universel d'identifiants	176
Distinguer adresses de localisation et d'identification?	177
La politique des identifiants	178
Distinguer noms et identifiants dans le DNS?	178
Pretty Good Privacy (PGP) et signature	179
Créer un réseau de confiance	182
Du trousseau de clés à l'IGC	182
Annuaire électronique et gestion de clés	183
Risques liés aux systèmes d'identification	184
Organiser un système d'identité numérique	186
Objectif SSO	186
Expérience de terrain	186

TROISIÈME PARTIE

Politiques de sécurité du système d'information 189

CHAPITRE 8

Une charte des utilisateurs 191

Préambule de la charte 192

Définitions 192

Accès aux ressources et aux services 193

Règles d'utilisation, de sécurité et de bon usage 193

Confidentialité 194

Respect de la législation 195

Préservation de l'intégrité des systèmes informatiques 195

Usage des services Internet (Web, messagerie, forum...) 196

Règles de bon usage 196

Publication sur l'Internet 197

Responsabilité légale 197

Dispositifs de filtrage de trafic 197

Surveillance et contrôle de l'utilisation des ressources 198

Rappel des principales lois françaises 198

Application 198

CHAPITRE 9

Une charte de l'administrateur système et réseau 201

Complexité en expansion et multiplication des risques 202

Règles de conduite 203

Secret professionnel 203

Mots de passe 204

Proposition de charte 205

Définitions 206

Responsabilités du comité de coordination SSI 207

Responsabilités de l'administrateur de système et de réseau 207

Mise en œuvre et litiges 210

CHAPITRE 10

Une politique de sécurité des systèmes d'information 211

Préambule : les enjeux de la PSSI 211

Contexte et objectifs	212
Le contexte de l'INSIGU	212
Périmètres de sécurité	213
Lignes directrices pour la sécurité	214
Menaces, risques, vulnérabilités	217
Organisation et mise en œuvre	218
Organisation de la sécurité des systèmes d'information (SSI)	218
Coordination avec les autres organismes	222
Principes de mise en œuvre de la PSSI	223
Protection des données	225
Sécurité du système d'information	227
Mesure du niveau effectif de sécurité	231

QUATRIÈME PARTIE

Avenir de la sécurité informatique **235**

CHAPITRE II

Nouveaux protocoles, nouvelles menaces **237**

Le modèle client-serveur 237

Versatilité des protocoles : encapsulation HTTP 239

 Tous en HTTP! 239

 Vertus de HTTPS 240

Protocoles pair à pair (peer to peer) 240

 Définition et usage du pair à pair 240

 Problèmes à résoudre par le pair à pair 241

 Le pair à pair et la sécurité 243

 Exemples : KaZaA et Skype 244

 Franchir les pare-feu : vers une norme? 248

Téléphonie IP : quelques remarques 249

 Une grande variété de protocoles peu sûrs 250

 Précautions pour la téléphonie IP 250

BlackBerry 252

CHAPITRE I2

Tendances des pratiques de sécurisation des SI	255
Les six idées les plus stupides en sécurité, selon Ranum	256
Idée stupide n° 1 : par défaut, tout est autorisé	256
Idée stupide n° 2 : prétendre dresser la liste des menaces	257
Idée stupide n° 3 : tester par intrusion, puis corriger	258
Idée stupide n° 4 : les pirates sont sympas	259
Idée stupide n° 5 : compter sur l'éducation des utilisateurs	260
Idée stupide n° 6 : l'action vaut mieux que l'inaction	261
Quelques idioties de seconde classe	261
Les cinquante prochaines années	262
Détection d'intrusion, inspection en profondeur	262
Pare-feu à états	263
Détection et prévention d'intrusion	263
Inspection en profondeur	263
Critique des méthodes de détection	263
À qui obéit votre ordinateur?	264
Conflit de civilisation pour les échanges de données numériques	265
Dispositifs techniques de prohibition des échanges	266
Informatique de confiance, ou informatique déloyale?	269
Mesures de rétorsion contre les échanges de données	270
Signature électronique et sécurité des échanges	277
Gestion des droits numériques et politique publique	278

CHAPITRE I3

Sécurité informatique : dimension géostratégique	281
Les acteurs et leur terrain	282
Organisation de l'Internet	283
Le contexte économique	284
Du monopole au pluralisme	284
Internet et téléphonie classique : deux conceptions	285
L'hégémonie américaine en question	287
Un point stratégique : les noms de domaine (DNS)	287
L'opposition stérile des Européens	289
La réaction de la Chine	289
Un système de noms de domaine à deux étages	290

Quelles armes pour la guerre sur Internet?	291
Estonie et Géorgie	293
WikiLeaks	294
Stuxnet	297
Tunisie, Égypte : Internet pour la liberté	298
Peut-on éteindre l'Internet?	299
Par attaque à la racine du DNS?	299
Par attaque sur le routage?	300
La cybersécurité en 2011	301
Conclusion	303
Bibliographie	307
Index	319