

Sécurité

informatique

Principes et méthode

Laurent Bloch
Christoph Wolfhugel

Préfaces de
Christian Queinnec et Hervé Schauer

Avec la contribution de Solveig,
Florence Henry et Nat Makarévitch

© Groupe Eyrolles, 2007,
ISBN : 2-212-12021-4
ISBN 13 : 978-2-212-12021-9

EYROLLES



Table des matières

Avant-propos	1
PREMIÈRE PARTIE	
Principes de sécurité du système d'information	5
CHAPITRE 1	
Premières notions de sécurité	7
Menaces, risques, vulnérabilités	7
Aspects techniques de la sécurité	9
Définir risques et objets à protéger	9
Identifier et authentifier	11
Empêcher les intrusions	12
Défense en profondeur	13
Aspects organisationnels de la sécurité	14
Abandonner les utilisateurs inexpérimentés aux requins ?	14
Externalisation radicale ?	15
Sauvegarder données et documents	16
Vérifier les dispositifs de sécurité	17
S'informer auprès des CERT	17
Organisation des CERT	18
Faut-il publier les failles de sécurité ?	18

Le management de la sécurité	20
Les systèmes de management	20
Le système de management de la sécurité de l'information	21
Un modèle de maturité ?	24
Critères communs	24
Faut-il adhérer aux normes de sécurité de l'information ?	24
Législation financière et système d'information	26
Législation financière et SI	27
Brève critique de la sécurité financière	28
La sécurité procédurale n'est pas la solution	29
Richard Feynman à propos de la conduite de projet	32

CHAPITRE 2

Les différents volets de la protection du SI	35
L'indispensable sécurité physique	35
Protéger le principal : le système d'exploitation	37
Droits d'accès	37
Vérification des droits, imposition des protections	39
Gérer l'authentification	40
Séparation des privilèges	40
Identification et authentification	41
Le bon vieux mot de passe	43
Listes de contrôle d'accès	44
Le chiffrement asymétrique	45
Comprendre les failles et les attaques sur les logiciels	49
L'attaque par interposition (<i>Man in the middle</i>)	50
Vulnérabilité des cryptosystèmes	50

CHAPITRE 3

Malveillance informatique	53
Types de logiciels malveillants	53
Virus	54
Virus réticulaire (<i>botnet</i>)	55

Ver	56
Cheval de Troie	57
Porte dérobée	57
Bombe logique	57
Logiciel espion	57
Courrier électronique non sollicité (<i>spam</i>)	60
Attaques sur le Web et sur les données	60
Injection SQL	61
<i>Cross-site scripting</i>	62
Palimpsestes électroniques	62
Matériels de rebut	62
Lutte contre les malveillances informatiques	63
Antivirus	63
Les techniques de détection	65
Des virus blindés pour déjouer la détection	66
Quelques statistiques	67

DEUXIÈME PARTIE

Science de la sécurité du système d'information 69

CHAPITRE 4

La clé de voûte : le chiffrement 71

Chiffrement symétrique à clé secrète	72
Naissance de la cryptographie informatique : Alan Turing	73
<i>Data Encryption Standard (DES)</i>	74
Diffie et Hellman résolvent l'échange de clés	75
Le problème de l'échange de clés	75
Fondements mathématiques de l'algorithme Diffie-Hellman	76
Mise en œuvre de l'algorithme Diffie-Hellman	79
Le chiffrement asymétrique à clé publique	81
Évaluer la robustesse d'un cryptosystème	85
Robustesse du chiffrement symétrique	85
Robustesse du chiffrement asymétrique	86

Robustesse de l'utilisateur de cryptosystème	86
--	----

CHAPITRE 5

Sécurité du système d'exploitation et des programmes 89

Un modèle de protection : Multics	89
---	----

Les dispositifs de protection de Multics	91
--	----

Protection des systèmes contemporains	91
--	-----------

Débordements de tampon	92
---	-----------

Attaques par débordement sur la pile	93
--	----

Débordement de tampon : exposé du cas général	97
---	----

Débordement de tampon et langage C	97
--	----

Sécurité par analyse du code	98
---	-----------

Analyses statiques et méthodes formelles	98
--	----

Méthode B	99
---------------------	----

Perl en mode souillé	100
--------------------------------	-----

Séparation des privilèges dans le système	101
--	------------

Architectures tripartites	102
--	------------

CHAPITRE 6

Sécurité du réseau 105

Modèle en couches pour les réseaux	106
---	------------

Application du modèle à un système de communication	106
---	-----

Modèle ISO des réseaux informatiques	108
--	-----

Une réalisation : TCP/IP	110
------------------------------------	-----

Les réseaux privés virtuels (VPN)	114
--	------------

Principes du réseau privé virtuel	114
---	-----

IPSec	115
-----------------	-----

Autres réseaux privés virtuels	117
--	-----

Comparer les procédés de sécurité	118
--	------------

Partager des fichiers à distance	119
---	------------

Sécuriser un site en réseau	121
--	------------

Segmentation	122
------------------------	-----

Filtrage	123
--------------------	-----

Pare-feu	125
Listes de contrôle d'accès pour le réseau	132
Les pare-feu personnels pour ordinateurs sous <i>Windows</i>	133
Le système de noms de domaines (DNS)	138
Fonctionnement du DNS	139
Un espace abstrait de noms de serveurs et de domaines	140
Autres niveaux de domaines	142
Conversations entre serveurs de noms	143
Sécurité du DNS	145
Traduction d'adresses (NAT)	147
Le principe du standard téléphonique d'hôtel	148
Adresses non routables	149
Accéder à l'Internet sans adresse routable	149
Réalizations	150
Une solution, quelques problèmes	152
Promiscuité sur un réseau local	154
Rappel sur les réseaux locaux	154
Réseaux locaux virtuels (VLAN)	156
Sécurité du réseau de campus : VLAN ou VPN ?	157
Réseaux sans fil et sécurité	158
Types de réseaux sans fil	159
Vulnérabilités des réseaux sans fil 802.11	160

CHAPITRE 7

Identités, annuaires, habilitations	167
Qu'est-ce que l'identité dans un monde numérique ?	167
Problématique de l'identification	168
Trois types d'usage des identifiants	168
Vers un système universel d'identifiants	170
La politique des identifiants	171
Distinguer noms et identifiants dans le DNS ?	172
<i>Pretty Good Privacy (PGP) et signature</i>	173

Créer un réseau de confiance	175
Du trousseau de clés à l'IGC	175
Annuaire électronique et gestion de clés	176
Risques liés aux systèmes d'identification	177
Organiser un système d'identité numérique	179
Objectif SSO	179
Expérience de terrain	179

TROISIÈME PARTIE

Politiques de sécurité du système d'information 183

CHAPITRE 8

Une charte des utilisateurs 185

Préambule de la charte	186
Définitions	186
Accès aux ressources et aux services	187
Règles d'utilisation, de sécurité et de bon usage	187
Confidentialité	188
Respect de la législation	189
Préservation de l'intégrité des systèmes informatiques	189
Usage des services Internet (Web, messagerie, forum...)	190
Règles de bon usage	190
Publication sur l'Internet	191
Responsabilité légale	191
Dispositifs de filtrage de trafic	191
Surveillance et contrôle de l'utilisation des ressources	192
Rappel des principales lois françaises :	192
Application	192

CHAPITRE 9

Une charte de l'administrateur système et réseau 195

Complexité en expansion et multiplication des risques	196
Règles de conduite	197

Secret professionnel	197
Mots de passe	198
Proposition de charte	199
Définitions	200
Responsabilités du comité de coordination SSI	201
Responsabilités de l'administrateur de système et de réseau	201
Mise en œuvre et litiges	204

QUATRIÈME PARTIE

Avenir de la sécurité du système d'information 205

CHAPITRE 10

Nouveaux protocoles, nouvelles menaces 207

Le modèle client-serveur	207
Versatilité des protocoles : encapsulation HTTP	209
Tous en HTTP!	209
Vertus de HTTPS	209
Protocoles poste à poste (<i>peer to peer</i>)	210
Définition et usage du poste à poste	210
Problèmes à résoudre par le poste à poste	211
Le poste à poste et la sécurité	213
Exemples : KaZaA et Skype	214
Franchir les pare-feu : vers une norme ?	218
Téléphonie IP : quelques remarques	219
Une grande variété de protocoles peu sûrs	219
Précautions pour la téléphonie IP	220

CHAPITRE 11

Tendances des pratiques de sécurisation des SI 223

Les six idées les plus stupides en sécurité, selon Ranum	224
Idée stupide n° 1 : par défaut, tout est autorisé	224
Idée stupide n° 2 : prétendre dresser la liste des menaces	225
Idée stupide n° 3 : tester par intrusion, puis corriger	226

Idée stupide n° 4 : les pirates sont sympas	227
Idée stupide n° 5 : compter sur l'éducation des utilisateurs	228
Idée stupide n° 6 : l'action vaut mieux que l'inaction	229
Quelques idioties de seconde classe	229
Les cinquante prochaines années	230
Détection d'intrusion, inspection en profondeur	230
Pare-feu à états	231
Détection et prévention d'intrusion	231
Inspection en profondeur	231
Critique des méthodes de détection	231
À qui obéit votre ordinateur ?	232
Conflit de civilisation pour les échanges de données numériques	233
Dispositifs techniques de prohibition des échanges	234
Informatique de confiance, ou informatique déloyale ?	237
Mesures de rétorsion contre les échanges de données	238
Gestion des droits numériques (DRM) et politique publique	240
Conclusion	243
Bibliographie	247
Index	255