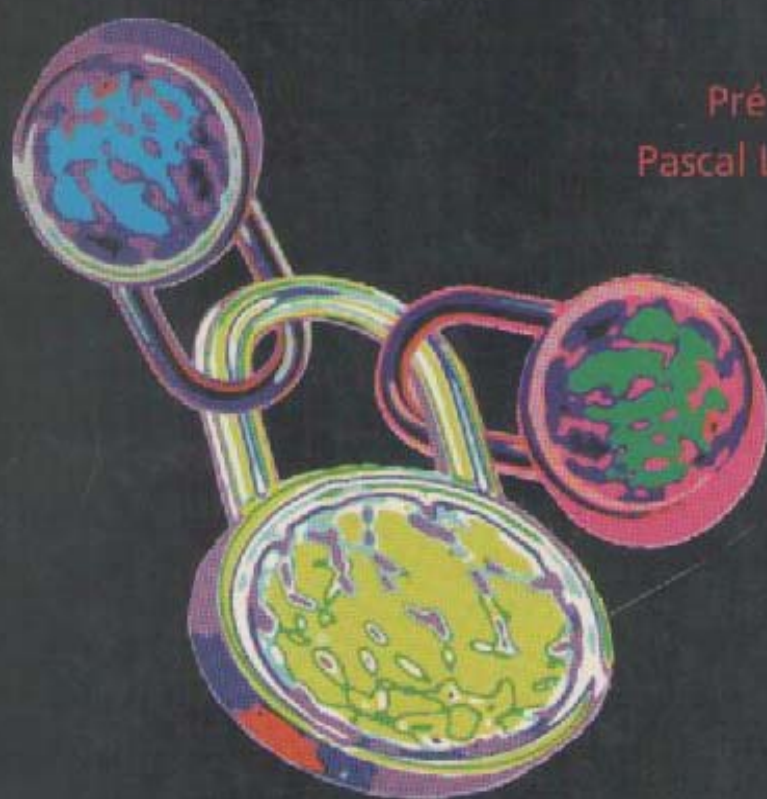


DAVID J. STANG
SYLVIA MOON

Sécurité réseaux

Préface de
Pascal Lointier



DUNOD

2-005-13-1

2-005-13-1

DAVID J. STANG • SYLVIA MOON

Sécurité réseaux



*Traduit de l'américain par
Vincent Grenet, Pascal Lointier, Francis Piérot*

DUNOD

TABLE DES MATIÈRES

PRÉFACE

PARTIE 1

QUELS RISQUES ?

1. LISTE DES RISQUES 2

Acheminement erroné 4

Analyseur de protocole 4

Bombe logique 5

Cheval de Troie 6

Contrefaçon 7

Compromission 7

Doublon 7

Écoute 8

Erreur de développement 9

Erreur d'exploitation 10

Faux rapport 10

Fouille des ordures 11

Fraude 12

Incendie 12

Information obsolète 13

Mascarade 13

Panne matérielle 14

Piratage 15

Porte dérobée (Back / Trapdoor)	16
Restriction d'emploi	16
Sabotage	17
Sabotage immatériel	17
Surcharge	18
Virus	18
Vols d'équipements	19
Vol de temps machine et vol de ressources	20

2. UN PEU DE RÉFLEXION 22

Terminologie	23
Gestion des risques	23
Quelques principes de base	27
Psychologie du risque	28
Menace perçue et réelle	28
Désinformation	28
Sous-inquiétude	32
Compréhension des événements rares	33
Quelques faits à propos des risques	34
Principes de base de l'analyse de risques	37
Avantages d'une analyse	37
Quand faut-il y recourir ?	37
Participants	37
Stratégies de réduction des risques	38
Fréquence ou gravité de la perte ?	38
Analyse des coûts et bénéfices	39
Mesurer les stratégies	40

3. ÉVALUER LES RISQUES 42

Difficultés	43
Effets de l'architecture	44
Créer des catégories : structures des expositions	44

Études existantes	45
Étude de EXECUTIVE INFORMATION NETWORK : fréquence	45
Étude de COOPERS & LYBRAND : gravité	46
SAFEWARE : fréquence et gravité	47
Panel de Delphi	48
Fonctionnement du panel	49
Exemple de panel de Delphi	50
Résultats du questionnaire	50
Commentaires	52
Méthodes de classement	52
Approche par audit	55
Score des fonctionnalités	57
Calcul d'un indice de risque	58
Approche par questionnaires	60
En bref	62

4. OUTILS ET SERVICES 64

Choisir un outil d'analyse des risques	65
Premier aperçu	65
Éléments fondamentaux d'un outil d'analyse	66
Critères de sélection spécifiques	69
Processus de sélection	72
Outils	75
@RISK	75
ALRAM	
(AUTOMATED LIVERMORE RISK ANALYSIS METHODOLOGY)	76
APPLICATION CONTROL MATRIX	76
BDSS (BAYESIAN DECISION SUPPORT SYSTEM)	77
BUDDY SYSTEM	77
CONTRAT (CONTROL MATRIX)	79
CONTROL-IT	79
CRAMM	
(CCTA RISK ANALYSIS AND MANAGEMENT METHODOLOGY)	80

CRITI-CALC	81
GRA/SYS	81
IST/RAMP (INTERNATIONAL SECURITY TECHNOLOGY / RISK ANALYSIS MANAGMENT PROGRAM)	82
JANBER	82
LAVA (LOS ALAMOS VULNERABILITY AND RISK ASSESSMENT)	83
LRAM (LIVERMORE RISK ANALYSIS METHODOLOGY)	83
MARION (METHODOLOGIE D'ANALYSE DE RISQUE PAR OPTIMISATION DES NIVEAUX)	84
MICROSECURE SELF ASSESSMENT)	84
MINIRISK	85
PRISM	85
QUICKRISK	86
RANK-IT	86
RA/SYS (RISK ANALYSIS SYSTEM)	87
RISKPAC	87
RISKWATCH	90
SOS (SECURITY ONLINE SYSTEM)	90

Services 91

5. VOS PROPRES RISQUES 94

Utilisation du questionnaire	95
Protection du bureau	96
Protection des stations de travail	101
Protection du serveur	105
Protection des applications et des données	115
Protection des imprimantes réseau	117
Protection du câblage entre stations et serveur	118
Protection des connexions externes	119

PARTIE 2

QUELQUES MENACES PRÉCISES

6. LES ACTEURS 124

Les directeurs 125

Les professionnels de la sécurité informatique 126

Les administrateurs de réseaux locaux 128

Les utilisateurs 129

Les avis différent 130

La faute à qui ? 130

Distinguer les utilisateurs 131

Les hackers 132

Etendue du problème 132

Pseudonymes 136

Organisation 136

Sous-groupes 137

Rareté 138

Origine du terme hacker 138

Convictions 138

L'attaque 139

Qualités personnelles 140

L'âge du hacker 143

Quelques mobiles 144

Quelques hackers 144

Comment attraper un hacker 148

Réagir à une effraction 148

Faut-il blâmer la victime ? 148

Effraction et intrusion 149

En fin de compte 150

L'auto-défense est-elle nécessaire ? 151

Les autres intrus 151

Répartir la faute 151

7. RÉSEAU ET RISQUES 154

Réseaux en bus 155

Réseaux connectés téléphoniquement 156

Réseaux hétérogènes 156

Points faibles 156

Mesures appropriées 157

Réseaux locaux 157

Points forts 157

Points faibles 158

Réseaux maillés 158

Points faibles 158

Mesures appropriées 158

Réseaux à commutation de paquets 159

Réseaux en anneau 159

Réseaux SNA 159

Réseaux en étoile 160

Points forts 161

Points faibles 161

Mesures appropriées 161

8. VIRUS 162

Qu'est-ce qu'un virus ? 163

Qu'infecte un virus ? 163

Comment un virus infecte-t-il un secteur de démarrage ? 165

Comment un virus infecte-t-il un fichier ? 165

Qui écrit des virus ? 167

D'où viennent les virus ? 169

Comment attrape-t-on un virus ? 169

Création de nouveaux virus 170

Les virus sont-ils fréquents ? 171

Quels dégâts ?	172
Quel est le coût des dommages ?	173
Quels sont les virus les plus courants ?	174
Les meilleurs logiciels	176
Autodéfense par le bon sens	179
Prévenir l'infection	179
Fausse alarmes	180
Passons aux choses sérieuses	181

9. NETWARE ET LES VIRUS 184

Fondements	185
Ce que nous avons testé	186
Éléments de compréhension	188
Que font les virus ?	190
Virus spécifiques à NetWare	193
Station avec un virus système	194
Démarrer le serveur avec un virus	195
Attaque depuis le serveur	195
Protéger le serveur avec NetWare	197

PARTIE 3

QUELQUES SOLUTIONS PRÉCISES

10. LA DÉFENSE PAR LE BON SENS 202

Prévenir les pertes par des sauvegardes	203
Aider les utilisateurs à se débrouiller	205
Prévenir les vols	205
Prévenir les virus système	206
Prévenir les virus des fichiers	207

Contrôle des accès aux PC	207
Prévenir le piratage de logiciels	208
Prévenir la diffusion d'informations	208
Protéger le serveur	209
Utiliser les protections du système	210
Prévenir les attaques extérieures	210
N'aidez pas les pannes matérielles prématurées	211
Se préparer aux catastrophes	212
Apprendre à récupérer les fichiers	212
Règlements	213

11. CONTRÔLES DE SÉCURITÉ RÉSEAU 214

Contrôle des accès physiques	215
Zones à risque	215
Contrôle des accès logiques	216
Contrôle de l'organisation	217
Contrôle du personnel	219
Contrôle des opérations	220
Contrôle du développement d'applications	221
Contrôle des stations de travail	222
Contrôle des serveurs	223
Protection des transmissions de données	224
Auto-test : êtes-vous en sécurité ?	225
Contrôle des accès physiques	225
Contrôle des accès logiques	226
Contrôle de l'organisation	226
Contrôle du personnel	226
Contrôle des opérations	226
Contrôle du développement d'applications	226
Contrôle des stations de travail	227
Contrôle des transmissions	227

12. CONTRÔLE DES ACCÈS 228

Contrôle des accès 229

Problème du contrôle des accès sur un réseau 230

Définition des besoins 231

Portables 234

Architecture ouverte des contrôles d'accès 235

Modèle de transfert de données 237

Pourquoi utiliser une architecture ? 238

Définition de l'architecture ouverte 239

Fonctions et contrôles des produits ASO 240

Bénéfices de l'ASO 245

Contrôle des accès aux mainframes 246

Impératifs préliminaires 246

Formation 248

Connexion, surveillance et rapports 248

Administration des comptes 249

Conception système 251

Contrôle d'accès pour micro-ordinateur 252

Perspectives 253

Problèmes 254

Choix des produits 256

Contrôle des accès système 256

Trace de la surveillance 279

Prévention et réparation des catastrophes 286

Facilité d'utilisation 289

Contrôle des accès fichier 294

Fonctions diverses 300

Protection contre la diffusion 302

Protection contre les virus et modifications 305

Informations sur les produits 306

Commentaires sur les produits 306

Fabricants et éditeurs 307

13. IDENTIFICATION 310

Problèmes de mots de passe 311

Quelques bonnes raisons 311

Contourner les systèmes à mots de passe 313

TEMPSUP 313

NETCRACK 314

Attaquez tout avec NetUtils 315

Attaques de fichiers 316

Trouver l'information 316

Défenses contre NetUtils 317

Divination exhaustive 317

PASSTEST et NETCRACK 317

Prévention contre les attaques brutales 318

Utiliser un analyseur de réseau 321

Attaque avec dictionnaire 321

Attaques divinatoires 323

Utilisateurs sans mots de passe 323

Prévention 324

Mots de passe empruntés 324

Mots de passe partagés 325

Prévenir le partage des mots de passe 325

Algorithmes inverses 326

Attaques avec TSR 326

Prévention 327

Détection des attaques par TSR 328

Attaques pendant les réunions 328

Faux LOGIN 329

Attaques par d'anciens utilisateurs 329

Solutions générales 330

Synthétiseur de voix 330

Signatures 331

Modem de rappel 331

Clés 331

Systèmes biométriques 332

Générateurs de mots de passe 334

Gestion des mots de passe 335

Responsabilités de l'administrateur de réseau 335

Responsabilités de l'utilisateur 336

Mécanismes d'authentification 337

Protection des mots de passe 338

14. CHIFFREMENT ET SIGNATURE 340

Fonctionnement 342

Implémentation 342

Couche liaison 343

Couche transport 343

Couche application 343

Questions courantes sur le chiffrement 344

Authentification 344

Cryptographie à clé publique 344

Le pour et le contre 345

Brevets 345

Exportation 345

Data Encryption Standard (DES) 346

La loi 347

Comment ça marche 347

Quelle sécurité ? 347

Questions courantes sur RSA 348

Qu'est-ce que RSA ? 348

RSA ou DES ? 348

Et la sécurité ? 349

Implémentations matérielles 349

Augmentation de taille 349

Utilisation pratique en cryptographie 349

Utilisation pratique en authentification 349

Détection des erreurs	350
Protection contre les virus	350
Alternatives	350
RSA est-il utilisé ?	351
RSA est-il un standard officiel ?	352
RSA est-il un standard de fait ?	352
DSS	352
KERBEROS	353
Temps de calcul	353
Exemple d'utilisation	353
Authentification avec X9.9	354
Problème fondamental	354

15. TOLÉRANCE DE PANNES 356

Causes et effets	357
Quel est le problème ?	357
Utilisateurs à tolérance de pannes	361
Quelques trucs pour prévenir les pertes de données	361
Améliorer la récupération	366
8 trucs pour bien récupérer les données	366
Tolérance aux pannes matérielles	368
Contrats de maintenance	368
Pièces détachées	368
Deux, c'est mieux qu'une	369
Substitution	369
Tolérance de pannes par stockage	369
Redondance maison	369
Groupes de disques	369
Disques miroirs	372
Disques en duplex	373
Disques à mémoire permanente	373
Disques amovibles	373

Sauvegarde 374

Les sauvegardes DAT 377

Systèmes de sauvegardes proposés 378

Supports amovibles 380

Alimentation à tolérance de pannes 381

Réseaux à tolérance de pannes 384

16. SERVEURS TÉLÉMATIQUES 386

Pourquoi appeler un serveur télématique ? 387

Sécurité des appelants 388

Les mythes des serveurs 388

Ce qui vous concerne 391

Avantages d'un serveur 391

Les logiciels serveurs 392

Est-ce nécessaire ? 392

Comment évaluer la sécurité 393

Les serveurs télématiques comparés aux grands systèmes 398

Le côté obscur de la force 399

Certains des fichiers disponibles 399

Les documents qu'on y trouve 399

Quelques "bons" serveurs 402

Le serveur de Norman Data Defense Systems 403

Le serveur du Laboratoire de Sécurité Informatique (CSL) 403

17. CONNEXIONS 404

Connexions permanentes 405

Les ponts et les routeurs 407

Similitudes entre les ponts et les routeurs 408

Différences entre les ponts et les routeurs 408

Les ponts-routeurs 410

Avantages des ponts sur les routeurs 410

Avantages des routeurs sur les ponts 410

Les produits disponibles sur le marché 411

Insuffisances des routeurs en matière de sécurité	412
Les passerelles	413
Comment sécuriser une passerelle	413
Etude de cas : DIGITAL met en place un pare-feu	416
Introduction	416
Objectifs du système	417
Configuration générale du système	417
La messagerie électronique	420
Telnet et FTP	421
Les autres services	422
Les différentes approches	422
Expériences et observations	423
Une tentative d'intrusion	424
Les développements futurs	426
Conclusions	426
Disponibilité	427
Remerciements	427

PARTIE 4

RÉSEAUX LOCAUX

18. TOLÉRANCE DE PANNES 432

Introduction à la tolérance aux pannes	433
Caractéristiques à rechercher	434
Duplication de la FAT	435
Défauts des disques	436
Disques miroirs	437
Disques duplexés	438
Duplication de fichiers	438
Trace des transactions	439
Surveillance de l'alimentation	440

Reconnexion automatique 441

Récupération et destruction de fichiers 442

Autres caractéristiques 443

19. MICROSOFT LAN MANAGER 444

Microsoft contre-attaque 445

Vue d'ensemble 447

Administration 448

Administration à distance 450

Domaines 450

Surveillance du réseau 451

Amorçage à distance 452

LAN Manager et SNMP 452

NetView 452

Sécurité des serveurs 452

Protection des répertoires 454

Scripts de connexion 454

Comptes utilisateurs 454

Protection des fichiers 455

Quelques trucs pratiques 456

Windows pour Workgroups 457

Contrôle des ressources partagées 457

Stations sans disques 458

Accès à distance 458

Sécurité du serveur 458

Surveillance 459

Tolérances aux pannes 459

20. IBM LAN SERVER 462

Token Ring et les autres 463

Installation 464

Planification 465

Configurer le contrôleur de domaine	465
Pairs	466
Créer des utilisateurs	466
Comptes d'invités	468
Contrôle d'accès	468
Quelques trucs	470
Sécurité locale	471
Droits locaux	471
Programmes privilégiés	472
Traces	472
VENDOR	473
Services entre égaux	473
Câblage	474
Tolérance aux pannes	474
Alimentations ininterrompibles	475
Exploitation	475
Empêcher les connexions	475
Sauvegardes	476

21. LANTASTIC 477

Introduction à LANTastic	477
Sécurité	478
Sécurité de connexion	478
Liste de contrôle d'accès	480
Les traces	482

22. NETWARE 484

NetWare en bref	485
Les différentes versions de NetWare	485
Les possibilités de NetWare en matière de sécurité	488
NetWare n'est pas sécurisé par défaut	489
Configuration initiale : SYSCON	490
Menu "Accounting"	492

Menu "Group Information"	494
Menu "Supervisor Options"	495
Menu "User Information"	503
Les attributs et les droits d'accès	506
Les protections au niveau du fichier	507
Utiliser les attributs de fichier pour contrôler les accès	512
Virus et attributs de fichier	513
Modifier ou visualiser les attributs de fichier	513
Attributs de répertoire	514
Répertoires, fichiers et droits des abonnés	516
Comprendre les droits d'accès	519
Construire l'arborescence des fichiers	520
Créer les groupes de travail	521
Créer les gestionnaires de groupes de travail (NetWare 3.x)	522
Tester	522
Ajouter un utilisateur	522
Fonctionnement de LOGIN	523
Autres moyens de sécuriser NetWare	525
Créer un script d'ouverture de session système	525
Chiffrer les mots de passe	526
Commandes de NetWare relatives à la sécurité	527
Fonctionnalités de tolérance aux pannes de NetWare	531
Tables d'allocation de fichiers redondantes	531
Vérification de lecture après écriture et la zone "Hot Fix"	532
Défragmentation en temps réel	533
Système de suivi de transactions	533
Disques en miroir	534
Disques en duplex	535
Gestion d'une alimentation ininterrompible	535
Mise en place d'un réseau NetWare sécurisé	535
Conception du système	535
Câblage	536

Les communications distantes	537
Règlement à l'usage des utilisateurs	537
Répertoires des applications	537
Les astuces de David	538
Verrouillez le serveur	538
Sauvegardez tout	540
Remarques diverses	540
Blem Wit	540
Structure des répertoires	541
Réutilisation de l'espace disque	542
Protection de la bindery	542

23. UNIX 544

Généralités sur UNIX	545
Les problèmes de confidentialité	548
Mettre en place une configuration UNIX sécurisée	550
Sécurité des comptes	550
Sécurité des connexions extérieures	553
Sécurité des fichiers et des répertoires	559
La surveillance du système	561
Surveillance des comptes	561
Surveillance des connexions réseau	563
Surveillance de la sécurité des fichiers	564
Renforcer la sécurité avec des logiciels add-ons	566
Les logiciels du domaine public	566
Les produits commerciaux	567
Comment se maintenir à niveau	568

24. BANYAN VINES 570

VINES en bref	571
Créer des types d'utilisateurs	573
Contrôle des connexions	573
Contrôles de connexion des utilisateurs	575

Pour les groupes	579
Sécurité du serveur	579
Liste d'accès téléphonique	579
Restrictions inter-réseaux	580
Droits d'accès	581
Droits pour VINES, DOS et OS/2	581
Droits pour les Macintosh	582
Héritage des droits	582
Vérification des droits	583
Attributs	584
Génération de journaux et rapports	585
Journaux	586
Rapports StreetTalk	586
Rapports d'accès	586
Sécurité de la console	587

PARTIE 5

PASSER À L'ACTION

25. MISE EN PLACE 590

Les différents plans de sécurité	591
Les contre-mesures	591
Lutte contre l'incendie, prévention, détection, éradication et protection	592
Dégâts des eaux, prévention, détection et protection/correction	592
Alimentation électrique	593
Équipements gérant l'environnement	594
Désastres naturels	595
Entretien et maintenance	595
Avant le jour J	596
La planification des interventions	600

Les plans d'intervention	600
Les différents niveaux d'intervention	601
Les étapes constitutives d'un plan d'intervention	602
Participation de la direction	607
La formation à la sécurité informatique	607
Qu'est-ce que la formation ?	607
Avantages et inconvénients de la formation	608
Quelques conseils pour les formateurs et la direction de la formation	608
Quelques principes d'enseignement	610
Quelques principes de formation	610
Les supports de formation	613
Les stratégies de sécurité	614
Genèse d'une stratégie	614
Amélioration de la stratégie	616
Les grands thèmes d'une politique de sécurité	618

26. ADMINISTRATION RÉSEAU 627

Des intrus autorisés	627
Détection d'intrus	628
Comment détecter les intrus	629
Autres avantages	631
Logiciel maison	632
PAUDIT de NetWare	633
PAUDIT2	633
Détection des pannes du réseau	640
Solutions aux problèmes	642
Relations sociales	642
Exercices d'incendie	643
Si c'est cassé, devez-vous le réparer ?	643
Plan d'action	643

INDEX 646