



**Comment  
ça marche**.net

Jean-François PILLOU  
Jean-Philippe BAY

# Tout sur la Sécurité informatique

5<sup>e</sup> édition



**DUNOD**

DNS blockchain

Sim swap

Meltdown et Spectre

Chiffrement  
homomorphe

Phone scamming

Port knocking

ANSSI

MÉHARI

Ransomware

DNS rebinding

WPA3

Cryptomineur

ASLR

NIS/RPGD, etc.

Directeur de collection : Jean-François Pillou

Illustration de couverture : Rachid Maraiï

© Dunod, 2020  
11 rue Paul Bert, 92240 Malakoff  
[www.dunod.com](http://www.dunod.com)  
ISBN 978-2-10-081347-6

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2° et 3° a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.



|                                                                  |           |
|------------------------------------------------------------------|-----------|
| <b>Avant-propos</b>                                              | <b>1</b>  |
| <b>1. Les menaces informatiques</b>                              | <b>3</b>  |
| Introduction aux attaques informatiques                          | 3         |
| Pirates informatiques                                            | 8         |
| Méthodologie d'une attaque réseau                                | 11        |
| > Méthodologie globale                                           | 12        |
| > Collecte d'informations                                        | 13        |
| > Écoute du réseau                                               | 17        |
| > Analyse de réseau                                              | 19        |
| Intrusion                                                        | 20        |
| > Exploit                                                        | 21        |
| > Compromission                                                  | 22        |
| > Porte dérobée                                                  | 22        |
| Nettoyage des traces                                             | 22        |
| La réalité de la menace                                          | 23        |
| > Ransomware et minage : la martingale du cybercrime             | 24        |
| > Cyberguerre : les États à la manœuvre                          | 25        |
| > Obsolescence et l'Internet des objets                          | 25        |
| > L'institutionnalisation de la sécurité                         | 26        |
| > Un resserrement de la législation                              | 26        |
| > Intelligence artificielle : vers des malwares plus efficaces ? | 27        |
| <b>2. Les malwares</b>                                           | <b>29</b> |
| Virus                                                            | 29        |
| > Types de virus                                                 | 30        |
| > Éviter les virus                                               | 32        |
| Vers réseau                                                      | 33        |
| > Principe de fonctionnement                                     | 33        |
| > Parades                                                        | 34        |

|                                              |           |
|----------------------------------------------|-----------|
| Chevaux de Troie                             | 35        |
| > Symptômes d'une infection                  | 36        |
| > Principe de fonctionnement                 | 36        |
| > Parades                                    | 37        |
| Bombes logiques                              | 37        |
| <i>Spywares</i> (espioniciels)               | 38        |
| > Types de spywares                          | 39        |
| > Parades                                    | 39        |
| <i>Ransomwares</i>                           | 40        |
| > Parades                                    | 41        |
| Keyloggers                                   | 41        |
| > Parades                                    | 42        |
| Spam                                         | 42        |
| > Inconvénients                              | 43        |
| > Parades                                    | 44        |
| Rootkits                                     | 46        |
| > Principe de fonctionnement                 | 46        |
| > Détection et parade                        | 47        |
| « Faux » logiciels ( <i>rogue software</i> ) | 48        |
| > Principes                                  | 48        |
| > Parades                                    | 48        |
| Hoax (canulars)                              | 49        |
| <b>3. Les techniques d'attaque</b>           | <b>51</b> |
| Attaques de mots de passe                    | 52        |
| > Attaque par force brute                    | 52        |
| > Attaque par dictionnaire                   | 53        |
| > Attaque hybride                            | 53        |
| > L'utilisation du calcul distribué          | 54        |
| > Choix des mots de passe                    | 55        |
| Usurpation d'adresse IP                      | 57        |
| > Modification de l'en-tête TCP              | 58        |
| > Liens d'approbation                        | 58        |
| > Annihilation de la machine spooftée        | 61        |
| > Prédiction des numéros de séquence         | 61        |
| Attaques par déni de service                 | 62        |
| > Attaque par réflexion                      | 63        |
| > Attaque par amplification                  | 64        |
| > Attaque du ping de la mort                 | 66        |
| > Attaque par fragmentation                  | 66        |

|                                                      |           |
|------------------------------------------------------|-----------|
| > Attaque LAND                                       | 67        |
| > Attaque SYN                                        | 67        |
| > Attaque de la faille TLS/SSL                       | 68        |
| > Attaque par <i>downgrade</i>                       | 69        |
| > Attaque par requêtes élaborées                     | 69        |
| > Parades                                            | 70        |
| Attaques <i>man in the middle</i>                    | 70        |
| > Attaque par jeu                                    | 71        |
| > Détournement de session TCP                        | 71        |
| > Attaque du protocole ARP                           | 72        |
| > Attaque du protocole BGP                           | 73        |
| Attaques par débordement de tampon                   | 73        |
| > Principe de fonctionnement                         | 74        |
| > <i>Shellcode</i>                                   | 75        |
| > Parades                                            | 75        |
| Attaque par faille matérielle                        | 76        |
| > Le matériel réseau                                 | 76        |
| > PC et appareils connectés                          | 79        |
| > Attaques APT ( <i>Advanced Persistent Threat</i> ) | 82        |
| > Attaques biométriques                              | 83        |
| Attaque par ingénierie sociale                       | 85        |
| > Réseaux sociaux                                    | 85        |
| > Attaque par <i>watering hole</i>                   | 86        |
| > Aide de la voix sur IP (VoIP)                      | 86        |
| > Attaque par réinitialisation de mot de passe       | 87        |
| > Attaque par usurpation d'identité informatique     | 89        |
| <b>4. La cryptographie</b>                           | <b>91</b> |
| Introduction à la cryptographie                      | 91        |
| > Objectifs de la cryptographie                      | 93        |
| > Cryptanalyse                                       | 93        |
| Chiffrement basique                                  | 94        |
| > Chiffrement par substitution                       | 94        |
| > Chiffrement par transposition                      | 95        |
| Chiffrement symétrique                               | 96        |
| Chiffrement asymétrique                              | 98        |
| > Avantages et inconvénients                         | 99        |
| > Notion de clé de session                           | 99        |
| > Algorithme d'échange de clés                       | 100       |
| > Le chiffrement et le cloud                         | 101       |

|                                            |            |
|--------------------------------------------|------------|
| Signature électronique                     | 101        |
| > Fonction de hachage                      | 102        |
| > Vérification de l'intégrité d'un message | 103        |
| > Scellement des données                   | 103        |
| Certificats                                | 104        |
| > Structure d'un certificat                | 105        |
| > Niveau de signature                      | 107        |
| > Types d'usages                           | 107        |
| Quelques exemples de cryptosystèmes        | 108        |
| > Chiffre de Vigenère                      | 108        |
| > Cryptosystème Enigma                     | 109        |
| > Cryptosystème DES                        | 112        |
| > Cryptosystème RSA                        | 117        |
| > Cryptosystème PGP                        | 118        |
| <b>5. Les protocoles sécurisés</b>         | <b>123</b> |
| Protocole SSL                              | 123        |
| Protocole SSH                              | 126        |
| Protocole Secure HTTP                      | 129        |
| Protocole SET                              | 130        |
| Protocole S/MIME                           | 131        |
| Protocole DNSsec                           | 132        |
| <b>6. Les dispositifs de protection</b>    | <b>133</b> |
| Gestion des utilisateurs                   | 133        |
| > Moindre privilège et « 4 yeux »          | 134        |
| > Listes de contrôle d'accès               | 135        |
| Gestion des mots de passe                  | 135        |
| > Robustesse et capacité humaine           | 135        |
| > Stockage, hachage et salage              | 136        |
| > Découpage des nouveaux mots de passe     | 137        |
| Gestion des programmes                     | 137        |
| Antivirus                                  | 138        |
| > Principe de fonctionnement               | 138        |
| > Détection des <i>malwares</i>            | 138        |
| > Antivirus mais pas seulement             | 139        |
| Système pare-feu ( <i>firewall</i> )       | 140        |
| > Principe de fonctionnement               | 141        |

|                                                          |     |
|----------------------------------------------------------|-----|
| > Pare-feu personnel                                     | 145 |
| > Zone démilitarisée (DMZ)                               | 145 |
| > Limites des systèmes pare-feu                          | 147 |
| > <i>Honeypots</i>                                       | 147 |
| Serveurs mandataires (proxys)                            | 148 |
| > Principe de fonctionnement                             | 148 |
| > Fonctionnalités d'un serveur proxy                     | 149 |
| > Translation d'adresses (NAT)                           | 150 |
| > <i>Reverse-proxy</i>                                   | 153 |
| Systèmes de détection d'intrusions                       | 153 |
| > Techniques de détection                                | 155 |
| > Méthodes d'alertes                                     | 156 |
| > Enjeu                                                  | 157 |
| Réseaux privés virtuels                                  | 157 |
| > Fonctionnement d'un VPN                                | 158 |
| > Protocoles de tunnelisation                            | 159 |
| > Protocole PPTP                                         | 160 |
| > Protocole L2TP                                         | 160 |
| > Protocole SSTP                                         | 161 |
| > Protocole IPSec                                        | 161 |
| IPv6 et la sécurité                                      | 162 |
| > Les améliorations apportées par IPv6                   | 162 |
| > Des PC directement exposés                             | 162 |
| > Menaces sur la vie privée                              | 163 |
| > Rareté = danger                                        | 163 |
| Biométrie et carte à puce                                | 163 |
| > Les lecteurs d'empreintes digitales, d'iris ou vocales | 163 |
| > L'identification par cartes à puce                     | 164 |
| Les solutions de DLP                                     | 165 |
| Les webapps et services de sécurité en ligne             | 165 |
| > Akismet et Captcha                                     | 165 |
| > <i>Botnet vs greenlist</i>                             | 166 |
| > Les pare-feu WAF                                       | 166 |
| > Les scanners de vulnérabilités                         | 167 |
| La sécurité par la virtualisation                        | 167 |
| > Virtualisation complète                                | 168 |
| > Virtualisation applicative                             | 168 |
| La sécurité des e-mails                                  | 168 |
| Les TPM                                                  | 169 |

|                                                                          |            |
|--------------------------------------------------------------------------|------------|
| <b>7. L'authentification</b>                                             | <b>171</b> |
| Principe d'authentification                                              | 171        |
| Protocole PAP                                                            | 172        |
| Protocole CHAP                                                           | 173        |
| Protocole MS-CHAP                                                        | 174        |
| Protocole EAP                                                            | 175        |
| Protocole RADIUS                                                         | 175        |
| Protocole Kerberos                                                       | 177        |
| L'authentification distribuée : la blockchain                            | 179        |
| > Blockchain : des paquets authentifiés sans tiers de confiance          | 179        |
| > De l'utilité de la blockchain dans l'authentification : le cas des DNS | 180        |
| > La chaîne pour les certificats                                         | 180        |
| L'authentification multi-facteurs (MFA)                                  | 181        |
| > Authentification par SMS                                               | 182        |
| Analyse du contexte et analyse comportementale                           | 182        |
| <b>8. La sûreté de fonctionnement</b>                                    | <b>185</b> |
| Haute disponibilité                                                      | 186        |
| > Évaluation des risques                                                 | 186        |
| > Tolérance aux pannes                                                   | 187        |
| > Sauvegarde                                                             | 188        |
| > Équilibrage de charge                                                  | 188        |
| > <i>Clusters</i>                                                        | 189        |
| Technologie RAID                                                         | 189        |
| > Comparatif                                                             | 194        |
| > Mise en place d'une solution RAID                                      | 195        |
| Sauvegarde                                                               | 196        |
| > NAS                                                                    | 196        |
| > SAN                                                                    | 196        |
| Protection électrique                                                    | 197        |
| > Types d'onduleurs                                                      | 198        |
| > Caractéristiques techniques                                            | 199        |
| > Salle d'autosuffisance                                                 | 199        |
| <b>9. La sécurité des applications web</b>                               | <b>201</b> |
| Vulnérabilités des applications web                                      | 202        |



|                                                            |            |
|------------------------------------------------------------|------------|
| Falsification de données                                   | 203        |
| Manipulation d'URL                                         | 204        |
| > Falsification manuelle                                   | 205        |
| > Tâtonnement à l'aveugle                                  | 205        |
| > Traversal de répertoires                                 | 206        |
| > Parades                                                  | 207        |
| Attaques <i>cross-site scripting</i>                       | 208        |
| > Conséquences                                             | 209        |
| > Persistance de l'attaque                                 | 209        |
| > Parades                                                  | 211        |
| Attaques <i>cross-site request forgery</i>                 | 212        |
| > Parades                                                  | 212        |
| Attaques par injection de commandes SQL                    | 213        |
| > Procédures stockées                                      | 213        |
| > Parades                                                  | 214        |
| Attaque du mode asynchrone (Ajax)                          | 214        |
| > Parades                                                  | 215        |
| Le détournement de navigateur web                          | 215        |
| > <i>Phishing</i>                                          | 215        |
| > <i>Tabnabbing</i>                                        | 216        |
| > Détournement du navigateur par ajout de composants       | 216        |
| > Détournement du navigateur par l'exploitation de failles | 217        |
| > Détournement de DNS                                      | 218        |
| > <i>Click-jacking</i>                                     | 219        |
| > Attaque par DNS rebinding                                | 219        |
| > Parades                                                  | 220        |
| > Attaque sur les API                                      | 220        |
| > Parades                                                  | 221        |
| > Attaque par les moteurs de recherche                     | 222        |
| <b>10. La sécurité des réseaux sans fil</b>                | <b>225</b> |
| <i>War driving</i>                                         | 227        |
| Risques en matière de sécurité                             | 227        |
| > Interception de données                                  | 228        |
| > Faux point d'accès (attaque evil twin)                   | 228        |
| > Intrusion                                                | 229        |
| > Brouillage radio                                         | 229        |
| > Déni de service                                          | 229        |
| Sécurisation d'un réseau sans fil                          | 230        |
| > Configuration des points d'accès                         | 230        |

|                                           |     |
|-------------------------------------------|-----|
| > Filtrage des adresses MAC               | 231 |
| > Protocole WEP                           | 231 |
| > WPA                                     | 232 |
| > 802.1x                                  | 232 |
| > 802.11i (WPA2)                          | 234 |
| > WPA2 : la sécurité qui a fait Krack     | 235 |
| > Protocole WPA3                          | 236 |
| > Mise en place d'un réseau privé virtuel | 237 |
| > Amélioration de l'authentification      | 237 |

## **11. La sécurité des ordinateurs portables** **239**

|                                   |     |
|-----------------------------------|-----|
| La protection du matériel         | 239 |
| > Les antivols                    | 240 |
| > Les systèmes de récupération    | 240 |
| La protection des données         | 241 |
| > Les solutions de sauvegarde     | 241 |
| > Les connexions réseau           | 241 |
| > Les mots de passe du disque dur | 242 |
| > Le cryptage des données         | 242 |

## **12. La sécurité des smartphones et des tablettes** **245**

|                                     |     |
|-------------------------------------|-----|
| Les enjeux                          | 245 |
| La sécurité des différents systèmes | 246 |
| > Les stores d'applis               | 247 |
| > Droits et rootage                 | 247 |
| Les attaques                        | 248 |
| > Attaque par SMS/MMS               | 248 |
| > Attaque par code QR               | 249 |
| > Attaque NFC                       | 249 |
| > Le paiement par téléphone         | 250 |

## **13. La sécurité et le système d'information** **251**

|                                           |     |
|-------------------------------------------|-----|
| Objectifs de la sécurité                  | 251 |
| Nécessité d'une approche globale          | 252 |
| Mise en place d'une politique de sécurité | 252 |
| > Phase de définition                     | 254 |
| > Phase de mise en œuvre                  | 256 |
| > Phase de validation                     | 256 |

|                                                                          |            |
|--------------------------------------------------------------------------|------------|
| > Phase de détection d'incidents                                         | 257        |
| > Phase de réaction                                                      | 258        |
| > Les méthodes d'évaluation du risque EBIOS et MÉHARI                    | 260        |
| > EBIOS                                                                  | 260        |
| > MÉHARI                                                                 | 261        |
| <b>14. La législation</b>                                                | <b>263</b> |
| Les sanctions contre le piratage                                         | 263        |
| La sécurité des données personnelles                                     | 265        |
| > Le Règlement général sur la protection des données (RGPD)              | 265        |
| > La directive Network & Internet Security (NIS) et le Cybersecurity Act | 268        |
| > Responsabilité concernant le propriétaire d'une connexion à Internet   | 269        |
| <b>15. Structures et institutions de la sécurité informatique</b>        | <b>271</b> |
| Les institutions internationales                                         | 273        |
| > Le FIRST                                                               | 273        |
| > MITRE                                                                  | 274        |
| > L'ENISA                                                                | 274        |
| > L'EC3                                                                  | 274        |
| > Le SANS                                                                | 275        |
| Les institutions françaises                                              | 276        |
| > L'ANSSI                                                                | 276        |
| > Les CERT français                                                      | 276        |
| > Les autres structures : CLUSIF, OSSIR                                  | 277        |
| <b>16. Les bonnes adresses de la sécurité</b>                            | <b>279</b> |
| Les sites d'informations                                                 | 279        |
| Les sites sur les failles de sécurité                                    | 280        |
| Les sites sur les <i>malwares</i>                                        | 281        |
| Les sites sur le <i>phishing</i>                                         | 282        |
| Les sites sur le spam                                                    | 283        |
| <b>Index</b>                                                             | <b>284</b> |





## **Avant-propos**

---

Nul ne peut aujourd'hui ignorer les dangers liés à l'utilisation d'Internet : virus, spam et pirates informatiques sont les maîtres mots utilisés par les médias. Mais que connaissez-vous exactement de ces risques ?

De plus en plus de sociétés ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs et donnent l'accès à Internet à leurs employés. Quelles menaces les guettent ?

Avec le nomadisme et la multiplication des réseaux sans fil, les individus peuvent aujourd'hui se connecter à Internet à partir de n'importe quel endroit. Tout le monde s'accorde à dire qu'il existe un risque, mais quel est-il pour les particuliers et quelles peuvent en être les conséquences ?

Sur le plan professionnel, les employés sont amenés à « transporter » une partie du système d'information hors de l'infrastructure sécurisée de l'entreprise. Comment protéger les informations vitales de l'entreprise ?

Pour toutes ces raisons, à domicile comme au bureau, il est nécessaire de connaître les risques liés à l'utilisation d'Internet et les principales parades. Cet ouvrage se veut ainsi un concentré d'informations et de définitions sur tout ce qui touche à la sécurité informatique.

## Remerciements

Jean-François Pillou remercie Cyrille Larrieu pour l'article sur les systèmes de détection d'intrusion et Sébastien Delsiré pour l'article concernant Enigma.



---

# Les menaces informatiques

Une **menace** (*threat*) représente une action susceptible de nuire, tandis qu'une **vulnérabilité** (*vulnerability*, appelée parfois faille ou brèche) représente le niveau d'exposition face à la menace dans un contexte particulier. La **contre-mesure** (ou parade), elle, représente l'ensemble des actions mises en œuvre en prévention de la menace.

Les contre-mesures ne sont généralement pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'attention des utilisateurs, ainsi qu'un ensemble de règles clairement définies.

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon de procéder de l'« ennemi ». Le but de cet ouvrage est ainsi de donner un aperçu des menaces, des motivations éventuelles des pirates, de leur façon de procéder, afin de mieux comprendre comment il est possible de limiter les risques.

## Introduction aux attaques informatiques

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.