

---

# Contents

---

<b>List of Acronyms</b> . . . . .	xi
<b>Introduction</b> . . . . .	xiii
<b>Chapter 1. General Concepts in Security</b> . . . . .	1
1.1. Introduction . . . . .	1
1.2. Reasons for security . . . . .	2
1.2.1. Technical issues . . . . .	2
1.2.2. Social factors . . . . .	4
1.3. Security attacks . . . . .	5
1.3.1. Passive/active classification of attacks . . . . .	5
1.3.2. Direct/indirect classification of attacks . . . . .	8
1.3.3. Examples of attacks . . . . .	10
1.3.4. Some statistics . . . . .	12
1.4. Security objectives . . . . .	13
1.4.1. Establishing a culture . . . . .	13
1.4.2. Establishing technical solutions . . . . .	13
1.5. Security fields . . . . .	14
1.5.1. Energy security . . . . .	14
1.5.2. Organizational and physical security . . . . .	15
1.5.3. Software security . . . . .	16
1.6. Normalization of security . . . . .	18
1.6.1. Fundamental issues and general presentation . . . . .	18
1.6.2. ISO 7498-2 norm . . . . .	19
1.7. Security services . . . . .	24
1.7.1. Authentication . . . . .	25
1.7.2. Confidentiality . . . . .	27

1.7.3. Integrity . . . . .	27
1.7.4. Non-repudiation. . . . .	27
1.7.5. Traceability and access control. . . . .	27
1.7.6. Service availability . . . . .	27
1.8. Security mechanisms . . . . .	28
1.8.1. Encryption . . . . .	28
1.8.2. Integrity check . . . . .	29
1.8.3. Access check . . . . .	29
1.8.4. Electronic signature . . . . .	30
1.8.5. Notarization . . . . .	30
1.9. Good practices . . . . .	31
1.10. Conclusion . . . . .	31
<b>Chapter 2. Security Weaknesses . . . . .</b>	<b>33</b>
2.1. Introduction. . . . .	33
2.2. Weakness in the TCP/IP . . . . .	34
2.2.1. ARPANet, the ancestor of the Internet . . . . .	34
2.2.2. The Internet and security problems . . . . .	34
2.2.3. The Internet and the ability to analyze . . . . .	35
2.3. Weaknesses due to malware and intrusion tools . . . . .	36
2.3.1. Viruses . . . . .	37
2.3.2. Worms . . . . .	40
2.3.3. Spam . . . . .	41
2.3.4. Software bomb . . . . .	42
2.3.5. Trojan horse . . . . .	42
2.3.6. Spyware . . . . .	43
2.3.7. Keylogger . . . . .	44
2.3.8. Adware . . . . .	44
2.3.9. Other malware. . . . .	45
2.3.10. Comparison of intrusion tools. . . . .	46
2.4. Conclusion . . . . .	46
<b>Chapter 3. Authentication Techniques and Tools . . . . .</b>	<b>49</b>
3.1. Introduction. . . . .	49
3.2. Theoretical concepts of authentication . . . . .	50
3.2.1. Identification . . . . .	50
3.2.2. Authentication. . . . .	51
3.3. Different types of authentications. . . . .	51
3.3.1. Local service authentication . . . . .	51
3.3.2. Network authentication . . . . .	52

---

3.4. AAA service . . . . .	56
3.4.1. Local AAA . . . . .	57
3.4.2. Server AAA . . . . .	59
3.5. Conclusion . . . . .	63
<b>Chapter 4. Techniques and Tools for Controlling Access, ACL and Firewalls . . . . .</b>	<b>65</b>
4.1. Introduction . . . . .	65
4.2. Access control list . . . . .	66
4.2.1. ACL classification . . . . .	66
4.2.2. ACL configuration in Cisco . . . . .	68
4.2.3. ACL configuration for Huawei . . . . .	74
4.3. Firewall . . . . .	78
4.3.1. Filtering function . . . . .	79
4.3.2. Functionalities of tracing and NAT . . . . .	81
4.3.3. Firewall architecture . . . . .	82
4.3.4. How a firewall works . . . . .	84
4.3.5. Firewall classifications . . . . .	84
4.3.6. Stateful firewall . . . . .	86
4.3.7. Zone-based firewall . . . . .	87
4.3.8. Firewall examples . . . . .	90
4.4. The concept of a DMZ . . . . .	92
4.4.1. Implementation of topologies . . . . .	92
4.5. Conclusion . . . . .	95
<b>Chapter 5. Techniques and Tools for Detecting Intrusions . . . . .</b>	<b>97</b>
5.1. Introduction . . . . .	97
5.2. Antivirus . . . . .	97
5.2.1. Functions of an antivirus . . . . .	97
5.2.2. Methods for detecting a virus . . . . .	98
5.2.3. Actions taken by an antivirus . . . . .	98
5.2.4. Antivirus components . . . . .	99
5.2.5. Antivirus and firewall comparison . . . . .	99
5.3. Intrusion detection systems . . . . .	100
5.3.1. IDS purposes . . . . .	100
5.3.2. IDS components and functions . . . . .	100
5.3.3. IDS classification . . . . .	102
5.3.4. Examples of IDS/IPS . . . . .	105
5.4. Conclusion . . . . .	107

---

<b>Chapter 6. Techniques and Tools for Encryption, IPSec and VPN</b> . . . . .	109
6.1. Introduction. . . . .	109
6.2. Encryption techniques . . . . .	110
6.2.1. Basic principles of encryption . . . . .	111
6.2.2. Cryptoanalysis. . . . .	112
6.2.3. Evolution of cryptography . . . . .	113
6.2.4. The concept of certificates . . . . .	117
6.2.5. Comparison of encryption techniques . . . . .	118
6.3. IPSec. . . . .	119
6.3.1. AH . . . . .	120
6.3.2. ESP . . . . .	120
6.3.3. Different IPSec modes. . . . .	121
6.3.4. Different IPSec implementations. . . . .	122
6.3.5. Different IPSec encapsulations . . . . .	122
6.3.6. IKE protocol. . . . .	125
6.4. VPNs . . . . .	126
6.4.1. Issues and justifications . . . . .	126
6.4.2. VPN principles . . . . .	127
6.4.3. Different types of VPNs. . . . .	127
6.4.4. Different tunneling protocols . . . . .	128
6.4.5. Site-to-site IPSec VPN configuration . . . . .	129
6.5. Conclusion . . . . .	131
<b>Chapter 7. New Challenges and Trends in Security, SDN and IoT</b> . . . . .	133
7.1. Introduction. . . . .	133
7.2. SDN security . . . . .	134
7.2.1. General description of an SDN . . . . .	134
7.2.2. SDN architecture . . . . .	135
7.2.3. SDN components . . . . .	136
7.2.4. Security issues in SDNs . . . . .	138
7.2.5. Security solutions for SDNs . . . . .	139
7.3. IoT/IoE security . . . . .	141
7.3.1. Sensor networks. . . . .	141
7.3.2. Security issues in the IoT . . . . .	143
7.3.3. Blockchain: an IoT security solution . . . . .	145
7.4. Conclusion . . . . .	146

---

<b>Chapter 8. Security Management</b> . . . . .	147
8.1. Introduction. . . . .	147
8.2. Security audits . . . . .	148
8.2.1. Objectives . . . . .	148
8.2.2. Audit action diagram. . . . .	149
8.2.3. Organizational and physical audit . . . . .	150
8.2.4. Technical audit . . . . .	151
8.2.5. Intrusive test. . . . .	152
8.2.6. Audit methodologies . . . . .	152
8.3. Security policy demonstration. . . . .	155
8.3.1. Security test and evaluation. . . . .	155
8.3.2. Security policy development . . . . .	159
8.3.3. Elements of a security policy . . . . .	161
8.4. Norms, directives and procedures. . . . .	162
8.4.1. ISO 27000 norm . . . . .	163
8.4.2. ISO/FDIS 31000 norm. . . . .	163
8.4.3. ISO/IEC 38500 norm. . . . .	164
8.5. Conclusion . . . . .	164
<b>References</b> . . . . .	165
<b>Index</b> . . . . .	167