Segurança

SEGURANÇA EM REDES INFORMÁTICAS

4ª Ed. Aumentada

André Zúquete

50 anos grupo LIDEL

- O "clássico" da Segurança em português
- Novo! Capítulo sobre autenticação (de pessoas e máquinas) e formas de a realizar (ex.: Cartão de Cidadão e Passaporte Eletrónico)

FCA

Segurança em Redes Informáticas

4ª Edição Aumentada

Segurança em Redes Informáticas

4ª Edição Aumentada

André Zúquete

FCA - Editora de Informática, Lda.
www.fca.pt

Distribuição

Lidel – edições técnicas, lda

Sede
R. D. Estefânia, 183, R/C Dto. – 1049-057 LISBOA
Tel: +351 213 511 448 * Fax: +351 213 522 684
Revenda: revenda@lidel.pt
Exportação: depinternacional@lidel.pt
Venda online: livraria@lidel.pt
Marketing: marketing@lidel.pt

Livraria
Av. Praia da Vitória, 14 A – 1000-247 LISBOA
Tel: +351 213 511 448 * Fax: +351 213 173 259
livraria@lidel.pt

Edição

FCA – Editora de Informática

Av. Praia da Vitória, 14 A – 1000-247 LISBOA
Tel: +351 213 511 448
Email: fca@fca.pt

FCA – Editora de Informática, Lda.
ISBN: 978-972-722-767-9
Capa: José M. Ferrão – *Look-Ahead*
Reimpressão (revista da 4ª edição aumentada) de abril 2014
Impressão e acabamento: Cafilesa – Soluções Gráficas, Lda.
Depósito Legal N.º 358452/13
Livro segundo o Novo Acordo Ortográfico

Todos os nossos livros passam por um rigoroso controlo de qualidade, no entanto, aconselhamos a consulta periódica do nosso *site* (www.fca.pt) para fazer o *download* de eventuais correções.

Para as minhas meninas, Gi, Mafalda e Joana.

Prefácio

Atualmente muitas pessoas possuem computadores pessoais ou redes domésticas ligados de forma intermitente ou permanente à Internet. Pequenas e médias empresas investem igualmente na ligação das suas redes à Internet, tanto para fornecerem uma interação mais rica e atual com os seus clientes como para dinamizarem o seu processo criativo ou de negócio. Em ambos os casos os utentes e administradores das máquinas ou redes ligadas à Internet pouco sabem objetivamente acerca dos riscos de segurança a que estão expostos.

Este livro alerta para os problemas de segurança que podem advir na ligação de uma máquina ou rede local à Internet e explica de que forma os problemas podem ser minimizados ou evitados. Ajuda também os gestores das máquinas ou redes locais a saberem identificar os seus problemas de segurança e a perceberem bem o âmbito e alcance das políticas de proteção que podem implantar e dos mecanismos de segurança que existem para esse efeito.

O conteúdo deste livro não é um catálogo de problemas e soluções – ele fundamentalmente alerta para o tipo de vulnerabilidades que tipicamente existem e são exploradas em ataques; como podem ser detetadas as vulnerabilidades ou a sua exploração; como pode ser minimizada a exploração de vulnerabilidades existentes e como se pode tomar medidas ativas e eficazes de proteção quando se interage com ou através da Internet, que é um meio inseguro por natureza.

Finalmente, muitos dos mecanismos de segurança atualmente usados recorrem a técnicas criptográficas, que não são normalmente conhecidas pela grande maioria dos utentes da Internet. Nesta obra faz-se uma introdução alargada, mas acessível, às técnicas criptográficas mais usadas e, muito em particular, às políticas atuais de gestão de chaves assimétricas e certificados de chaves públicas, que cada vez mais são usadas, mas que muitas vezes são desconhecidas ou mal compreendidas.

Esta publicação enquadra-se numa área científica que se pode designar genericamente como Segurança em Redes. Assim, e tendo em conta os conhecimentos subjacentes a esta área específica do saber, ela destina-se fundamentalmente a duas audiências-alvo: em primeiro lugar, aos utentes ou administradores de redes locais domésticas ou de redes de PME (Pequenas e Médias Empresas). Em segundo lugar, aos alunos de cadeiras de graduação – licenciatura, mestrado ou doutoramento – ou de cursos de pós-graduação na área da Segurança de Redes.

Neste documento pressupõe-se que o leitor esteja familiarizado com a pilha de protocolos OSI (*Open Systems Interconnection*) [101] e com a sua instanciação parcial na pilha de protocolos TCP/IP. Assume-se ainda que o leitor está familiarizado com as funcionalidades básicas dos equipamentos de interligação de redes (*hubs*, *switches*, *gateways*, *routers*, etc.). Consequentemente, não é feita qualquer introdução aos mecanismos-base da comunicação de dados em redes IP, o mais usado hoje em dia e o padrão da Internet. No entanto, certos aspetos relacionados com o funcionamento da Internet e das redes locais, como é o caso da resolução de nomes DNS (*Domain Name System*) e da resolução local de mapeamentos entre endereços IP e endereços MAC (*Medium Access Control*), serão descritos de forma sumária para melhor preparar o leitor para a apresentação das questões de segurança que lhes são inerentes.

Sobre o Autor

André Ventura da Cruz Marnoto Zúquete é licenciado em Engenharia Eletrotécnica e Computadores (Ramo de Sistemas e Computadores) pelo Instituto Superior Técnico (IST). Também no IST obteve o mestrado em Engenharia Eletrotécnica e Computadores e o doutoramento em Engenharia Informática e Computadores. É atualmente professor auxiliar do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro, investigador do IEETA (Instituto de Engenharia Eletrónica e Telemática de Aveiro) e colaborador do IT (Instituto de Telecomunicações). No IEETA é ainda o Investigador Principal do Laboratório de Sistemas de Informação e Telemática.

As suas principais áreas de investigação são a Segurança em Sistemas Distribuídos, os Sistemas Operativos, a Mobilidade, as Arquiteturas de Autenticação, a Deteção de Intrusões e a Privacidade. Publicou, como autor ou coautor, diversos artigos sobre temas relacionados com a segurança informática apresentados em *workshops*, conferências e revistas, tanto de divulgação como científicas. Também sobre temas relativos à segurança em sistemas distribuídos, foi orador convidado em diversos fóruns de divulgação, participou na organização e lecionação de cursos de pós-graduação e foi membro de comités técnicos e de comités de programa de diversas conferências. Foi também membro de uma equipa de avaliação de sistemas de votação eletrónica testados em processos eleitorais nacionais.

Contactos:

E-mail: `andre.zuquete@ua.pt`

URL: `www.ieeta.pt/~avz`

`wiki.ieeta.pt/wiki/index.php/Andr%C3%A9_Z%C3%BAquete`

Índice

Prefácio vii

1 Introdução 1
1.1 Introdução . . . 1
1.1.1 Defesa contra catástrofes físicas . . . 1
1.1.2 Defesa contra faltas ou falhas previsíveis . . . 2
1.1.3 Defesa contra atividades não autorizadas . . . 4
1.2 Vulnerabilidades, ataques, riscos e defesas . . . 6
1.2.1 Complexidade do problema . . . 7
1.2.2 Atitudes realistas . . . 9
1.2.3 Defesa de perímetro *versus* defesa em profundidade . . . 10
1.3 Políticas *versus* mecanismos de segurança . . . 10
1.3.1 Definição de políticas . . . 11
1.3.2 O padrão ISO 17799 . . . 12
1.3.3 Escolha de mecanismos . . . 14
1.3.4 Segurança pela ocultação (*security by obscurity*) . . . 18
1.4 Segurança em sistemas distribuídos . . . 19
1.4.1 Riscos . . . 19
1.5 Estrutura do livro . . . 22

2 Criptografia 25
2.1 Introdução . . . 25
2.2 Criptografia e criptanálise . . . 26
2.3 Evolução da tecnologia de cifra . . . 27
2.4 Tipos de cifra . . . 29
2.4.1 Cifras monoalfabéticas . . . 31
2.4.2 Cifras polialfabéticas . . . 32
2.4.2.1 Teste de Kasiski . . . 33
2.4.2.2 Índice de coincidência . . . 34
2.5 Aproximações à criptografia . . . 35
2.5.1 Aproximações teóricas . . . 35

2.5.2 Aproximações práticas 36
2.5.2.1 Difusão e confusão 38
2.5.2.2 Boas práticas 38
2.5.3 Cifras contínuas 39
2.6 Cifras modernas 41
2.6.1 Modo de operação 41
2.6.1.1 Cifras por blocos 42
2.6.1.2 Cifras contínuas 42
2.6.2 Tipo de chave 42
2.6.2.1 Cifras simétricas 42
2.6.2.2 Cifras assimétricas 43
2.6.2.3 Cifras mistas ou híbridas 44
2.7 Exemplos de cifras modernas 45
2.7.1 Cifras simétricas por blocos 45
2.7.1.1 Caso de estudo: DES 47
2.7.2 Cifras simétricas contínuas 49
2.7.2.1 Caso de estudo: A5 50
2.7.3 Cifras assimétricas (por blocos) 52
2.7.3.1 Caso de estudo: RSA 54
2.7.3.2 Caso de estudo: ElGamal 55
2.8 Aplicação das cifras por blocos: modos de cifra 56
2.8.1 ECB e CBC 57
2.8.2 OFB e CFB de *n bits* 59
2.8.3 CTR 61
2.8.4 Comparação dos modos de cifra 61
2.8.5 Tratamento de sub-blocos 63
2.8.6 Reforço da segurança 65
2.8.6.1 Cifra múltipla 65
2.8.6.2 Branqueamento (*whitening*) 66
2.8.7 Padrão PKCS #1 67
2.8.7.1 RSAES-PKCS1-v1_5 67
2.8.7.2 RSAES-OAEP 68
2.9 Funções de síntese 69
2.10 Autenticadores de dados 73
2.10.1 Autenticadores de mensagens (MAC) 73
2.10.1.1 Caso de estudo: CBC-MAC 74
2.10.1.2 Caso de estudo: DES-MAC 75
2.10.1.3 Caso de estudo: Keyed-MD5 75
2.10.1.4 Caso de estudo: HMAC 75
2.10.2 Assinaturas digitais 76
2.10.2.1 Caso de estudo: ElGamal 77
2.10.2.2 Caso de estudo: DSS e DSA 77

2.10.3 Assinaturas às cegas 79

3 Gestão de Chaves Públicas **81**
3.1 Introdução 81
3.2 Geração, salvaguarda e uso das chaves privadas 81
3.2.1 *Smartcards* 82
3.2.2 Padrão PKCS #11 83
3.2.3 CryptoAPI (*Cryptographic Application Programming Interface*) . 83
3.3 Distribuição de chaves públicas 83
3.3.1 Distribuição manual 85
3.3.2 Distribuição embebida 85
3.3.3 Distribuição interativa 86
3.3.4 Distribuição *ad hoc* 86
3.4 Certificação digital 86
3.4.1 Estrutura dos certificados digitais 87
3.4.2 Cadeias de certificação 88
3.4.3 Gestão de certificados autocertificados 89
3.4.4 Modelos de certificação 90
3.4.4.1 Monopólio 90
3.4.4.2 Oligarquia 92
3.4.4.3 Certificação cruzada 93
3.4.4.4 Malha (*mesh*) 94
3.4.4.5 Anárquico 94
3.4.5 Infraestruturas de gestão de chaves públicas 95
3.4.5.1 CRL (*Certificate Revocation List*) 96
3.4.5.2 OCSP (*Online Certificate Status Protocol*) 98
3.5 Caso de estudo: Cartão de Cidadão 98
3.5.1 Autenticação com o *smartcard* do Cartão de Cidadão 100
3.5.2 Assinaturas digitais com o *smartcard* do Cartão de Cidadão . 101
3.5.3 Hierarquias de certificação do Cartão de Cidadão 101
3.5.4 Segurança oferecida pelo Cartão de Cidadão 102
3.5.5 *Middleware* do Cartão de Cidadão 106
3.6 Caso de estudo: PGP 107
3.6.1 Chaveiros 107
3.6.2 Geração de um par de chaves 108
3.6.3 Gestão de chaves 109
3.6.3.1 Divulgação de chaves públicas 109
3.6.3.2 Importação de chaves públicas 109
3.6.3.3 Certificação de chaves públicas 110
3.6.4 Cadeias de certificação 111
3.6.5 Cifra e decifra de conteúdos 113
3.6.6 Assinatura de conteúdos 113

3.6.7 Cifra, decifra e assinatura de conteúdos 114
3.6.8 Revogação de pares de chaves 114

4 Vulnerabilidades em Máquinas de Sistemas Distribuídos 117
4.1 Introdução 117
4.2 Detetores de vulnerabilidades 117
4.2.1 Identificação de sistemas operativos 118
4.2.1.1 Flâmulas (*banners*) 118
4.2.1.2 Impressão digital da pilha IP (*IP fingerprinting*) . . . 118
4.2.1.3 Caso de estudo: `nmap` 119
4.2.1.4 Caso de estudo: `RING` 122
4.2.2 Inventariação de serviços 123
4.2.2.1 Portos TCP 124
4.2.2.2 Portos UDP 126
4.2.2.3 Portos de transporte não fixos 127
4.2.2.4 Reconhecimento de versões de servidores 127
4.2.3 Inventariação de deficiências de administração 129
4.2.3.1 Caso de estudo: OpenVAS e Nessus 130
4.3 Cenários absurdos 132
4.3.1 *Land Attack* 132
4.3.2 *Teardrop attack* 133
4.3.3 Ataque ECHO-CHARGEN 133
4.3.4 Sobrefragmentação de datagramas IP: *Ping-of-Death* 134
4.3.5 Excesso de meias-ligações TCP: SYN *flooding attack* 134
4.4 Problemas de realização 137
4.4.1 Ataque de esmagamento da pilha (*stack smashing attack*) . . . 139
4.4.2 Ataque com sequências de formatação (*format string attack*) . . 143

5 Vulnerabilidades em Redes Locais e de Grande Escala 145
5.1 Introdução 145
5.2 Levantamento de informação arquitetural 145
5.3 Tradução de nomes 146
5.3.1 Uso de nomes DNS enganadores 148
5.3.2 Resolução errada de nomes DNS (DNS *spoofing*) 149
5.3.3 Obtenção errada de endereços MAC (MAC *spoofing*) 153
5.4 Confidencialidade 155
5.4.1 Captura de senhas 157
5.4.2 Captura de dados em ligações sem fios 159
5.4.2.1 Caso de estudo: 802.11 WLAN e WEP 159
5.5 Autenticidade 160
5.5.1 Pedidos fraudulentos sobre UDP 161
5.5.2 Iniciação fraudulenta de ligações TCP 161

5.5.3 Reencaminhamento de tráfego IP . . . 162
5.5.3.1 Datagramas ICMP *Redirect* . . . 162
5.5.3.2 Opção *Source Route* do IP . . . 163
5.5.4 Sequestro de ligações TCP (*TCP hijacking*) . . . 163
5.5.5 Problemas de autoria e integridade em correio eletrónico . . . 166
5.6 Prestação de serviços . . . 167
5.6.1 Amplificação de ataques . . . 168
5.6.2 Caso de estudo: ataques *Smurf* e *Fraggle* . . . 169
5.6.3 Caso de estudo: amplificação de tráfego com servidores . . . 171
5.6.4 Ataques ao serviço DNS . . . 173

6 *Firewalls* 175
6.1 Introdução . . . 175
6.2 Arquitetura de uma *firewall* . . . 177
6.2.1 Estrutura básica . . . 177
6.2.2 *Firewalls* pessoais . . . 178
6.2.3 Componentes . . . 179
6.2.4 DMZ (zona desmilitarizada) . . . 180
6.2.5 Barreiras múltiplas . . . 181
6.2.6 Localização de serviços públicos . . . 181
6.2.7 Tradução de endereços (NAT) . . . 182
6.2.7.1 IP *masquerading* . . . 183
6.2.7.2 *Port forwarding* . . . 183
6.2.8 Encapsulamento (*tunneling*) . . . 184
6.3 Modelo de intervenção . . . 184
6.3.1 Filtro de datagramas (*packet filter*) . . . 184
6.3.1.1 Exemplos de filtragem . . . 185
6.3.1.2 Limitações . . . 186
6.3.1.3 Aspetos operacionais . . . 188
6.3.2 Filtro de circuitos (*circuit gateway*) . . . 189
6.3.3 Filtro aplicacional (*application gateway*) . . . 192
6.3.3.1 Controlo de acesso de utentes . . . 193
6.3.3.2 Análise e alteração de conteúdos . . . 193
6.3.3.3 Registo pormenorizado . . . 194
6.3.3.4 Representação . . . 194
6.4 Serviços oferecidos . . . 195
6.4.1 Autorização . . . 195
6.4.2 Controlo de operações e conteúdos . . . 196
6.4.3 Redirecionamento . . . 196
6.4.4 Comunicação segura . . . 196
6.4.5 Proteção face a ataques DoS ou de reconhecimento de sistemas 197
6.5 Topologias elementares . . . 198

6.5.1 *Gateway* simples (*dual-homed gateway*) 199
6.5.2 Máquina escondida (*screened host*) 200
6.5.3 Sub-rede escondida (*screened subnet*) 201
6.6 Caso de estudo: `iptables` 202
6.7 Caso de estudo: sistemas MS Windows 204

7 Sistemas de Deteção de Intrusões **209**
7.1 Introdução 209
7.1.1 Intrusões e sua deteção 210
7.1.2 Perfil de uma intrusão 210
7.1.3 Perfil da defesa contra intrusões 211
7.2 Arquitetura dos IDS 212
7.3 Classificação dos IDS 214
7.3.1 Método de deteção 214
7.3.2 Fonte de eventos 216
7.3.3 Instante de deteção 217
7.3.4 Reatividade 218
7.3.5 Tipo de análise 219
7.4 Limitações dos IDS 220
7.5 Caso de estudo: `Tripwire` 221
7.6 Caso de estudo: `Snort` 222
7.7 Caso de estudo: `AntiSniff` 224

8 Redes Privadas Virtuais (VPN) **227**
8.1 Introdução 227
8.2 Definição 228
8.3 Chaves de sessão 228
8.3.1 Algoritmo de Diffie-Hellman 230
8.4 Tipos de VPN 232
8.5 Tecnologias usadas pelas VPN 233
8.6 Caso de estudo: VPN SSH 233
8.6.1 Túneis seguros 234
8.6.1.1 Túneis de saída 234
8.6.1.2 Túneis de entrada 236
8.6.2 Túneis dinâmicos 237
8.6.3 Autenticação e autorização 237
8.6.4 Especificações 238
8.6.5 Limitações 238
8.7 Caso de estudo: VPN SSL/TLS 239
8.8 Caso de estudo: VPN IPSec 241
8.8.1 Associações de segurança 241
8.8.2 Negociação e instalação das associações de segurança 241

8.8.3 Afetação das associações de segurança à comunicação 243
8.8.4 Modo transporte e modo túnel 243
8.8.5 Mecanismos AH e ESP 244
8.8.6 Utilização típica numa VPN 246
8.9 Caso de estudo: VPN PPTP 246
8.9.1 Comunicação sobre PPTP 248
8.9.2 Segurança numa interação PPTP 251
8.9.3 Considerações finais 254
8.10 Caso de estudo: VPN L2TP 255
8.10.1 Comunicação sobre L2TP 256
8.10.2 Segurança numa interação L2TP 256
8.11 Caso de estudo: `OpenVPN` 257
8.12 Casos de estudo: PPP sobre SSL ou sobre SSH 258

9 Segurança em Redes Sem Fios 802.11 (WLAN ou Wi-Fi) 259
9.1 Introdução 259
9.2 Arquitetura de uma rede 802.11 260
9.2.1 Identificadores de rede 260
9.2.2 Comunicação em redes estruturadas 261
9.2.3 Localização de redes 262
9.2.4 Associação a redes 263
9.3 Visão geral da segurança em redes estruturadas 802.11 265
9.4 WEP (*Wired Equivalent Privacy*) 266
9.4.1 Autenticação 266
9.4.2 Confidencialidade e controlo de integridade 269
9.4.3 Problemas 272
9.4.4 Algumas soluções consideradas 276
9.5 Evolução 276
9.5.1 WPA (*Wi-Fi Protected Access*) 276
9.5.2 802.11i (ou WPA2) 277
9.5.3 Alterações nas tramas 802.11 278
9.6 TKIP (*Temporal Key Integrity Protocol*) 279
9.6.1 Confidencialidade 280
9.6.2 Controlo de integridade 282
9.7 AES-CCMP 284
9.8 802.1X (*Port-based Authentication Protocol*) 287
9.8.1 Interlocutores 287
9.8.2 Portos 288
9.8.3 Etapas 289
9.8.3.1 Primeira etapa: descoberta e associação 802.11 289
9.8.3.2 Segunda etapa: autenticação EAP 289
9.8.3.3 Terceira etapa: acordo em quatro passos 291

9.8.4 Simplificação para ambientes SOHO 292
9.8.5 Chaves de chave de sessão 292
9.8.6 Protocolo de acordo em quatro passos 295
9.8.7 Protocolo de acordo de chaves de grupo 297
9.9 EAP (*Extensible Authentication Protocol*) 298
9.9.1 Requisitos 298
9.9.2 EAP-TLS 299
9.9.3 EAP-TTLS (*TLS-Tunneled EAP*) 300
9.9.4 PEAP (*Protected EAP*) 300
9.9.5 EAP-PSK 301
9.9.6 EAP-SIM e EAP-AKA 303
9.10 Ataques de negação de prestação de serviço (DoS) 304

10 Protocolos de Autenticação **307**
10.1 Introdução 307
10.2 Caracterização dos protocolos de autenticação 308
10.2.1 Elemento de prova 308
10.2.2 Ataques com dicionários 309
10.2.2.1 Medidas defensivas 310
10.2.3 Apresentação da prova 311
10.2.3.1 Desafio-resposta com funções invertíveis 311
10.2.3.2 Desafio-resposta com funções não invertíveis 313
10.2.3.3 Frescura das respostas 314
10.2.3.4 Senhas descartáveis 315
10.2.4 Autenticação mútua 316
10.2.4.1 Ataques por reflexão 317
10.2.4.2 Medidas defensivas contra ataques DoS 319
10.2.4.3 Medidas defensivas contra ataques com dicionários 320
10.2.5 Distribuição de chaves de sessão 320
10.2.6 Autenticação mediada por entidade terceira confiável 321
10.2.7 Autenticação indireta 323
10.2.8 *Single Sign-On* (SSO) 324
10.3 Autenticação de pessoas 325
10.3.1 Autenticação com senha memorizada 325
10.3.1.1 Caso de estudo: autenticação Unix 326
10.3.1.2 Caso de estudo: autenticação MS Windows 326
10.3.1.3 Avaliação 326
10.3.2 Autenticação com chave secreta partilhada 327
10.3.2.1 Caso de estudo: autenticação com marcadores RFID 327
10.3.2.2 Caso de estudo: autenticação em redes GSM 329
10.3.3 Autenticação com chave privada 331
10.3.3.1 Caso de estudo: autenticação de cliente SSH 332

10.3.3.2 Caso de estudo: autenticação de cliente SSL/TLS . . 334
10.3.4 Autenticação com senhas descartáveis 337
10.3.4.1 Caso de estudo: S/Key e OTP 338
10.3.4.2 Caso de estudo: RSA SecurID 342
10.3.4.3 Caso de estudo: HOTP 344
10.3.5 Autenticação biométrica 345
10.3.5.1 Autenticação *versus* identificação 345
10.3.5.2 Fases 346
10.3.5.3 Requisitos 347
10.3.5.4 Afinação e erros 348
10.3.5.5 Vantagens e desvantagens 349
10.3.5.6 Exploração em sistemas de identificação nacionais . 351
10.3.6 Metaprotocolos de autenticação 352
10.3.6.1 Caso de estudo: *SAML Web Browser SSO Profile* . . . 352
10.3.6.2 Caso de estudo: OpenID 356
10.3.7 *Middleware* integrador 357
10.3.7.1 Caso de estudo: PAM (*Pluggable Authentic. Modules*) 358
10.4 Autenticação de máquinas ou servidores 360
10.4.1 Distribuição da chave pública da máquina ou do servidor . . 361
10.5 Serviços de autenticação 362
10.5.1 Caso de estudo: Kerberos 362
10.5.1.1 O protocolo Needham-Schroeder 363
10.5.1.2 O KDC do Kerberos 364
10.5.1.3 *Principals*, domínios e nomes 364
10.5.1.4 As credenciais do Kerberos 365
10.5.1.5 Protocolo 367
10.5.1.6 Sincronização de relógios 367
10.5.1.7 Pré-autenticação e ataques com dicionários 369
10.5.1.8 Interligação entre domínios 369
10.5.2 Caso de estudo: RADIUS 370
10.5.2.1 Estrutura das mensagens RADIUS 372
10.5.2.2 Níveis de indireção 374
10.5.2.3 Novos mecanismos de proteção 375
10.5.2.4 Problemas de segurança do RADIUS 377

Glossário de Termos – Português Europeu / Português do Brasil **379**

Bibliografia **381**

Índice Remissivo **397**

Anexo – Perguntas de Exames: Disponível para *download* em `www.fca.pt`