

Obsah

KAPITOLA 1

ÚVOD

1.1	Kontrolní součet (Hash)	4
1.2	Symetrické šifry	7
1.3	Asymetrická šifra	8
1.4	Elektronická obálka	9
1.5	Elektronický podpis	10
1.6	Podtržení veřejného klíče	11
1.7	Certifikace veřejného klíče	13
1.8	Elektronický podpis podruhé	14
1.9	Atributový certifikát	14
1.10	Časová razítka	15
1.11	DV-certifikát	17
1.12	Architektura systému vydávání „elektronických podacích lístků“	18

KAPITOLA 2

RODINA PROTOKOLŮ TCP/IP

2.1	Protokoly fyzické vrstvy	23
2.1.1	Přerušování komunikace	23
2.1.2	Rušení komunikace	23
2.1.3	Odposlech	24
2.1.4	Modifikace přenášených dat	24
2.1.5	Šifrátoři	25
2.2	Linkové protokoly	25
2.2.1	Ethernet	26
2.2.2	FrameRelay	26
2.2.3	PPP	27
2.2.4	WLAN (IEEE 802 .11)	34
2.3	IPv4	35
2.3.1	Protokol ICMP	36
2.3.2	Bezpečnostní aspekty IP	39

2.4	IPv6	39
2.5	NAT a NAT-PT	40
2.6	IPsec	41
2.7	Virtuální privátní sítě (VPN)	42
2.7.1	Privátní adresace	42
2.7.2	Tunel	43
2.8	TCP	43
2.9	UDP	47
2.10	Zabezpečení aplikačních dat	48
2.11	Prezentace dat	48
2.12	Aplikační protokoly	48
2.12.1	DNS	49
2.12.2	Protokol HTTP	57
2.12.3	Elektronická pošta	58
2.12.4	Protokol NTP	64
2.13	Proxy, brány a aplikační tunely	69
2.13.1	Proxy	69
2.13.2	Brána	72
2.13.3	Tunel	73
2.13.4	Více mezilehlých uzlů	74
2.14	Aplikace	76
2.15	PKIX a PKI	76
2.16	IDS (Intrusion Detection System)	77
2.17	Dokumentace	78

KAPITOLA 3
MIME**79**

3.1	Hlavičky MIME	80
3.1.1	Hlavička Mime-Version	80
3.1.2	Hlavička Content-Type	80
3.1.3	Hlavička Content-Transfer-Encoding	81
3.1.4	Hlavička Content-ID	82
3.1.5	Hlavička Content-Description	82
3.1.6	Hlavička Content-Disposition	82
3.2	Standardní kódovací mechanismy	83
3.2.1	Quoted-printable	83
3.2.2	Base64	84
3.2.3	Radix-64	86
3.3	Znaky v hlavičce, které nejsou ASCII	86

16.2.4	Další pomocné programy pro práci s SSH	500
16.2.5	Soubory, které souvisejí s SSH	501
16.2.6	Šifrovací kanál pro protokol Telnet	501
16.2.7	SCP	501
16.2.8	Rozdíly mezi verzemi SSH1 a verzemi SSH2	502
16.2.9	Stažení SSH	502

KAPITOLA 17

ELEKTRONICKÉ BANKOVNICTVÍ A INTERNET 503

17.1	HomeBanking, InternetBanking apod.	503
17.2	Karty a SET (Secure Electronic Transactions)	506
17.2.1	Vydání certifikátu	509
17.2.2	Duální elektronický podpis	513
17.2.3	Platba	514
17.2.4	Autorizace platby	517
17.2.5	Vypořádání obchodníka s bankou	518
17.3	3D-SET	519

KAPITOLA 18

XML A ELEKTRONICKÝ PODPIS 521

18.1	Validace dokumentů	522
18.2	Využívání URI	523
18.3	XML Namespace	524
18.4	XML a elektronický podpis	525
18.4.1	XML Encryption	525
18.4.2	XML Signature	525
18.4.3	XML kanonizace	526
18.4.4	Struktura XML digitálního podpisu	526
18.4.5	Příklad digitálního podpisu v XML	527
18.4.6	Pravidla pro zpracování	528
18.4.7	Typy klíčů a podepisovacích algoritmů	529

KAPITOLA 19

PROTOKOL KERBEROS 531

19.1	Autentikátory	531
19.2	Key Distribution Center KDC – třetí hlava Kerbera	532
19.3	Lístky relace	534

19.4	Lístky na vydávání lístků	534
19.5	Autentizace mezi doménami	535
19.5.1	Autentizace mezi dvěma doménami	535
19.5.2	Autentizace mezi více doménami	535
19.6	Podprotokoly protokolu Kerberos	537
19.6.1	Autentizační služba AS	537
19.6.2	Služba na vydávání lístků TGS	538
19.6.3	CS Exchange	538
19.7	Celý proces	539
19.8	Struktura lístků	539
19.8.1	Doba životnosti lístku	541
19.8.2	Obnovitelné TGT	541
19.8.3	Delegování autentizace	541
19.9	Struktura KDC	542
19.10	Programky	542
19.11	Implementace Kerbera v. 5 ve Windows 2000	545
19.11.1	Doménový účet	546
19.11.2	Databáze účtů	547
19.11.3	Politika Kerbera	547
19.11.4	Služby používající protokol Kerberos	547
19.11.5	DNS a Kerberos	548
19.11.6	Autorizační data	548
19.11.7	Přihlašování pomocí čipové karty	549

KAPITOLA 20

OPENSSL	551	
20.1	Popis systému	551
20.1.1	Instalace	551
20.1.2	Použití	552
20.2	Jednoduchá testovací certifikační autorita	554
20.2.1	req	556
20.2.2	ca	558
20.3	asn1parse	560
20.4	SSL/TLS	560

KAPITOLA 21

BEZPEČNOST DAT	561
REJSTRÍK	565

1	Úvod	13	Elektronický podpis komponent
2	Rodina protokolů TCP/IP	14	Úložiště certifikátů
3	MIME	15	IPsec
4	Autentizace uživatele a autorizace dat	16	SSH
5	Filtrace, proxy, firewall a internetový FrontEnd	17	Elektronické bankovníctví a Internet
6	ASN.1, BER & DER	18	XML a elektronický podpis
7	Kryptografie	19	Protokol Kerberos
8	PKI	20	OpenSSL
9	Certifikační autorita	21	Bezpečnost dat
10	Bezpečná pošta: S/MIME, ESS a elektronický podpis	R	Rejstřík
11	Bezpečný web: SSL a TLS		
12	LDAP		



3.4	Jednoduché typy dat v hlavičce Content-Type	87
3.4.1	Text	87
3.4.2	Application	87
3.4.3	Image	88
3.4.4	Audio	88
3.4.5	Video	89
3.4.6	Model	89
3.5	Kompozitní typy v Content-Type	89
3.5.1	Multipart	90
3.5.2	Message	94

KAPITOLA 4

4	AUTENTIZACE UŽIVATELE A AUTORIZACE DAT	97
4.1	Hesla	98
4.2	Jednorázová hesla	98
4.2.1	Seznam jednorázových hesel	98
4.2.2	Rekurentní algoritmus	100
4.2.3	S/KEY	101
4.2.4	OTP (One Time Password)	102
4.2.5	Autentizace uživatele a autorizace dat za využití sdíleného tajemství	103
4.2.6	Autentizační kalkulatory	105
4.2.7	Jednorázová hesla přes GSM	107
4.3	Asymetrická kryptografie	108
4.3.1	Uložení soukromého klíče na disku	109
4.3.2	Hardwarový klíč	109
4.4	Biometrika	111
4.5	Charakteristika prostředí	111
4.6	Wrapper	112
4.6.1	tcpd	115
4.6.2	Identifikační protokol	115
4.7	Protokoly RADIUS a TACACS+	116
4.7.1	Některé atributy RADIUS protokolu	119
4.7.2	Protokol RADIUS Accounting	120
4.7.3	Zpracování RADIUS Accounting logů	121

KAPITOLA 5

**FILTRACE, PROXY, FIREWALL
A INTERNETOVÝ FRONTEND****125**

5.1	Filtrace	125
5.1.1	Filtrace na úrovni protokolu IP	127
5.1.2	Filtrace na úrovni TCP	132
5.1.3	Reflexivní filtry	136
5.1.4	Filtrace protokolů UDP, ICMP a případně dalších protokolů	139
5.1.5	Zakázané adresy	140
5.1.6	Aplikační protokoly a filtrace	140
5.1.7	Závěr	144
5.2	Proxy	145
5.2.1	Klasická proxy	147
5.2.2	Generická proxy	148
5.2.3	Transparentní proxy	150
5.2.4	Závěr	151
5.3	SOCKS	151
5.3.1	SOCKS-protokol	154
5.4	WIN SOCKS	158
5.5	Skryté sítě	160
5.5.1	Směrování	161
5.6	NAT	162
5.6.1	Jednoduchý NAT	162
5.6.2	Rozšířený NAT	164
5.6.3	Dvojitý NAT	165
5.6.4	Rozložení výkonu	165
5.6.5	ALG	166
5.7	Firewall	167
5.7.1	Jaký firewall si zvolit?	171
5.7.2	Demilitarizované zóny	172
5.7.3	Firewall on Firewall	173
5.7.4	Extranet	174
5.7.5	Přístup z Internetu do vnitřní sítě	175
5.7.6	Aplikační protokoly	176
5.8	Internet FrontEnd	179
5.9	Personální firewall	183
5.10	Závěr	184

KAPITOLA 6

ASN.1, BER & DER **187**

6.1	Typy a identifikátory	188
6.2	Kódování BER	189
6.2.1	Pole typu dat	190
6.2.2	Pole délka dat	192
6.2.3	Pole data	193
6.2.4	Příklady	193
6.2.5	Jak je v BER-kódování kódován prázdný typ?	194
6.2.6	Jak je kódován typ BOOLEAN?	194
6.2.7	Jak je to s kódováním typu INTEGER?	194
6.2.8	Výčet	195
6.2.9	Typy SEQUENCE, SEQUENCE OF, SET a SET OF	195
6.2.10	Čas	195
6.2.11	Bit string	195
6.3	Identifikace objektů	195
6.3.1	Kódování identifikace objektů v BER	198
6.4	Odvozené typy	199
6.5	CHOICE	202
6.6	ANY	203
6.7	Kódování UTF-8	203

KAPITOLA 7

KRYPTOGRAFIE **211**

7.1	Základní historické systémy	213
7.2	Symetrické šifry	214
7.3	Módy blokových šifer	215
7.4	Jednosměrné funkce – Hash	217
7.5	Kryptografické systémy s veřejným klíčem	218
7.6	Digitální podpis	220
7.7	Kryptoanalýza	221

KAPITOLA 8

PKI **223**

8.1	Certifikát	224
8.1.1	Verze certifikátu	229

8.1.2	Sériové číslo certifikátu	229
8.1.3	Algoritmus	230
8.1.4	Platnost certifikátu	230
8.1.5	Jedinečná jména	231
8.1.6	Identifikační údaje CA (vystavitel certifikátu) – Issuer	236
8.1.7	Identifikační údaje uživatele (předmět certifikátu) – subject	237
8.1.8	Veřejný klíč	238
8.1.9	Jednoznačné identifikátory	239
8.1.10	Standardní rozšíření certifikátu	240
8.1.11	Privátní rozšíření certifikátu	254
8.1.12	Rozšíření používaná Microsoftem	256
8.1.13	Příklad certifikátu	257
8.2	Kvalifikované certifikáty	260
8.2.1	Identifikační údaje CA – issuer	261
8.2.2	Identifikační údaje uživatele (předmět certifikátu)	261
8.2.3	Požadavky na standardní rozšíření certifikátu	261
8.2.4	Nově zavedená rozšíření	263
8.3	Žádost o odvolání certifikátu	264
8.4	Seznam odvolaných certifikátů – CRL	264
8.4.1	Rozšíření CRL	267
8.4.2	Rozšíření položky CRL	268
8.4.3	Příklad CRL	269
8.5	Online zjišťování platnosti certifikátu – OCSP	271
8.5.1	OCSP dotaz	271
8.5.2	OCSP odpověď	272
8.5.3	Transportní protokol	274
8.6	Žádost o certifikát tvaru PKCS#10	274
8.6.1	Formát žádosti o certifikát	275
8.6.2	Příklad žádosti	276
8.7	Žádost o certifikát tvaru CRMF	277
8.7.1	Důkaz vlastnictví soukromého klíče	277
8.7.2	Vlastní žádost o certifikát	278
8.8	Protokol CMP	280
8.8.1	Záhlaví CMP zprávy	281
8.8.2	Tělo CMP zprávy	282
8.8.3	Pole ochrana	283
8.8.4	Žádost o certifikát	284
8.8.5	Odpověď na žádosti o certifikát	285
8.8.6	Obnovení klíčů	285
8.8.7	Odvolání certifikátu	286
8.8.8	Vydání nového certifikátu kořenové CA	286
8.8.9	Potvrzení	287
8.8.10	Další zprávy	287
8.8.11	Přenos protokoly TCP/IP a rozšíření souborů	287

8.9	PKCS#7 a CMS	288
8.9.1	Typ dat	289
8.9.2	Typ zprávy „Data“	290
8.9.3	Typ zprávy „Signed Data“	290
8.9.4	Příklad podepsané zprávy	294
8.9.5	Export certifikátu	299
8.9.6	Typ zprávy „Enveloped Data“	300
8.9.7	Typ zprávy „Digest Data“	304
8.9.8	Typ zprávy „Encrypted Data“	304
8.9.9	Typ zprávy „Authenticated Data“	304
8.10	Protokol CMC	305
8.10.1	Formát CMC zpráv	306
8.10.2	Atributy	310
8.10.3	MIME a rozšíření souborů	315
8.11	Přenosové protokoly pro certifikáty a CRL	316
8.12	Time Stamp Protocol (TSP)	316
8.12.1	Žádost o časové razítko	318
8.12.2	Časové razítko	318
8.12.3	Transportní protokoly	320
8.13	Protokol DVCSP	320
8.13.1	DVC-server	322
8.13.2	Žádost o DV-certifikát	323
8.13.3	Odpověď DVC-serveru	325
8.13.4	DV-certifikát	325
8.13.5	Sekvence TargetEtcChain	326
8.13.6	Chybová hláška DVC-serveru	327
8.13.7	Příklad	327
8.14	Atributové certifikáty	327
8.14.1	Atributy	330
8.14.2	Rozšíření A-certifikátu	330

KAPITOLA 9

CERTIFIKAČNÍ AUTORITA	331	
9.1	Řetězec certifikátů	334
9.2	Křížová certifikace	335
9.3	Obnovení certifikátu CA	338
9.4	Certifikační politiky (certifikační zásady)	338
9.4.1	Testovací certifikační autority	339
9.5	Vytvoření žádosti o certifikát	340
9.5.1	Vytvoření žádosti pomocí komponenty	340
9.5.2	Žádost formátu SPK	341

9.6	PKI v prostředí Windows 2000	342
9.6.1	Hlavní součásti PKI ve Windows 2000	343
9.6.2	Služby a aplikace využívající certifikáty	345
9.6.3	Šablony certifikátů	345
9.6.4	Konzola Microsoft certifikační autority MMC	346
9.6.5	Mapování certifikátů na uživatelské účty	347
9.6.6	Hierarchie MSCA	348

KAPITOLA 10

BEZPEČNÁ POŠTA: S/MIME, ESS A ELEKTRONICKÝ PODPIS **351**

10.1	Zpráva CMS používaná v S/MIME	351
10.2	Certifikáty a CRL	354
10.3	MIME: Multipart/Signed a Multipart/Encrypted	354
10.4	S/MIME	357
10.5	Příklad elektronicky podepsané a šifrované zprávy	360
10.5.1	Příklad šifrované zprávy	368
10.6	Jaká nebezpečí číhají na adresáta	373
10.7	Rozšířené S/MIME (Enhanced Security Services for S/MIME – ESS)	374
10.7.1	Žádost o doručení	375
10.7.2	Pokyny ke zpracování (Podepsaný předmět zprávy)	376
10.7.3	Bezpečnostní návěští (Security Labels)	377
10.7.4	Bezpečné konference	377
10.7.5	Certifikát určený k ověření podpisu	379
10.8	MS Outlook XP	380
10.8.1	Odesíláme zprávu	380
10.8.2	Přijímáme zprávu	381
10.9	Elektronický podpis	384
10.9.1	Paralelní a sériový podpis	386
10.9.2	Některé zmiňované atributy podpisu	386

KAPITOLA 11

BEZPEČNÝ WEB: SSL A TLS **389**

11.1	Record Layer Protocol	394
11.2	Alert Protocol	397
11.3	Change Cipher Specification Protocol	398

11.4 Handshake Protocol (HP)	399
11.4.1 Zřízení nové relace	400
11.4.2 Obnovení relace	401
11.4.3 Zprávy ServerHello, Certificate, CertificateRequest a ServerHelloDone	407
11.4.4 Zprávy Certificate, ClientKeyExchange a CertificateVerify	411
11.4.5 ServerKeyExchange	413
11.4.6 HelloRequest	414
11.5 Jak došlo k autentizaci?	414
11.6 SGC	414
11.7 HTTPS (bezpečný web)	414
11.7.1 Protocol upgrade	415
11.8 Protokoly POP3 a IMAP4	416
11.9 Propuštění SSL/TLS firewallem	416

KAPITOLA 12

LDAP	417
12.1 Navázání a ukončení relace	421
12.2 Search Request	423
12.3 Search Response	428

KAPITOLA 13

ELEKTRONICKÝ PODPIS KOMPONENT	433
13.1 Komponenty ActiveX v prohlížeči	433
13.1.1 Inicializace objektu ActiveX	433
13.1.2 Bezpečnostní nastavení Microsoft Internet Exploreru	435
13.1.3 Utilita pro podepisování souborů SignCode.exe	437
13.2 Důvěryhodné Java Applety	437
13.2.1 Důležité vlastnosti jazyka Javy	437
13.2.2 Java platforma	438
13.2.3 Bezpečnostní model Javy	439
13.2.4 Aplikace versus Applet	439
13.2.5 Co je nutné ke správnému chodu podepsaného appletu	440
13.2.6 Příklad – jakým způsobem podepsat applet	442
13.2.7 Java plug-in 1.3	443

KAPITOLA 14

ÚLOŽIŠTĚ CERTIFIKÁTŮ	445
14.1 Architektura kryptografických komponent	445
14.2 CSP a CryptoSPI	446
14.3 CryptoAPI	449
14.4 Logická a fyzická úložiště certifikátů	453
14.5 Propojení certifikátů a klíčů	454
14.6 Typický způsob použití	456
14.7 Jak vzniká vazba mezi certifikátem a párem klíčů?	456
14.8 Protected Storage System	457
14.9 Zdroje	459

KAPITOLA 15

IPSEC	461
15.1 Protokoly AH a ESP	463
15.1.1 Protokol AH	464
15.1.2 Protokol ESP	466
15.1.3 SPI	467
15.2 Protokol ISAKMP	469
15.2.1 Paket protokolu ISAKMP	470
15.3 Protokol IKE	481
15.3.1 První fáze	482
15.3.2 Druhá fáze (<i>Quick Mode</i>)	483
15.3.3 PFS	484

KAPITOLA 16

SSH	485
16.1 Protokol SSH verze 2	486
16.1.1 Transport Layer Protocol	486
16.1.2 Authentication Protocol	491
16.1.3 Connection Protocol	493
16.1.4 SecureFTP	497
16.2 Praktická část	497
16.2.1 Autentizace	497
16.2.2 SSH server (pro platformy UNIX)	498
16.2.3 SSH klient (pro platformy UNIX)	499