
KAPITOLA 1

ÚVOD

1

KAPITOLA 2

APLIKAČNÍ PROTOKOLY

5

2.1 Telnet

19

2.1.1 Protokol Virtuální terminál (NVT)

6

2.1.2 Příkazy protokolu Telnet

8

2.1.3 Příklad komunikace klienta z Windows NT

14

2.1.4 Příklad komunikace klienta z UNIXu

17

2.2 FTP

19

2.2.1 Architektura

19

2.2.2 Aktivní režim komunikace protokolu FTP

22

2.2.3 Pasivní režim komunikace protokolu FTP

24

2.2.4 Příkazy FTP

26

2.2.5 Proxy

28

2.2.6 Návratové kódy

29

2.2.7 Abnormální ukončení příkazu

30

2.2.8 Anonymní FTP

31

2.3 HTTP

32

2.3.1 Klient/server

32

2.3.2 Proxy

36

2.3.3 Brána

39

2.3.4 Tunel

40

2.3.5 Více mezilehlých uzlů

42

2.3.6 URI

43

2.3.7 Relativní URI

45

2.3.8 HTTP dotaz

46

2.3.9 HTTP odpověď

53

2.3.10 Ostatní hlavičky

54

2.3.11 Cookie

59

2.4 Architektura elektronické pošty

62

2.4.1 DNS a elektronická pošta

67

2.5	Formát poštovní zprávy	68
2.5.1	Přehled základních hlaviček z RFC-822	69
2.6	SMTP	70
2.7	ESMTP	73
2.7.1	Potvrzení o doručení zprávy	76
2.8	POP3	81
2.9	IMAP4	83
2.9.1	Neautentizovaný stav	86
2.9.2	Autentizovaný stav	87
2.9.3	Otevřená schránka	91
2.10	Konference	96
2.11	Diskusní skupiny	97
2.11.1	Formát zprávy	99
2.11.2	Protokol NNTP	99

KAPITOLA 3

MIME	105
3.1 Hlavičky MIME	106
3.1.1 Hlavička Mime-Version	106
3.1.2 Hlavička Content-Type	106
3.1.3 Hlavička Content-Transfer-Encoding	107
3.1.4 Hlavička Content-ID	108
3.1.5 Hlavička Content-Description	108
3.1.6 Hlavička Content-Disposition	108
3.2 Standardní kódovací mechanismy	109
3.2.1 Quoted-printable	109
3.2.2 Base64	110
3.2.3 Radix-64	112
3.3 Znaky v hlavičce, které nejsou ASCII	112
3.4 Jednoduché typy dat v hlavičce Content-Type	113
3.4.1 Text	113
3.4.2 Application	113
3.4.3 Image	114
3.4.4 Audio	114
3.4.5 Video	115
3.4.6 Model	115
3.5 Kompozitní typy v Content-Type	115
3.5.1 Multipart	116
3.5.2 Message	120

KAPITOLA 4

AUTENTIZACE UŽIVATELE A AUTORIZACE DAT	123
4.1 Hesla	124
4.2 Jednorázová hesla	124
4.2.1 Seznam jednorázových hesel	124
4.2.2 Rekurentní algoritmus	126
4.2.3 S/KEY	127
4.2.4 OTP (One Time Password)	129
4.2.5 Autorizace dat	129
4.2.6 Autentizační kalkulátory	129
4.2.7 Jednorázová hesla přes GSM	131
4.3 Asymetrická kryptografie	132
4.3.1 Uložení soukromého klíče na disku	133
4.3.2 Hardwarový klíč	133
4.4 Biometrika	135
4.5 Charakteristika prostředí	135
4.6 Wrapper	136
4.6.1 tcpd	139
4.6.2 Identifikační protokol	139
4.7 Protokoly RADIUS a TACACS+	140
4.7.1 Některé atributy RADIUS protokolu	143
4.7.2 Protokol RADIUS Accounting	144
4.7.3 Zpracování RADIUS Accounting logů	145
4.8 Kerberos	148
4.8.1 Služba AS	150
4.8.2 Služby TGS a AS	151
4.8.3 Lístky	153

KAPITOLA 5

FILTRACE, PROXY, FIREWALL A INTERNETOVÝ FRONTEND	155
5.1 Filtrace	155
5.1.1 Filtrace na úrovni protokolu IP	155
5.1.2 Filtrace na úrovni TCP	160
5.1.3 Reflexivní filtry	164

5.1.4	Filtrace protokolů UDP, ICMP a případně dalších protokolů	167
5.1.5	Zakázané adresy	168
5.1.6	Aplikační protokoly a filtrace	168
5.1.7	Závěr	172
5.2	Proxy	173
5.2.1	Klasická proxy	175
5.2.2	Generická proxy	176
5.2.3	Transparentní proxy	178
5.2.4	Závěr	179
5.3	SOCKS	179
5.3.1	SOCKS-protokol	182
5.4	WIN SOCKS	186
5.5	Skryté sítě	188
5.5.1	Směrování	189
5.6	NAT	190
5.6.1	Jednoduchý NAT	190
5.6.2	Rozšířený NAT	192
5.6.3	Dvojitý NAT	193
5.6.4	Rozložení výkonu	193
5.6.5	ALG	194
5.7	Firewall	195
5.7.1	Jaký firewall si zvolit?	199
5.7.2	Demilitarizované zóny	200
5.7.3	Firewall on Firewall	201
5.7.4	Extranet	202
5.7.5	Přístup z Internetu do vnitřní sítě	203
5.7.6	Aplikační protokoly	204
5.8	Internet FrontEnd	207
5.9	Závěr	211

KAPITOLA 6

ASN.1, BER & DER	213
6.1 Typy a identifikátory	214
6.2 BER kódování	215
6.2.1 Pole typu dat	216
6.2.2 Pole délka dat	218
6.2.3 Pole data	219
6.2.4 Příklady	219
6.2.5 Jak je v BER-kódování kódován prázdný typ?	220

6.2.6	Jak je kódován typ BOOLEAN?	220
6.2.7	Jak je to s kódováním typu INTEGER?	220
6.2.8	Výčet	221
6.2.9	Typy SEQUENCE, SEQUENCE OF, SET a SET OF	221
6.2.10	UTCTime	221
6.2.11	Bit string	222
6.3	Identifikace objektů	222
6.3.1	Kódování identifikace objektů v BER	224
6.4	Odvozené typy	225
6.5	CHOICE	228
6.6	ANY	229
6.7	Kódování UTF-8	229

KAPITOLA 7

KRYPTOGRAFIE	237
7.1 Základní historické systémy	239
7.2 Symetrické šifry	240
7.3 Módy blokových šifer	241
7.4 Jednosměrné funkce – Hash	243
7.5 Kryptografické systémy s veřejným klíčem	244
7.6 Digitální podpis	246
7.7 Kryptoanalýza	247

KAPITOLA 8

PKI	249
8.1 Certifikát	250
8.1.1 Verze certifikátu	254
8.1.2 Sériové číslo certifikátu	255
8.1.3 Algoritmus	255
8.1.4 Platnost certifikátu	255
8.1.5 Jedinečná jména	256
8.1.6 Identifikační údaje CA (vystavitel certifikátu) – Issuer	260
8.1.7 Identifikační údaje uživatele (předmět certifikátu) – subject	261
8.1.8 Veřejný klíč	262
8.1.9 Jednoznačné identifikátory	263

8.1.10	Rozšíření certifikátu	263
8.1.11	Privátní rozšíření certifikátu	276
8.1.12	Příklad certifikátu	277
8.2	Kvalifikované certifikáty	279
8.2.1	Identifikační údaje CA – issuer	279
8.2.2	Identifikační údaje uživatele (předmět certifikátu)	280
8.2.3	Požadavky na standardní rozšíření certifikátu	280
8.2.4	Nově zavedená rozšíření	282
8.3	Žádost o odvolání certifikátu	283
8.4	Seznam odvolaných certifikátů – CRL	283
8.4.1	Rozšíření CRL	285
8.4.2	Rozšíření položky CRL	286
8.4.3	Příklad CRL	287
8.5	On Line zjišťování platnosti certifikátu – OCSP	288
8.5.1	OCSP dotaz	289
8.5.2	OCSP odpověď	290
8.5.3	Transportní protokol	292
8.6	Žádost o certifikát tvaru PKCS#10	292
8.6.1	Formát žádosti o certifikát	293
8.6.2	Příklad žádosti	294
8.7	Žádost o certifikát tvaru CRMF	295
8.7.1	Důkaz vlastnictví soukromého klíče	295
8.7.2	Vlastní žádost o certifikát	296
8.8	Protokol CMP	298
8.8.1	Záhlaví CMP zprávy	299
8.8.2	Tělo CMP zprávy	299
8.8.3	Pole ochrana	301
8.8.4	Žádost o certifikát	302
8.8.5	Odpověď na žádosti o certifikát	303
8.8.6	Obnovení klíčů	304
8.8.7	Odvolání certifikátu	304
8.8.8	Vydání nového certifikátu kořenové CA	305
8.8.9	Potvrzení	305
8.8.10	Další zprávy	305
8.8.11	Přenos protokoly TCP/IP a rozšíření souborů	305
8.9	PKCS#7 a CMS	306
8.9.1	Typy dat	307
8.9.2	Typ zprávy „Data“	308
8.9.3	Typ zprávy „Signed Data“	308
8.9.4	Příklad podepsané zprávy	312
8.9.5	Export certifikátu	317

8.9.6	Typ zprávy „Enveloped Data“	318
8.9.7	Typ zprávy „Digest Data“	321
8.9.8	Typ zprávy „Encrypted Data“	322
8.9.9	Typ zprávy „Authenticated Data“	322
8.10	Protokol CMC	323
8.10.1	Formát CMC zpráv	324
8.10.2	Atributy	328
8.10.3	MIME a rozšíření souborů	333
8.11	Přenosové protokoly pro certifikáty a CRL	333
8.12	Protokol DVCSP	334
8.12.1	DVCS server	336
8.12.2	Žádost o DVC certifikát	337
8.12.3	Odpověď DVCS serveru	339
8.12.4	DVC certifikát	339
8.12.5	Sekvence TargetEtcChain	340
8.12.6	Chybová hláška DVCS serveru	341
8.13	Time Stamp Protocol (TSP)	341
8.13.1	Žádost o časové razítko	342
8.13.2	Časové razítko	343
8.13.3	Transportní protokoly	344

KAPITOLA 9

CERTIFIKAČNÍ AUTORITA	347
9.1 Řetězec certifikátů	350
9.2 Křížová certifikace	352
9.3 Obnovení certifikátu CA	354
9.4 Certifikační politiky (certifikační zásady)	354
9.4.1 Testovací certifikační autority	355
9.5 Vytvoření žádosti o certifikát	356
9.5.1 Vytvoření žádosti pomocí komponenty	356
9.5.2 Žádost formátu SPK	358

KAPITOLA 10

BEZPEČNÁ POŠTA: S/MIME	359
10.1 Zpráva CMS používaná v S/MIME	359
10.2 Certifikáty a CRL	361

10.3	MIME: Multipart/Signed a Multipart/Encrypted	362
10.4	S/MIME	365
10.5	Příklad elektronicky podepsané a šifrované zprávy	368
10.5.1	Příklad šifrované zprávy	376
10.6	Jaká nebezpečí číhají na adresáta	381
10.7	Rozšířené S/MIME (Enhanced Security Services for S/MIME – ESS)	382
10.7.1	Doručenka (Receipt)	383
10.7.2	Pokyny ke zpracování	384
10.7.3	Bezpečnostní návěští (Security Labels)	385
10.7.4	Bezpečné konference	385
10.7.5	Certifikát určený k ověření podpisu	387

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	414
11.4.6 HelloRequest	414
11.5 SGC	414
11.6 HTTPS (bezpečný web)	414
11.6.1 Protocol upgrade	415
11.7 Protokoly POP3 a IMAP4	416

KAPITOLA 12

LDAP	317
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 (Quick Mode)	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
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

DNSSEC	531
19.8 DNSsec	531
19.8.1 Věta typu KEY	532
19.8.2 Věta typu SIG	534
19.8.3 Věta typu NXT	538
19.8.4 Podpis zóny	540
19.8.5 Výpis	541
19.8.6 Protokol DNS	542
19.9 TSIG	544
19.9.1 TKEY	544
19.10 Uložení certifikátů do DNS	545

KAPITOLA 20

OPENSSL	547
20.1 Popis systému	547
20.1.1 Instalace	547
20.1.2 Použití	548
20.2 Jednoduchá testovací certifikační autorita	550
20.2.1 req	552
20.2.2 ca	554
20.3 asn1parse	556
20.4 SSL/TLS	556

KAPITOLA 21

BEZPEČNOST DAT	557
-----------------------	------------

REJSTŘÍK	561
-----------------	------------