

Obsah

Předmluva	9
1. Bezpečnost počítačových sítí.....	11
1.1 Základy problematiky	11
1.2 Bezpečnostní funkce v počítačových sítích	12
1.2.1 Zabezpečení přenosu zpráv a zabezpečení spojení.....	13
1.2.2 Bezpečnostní služby v počítačových sítích.....	14
1.3 Implementace bezpečnostních služeb v jednotlivých vrstvách OSI.....	15
1.4 Kryptografické algoritmy	17
1.4.1 Kryptografické algoritmy s tajným klíčem.....	18
1.4.2 Kryptografické algoritmy s veřejným klíčem	19
1.4.3 Kryptografický kontrolní součet.....	20
1.4.4 Omezení exportu kryptografických mechanismů z USA	21
1.4.5 Depozitní kryptografie a Clipper.....	21
1.5 Elektronický podpis	23
1.5.1 Kryptografie a elektronický podpis.....	23
1.5.2 Aplikace elektronického podpisu	24
1.5.3 Bezpečnost elektronického podpisu	26
1.5.4 Podpůrné funkce.....	26
1.5.5 Aplikace elektronického podpisu ve státní správě USA.....	27
1.6 Certifikáty veřejných klíčů.....	27
1.6.1 Certifikát a certifikační strom	29
1.6.2 Certifikát: Formáty a hodnoty	29
1.6.3 Formát jména	30
1.6.4 Pořadové číslo certifikátu	30
1.6.5 Platnost certifikátu	31
1.7 Příklady bezpečnostních protokolů	31
1.7.1 Bezpečná elektronická pošta	31
1.7.2 Secure Socket Layer (SSL)	33
1.7.3 PCT.....	33
1.7.4 Bezpečné WWW.....	33
1.7.5 Bezpečný Shell.....	34
1.7.6 Adresářové služby (Directory Services).....	34
1.8 Moderní autentizační metody.....	34
1.9 Elektronický obchod	36
1.9.1 Moderní platební protokoly	38

2. Bezpečnostní brána (firewall)	41
2.1 Obecná filosofie bezpečnostní brány	41
2.2 Bezpečnostní brány - zdroje informací.....	42
2.2.1 Jiná bezpečnostní softwarová řešení	43
2.2.2 Kontrolní sady programů.....	43
2.3 Filtrace paketů.....	44
2.4 Sledované protokoly.....	45
2.5 Bezpečnostní brána IBM.....	46
2.5.1 Instalace bezpečnostní brány.....	47
2.5.2 Konfigurace bezpečnostní brány.....	47
3. Servery WWW	51
3.1 Základní otázky.....	51
3.1.1 Flirt nebo seriózní provoz.....	51
3.1.2 Komerční a nekomerční provoz	52
3.1.3 Intranet.....	53
3.1.4 Prezentační a interaktivní služba.....	53
3.1.5 Bezpečný a nechráněný provoz.....	53
3.2 Protokol SSL.....	54
3.2.1 Integrita a autentičnost zpráv.....	55
3.2.2 Ověření a certifikáty.....	56
3.2.3 Vlastnosti protokolu SSL.....	57
4. Firemní WWW servery	60
4.1 Řada serverů Netscape.....	60
4.1.1 Podpora SSL u produktů Netscape	61
4.1.2 Trendy produktů Netscape	62
4.2 Server Netscape FastTrack.....	64
4.2.1 Instalace serveru.....	64
4.2.2 Systémová konfigurace serveru.....	68
4.2.3 Přístupová oprávnění.....	70
4.2.4 Správa informačního obsahu serveru	74
4.2.5 Monitorování činnosti serveru.....	78
4.2.6 Konfigurační styly.....	81
4.2.7 Konfigurace přídatných programů.....	81
4.2.8 Násobné a virtuální servery.....	83
4.2.9 Bezpečná komunikace - konfigurace SSL	84
4.2.10 Konfigurační soubory.....	89
4.3 Microsoft Internet Information Server.....	96
4.3.1 Instalace serveru.....	96
4.3.2 Konfigurace serveru.....	97
4.3.3 Bezpečnost.....	96
4.3.4 Specifické vlastnosti serveru.....	100

4.4	Apache server.....	104
4.4.1	Instalace serveru Apache.....	105
4.4.2	Konfigurace serveru Apache.....	107
5.	Netscape Proxy Server.....	113
5.1	Instalace serveru.....	114
5.2	Konfigurace serveru.....	114
5.2.1	Číslo portu.....	115
5.2.2	Procesy proxy serveru.....	115
5.2.3	Úrovně DNS.....	115
5.2.4	Persistentní spojení.....	115
5.2.5	Oblasti URL.....	115
5.2.6	Povolení činnosti proxy, přesměrování a mapování požadavku.....	116
5.2.7	Speciální režimy.....	116
5.2.8	Reverzní proxy server.....	116
5.2.9	Přístupová práva.....	117
5.2.10	Kešování.....	117
5.2.11	Další možnosti filtrace zdrojů.....	118
5.2.12	Autokonfigurace klientů.....	119
5.2.13	Socks démon.....	119
5.2.15	Záznamy transakcí.....	120
6.	Malé WWW servery.....	121
6.1	Přehled používaných malých WWW serverů.....	121
6.2	Instalace a zpráva malých WWW serverů.....	123
6.2.1	ZBS Web/Gopher Server.....	123
6.2.2	W4 Server.....	131
6.2.3	HTTPS server pro Windows NT.....	138
6.3	Front Page 97 Microsoft WWW server.....	140
6.3.1	Instalace a konfigurace systému.....	141
6.3.2	Tvorba a správa obsahu WWW serveru.....	142
6.3.3	Jak vytvořit nový WWW strom dokumentů?.....	142
Příloha	146	
Literatura	153	
Rejstřík	155	