

Přehled

Několik slov na vysvětlenou	23
1 Objasnění nebezpečí: Úvod do internetovských sítí	25
2 Co jsou sítě & TCP/IP	57
3 Používání firewallů	97
4 Ochrana přenosů pomocí šifrování	121
5 Ověřování původu informací pomocí digitálních podpisů	151
6 Hypertext Transport Protocol (HTTP)	173
7 Secure Hypertext Transport Protocol (S-HTTP)	207
8 Secure Socket Layer (SSL) a její použití pro bezpečné přenosy v Internetu	237
9 Identifikace některých hackerských útoků a obrana proti nim	259
10 Výměna klíčů Kerbera v distribuovaných systémech	295
11 Jak se chránit při obchodování na Internetu	319
12 Použití auditních záznamů k odhalení a odehnání vetřelců	333
13 Otázky bezpečnosti kolem programovacího jazyka Java	359
14 Inokulace systému proti virům	385
15 Zabezpečení sítí Windows NT proti útokům	411
16 Bezpečnostní otázky v sítích Novell NetWare	447
17 Bezpečnost systému Unix a XWindow	487
18 Testování zranitelnosti systému	519
19 Vystavujeme se světu: Otázky bezpečnosti webovského prohlížeče	545
20 Ochrana proti nepřátelským skriptům	569
21 Celkové shrnutí: Vytvoření bezpečnostní politiky sítě	613
Rejstřík	633

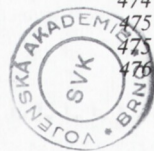
OBSAH

Několik slov na vysvětlenou	23
1 Objasnění nebezpečí: Úvod do internetovských sítí	25
1988 červu Internetu	26
☞ <i>Jak pracuje multitaskingový operační systém</i>	27
Činnost červa na Internetu	28
Důsledky působení červa	29
Růst nebezpečí	29
Pochopení Internetu	32
☞ <i>Domény</i>	34
Přepojování paketů: stavební kamen většiny sítí	36
Přenášení dat s přepojováním paketů	36
Předchůdce Internetu: ARPANet	38
Rozšíření komunikačních schopností ARPANetu: TCP/IP	39
Úvod do WWW (World Wide Web)	39
Web jako příležitost a nutnost obchodu	42
Uvědomění si nebezpečí	43
Zamyšlení nad pojmem hacker	44
Druhy hrozeb: přehled	45
Chytrý bratranec Internetu: uzavřený intranet	49
Typy hackerů a kde se dozvíte více	50
Elektronické konference a diskusní skupiny se vztahem k bezpečnosti	51
Shrnutí	53
Kde získat další informace na Internetu	54
2 Co jsou sítě & TCP/IP	57
Základní informace o sítích a TCP/IP v kostce	57
Definování komponent sady protokolů TCP/IP	58
Síťový model ISO/OSI	59
Definování sady protokolů	59
Jak se data přenášejí mezi vrstvami	60
TCP/IP implementace modelu ISO/OSI	61
☞ <i>Služby End-to-end versus hop-by-hop</i>	63
Fyzická vrstva	63
Linková vrstva	63
Síťová vrstva	64
☞ <i>Co to je zapouzdření</i>	64
Transportní vrstva	65
Služba toku bajtů versus služba datagram	65
Aplikační vrstva	66
☞ <i>Model klient-server</i>	66
Adresovací schéma TCP/IP	67
Třídy adres	68
Definování typů adres	68
☞ <i>Ještě jednou oktet</i>	69
Transmission Control Protokol – TCP	70
Zajištění spolehlivosti	70
☞ <i>Jednoduchý handshaking ACK</i>	71
Posuvné okno	71
Definování TCP zprávy	73
Navázání TCP spojení	74

Význam původu apletu	378
Vytváření důvěryhodné počítačové báze v Javě	379
Projekt Kimera	379
Použití disassembleru a verifikátoru mezikódu Kimery pro testování tříd	380
Ještě jednou o některých zákeřných apletech	381
Server Jigsaw	382
Shrnutí	383
Kde získat další informace na Internetu o bezpečnosti Javy	383
14 Inokulace systému proti virům	385
Jak funguje virus	385
<i>☞ Běžné projevy viru</i>	387
<i>☞ Stanovení rizika a počtu počítačových virů</i>	388
Nejběžnější způsoby nákazy	388
Hrozba přenosu virů prostřednictvím e-mailu	389
<i>☞ Vytvoření viru pro spustitelný soubor</i>	390
Různé typy virů	390
Trojské koně	391
Polymorfní viry	391
Neviditelné viry	392
Pomalé viry	393
Retroviry	394
Multipartitní viry	394
Pancéřové viry	395
Doprovodné viry	395
Fágy	395
Opět červi	395
Virové hrozby specifické pro síť a Internet	396
O souborových virech	396
O makrovirech	398
<i>☞ Příklad makroviru</i>	399
Některé převládající makroviry	400
Ochrana proti makrovirům	404
Falešné virové popluchy na Internetu	404
Virus Irina	404
Virus Good Times	405
AOL4FREE.COM: Poplach, který již není falešný	405
Jak rozpoznat skutečné varování před virem	405
Prevence napadení sítě virem z Internetu	406
Jak antivirový software odhalí virus	406
Výrobci antivirového softwaru	407
Shrnutí	409
Kde získat další informace na Internetu týkající se virů	409
15 Zabezpečení sítě Windows NT proti útokům	411
Úvod do Windows NT	411
Jak je to se sdílením	412
Kde jsou slabiny NTFS	412
Jak vypadá základní bezpečnostní model ve Windows NT	413
<i>☞ Přehled bezpečnostních standardů</i>	416
O tom, jak SAM ověřuje uživatele	417
<i>☞ Co jsou domény a pracovní skupiny</i>	418
<i>☞ Co jsou servisní balíčky (Service Pack)</i>	420
Něco víc o skupinách a oprávněních	420
Co jsou výchozí skupiny v doméně NT	420
Co jsou lokální výchozí skupiny NT	421
O výchozích oprávněních pro složky ve Windows NT	422

Správci a jejich ekvivalenty	423
Používání správcovských ID	423
Co je ve skupině <i>Nástroje administrace (společné)</i>	424
Zabezpečení skupiny Administrators	424
Jak Windows NT ukládá hesla	425
Co <i>Zabezpečení NT Serveru</i>	426
Jak hackeři lámou hesla	427
Použití útoku hrubou silou ve Windows NT	427
Obrana Windows NT proti slovníkovému útoku	428
Co <i>Jak dosáhnout lepších hesel</i>	428
Windows NT bez zamykání účtů	428
Správce Windows NT bez hesla	429
Účet správce Windows NT	429
Účet hosta bez hesla ve Windows NT	429
Co <i>Fyzická ochrana serveru</i>	429
NT a jeho vztah k TCP/IP a HTTP	430
Co <i>IIS 4.0 k nahrání</i>	431
Windows NT podporuje několik bezpečnostních protokolů	431
Úvod do služeb Secure Message Blocks	432
Pochopení významu aplikace Samba	433
Co <i>Chyba v aplikaci Samba</i>	433
Seznámení s některými zranitelnými místy Windows NT	434
Služby Alerter a Messenger	434
Obrana sítě před sdíleným prostředkem NetBIOS se všemi právy	434
Pochopení bezpečnosti LAN Manageru	434
Síťový monitor Windows NT	435
Služba RSH ve Windows NT	435
Služba Schedule ve Windows NT	435
Registr Windows NT	436
Systémy NT a počítačové viry	436
Co <i>NT a útok Ping of Death</i>	437
Bezpečnost FTP serveru a NT	437
Pomocný program rollback.exe	438
Co <i>Získání nástroje NetBios Auditing Tool</i>	438
Bezpečnost Remote Access Services pod Windows NT	438
Protokoly a audit v NT	441
Co <i>Nahrání nástroje pro snížení zranitelnosti ve Windows NT v důsledku uživatele "anonymous"</i>	441
Specifické útoky vůči Windows NT Serveru	442
Útok "network sniffing" (čmouchání v síti)	442
Útok typu odmítnutí služby	443
Zranitelnost Windows NT útokem TCP	443
Co <i>Zvláštní upozornění pro správce a uživatele NT na důležitou opravu chyby</i>	443
Shrnutí	444
Kde získat další informace na Internetu o Windows NT	444
16 Bezpečnostní otázky v sítích Novell NetWare	447
Úvod do Novell NetWare	448
Úvod do základů bezpečnosti v NetWare	448
Připojení uživatelů a počítačů k síti	449
Co <i>Jak vypadají uživatelé, skupiny a servery v NetWare</i>	449
Co je to udělení pověření	450
Co <i>Kdo je to administrátor, supervisor a ekvivalent supervisor</i>	451
Co je to Inherited Rights Mask	451
Co <i>Udělení práv aplikacím</i>	452
Jak dojde k náhradě udělených pověření	452

Řízení hesel	453
☞ <i>Jak NetWare šifruje heslo</i>	453
Práce s hesly pomocí syscon	454
Řízení přístupu k souborovému serveru	454
☞ <i>Přístup k domovskému adresáři</i>	455
Co je to ID supervisor a jeho ekvivalenty	455
Použití ID pro správu bezpečnosti	455
O zjišťování vetřelců	456
Odemknutí uživatelů	456
☞ <i>NetWare 4.0 ukládá hesla do pracovního souboru</i>	457
Jak chápat přihlašovací skripty	457
NetWare neposkytuje žádný audit	458
Jaké jsou zodpovědnosti při správě bezpečnosti	458
Zahájení kontroly bezpečnosti vaší instalace	459
Program security v NetWare	459
☞ <i>Freeware pro audit v NetWare verze 4</i>	460
K čemu je v NetWare program filer	460
Slabiny bezpečnosti NetWare	460
Základní obrana: zabezpečení serveru	461
Fyzické zabezpečení serveru	461
Důležité soubory zabezpečte mimo počítač	461
Ochrana přihlašovacích skriptů	462
Vytvořte seznam uživatelů a jejich přístupů	462
Sledování konzoly	463
Zapnutí účtování	463
Nepoužívejte účet supervisor	463
Použití podpisů paketů	463
☞ <i>Co jsou podpisy paketů</i>	464
Jak hackeři obcházejí podpisy paketů	465
Program rconsole používejte výjimečně	465
Kontrolujte jméno a umístění rconsole	466
Všechny konfigurační soubory NetWare přesuňte do bezpečnějšího místa	466
Přechod na NetWare 4.x	466
V NDS 4.1 odstraňte [public] z [root]	466
Přístup k účtům NetWare	466
Standardní a systémové účty NetWare	467
Ochrana jmen účtů	467
☞ <i>Techniky nízké úrovně pro obnovení systému</i>	468
Útoky proti heslům a obrana proti nim	468
Jak hackeři luští hesla Novellu	469
Použití útoků ve stylu hrubé síly v NetWare	470
Obrana NetWare proti slovníkovým útokům	470
☞ <i>Jiný důvod pro fyzické zabezpečení konzoly</i>	471
Účtování a bezpečnost účtů	471
Jak překonat účtování	471
☞ <i>Získání výpisů o účtování</i>	471
Omezení hackerů restrikcemi stanice a času	472
Ochrana konzoly	472
Jak hackeři překonávají přihlášení ke konzole	472
Jak se hackeři dostanou přes zamknutý monitor	473
Ochrana souborů a adresářů	473
Jak hacker po změně souborů ukryje svoji přítomnost	474
☞ <i>Co jsou Trojané v NetWare</i>	474
Co je NFS v NetWare a jeho bezpečnost	475
☞ <i>Použití příkazového řádku pro zjištění vašich práv</i>	475
Ochrana požadavků na místo na disku	476



Jak chápat některé bezpečnostní úvahy u velkých instalací	477
☞ <i>Proč programy v NetWare nemají tolik trhlín jako programy Unixu</i>	478
NetWare a Windows 95	478
Základní problémy s provozem Windows 95 nad NetWare	478
Pokračující problémy Windows 95 a NetWare	479
Interakce mezi hesly Windows 95 a NetWare	479
Přihlášení k Windows obchází bezpečnost NetWare	480
Novell IntranetWare pro NetWare	480
Použití IntranetWare pro řízení přístupu podle denního času	481
Použití IntranetWare pro řízení přístupu podle aplikací	481
Řízení přístupu podle zdroje a cíle IP adres	481
Nástroje IntranetWare pro výpisy přístupů a audit	482
Bezpečnost IntranetWare	482
Jak hackeři mohou ohrozit IntranetWare	482
Chyby v IntranetWare FTP NLM	483
Ochrana serverů IntranetWare před ohrožením z Internetu	483
Ochrana souboru s hesly	484
Shrnutí	484
Kde získat další informace na Internetu o Novell NetWare	485
17 Bezpečnost systému Unix a XWindow	487
Úvod do Unixu	487
Co jsou účty Unixu	488
☞ <i>Jaký je formát jména uživatele</i>	489
O heslech v Unixu	489
☞ <i>Speciální znaky v Unixu</i>	490
Jak pracuje unixovský shell	490
Struktura souborů a adresářů v Unixu	491
Úvod do základů množiny příkazů Unixu	493
Co jsou divoké karty	493
Přesměrování vstupů a výstupů	493
Volby na příkazovém řádku	494
Znak pro rouru	494
Spuštění na pozadí	495
K čemu je příkaz <i>ping</i>	495
Úvod do příkazu <i>finger</i>	496
Berkeley příkazy <i>r-</i> (<i>remote</i>)	497
Úvod do příkazu <i>rlogin</i>	498
Úvod do příkazu <i>rcp</i>	499
Úvod do příkazu <i>rsh</i>	499
☞ <i>Vypnutí příkazů r-</i>	499
Seznámení s příkazem <i>su</i> pro přepnutí uživatele	500
☞ <i>Použít či nepoužít příkaz <i>su</i>?</i>	500
Seznámení s démony	500
Seznámení s démonem <i>init</i>	501
Seznámení s démonem <i>lpd</i>	501
Seznámení s démonem <i>sendmail</i>	501
Shrnutí přehledu o Unixu	502
Jak Unix ukládá hesla	502
Jak hackeři louskají hesla	503
☞ <i>Pro větší bezpečnost soubor s hesly stínujte</i>	503
Použití útoku hrubou silou v Unixu	504
Obrana proti slovníkovým útokům	504
☞ <i>Vynucení lepších hesel</i>	505
Ochrana souborů a adresářů v Unixu	505
Příkaz <i>chmod</i>	506

Speciální soubory v Unixu	508
Známá zranitelná místa v Unixu	509
☞ <i>Sedm hlavních cílů hackerů</i>	509
Uvahy o odstranění <i>/etc/hosts.equiv</i>	509
Ochrana proti více kopiím <i>\$HOME/.rhosts</i>	510
O slabině <i>sendmail</i> debug	511
O slabině <i>sendmail</i> při vracení chybné pošty	511
Problém s <i>fingerd</i>	511
Šifrování souborů v Unixu	511
Bezpečné programovací metody pro Unix	512
Filtrování v Unixu	512
Co to je XWindow	513
Jak XWindow pracuje	513
Jak hackeri najdou otevřené X displeje	514
Problém lokálního hostitele v XWindow	515
Techniky špehování v XWindow – snímání oken	515
Techniky špehování v XWindow	516
Co je to volba <i>xterm</i> secure keyboard	516
Shrnutí	516
Kde získat další informace na Internetu o bezpečnosti Unixu	517
18 Testování zranitelnosti systému	519
Seznámení se Satanem	519
☞ <i>Jak se instaluje Satan</i>	520
☞ <i>Použití Satana pod systémem Linux</i>	521
Přehled struktury Satana	522
Jak funguje Magic Cookie Generator	523
Jak funguje rozhodovací mechanismus (policy engine)	523
Bližší seznámení s úrovněmi vzdálenosti	524
☞ <i>Proč se musíte se Satanem vyhybat jiným sítím</i>	524
Jak funguje výběr cílů	524
☞ <i>Jak funguje testování podsítě</i>	525
Jak funguje modul sběru dat	525
Jak fungují testovací úrovně	525
Jak funguje dedukční mechanismus	526
Výsledné sestavy a analýza	527
Paralelní procesy v Satanovi	527
První spuštění Satana	528
Analýza Satanových výsledků	528
Ještě o prohlížení a vyhodnocování výsledků	529
Ještě o zranitelných místech	530
Tisk sestav	530
Ještě o informacích o počítačích	530
Omezení Satanovy analýzy zranitelnosti	531
Analýza sítí NetWare a Windows NT	532
☞ <i>Testovací kopie KSA</i>	532
☞ <i>KSA pro Windows NT</i>	533
Spuštění KSA	533
Nastavení bezpečnostního standardu	534
Nastavení voleb pro přístup k účtům	534
Nastavení voleb pro sílu hesel	535
Nastavení voleb pro řízení přístupu	536
Nastavení voleb pro monitorování systému	536
Nastavení voleb pro datovou integritu	536
Nastavení voleb pro důvěrnost dat	536

Spuštění analýzy	537
Analýza výsledkové karty	538
Prohlídka seznamu rizik	538
Různé volby	539
Výpis výsledků KSA	540
Shrnutí	540
Kde získat další informace na Internetu o správě bezpečnosti sítí	541
19 Vystavujeme se světu: Otázky bezpečnosti webovského prohlížeče	545
Prohlížeč – obousměrné okno do Webu	545
Dva hlavní prohlížeče	546
☞ Účel popisu chyb	547
Význam čísel verzí	547
☞ Získání posledních záplat	547
Bezpečnostní trhliny v Microsoft Internet Exploreru	548
Internet Explorer 3.02	548
☞ Co jsou to soubory LNK	548
Internet Explorer 3.01 – Chyba zjištěná na WPI	549
Chyba zjištěná na MIT	551
☞ Microsoft – opravy chyb	552
Bezpečnostní problém s přeměrováním Javy v Internet Exploreru	553
☞ Základní problém	553
Bezpečnostní problémy s ActiveX	554
☞ Proč se komponenty ActiveX ukládají na váš disk	554
Specifické rysy bezpečnosti ActiveX	555
☞ Komponenty ActiveX v Navigátoru	557
Komponenta Chaos Computer	558
Komponenta Exploder	558
Bezpečnostní trhliny v Internet Exploreru 4.0	559
Bezpečnostní trhliny v Netscape Navigatoru	559
Berkeleyská chyba	559
☞ Microsoft a Netscape potvrzují chybu v bezpečných transakcích	560
Jak funguje cookie	560
Použití obsahu souboru cookies.txt	561
☞ Anonymizer	561
Obsah souboru cookies.txt	562
Editování cookie	562
☞ Ochrana před individuálními cookies	562
☞ Odříznutí cookies	563
Ochrana e-mailové adresy	563
☞ Jak ošidit dotěrný server	566
Shrnutí	567
Kde získat další informace na Internetu o bezpečnosti prohlížečů	567
20 Ochrana proti nepřátelským skriptům	569
Jak funguje CGI	570
☞ CGI skripty	571
Proč webovské stránky používají CGI	571
Kam se CGI skript zařadí	573
Program serveru musí vyvolat CGI skript	574
Podívejme se na CGI	574
Vztah mezi serverem a CGI skripty	575
☞ Jak uděláte z vašeho počítače webovský server	575
Jak získáte vlastní IP adresu	576
Jak kontaktujete svůj server	576
☞ Co je to pevná IP adresa	577

Základní rozhraní mezi webovským serverem a CGI skripty	577
Jak fungují proměnné prostředí CGI	578
K čemu je proměnná AUTH_TYPE	578
K čemu je proměnná CONTENT_LENGTH	578
K čemu je proměnná CONTENT_TYPE	578
K čemu je proměnná GATEWAY_INTERFACE	578
K čemu je proměnná PATH_INFO	579
K čemu je proměnná PATH_TRANSLATED	579
K čemu je proměnná QUERY_STRING	579
K čemu je proměnná REMOTE_ADDR	580
K čemu je proměnná REMOTE_HOST	580
K čemu je proměnná REMOTE_IDENT	580
K čemu je proměnná REMOTE_USER	580
K čemu je proměnná REQUEST_METHOD	580
K čemu je proměnná SCRIPT_NAME	581
K čemu je proměnná SERVER_NAME	581
K čemu je proměnná SERVER_SOFTWARE	581
K čemu je proměnná HTTP_ACCEPT	581
Jak fungují volby v příkazovém řádku CGI	581
Jak funguje přímý výstup z CGI na prohlížeč	582
Jak fungují CGI hlavičky	582
Prohlédněte si svůj první CGI skript s použitím C++	583
Jazyky vhodné pro programování skriptů	585
<i>Skripty nejsou jediným řešením</i>	585
Perl je programovací jazyk	586
Historie Perlu	586
Perl je interpretovaný programovací jazyk	586
Srovnání Perlu s programovacími jazyky C/C++	586
Perl nabízí mnoho možností	587
Perl jako datový filtr	587
Perl jako bezpečnostní brána	588
Perl jako frontend k databázi	588
Perl jako jazyk pro CGI skripty	589
Začínáme s Perlem	589
"Hello world" v Perlu	589
Jak se Perl vyvolá	590
Jak fungují příkazy Perlu	590
Jednoduché a složené příkazy	591
<i>Jak psát skripty, aby byly čitelnější a srozumitelnější</i>	591
<i>Volání externích programů z perlovského skriptu</i>	592
Bezpečnost CGI skriptů	592
<i>Bezpečnostní trhliny odhalené v poslední době</i>	592
Jak ovlivní prolomení skriptu bezpečnost	593
Úrovně přístupu na webovský server	593
Příklady bezpečnostních trhlin v CGI skriptech	593
Rozdvojení shellu	594
Nejlepší způsoby zabezpečení CGI skriptů	595
<i>Varování CERT ohledně zranitelnosti CGI</i>	596
Důsledek zranitelnosti CGI skriptu	597
Řešení problému se zranitelností CGI skriptu	597
Globální pravidla pro skripty v Perlu	597
Základní bezpečnostní problémy JavaScriptu	598
Kam se dává JavaScript	599
Potlačení výpisu příkazů JavaScriptu pomocí HTML komentářů	600
Komentáře v JavaScriptu	601

Prvek <SCRIPT>	601
Jak fungují textové řetězce v JavaScriptu	602
Jednoduchý výstup pomocí JavaScriptu	602
Vytvoření jednoduchého okénka se zprávou	602
Proměnné v JavaScriptu	604
Získání textového vstupu od uživatele	604
Jak fungují v JavaScriptu funkce	605
Jak fungují objekty v JavaScriptu	605
Vytváření vlastních objektů v JavaScriptu	606
Jak fungují události v JavaScriptu	607
Použití JavaScriptu pro interakci s formuláři	607
<i>Co je to LiveWire</i>	608
Bezpečnostní rizika skrytá v JavaScriptu	608
Další bezpečnostní problémy v novějších verzích Navigátoru	609
Oprava Bell Labs pro problém s ochranou soukromí v JavaScriptu je k dispozici	609
Vysvětlení problému odhaleného v Bell Labs	609
Shrnutí	610
Kde získat další informace na Internetu o skriptech	611
21 Celkové shrnutí: Vytvoření bezpečnostní politiky sítě	613
Co je to bezpečnostní politika	613
Rozhodnete se, proč potřebujete bezpečnostní politiku	614
Základní přístup k vytvoření bezpečnostní politiky	614
Vytvoření oficiální politiky počítačové bezpečnosti	616
Stanovte zodpovědnost za vytvoření politiky	616
Zodpovědnost za realizaci	617
Hodnocení rizik	617
Identifikace aktiv ve vašem systému	618
Identifikace hrozeb	618
Konkretizace politiky	619
Kdo smí používat jednotlivé zdroje	620
Jak se má každý zdroj správně používat	620
Kdo je oprávněn povolovat přístup a schvalovat využívání	621
Kdo bude mít pravomoci správce systému	622
Oprávnění a zodpovědnost uživatelů	623
Oprávnění a zodpovědnost správce systému a ostatních uživatelů	624
Zabezpečení a ochrana citlivých a normálních informací	624
Reakce na případy narušení politiky	624
Určení reakce na porušení politiky	625
Vaše reakce v případě, že lokální uživatel poruší politiku na vzdáleném počítači	625
Kontakty s cizími organizacemi a odpovědnost vůči nim	625
Problematika procedur pro vyřizování incidentů	626
Uzavřít se před vetřelci, nebo na ně číhat?	626
Výklad politiky	627
Zveřejnění politiky	628
Vytvoření procedur pro prevenci bezpečnostních problémů	628
Rozpoznání možných problémů	628
Výběr kontrolních mechanismů pro ochranu aktiv s přiměřenými náklady	629
<i>Místní bezpečnostní příručka</i>	630
Shrnutí	630
Internetovské zdroje vztahující se k bezpečnostním politikám	631
Rejstřík	633

Počáteční pořadové číslo	75
Potvrzování přenosu dat	75
Oficiální navázání spojení	76
Pořadová čísla	76
Používání plně duplexních služeb (Full-Duplex services)	77
Ukončení TCP spojení	78
TCP hlavička	78
Zdrojový a cílový port	78
Pořadové číslo	78
Potvrzovací číslo	79
Délka hlavičky	79
Příznaky (Flags)	79
Velikost okna	80
TCP kontrolní součet	80
Urgent pointer	80
Volby	81
Od návrhu k realizaci	82
Topologie sítí	82
Topologie hvězdy	82
Topologie kruhu	83
Topologie sběrnice	84
Zpracování kolizí na sběrnici	84
<i>~ Něco více o zpracování kolizí</i>	85
Předávání tokenů	85
Různě vymezené síťové technologie	85
Definice Ethernetu	86
Definice ARCNETU	86
Definice IBM Token Ring	86
Definice sítí typu Asynchronous Transfer Mode	87
Spojování počítačových sítí	88
Útlum a opakováče	88
Správa chyb a kontrolní součty	89
Používání můstků k lepšímu využití sítě	90
Použití směrovače	90
Použití přenosových bran	91
Fyzická struktura sítí	92
Různé typy broadcast kanálů	92
Shrnutí	93
Kde získat další informace na Internetu k ISO/OSI modelu a TCP/IP	94
3 Používání firewallů	97
Různé formy zabezpečení	97
<i>~ Strážné počítače (Bastion Hosts)</i>	98
Ochrana vaší sítě proti vnějším narušitelům	98
Ochranné směrovače	99
Ochrana proti nedovolenému přístupu mezi odděleními	100
Architektura firewallů	100
Firewall	102
<i>~ Izolování vaší sítě</i>	102
Rizikové oblasti	103
Omezení firewallů	104
Návrh firewallu	105
Tři typy firewallu	105
Firewall síťové úrovně	106
Firewall aplikační úrovně	107
Firewall okružové úrovně	109
Architektury firewallu	110

Firewall se dvěma domovskými podsítěmi	110
Firewall s odstíněným hostitelským počítačem	112
Firewall s odstíněnou podsítí	112
Skupiny bezpečnosti	113
Rozdělení skupiny bezpečnosti třídy D	113
Rozdělení skupiny bezpečnosti třídy C	113
Třída C1	113
Třída C2	114
Rozdělení skupiny bezpečnosti třídy B	114
Třída B1	114
Třída B2	115
Třída B3	115
Rozdělení skupiny bezpečnosti třídy A	116
Třída A1	116
<i>≈ Něco více o skupinách v Oranžové knize</i>	117
Shrnutí	119
Kde získat další informace na Internetu k firewallům	119
4 Ochrana přenosů pomocí šifrování	121
Proč je šifrování tak zajímavé	122
Základy šifrování	122
Omezení konvenčních kryptosystémů s tajným klíčem	123
<i>≈ Používání PGP for Windows k šifrování dokumentů</i>	123
Kryptosystémy s veřejným klíčem	126
<i>≈ Umístění privátních a veřejných klíčů</i>	127
Algoritmus RSA (Rivest, Shamir, Adleman)	127
Vlastní algoritmus RSA	128
<i>≈ Matematické pozadí algoritmu RSA</i>	129
<i>≈ Nahrání RSA Software</i>	130
Diffie a Hellman	131
Šifrovací algoritmus Diffie-Hellman	131
<i>≈ RSA versus Diffie-Hellman</i>	132
Autentizace zpráv jako část protokolu s veřejným klíčem	132
Odolnost kryptografických technik	133
Jak efektivně zacházet se šifrováním s veřejným klíčem	133
Certifikáty klíčů a klíčenky	134
Message Digest	136
<i>≈ Nahrání unixovských verzí kryptografických kontrolních součtů.</i>	136
Privacy Enhanced Mail (PEM)	137
Autentizace odesílatele pomocí PEM	137
Utajení v PEM	138
Integrita dat v PEM	138
<i>≈ Nahrání některých standardních PEM programů</i>	138
Přehled hlavních kryptografických programů	138
Pretty Good Privacy (PGP)	139
PGP používá více kryptografických metod	139
Stavba veřejného klíče	140
Rozšířenost PGP	141
<i>≈ Vyhledávání klíčů ve veřejné klíčence</i>	141
<i>≈ Download freeware PGP</i>	141
Šifrování a Enigma	142
UUEncode a SMTP	142
Microsoft CryptoAPI	142
<i>≈ Používání CryptoAPI</i>	144
Časový útok (timing attack)	146

Nová vlna v šifrování: Elliptic-Curve Cryptography (ECC)	146
Bezpečnost eliptických křivek	147
Matematický pohled na ECC	148
Je ECC lepší než současné kryptosystémy ?!	148
Shrnutí	148
Kde získat další informace na Internetu týkající se šifrování a přenosu dokumentů	149
5 Ověřování původu informací pomocí digitálních podpisů	151
Konstrukce digitálního podpisu	151
Důležitost digitálních podpisů	153
<i>☞ Použití PGP for Windows pro digitální podepisování dokumentu</i>	154
Digitální podpisy versus elektronické podpisy	156
Použití digitálních podpisů	157
Americký Digital Signature Standard	158
Znepokojení okolo DSS	158
Postavení NSA	159
<i>☞ Neúspěch s čipem Clipper</i>	159
Zapojení NSA do vývoje bezpečnostních standardů	160
Vývoj DSS	161
Digitální podpisy a Privacy Enhanced Mail (PEM)	162
<i>☞ Nahrání perlovského interface pro SHA</i>	162
<i>☞ Seznam NIST uvádějící software splňující podmínky pro DSS/SHS</i>	162
Ještě jednou algoritmus Diffie-Hellman	163
<i>☞ Nahrání demoverze HASHCipher pro SHA</i>	163
Budoucnost digitálních podpisů	164
<i>☞ Digitální podepisování souborů na UNIXu pomocí PGP</i>	165
Digitální podpisy a podepisování souborů	166
Certifikační autority	168
<i>☞ Podepisování softwaru</i>	169
Shrnutí	170
Kde získat další informace na Internetu o digitálních podpisech	170
6 Hypertext Transport Protocol (HTTP)	173
HTTP je nativní protokol webu	173
MIME	174
<i>☞ Postavení webu a internetovské standardy</i>	174
Používání MIME na webu	175
Typy a podtypy MIME	176
Bližší pohled na typy MIME	177
Více o HTTP	179
Bližší pohled na efektivitu bezstavové komunikace	179
HTTP podporuje dynamické formáty	180
Informace v hlavičce HTTP	180
HTTP je "human-readable"	180
HTTP je obecný protokol	181
Jak HTTP vyhledává, nahrává a oznamuje výsledek	182
Vyhledávání zdroje	182
Nahrání objektu	182
Oznámení výsledku	182
Čtyři kroky transakce HTTP	183
Krok 1: Ustanovení spojení	183
Krok 2: Klient zašle požadavek	183
Krok 3: Klient zašle odpověď	184
Krok 4: Server ukončuje spojení	185
Stavové kódy HTTP	185
Bližší pohled na URI	187

Ještě jednou o URL	187
Souvislosti URL, protokolů a typů souborů	188
Části URL	188
Pohled na URL a HTML	189
Absolutní a relativní URL	190
Absolutní URL	190
Relativní URL	190
Další informace o relativních URL	190
Definice metod HTTP	191
Metoda GET	192
Metoda HEAD	192
Metoda POST	193
Ostatní metody HTTP	193
Pole General-Header	194
Pole HTTP Date	195
Pole MIME-version	195
Pole Pragma	195
Pole Request Header	196
Definování pole Accept	196
Definování pole Authorization	196
Definování pole From	197
Definování pole If-Modified-Since	197
Definování pole Referer	197
Definování pole User-Agent	198
Definování polí Entity-Header	198
Pole Allow	198
Pole Content-Encoding	199
Pole Content-Length	199
Pole Content-Type	199
Pole Expires	200
Pole Extension-Header	200
Pole Last-Modified	200
Responses – odpovědi	201
Pole v záhlaví Response-Header	201
Pole Location	201
Jak funguje pole Server	202
Co je to pole WWW-Authenticate	202
Definování těla entity	202
Datová komunikace na Webu	203
Příklad transakce HTTP	203
Shrnutí	204
Kde získat další informace na Internetu o HTTP	204
7 Secure Hypertext Transport Protocol (S-HTTP)	207
Úvod do S-HTTP	207
Jak S-HTTP vytváří zprávy	208
Dešifrování zprávy S-HTTP	209
Šifrovací metoda S-HTTP	211
🔗 <i>SSL versus S-HTTP</i>	213
Podrobnosti o S-HTTP	214
🔗 <i>Získání S-HTTP</i>	215
Co hlavního je v S-HTTP nového vůči HTTP	215
Režimy kryptografického algoritmu a digitálního podpisu pro S-HTTP	216
Digitální podpis a S-HTTP	216
Výměny klíčů a šifrování	217
Integrita zpráv a autentizace odesilatele	217

Občerstvení transakcí S-HTTP	218
Zapouzdření HTTP	218
Co je to řádek požadavku S-HTTP	218
Co je to řádek odpovědi S-HTTP	219
Řádky záhlaví S-HTTP	219
Typy obsahu přijímané v S-HTTP	219
Rozložení záhlaví S-HTTP: Prearranged-Key-Info	220
Co je to záhlaví MAC-Info	220
Obsah zpráv S-HTTP	221
S-HTTP a Content-Privacy-Domain: PEM	222
Jak si odpovídají režimy PEM a S-HTTP	222
Dohadování v rámci S-HTTP	223
Formát dohadovacího záhlaví	223
Co to jsou dohadovací záhlaví S-HTTP	224
Parametry klíčových vzorů	226
<i>~Příklad bloku záhlaví pro typický server S-HTTP</i>	227
Výchozí hodnoty S-HTTP	227
Řádky záhlaví S-HTTP	228
Řádek záhlaví Certificate-Info	228
Záhlaví Key-Assign	229
Použití přiřazení inband key	229
Použití Kerberos Key Assignment	230
Použití S-HTTP nonces	230
Zpracování hlášení o stavové chybě serveru pod S-HTTP	230
Specifické chování S-HTTP při opakovaných pokusech	231
Omezení automaticky opakovaných pokusů pod S-HTTP	231
Automatický pokus o zašifrování	231
Prvky S-HTTP HTML	232
Rozšíření formátů S-HTTP HTML a URL	232
Co jsou prvky CERTS	233
Co je to prvek CRYPTOPTS	233
Shrnutí	233
Kde získat další informace na Internetu zabývající se S-HTTP	233
8 Secure Socket Layer (SSL) a její použití pro bezpečné přenosy v Internetu	237
Základní principy SSL verze 3.0.	237
<i>~Zachování soukromí při komunikaci</i>	238
Zajištění bezpečnosti přenosů pomocí SSL	239
Použití digitálních certifikátů v SSL k ověření serveru	239
<i>~Zabezpečení transakcí pomocí SSL od počátku až do konce</i>	240
SSL a šifrování RSA	242
SSL a vytváření bezpečných spojení	242
Popis SSL a jeho použití v prohlížečích a v servech	242
Jak zjistit, zda spojení, které používáme, je bezpečné ?	242
Ověření bezpečné komunikace při používání Netscape Navigatoru a Internet Exploreru	243
SSL Servery	244
<i>~Knihovna SSLRef</i>	245
SSLD – démon SSL	246
Konfigurační soubor SSLD	247
Závěrečné poznámky k SSLD	248
SSL a tunelové spojení přes firewally	249
SSL tunelování a metoda "Connect"	250
<i>~SSL Plus od firmy Consensus Development</i>	251
Poznámky k bezpečnosti SSL tunelování	252
SSL tunelování a rozšiřitelnost	252

☞ <i>Produkt SSLava od firmy Phaos Technologies</i>	253
Secure MIME	254
Podepisování objektů	255
Bezpečnostní API firmy Netscape	256
☞ <i>Jak se dozvědět více o SSL protokolu</i>	256
Shrnutí	257
Kde získat další informace na Internetu o SSL	257
9 Identifikace některých hackerských útoků a obrana proti nim	259
Nejjednodušší hackerský útok	260
☞ <i>Obrana proti útokům založeným na uhodnutí pořadového čísla</i>	261
Únos TCP protokolu	261
Útoky odposlouchávače	262
Aktivní desynchronizační útoky	263
Post-desynchronizační únos	264
Záplava TCP ACK	266
Desynchronizace při zahájení	267
Desynchronizace prázdnými daty	268
Útok na relaci Telnet	269
Více o záplavách ACK	270
Odhalení a vedlejší účinky	270
Prevence postdesynchronizačních únosů	271
Další scénář odposlouchávání – maskovaný útok	271
Vše o falšování	273
Falšování e-mailu	274
☞ <i>Falšování e-mailu z vašeho internetovského poštovního programu</i>	274
Detekce falšování	275
☞ <i>Obrana proti falšování použitím nástrojů tcpdump a netlog</i>	275
Jak předcházet falšování	276
Vše o únosech relací	276
Odhalení únosu relace	276
Ochrana před únosem	277
Falšování odkazů: útok na autentizaci SSL serverů	277
Ze zákulisí falešných odkazů	278
Podvržený odkaz v akci	278
Několik možností, jak předcházet napálení falešným odkazem	279
Dlouhodobé řešení	282
Falšování Webu	284
Důsledky napálení podvrženým odkazem	284
Falšování celého Webu	285
Jak útok funguje	285
Formuláře a bezpečná spojení	286
Zahájení útoku	287
Dokončení iluze – stavový řádek	287
Řádek Location	288
Prohlížení zdroje dokumentu	289
Prohlížení informací o dokumentu	289
Vystopování hackera	289
Opatření proti napálení falešným Webem	289
Dlouhodobé řešení	290
Shrnutí	290
Kde získat další informace na Internetu o běžných hackerských útocích	291
10 Výměna klíčů Kerbera v distribuovaných systémech	295
Úvod do systému Kerberos	295
☞ <i>Co jsou distribuované systémy</i>	296

System Kerberos z jiného pohledu	299
☞ <i>Bezplatné stažení systému Kerberos, verze 5, patch level 1</i>	299
☞ <i>Omezení exportu systému Kerberos</i>	299
Ještě jednou autentizační proces systému Kerberos	299
Kerberův protokol	300
☞ <i>Něco o přehraní</i>	302
Vzdálené operace	302
Klíče pro komunikaci mezi říšemi	303
Něco o autentizační cestě	304
☞ <i>Bezzubý Kerberos</i>	305
Příznaky lístků a žádosti o lístky	306
Zahajovací lístky	306
Preautentizované lístky	306
Neplatné lístky	306
Obnovitelné lístky	306
Postdatované lístky	307
Proxy lístky	308
Přenositelné lístky	309
Jiná nastavení autentizačního serveru	310
Databáze Kerbera	310
Obsah databáze	310
Další databázová pole	311
Často měněná pole databáze	311
Jména říší	312
Jména činitelů	312
Znamá citlivá místa systému Kerberos	314
Nevyhnutelné předpoklady, které Kerberos činí	314
☞ <i>Kompatibilita verze 4 a verze 5 systému Kerberos</i>	315
Kerberovské elektronické konference	315
Shrnutí	316
Kde získat další informace na Internetu o systému Kerberos	316
11 Jak se chránit při obchodování na Internetu	319
Základní prvky obchodování na Internetu	319
Elektronická hotovost	321
☞ <i>Něco víc o systému CyberCash</i>	321
Jak zaručí systém elektronické hotovosti soukromí pro transakce	322
Bezpečnost elektronické hotovosti	324
Problémy s elektronickou hotovostí	325
Význam "maskování" podpisů	325
☞ <i>Nejnámější systém elektronické hotovosti – ecash</i>	327
Internet a použití kreditních karet	327
☞ <i>Verifikace bezpečné komunikace v programech Netscape Navigator a Internet Explorer</i>	328
Prohlížení certifikátů	330
☞ <i>Bezpečnost kreditních karet u First Virtual</i>	330
Shrnutí	331
Kde získat další informace na Internetu o obchodování na Internetu	331
12 Použití auditních záznamů k odhalení a odehnání vetřelců	333
Zjednodušení auditních záznamů	333
☞ <i>Jak nastavit generování auditních záznamů</i>	334
Problémy s auditem	335
☞ <i>Auditní nástroje dostupné online</i>	335
Auditní záznamy a Unix	335
Kontrola posledního přihlášení uživatele pomocí utility lastlog	336

<i>~</i> <i>Auditní nástroj Stalker</i>	336
Sledování přihlášených uživatelů pomocí <i>utmp</i>	337
Další software pro odhalování vetřelců	337
Sledování dříve přihlášených uživatelů pomocí <i>wtmp</i>	337
Použití deníku <i>syslog</i>	339
<i>~</i> <i>Program WatchDog pro auditní záznamy v systému SunOS</i>	341
Sledování změn uživatele pomocí utility <i>slolog</i>	342
Sledování dial-out přístupu pomocí utility <i>aculog</i>	342
Záznam načasovaných transakcí	342
Jak odhalit napadení SMTP použitím deníku programu <i>sendmail</i>	343
Deník historie shellu	343
Audit ve Windows NT	343
Aktivace bezpečnostního zaznamenávání v systému NT	344
Audit bazových objektů v systému NT	346
Audit bazových objektů	346
Audit privilegií v NT	348
Ukončení běhu systému při přeplnění auditního deníku ve Windows NT	349
Audit v systému Novell NetWare	351
Jak jsou v NetWaru definované auditní služby	351
<i>~</i> <i>Nastavení auditu v NetWare</i>	351
Prohlížení auditních záznamů	352
Nastavení auditora v systému Novell NetWare	352
Nastavení auditu pro svazek	353
Nastavení auditu pro NDS kontejner	354
<i>~</i> <i>Auditní nástroje v jiných jazycích</i>	355
Shrnutí	356
Kde získat další informace na Internetu o auditních záznamech	357
13 Otázky bezpečnosti kolem programovacího jazyka Java	359
Jak chápat jazyk Java	360
<i>~</i> <i>Co je bajtový kód</i>	360
<i>~</i> <i>Odkud stáhnout Javu</i>	362
Co se děje s Javou v prohlížeči	363
Komponenty Javy	364
Zavaděč třídy	364
<i>~</i> <i>Více o prostoru jmen</i>	364
Verifikátor apletů	365
<i>~</i> <i>Chyba v implementaci verifikátoru</i>	365
Manažer bezpečnosti apletů	366
Základní problémy bezpečnosti apletů Javy	366
<i>~</i> <i>Bezpečnost Javy</i>	367
Základní principy Javy	368
Omezenost funkčnosti apletů	368
Jak aplety pracují se soubory	368
Jak povolit čtení souborů	369
<i>~</i> <i>Prohlížeč HotJava</i>	370
Jak povolit zápis do souborů	371
Čtení vlastností systému v rámci apletu	371
Zakrytí systémových vlastností	372
Zobrazování chráněných systémových vlastností	372
Otevření spojení s jiným počítačem v rámci apletu	373
Otevírání síťového spojení s uzlem, odkud aplet pochází	374
Udržování perzistentních apletů	374
Spouštění programů z apletů	375
<i>~</i> <i>Základní opatření proti útokům prostřednictvím Javy</i>	375
Tvorba bezpečných apletů	377