

Stučný obsah

Bezpečný kód

Část I

Bezpečnost v současném světě

Kapitola 1	Proč je potřeba zabezpečovat systémy	37
Kapitola 2	Proaktivní procesy vývoje s bezpečností	55
Kapitola 3	Bezpečnostní principy pro život	79
Kapitola 4	Modelování hrozeb	97

Část II

Techniky bezpečného kódování

Kapitola 5	Veřejný nepřítel číslo 1: přetečení bufferu	149
Kapitola 6	Jak stanovit správné řízení přístupu	187
Kapitola 7	Spouštět vždy s nejmenšími oprávněními	219
Kapitola 8	Slabiny v kryptografii	265
Kapitola 9	Jak ochránit tajná data	301
Kapitola 10	Veškerý vstup je zlo!	337
Kapitola 11	Problémy s kanonickou reprezentací	357
Kapitola 12	Problémy se vstupem v databázích	387
Kapitola 13	Zvláštní problémy se vstupem ve webovém prostředí	401
Kapitola 14	Problémy s mezinárodním prostředím	425

Část III

Další techniky bezpečného kódování

Kapitola 15	Bezpečnost soketů	439
Kapitola 16	Zabezpečení RPC, ovládacích prvků ActiveX a modelu DCOM	459
Kapitola 17	Ochrana proti útokům s odepřením služeb	495
Kapitola 18	Jak psát bezpečný kód .NET	511

Část IV

Speciální témata

Kapitola 19	Testování bezpečnosti	541
Kapitola 20	Provedení bezpečnostní revize kódu	583
Kapitola 21	Bezpečná instalace softwaru	595
Kapitola 22	Obecné doporučené postupy	609
Kapitola 23	Jak psát bezpečnostní dokumentaci a chybové zprávy	639

Část V

Přílohy

Příloha A	Nebezpečná volání API	657
Příloha B	Nejhloupější výmluvy, které můžeme slyšet	669
Příloha C	Seznam bezpečnostních kontrol pro návrháře	677
Příloha D	Seznam bezpečnostních kontrol pro vývojáře	679
Příloha E	Seznam bezpečnostních kontrol pro testera	685

	Jedna myšlenka na závěr: kanonizační problémy jiného než souborového charakteru	383
	Názvy serverů	383
	Uživatelská jména	384
	Shrnutí	386
Kapitola 12	Problémy se vstupem v databázích	387
	Charakteristika problému	388
	Pseudo-náprava číslo 1: Citování vstupu	390
	Pseudo-náprava číslo 2: Volání uložených procedur	391
	Skutečná náprava číslo 1: Nikdy se nepřipojujte jako sysadmin	392
	Skutečná náprava číslo 2: Bezpečné sestavování příkazů SQL	393
	Jak bezpečně sestavovat uložené procedury SQL	394
	Hloubková obrana v hloubkovém příkladu	395
	Shrnutí	399
Kapitola 13	Zvláštní problémy se vstupem ve webovém prostředí	401
	Křížové volání skriptů mezi servery: když výstup zlobí	402
	Někdy útočník nepotřebuje blok <SCRIPT>	405
	Útočník ani nepotřebuje, aby uživatel klepnul na odkaz	405
	Ostatní útoky spojené s křížovými skripty	406
	Útoky s křížovými skripty proti místním souborům	406
	Útoky s křížovými skripty proti prostředkům HTML	408
	Náprava problémů s křížovými skripty	408
	Kódování výstupu	409
	Zápis uvozovek okolo všech vlastností značek	409
	Vkládání dat do vlastnosti innerText	410
	Vynucení kódové stránky	410
	Možnosti cookies HttpOnly v Internet Exploreru 6.0 SP1	411
	Kategorizace webu v Internet Exploreru	412
	Atribut <FRAME SECURITY> v Internet Exploreru	413
	Konfigurační volba ValidateRequest v ASP.NET 1.1	413
	Nevyhledávejte nebezpečné konstrukce	414
	Ale já chci, aby mohli uživatelé vkládat do mého webu HTML	416
	Jak v kódu kontrolovat chyby s křížovými skripty	417
	Ostatní témata k webové bezpečnosti	417
	I volání eval() může být špatné	417
	Problémy s důvěryhodností HTTP	418
	Aplikace a filtry ISAPI	419
	Dávejte pozor na předvidatelné cookies	421
	Problémy klientů SSL/TLS	422
	Shrnutí	423

Kapitola 14	Problémy s mezinárodním prostředím	425
	Zlatá pravidla pro bezpečnost mezinárodních aplikací	426
	V aplikacích používejte Unicode	426
	Jak zabránit přetečení bufferu v mezinárodních aplikacích	426
	Slova a bajty	427
	Ověřování v mezinárodním prostředí	428
	Vizuální ověřování	428
	Neověřujte řetězce s voláním LCMaPString	429
	Názvy souborů ověřujte pomocí volání CreateFile	429
	Problémy s převodem znakové sady	429
	Do volání MultiByteToWideChar předávejte parametry MB_PRECOMPOSED a MB_ERR_INVALID_CHARS	430
	Do volání WideCharToMultiByte předávejte parametr WC_NO_BEST_FIT_CHARS	430
	Porovnávání a řazení	432
	Vlastnosti znaků Unicode	433
	Normalizace	434
	Shrnutí	435

Část III

Další techniky bezpečného kódování

Kapitola 15	Bezpečnost soketů	439
	Jak zabránit únosu serveru	440
	Útoky s oknem protokolu TCP	446
	Výběr serverových rozhraní	447
	Příjem spojení	447
	Jak psát aplikace s ohledem na firewally	452
	Potřebné operace proveďte nad jedním spojením	452
	Nepožadujte od serveru zpětné spojení ke klientu	453
	Používejte spojované protokoly	453
	Nepřepínejte aplikaci přes jiný protokol	454
	Nevkládejte hostitelské IP adresy do dat aplikační vrstvy	454
	Aplikaci musí být možné konfigurovat	454
	Falšování komunikace a důvěra podle hostitelů a podle portů	454
	Přichází IPv6!	455
	Shrnutí	457
Kapitola 16	Zabezpečení RPC, ovládacích prvků ActiveX a modelu DCOM	459
	Abeceda RPC	460
	Co je to RPC?	460
	Vytváření aplikací RPC	461
	Jak aplikace v RPC komunikují	463

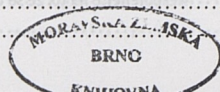
Nejlepší postupy pro bezpečné RPC	464
Použijte přepínač /robust v kompilátoru MIDL	464
Použijte atribut [range]	465
Vyžadujte autentizaci spojení	465
Zajistěte soukromí a integritu paketů	470
Použijte striktní popisovače kontextu	471
Nespoléhejte se na popisovač kontextu při kontrole přístupu	473
Dávejte pozor na prázdné popisovače kontextu	474
Ani „příteli“ nevěřte	475
Bezpečnostní zpětná volání	476
Důsledky několika serverů RPC v jediném procesu	478
Použijte známé protokoly	479
Nejlepší postupy pro bezpečný DCOM	480
Základy modelu DCOM	480
Bezpečnost na úrovni aplikací	482
Uživatelské kontexty v DCOM	482
Programová bezpečnost	485
Zdroje a jímky	488
Abeceda ActiveX	488
Nejlepší postupy pro bezpečné ActiveX	489
Jaké komponenty ActiveX jsou bezpečné pro inicializaci a pro skriptování	489
Nejlepší postupy pro bezpečnou inicializaci a skriptování	491
Shrnutí	494
Kapitola 17 Ochrana proti útokům s odepřením služeb	495
Útoky s havárií aplikace	496
Útoky se strádáním procesoru	499
Útoky se strádáním paměti	505
Útoky se strádáním prostředků	506
Útoky na šířku pásma sítě	508
Shrnutí	509
Kapitola 18 Jak psát bezpečný kód .NET	511
Bezpečnost kódu pro přístup obrazem	513
Nástroj FxCop: povinná výbava	515
Sestavení musí mít silné názvy	516
Silné názvy sestavení a ASP.NET	518
Stanovení požadavků na oprávnění v sestavení	518
Žádejte minimální množinu oprávnění	518
Nepotřebná oprávnění odmítněte	519
Vyžádejte si volitelná oprávnění	519
Přilíš horlivá volání Assert	520
Další informace k voláním Demand a Assert	522

002	Aserktivní okno při uplatnění musí být malé	523
102	Požadavky a požadavky na odkaz	525
082	Příklad bezpečnostní chyby s voláním LinkDemand	525
002	S atributem SuppressUnmanagedCodeSecurityAttribute opatrně	527
002	Vzdálené požadavky	527
002	Omezte přístup k vašemu kódu	528
002	V kódu XML ani konfiguračních souborech nesmí být citlivá data	529
102	Kontrolujte sestavení, která umožňují částečnou důvěru	530
102	Kontrolujte správnost řízených obálek nad neřízeným kódem	531
002	Problémy s delegáty	531
002	Problémy se serializací	532
002	Role izolovaného úložiště	533
002	Před nasazením aplikací ASP.NET vypněte trasování a ladění	534
002	Na dálku nevyepisujte podrobné chybové informace	535
002	Deserializace dat z nedůvěryhodných zdrojů	535
002	Při havárii neprozrazujte útočníkovi zbytečně mnoho informací	536
002	Shrnutí	537

Část IV

Speciální témata

Kapitola 19	Testování bezpečnosti	541
002	Role bezpečnostního testera	542
010	Testování bezpečnosti je jiné	542
010	Vytvoření plánu bezpečnostních testů z modelu hrozeb	543
110	Dekompozice testované aplikace	544
010	Identifikace rozhraní jednotlivých komponent	544
010	Ohodnocení všech rozhraní podle zranitelnosti	545
010	Kontrola datových struktur, používaných nad jednotlivými rozhraními	546
010	Útok na aplikace s metodikou STRIDE	547
010	Útok s pozměněním dat	549
010	Před testováním	559
010	Vytvoření nástrojů pro hledání chyb	560
010	Testování klientů s falešnými servery	575
010	Možnost vidět nebo modifikovat data	576
010	Testování se šablonami zabezpečení	576
010	Pokud jste našli nějakou chybu, ještě nejste hotovi	578
010	I testovací kód musí mít vysokou kvalitu	579
010	Testování celého řešení	579
050	Zjištění útočné plochy	579
050	Zjištění velikosti útočného vektoru	580
050	Zjištění sklonu útočného vektoru	580



	Vypočtení součinu vektorů násobených sklonem	580
	Shrnutí	581
Kapitola 20	Provedení bezpečnostní revize kódu	583
	Jak zvládnout rozsáhlou aplikaci	585
	Metoda více průchodů	586
	Snadno dostupné ovoce	586
	Přetečení celých čísel	588
	Související problém: podtečení	591
	Kontrola návratů z rutin	591
	Kód s ukazateli podrobte další revizi	592
	Datům nikdy nedůvěřujte	592
	Shrnutí	593
Kapitola 21	Bezpečná instalace softwaru	595
	Zásada nejmenších oprávnění	596
	Uklízejte po sobě!	598
	Editor konfigurace zabezpečení	598
	Bezpečnostní volání API na nízké úrovni	606
	Instalační služba systému Windows	606
	Shrnutí	608
Kapitola 22	Obecné doporučené postupy	609
	Útočníkovi nic neříkejte	609
	Doporučené postupy pro služby	610
	Bezpečnost, služby a interaktivní plocha	610
	Zásady pro práci s účty služeb	611
	Neprozrazujte informace v textových řetězcích	613
	Pozor na změnu chybových zpráv v rámci opravy aplikace	613
	Kód v chybové cestě důkladně zkontrolujte	614
	Nechte to vypnuté!	614
	Omyly s režimem jádra	614
	Problémy s bezpečností na vysoké úrovni	614
	Popisovače	615
	Symbolické odkazy	616
	Kvóty	616
	Serializační primitiva	616
	Problémy s ošetřením bufferů	616
	Stornování balíčku s požadavkem IRP	619
	Do kódu zapisujte bezpečnostní komentáře	619
	Využívejte funkci operačního systému	620
	Nespoléhejte na to, že se uživatel rozhodne dobře	620

Bezpečné volání CreateProcess	621
Do parametru lpApplicationName nepředávejte hodnotu NULL	622
Cestu ke spustitelnému souboru v parametru lpCommandLine zapisujte do uvozovek	622
Nevytvářejte sdílené a zapisovatelné segmenty	622
Používejte správně funkce pro zosobnění	623
Do složky \Program Files nezapisujte uživatelské soubory	623
Do registrační větve HKLM nezapisujte uživatelská data	624
Neotevírejte objekty s oprávněním FULL_CONTROL nebo ALL_ACCESS	624
Omyly při vytváření objektů	624
Jak pečovat o volání CreateFile a čím ho nakrmit	626
Jak bezpečně vytvářet dočasné soubory	627
Důsledky instalačních programů a systému EFS	630
Problémy se spojovacími body v souborovém systému	631
Bezpečnost na straně klienta je protimluv	631
Ukázkové aplikace jsou vzorem	632
Stůjte si za svým	632
Budete dlužní uživatelům, když.	633
Jak stanovit přístup podle SID administrátora	633
Povolte dlouhá hesla	634
S funkcí _alloca opatrně.	634
Konverzní makra knihovny ATL	635
Nikam nevkládejte názvy platné uvnitř firmy	635
Řetězce přešuněte do knihovny DDL s prostředky	636
Záznam do aplikačního protokolu	636
Převěďte nebezpečný kód C/C++ na řízený kód	637
Kapitola 23 Jak psát bezpečnostní dokumentaci a chybové zprávy	639
Bezpečnostní problémy v dokumentaci	640
Základy	640
Potlačování hrozeb prostřednictvím dokumentace	641
Dokumentování doporučených bezpečnostních postupů	641
Bezpečnostní problémy v chybových zprávách	643
Typické bezpečnostní zprávy	643
Problémy s prozrazením informací	644
Informovaný souhlas	645
Progresivní prozrazování	647
Buďte konkrétní	648
Zvažte, že určitou otázku nemusíte pokládat	649
Testování použitelnosti bezpečnostních zpráv	651
Poznámka ke kontrole specifikací produktu	651
Použitelnost bezpečnostních funkcí	652
Shrnutí	653

Část V**Přílohy**

Příloha A	Nebezpečná volání API	657
	Volání API s rizikem přetečení bufferu	658
	Volání API s rizikem podvržení názvu	660
	Volání API s rizikem trojských koňů	661
	Styly oken a typy ovládacích prvků	662
	Volání API pro zosobnění	663
	Volání API s rizikem odepření služeb	664
	Problémy se síťovými voláními API	665
	Různá jiná volání API	666
Příloha B	Nejhloupejší výmluvy, které můžeme slyšet	669
Příloha C	Seznam bezpečnostních kontrol pro návrháře	677
Příloha D	Seznam bezpečnostních kontrol pro vývojáře	679
	Obecné	680
	Webové a databázové	681
	Volání RPC	681
	ActiveX, COM a DCOM	682
	Řízení kryptografie a tajných informací	682
	Řízený kód	682
Příloha E	Seznam bezpečnostních kontrol pro testera	685
Myšlenka na závěr		687
Literatura		689
	Citovaná literatura	689
	Další doporučená literatura	693
Autoři		695
	Michael Howard	695
	David LeBlanc	695

Bezpečný kód pro Windows Vista	757
Předmluva	699
Úvod	701
Pro koho je tato kniha určena	702
Jakou má tato kniha souvislost s publikací Bezpečný kód.	702
Jak číst tuto knihu.	702
Práce s kódem v této knize.	703
Co je na doprovodné webové stránce.	704
Požadavky na systém	704
Podpora Microsoft Press	705
Dotazy a připomínky.	705
Poznámka redakce českého vydání	706
Kapitola 1 Kvalita kódu	707
Přehled	707
Brány kvality ve Windows Vista.	709
Všechny řetězcové zásobníky C/C++ mají anotaci SAL	709
Ukázka SAL	710
__in	711
__out	711
__in_opt	711
__inout	712
__inout_bcount_full(n)	712
__inout_bcount_part(n,m)	712
__deref_out_bcount(n)	713
Jak použít SAL v existujícím kódu	713
Zakázané API je potřeba odstranit z kódu	714
Zakázanou kryptografii je nutné odstranit z kódu	715
Statická analýza slouží ke hledání a opravě chyb	715
Varování direktivy /analyze	716
Varování nástroje Application Verifier	717
Varování FxCop.	717
Neřízený kód C/C++ kompilovaný s volbami /GS a linkovaný s volbami /SafeSEH, /DynamicBase a /NXCompat.	717
Realizace	717
Literatura	718
Kapitola 2 Řízení uživatelských účtů, tokeny a úrovně integrity	719
Přehled	719
Podrobnosti o řízení uživatelských účtů.	720
Začneme od začátku – uživatelské tokeny.	721

Povyšení oprávnění na administrátora	724
Mírná odchylka: „Administrátor se schvalovacím režimem“	724
Aktualizovaný formát tokenu ve Windows Vista	726
Určení, jde-li o proces s povýšeným oprávněním	726
Jak vyžádat, aby aplikace běžela pod administrátorským účtem	727
Jak vynutit, aby si aplikace vyžádala přihlašovací údaje nebo souhlas	730
Spuštění komponent COM s pomocí COM Elevation Monikeru	731
Spuštění aplikací se zvýšeným oprávněním s řízeným kódem	732
Úvahy o uživatelském rozhraní	732
Virtualizace	733
Jak zakázat ve své aplikaci virtualizaci	736
Úrovně integrity	737
Pravidla pro nastavení integrity	746
Masky NW, NR a NX	746
Defenzivní model s použitím úrovně integrity	746
Ladění problémů spojených s kompatibilitou aplikací ve Windows Vista	747
Souborová varování	748
Varování týkající se registru	748
Varování týkající se INI	748
Varování týkající se tokenu	748
Varování týkající se oprávnění	748
Varování týkající se jmenného prostoru	749
Varování týkající se dalších objektů	749
Varování týkající se procesů	749
Význam podepisování kódu	749
Nová oprávnění ve Windows Vista	750
SE_TRUSTED_CREDMAN_ACCESS_NAME (“SeTrustedCredManAccessPrivilege”)	750
SE_TRUSTED_CREDMAN_ACCESS_PRIVILEGE (31L)	750
SE_RELABEL_NAME (“SeRelabelPrivilege”)	750
SE_RELABEL_PRIVILEGE (32L)	750
SE_INC_WORKING_SET_NAME (“SeIncreaseWorkingSetPrivilege”)	750
SE_INC_WORKING_SET_PRIVILEGE (33L)	750
SE_TIME_ZONE_NAME (“SeTimeZonePrivilege”)	750
SE_TIME_ZONE_PRIVILEGE (34L)	750
SE_CREATE_SYMBOLIC_LINK_NAME (“SeCreateSymbolicLinkPrivilege”)	750
SE_CREATE_SYMBOLIC_LINK_PRIVILEGE (35L)	750
Realizace	751
Literatura	751
Kapitola 3 Ochrana proti přetečení zásobníku	753
Přehled	753
ASLR	755

Omezení ASLR	757
Důsledky pro výkon a kompatibilitu	757
Náhodné umístění zásobníku	758
Důsledky pro výkon a kompatibilitu	759
Ochrana haldy	759
NX	763
Důsledky pro výkon a kompatibilitu	765
/GS	767
SafeSEH	770
Shrnutí	774
Realizace	775
Literatura	775
Kapitola 4 Síťové ochrany	777
Přehled	777
Obecně o IPv6	778
Teredo	780
Správce síťového seznamu (Network List Manager)	782
Platforma Windows Vista RSS	783
Rozšíření rozhraní Winsock Secure Socket	785
Firewall ve Windows s pokročilou bezpečností (Advanced Security)	786
Globální nastavení firewallu	786
Tvorbá pravidel	788
Práce se skupinami pravidel	793
Realizace	795
Literatura	795
Kapitola 5 Bezpečné a odolné služby	797
Základní popis služeb	797
Účty pro služby	799
Omezení oprávnění	802
Oprávnění na vysoké úrovni	804
Neškodná oprávnění	806
Řízení síťového přístupu	807
Komunikace s plochou	809
Jednoduché zprávy	811
Sdílená paměť	811
Pojmenované roury (Named pipes)	812
Sokety	816
RPC/COM	816
Lekce ze života	817
Realizace	818
Literatura	818

Bezpečný kód pro Windows Vista

Kapitola 1	Kvalita kódu	707
Kapitola 2	Řízení uživatelských účtů, tokeny a úrovně integrity	719
Kapitola 3	Ochrana proti přetečení zásobníku	753
Kapitola 4	Sítové ochrany	777
Kapitola 5	Bezpečné a odolné služby	797
Kapitola 6	Ochrany v Internet Exploreru 7	819
Kapitola 7	Vylepšená kryptografie	827
Kapitola 8	Autentizace a autorizace	849
Kapitola 9	Různé technologie v oblasti ochrany a bezpečnosti	861

Bezpečnost v současném světě

Kapitola 1	Proč je potřeba zabezpečovat systémy	37
	Applikace v prostředí „Wild Wild Webu“	39
	Proč jsou potřeba důvěryhodné počítačové technologie	41
	Všechny heavy dostrumady	41
	„Jak organizaci prodat“ bezpečnost s cílem	41
	Podvratné metody	45
	Několik námětů k prosazování kultury bezpečnosti	46
	Prinějte šéfa k rozetiání e-mailové zprávy	46
	Invenjře bezpečnostního kazuete	47
	Výhoda otočnicků a dilema obránců	51
	Priněje číslo 1: obránce musí chránit všechna místa, útočník si může zvolit jen to nejtahší	51
	Priněje číslo 2: obránce se může bránit jen proti známým útokům, útočník může zlozčínit i dosud neznámá zranitelná místa	51
	Priněje číslo 3: obránce musí být ve střehu neustále, útočník může udeřit kdykoli i zneodnáni	52
	Priněje číslo 4: obránce musí dodržovat pravidla hry, útočník žádná pravidla nemá	52
	Shrnutí	52
Kapitola 2	Proaktivní procesy vývoje s bezpečností	55
	Zlepšovací procesy	57
	Význam vzdělávání	58
	Odpor k pozitivnímu školění	60
	Problémové vzdělávání	61
	Všecký pokrok v bezpečnosti	61

Kapitola 6	Ochrany v Internet Exploreru 7	819
	Přehled	819
	Zásadní ochrany	820
	Volitelné ActiveX	821
	Chráněný režim (Protected Mode)	822
	Prevence spouštění dat (Data Execution Prevention, DEP)	825
	Rozhraní cURL a IUri	828
	Uzamčení prvku ActiveX	829
	Další skutečnosti, které byste o Internet Exploreru 7 měli vědět	830
	Zrušení přístupu do schránky	830
	Adresy URL pro skripty	830
	Sbohem PCT a SSL2 (a Good Riddance), ať žije AES!	830
	Původ okna	831
	Realizace	831
	Literatura	832
Kapitola 7	Vylepšená kryptografie	833
	Přehled	833
	Režim jádra a uživatelský režim	834
	Kryptografická pružnost	834
	Kryptografická pružnost v CNG	835
	Nové algoritmy v CNG	836
	Práce s CNG	839
	Šifrování dat	839
	Hašování dat	839
	Kódování MAC	840
	Generování náhodných čísel	840
	CNG a FIPS	840
	Vylepšené auditování	841
	Co v CNG chybí	842
	Vylepšení SSL/TLS	843
	Ověření zrušení SSL/TLS a OCSP	844
	Kořenové certifikáty ve Windows Vista	846
	Zrušené kryptografické funkce ve Windows Vista	847
	Realizace	847
	Literatura	847
Kapitola 8	Autentizace a autorizace	849
	CardSpace a informační karty ve Windows	849
	Datový tok systému informačních karet	850
	Windows CardSpace a phishing	851
	Serverová autentizace	851

CardSpace a phishing – příklad	852
Informační karty v akci	854
Co se nachází v informační kartě	854
Programový přístup k informačním kartám	855
Shrnutí technologie CardSpace	857
Změny v grafické identifikaci a autorizaci	
(Graphical Identification and Authorization, GINA)	857
Změny ve vlastnických SID	858
Realizace	859
Literatura	859
Kapitola 9 Různé technologie v oblasti ochrany a bezpečnosti	861
Přehled	861
Rodičovská kontrola v aplikaci	862
Kód	863
Časové limity	863
Chyba 450	864
Zjištění, je-li zapnuto blokování stahování souborů	864
Vypnutí filtrování pro vaši aplikaci nebo URL	864
Protokoly událostí	865
Rozhraní API Windows Defender	865
Přečtěte si dokumentaci ohledně pravidel pro Windows Defender!	866
Podepište svůj kód	866
Požadavek na přidání na seznamy „Known“ (Znamé) nebo „Not Yet Classified“ (Zatím nehodnoceno)	867
Nové API pro přihlašování uživatele	867
Používání bezpečnostního protokolu událostí	869
Šifrování ukazatelů	870
Problémy s laděním režimu jádra	873
Programování Trusted Platform Module (TPM)	873
Přístup k TPM na nízké úrovni	875
Úvahy o procesu Postranní panel Windows a bezpečnosti doplňků	878
Literatura	879

Obsah

Bezpečný kód

Úvod	29
Pro koho je tato kniha určena	30
Uspořádání knihy	30
Instalace a používání ukázkových souborů	31
Stahování lokalizovaných zdrojových kódů	31
Systémové požadavky	31
Informace o podpoře	32
Poděkování	32

Část I

Bezpečnost v současném světě

Kapitola 1	Proč je potřeba zabezpečovat systémy	37
	Aplikace v prostředí „Wild Wild Webu“	39
	Proč jsou potřeba důvěryhodné počítačové technologie	41
	Všechny hlavy dohromady	41
	Jak organizaci prodávat bezpečnost s citem	41
	Podratné metody	45
	Několik námětů k prosazování kultury bezpečnosti	46
	Přimějte šéfa k rozeslání e-mailové zprávy	46
	Jmenujte bezpečnostního kazatele	47
	Výhoda útočníků a dilema obránců	51
	Princip číslo 1: obránce musí chránit všechna místa, útočník si může zvolit jen to nejslabší	51
	Princip číslo 2: obránce se může bránit jen proti známým útokům, útočník může zkusit i dosud neznámá zranitelná místa	51
	Princip číslo 3: obránce musí být ve střehu neustále, útočník může udeřit kdykoli a znenadání	52
	Princip číslo 4: obránce musí dodržovat pravidla hry, útočník žádná pravidla nectí	52
	Shrnutí	52
Kapitola 2	Proaktivní procesy vývoje s bezpečností	55
	Zlepšování procesů	57
	Význam vzdělávání	58
	Odpor k povinnému školení	60
	Průběžné vzdělávání	61
	Vědecký pokrok v bezpečnosti	61

Vzdělání dokazuje, že i více očí se může mýlit	62
A teď důkazy!	63
Fáze návrhu	63
Otázky na bezpečnost při pohovorech	64
Jak definovat bezpečnostní cíle produktu	65
Bezpečnost je jednou z vlastností produktu	66
Udělejte si na bezpečnost čas	69
Modelování hrozeb vede k bezpečnému návrhu	70
Připravte plán ukončení života nebezpečných funkcí	70
Zvedněte latku bezpečnosti	70
Týmová revize bezpečnosti	71
Fáze vývoje	72
Přísně hlídejte, kdo smí registrovat nový kód (kontrola vracení kódu)	72
Bezpečnostní revize nového kódu partnerem (kontrola vracení kódu)	72
Definice zásad bezpečného kódování	72
Revize starých defektů	73
Externí revize bezpečnosti	73
Bezpečnostní akce	73
Rozumně s počtem chyb	74
Sledujte chybové metriky	74
Žádná překvapení a žádná „velikonoční vajíčka“	75
Fáze testování	75
Fáze dodávky produktu a údržby	75
Jak zjistíte, že jste hotovi	75
Proces reakce na problémy	76
Odpovědnost	76
Shrnutí	76
Kapitola 3 Bezpečnostní principy pro život	79
SD ³ , bezpečnost na třetí: zabezpečení při vývoji, výchozím nastavení a instalaci	79
Secure by Design – Zabezpečení při vývoji	80
Secure by Default – Zabezpečení při výchozím nastavení	81
Secure by Deployment – Zabezpečení při instalaci	81
Základní bezpečnostní principy	82
Poučte se z chyb	82
Minimalizujte plochu útoku	84
Zavedte bezpečné výchozí hodnoty	85
Používejte hloubkovou obranu	86
Používejte nejmenší možná oprávnění	87
Zpětná kompatibilita je vždy neštěstím	89
Externí systémy považujte za nebezpečné	90
Připravte se na selhání	91

Při havárii přejděte do bezpečného stavu	91
Bezpečnostní funkce nejsou totéž co bezpečné funkce	93
Nikdy se nespolehejte jen na princip „bezpečnost za cenu nesrozumitelnosti“	93
Nesměšujte kód a data	93
Bezpečnostní problémy správně opravte	94
Shrnutí	95
Kapitola 4 Modelování hrozeb	97
Bezpečný návrh a modelování hrozeb	98
Sestavte tým pro modelování hrozeb	100
Dekomponujte aplikaci	100
Určete hrozby, kterým je systém vystaven	109
Ohodnotte hrozby snížením rizik	117
Vyberte způsob reakce na hrozby	130
Vyberte techniky pro potlačení hrozeb	131
Bezpečnostní techniky	132
Autentizace	132
Autorizace	137
Technologie s odolností proti pozměnění a s posílením soukromí	138
Tajné informace chráňte, nebo je ještě lépe neukládejte	139
Šifrování, haše, kódy MAC a digitální podpisy	139
Audit	140
Filtrování, zpomalení provozu a kvalita služeb	140
Nejmenší oprávnění	141
Jak potlačit hrozby v ukázkové mzdové aplikaci	141
Sbírka hrozeb a jejich řešení	142
Shrnutí	146

Část II

Techniky bezpečného kódování

Kapitola 5 Veřejný nepřítel číslo 1: přetečení bufferu	149
Přetečení zásobníku	151
Přetečení haldy	158
Chyby při indexování polí	163
Chyby s formátováním řetězců	165
Nesoulad velikosti bufferů pro řetězce Unicode a ANSI	170
Reálný příklad s chybou Unicode	171
Jak zabránit přetečení bufferu	172
Bezpečné zpracování řetězců	173
Upozornění k funkcím pro zpracování řetězců	182
Volba kompilátoru Visual C++ .NET /GS	183
Shrnutí	185

Kapitola 6	Jak stanovit správné řízení přístupu	187
	Proč jsou přístupové seznamy důležité	188
	Malé odbočení: oprava kódu pro manipulaci s registrem	189
	Z čeho se skládá přístupový seznam	191
	Postup pro zvolení dobrého přístupového seznamu	193
	Jak vytvořit položku s účinným odepřením	195
	Vytvoření přístupového seznamu	196
	Vytvoření přístupového seznamu ve Windows NT 4	196
	Vytvoření přístupového seznamu ve Windows 2000	199
	Vytvoření přístupového seznamu v Active Template Library	203
	Jak definovat správné pořadí položek řízení přístupu	204
	Nezapomeňte na SID terminálového serveru a vzdálené plochy	206
	Prázdné volitelné seznamy řízení přístupu a další nebezpečné typy položek	207
	Prázdné volitelné seznamy řízení přístupu a audit	209
	Nebezpečné typy položek řízení přístupu	210
	Co když prázdný DACL nemohu změnit	211
	Ostatní mechanismy řízení přístupu	211
	Role v .NET Framework	212
	Role v COM+	213
	Omezení provozu IP	214
	Spouště a oprávnění SQL Serveru	215
	Příklad ze zdravotnictví	215
	Důležitá poznámka k mechanismům řízení přístupu	216
	Shrnutí	217
Kapitola 7	Spouštět vždy s nejmenšími oprávněními	219
	Nejmenší možné oprávnění v reálném světě	220
	Viry a trojské koně	220
	Pozměnění webového serveru	221
	Stručný přehled řízení přístupu	222
	Stručný přehled oprávnění	222
	Problémy s oprávněním SeBackupPrivilege	223
	Problémy s oprávněním SeRestorePrivilege	226
	Problémy s oprávněním SeDebugPrivilege	226
	Problémy s oprávněním SeTcbPrivilege	227
	Problémy s oprávněním SeAssignPrimaryTokenPrivilege a SeIncreaseQuotaPrivilege	227
	Problémy s oprávněním SeLoadDriverPrivilege	227
	Problémy s oprávněním SeRemoteShutdownPrivilege	228
	Problémy s oprávněním SeTakeOwnershipPrivilege	228
	Stručný přehled tokenů	228
	Jak spolu souvisejí tokeny, oprávnění, SID, ACL a procesy	229
	SID a kontrola přístupu, oprávnění a kontrola oprávnění	230

Tři důvody, pro které aplikace vyžadují zvýšená oprávnění	230
Problémy s přístupovými seznamy	230
Problémy s oprávněními	231
Tajné informace LSA	232
Jak vyřešit problémy se zvýšenými oprávněními	232
Jak vyřešit problémy s ACL	232
Jak vyřešit problémy s oprávněními	233
Jak vyřešit problémy s LSA	233
Postup při stanovení odpovídajících oprávnění	233
Krok 1: Zjistit, jaké prostředky daná aplikace potřebuje	234
Krok 2: Zjistit, která privilegovaná volání API daná aplikace používá	234
Krok 3: Který účet budeme vlastně potřebovat?	235
Krok 4: Sestavit obsah tokenu	235
Krok 5: Jsou všechny SID a všechna oprávnění skutečně potřeba?	240
Krok 6: Upravit token	241
Účty služeb s nejnižším oprávněním ve Windows XP a Windows .NET Server 2003	253
Oprávnění k zosobnění a Windows .NET Server 2003	255
Ladění problémů s nejmenšími oprávněními	256
Proč aplikace pod normálním uživatelem havarují	257
Jak zjistit příčinu havárií aplikace	257
Shrnutí	263
Kapitola 8 Slabiny v kryptografii.	265
Nevhodná náhodná čísla	266
Problém: volání rand	266
Kryptograficky náhodná čísla ve Win32	268
Kryptograficky náhodná čísla v řízeném kódu	273
Kryptograficky náhodná čísla ve webových stránkách	273
Odození kryptografických klíčů z hesel	274
Jak změřit efektivní bitovou velikost hesla	274
Problémy správy klíčů	276
Dlouhodobé a krátkodobé klíče	278
Pro správnou ochranu dat je třeba zvolit odpovídající délku klíčů	278
Klíče uchovávejte blízko zdroje	279
Problémy výměny klíčů	282
Jak si vytvořit vlastní kryptografické funkce	284
Jak používat proudové šifry se stejným šifrovacím klíčem	286
Proč lidé používají proudové šifry	286
Nástrahy proudových šifer	287
Co když musíte používat stejný klíč?	289
Útoky se změnou bitů proti proudovým šifrům	290

Řešení útoků se změnou bitů	291
Kdy použít haš, klíčovaný haš a digitální podpis	292
Opětovné využití bufferu pro prostý a šifrovaný text	297
Potlačování hrozeb s pomocí šifrování	298
Kryptografické mechanismy nezapomeňte dokumentovat	298
Shrnutí	299
Kapitola 9 Jak ochránit tajná data	301
Útok na tajná data	302
Někdy není nutné tajné informace ukládat	303
Vytvoření haše se „soli“	303
Jak zpříjemnit útočníkovi život pomocí PKCS #5	305
Jak načíst tajné informace od uživatele	306
Ochrana tajných informací ve Windows 2000 a novějších	306
Speciální případ: Klientské pověření ve Windows XP	309
Ochrana tajných informací ve Windows NT 4	311
Ochrana tajných informací ve Windows 95, Windows 98, Windows ME a Windows CE	315
Jak zjistit informace o zařízení z PnP	316
Proč nevolit nejmenšího společného jmenovatele	319
Správa tajných informací v paměti	320
Upozornění k optimalizaci kompilátoru	321
Šifrování tajných dat v paměti	324
Ochrana proti stránkování citlivých dat pomocí uzamčení paměti	325
Ochrana tajných dat v řízeném kódu (Managed Code)	326
Správa tajných informací v paměti z řízeného kódu	332
Zvedáme latku bezpečnosti	333
Ukládání dat do souboru v souborovém systému FAT	333
Kódování dat pomocí vloženého klíče a operace XOR	333
Šifrování dat pomocí vloženého klíče a algoritmu 3DES	334
Šifrování dat s algoritmem 3DES a uložení hesla do registru	334
Šifrování dat s algoritmem 3DES a uložení silného klíče do registru	334
Šifrování dat s algoritmem 3DES, uložení silného klíče do registru a ochráníení souboru i registračního klíče přístupovým seznamem	334
Šifrování dat s algoritmem 3DES, uložení silného klíče do registru, vyžádání hesla od uživatele a ochráníení souboru i registračního klíče přístupovým seznamem	334
Kompromisy při ochraně tajných dat	335
Shrnutí	335
Kapitola 10 Veškerý vstup je zlo!	337
Charakteristika problému	338
Důvěra na nepravém místě	339
Strategie obrany proti útokům na vstupu	340

Jak kontrolovat platnost vstupu	342
Zamořené proměnné v Perlu	344
Regulární výrazy v Perlu	345
Dávejte pozor, co najdete – chtěli jste přece ověřovat	347
Regulární výrazy a Unicode	348
Mozaika regulárních výrazů	352
Regulární výrazy v Perlu	352
Regulární výrazy v řízeném kódu	353
Regulární výrazy ve skriptech	354
Regulární výrazy v C++	354
Nejlepší postupy bez regulárních výrazů	355
Shrnutí	355
Kapitola 11 Problémy s kanonickou reprezentací	357
Co znamená kanonická reprezentace a proč je takovým problémem	358
Problémy s kanonickými názvy souborů	358
Obcházení filtrování názvů v Napsteru	358
Zranitelné místo v systému Apple Mac OS X a Apache	359
Zranitelné místo v dosových názvech zařízení	359
Zranitelné místo v symbolickém odkazu na adresář /tmp ze StarOffice pod Sun Microsystems	359
Nejběžnější omyly s kanonickými názvy souborů ve Windows	360
Kanonické problémy ve webovém prostředí	366
Obcházení rodičovských kontrol v AOL	366
Jak obejít bezpečnostní kontroly eEye	366
Zóny sítě Internet a chyba s IP adresou bez teček v Internet Exploreru 4	367
Zranitelné místo s typem ::\$DATA v Internet Information Serveru 4.0	368
Kdy se řádek ve skutečnosti skládá ze dvou?	369
Další webový problém – změnové znaky	370
Útoky s vizuální ekvivalencí a homografický útok	373
Jak zabránit kanonizačním omylům	374
Podle názvu neprovádějte rozhodnutí	375
Vhodným regulárním výrazem omezte povolený obsah názvu	375
Jak zastavit generování názvů 8.3	376
Nedůvěřujte proměnné PATH – používejte plný název cesty	376
Pokus o kanonizaci názvu	377
Bezpečné volání CreateFile	381
Jak napravit webové kanonizační problémy	381
Omezení množiny platného vstupu	381
Pozor při práci s kódováním UTF-8	381
Rozhraní ISAPI – trnitá cesta	382