

Stručný obsah

Kapitola 1

Úvod31

Kapitola 2

Model zabezpečení aplikací typu ASP.NET37

Kapitola 3

Návrh ověřování a autorizace55

Kapitola 4

Zabezpečená komunikace79

Kapitola 5

Zabezpečení intranetu89

Kapitola 6

Zabezpečení v extranetu123

Kapitola 7

Zabezpečení v Internetu137

Kapitola 8

Zabezpečení v prostředí ASP.NET153

Kapitola 9

Zabezpečení služeb modelu Enterprise Services203

Kapitola 10

Zabezpečení webových služeb231

Kapitola 11

Zabezpečení technologie .NET Remoting261

Kapitola 12

Zabezpečení přístupu k datům287

Kapitola 13

Řešení problémů se zabezpečením317

Rejstřík tipů Jak na to333

Jak na to:

Tvorba zvláštního účtu pro spouštění aplikací ASP.NET .335

Jak na to:

Užití formulářového ověřování ve službě Active Directory .341

Jak na to:

Formulářové ověřování a SQL Server 2000351

Jak na to:

Tvorba objektů typu GenericPrincipal pomocí formulářového ověřování .361

Jak na to:

Implementace delegování metodou Kerberos v systému Windows 2000369

Jak na to:

Implementace rozhraní IPrincipal373

Jak na to:

Tvorba knihovny DPAPI381

Jak na to:

Volání funkcí DPAPI (úložiště počítače) z aplikace ASP.NET .389

Jak na to:

Volání funkcí DPAPI (úložiště uživatele) z aplikace ASP.NET pomocí aplikace modelu Enterprise Services (COM+) .395

Jak na to:

Tvorba šifrovací knihovny .407

Jak na to:

Ukládání šifrovaných spojovacích řetězců v registru .417

Jak na to:

Zabezpečení založené na rolích a služby rozlehlé sítě .423

Jak na to:

Volání webové služby z prostředí ASP.NET pomocí klientských certifikátů .429

Jak na to:

Volání webové služby pomocí protokolu SSL .441

Jak na to:

Hostování vzdáleného objektu ve službě systému Windows .447

Jak na to:

Nastavení protokolu SSL na webovém serveru .453

Jak na to:

Nastavení klientských certifikátů .459

Jak na to:

Užití protokolu IPsec k zajištění zabezpečené komunikace mezi dvěma servery .463

Jak na to:

Užití protokolu SSL k zabezpečení komunikace s aplikací SQL Server 2000 .473

Základní konfigurace .481

Konfigurační úložiště a nástroje .483

Centrum odkazů .489

Jak to funguje? .497

Matice identity ASP.NET .505

Kryptografie a certifikáty .507

Zabezpečení webových aplikací .NET .513

Kapitola 12

Zabezpečení přístupu k datům	287
Úvod do zabezpečení přístupu k datům	287
Správci přístupu SQL Server	288
Model důvěryhodného podsystému versus model zosobnění a delegování	289
Ověřování	290
Integrované ověřování systému Windows	290
Ověřování službou SQL Server	296
Ověřování v jiných databázích, než je SQL Server	297
Autorizace	297
Jak používat více databázových rolí	298
Zabezpečená komunikace	299
Možnosti	299
Kterou cestu zvolit?	300
Jak se připojit s nejmenšími oprávněními	300
Databáze důvěřuje aplikaci	300
Databáze důvěřuje různým rolím	301
Databáze důvěřuje spouštějícímu uživateli	301
Tvorba databázového účtu s nejmenšími oprávněními	301
Bezpečné ukládání databázových spojovacích řetězců	303
Možnosti	303
Ukládání spojovacích řetězců pomocí funkcí rozhraní DPAPI	303
Proč ne úložiště LSA?	303
Pracujeme se soubory Web.config a Machine.config	307
Pracujeme se soubory UDL	307
Pracujeme s vlastními textovými soubory	308
Pracujeme s registrem	308
Pracujeme s katalogem COM+	309
Ověřování uživatelů podle databáze	309
Ukládání jednosměrných hešových kódů s přísadou	310
Útoky vloženým kódem SQL (SQL Injection)	310
Auditování	314
Identita procesu služby SQL Server	315
Shrnutí	315

Kapitola 13

Řešení problémů se zabezpečením	317
Jak odstraňovat problémy	317
Jak hledat implementační řešení	318
Řešení problémů s ověřováním	318
Problémy s ověřováním službou IIS	319
Integrované ověřování systémem Windows	320

Formulářové ověřování	320
Řešení problémů s protokolem Kerberos	320
Řešení problémů s autorizací	321
Kontrola seznamů ACL	321
Kontrola identity	321
Zkontrolujte prvek <authorization>	322
ASP.NET	322
Povolte trasování	322
Konfigurační nastavení	322
Jak určit identitu	323
Jak určit identitu ve webové stránce	323
Jak určit identitu ve webové službě	325
Jak určit identitu v objektu COM vytvořeném v jazyce Visual Basic 6	325
Rozhraní .NET Remoting	326
Protokol SSL	326
Protokol IPsec	327
Auditování a protokolování	327
Protokoly zabezpečení systému Windows	327
Auditování v aplikaci SQL Server	328
Protokolování služby IIS	329
Nástroje pro odstraňování problémů	329
Fusion Log Viewer (fuslogvw.exe)	330
ISQL.exe	330
Správce úloh systému Windows	331
Sledování sítě	331
Registry Monitor (regmon.exe)	331
WFetch.exe	332
Nástroje vývojového prostředí Visual Studio .NET	332
WebServiceStudio	332
Sada nástrojů Windows 2000 Resource Kit	332
Rejstřík tipů Jak na to	333
ASP.NET	333
Ověřování a autorizace	333
Kryptografie	333
Zabezpečení služeb rozlehlé sítě	
(Enterprise Services)	333
Zabezpečení webových služeb	333
Zabezpečení vzdálené komunikace	333
Zabezpečená komunikace	334

Jak na to:

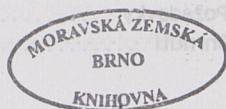
Tvorba zvláštního účtu pro spouštění aplikací ASP.NET	335
Identita pracovního procesu ASP.NET	335
Zosobnění předdefinovaných identit	336
Poznámky	336
Shrnutí	336
1. Tvorba nového místního účtu	336
2. Přiřazení minimálních oprávnění	337
3. Přiřazení oprávnění NTFS	337
4. Konfigurace prostředí ASP.NET pro spouštění pomocí nového účtu	339

Jak na to:

Užití formulářového ověřování ve službě Active Directory	341
Požadavky	341
Shrnutí	341
1. Tvorba webové aplikace s přihlašovací stránkou	342
2. Konfigurace webové aplikace pro formulářové ověřování	343
3. Tvorba ověřovacího kódu LDAP pro vyhledání uživatele v adresářové službě Active Directory	344
4. Tvorba kódu pro zjišťování členství uživatele ve skupinách LDAP	345
5. Ověřování uživatele a tvorba formulářového ověřovacího listku	346
6. Implementace metody pro ošetření požadavků na ověření a pro tvorbu objektu typu GenericPrincipal	347
7. Testování aplikace	349

Jak na to:

Formulářové ověřování a SQL Server 2000	351
Požadavky	351
Shrnutí	352
1. Tvorba webové aplikace s přihlašovací stránkou	352
2. Konfigurace webové aplikace pro formulářové ověřování	353
3. Tvorba funkcí pro generování miniatur s kryptografickými přísadami	353
4. Tvorba databáze uživatelských účtů	354
5. Ukládání podrobností o účtu do databáze pomocí ADO.NET	355
6. Ověření uživatelských pověření na základě databáze	356
7. Testování aplikace	358
Další prameny	359



Jak na to:

Tvorba objektů typu GenericPrincipal pomocí formulářového ověřování	361
Požadavky	362
Shrnutí	362
1. Tvorba webové aplikace s přihlašovací stránkou	362
2. Konfigurace webové aplikace pro formulářové ověřování	363
3. Tvorba ověřovacího lístku pro ověřené uživatele	363
4. Tvorba objektů typu GenericPrincipal a FormsIdentity	365
5. Testování aplikace	366
Další prameny	367

Jak na to:

Implementace delegování metodou Kerberos v systému Windows 2000	369
Poznámky	369
Požadavky	370
Shrnutí	370
1. Nastavení klientského uživatelského účtu pro delegování	370
2. Nastavení účtu serverového procesu jako důvěryhodného pro delegování	370
Další prameny	371

Jak na to:

Implementace rozhraní IPrincipal	373
Požadavky	374
Shrnutí	374
1. Tvorba jednoduché webové aplikace	374
2. Konfigurace webové aplikace pro formulářové ověřování	375
3. Tvorba ověřovacího lístku pro ověřeného uživatele	375
4. Tvorba třídy obsahující rozšířenou implementaci rozhraní IPrincipal	377
5. Tvorba objektu typu CustomPrincipal	378
6. Testování aplikace	379
Další prameny	380

Jak na to:

Tvorba knihovny DPAPI	381
Poznámky	381
Požadavky	382
Shrnutí	382

1. Tvorba knihovny třídy v jazyce C#	382
2. Jak doplnit sestavení o silný název (nepovinné)	387
Další prameny	388

Jak na to:

Volání funkcí DPAPI (úložiště počítače) z aplikace ASP.NET	389
Poznámky	389
Požadavky	390
Shrnutí	390
1. Tvorba klientské webové aplikace ASP.NET	390
2. Testování aplikace	392
3. Úprava webové aplikace, aby načítala šifrované řetězce ze souboru Web.config	392
Další prameny	393

Jak na to:

Volání funkcí DPAPI (úložiště uživatele) z aplikace ASP.NET pomocí aplikace modelu Enterprise Services (COM+)	395
Poznámky	395
Proč je třeba použít službu rozlehlé sítě?	396
Proč je třeba použít službu systému Windows?	397
Požadavky	397
Shrnutí	398
1. Tvorba serverové komponenty nabízející metody Encrypt a Decrypt	398
2. Volání spravované knihovny tříd DPAPI	399
3. Tvorba umělé třídy používané ke spuštění serverové komponenty	399
4. Tvorba účtu systému Windows používaného ke spuštění služby rozlehlé sítě a služby systému Windows	400
5. Konfigurace, tvorba silného názvu a registrace serverové komponenty	400
6. Tvorba služby systému Windows používané ke spuštění serverové komponenty	401
7. Instalace a spuštění služby systému Windows	403
8. Tvorba webové aplikace pro testování kryptografických funkcí	403
9. Úprava webové aplikace pro načítání šifrovaného spojovacího řetězce z konfiguračního souboru	405
Další prameny	406

Jak na to:

Tvorba šifrovací knihovny	407
Požadavky	407

Shrnutí	407
1. Tvorba knihovny tříd v jazyce C#	407
2. Tvorba konzolové testovací aplikace	413
Další prameny	415

Jak na to:

Ukládání šifrovaných spojovacích řetězců v registru	417
Poznámky	417
Požadavky	417
Shrnutí	417
1. Uložení šifrovaných dat v registru	418
2. Tvorba webové aplikace ASP.NET	421
Další prameny	422

Jak na to:

Zabezpečení založené na rolích a služby rozlehlé sítě	423
Poznámky	423
Požadavky	423
Shrnutí	423
1. Tvorba knihovny tříd v jazyce C#, která bude hostitelem nabízené komponenty	424
2. Tvorba nabízené komponenty	424
3. Konfigurace nabízené komponenty	425
4. Tvorba silného názvu pro sestavení	425
5. Kompilace sestavení a jeho přidání do globální mezipaměti sestavení	426
6. Ruční registrace nabízené komponenty	426
7. Kontrola konfigurované aplikace	427
8. Tvorba testovací klientské aplikace	427

Jak na to:

Volání webové služby	
z prostředí ASP.NET pomocí klientských certifikátů	429
Proč je třeba použít serverovou komponentu?	429
K čemu je nutný uživatelský profil?	430
Požadavky	430
Shrnutí	430
1. Tvorba jednoduché webové služby	431
2. Konfigurace virtuálního adresáře webové služby pro ověřování klientských certifikátů	431
3. Tvorba zvláštního účtu pro spuštění nabízené serverové komponenty	432
4. Vyžádání klientského certifikátu pro vlastní účet	432

5. Testování klientského certifikátu pomocí prohlížeče	434
6. Export klientského certifikátu do souboru	435
7. Tvorba serverové komponenty používané k volání webové služby	435
8. Konfigurace a instalace serverové komponenty	438
9. Tvorba webové aplikace, která volá serverovou komponentu	439
Další prameny	440

Jak na to:

Volání webové služby pomocí protokolu SSL	441
Požadavky	441
Shrnutí	441
1. Tvorba jednoduché webové služby	442
2. Konfigurace virtuálního adresáře webové služby pro ověřování klientských certifikátů	442
3. Testování webové služby v prohlížeči	443
4. Instalace certifikátu certifikačního úřadu na klientském počítači	444
5. Tvorba webové aplikace, která bude volat nabízenou komponentu	445
Další prameny	446

Jak na to:

Hostování vzdáleného objektu ve službě systému Windows	447
Poznámky	447
Požadavky	447
Shrnutí	448
1. Tvorba třídy vzdáleného objektu	448
2. Tvorba hostitelské aplikace typu služba systému Windows	448
3. Tvorba účtu systému Windows pro spouštění služby	450
4. Instalace služby systému Windows	451
5. Tvorba testovací klientské aplikace	451
Další prameny	452

Jak na to:

Nastavení protokolu SSL na webovém serveru	453
Požadavky	453
Shrnutí	453
1. Tvorba žádosti o certifikát	453
2. Vyžádání certifikátů pomocí webových stránek Certifikační služby systému Windows	455
3. Vydání certifikátu	456
4. Instalace certifikátu na webovém serveru	456
5. Konfigurace přístupu k prostředkům přes protokol SSL	457

Jak na to:

Nastavení klientských certifikátů	459
Požadavky	459
Shrnutí	459
1. Tvorba jednoduché webové aplikace	460
2. Konfigurace webové aplikace pro ověřování klientských certifikátů	460
3. Žádost o certifikát a instalace klientského certifikátu	461
4. Ověření funkce klientského certifikátu	462
Další prameny	462

Jak na to:

Užití protokolu IPsec k zajištění zabezpečené komunikace mezi dvěma servery	463
Poznámky	464
Požadavky	465
Shrnutí	465
1. Tvorba filtru adres IP	465
2. Tvorba akcí filtru	466
3. Tvorba pravidel zabezpečení	467
4. Export zásady protokolu IPsec na vzdálený počítač	469
5. Přidělení zásad	469
6. Ověření funkce vytvořeného řešení	469
Další prameny	472

Jak na to:

Užití protokolu SSL k zabezpečení komunikace s aplikací SQL Server 2000	473
Poznámky	473
Požadavky	473
Shrnutí	474
1. Instalace certifikátu pro ověření serveru	474
2. Ověření instalace certifikátu	475
3. Instalace certifikátu certifikačního úřadu na klientském počítači	476
4. Jak vynutit užití protokolu SSL všemi klienty	476
5. Jak nechat rozhodnutí o užití protokolu SSL na klientovi	477
6. Kontrola, zda je komunikace šifrována	478
Další prameny	480

Základní konfigurace	481
-----------------------------	------------

Konfigurační úložiště a nástroje	483
---	------------

Centrum odkazů	489
Hledání ve znalostní bázi	489
Tipy	490
Zabezpečení platformy .NET Framework	490
Centra	490
Služba Active Directory	490
Centra	490
Klíčové poznámky	491
Články	491
ADO.NET	491
Podrobné a stručné popisy	491
Semináře a přímé přenosy (WebCasts) po Internetu	491
ASP.NET	491
Centra	491
Podrobné a stručné popisy	492
Znalostní báze	492
Články	492
Články HOWTO:	492
Semináře a přímé přenosy (WebCasts) po Internetu	493
Služby rozlehlé sítě (Enterprise Services)	493
Znalostní báze	493
Podrobné návody a stručné souhrny	493
Články HOWTO	493
Časté otázky	494
Semináře a přímé přenosy (WebCasts) po Internetu	494
Služba IIS (Internetová informační služba)	494
Centra	494
.NET Remoting	494
Podrobné návody a stručné souhrny	494
Články HOWTO:	494
Semináře a přímé přenosy (WebCasts) po Internetu	494
SQL Server	495
Centra	495
Semináře a přímé přenosy (WebCasts) po Internetu	495
Visual Studio .NET	495
Centra	495
Podrobné návody a stručné souhrny	495
Webové služby	495
Centra	495
Podrobné návody a stručné souhrny	495
Články HOWTO	496
Semináře a přímé přenosy (WebCasts) po Internetu	496
Windows 2000	496
Centra	496

Jak to funguje?	497
Zpracování v prostředí ASP.NET a ve službě IIS	497
Izolace aplikací	498
Rozšíření ISAPI ASP.NET	498
Služba IIS 6.0 a systém Windows Server 2003	498
Zřetěžené zpracování v prostředí ASP.NET	499
Anatomie webového požadavku	500
Ošetření událostí	503
Implementace vlastního modulu HTTP	504
Implementace vlastního obslužného objektu HTTP	504
Matice identity ASP.NET	505
Kryptografie a certifikáty	507
Klíče a certifikáty	507
Digitální certifikáty ve formátu X.509	508
Úložiště certifikátů	508
Kryptografie	509
Pro jakou techniku se rozhodnout	509
Kryptografie v prostředí .NET Framework	510
Shrnutí	512
Zabezpečení webových aplikací .NET	513
Glosář	515
Rejstřík	531

Obsah

Poděkování	25
Předmluva	27
Kapitola 1	
Úvod	31
Když je vše propojeno	31
Základy	32
Ověřování	32
Autorizace	32
Zabezpečená komunikace	32
Propojení technologií	33
Principy návrhu	34
Shrnutí	35
Kapitola 2	
Model zabezpečení aplikací typu ASP.NET	37
Webové aplikace založené na technologii .NET	37
Logické vrstvy	37
Modely fyzického zavádění	38
Implementační technologie	39
Architektura zabezpečení	40
Zabezpečení napříč vrstvami	40
Ověřování	42
Autorizace	45
Správci přístupu a brány	46
Úvod do zabezpečení platformy .NET Framework	49
Zabezpečení přístupu ke kódu	49
Ověření klientů a identity	50
Třídy WindowsPrincipal a WindowsIdentity	51
Třída GenericPrincipal a přidružené objekty identity	52
Prostředí ASP.NET a vlastnost HttpContext.User	52
Vzdálená komunikace metodou .NET Remoting a webové služby	53
Shrnutí	53
Kapitola 3	
Návrh ověřování a autorizace	55
Návrh strategie ověřování a autorizace	56
Určování prostředků	56
Volba autorizační strategie	56

Volba identit pro přístup k prostředkům	57
Úvahy o předávání identit	58
Volba způsobu ověřování	58
Jak rozhodnout o způsobu předávání identit	58
Způsoby autorizace	59
Autorizace založená na rolích	59
Autorizace orientovaná na prostředky	60
Schémata přístupu k prostředkům	60
Model důvěryhodného podsystému	61
Model zosobnění a delegování	62
Volba modelu pro kontrolu přístupu	63
Předávání identit	65
Přenos identit na úrovni aplikace versus přenos identit na úrovni operačního systému	65
Zosobnění a delegování	65
Autorizace založená na rolích	67
Role modelu .NET	67
Role modelu Enterprise Services (COM+)	68
Uživatelsky definované databázové role v aplikaci SQL Server	68
Aplikační role služby SQL Server	68
Role modelu .NET versus role modelu COM+	69
Práce s rolemi modelu .NET	69
Volba mechanismu ověřování	73
Internetové scénáře	74
Intranetové a extranetové scénáře	75
Porovnání metod ověřování	76
Shrnutí	76

Kapitola 4

Zabezpečená komunikace	79
Je třeba vědět, co zabezpečovat	79
Protokoly SSL/TLS	80
Jak používat protokol SSL	80
Protokol IPSec	81
Jak používat protokol IPSec	82
Šifrování RPC	82
Jak používat šifrování RPC	83
Dvoubodové zabezpečení	83
Komunikace mezi prohlížečem a webovým serverem	83
Komunikace mezi webovým a vzdáleným aplikačním serverem	84
Komunikace mezi aplikačním a databázovým serverem	84
Volba mezi protokoly IPSec a SSL	86
Farmy a vyrovnávání zátěže (Load Balancing)	86
Shrnutí	86

Kapitola 5

Zabezpečení intranetu

89

Komunikace mezi prostředím ASP.NET a aplikací SQL Server	90
Základní charakteristika	90
Jak zabezpečit tento scénář	90
Výsledek	91
Jak postupovat při konfiguraci zabezpečení	92
Analýza	93
Otázky a odpovědi	94
Související scénáře	95

Komunikace mezi prostředím ASP.NET, službami rozlehlé sítě (Enterprise Services) a aplikací SQL Server

97

Charakteristika	97
Jak zabezpečit tento scénář	97
Výsledek	98
Jak postupovat při konfiguraci zabezpečení	99
Analýza	100
Skryté nástrahy	101

Komunikace mezi prostředím ASP.NET, webovými službami a aplikací SQL Server

101

Základní charakteristika	102
Jak tento scénář zabezpečit	102
Výsledek	103
Jak postupovat při konfiguraci zabezpečení	104
Analýza	106
Skryté nástrahy	107
Otázky a odpovědi	108

Komunikace mezi prostředím ASP.NET, službami vzdálené komunikace a aplikací SQL Server

108

Základní charakteristika	108
Jak tento scénář zabezpečit	109
Výsledek	109
Jak postupovat při konfiguraci zabezpečení	109
Analýza	112
Skryté nástrahy	113

Předávání spouštějícího uživatele do databáze

114

ASP.NET/SQL Server	114
ASP.NET/slужby rozlehlé sítě (Enterprise Services)/SQL Server	115
Výsledek	116
Analýza	120
Skryté nástrahy	121

Shrnutí

121

Kapitola 6

Zabezpečení v extranetu

Nabízení webové služby	123
Základní charakteristika	124
Zabezpečení scénáře	124
Výsledek	125
Postup při zabezpečování scénáře	125
Analýza	128
Skryté nástrahy	129
Dotazy a odpovědi	129
Nabízení webové aplikace	129
Základní charakteristika	130
Zabezpečení scénáře	130
Výsledek	131
Analýza	133
Skryté nástrahy	134
Shrnutí	135

Kapitola 7

Zabezpečení v Internetu

ASP.NET/SQL Server	138
Základní charakteristika	138
Zabezpečení scénáře	138
Výsledek	139
Jak postupovat při zabezpečování	140
Analýza	141
Skryté nástrahy	143
Související scénáře	143
ASP.NET/Vzdálené služby modelu Enterprise Services/SQL Server	144
Základní charakteristika	145
Zabezpečení scénáře	145
Výsledek	146
Jak postupovat při zabezpečování	146
Analýza	150
Skryté nástrahy	151
Související scénáře	151
Shrnutí	152

Kapitola 8

Zabezpečení v prostředí ASP.NET

Architektura zabezpečení ASP.NET	153
Správci přístupu	155
Strategie ověřování a autorizace	157

Dostupné možnosti ověřování	157
Integrované ověřování systému Windows se zosobněním	158
Integrované ověřování systému Windows bez zosobnění	160
Integrované ověřování systému Windows s pevnou identitou	161
Ověřování pomocí formulářů	162
Ověřování službou Passport	163
Konfigurace zabezpečení	164
Konfigurace nastavení služby IIS	165
Konfigurace nastavení ASP.NET	165
Zabezpečení prostředků	168
Zabezpečená komunikace	170
Jak programovat zabezpečení	171
Vzor autorizace	171
Tvorbá vlastní implementace rozhraní IPrincipal	173
Integrované ověřování systému Windows	174
Formulářové ověřování	175
Jak vyvíjet ověřování pomocí formulářů	176
Rady týkající se implementace formulářů	179
Hostování více aplikací používajících formulářové ověřování	180
Formulářové ověřování bez souborů cookie	180
Ověřování službou Passport	180
Vlastní způsoby ověřování	181
Identita procesu ASP.NET	182
Užití nejméně privilegovaného účtu	182
Nespouštějte proces ASP.NET pomocí systémového účtu	182
Práce s implicitním účtem ASP.NET	183
Zosobňování	185
Zosobňování a místní prostředky	185
Zosobňování a vzdálené prostředky	185
Zosobňování a vlákna	186
Přístup k systémovým prostředkům	186
Přístup k protokolu událostí	186
Přístup k registru	187
Práce s objekty modelu COM	187
Objekty modelu Apartment	187
Přístup k síťovým prostředkům	189
Užití identity procesu ASP.NET	189
Práce se serverovými komponentami	190
Práce s účtem anonymního internetového uživatele	191
Práce s funkcí LogonUser a zosobnění vybrané identity systému Windows	192
Užití identity spouštějícího uživatele	193
Přístup k souborům ve sdílených položkách UNC	194
Přístup k síťovým prostředkům jiných platforem než systému Windows	194

Zabezpečená komunikace	194
Ukládání tajných informací	195
Možnosti ukládání tajných informací v aplikaci ASP.NET	196
Ukládání tajných dat na samostatných logických jednotkách	196
Zabezpečení stavu relace a objektu ViewState	197
Zabezpečení objektu ViewState	197
Zabezpečení souborů cookie	197
Zabezpečení stavu relace uloženého v databázi SQL	197
Úvahy o webové farmě	199
Sledování stavu relace	199
Rozhraní DPAPI	200
Formulářové ověřování na webové farmě	200
Prvek <machineKey>	200
Shrnutí	202

Kapitola 9

Zabezpečení služeb modelu Enterprise Services	203
Architektura zabezpečení	203
Správci přístupu a brány	204
Pro lepší zabezpečení používejte serverové aplikace	206
Zabezpečení serverových a knihovnic aplikací	206
Požadavky na zabezpečení přístupu ke kódu	206
Konfigurace zabezpečení	207
Konfigurace serverové aplikace	207
Konfigurace klientské webové aplikace ASP.NET	213
Konfigurace úrovně zosobnění u aplikace modelu Enterprise Services	214
Programování zabezpečení	214
Programové zabezpečení založené na rolích	214
Identifikace volajících	215
Volba identity procesu	215
Ke spouštění aplikace nepoužívejte identitu interaktivního uživatele	216
Používejte vlastní účet s nejmenšími oprávněními	216
Přístup k síťovým prostředkům	216
Používání identity spouštějícího uživatele	217
Používání identity aktuálního procesu	217
Používání účtu specifické služby	218
Zosobnění spouštějícího uživatele	218
Volání metody ColmpersonateClient	219
Šifrování RPC	220
Tvorba nabízených komponent	220
Problémy se zamykáním knihoven DLL	220
Správa verzí	220
Výjimky typu QueryInterface	221

Model DCOM a bezpečnostní brány	222
Volání nabízených komponent z aplikace ASP.NET	222
Identita volajícího	222
Používání integrovaného ověřování systému Windows a zosobnění ve webové aplikaci	222
Konfigurace ověřování a zosobnění v souboru Machine.config	223
Konfigurace objektů proxy rozhraní	223
Zabezpečení – základní pojmy	225
Role služeb rozlehle sítě a role modelu .NET	226
Ověřování	227
Zosobnění	228
Shrnutí	230

Kapitola 10

Zabezpečení webových služeb	231
Model zabezpečení webové služby	231
Zabezpečení na úrovni platformy (transportu)	231
Zabezpečení na úrovni aplikace	232
Zabezpečení na úrovni zprávy	233
Architektura zabezpečení na úrovni platformy (transportu)	234
Správci přístupu	236
Strategie ověřování a autorizace	236
Integrované ověřování systému Windows se zosobněním	237
Integrované ověřování systému Windows bez zosobnění	239
Integrované ověřování systému Windows a předdefinovaná identita	240
Konfigurace zabezpečení	241
Konfigurace nastavení služby IIS	241
Konfigurace prostředí ASP.NET	242
Zabezpečené prostředky	242
Zakažte protokoly HTTP-GET a HTTP-POST	242
Zabezpečte komunikaci	243
Jak se předávají pověření pro ověření webovou službou	243
Jak určit klientská pověření pro integrované ověřování systému Windows	244
Jak volat webové služby z jiných platform než Windows	246
Ověřování pomocí serveru proxy	246
Předávání identity spouštějícího uživatele	246
Implicitní pověření a delegování protokolem Kerberos	247
Explicitní pověření a základní nebo formulářové ověřování	249
Důvěryhodný podsystém	251
Předávání identity volajícího	252
Jak postupovat při konfiguraci	252
Přístup k systémovým prostředkům	254
Přístup k síťovým prostředkům	254

Práce s objekty modelu COM	254
Klientské certifikáty a webové služby	255
Ověřování certifikátů u klientů typu prohlížeč	255
Práce s modelem důvěryhodného podsystému	255
Zabezpečená komunikace	258
Možnosti zabezpečení na úrovni transportu	258
Možnosti zabezpečení na úrovni zprávy	258
Shrnutí	259

Kapitola 11

Zabezpečení technologie .NET Remoting	261
Architektura technologie .NET Remoting	261
Příjemci ve vzdálené komunikaci	262
Anatomie požadavku na vzdálený objekt umístěný v prostředí ASP.NET	263
ASP.NET a kanál HTTP	264
Správci přístupu v rozhraní .NET Remoting	265
Ověřování	266
Hostitelem je aplikace ASP.NET	266
Hostitelem je webová služba	267
Autorizace	267
Užití autorizace souborů	268
Strategie ověřování a autorizace	269
Přístup k systémovým prostředkům	270
Přístup k síťovým prostředkům	270
Jak předávat pověření pro ověřování ve vzdálených objektech	270
Jak specifikovat pověření klienta	271
Předávání spouštějícího uživatele	273
Implicitní pověření a delegování metodou Kerberos	274
Explicitní pověření a základní nebo formulářové ověřování	275
Důvěryhodný podsystém	278
Předávání identity volajícího	279
Volba hostitele	279
Jak postupovat při konfiguraci	280
Zabezpečená komunikace	281
Možnosti zabezpečení na úrovni platformy	281
Možnosti zabezpečení na úrovni zprávy	282
Volba hostitelského procesu	282
Doporučení	282
Hostitelem je prostředí ASP.NET	282
Hostitelem je služba systému Windows	283
Hostitelem je konzolová aplikace	284
Vzdálená komunikace versus webové služby	285
Shrnutí	286