

# STRUČNÝ OBSAH

## ČÁST 1 ÚVOD DO ARCHITEKTURY A TECHNOLOGIE J2EE

- ▼ 1. Základy technologie Java: Zabezpečení od podlahy ..... 3
- ▼ 2. Bezpečnostní balíčky JAAS, JCE a JSSE: Úvod ..... 21
- ▼ 3. Architektura J2EE a její zabezpečení ..... 57

## ČÁST 2 ZABEZPEČENÍ SÍTĚ A APLIKACÍ V JAZYCE JAVA

- ▼ 4. Ochrana aplikací šifrováním a ověřováním ..... 95
- ▼ 5. Softwarové pirátství a schémata udělování licencí pro komerční využití kódu ..... 129
- ▼ 6. Zpětný překlad bajtových kódů ..... 151
- ▼ 7. Hacking aplikací typu klient/server: další vrstva v ohrožení! ..... 175
- ▼ 8. Síťové aplikace v jazyce Java: Útoky na slabá místa ..... 229

## ČÁST 3 ZABEZPEČENÍ ARCHITEKTURY J2EE V SÍTI WWW A V APLIKAČNÍ VRSTVĚ

- ▼ 9. Napadení komponent jazyka Java ve webové vrstvě ..... 273
  - ▼ 10. Otřes v samotných základech: Síla a slabiny webového kontejneru ..... 313
  - ▼ 11. Zabezpečení webových služeb v jazyce Java ..... 339
  - ▼ 12. Enterprise JavaBeans: Zabezpečení aplikační vrstvy ..... 373
- Rejstřík ..... 403

# OBSAH

Poděkování .....	xv
Úvod .....	xvii

## ČÁST 1

### ÚVOD DO ARCHITEKTURY A TECHNOLOGIE J2EE

▼ 1. Základy technologie Java: Zabezpečení od podlahy .....	3
Java tehdy a nyní .....	4
Architektura jazyka Java .....	5
Virtuální stroj jazyka Java (JVM) .....	5
Interpretovaný jazyk: Bajtové kódy jazyka Java .....	6
Zavaděč tříd jazyka Java a vestavěné zabezpečení .....	6
Další vlastnosti jazyka .....	7
Architektura zabezpečení jazyka Java .....	7
Ochranné domény .....	8
Prvky řídicí zabezpečení procesu zavádění tříd jazyka Java .....	10
Oprávnění v jazyce Java .....	12
Zásady zabezpečení jazyka Java .....	13
Soubor vlastností zabezpečení jazyka Java .....	14
Soubor zásad zabezpečení jazyka Java .....	15
Jak ověřit správce zabezpečení .....	18
Názvy pro rozhraní Principal a subjekty .....	19
Shrnutí .....	20

<b>▼ 2. Bezpečnostní balíčky JAAS, JCE a JSSE: Úvod .....</b>	<b>21</b>
Služby ověřování a autorizace JAAS .....	22
Architektura balíčku JAAS .....	23
Ověřování JAAS .....	24
Autorizace JAAS .....	36
Šifrování v jazyce Java .....	39
Základy šifrování .....	39
Balíček JCE (Java Cryptography Extension) .....	42
Nástroj keytool .....	44
Balíček JSSE (Java Secure Sockets Extension) .....	46
Instalace knihovny a certifikátu .....	47
Zabezpečení archivů JAR .....	54
Nástroj jarsigner .....	54
Direktiva Sealed .....	54
Shrnutí .....	55
<b>▼ 3. Architektura J2EE a její zabezpečení .....</b>	<b>57</b>
Střední vrstva a distribuované softwarové komponenty .....	58
Vývoj vrstvy aplikačního serveru .....	58
Vývoj vícevrstvé aplikace .....	60
Vícevrstvé prostředí .....	61
Vícevrstvé technologie J2EE .....	61
Komponenty webové vrstvy: servery a stránky JSP .....	63
Servery .....	63
JSP .....	66
Práce s technologií JSP .....	68
Komponenty aplikační vrstvy: komponenty EJB .....	69
Služby nabízené kontejnerem EJB .....	69
Typy komponent EJB .....	70
Nasazení komponenty EJB .....	73
Vývoj EJB .....	76
Další rozhraní API sady J2EE .....	82
Architektura zabezpečení EJB .....	83
Názvy pro rozhraní Principal a role .....	84
Deklarativní a programové zabezpečení .....	84
Zabezpečení na úrovni systému .....	85
Zabezpečení v prezentační vrstvě .....	86
Zabezpečení v aplikační vrstvě .....	88
Shrnutí .....	91



## ČÁST 2

## ZABEZPEČENÍ SÍTĚ A APLIKČÍ V JAZYCE JAVA

▼ 4. Ochrana aplikací šifrováním a ověřováním .....	95
Zabezpečení aplikace: Proces .....	96
Zabezpečení systému versus zabezpečení aplikací .....	96
Techniky zabezpečení aplikace .....	97
Jaká nebezpečí číhají na lokálně uložená data? .....	98
Shrnutí .....	127
▼ 5. Softwarové pirátství a schémata udělování licencí pro komerční využití kódu .....	129
Nebezpečí zneužití kódu .....	130
Implementace třídy SimpleSymmetricLicense .....	135
Další strategie správy licencí .....	140
Shrnutí .....	149
▼ 6. Zpětný překlad bajtových kódů .....	151
Nebezpečí zpětné analýzy .....	152
Nebezpečí vnořených řetězců .....	172
Shrnutí .....	174
▼ 7. Hacking aplikací typu klient/server: další vrstva v ohrožení! .....	175
Implementace aplikace typu klient/server .....	176
Rizika architektury typu klient/server .....	177
Pohled do košíku: Zabezpečení databáze .....	178
Zabezpečení databázového připojení .....	181
Ochrana klientské vrstvy .....	194
Ochrana klientských aplikací typu applet .....	207
Ochrana klientů služby Java WebStart .....	221
Shrnutí .....	226
▼ 8. Síťové aplikace v jazyce Java: Útoky na slabá místa .....	229
Nebezpečí ze strany rozhraní RMI .....	230
Původní verze aplikace modelu RMI .....	230
Šifrování čísel účtů a hodnot zůstatků .....	240
Spojení SSL mezi klientem a serverem .....	247
Ověřování výzvou a odezvou .....	251
Práce s kanálem pro ověřenou komunikaci .....	255
Nebezpečí zavádění tříd a archivů JAR ze vzdálených počítačů .....	268
Shrnutí .....	270

## ČÁST 3

## ZABEZPEČENÍ ARCHITEKTURY J2EE V SÍTI WWW A V APLIKAČNÍ VRSTVĚ

▼ 9. Napadení komponent jazyka Java ve webové vrstvě .....	273
Ukázková aplikace: Na bázi webu .....	275
Implementace strategie řízení klientské mezipaměti .....	307
Shrnutí .....	311
▼ 10. Otřes v samotných základech: Síla a slabiny webového kontejneru .....	313
Důsledky povolení procházení adresářů .....	315
Servlet invoker .....	316
Aktivace protokolu HTTPS v kontejneru Tomcat .....	325
Testování instalace .....	325
Rozšíření o záruku přenosu .....	326
Ověřování klientskými certifikáty .....	327
Konfigurace kontejneru Tomcat pro užívání protokolu SSL a ověřování klientskými certifikáty .....	329
Ověřování kontejneru pomocí klientského certifikátu .....	330
Jak se vypořádat s překrýváním rolí v aplikacích .....	334
Shrnutí .....	336
▼ 11. Zabezpečení webových služeb v jazyce Java .....	339
Webové služby v jazyce Java .....	340
Technologie webových služeb .....	341
Sada WSDP .....	342
Jak implementovat aplikaci založenou na webových službách .....	343
Sada penzijních webových služeb: Serverová část .....	344
Sada webových služeb penzijní aplikace: Klientská část .....	347
Slabá místa aplikace založené na architektuře webových služeb .....	352
Implementace ověřování HTTP .....	358
Zákaz šíření dokumentů WSDL .....	360
Jak povolit programové ověřování .....	361
Hesla do databáze předávaná jako kontextové parametry .....	364
Jak zabezpečit tok činností webové služby .....	366
Budoucnost zabezpečení webových služeb .....	369
Bezpečnostní rozšíření SOAP: Digitální podpis .....	370
Technologie WS-Security .....	370
Shrnutí .....	371

▼ 12. Enterprise JavaBeans: Zabezpečení aplikační vrstvy .....	373
Implementace aplikace založené na modelu EJB .....	374
Služba persistence EJB .....	375
Metody pro zobrazení a změnu zůstatků .....	376
Objekty EJB .....	377
Slabá místa aplikace modelu EJB .....	381
Častá úskalí užití zprávami řízených objektů EJB .....	391
Implementace objektu JavaBeans řízeného zprávami .....	391
Shrnutí .....	400
Rejstřík .....	403