

# 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**

---

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

**Část IV****Speciální témata**

---

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

**Část V****Přílohy**

---

<b>Příloha A</b>	<b>Nebezpečná volání API .....</b>	<b>657</b>
<b>Příloha B</b>	<b>Nejhloupejší výmluvy, které můžeme slyšet. ....</b>	<b>669</b>
<b>Příloha C</b>	<b>Seznam bezpečnostních kontrol pro návrháře .....</b>	<b>677</b>
<b>Příloha D</b>	<b>Seznam bezpečnostních kontrol pro vývojáře .....</b>	<b>679</b>
<b>Příloha E</b>	<b>Seznam bezpečnostních kontrol pro testera .....</b>	<b>685</b>

---

## 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	Síťové 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



# Obsah

## Bezpečný kód

### Úvod

29

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

### Část I

#### Bezpečnost v současném světě

<b>Kapitola 1</b>	<b>Proč je potřeba zabezpečovat systémy .....</b>	<b>37</b>
	Aplikace v prostředí „Wild Wild Webu“ .....	39
	Proč jsou potřeba důvěryhodné počítačové technologie .....	41
	Všechny hlavy dohromady .....	41
	Jak organizaci prodávát bezpečnost s cítem .....	41
	Podvratné metody .....	45
	<b>Několik námětů k prosazování kultury bezpečnosti .....</b>	<b>46</b>
	Přimějte šéfa k zosazení e-mailové zprávy .....	46
	Jmenujte bezpečnostního kazatele .....	47
	<b>Výhoda útočníků a dilema obránců .....</b>	<b>51</b>
	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 zkoušet 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 necítí .....	52
	<b>Shrnutí .....</b>	<b>52</b>
<b>Kapitola 2</b>	<b>Proaktivní procesy vývoje s bezpečností .....</b>	<b>55</b>
	Zlepšování procesů .....	57
	<b>Význam vzdělávání .....</b>	<b>58</b>
	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
<b>Fáze návrhu .....</b>	<b>63</b>
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
<b>Fáze vývoje.....</b>	<b>72</b>
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
<b>Fáze testování .....</b>	<b>75</b>
<b>Fáze dodávky produktu a údržby .....</b>	<b>75</b>
Jak zjistíte, že jste hotovi .....	75
Proces reakce na problémy .....	76
Odpovědnost .....	76
<b>Shrnutí .....</b>	<b>76</b>
<b>Kapitola 3   Bezpečnostní principy pro život.....</b>	<b>79</b>
<b>SD<sup>3</sup>, bezpečnost na třetí: zabezpečení při vývoji, výchozím nastavení a instalaci .....</b>	<b>79</b>
Secure by Design – Zabezpečení při vývoji .....	80
Secure by Default – Zabezpečení při výchozím nastavení .....	81
Secure by Deployment – Zabezpečení při instalaci .....	81
<b>Základní bezpečnostní principy.....</b>	<b>82</b>
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
	<b>Shrnutí .....</b>	<b>95</b>
<b>Kapitola 4</b>	<b>Modelování hrozeb .....</b>	<b>97</b>
	<b>Bezpečný návrh a modelování hrozeb .....</b>	<b>98</b>
	Sestavte tým pro modelování hrozeb .....	100
	Dekomponujte aplikaci .....	100
	Určete hrozby, kterým je systém vystaven .....	109
	Ohodnoťte hrozby snížením rizik .....	117
	Vyberte způsob reakce na hrozby .....	130
	Vyberte techniky pro potlačení hrozeb .....	131
	<b>Bezpečnostní techniky .....</b>	<b>132</b>
	Autentizace .....	132
	Autorizace .....	137
	Technologie s odolností proti pozmenění a s posílením soukromí .....	138
	Tajné informace chraňte, 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
	<b>Jak potlačit hrozby v ukázkové mzdové aplikaci .....</b>	<b>141</b>
	<b>Sbírka hrozeb a jejich řešení .....</b>	<b>142</b>
	<b>Shrnutí .....</b>	<b>146</b>

## Část II

### Techniky bezpečného kódování

<b>Kapitola 5</b>	<b>Veřejný nepřítel číslo 1: přetečení bufferu .....</b>	<b>149</b>
	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
	<b>Jak zabránit přetečení bufferu .....</b>	<b>172</b>
	Bezpečné zpracování řetězců .....	173
	Upozornění k funkcím pro zpracování řetězců .....	182
	<b>Volba kompilátoru Visual C++ .NET /GS .....</b>	<b>183</b>
	<b>Shrnutí .....</b>	<b>185</b>

<b>Kapitola 6</b>	<b>Jak stanovit správné řízení přístupu</b>	<b>187</b>
	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
	<b>Vytvoření přístupového seznamu</b>	<b>196</b>
	Vytvoření přístupového seznamu ve Windows NT 4	196
	Vytvoření přístupového seznamu ve Windows 2000	199
	Vytvoření přístupového seznamu v Active Template Library	203
	<b>Jak definovat správné pořadí položek řízení přístupu</b>	<b>204</b>
	<b>Nezapomeňte na SID terminálového serveru a vzdálené plochy</b>	<b>206</b>
	<b>Prázdné volitelné seznamy řízení přístupu a další nebezpečné typy položek</b>	<b>207</b>
	Prázdné volitelné seznamy řízení přístupu a audit	209
	Nebezpečné typy položek řízení přístupu	210
	Co když prázdný DACL nemohu změnit	211
	<b>Ostatní mechanismy řízení přístupu</b>	<b>211</b>
	Role v .NET Framework	212
	Role v COM+	213
	Omezení provozu IP	214
	Spouštěč a oprávnění SQL Serveru	215
	Příklad ze zdravotnictví	215
	Důležitá poznámka k mechanismům řízení přístupu	216
	<b>Shrnutí</b>	<b>217</b>
<b>Kapitola 7</b>	<b>Spouštěč vždy s nejmenšími oprávněními</b>	<b>219</b>
	<b>Nejmenší možné oprávnění v reálném světě</b>	<b>220</b>
	Viry a trojské koně	220
	Pozměnění webového serveru	221
	<b>Stručný přehled řízení přístupu</b>	<b>222</b>
	<b>Stručný přehled oprávnění</b>	<b>222</b>
	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
	<b>Stručný přehled tokenů</b>	<b>228</b>
	<b>Jak spolu souvisejí tokeny, oprávnění, SID, ACL a procesy</b>	<b>229</b>
	SID a kontrola přístupu, oprávnění a kontrola oprávnění	230



<b>Tři důvody, pro které aplikace vyžadují zvýšená oprávnění</b> .....	<b>230</b>
Problémy s přístupovými seznamy .....	230
Problémy s oprávněními .....	231
Tajné informace LSA .....	232
<b>Jak vyřešit problémy se zvýšenými oprávněními</b> .....	<b>232</b>
Jak vyřešit problémy s ACL .....	232
Jak vyřešit problémy s oprávněními .....	233
Jak vyřešit problémy s LSA .....	233
<b>Postup při stanovení odpovídajících oprávnění</b> .....	<b>233</b>
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
<b>Účty služeb s nejnižším oprávněním ve Windows XP a Windows .NET Server 2003</b> .....	<b>253</b>
<b>Oprávnění k zosobnění a Windows .NET Server 2003</b> .....	<b>255</b>
<b>Ladění problémů s nejmenšími oprávněními</b> .....	<b>256</b>
Proč aplikace pod normálním uživatelem havarují .....	257
Jak zjistit příčinu havárií aplikace .....	257
<b>Shrnutí</b> .....	<b>263</b>
<b>Kapitola 8 Slabiny v kryptografii</b> .....	<b>265</b>
<b>Nevhodná náhodná čísla</b> .....	<b>266</b>
Problém: volání rand .....	266
Kryptograficky náhodná čísla ve Win32 .....	268
Kryptograficky náhodná čísla v řízeném kódu .....	273
Kryptograficky náhodná čísla ve webových stránkách .....	273
<b>Odvození kryptografických klíčů z hesel</b> .....	<b>274</b>
Jak změřit efektivní bitovou velikost hesla .....	274
<b>Problémy správy klíčů</b> .....	<b>276</b>
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
<b>Jak si vytvořit vlastní kryptografické funkce</b> .....	<b>284</b>
<b>Jak používat proudové šifry se stejným šifrovacím klíčem</b> .....	<b>286</b>
Proč lidé používají proudové šifry .....	286
Nástrahy proudových šifer .....	287
Co když musíte používat stejný klíč? .....	289
<b>Útoky se změnou bitů proti proudovým šifrům</b> .....	<b>290</b>

Řešení útoků se změnou bitů.....	291
Kdy použít haš, klíčovaný haš a digitální podpis.....	292
<b>Opětné využití bufferu pro prostý a šifrovaný text .....</b>	<b>297</b>
<b>Potlačování hrozeb s pomocí šifrování.....</b>	<b>298</b>
<b>Kryptografické mechanismy nezapomeňte dokumentovat .....</b>	<b>298</b>
<b>Shrnutí .....</b>	<b>299</b>
<b>Kapitola 9    Jak ochránit tajná data .....</b>	<b>301</b>
Útok na tajná data .....	302
Někdy není nutné tajné informace ukládat.....	303
Vytvoření haše se „solí“.....	303
Jak znepříjemnit 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 ochránění souboru i registračního klíče přístupovým seznamem.....	334
Šifrování dat s algoritmem 3DES, uložení silného klíče do registru, vyžádání hesla od uživatele a ochránění souboru i registračního klíče přístupovým seznamem .....	334
Kompromisy při ochraně tajných dat .....	335
Shrnutí .....	335
<b>Kapitola 10    Veškerý vstup je zlo! .....</b>	<b>337</b>
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
Kontrola vstupu s regulárními výrazy .....	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
<b>Kapitola 11 Problémy s kanonickou reprezentací .....</b>	<b>357</b>
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 – použijte 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

	Jedna myšlenka na závěr: kanonizační problémy jiného než souborového charakteru . . . . .	383
	Názvy serverů . . . . .	383
	Uživatelská jména . . . . .	384
	Shrnutí . . . . .	386
<b>Kapitola 12</b>	<b>Problémy se vstupem v databázích . . . . .</b>	<b>387</b>
	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
	Hlubková obrana v hloubkovém příkladu . . . . .	395
	Shrnutí . . . . .	399
<b>Kapitola 13</b>	<b>Zvláštní problémy se vstupem ve webovém prostředí . . . . .</b>	<b>401</b>
	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 předvídatelné cookies . . . . .	421
	Problémy klientů SSL/TLS . . . . .	422
	Shrnutí . . . . .	423

<b>Kapitola 14</b>	<b>Problémy s mezinárodním prostředím</b>	<b>425</b>
	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

<b>Kapitola 15</b>	<b>Bezpečnost soketů</b>	<b>439</b>
	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
<b>Kapitola 16</b>	<b>Zabezpečení RPC, ovládacích prvků ActiveX a modelu DCOM</b>	<b>459</b>
	Abeceda RPC	460
	Co je to RPC?	460
	Vytváření aplikací RPC	461
	Jak aplikace v RPC komunikují	463

<b>Nejlepší postupy pro bezpečné RPC</b> .....	<b>464</b>
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
<b>Nejlepší postupy pro bezpečný DCOM</b> .....	<b>480</b>
Základy modelu DCOM .....	480
Bezpečnost na úrovni aplikací .....	482
Uživatelské kontexty v DCOM .....	482
Programová bezpečnost .....	485
Zdroje a jímky .....	488
<b>Abeceda ActiveX</b> .....	<b>488</b>
<b>Nejlepší postupy pro bezpečné ActiveX</b> .....	<b>489</b>
Jaké komponenty ActiveX jsou bezpečné pro inicializaci a pro skriptování .....	489
Nejlepší postupy pro bezpečnou inicializaci a skriptování .....	491
<b>Shrnutí</b> .....	<b>494</b>
<b>Kapitola 17 Ochrana proti útokům s odepřením služeb</b> .....	<b>495</b>
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
<b>Shrnutí</b> .....	<b>509</b>
<b>Kapitola 18 Jak psát bezpečný kód .NET</b> .....	<b>511</b>
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
<b>Příliš horlivá volání Assert</b> .....	<b>520</b>
<b>Další informace k voláním Demand a Assert</b> .....	<b>522</b>

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

## Část IV

### Speciální témata

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

	Vypočtení součinu vektorů násobených sklonem .....	580
	Shrnutí .....	581
<b>Kapitola 20</b>	<b>Provedení bezpečnostní revize kódu .....</b>	<b>583</b>
	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
<b>Kapitola 21</b>	<b>Bezpečná instalace softwaru .....</b>	<b>595</b>
	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
<b>Kapitola 22</b>	<b>Obecné doporučené postupy .....</b>	<b>609</b>
	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 paketu s požadavkem IRP .....	619
	Do kódu zapisujte bezpečnostní komentáře .....	619
	Využívejte funkcí 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 nezapíšíte uživatelské soubory .....	623
Do registrační větve HKLM nezapíšíte 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 nevkláděte názvy platné uvnitř firmy .....	635
Řetězce přesuňte do knihovny DDL s prostředky .....	636
Záznam do aplikačního protokolu .....	636
Převěďte nebezpečný kód C/C++ na řízený kód .....	637
<b>Kapitola 23 Jak psát bezpečnostní dokumentaci a chybové zprávy .....</b>	<b>639</b>
<b>Bezpečnostní problémy v dokumentaci .....</b>	<b>640</b>
Základy .....	640
Potlačování hrozeb prostřednictvím dokumentace .....	641
Dokumentování doporučených bezpečnostních postupů .....	641
<b>Bezpečnostní problémy v chybových zprávách .....</b>	<b>643</b>
<b>Typické bezpečnostní zprávy .....</b>	<b>643</b>
<b>Problémy s prozrazením informací .....</b>	<b>644</b>
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
<b>Použitelnost bezpečnostních funkcí .....</b>	<b>652</b>
<b>Shrnutí .....</b>	<b>653</b>

**Část V****Přílohy**

<b>Příloha A</b>	<b>Nebezpečná volání API</b> .....	<b>657</b>
	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
<b>Příloha B</b>	<b>Nejhlupejší výmluvy, které můžeme slyšet</b> .....	<b>669</b>
<b>Příloha C</b>	<b>Seznam bezpečnostních kontrol pro návrháře</b> .....	<b>677</b>
<b>Příloha D</b>	<b>Seznam bezpečnostních kontrol pro vývojáře</b> .....	<b>679</b>
	Obecné .....	680
	Webové a databázové .....	681
	Volání RPC .....	681
	ActiveX, COM a DCOM .....	682
	Řízení kryptografie a tajných informací .....	682
	Řízený kód .....	682
<b>Příloha E</b>	<b>Seznam bezpečnostních kontrol pro testera</b> .....	<b>685</b>
	 <b>Myšlenka na závěr</b>	 <b>687</b>
	 <b>Literatura</b>	 <b>689</b>
	Citovaná literatura .....	689
	Další doporučená literatura .....	693
	 <b>Autoři</b>	 <b>695</b>
	Michael Howard .....	695
	David LeBlanc .....	695

# Bezpečný kód pro Windows Vista

<b>Předmluva</b>	<b>699</b>
<b>Úvod</b>	<b>701</b>
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
<b>Kapitola 1 Kvalita kódu .....</b>	<b>707</b>
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
<b>Kapitola 2 Řízení uživatelských účtů, tokeny a úrovně integrity .....</b>	<b>719</b>
Přehled .....	719
Podrobnosti o řízení uživatelských účtů .....	720
Začneme od začátku – uživatelské tokeny .....	721

Povýšení 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
Spouštění komponent COM s pomocí COM Elevation Monikeru . . . . .	731
Spuštění aplikací se zvýšeným oprávněním s řízeným kódem . . . . .	732
<b>Úvahy o uživatelském rozhraní . . . . .</b>	<b>732</b>
<b>Virtualizace . . . . .</b>	<b>733</b>
Jak zakázat ve své aplikaci virtualizaci . . . . .	736
<b>Úrovně integrity . . . . .</b>	<b>737</b>
Pravidla pro nastavení integrity . . . . .	746
Masky NW, NR a NX . . . . .	746
Defenzivní model s použitím úrovně integrity . . . . .	746
<b>Ladění problémů spojených s kompatibilitou aplikací ve Windows Vista . . . . .</b>	<b>747</b>
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
<b>Význam podepisování kódu . . . . .</b>	<b>749</b>
<b>Nová oprávnění ve Windows Vista . . . . .</b>	<b>750</b>
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
<b>Realizace . . . . .</b>	<b>751</b>
<b>Literatura . . . . .</b>	<b>751</b>
<b>Kapitola 3 Ochrana proti přetečení zásobníku . . . . .</b>	<b>753</b>
Přehled . . . . .	753
ASLR . . . . .	755

	Omezení ASLR .....	757
	Důsledky pro výkon a kompatibilitu .....	757
	<b>Náhodné umístění zásobníku .....</b>	<b>758</b>
	Důsledky pro výkon a kompatibilitu .....	759
	<b>Ochrana haldy .....</b>	<b>759</b>
	<b>NX .....</b>	<b>763</b>
	Důsledky pro výkon a kompatibilitu .....	765
	/GS .....	767
	SafeSEH .....	770
	Shrnutí .....	774
	Realizace .....	775
	Literatura .....	775
<b>Kapitola 4</b>	<b>Síťové ochrany .....</b>	<b>777</b>
	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
	Tvorba pravidel .....	788
	Práce se skupinami pravidel .....	793
	Realizace .....	795
	Literatura .....	795
<b>Kapitola 5</b>	<b>Bezpečné a odolné služby .....</b>	<b>797</b>
	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

<b>Kapitola 6</b>	<b>Ochrany v Internet Exploreru 7</b>	<b>819</b>
	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
<b>Kapitola 7</b>	<b>Vylepšená kryptografie</b>	<b>833</b>
	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
<b>Kapitola 8</b>	<b>Autentizace a autorizace</b>	<b>849</b>
	CardSpace a informační karty ve Windows	849
	Datový tok systému informačních karet	850
	Windows CardSpace a phishing	851
	Serverová autentizace	851

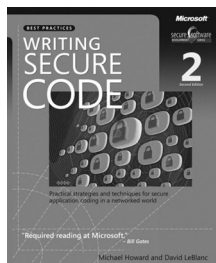
	CardSpace a phishing – příklad .....	852
	Informační karty v akci .....	854
	Co se nachází v informační kartě .....	854
	Programový přístup k informačním kartám .....	855
	Shrnutí technologie CardSpace .....	857
	<b>Změny v grafické identifikaci a autorizaci</b>	
	<b>(Graphical Identification and Authorization,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





# Knih první

## BEZPEČNÝ KÓD



*Věnováno Cheryl a Blake, dvěma nejbáječnějším lidem, které znám.  
– Michael*

*Věnováno Jennifer, která statečně snášela všechny ty ztracené víkendy,  
přestože jsme je mohli strávit společnou vyjíždkou na koních.  
– David*

# Úvod

Během měsíců února a března 2002 se všechny normální práce na funkcích Microsoft Windows zastavily. Celý vývojový tým se po uvedení nové verze systému, tedy Windows .NET Serveru 2003. Cílem této iniciativy, známé jako Windows Security Push, bylo proškolení celého vývojového týmu z nejnovějších technik bezpečného kódování, vyhledat chyby v návrhu i ve vlastním kódu a zlepšit kód a dokumentaci testů. První vydání knihy bylo během této bezpečnostní akce Security Push pro všechny členy týmu „povinnou četbou“ a ve druhém vydání, které nyní otevíráte, se již odrážejí závěry a zkušenosti z této i následných akcí Security Push pro jiné produkty Microsoft, jako je SQL Server, Office, Exchange, Systems Management Server, Visual Studio .NET, společná běhová knihovna .NET a řada dalších.

Hlavním popudem pro vznik iniciativy Windows Security Push (a pro celou řadu dalších podobných iniciativ) bylo prohlášení Billa Gatese z 15. ledna 2002, ve kterém pod názvem „Trustworthy Computing“ vymezil obecnou strategii tvorby nové generace počítačových systémů s vyšší bezpečností i dostupností. Od doby vydání tohoto prohlášení jsme my oba autoři hovořili nebo přímo spolupracovali s tisíci vývojářů ze samotného Microsoftu i mimo něj a všichni nám říkali to stejné: „Chceme dělat tu správnou věc – chceme psát bezpečnější software – ale zatím toho dost nevíme.“ Toto přání a zároveň nejistota má přímou souvislost s cílem této knížky: naučit lidi něco, co se ve školách nikdy neučili, a sice jak navrhovat, vytvářet, testovat a dokumentovat bezpečný software. Výrazem *bezpečný software* zde ale nemyslíme nějaký bezpečnostní kód nebo kód, který implementuje bezpečnostní funkce; myslíme tím kód, který je navržen takovým způsobem, aby odolal útoku zlomyslných útočníků. Bezpečný kód je zároveň robustním kódem.

Naším cílem je, aby tato knížka byla především neúprosně praktická. Jako jakýsi „vedlejší efekt“ byste měli také pochopit, že i váš programový kód se nakonec *stane* cílem útoku. Tato pravda se snad nedá říci stručněji, takže ještě jednou: pokud napíšete aplikaci, která poběží na jednom nebo více počítačích připojených do sítě, nebo dokonce do největší ze světových sítí jménem Internet, pak se cílem útoku jednoho krásného dne stane.

Napadení počítačového systému může mít celou řadu různých důsledků, ať je to ztráta produkce, ztráta důvěry zákazníků a přímá finanční ztráta. Pokud se například útočníkovi podaří napadnout aplikaci a třeba ji vyřadí z provozu, mohou klienti odejít jinam. Většina lidí u internetových služeb nečeká příliš dlouho: jakmile určitá služba není dostupná, „utrátí“ raději svůj zájem i peníze u konkurence.

Skutečný problém mnoha firem zaměřených na vývoj softwaru je, že na bezpečnost nepohlížejí jako na přímý zdroj příjmů. Vedení firmy proto často nerado vynakládá velké peníze na školení vývojářů ze psaní bezpečného kódu. Za bezpečnostní technologie nějaké peníze utratí, ale většinou až po nějakém úspěšném útoku! A v tom okamžiku už je příliš pozdě – útočníkovi se již podařilo nějaké škody napáchat. Oprava aplikací až po útoku je nákladná – stojí jednak čas a peníze, a jednak i ztrátu dobrého jména.

Důležitost ochrany majetku před krádeží a napadením už je léty prověřená a nikdo o ní nepochybuje. Již v dávných dobách zavedli naši předkové zákony, podle kterých se trestá jakákoli krádež, poškození nebo zneužití cizího majetku. Lidé zkrátka chápou, že určitý

movitý i nemovitý majetek je soukromý a že musí jeho soukromí ctít. Stejná pravidla platí ale i v digitálním světě a úlohou nás vývojářů je vytvářet takové aplikace a taková řešení, která ochrání digitální „majetek“ či aktiva.

Jistě si všimnete, že tato kniha hovoří také o některých základních otázkách, které by se měly probírat už ve škole, a to v souvislosti s návrhem a výstavbou bezpečných systémů. Možná si myslíte, že návrh aplikací je úkolem softwarových architektů nebo programových manažerů – a opravdu tomu tak je – ale procesům, pomocí nichž navrhujeme systémy odolné proti útokům, musí rozumět i vývojáři a testěři.

Víme, že nějaké zranitelné místo bude v každém softwaru, i když do vývoje jeho bezpečnosti investujeme jakékoli množství času a práce, protože budoucí vývoj na poli bezpečnosti zkrátka nelze předvídat. Víme, že toto tvrzení platí i o systému Microsoft Windows .NET Server 2003, ale současně víme, že při dodržování rad popsanych v této knížce můžeme vytvořit takový kód, ve kterém bude dohromady méně zranitelných míst a zbylá zranitelná místa bude pro útočníka mnohem obtížnější najít a zneužít.

## Pro koho je tato kniha určena

Tuto knížku potřebuje ke své práci každý, kdo se podílí na návrhu aplikací nebo na vytváření testování a dokumentaci ucelených řešení. Potřebovat ji budete bez ohledu na to, jestli pracujete s webově orientovanými aplikacemi nebo s aplikacemi pod Win32. A potřebujete ji také v případě, že se učíte pracovat se systémem Microsoft .NET Framework nebo s ním již nějaké aplikace píšete. Zkrátka, pokud jste jakkoli „namočení“ do vývoje aplikací, kniha pro vás bude přínosná.

Velkou část látky v této knížce využijete ovšem i při vývoji kódu, který nepoběží na platformách Microsoft. S výjimkou několika málo kapitol orientovaných výhradně na systémy Microsoft hovoří totiž kniha o obecných problémech, jež vznikají pod jakoukoli platformou. I poznatky, které zdánlivě platí jen pro svět Windows, mají často širší uplatnění. Přístupový seznam s právem úplného řízení pro všechny (Full Control pro skupinu Everyone) ve Windows znamená například stejný problém, jako když v Unixu nastavíme právo zápisu pro všechny (World – Writable); také problémy křížového volání skriptů mezi různými weby (cross-site scripting) jsou univerzální.

## Uspořádání knihy

Kniha je rozdělena do pěti částí: první čtyři kapitoly tvoří část I s názvem „Bezpečnost v současném světě“, přičemž uvádějí důvody, pro které je třeba systémy zabezpečovat před útokem, a popisují návody a techniky analýzy pro návrh takovýchto systémů.

Jádrum knihy jsou části II a III. Druhá část s titulem „Techniky bezpečného kódování“ obsahuje kapitoly 5 až 14 a popisuje nejdůležitější techniky kódování, které platí téměř pro jakoukoli aplikaci. Třetí část, „Další techniky bezpečného kódování“, se skládá ze čtyř kapitol (číslo 15 až 18) a zaměřuje se na síťové aplikace a na kód .NET.

Do čtvrté části, „Speciální témata“, jsme zařadili šest kapitol (19 až 24) věnovaných méně často probíraným tématům, jako je testování, provádění bezpečnostních revizí kódu, soukromí a bezpečná instalace softwaru. Kapitola 23 obsahuje obecné postupy, které se nevešly do žádné jiné kapitoly.

Část V obsahuje pět příloh, které popisují nebezpečná volání API, nejhlupejší výmluvy pro nedostatečné zabezpečení systémů a seznamy bezpečnostních kontrol pro návrháře, vývojáře a testery.

Na rozdíl od autorů celé řady jiných knížek věnovaných bezpečnosti vám nebudeme jenom říkat, jak nebezpečné aplikace se píší, a nebudeme jenom naříkat, jak lidé nedbají zabezpečování systémů. Kniha je naopak ryze pragmatická, a jak jsme říkali, neúprosně praktická. Vysvětlíme si, jakým způsobem je možné systémy napadnout, jakých chyb se lidé nejčastěji dopouštějí, a co je nejdůležitější, jak budovat bezpečné systémy. (Mimořadně, dívejte se také na ikony v okraji, které vás upozorní na různé humorné příhody spojené s bezpečností.)

## Instalace a používání ukázkových souborů



Z webové stránky doprovodného obsahu knihy (Companion Content) na adrese <http://www.microsoft.com/mspress/books/5957.asp> si můžete stáhnout ukázkové soubory. V poli More Information v pravé části stránky klepněte na odkaz Companion Content; tím otevřete webovou stránku Companion Content, která již obsahuje odkaz pro přímé stažení souborů a také odkaz na stránky odborné pomoci Microsoft Press Support. Pro zkopírování ukázkových souborů klepněte na odkaz pro stažení, tím vyvolejte spustitelný soubor, a dále klepnutím potvrďte souhlas s licenční smlouvou. Podle výchozího nastavení se soubory zkopírují do složky Dokumenty\Microsoft Press\Secureco2; během instalace můžete ale cílovou složku změnit.

## Stažení lokalizovaných zdrojových kódů



Částečně lokalizované zdrojové kódy (pouze řetězce a komentáře) jsou ke stažení na webu českého vydání na adrese <http://knihy.cpress.cz/K1451>. V záložce *Soubory ke stažení* klepněte na soubor *Bezpečný kód*. Po uložení a rozbalení lze s kódy ihned pracovat.

## Systémové požadavky

Většina ukázek v této knížce je napsána v jazyce C nebo C++ a vyžaduje ke své činnosti Microsoft Visual Studio .NET, i když většina příkladů z C/C++ pracuje správně také ve většině jiných kompilátorů, mimo jiné i v Microsoft Visual C++ 6.0. Příklady v jazyce Perl byly testovány v prostředí ActiveState Perl 5.6 nebo ActivateState Visual Perl 1.0, které je k dispozici na webové adrese <http://www.activestate.com>. Kód pro Microsoft Visual Basic Scripting Edition a pro jazyk JScript byl testován v prostředí Windows Scripting Host, který je součástí verze systému Windows 2000 a novějších. Příklady v jazyce SQL byly testovány pod Microsoft SQL Serverem 2000. A konečně, aplikace pro jazyky Visual Basic .NET a Visual C# byly napsány a testovány v prostředí Visual Studio .NET.

S výjimkou dvou aplikací poběží veškeré aplikace z této knížky na jakémkoli počítači s Windows 2000, jenž splňuje doporučené požadavky operačního systému. Příklad Safer v kapitole 7 a příklad UTF8 MultiByteToWideChar v kapitole 11 vyžadují ke správné činnosti systém Windows XP nebo Windows .NET Server. Pro kompilaci kódu je ale vhodné prostředí výkonnějšího počítače, který by měl odpovídat systémovým požadavkům použitého kompilátoru.

## Informace o podpoře



Práci na knize i doprovodném obsahu bylo věnováno maximální možné úsilí a snažili jsme se zde uvést co nejpřesnější informace. Opravy chyb v knihách nabízí Microsoft Press přes síť World Wide Web, na adrese <http://www.microsoft.com/mspress/support/>. Prostřednictvím webové adresy <http://www.microsoft.com/mspress/support/search.asp> se můžete připojit přímo k databázi znalostí Microsoft Press Knowledge Base a zadat dotaz či problém, s jehož řešením potřebujete pomoci.

## Poděkování

Na obálce uvidíte jména jen dvou autorů, ale knížka by samozřejmě vůbec nemohla vzniknout bez přispění mnoha jiných lidí. Některé jsme doslova „otravovali“ až do úmoru, zatímco jiní nám pomohli velmi ochotně.

Ze všeho nejdříve bychom rádi poděkovali lidem ve vydavatelství Microsoft Press, konkrétně Danielle Birdové za souhlas s přípravou druhého vydání, Devon Musgraveové za přetvoření našeho „neotesaného“ rukopisu do čtivého jazyka a za cenné lekce z gramatiky a Brianu Johnsonovi za to, že nám v knize opravil některé nepravdy. Děkujeme také Kerrimu DeVaultovi za vnitřní úpravu knihy a Robovi Nancemu za úvodní stránky jednotlivých částí a další obrázky.

Další lidé nám odpověděli na různé otázky a přispěli tak k maximální přesnosti informací v knížce; z Microsoftu to byli mimo jiné: Saji Abraham, Ümit Akkuş, Doug Bayer, Tina Birdová, Mike Blaszcak, Grant Bolitho, Christopher Brumme, Neill Clift, David Cross, Scott Culp, Mike Danseglio, Bhavesh Doshi, Ramsey Dow, Werner Dreyer, Kedar Dubhashi, Patrick Dussud, Vadim Eydelman, Scott Field, Cyrus Gray, Brian Grunkemeyer, Caglar Gunyakti, Ron Jacobs, Jesper Johansson, Willis Johnson, Loren Kohnfelder, Sergey Kuzin, Mike Lai, Bruce Leban, Yung-Shin „Bala“ Lin, Steve Lipner, Eric Lippert, Matt Lyons, Erik Olson, Dave Quick, Art Shelest, Daniel Sie, Frank Swiderski, Matt Thomlinson, Chris Walker, Landy Wang, Jonathan Wilkins a Mark Zbikowski.

Za cenné připomínky, opravy drobných chyb a námětů ke zlepšení děkujeme také celé divizi Windows – bylo vás tolik, že bychom všechny nedovedli ani vyjmenovat!

Někteří lidé si zaslouhují zvláštní uznání za cenný materiál, který do knihy poskytli – velká část materiálu byla vytvořena v rámci příslušné bezpečnostní akce Security Push daného produktu. Brandon Bray a Raymond Fowkes dodali množství námětů a materiálů k přečtení bufferu. Dave Ross, Tom Gallagher a Richie Lai jsou tři z nejlepších expertů na otázky webové bezpečnosti, zejména pak na problém „křížových skriptů“ mezi různými weby. John McConnell, Mohammed El-Gammal a Julie Bennettová vytvořili jádro kapitoly o mezinárodním prostředí; navíc se s nimi báječně pracovalo. Kapitola o bezpečném kódu pro .NET by nemohla být úplná bez pomoci Erika Olsona a Ivana Medvedeva; osobitě uznání si zaslouží především Ivan a jeho myšlenka „bezpečnosti kódu pro přístup v obrazech“. Adrian Oney a Peter Viscarola ze společnosti Open Systems Resources, Inc., napsali během chvilky doporučené postupy při práci se zařízeními a s režimem jádra. J. C. Cannon se statečně zhostil kapitoly věnované soukromí. A konečně, Ken Jones, Todd Stedl, David Wright, Richard Carey a Everett McKay napsali obrovské množství

materiálu, který dal vzniknout kapitole o dokumentaci. V kapitole věnované provádění bezpečnostních revizí kódu nám pomohly cenné připomínky a odkazy od Ramseye Dowa a prezentace PowerPoint od Neilla Clifta. Vadim Eydelman provedl podrobnou analýzu potenciálních problémů s volbou socketů `SO_EXCLUSIVEADDR` a podal několik řešení, které se objevily jednak v této knížce, jednak v článku databáze znalostí Microsoft Knowledge Base. Skláníme se před tvojí ochotou, s jakou jsi nám poskytl tento rozsáhlý a bohatý materiál.

Tito lidé přispěli cennými podněty do prvního vydání knihy, a proto jim děkujeme i zde, ve druhém vydání: Eli Allenová, John Biccum, Thomas Deml, Monica Ene-Pietrosanová, Sean Finnegan, Tim Fleehart, Damian Haase, David Hubbard, Louis Lafreniere, Brian LaMacchia, John Lambert, Lawrence Landauer, Paul Leach, Terry Leeperová, Rui Maximo, Daryl Pecelj, Jon Pincus, Rain Forest Puppy, Fritz Sands, Eric Schultze, Alex Stockton, Hank Voight, Richard Ward, Richard Waymire a Mark Zhou.

Svůj drahocenný čas nám při přípravě knížky věnovalo také spousta lidí mimo samotný Microsoft. Naše nejpřímnější díky si proto zasluhují: Peter Gutmann, Steve Hayr ze společnosti Accenture, Christopher W. Klaus z Internet Security Systems, John Pescatore z Gartner Inc., Herbert H. Thompson a James A. Whittaker z Florida Tech a nakonec také Chris „Weld Pond“ Wysopal ze společnosti *@Stake*.

A na závěr vyslovme ten nejdůležitější dík, který patří všem v Microsoftu za důsledné a naléhavé volání po bezpečnosti v iniciativě Trustworthy Computing. Všem vám moc děkujeme.