Stučný obsah

Bezpečný kód

Bezpečný kód pro Windows Vista

Obsah

Bezpečný kód

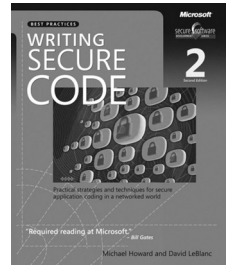
Část V

Přílohy

Bezpečný kód pro Windows Vista

Kniha 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 vyjížďkou na koních.
– David

Úvod

Během měsíců února a března 2002 se všechny normální práce na funkcích Microsoft Windows zastavily. Celý vývojový tým se po uvedenou dobu soustředil na zlepšení bezpečnosti nejbližší nové verze systému, tedy Windows .NET Serveru 2003. Cílem této iniciativy, známé jako Windows Security Push, bylo proškolit celý vývojový tým 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, „utratí" 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 testeři.

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 popsaných 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 „namočeni“ 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.

Jádrem 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, nejhloupější 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. (Mimochodem, 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 Blaszczak, 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 zasluhují 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 přetečení 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; osobité 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 soketů `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 nejupřímnější 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.