



Programming Windows Security

By Keith Brown

Download now

Read Online 

Programming Windows Security By Keith Brown

--George V. Reilly, IIS Performance Lead, Microsoft Windows security has often been considered a dry and unapproachable topic. For years, the main examples of programming security were simply exercises in ACL manipulation.

Programming Windows Security is a revelation providing developers with insight into the way Windows security really works. This book shows developers the essentials of security in Windows 2000, including coverage of Kerberos, SSL, job objects, the new ACL model, COM+ and IIS 5.0. Also included are highlights of the differences between security in Windows 2000 and in Windows NT 4.0. Programming Windows Security is written by an experienced developer specifically for use by other developers. It focuses on the issues of most concern to developers today: the design and implementation of secure distributed systems using the networking infrastructure provided by Windows, the file server, the web server, RPC servers, and COM(+) servers. Topics covered include:

- *COM(+) security, from the ground up
- *IIS security
- *How the file system redirector works and why developers should care
- *The RPC security model
- *Kerberos, NTLM, and SSL authentication protocols and SSPI
- *Services

 [Download Programming Windows Security ...pdf](#)

 [Read Online Programming Windows Security ...pdf](#)

Programming Windows Security

By Keith Brown

Programming Windows Security By Keith Brown

--George V. Reilly, IIS Performance Lead, Microsoft Windows security has often been considered a dry and unapproachable topic. For years, the main examples of programming security were simply exercises in ACL manipulation. Programming Windows Security is a revelation providing developers with insight into the way Windows security really works. This book shows developers the essentials of security in Windows 2000, including coverage of Kerberos, SSL, job objects, the new ACL model, COM+ and IIS 5.0. Also included are highlights of the differences between security in Windows 2000 and in Windows NT 4.0. Programming Windows Security is written by an experienced developer specifically for use by other developers. It focuses on the issues of most concern to developers today: the design and implementation of secure distributed systems using the networking infrastructure provided by Windows, the file server, the web server, RPC servers, and COM(+) servers. Topics covered include: *COM(+) security, from the ground up *IIS security *How the file system redirector works and why developers should care *The RPC security model *Kerberos, NTLM, and SSL authentication protocols and SSPI *Services

Programming Windows Security By Keith Brown Bibliography

- Sales Rank: #1799196 in Books
- Published on: 2000-07-15
- Released on: 2000-07-05
- Original language: English
- Number of items: 1
- Dimensions: 9.00" h x 1.40" w x 7.30" l, 2.15 pounds
- Binding: Paperback
- 608 pages

 [Download Programming Windows Security ...pdf](#)

 [Read Online Programming Windows Security ...pdf](#)

Editorial Review

From the Inside Flap

As with most of my friends, I learned to program Windows by reading Charles Petzold's classic tome, *Programming Windows*. I then moved on to Jefferey Richter's seminal book for systems developers, *Advanced Windows NT*. Finally, I moved into the realm of objects with Kraig Brockschmidt's *Inside OLE 2*. With the release of Windows NT 4.0, I started using (and eventually teaching) COM as a way to build distributed applications. Until this point in my life, I'd been able to safely ignore security, and had long since suppressed the pangs of guilt I used to feel when passing NULL for LPSECURITY_ATTRIBUTES. Little did I know that my life was about to change forever.

It was a beautiful sunny day in Bellevue, Washington, when I drove up to the offices of Saros, a software development company where I was scheduled to give my first on-site presentation of Essential COM, DevelopMentor's flagship COM course that included coverage of the relatively new Windows NT 4.0 feature called DCOM. All the students in the class had packed in their own computers (these students were worn and grizzled Windows programmers, some of whom had lost the covers to their machines long ago). What made the situation interesting was that some of the students had machines belonging to various Windows NT domains, whereas others had standalone machines not associated with any domain. One student was even running Windows 95. It was a recipe for disaster. Everything had been going smoothly, and the students (and myself) were thoroughly enjoying the class, but the radical configuration in the classroom put quite a crimp in the DCOM lab exercise that morning. Virtually all the students were getting E_ACCESSDENIED and various and sundry error codes, and of course they all looked to me to fix the problem. I failed miserably that day, and had to admit to myself (and the students) that I didn't yet have a good enough grasp of Windows security to solve their problems. I've rarely felt so small.

Shortly after this soul-wrenching experience, I dedicated myself to the pursuit of a deep and practical understanding of Windows security. I solidified my commitment by agreeing to write a new course for DevelopMentor about services and security, and proceeded to spend three months of virtually uninterrupted time studying and experimenting with the Windows security APIs. I never knew that I'd end up falling in love. Since then, I've learned loads more and answered hundreds of questions on the DCOM mailing list regarding security issues, and reached thousands of students, conference attendees, and readers of Microsoft Systems Journal (now MSDN Magazine) with the message that security is a fascinating and approachable topic.

As the culmination of my effort, this book attempts to fill the gaping hole in the Windows systems programming canon by providing a reference for programmers that covers Windows security from the basics of principals, authorities, logon sessions, and DACLs all the way through COM+ security, one of the most subtle and sensitive beasts you'll encounter as a Windows programmer.

As a side effect of my predilection for distributed programming, this book is unique in that it addresses security with the distributed systems developer in mind; in fact, the original title of the book was *Distributed Security in Windows NT*. Of course, Microsoft's decision to rename their (beta, at the time) operating system from "Windows NT 5.0" to "Windows 2000" didn't bode well for my original title. Frankly, *Distributed Security in Windows NT/2000* sounded really goofy. Thus the new title.

In any case, if you're a programmer who, not unlike myself a few years ago, feels a hollowness in the pit of

your stomach as a result of being asked to add a security-related feature or debug a security-related problem in an application, I hope you'll find that this book completes you. Which Windows?

This book covers security programming on Windows 2000 and Windows NT 4. Therefore, to avoid crossing the reader's eyes with "Windows 2000/NT" or similar nastiness, I'll simply refer to both of these operating systems as Windows. If I find the need to say anything specific about a distinct operating system (including Windows 9x), I'll use the full name. Who Should Read This Book

This book was written for professional software developers involved in systems programming on Windows. The third part of the book was written for the subset of these programmers developing distributed systems (especially those using COM).

The first part of the book (the first three chapters) intentionally has no code in it, and instead speaks to the big picture, introducing terminology and concepts that will likely be useful not just for programmers but also for technical managers and advanced Windows users. If you are a manager and want to get a better understanding of Windows security, borrow this book from one of the developers on your team and rip out the first three chapters for yourself. Sharing a common terminology will help you and your development team play better together. What a Developer Should Already Know

I assume you have a basic understanding of Windows system programming; that is, you know the difference between a process and a thread, and you've written a DLL before and perhaps even written a service or two. I casually mention features such as thread local storage and assume that you know what I'm talking about. If you're unsure of your ability in this area, my favorite book on the subject is *Advanced Windows*, by Jefferey Richter (as of this writing the fourth edition is hot off the press).

In the COM chapter (Chapter 9), I assume you feel comfortable with the basics of IUnknown and that you know what a proxy and stub are. If you're unsure, my favorite COM book is *Essential COM* by Don Box.

Much of the later material in the COM chapter talks about COM+ features in Windows 2000, which *Essential COM* doesn't address (as of this writing, *Essential COM* is in its first edition). My favorite COM+ book in print as I write this is *Programming Distributed Applications with COM and Visual Basic 6.0* by Ted Pattison. Tim Ewald's book *Transactional COM+: Designing Scalable Applications* will likely be a must-read as well, although it's not yet gone to press as I write this.

Although this book often shows full declarations of Windows API functions, I won't always bother to tell you the details of what each and every parameter means if it's not relevant to the topic at hand. I hope you find that this book works well as a complement to the Windows API documentation, as opposed to a replacement for it. How to Approach This Book

I know that most developers don't relish thinking about security issues, which is often why security ends up getting retrofitted into existing products (or left until the last minute in new products). Most of my students are really surprised to learn that security is actually quite an interesting topic, and they really enjoy sitting through DevelopMentor's security class. However, I'm aware that this is a self-selecting group; these folks have chosen to take the class, often because there is a distinct set of problems that they need to be able to solve, whether they like it or not. Whatever your predisposition is toward security, I designed this book to be readable front to back, but also to be readable in chunks.

Many people will buy this book because it contains (at least as of this writing) an exhaustive coverage of COM security, and will want to dive right in to the chapter on COM. However, you can't possibly understand COM security without having a basic understanding of the fundamentals, and no matter how much I urge folks to read chapter 4, there will be a large group of people who don't have the time for this. If it's you I'm

describing, do spend the time to read the first three (very short) chapters of this book before you start diving into the nitty-gritty details of COM security. These chapters will help you develop a more intuitive feel for how Windows security works and why it works the way it does. This Is Not a Cookbook

In the vein of my last book project, Effective COM (coauthored with Don Box, Tim Ewald, and Chris Sells), I've purposely avoided making this a cookbook that provides lots of code for you to cut and paste to solve a particular set of problems that you may or may not be faced with. Instead, this book is about helping you understand how things work. I'd love to see a Windows security cookbook written. I find that cookbooks increase my long-term productivity once I have a basic understanding of the topic at hand.

The code snippets in this book should all compile correctly. However, although some of them might be appropriate for cutting and pasting into your projects, be aware that a number of them exist solely to foster insight and understanding and will necessarily be a bit more abstract than what you'd expect to find in a cookbook. The Bad Guys

Often I'll refer to the "bad guys" when I want to indicate someone who may be trying to break into your system either to do malicious damage, or just for fun. The bad guys

From the Back Cover

"Keith Brown lucidly explains the Win32 security architecture and how it pervades Windows NT and Windows 2000. He demystifies authentication, authorization, auditing, COM+ security, logon sessions, and much more."

--George V. Reilly, IIS Performance Lead, Microsoft

Windows security has often been considered a dry and unapproachable topic. For years, the main examples of programming security were simply exercises in ACL manipulation. *Programming Windows Security* is a revelation providing developers with insight into the way Windows security really works. This book shows developers the essentials of security in Windows 2000, including coverage of Kerberos, SSL, job objects, the new ACL model, COM+ and IIS 5.0. Also included are highlights of the differences between security in Windows 2000 and in Windows NT 4.0.

Programming Windows Security is written by an experienced developer specifically for use by other developers. It focuses on the issues of most concern to developers today: the design and implementation of secure distributed systems using the networking infrastructure provided by Windows, the file server, the web server, RPC servers, and COM(+) servers.

Topics covered include:

- COM(+) security, from the ground up
- IIS security
- How the file system redirector works and why developers should care
- The RPC security model
- Kerberos, NTLM, and SSL authentication protocols and SSPI
- Services and the Trusted Computing Base (TCB)
- Logon sessions and tokens
- Window stations, desktops, and user profiles
- The Windows 2000 ACL model, including the new model of inheritance
- Using private security descriptors to secure objects
- Accounts, groups, aliases, privileges, and passwords

- Comparison of three strategies for performing access control--impersonation, role-centric, and object-centric--and their impact on the design of a distributed application

Programming Windows Security provides the most comprehensive coverage of COM(+) security available in one place, culled from the author's extensive experience in diagnosing COM security problems in the lab and via correspondence on the DCOM mailing list.

0201604426B04062001

About the Author

Keith Brown focuses on application security at Pluralsight, which he cofounded with several other .NET experts to foster a community, develop content, and provide premier training. Keith regularly speaks at conferences, including TechEd and WinDev, and serves as a contributing editor and columnist to *MSDN Magazine*.

Users Review

From reader reviews:

Donald McLaughlin:

The book *Programming Windows Security* give you a sense of feeling enjoy for your spare time. You should use to make your capable far more increase. Book can to get your best friend when you getting strain or having big problem together with your subject. If you can make examining a book *Programming Windows Security* being your habit, you can get far more advantages, like add your own personal capable, increase your knowledge about a few or all subjects. It is possible to know everything if you like available and read a guide *Programming Windows Security*. Kinds of book are several. It means that, science guide or encyclopedia or other people. So , how do you think about this e-book?

Elizabeth Hart:

What do you ponder on book? It is just for students since they are still students or the item for all people in the world, exactly what the best subject for that? Just simply you can be answered for that question above. Every person has distinct personality and hobby per other. Don't to be pressured someone or something that they don't wish do that. You must know how great along with important the book *Programming Windows Security*. All type of book can you see on many solutions. You can look for the internet methods or other social media.

Alan Malbrough:

Nowadays reading books become more and more than want or need but also turn into a life style. This reading habit give you lot of advantages. The huge benefits you got of course the knowledge the rest of the

information inside the book this improve your knowledge and information. The information you get based on what kind of guide you read, if you want have more knowledge just go with education and learning books but if you want truly feel happy read one having theme for entertaining for instance comic or novel. Typically the Programming Windows Security is kind of reserve which is giving the reader unpredictable experience.

Cindi Russell:

Do you like reading a book? Confuse to looking for your best book? Or your book was rare? Why so many query for the book? But any kind of people feel that they enjoy intended for reading. Some people likes reading, not only science book but additionally novel and Programming Windows Security or perhaps others sources were given know-how for you. After you know how the fantastic a book, you feel would like to read more and more. Science e-book was created for teacher or perhaps students especially. Those books are helping them to increase their knowledge. In various other case, beside science book, any other book likes Programming Windows Security to make your spare time more colorful. Many types of book like this.

**Download and Read Online Programming Windows Security By
Keith Brown #R6GVEBT48IM**

Read Programming Windows Security By Keith Brown for online ebook

Programming Windows Security By Keith Brown Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Programming Windows Security By Keith Brown books to read online.

Online Programming Windows Security By Keith Brown ebook PDF download

Programming Windows Security By Keith Brown Doc

Programming Windows Security By Keith Brown Mobipocket

Programming Windows Security By Keith Brown EPub

R6GVEBT48IM: Programming Windows Security By Keith Brown