

BookReviews

A .NET Gold Mine

SCOTT FORBES
Microsoft

By helping developers more easily implement security and cryptography features into their code using Microsoft's .NET platform, *.NET Security and Cryptography* admirably achieves its goal.

Although the authors introduce

With the exception of the introductory material, each chapter describes a security topic using its related classes (for example, `Rijndael` and `SecurityPermission`), methods (`SetAuthCookie` and `Authenticate`), and the authors' coding recommendations. Together, these items summarize how a given set of classes and related features fit into the overall .NET framework, what these classes were designed to accomplish, and, most important, why these classes matter for .NET programmers attempting to write secure code.

Chapter five, which is dedicated to digital signatures, discusses hash algorithms, the `HashAlgorithm` class, its derived abstract classes such as `MD5`, `SHA1`, and `SHA384`, and that by using these classes when necessary, programmers can avoid having to design their own cryptographic algorithm or write dozens of lines of code without .NET's object-oriented interface. Designing a proprietary algorithm in isolation, without public evaluation, is more likely to generate an exploitable flaw than create a stronger algorithm.

Both authors have published extensively on the .NET platform and their experience shows. They are able to distill .NET's fundamental security advantages into two themes: the promotion of verifiably type-safe managed code and the vigilance of the Common Runtime Language. These technologies work together to provide a dual layer of security against common malicious activity that includes virus code fragment insertion, stack-overflow attacks, and

other techniques that exploit the absence of an administrator-defined security policy.

Because the book is practical in nature and purposefully focused on .NET security and cryptography—as opposed to a sweeping discussion of security in general—the authors had some difficulty in the introductory chapter framing and answering many overarching questions that readers might be asking themselves: Why does security matter? How does it help ensure privacy? Why does having privacy when you are not a criminal matter? How is security different than privacy?

Yet the slightly disjointed discussions used to flesh out these broader questions are not a major flaw. Instead, those remarks force readers to think at a high level about security and cryptography and presumably draw the same overall conclusion reached in the book: security is no longer an option in today's marketplace.

In a business environment where consumers expect more and better security features in their software products and services, programmers must find new ways to efficiently and cost-effectively include those features in their next software release. *.NET Security and Cryptography* is a timely and straightforward technical resource for developers needing a better practical understanding of security within the .NET platform. □

Scott Forbes is the security and privacy compliance manager in Microsoft's Law and Corporate Affairs group. He has a PhD in telecommunications from Pennsylvania State University. Contact him at scottfo@microsoft.com.

Reviewed in this issue:

Peter Thorsteinson and G. Gnana Arun Ganesh, *.NET Security and Cryptography*, Prentice Hall, 2004, ISBN 013100851-X, 466 pages, US\$49.99.

major topics with short and moderately technical discussions, readers without a programming background will find it difficult to make meaningful use of most material after the first chapter.

Yet for the .NET developer, this book is a gold mine of information. Multiple screen shots, example code, tables of commands, and block diagrams showing everything from a typical Web service architecture to the Code access security policy (Caspol) command-line options simply illustrate otherwise dense and unwieldy topics. The book provides numerous links to external sources to help readers clarify more arcane points, such as the XML Signature Syntax and Processing specification found at the World Wide Web Consortium Web site, or an article by respected encryption guru Bruce Schneier on the tension between the public's demand for exciting new features and more mundane behind-the-scenes security enhancements.