The Art Of Software Security Assessment: Identifying And Preventing Software Vulnerabilities (2 Volume Set)
There are a number of secure programming books on the market, but none that go as deep as this one. The depth and detail exceeds all books that I know about by an order of magnitude.

– Halvar Flake, CEO and head of research, SABRE Security GmbH

Note: This is now a 2 volume set which is shrink wrapped.

The Definitive Insider’s Guide to Auditing Software Security

This is one of the most detailed, sophisticated, and useful guides to software security auditing ever written. The authors are leading security consultants and researchers who have personally uncovered vulnerabilities in applications ranging from sendmail to Microsoft Exchange, Check Point VPN to Internet Explorer. Drawing on their extraordinary experience, they introduce a start-to-finish methodology for çrippling apartâ • applications to reveal even the most subtle and well-hidden security flaws.

The Art of Software Security Assessment covers the full spectrum of software vulnerabilities in both UNIX/Linux and Windows environments. It demonstrates how to audit security in applications of all sizes and functions, including network and Web software. Moreover, it teaches using extensive examples of real code drawn from past flaws in many of the industry’s highest-profile applications.

Coverage includes:

- Code auditing: theory, practice, proven methodologies, and secrets of the trade
- Bridging the gap between secure software design and post-implementation review
- Performing architectural assessment: design review, threat modeling, and operational review
- Identifying vulnerabilities related to memory management, data types, and malformed data
- UNIX/Linux assessment: privileges, files, and processes
- Windows-specific issues, including objects and the filesystem
- Auditing interprocess communication, synchronization, and state
- Evaluating network software: IP stacks, firewalls, and common application protocols
- Auditing Web applications and technologies

This book is an unprecedented resource for everyone who must deliver secure software or assure the safety of existing software: consultants, security specialists, developers, QA staff, testers, and administrators alike.

Contents

ABOUT THE AUTHORS

ACKNOWLEDGMENTS

I Introduction to Software Security Assessment

1 SOFTWARE VULNERABILITY FUNDAMENTALS

2 DESIGN REVIEW

3 OPERATIONAL REVIEW

4 APPLICATION REVIEW

PROCESS

5 MEMORY CORRUPTION

6 LANGUAGE ISSUES

7 PROGRAM BUILDING BLOCKS

8 STRINGS AND METACHARACTERS

9 UNIX I: PRIVILEGES AND FILES

10 UNIX II: PROCESSES

11 WINDOWS I: OBJECTS AND THE FILE SYSTEM

12 WINDOWS II: INTERPROCESS COMMUNICATION

13 SYNCHRONIZATION AND STATE
This should have been the third book in line to be reviewed, but as I leafed through it, once, twice, and a third time I started to realize this is one of those rare security books that has a chance to revolutionize the industry like Applied Cryptography, Snort 2.0, or Hacking Exposed. The longer you wait to read this book, the further you will fall behind. Nuff said?Every week that goes by we see an increasing understanding in the community about how important secure software is and that it takes the appropriate development process to create secure software. This book is hitting the marketplace at the perfect time, I hope the authors and publishing team have a runaway success, you deserve it. I also hope people will be encouraged by this book, secure software development is certainly possible, this book clearly shows that. It takes management support in terms of resources, training and good process, but it can certainly be done. At 1128 content pages, much of this material will be things that you have picked up in other places, such as other books or courses you have taken. Much of it will be things you once knew and forgot. But this is the most complete book on software security out there covering Windows, Unix, Network Protocols, Web and other Applications. What I particularly love is the how approachable the majority of the information is. Please do not get me wrong, if you have never written a line of code you are going to be lost during the code examples,
the only signpost you get is the occasional bolded line, but you will still be able to clearly follow the discussion before the code example and right after the code example. Section 1 of the book is called an Introduction to Software Security Assessment.

Download to continue reading...


Dmca