

Praise for *Exploiting Software*

“*Exploiting Software* highlights the most critical part of the software quality problem. As it turns out, software quality problems are a major contributing factor to computer security problems. Increasingly, companies large and small depend on software to run their businesses every day. The current approach to software quality and security taken by software companies, system integrators, and internal development organizations is like driving a car on a rainy day with worn-out tires and no air bags. In both cases, the odds are that something bad is going to happen, and there is no protection for the occupant/owner.

This book will help the reader understand how to make software quality part of the design—a key change from where we are today!”

Tony Scott
Chief Technology Officer, IS&S
General Motors Corporation

“It’s about time someone wrote a book to teach the good guys what the bad guys already know. As the computer security industry matures, books like *Exploiting Software* have a critical role to play.”

Bruce Schneier
Chief Technology Officer
Counterpane
Author of Beyond Fear and Secrets and Lies

“*Exploiting Software* cuts to the heart of the computer security problem, showing why broken software presents a clear and present danger. Getting past the ‘worm of the day’ phenomenon requires that someone other than the bad guys understands how software is attacked.

This book is a wake-up call for computer security.”

Elinor Mills Abreu
Reuters’ correspondent

“Police investigators study how criminals think and act. Military strategists learn about the enemy’s tactics, as well as their weapons and personnel capabilities. Similarly, information security professionals need to study their criminals and enemies, so we can tell the difference between popguns and weapons of mass destruction. This book is a significant advance in helping the ‘white hats’ understand how the ‘black hats’ operate.

Through extensive examples and ‘attack patterns,’ this book helps the reader understand how attackers analyze software and use the results of the analysis to attack systems. Hوجلund and McGraw explain not only how hackers attack servers, but also how malicious server operators can attack clients (and how each can protect themselves from the other). An excellent book for practicing security engineers, and an ideal book for an undergraduate class in software security.”

Jeremy Epstein

Director, Product Security & Performance

webMethods, Inc.

“A provocative and revealing book from two leading security experts and world class software exploiters, *Exploiting Software* enters the mind of the cleverest and wickedest crackers and shows you how they think. It illustrates general principles for breaking software, and provides you a whirlwind tour of techniques for finding and exploiting software vulnerabilities, along with detailed examples from real software exploits.

Exploiting Software is essential reading for anyone responsible for placing software in a hostile environment—that is, everyone who writes or installs programs that run on the Internet.”

Dave Evans, Ph.D.

Associate Professor of Computer Science

University of Virginia

“The root cause for most of today’s Internet hacker exploits and malicious software outbreaks are buggy software and faulty security software deployment. In *Exploiting Software*, Greg Hoglund and Gary McGraw help us in an interesting and provocative way to better defend ourselves against malicious hacker attacks on those software loopholes.

The information in this book is an essential reference that needs to be understood, digested, and aggressively addressed by IT and information security professionals everywhere.”

Ken Cutler, CISSP, CISA
Vice President, Curriculum Development & Professional Services,
MIS Training Institute

“This book describes the threats to software in concrete, understandable, and frightening detail. It also discusses how to find these problems before the bad folks do. A valuable addition to every programmer’s and security person’s library!”

Matt Bishop, Ph.D.
Professor of Computer Science
University of California at Davis
Author of Computer Security: Art and Science

“Whether we slept through software engineering classes or paid attention, those of us who build things remain responsible for achieving meaningful and measurable vulnerability reductions. If you can’t afford to stop all software manufacturing to teach your engineers how to build secure software from the ground up, you should at least increase awareness in your organization by demanding that they read *Exploiting Software*. This book clearly demonstrates what happens to broken software in the wild.”

Ron Moritz, CISSP
Senior Vice President, Chief Security Strategist
Computer Associates

“*Exploiting Software* is the most up-to-date technical treatment of software security I have seen. If you worry about software and application vulnerability, *Exploiting Software* is a must-read. This book gets at all the timely and important issues surrounding software security in a technical, but still highly readable and engaging, way.

Hoglund and McGraw have done an excellent job of picking out the major ideas in software exploit and nicely organizing them to make sense of the software security jungle.”

George Cybenko, Ph.D.

Dorothy and Walter Gramm Professor of Engineering,

Dartmouth

Founding Editor-in-Chief, IEEE Security and Privacy

“This is a seductive book. It starts with a simple story, telling about hacks and cracks. It draws you in with anecdotes, but builds from there. In a few chapters you find yourself deep in the intimate details of software security. It is the rare technical book that is a readable and enjoyable primer but has the substance to remain on your shelf as a reference. Wonderful stuff.”

Craig Miller, Ph.D.

Chief Technology Officer for North America

Dimension Data

“It’s hard to protect yourself if you don’t know what you’re up against. This book has the details you need to know about how attackers find software holes and exploit them—details that will help you secure your own systems.”

Ed Felten, Ph.D.

Professor of Computer Science

Princeton University