

Exploiting Online Games: Cheating Massively Distributed Systems

By Greg Hoglund, Gary McGraw

Download now

Read Online

Exploiting Online Games: Cheating Massively Distributed Systems By Greg Hoglund, Gary McGraw

"Imagine trying to play defense in football without ever studying offense. You would not know when a run was coming, how to defend pass patterns, nor when to blitz. In computer systems, as in football, a defender must be able to think like an attacker. I say it in my class every semester, you don't want to be the last person to attack your own system--you should be the first.

"The world is quickly going online. While I caution against online voting, it is clear that online gaming is taking the Internet by storm. In our new age where virtual items carry real dollar value, and fortunes are won and lost over items that do not really exist, the new threats to the intrepid gamer are all too real. To protect against these hazards, you must understand them, and this groundbreaking book is the only comprehensive source of information on how to exploit computer games. Every White Hat should read it. It's their only hope of staying only one step behind the bad guys."

--*Aviel D. Rubin, Ph.D.*
Professor, Computer Science
Technical Director, Information Security Institute
Johns Hopkins University

"Everyone's talking about virtual worlds. But no one's talking about virtual-world security. Greg Hoglund and Gary McGraw are the perfect pair to show just how vulnerable these online games can be."

--*Cade Metz*
Senior Editor
PC Magazine

"If we're going to improve our security practices, frank discussions like the ones in this book are the only way forward. Or as the authors of this book might say, when you're facing off against Heinous Demons of Insecurity, you need experienced companions, not to mention a Vorpal Sword of Security Knowledge."

--Edward W. Felten, Ph.D.
Professor of Computer Science and Public Affairs
Director, Center for Information Technology Policy
Princeton University

"Historically, games have been used by warfighters to develop new capabilities and to hone existing skills--especially in the Air Force. The authors turn this simple concept on itself, making games themselves the subject and target of the 'hacking game,' and along the way creating a masterly publication that is as meaningful to the gamer as it is to the serious security system professional.

"Massively distributed systems will define the software field of play for at least the next quarter century. Understanding how they work is important, but understanding how they can be manipulated is essential for the security professional. This book provides the cornerstone for that knowledge."

--Daniel McGarvey
Chief, Information Protection Directorate
United States Air Force

"Like a lot of kids, Gary and I came to computing (and later to computer security) through games. At first, we were fascinated with playing games on our Apple][s, but then became bored with the few games we could afford. We tried copying each other's games, but ran up against copy-protection schemes. So we set out to understand those schemes and how they could be defeated. Pretty quickly, we realized that it was a lot more fun to disassemble and work around the protections in a game than it was to play it.

"With the thriving economies of today's online games, people not only have the classic hacker's motivation to understand and bypass the security of games, but also the criminal motivation of cold, hard cash. That's a combination that's hard to stop. The first step, taken by this book, is revealing the techniques that are being used today."

--Greg Morrisett, Ph.D.
Allen B. Cutting Professor of Computer Science
School of Engineering and Applied Sciences
Harvard University

"If you're playing online games today and you don't understand security, you're at a real disadvantage. If you're designing the massive distributed systems of tomorrow and you don't learn from games, you're just plain sunk."

--Brian Chess, Ph.D.
Founder/Chief Scientist, Fortify Software
Coauthor of Secure Programming with Static Analysis

"This book offers up a fascinating tour of the battle for software security on a whole new front: attacking an online game. Newcomers will find it incredibly eye opening and even veterans of the field will enjoy some of the same old programming mistakes given brilliant new light in a way that only massively-

multiplayer-supermega-blow-em-up games can deliver. w00t!"

--Pravir Chandra
Principal Consultant, Cigital
Coauthor of Network Security with OpenSSL

If you are a gamer, a game developer, a software security professional, or an interested bystander, this book exposes the inner workings of online-game security for all to see.

From the authors of the best-selling *Exploiting Software*, ***Exploiting Online Games*** takes a frank look at controversial security issues surrounding MMORPGs, such as World of Warcraft™ and Second Life®. This no-holds-barred book comes fully loaded with code examples, debuggers, bots, and hacks.

This book covers

- Why online games are a harbinger of software security issues to come
- How millions of gamers have created billion-dollar virtual economies
- How game companies invade personal privacy
- Why some gamers cheat
- Techniques for breaking online game security
- How to build a bot to play a game for you
- Methods for total conversion and advanced mods

Written by the world's foremost software security experts, this book takes a close look at security problems associated with advanced, massively distributed software. With hundreds of thousands of interacting users, today's online games are a bellwether of modern software. The kinds of attack and defense techniques described in ***Exploiting Online Games*** are tomorrow's security techniques on display today.

Download Exploiting Online Games: Cheating Massively Distri ...pdf

Read Online Exploiting Online Games: Cheating Massively Dist ...pdf

Exploiting Online Games: Cheating Massively Distributed Systems

By Greg Hoglund, Gary McGraw

Exploiting Online Games: Cheating Massively Distributed Systems By Greg Hoglund, Gary McGraw

"Imagine trying to play defense in football without ever studying offense. You would not know when a run was coming, how to defend pass patterns, nor when to blitz. In computer systems, as in football, a defender must be able to think like an attacker. I say it in my class every semester, you don't want to be the last person to attack your own system--you should be the first.

"The world is quickly going online. While I caution against online voting, it is clear that online gaming is taking the Internet by storm. In our new age where virtual items carry real dollar value, and fortunes are won and lost over items that do not really exist, the new threats to the intrepid gamer are all too real. To protect against these hazards, you must understand them, and this groundbreaking book is the only comprehensive source of information on how to exploit computer games. Every White Hat should read it. It's their only hope of staying only one step behind the bad guys."

--*Aviel D. Rubin, Ph.D.*
Professor, Computer Science
Technical Director, Information Security Institute
Johns Hopkins University

"Everyone's talking about virtual worlds. But no one's talking about virtual-world security. Greg Hoglund and Gary McGraw are the perfect pair to show just how vulnerable these online games can be."

--*Cade Metz*
Senior Editor
PC Magazine

"If we're going to improve our security practices, frank discussions like the ones in this book are the only way forward. Or as the authors of this book might say, when you're facing off against Heinous Demons of Insecurity, you need experienced companions, not to mention a Vorpal Sword of Security Knowledge."

--*Edward W. Felten, Ph.D.*
Professor of Computer Science and Public Affairs
Director, Center for Information Technology Policy
Princeton University

"Historically, games have been used by warfighters to develop new capabilities and to hone existing skills--especially in the Air Force. The authors turn this simple concept on itself, making games themselves the subject and target of the 'hacking game,' and along the way creating a masterly publication that is as meaningful to the gamer as it is to the serious security system professional.

"Massively distributed systems will define the software field of play for at least the next quarter century. Understanding how they work is important, but understanding how they can be manipulated is essential for the security professional. This book provides the cornerstone for that knowledge."

--Daniel McGarvey
Chief, Information Protection Directorate
United States Air Force

"Like a lot of kids, Gary and I came to computing (and later to computer security) through games. At first, we were fascinated with playing games on our Apple][s, but then became bored with the few games we could afford. We tried copying each other's games, but ran up against copy-protection schemes. So we set out to understand those schemes and how they could be defeated. Pretty quickly, we realized that it was a lot more fun to disassemble and work around the protections in a game than it was to play it.

"With the thriving economies of today's online games, people not only have the classic hacker's motivation to understand and bypass the security of games, but also the criminal motivation of cold, hard cash. That's a combination that's hard to stop. The first step, taken by this book, is revealing the techniques that are being used today."

--Greg Morrisett, Ph.D.
Allen B. Cutting Professor of Computer Science
School of Engineering and Applied Sciences
Harvard University

"If you're playing online games today and you don't understand security, you're at a real disadvantage. If you're designing the massive distributed systems of tomorrow and you don't learn from games, you're just plain sunk."

--Brian Chess, Ph.D.
Founder/Chief Scientist, Fortify Software
Coauthor of Secure Programming with Static Analysis

"This book offers up a fascinating tour of the battle for software security on a whole new front: attacking an online game. Newcomers will find it incredibly eye opening and even veterans of the field will enjoy some of the same old programming mistakes given brilliant new light in a way that only massively-multiplayer-supermega-blow-em-up games can deliver. w00t!"

--Pravir Chandra
Principal Consultant, Cigital
Coauthor of Network Security with OpenSSL

If you are a gamer, a game developer, a software security professional, or an interested bystander, this book exposes the inner workings of online-game security for all to see.

From the authors of the best-selling *Exploiting Software*, ***Exploiting Online Games*** takes a frank look at controversial security issues surrounding MMORPGs, such as World of Warcraft™ and Second Life®. This no-holds-barred book comes fully loaded with code examples, debuggers, bots, and hacks.

This book covers

- Why online games are a harbinger of software security issues to come
- How millions of gamers have created billion-dollar virtual economies
- How game companies invade personal privacy
- Why some gamers cheat
- Techniques for breaking online game security

- How to build a bot to play a game for you
- Methods for total conversion and advanced mods

Written by the world's foremost software security experts, this book takes a close look at security problems associated with advanced, massively distributed software. With hundreds of thousands of interacting users, today's online games are a bellwether of modern software. The kinds of attack and defense techniques described in ***Exploiting Online Games*** are tomorrow's security techniques on display today.

Exploiting Online Games: Cheating Massively Distributed Systems By Greg Hoglund, Gary McGraw Bibliography

- Rank: #1148159 in Books
- Published on: 2007-07-19
- Released on: 2007-07-09
- Original language: English
- Number of items: 1
- Dimensions: 9.10" h x .80" w x 6.90" l, 1.63 pounds
- Binding: Paperback
- 384 pages

Download Exploiting Online Games: Cheating Massively Distri ...pdf

Read Online Exploiting Online Games: Cheating Massively Dist ...pdf

Download and Read Free Online Exploiting Online Games: Cheating Massively Distributed Systems By Greg Hoglund, Gary McGraw

Editorial Review

From the Back Cover

"Imagine trying to play defense in football without ever studying offense. You would not know when a run was coming, how to defend pass patterns, nor when to blitz. In computer systems, as in football, a defender must be able to think like an attacker. I say it in my class every semester, you don't want to be the last person to attack your own system--you should be the first.

"The world is quickly going online. While I caution against online voting, it is clear that online gaming is taking the Internet by storm. In our new age where virtual items carry real dollar value, and fortunes are won and lost over items that do not really exist, the new threats to the intrepid gamer are all too real. To protect against these hazards, you must understand them, and this groundbreaking book is the only comprehensive source of information on how to exploit computer games. Every White Hat should read it. It's their only hope of staying only one step behind the bad guys."

"--Aviel D. Rubin, Ph.D.
Professor, Computer Science
Technical Director, Information Security Institute
Johns Hopkins University"

"Everyone's talking about virtual worlds. But no one's talking about virtual-world security. Greg Hoglund and Gary McGraw are the perfect pair to show just how vulnerable these online games can be."

"--Cade Metz
Senior Editor"
PC Magazine

"If we're going to improve our security practices, frank discussions like the ones in this book are the only way forward. Or as the authors of this book might say, when you're facing off against Heinous Demons of Insecurity, you need experienced companions, not to mention a Vorpal Sword of Security Knowledge."

"--Edward W. Felten, Ph.D.
Professor of Computer Science and Public Affairs
Director, Center for Information Technology Policy
Princeton University"

"Historically, games have been used by warfighters to develop new capabilities and to hone existing skills--especially in the Air Force. The authors turn this simple concept on itself, making games themselves the subject and target of the 'hacking game, ' and along the way creating a masterly publication that is as meaningful to the gamer as it is to the serious security system professional.

"Massively distributed systems will define the software field of play for at least the next quarter century. Understanding how they work is important, but understanding how they can be manipulated is essential for the security professional. This book provides the cornerstone for that knowledge."

"--Daniel McGarvey

Chief, Information Protection Directorate
United States Air Force"

"Like a lot of kids, Gary and I came to computing (and later to computer security) through games. At first, we were fascinated with playing games on our Apple][s, but then became bored with the few games we could afford. We tried copying each other's games, but ran up against copy-protection schemes. So we set out to understand those schemes and how they could be defeated. Pretty quickly, we realized that it was a lot more fun to disassemble and work around the protections in a game than it was to play it.

"With the thriving economies of today's online games, people not only have the classic hacker's motivation to understand and bypass the security of games, but also the criminal motivation of cold, hard cash. That's a combination that's hard to stop. The first step, taken by this book, is revealing the techniques that are being used today."

"--Greg Morrisett, Ph.D.
Allen B. Cutting Professor of Computer Science
School of Engineering and Applied Sciences
Harvard University"

"If you're playing online games today and you don't understand security, you're at a real disadvantage. If you're designing the massive distributed systems of tomorrow and you don't learn from games, you're just plain sunk."

"--Brian Chess, Ph.D.
Founder/Chief Scientist, Fortify Software
Coauthor of" Secure Programming with Static Analysis

"This book offers up a fascinating tour of the battle for software security on a whole new front: attacking an online game. Newcomers will find it incredibly eye opening and even veterans of the field will enjoy some of the same old programming mistakes given brilliant new light in a way that only massively-multiplayer-supermega-blow-em-up games can deliver. w00t!"

"--Pravir Chandra
Principal Consultant, Cigital
Coauthor of "Network Security with OpenSSL

If you are a gamer, a game developer, a software security professional, or an interested bystander, this book exposes the inner workings of online-game security for all to see.

From the authors of the best-selling "Exploiting Software," "Exploiting Online Games" takes a frank look at controversial security issues surrounding MMORPGs, such as World of Warcraft(TM) and Second Life(R). This no-holds-barred book comes fully loaded with code examples, debuggers, bots, and hacks.

This book covers Why online games are a harbinger of software security issues to comeHow millions of gamers have created billion-dollar virtual economiesHow game companies invade personal privacyWhy some gamers cheatTechniques for breaking online game securityHow to build a bot to play a game for youMethods for total conversion and advanced mods

Written by the world's foremost software security experts, this book takes a close look at security problems associated with advanced, massively distributed software. With hundreds of thousands of interacting users, today's online games are a bellwether of modern software. The kinds of attack and defense techniques

described in "Exploiting Online Games "are tomorrow's security techniques on display today.

About the Author

Greg Hoglund has been involved with software security for many years, specializing in Windows rootkits and vulnerability exploitation. He founded the website www.rootkit.com, and has coauthored several books on software security (*Exploiting Software: How to Break Code* and *Rootkits: Subverting the Windows Kernel*, both from Addison-Wesley). Greg is a long-time game hacker and spends much of his free time reverse engineering and tooling exploits for new games. Professionally, Greg offers in-depth training on rootkit development and software exploits. He is currently CEO of HBGary, Inc. (www.hbgary.com), building a world-class product for software reverse engineering and digital forensics.

Gary McGraw is the CTO of Cigital, Inc., a software security and quality consulting firm with headquarters in the Washington, D.C., area. He is a globally recognized authority on software security and the author of six best-selling books on this topic. The latest, *Software Security: Building Security In*, was released in 2006. His other titles include *Java Security* (Wiley), *Building Secure Software* (Addison-Wesley), and *Exploiting Software* (Addison-Wesley). He is the editor of the Addison-Wesley Software Security Series. Dr. McGraw has also written more than 90 peer-reviewed scientific publications, writes a monthly security column for darkreading.com, and is frequently quoted in the press. Besides serving as a strategic counselor for top business and IT executives, Gary is on the advisory boards of Fortify Software and Raven White. His dual Ph.D. is in cognitive science and computer science from Indiana University where he serves on the Dean's Advisory Council for the School of Informatics. Gary is an IEEE Computer Society Board of Governors member and produces the monthly Silver Bullet Security Podcast for IEEE Security & Privacy magazine.

Excerpt. © Reprinted by permission. All rights reserved.

Online games, including World of Warcraft, EverQuest, Second Life, and online poker, have taken the computer world by storm. Gaming has always been (and remains) among the prime drivers of PC technology, with deep penetration into the consumer market. In the last ten years, computer games have grown just as quickly as the Internet and can now be found in tens of millions of homes.

The Internet is experiencing plenty of adolescent growing pains along with its phenomenal growth. These pains are experienced mostly in terms of problematic and pervasive computer security issues. Online games, especially massively multiplayer online role-playing games (or MMORPGs for short), suffer from these security problems directly.

MMORPGs are made of very sophisticated software built around a massively distributed client-server architecture. Because these games push the limits of software technology, especially when it comes to state and time (not to mention the real-time interaction of hundreds of thousands of users), they are particularly interesting as a case study in software security. In fact, MMORPGs are a harbinger of technical software security issues to come. Modern software of all kinds (not just game software) is evolving to be massively distributed, with servers interacting with and providing services for thousands of users at once. The move to Web Services and Service Oriented Architectures built using technologies like AJAX and Ruby follows hard on the heels of online games. What we learn here today is bound to be widely applicable tomorrow in every kind of software.

Adding to the urgency of the security problem is the fact that online games are big business. The most popular MMORPG in the world, World of Warcraft by Blizzard Entertainment, has over 8 million users, each of whom pay $14 per month for the privilege of playing. Analysts estimate the gaming market will reach $12 billion by 2009.

Inside the virtual worlds created by MMORPGs, simple data structures come to have value, mostly a reflection of the time gamers spend playing the game. Players accumulate and trade virtual wealth (or play money). Many of these virtual economies have per capita GDPs greater than most small nations. Not surprisingly, direct connections between the virtual economies of games and the real economy exist all over the place. Until recently, it was possible to buy in-game play money with real dollars on eBay; now many other well-developed middle markets exist. And the reverse is possible, too. This has led to the emergence of a class of players more interested in wringing virtual wealth out of the game than playing the game itself.

Wherever money is at stake, criminals gather and linger. Cheating happens. In the case of MMORPGs, cheaters have real economic incentive to break the security of the game in order to accumulate virtual items and experience points for their characters. Many of these items and even the characters themselves are then sold off to the highest bidder.

Sophisticated hackers have been working the fertile fields of MMORPGs for years, some of them making a living directly from gaming (or cheating at gaming). This book describes explicitly and in a technical way the kinds of attacks and techniques used by hackers who target games.

Why Are We Doing This?

As you can imagine, game companies take a dim view of cheating in their games. If cheating becomes rampant in a game, unsatisfied noncheating players will simply move on to another. Game developers have taken a number of steps to improve security in their games, some of them controversial (monitoring game players' PCs behind the scenes), others legalistic (imposing strict software license agreements and terms of use), and some of them trivial to break (using symmetric cryptography but including the secret key in the game client code). Our hope is that by understanding the kinds of attacks and hacking techniques described in this book, game developers will do a better job with online game security.

We think our topic is important for several reasons: First, real money is at stake; second, many players are completely unaware of what is going on; and third, online game software security has many critical lessons that we can directly apply to other, more important software. Plus, it's fun and controversial.

For example, some game companies have been known to use stealthytechniques most often seen in rootkits to monitor gamers' PCs. They havealso been known to resort to strong-arm tactics to suppress hackers, eventhose not attempting in any way to be malicious or to make money. Willmanufacturers of other software or digital content adopt these techniquesfor themselves?

Not only are the technical issues captivating, the legal issues surrounding online games and their creative software license terms are also a harbinger of things to come. The legal battles between game companies, academics, and users are by no means over--in fact, they have just begun.

In the end, the topic of online game security poses a number of interesting questions, the most pressing one being this: How do you balance gamers' privacy rights against game developers' desires to prevent their games from being hacked?

Where Do We Draw the Line?

For the record, we do not condone cheating, malicious hacking, or any other game-related shenanigans. We are most interested in deeply understanding and discussing what's going on in online game security. As practical security experts, we believe that only by gaining direct technical understanding of what happens when games are exploited can we begin to build systems that can withstand real attacks. Because in this situation money is at stake, you can be sure that attacks and exploits today are both concerted and organized.

We think it is acceptable and necessary to understand both how games really work and how they fail. The only way to do this is to study them carefully. We pull no punches technically in this book, showing you how online game clients fail from a security perspective in living detail. We also explicitly describe techniques that can be used to exploit online games. We don't do this to create an army of online game hackers--that army is already brimming in numbers, and those already enlisted in it are unlikely to learn much from this book. We do this so that the good guys will know what they are really up against. Our main objective is to describe the kinds of weapons the existing active army of game attackers has.

In our research for this book, we have broken no laws. We expect our readers likewise not to break the law using the techniques we describe.

What's in the Book?

Like most books, this book starts out at a high level and becomes progressively more technical as it goes on.

Chapter 1, Why Games?, poses and answers some simple questions. How big are online games? How many people play? Why would anyone want to exploit them? What motivation is there to cheat in an online game? The answers to these questions will likely surprise you. Believe it or not, 10 million people play online games, billions of dollars are at stake, and some people even cheat for a living. We also provide a gentle introduction to game architecture in Chapter 1, describing the classic client-server model that most games use.

Things get more technical beginning in Chapter 2, Game Hacking 101, where we describe the very basics of game hacking. The chapter is organized around describing six basic techniques: (1) building a bot, (2) using the user interface, (3) operating a proxy, (4) manipulating memory, (5) drawing on a debugger, and (6) finding the future. We pay special attention to the topic of bots since most game exploits exist to create and operate them. Late in the chapter, we even show a very simple bot that we built so you can see exactly what bot software looks like. We then describe controversial moves taken by one game maker to thwart cheating--installing rootkit-like spyware on a gamer's PC to keep track of what's going on. We hold this approach in low opinion and have written a program to help you know what's going on with these monitoring programs on your own machine. We believe game makers would be better off spending their resources to build games that were less broken than to build monitoring technology.

The next two chapters take a break from technical material to cover money and the law. In particular, Chapter 3, Money, helps us understand why some players might want to cheat. The recent book Play Money by Julian Dibbell (Basic Books, 2006) describes one (pathetic) man's foray into professional game farming, something that a number of people actively pursue. There is enough money in play here that entire enterprises have grown up around providing middleman services for gamers, buying and selling virtual items in a marketplace. The biggest and most interesting company, Internet Gaming Entertainment, known as IGE to most people, deserves and gets a treatment of its own in this chapter.

Chapter 4, Enter the Lawyers, is about the law. Game companies (and indeed a whole host of other software makers) have created a licensing jungle in the form of end user license agreements (EULAs) and terms of use (TOU) documents. Though we are not lawyers, and by no means should you rely on our advice, we provide a brief description of U.S. copyright law and the Digital Millennium Copyright Act (DMCA). Then we go through an entertaining (and somewhat scary) parade of EULAs gone bad--from Sony's rootkit debacle to viruses protected by EULAs. We end up with a discussion of your rights as a software user and gamer.

Technical aspects of online game security begin to pick back up in Chapter 5, Infested with Bugs. We spend this chapter talking about the kinds of vulnerabilities found in many games, explaining how attackers use

them to build working exploits. We pay particular attention to bugs involving time and state, which, as we alluded to earlier, are the kinds of bugs we can expect to see much more of as other software evolves to become more like game software.

Chapter 6, Hacking Game Clients, really digs in and gets technical. As we move more deeply into games, we are forced to use a game or two as a particular target. We don't do this to single out any one game; instead, we do this to make our examples salient and technical. We have chosen to concentrate on World of Warcraft (WoW), a game produced by Blizzard Entertainment, mostly because it is the number one online game in the world. The kinds of techniques we demonstrate using WoW as an example can be applied by analogy to almost any online game (and to modern Web 2.0 software, for that matter). Chapter 6 begins with a discussion of the attacker's toolkit (many of the tools we describe are standard software testing tools). We then organize our discussion of game hacking techniques into four equally important areas: (1) getting over the game by using its user interface directly, (2) getting inside the game by manipulating memory, (3) getting under the game by interposing on services like video drivers, and (4) getting way outside the game by intercepting and manipulating network traffic.

Chapter 6 is in some sense the heart of the book, introducing a large number of techniques commonly used by game attackers. Chapter 6 has lots of data in it, probably too much. Sometimes it is easier to understand these kinds of techniques by seeing how they are put into practice. Toward that end, in Chapter 7, Building a Bot, we put together all of the lessons of Chapter 6. Chapter 7 is technical, with plenty of example code showing how the ideas in Chapter 6 work in concert to exploit a game.

Chapter 8, Reversing, is even more technical, focusing its attention on reverse engineering techniques that many attackers use to exploit software. Though the techniques we describe in this chapter are intense, they are by no means new. As we describe in our book *Exploiting Software* (Addison-Wesley, 2004), disassemblers and decompilers are used in computer security every day, both by good guys and by bad guys.

The final technical topic in our book is presented in Chapter 9, Advanced Game Hacking Fu. This chapter discusses what is known in the trade as total conversions and game mods. We describe the process by which some people take apart game data files in order to build their own games or combine different aspects of games in interesting ways. Though some game companies try hard to quash all discussion of total conversion, it happens anyway. We describe how.

Of course, our purpose in this book is to help those who build games understand how to do a better job with security. Chapter 10, Software Security Über Alles, provides a flyover of the new field of software security. Game developers would do well to adopt some of the best practices in common use in the financial vertical today. We also describe a set of questions that everyday gamers can ask their game companies about security. Our fervent hope is that this book will lead to more secure software--both in the game community and beyond.

The Software Security Series

This book is part of the Addison-Wesley Software Security Series of software security books for professional software developers. The series includes the following titles:

- *Exploiting Online Games: Cheating Massively Distributed Systems*
- *Secure Programming with Static Analysis*
- *Software Security: Building Security In*
- *Rootkits: Subverting the Windows Kernel*
- *Exploiting Software: How to Break Code*
- *Building Secure Software: How to Avoid Security Problems the Right Way*

Users Review

From reader reviews:

Elena Sparrow:

The actual book Exploiting Online Games: Cheating Massively Distributed Systems has a lot details on it. So when you make sure to read this book you can get a lot of help. The book was compiled by the very famous author. The writer makes some research ahead of write this book. This book very easy to read you will get the point easily after reading this article book.

Louise Suttle:

Playing with family within a park, coming to see the ocean world or hanging out with friends is thing that usually you have done when you have spare time, then why you don't try matter that really opposite from that. A single activity that make you not sensation tired but still relaxing, trilling like on roller coaster you have been ride on and with addition associated with. Even you love Exploiting Online Games: Cheating Massively Distributed Systems, you may enjoy both. It is good combination right, you still desire to miss it? What kind of hang type is it? Oh seriously its mind hangout people. What? Still don't obtain it, oh come on its called reading friends.

Kermit Moors:

Reading a book for being new life style in this 12 months; every people loves to study a book. When you go through a book you can get a large amount of benefit. When you read publications, you can improve your knowledge, mainly because book has a lot of information upon it. The information that you will get depend on what forms of book that you have read. If you would like get information about your analysis, you can read education books, but if you want to entertain yourself you can read a fiction books, these us novel, comics, in addition to soon. The Exploiting Online Games: Cheating Massively Distributed Systems provide you with new experience in reading through a book.

Deborah Fishman:

Do you like reading a reserve? Confuse to looking for your best book? Or your book has been rare? Why so many problem for the book? But just about any people feel that they enjoy regarding reading. Some people likes looking at, not only science book but novel and Exploiting Online Games: Cheating Massively Distributed Systems as well as others sources were given understanding for you. After you know how the truly amazing a book, you feel want to read more and more. Science book was created for teacher or students especially. Those textbooks are helping them to put their knowledge. In various other case, beside science publication, any other book likes Exploiting Online Games: Cheating Massively Distributed Systems to make your spare time a lot more colorful. Many types of book like here.

Download and Read Online Exploiting Online Games: Cheating Massively Distributed Systems By Greg Hoglund, Gary McGraw #WTN8IGY14CF

Read Exploiting Online Games: Cheating Massively Distributed Systems By Greg Hoglund, Gary McGraw for online ebook

Exploiting Online Games: Cheating Massively Distributed Systems By Greg Hoglund, Gary McGraw 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 Exploiting Online Games: Cheating Massively Distributed Systems By Greg Hoglund, Gary McGraw books to read online.

Online Exploiting Online Games: Cheating Massively Distributed Systems By Greg Hoglund, Gary McGraw ebook PDF download

Exploiting Online Games: Cheating Massively Distributed Systems By Greg Hoglund, Gary McGraw Doc

Exploiting Online Games: Cheating Massively Distributed Systems By Greg Hoglund, Gary McGraw Mobipocket

Exploiting Online Games: Cheating Massively Distributed Systems By Greg Hoglund, Gary McGraw EPub