# Securing Online Games

## Safeguarding the Future of Software Security

Gary McGraw
Cigital

Ming Chow
Tufts University

Exploiting Online Games, a book that one of us (McGraw) coauthored with Greg Hoglund, identifies three major threads that together make online game security a captivating subject—money and virtual economies, the nascent state of the law, and thorny technical issues surrounding massively distributed software systems.[1] This special issue covers all three threads.

### Games Aren't Just for Fun

The article "Walking on Water: A Cheating Game Study" (pp. 20–22) by Aaron Portnoy and Ali Rizvi-Santiago shows that games are, in fact, fun. Not only that, game hacking is fun, too.

By exploiting the fact that many games are designed with lots of client-side exposure, cheaters, hackers, and security researchers can cause games to exhibit unintended and often entertaining consequences. As an example, Portnoy and Rizvi-Santiago show how to exploit Disney's Pirates of the Caribbean game to let a character jump miles above the ground, fly, or even walk on water.

This work provides some idea of what happens when game designers ignore trust boundaries. Because most online games are massively distributed systems, designers often place too much essential functionality on the wrong side of a critical trust boundary—right on the very machine of a potential attacker. This kind of exposure is becoming more common as all kinds of software systems become ever more distributed.

### Virtual Economies Drive Cheating

Although the Pirates of the Caribbean hack is all innocent fun, many game hacks have much more nefarious aims. The Web-only feature "How World of Warcraft Almost Ruined My Credit Rating" by Chet Ignatowski offers a whimsical cautionary tale (see http://www2.computer.org/cms/Computer.org/dl/mags/sp/2009/03/extras/msp2009030011s.pdf).

In *Exploiting Online Games*, Hoglund and McGraw describe the financial benefits to be derived from hacking online games. Consider the economics of Blizzard's World of Warcraft (WoW). The game's virtual economy is impressive, rivaling the size in terms of gross domestic product per capita of many real-world countries. The WoW economy is directly interconnected with the real economy through a series of middle market companies that allow for currency exchange, the sale of virtual items, and, more generally, the monetization of gameplay. The upshot? Cheating can be directly monetized.

Cheating isn't the only way to benefit from virtual game economies. Gameplay itself is a weak form of wealth creation because virtual items and experience points have real value. By parallelizing gameplay in a sweatshop, third-world economics can be leveraged to create and monetize virtual wealth on a factory scale. In this case, a set of professional gameplayers earn a "living wage" to play the game, but their actions create more virtual wealth value than what they're paid.

Because cheating can be monetized, and because sweatshops seek to maximize virtual wealth creation, there's much activity in the black market surrounding systems for cheating in an undetectable manner. The technical arms race is in full swing.

## And It's Not Even against the Law

Once we understand the economics of cheating and other game hacking, it's important to take a look at the law. We're honored to include an article by the preeminent attorney working on online games and the law, Sean F. Kane (pp. 23–28).

His article, "Virtual Judgment: Legal Implications of Online Gaming," explains the state of flux that currently exists in online game law. Tricky, unresolved issues surrounding intellectual property, virtual wealth, hacking, property law, contracts, and the ubiquitous end user license agreement (EULA) exist. The legal implications of exploiting online games change every day, and the cases themselves are incredibly interesting.

As one example, consider what happens when a huckster sets up a virtual bank in Second Life and takes hundreds of thousands of dollars worth of deposits (in Linden dollars, of course), then promptly folds up shop and absconds with the money. If you thought banking regulation in the US was lax, check out the apparent utter lack of regulation inside online games! (For more examples, google "Ginko Financial.")

## Securing Massively Distributed Software Systems

We've now established that at least two very basic reasons make exploiting online games attractive—real money to be made and half-baked law. But we shouldn't overlook a third piece of the puzzle—thorny technical issues. Ultimately, we face the usual trade-offs when it comes to online game security. Massively distributed systems that push lots of state information around impose very real reliability and performance constraints on designers. There are important reasons for locating aspects of game computation outside of trust boundaries on gamers' boxes. And yet doing so involves taking on serious security risk.

We alluded to what's possibly the most important issue in securing online games (client-side exposure) in our discussion of the Pirates of the Caribbean hack, but many very real technical security concerns surround online games. "Reducing the Attack Surface in Massively Multiplayer Online Role Playing Games" by Stephen Bono, Dan Caselden, Gabriel Landau, and Charlie Miller (pp. 13–19) covers some of them.

Just as important as the notion of producing superior design is the notion of including countermeasures to thwart cheating. "Server-Side Bot Detection in Massively Multiplayer Online Games" by Stefan Mitterhofer, Christian Platzer, Christopher Kruegel, and Engin Kirda (pp. 29–36) makes headway in this direction. The sweatshops we mentioned earlier rely on bots to automate aspects of virtual wealth creation, so solving the bot-detection problem is a top priority.

## How about Some Science?

A few of us (including readers of this magazine) hold out hope that computer security still involves science in some capacity, or at least that it should. Hard-core computer security researchers will find the beginnings of a scientific framework for understanding online game cheating in "An Investigation of Cheating in Online Games" by Jeff Yan and Brian Randell (pp. 37–44).

Science is definitely called for because in our view, massively distributed online games are a bellwether for problems to come in software security. As cloud computing, service-oriented architecture, and Web 2.0 take off, we can expect to grapple with very similar technical issues to those currently facing online games. □

### Reference

1. G. Hoglund and G. McGraw, *Exploiting Online Games: Cheating Massively Distributed Systems*, Addison-Wesley Software Security Series, 2008.

***Gary McGraw** is CTO of Cigital and the author of* Exploiting Online Games *(Addison-Wesley, 2007),* Software Security: Building Security In *(Addison-Wesley, 2006),* Exploiting Software *(Addison-Wesley, 2004),* Building Secure Software *(Addison-Wesley, 2001), and five other books. He has a BA in philosophy from the University of Virginia and a dual PhD in computer science and cognitive science from Indiana University. Contact him at gem@cigital.com.*

***Ming Chow** is an instructor at Tufts University's Experimental College and its Department of Computer Science. His areas of interests are computer security, game development, and human-computer interaction. Chow has a BS and an MS in computer science from Tufts University. He's also a SANS GIAC Certified Incident Handler (GCIH). Contact him at mchow@cs.tufts.edu.*