Foreword

It's wise to learn from your mistakes. It's wiser still to learn from the mistakes of others. Too often, we in the security community fail to learn from mistakes because we refuse to talk about them or we pretend they don't exist.

This book talks frankly about game companies' mistakes and their consequences. For game companies, this is an opportunity to learn from their own mistakes and those of their peers. For the rest of us, it's an opportunity to learn what can go wrong so we can do better.

The debate over full disclosure goes back a long way, so there is no need to repeat the ethical and legal arguments we have all heard before. For most of us in the security community, the issue is simple: Experts and the general public both benefit from learning about the technologies that they depend on.

In today's world, we are asked all the time to bet our money, our time, our private information, and sometimes our lives on the correct functioning of technologies. Making good choices is difficult; we need all the help we can get.

In some fields, such as aviation security, we can be confident that problems will be identified and addressed. Nobody would tolerate an aircraft vendor hiding the cause of a crash or impeding an investigation. Nor would we tolerate a company misleading the public about safety or claiming there were no problems when it knew otherwise. This atmosphere of disclosure, investigation, and remediation is what makes air travel so safe.

In game design, the stakes may not be as high, but the issues are similar. As with aviation, the vendors have a financial stake in the system's performance, but others have a lot at stake, too. A successful game—especially a virtual world like World of Warcraft—generates its own economy, in several

senses. Objects in the game have real financial value, and a growing number of people make their living entirely or partially via in-game transactions. In-world currency trades against the dollar. Economists argue about the exact GDP of virtual worlds, but by any meaningful definition, virtual economies are just as "real" as the NASDAQ stock exchange.

Even nonplayers can have a lot at stake: the investor who bets his retirement account on a game company, the programmer who leaves a good job to work on a game, the family that owns the Indian restaurant across the street from the game company's headquarters. These people care deeply about whether the technology is sound. And would-be customers, before plunking down their hard-earned money for game software or a monthly subscription, want to know how well a game will stand up to attack.

If aviation shows us the benefits of openness, e-voting illustrates the harms caused by secrecy. We, the users of e-voting systems—citizens, that is—aren't allowed to know how the machines work. We know the machines are certified, but the certification process is itself shrouded in mystery. We're told that the details aren't really our concern. And the consequences are obvious: Designs are weak, problems go unfixed for years, and progress is slow. Even when things do go wrong in the field, it's very hard to get a vigorous investigation.

The virtue of this book is not only that it talks about real-world problems but also that it provides details. Some security problems exist only in theory but evaporate when real systems are built. Some problems look serious but turn out not to be a big deal in practice. And some problems are much worse than they look on paper. To tell the difference, we need to dig into the details. We need to see precisely how an attack would work and what barriers the attacker has to get over. This book, especially the later chapters, offers the necessary detail.

Because it touches on the popular, hot topic of massively multiplayer games, and because it offers both high-level and detailed views of game security, this book is also a great resource for students who want to learn how security really works. Theory is a valuable tool, but it does its best work when wielded by people with hands-on experience. I started out in this field as a practitioner, trying to learn how to get things done and how real systems behaved, before expanding my horizon to include formal computer science training. I suspect that many senior figures in the field would say the same. When I started out, books like this didn't exist (or if they did, I didn't know about them). Today's students are luckier.

Perhaps some vendors will be unhappy about this book. Perhaps they will try to blame the authors for the insecurity of their game software. Don't be fooled. 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.

We all make mistakes. Let's learn from our mistakes and the mistakes of others. That's our best hope if we want to do better next time.

—*Professor Edward Felten*
Princeton, New Jersey
June, 2007