Preface

INTRODUCTION

The virtual realm is upon us. Face to face meetings, sequestered retreats, and international conferences are becoming relics of the past. Instead, the connectivity supplied via a vast interconnected network is providing, among other conveniences, the virtual space to interact on projects via Google documents (Google, 2010), deploy robust software applications via a Web interface, or meet with avatars to produce working prototypes in minutes rather than months.

Yet this new frontier of nearly unlimited connectivity comes with unknown risks and challenges. The corporate world would never conduct its business on a subway or in a sports arena. Similarly, it must be assiduous in protecting sensitive information created and stored in virtual space. For example, can we trust Office Live (Microsoft, 2010) to protect proprietary data? Or should we conduct all business processes using software not installed on local machines? And how can we know avatars are who they say they are?

Moreover, determining how to interact with virtual realms and 3D Web environments can be perilous. Do we adhere to open standards and promote a free exchange of information? Or do we develop proprietary solutions that benefit distinct market segments? Finding a middle ground may avoid a recurrence of the "browser wars" of the mid-90s. Nonetheless, data and resources, whether intellectual property, people or business processes, must be protected from unscrupulous elements in cyberspace.

This book explores the promises and navigates the pitfalls of online interaction. It provides the approaches, discussions, frameworks and insights that will allow organizations and individuals to understand the immersive environments thriving online. We will explore how organizations can safely share and exchange data as well as interact in virtual realms to accomplish goals such as creating commerce or educational opportunities. With careful planning and an understanding of the virtual realm, organizations can guard against unintentional security incidents, as well as malicious user behavior.

WHY THIS BOOK NOW?

The concept of virtuality as represented in the 3D Web, immersive environments, and most recently virtual worlds such as Second Life (Linden Labs, 2010), permeates discussions of business, society, and culture. Undoubtedly we are moving into the next phase of interaction propelled at the same speed or faster than the Web revolution itself (Internet Society, 2010; Leiner, Cerf, Clark, Kahn, Kleinrock, Lynch, Postel, Roberts, & Wolff, 1997).

Although scholarly and popular publications have discussed and studied the usability, features, and functionality of the Web and, by extension, the 3D Web, little has been published on the complexities of creating a secure environment, except to note when attacks have occurred. Discussion is especially warranted when sensitive business data is manipulated via these applications. Risks of using social computing applications for business--or within a business environment--must be examined. Viruses embedded in Facebook (Arrington, 2008; Symons, 2010) are just the beginning of potential compromises. With the influx of interconnected communications comes easier phishing attacks via embedded hyperlinks or VoIP hacks to re-direct communications or intercept sensitive data.

Virtual worlds face security threats as well. Multi-user Virtual Environments (MuVE) are rife not only with technical exploits to glean sensitive data (Sastry, 2007) but also social engineering practices that routinely are used to acquire personal and business information and thus exploit both virtual and physical assets. Instances abound of users offering personal information to a "helpful" virtual citizen who then maliciously creates a profile linked to the real world (Brooke, Paige, Clark, & Stepney, 2004).

Alternatively, organizations once ready to move into public virtual realms, such as Second Life (Linden Labs, 2010), have measured virtual realm risks and have elected to create their own realms for improved security and protection of sensitive business data. IBM has stated that although it realizes the immense potential for virtual collaboration, it has opted to build its own realm for confidentiality and information assurance (Dignan, 2007). This initiative has created OSGrid (2010), an open source alternative to Second Life that allows an organization to create and maintain its own virtual world and to connect (or disconnect) it to others according to organizational policies and risk acceptance.

Although brief, these examples suggest great change and challenges in the digital realm. No longer just a place to check sports scores or weather, the Web is morphing into a realm both beyond, and intertwined, with the physical world. As people and organizations become interconnected, so too does the challenge of educating the Internet populace not only in acceptable interaction with others but also in the risks therein.

Moreover, those planning, deploying, and managing these offerings must be aware of the implications of doing so. Design and policy choices can affect online users at an exponential rate. This book attempts to provide researchers, practitioners, students, and users the knowledge and skills to plan, deploy, manage, and maintain robust and safe virtual realms as well as effectively interact within them.

WHAT TO EXPECT IN THIS BOOK

Our discussion begins with an overview of privacy infractions that can occur in virtual worlds. Roldan and Rea define these transgressions and suggest technological, behavioral and policy solutions. Next Sivan suggests a means to protect and manage one's virtual identity. His "3D3C Identity" enables users to participate in virtual worlds according to their own privacy and security preferences. From these discussions emerges a broader topic: the security risks that virtual environments bring to society. Jirovský examines behavioral anomalies in virtual communities, specifically those that might foster illegitimate uses and attacks.

Moving next to applications within virtual realms, Faramand and Spafford contemplate how organizations can manage and mitigate risk. The authors posit that only after organizations identify their unique risks can they successfully develop policies and implement procedures to reduce risk and enhance trust within virtual realms. Next Hai-Jew identifies how virtual teaching and learning environments have

security risks beyond those of brick and mortar classrooms. Using social design principles, Hai-Jew provides guidelines and techniques to mitigate security risks in this socio-technical virtual space.

Discussion of these powerful virtual realms extends next to the shared governance principles within successful Second Life communities. Johnston's detailed case study examines how a large virtual community uses social governance to manage community relationships and protect its members. The author evaluates which governance strategies work within a particular virtual community. Next Grimaldo, Lozano, Barber, and Orduna complement this discussion by examining the social behaviors that can be simulated in virtual realms to enhance the realness and interaction for participants. The authors provide theoretically informed guidelines for creating a sociability model for multi-agent systems.

Shifting to the technical side, the authors focus on security frameworks, objects, and programming challenges within virtual worlds. Bogdanovych and Simoff deploy a virtual worlds methodology to develop frameworks that specify normative institutional rules and design parameters. This formal specification permits the codification and enforcement of social norms and interactions within controlled virtual worlds. Virtual worlds also require safeguards for the objects with which participants need to interact. Reiners, Wriedt and Rea discuss an object-oriented architecture, termed the Global Object Management System (GOMS). This system not only can manage all objects within a virtual world but also allow each object to move among worlds adhering to copyright protections set by the object's owner. Using a multi-layered set of permissions and access controls, the authors' architecture will improve the security and protection of objects, thus encouraging development without relinquishing control of intellectual property.

Like virtual worlds, the World Wide Web also needs increased security measures as it morphs into a 3D-distributed network far too advanced for a standard SSL-encrypted transmission. Turning to the Web, Kloss and Schickel consider how the extensible 3D (X3D) specification may bring secure 3D object exchanges to organizations. X3D is the ISO/IEC standard for virtual world objects, can be implemented using open standards, and enables the use of well-known languages such as XML. Using X3D, the authors present a business case involving Bitmanagement, one of the leaders of interactive Web3D graphics software. In another approach to securing 3D Web transactions, Safonov focuses on aspect-oriented programming (AOP) and Aspect. NET. The author illustrates how his Aspect .NET development framework ensures 3D Web security and privacy and increases trustworthiness in sensitive transactions.

In our final chapters, Walczak explains how the Flex-VR environment allows granular control both of objects and the encompassing content model to create secure, yet malleable, virtual environments. Using VR Beans, developers can create semantically rich content that allows users and groups to have fine access control. Wójtowicz and Cellary extend this concept with their Virtual Reality–Privilege Representation, which allows for fine control of object interactions. Using illustrative cases, the authors demonstrate secure object interaction controlled via a series of meta-operations generated to dynamically create and modify object privileges.

WHERE DO WE GO FROM HERE?

Security research in virtual worlds, the 3D Web, and immersive environments is in its infancy. Yet security is paramount when millions of users interact in persistent virtual realms (Biancuzzi, 2007) such as World of Warcraft (Blizzard Entertainment, 2010). Just as Second Life has its security challenges, so too does the growing population of online gaming communities that reflect a microcosm of the larger economic, social, and cultural strata as well.

One book cannot hope to answer everything within this diverse scholarly discourse. We have written about pedagogy, privacy, virtual object management, and coding secure 3D Web frameworks. Perhaps we have left readers with more questions than answers. But, if you have been challenged to take on these issues, then we have accomplished our goal. Although each author comes from a different discipline, we agree that this burgeoning field demands more critical scholarship and informed application development.

ACKNOWLEDGMENT AND THANKS

Much thanks must go out to my family. Those closest to me realize that my staring at a screen for countless hours can have academic merit. And, lucky for me, life with them is still far more adventurous than virtual reality.

As for those who helped in the creation of this book, I have enjoyed pondering along with you the complexities that the virtual brings into our midst. Our team communicated via discussion lists, Web boards or virtual worlds, so I would not recognize many of them on the street. It's just another irony of our new reality.

Foremost, the authors of these chapters have been my colleagues over the course of this book. Already a few of us are collaborating on new projects as a result of our conversations. It was a pleasure be a part of your latest contributions to this new field of study.

I would be sorely remiss if I did not thank the Editorial Board for its assistance. Its members were always willing to look at "one last thing" from me, whether proposals or polished chapters. They regularly offered input, advice, and encouragement when needed. So thank you Doug, Glenn, Guido, Heinz, Lech, Malu, Mex, Rich, and Torsten.

Finally, I wanted to thank IGI Global for supporting this project. In particular, thanks to my development editor, Joel Gamon, for his patience with a new book editor throughout the process.

REFERENCES

Arrington, Michael. (2008). Elaborate Facebook Worm Virus Spreading. *TechCrunch*. Retrieved August 31, 2008 from http://www.techcrunch.com/2008/08/07/elaborate-facebook-worm-virus-spreading/

Biancuzzi, Federico. (2007). Real Flaws in Virtual Worlds. *SecurityFocus*. Retrieved September 1, 2008 from http://www.securityfocus.com/columnists/461

Blizzard Entertainment. (2010). *World of Warcraft* [Computer Software]. Retrieved from http://worldofwarcraft.com/

Brooke, P. J., Paige, R. F., Clark, J. A., and Stepney, S. (2004). Playing the Game: Cheating, Loopholes, and Virtual Identity. *SIGCAS Comput. Soc. 34*(2), 3.

Dignan, Larry. (2007). IBM Cooks Up Internal Virtual World for Confidentiality, Security. *ZDNet*. Retrieved August 31, 2008 from http://blogs.zdnet.com/BTL/?p=7382

Google. (2010). *Google Docs* [Computer Software]. Retrieved from http://docs.google.com

Internet Society. (2010). Histories of the Internet. Retrieved January 17, 2010 from http://www.isoc.org/internet/history/

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., and Wolff, S. S. (1997). The past and future history of the Internet. *Commun. ACM 40*(2), 102-108.

Linden Labs. (2010). *Second Life* [Computer Software]. Retrieved from http://secondlife.com/

Microsoft. (2010). *Office Live* [Computer Software]. Retrieved from http://www.officelive.com/

OS Grid. (2010). *OSGrid* [Computer Software]. Retrieved from http://www.osgrid.org/elgg/

Sastry, A. (2007). Security in Virtual Worlds: Blurring the Borders. *TechNewsWorld*. Retrieved August 31, 2008 from http://www.technewsworld.com/story/59399.html

Symons, S. (2010). Facebook Employee Interview Reveals Security Issues. *NeoWin*. Retrieved January 17. 2010 from http://www.neowin.net/news/main/10/01/12/facebook-employee-interview-reveals-security-issues

Alan Rea
Western Michigan University, USA