book reviews

BRANDON CHING AND SAM STOVER

THE SECOND LIFE GRID: THE OFFICIAL GUIDE TO COMMUNICATION, COLLABORATION, AND COMMUNITY ENGAGEMENT

Kimberly Rufer-Bach

Sybex Publishing, 2009. 368 pp.
ISBN 978-0470412916

REVIEWED BY BRANDON CHING

To the uninitiated, Second Life can be somewhat of a mystery. Most people that I have talked to about Second Life have heard of it, maybe have even tried it once or twice, but generally don't know much beyond that. While Second Life can serve whatever use the individual user wants it to, organizations from academia, government, business, and the nonprofit sector have for years been trying to gain a foothold in one of the most popular virtual worlds.

Unfortunately, these organizations have struggled to maintain a meaningful presence in Second Life and the challenges they have faced have been dynamic and difficult to identify. Enter Kimberly Rufer-Bach, whose *Second Life Grid* was written to identify and help organizations surmount these challenges.

The book has three parts and fifteen chapters in all. Part 1 introduces Second Life and outlines the effects that government, nonprofits, and educational institutions can achieve in-world. These chapters are full of real examples of organizations creating a successful presence in Second Life. While a little light on practical advice, this section is full of resources that any organization new to Second Life should find useful.

Part 2 covers in-world cultural issues and guides the reader through merging organizational culture with the norms and customs of the Second Life world. I found this to be the most important section of the book. Any organization embarking on a new venture needs to know as much as it can about the environment it is entering. The author provides valuable insights into topics such as etiquette, communication, avatar appearance, and current events.

Finally, Part 3 is where you get into the nitty-gritty of building your presence in Second Life. Setting up a virtual office, running an event, marketing, and resource management are all well covered. The remaining six chapters in this section take up roughly half the book and are loaded with expert information. While the technical details of content creation are largely absent from this text (as is appropriate), I cannot begin to express the level of excellent administrative and planning information these chapters contain.

All told, Rufer-Bach is certainly a Second Life expert, and this fact shows itself through the amazing amount of nuanced and valuable information packed into this book. Weighing in at nearly 370 pages, with a relatively small font and covering a very broad topic, this book is not for the faint-of-heart, but don't kid yourself by thinking that you'll be an expert at running a successful event/presence in Second Life after reading this book. Many of Rufer-Bach's recommendations revolve around simply getting your hands dirty and learning first-hand what goes on in Second Life.

While this book is targeted towards organizations seeking an in-world presence, it would also be of value to individuals looking to more fully understand the revolutions that are virtual worlds.

CLOUD SECURITY AND PRIVACY

Tim Mather, Subra Kumaraswamy, and Shahed Latif

O'Reilly Media, 2009. 336 pp.
ISBN 978-0596802769

REVIEWED BY SAM STOVER

As everyone knows, "The Cloud" is the next big thing, but since security always seems to lag behind Big Things, I was pleasantly surprised to find a decent primer on the subject. Weighing in at only 330 some-odd pages, the book seems a bit slight at first, but the authors do a good job within that footprint.

Chapter 1 is a brief, and I mean *brief*, introduction to the topic and a description of how this all came to be. It goes over how ISPs evolved into colos, then ASPs, which set the stage for cloud computing. Chapter 2 goes into the aspects of different

types of cloud computing, as well as some of the players in the game (Google, Amazon, Microsoft, etc.). The SPI framework is introduced: Software as a Service, Platform as a Service, and Infrastructure as a Service (SaaS, PaaS, and IaaS, respectively). Lots of technical jargon here to digest, but more importantly, this sets the stage for Chapter 3, "Infrastructure Security," Chapter 4, "Data Security and Storage," Chapter 5, "Identity and Access Management," and Chapter 6, "Security Management in the Cloud." These four chapters are the meat of what was interesting to me (but surely the audit and policy wonks will jump quickly to Chapter 8, "Audit and Compliance"). Chapter 7, "Privacy," ties in very nicely with the security issues presented in Chapters 3–6.

Being a network guy, I was particularly drawn to the "Infrastructure Security" chapter. The risks are broken down into familiar groups: data confidentiality and integrity, access control, and availability. The cloud-specific spin takes into account the difference between normal network "zones/tiers" and domains. The usual suspects include cleartext HTTP communications between the client and the provider, improper IP caching/reusability, BGP prefix hijacking, and DNS attacks. Also, as with anything Internet-connected, DDoS is always a potential threat. Not content with simply enumerating threats, the authors spend half of the chapter going over security countermeasures for hosts and networks, specific to the different aspects of the SPI framework. This all makes for good reading.

Chapter 9 starts to pull everything together by presenting eight different cloud providers and laying out their offerings. Amazon (IaaS), Google (SaaS, PaaS), Microsoft Azure (PaaS), Proofpoint (SaaS, IaaS), RightScale (IaaS), Salesforce.com (SaaS, PaaS), Sun Open Cloud Platform (all), and Workday (SaaS) are all briefly presented and, to a small degree, compared. I would like to have seen a little more depth in this particular chapter, but in some cases (e.g., Sun), the offerings are pretty new, so it will take some time for everything to fall out. Plus, if I want to be a stickler, this is really a book on *security*—there are plenty of other resources out there if I wanted to learn more about cloud providers and their core competencies.

Chapter 10 broaches the topic of Security as a Service (another SaaS). To this point, a lot of security issues have been discussed, from both the provider and the client sides, using the cloud. Security as a Service, however, can be divided into two main groups: InfoSec vendors who are migrating or encompassing delivery methods utilizing cloud mechanisms, and companies who provide "security only as a cloud service, and do not provide traditional client/server security products for networks, hosts, and/or applications." This was probably my least favorite chapter, but YMMV.

Chapter 11 deals with "The Impact of Cloud Computing on the Role of Corporate IT," and Chapter 12 rounds out the book as the "Conclusion, and the Future of the Cloud." Three appendices—a SAS 70 Report, a SysTrust Report, and "Open Security Architecture for Cloud Computing"—complete the work. The OSACC is a very interesting model devised by the Open Security Architecture group (http://www.opensecurityarchitecture.org/), which attempts to "illustrate core cloud functions, the key roles for oversight and risk mitigation, collaboration across various internal organizations and the controls that require additional emphasis." Whew, that's a mouthful, but it's an interesting read nonetheless.

Overall, this is a solid book both for security folks who want to learn more about cloud computing and for cloud computing users who want to learn more about the security behind the technology. It's pretty obvious that the authors are both passionate and knowledgeable, which is great to see in any book. There's plenty here to learn from, and I sincerely hope that this team of authors keeps putting out new editions as the cloudscape changes.