Volume 5, Issue 1, January 1998

Telecommunications Electronic Reviews (TER) is a publication of the Library and Information Technology Association.

Contents:

ter issues (/lita/publications/archive/ter)

REVIEW OF: Marcus Goncalves. Protecting Your Website with Firewalls. Upper Saddle River, NJ: Prentice Hall, 1997.

by Matthew M. Benzing

The title of this book may lead some of its potential readers to believe that it is a technical manual that describes how to set up and maintain firewalls; in reality, it is both less and more than that. Goncalves does include one chapter on the subject of firewall design and implementation that includes descriptions of some

effective applications of the concept; however, the real focus of the book is on clueing the reader into recognizing the multiple layers of vulnerability that are created when an organization establishes a presence on the Web.

System administrators looking for a thorough treatment of firewalls and their uses would be better off with more specialized works. This book is best seen as an introduction to Web security issues and would be better suited to library systems people who are just getting started on putting together a security program. Library directors with at least an intermediate user's grasp of Internet technology may also want to read this book in order to better understand security issues and to learn how to apply them to Internet policy decisions.

Like most computer security books, Protecting Your Website with Firewalls is targeted at a corporate audience. All of the examples in the book are taken from the world of business, and the types of information that Goncalves is most interested in protecting are primarily financial. Although some libraries may deal with online credit card transactions for services like document delivery and interlibrary loan, for the most part they are not as attractive to online thieves as commercial organizations are.

Libraries do hold information that must be guarded, however, and a poorly designed Web site can provide unauthorized access to patron records, employee passwords, and copyrighted databases--information that in some cases may be just as sensitive and just as dangerous in unauthorized hands. Online vandals may also choose to crack a library site just to make mischief or to use it as a base of operations for an attack on another site.

Just because library networks are not discussed in this book does not mean that they are not subject to the same problems as the business information systems that are covered. Library Web administrators would be wise to try to maintain the same level of security that Goncalves recommends for commercial sites. If there is one point that is made throughout this book it is that no Web site is completely safe, and that all sites should have multiple levels of security so that one breech of the system will not result in an intruder having access to all the files on the network.

One of the strong points of this book is its attention to detail. Goncalves does not make many generalizations; he usually gives very specific examples for most of his points. He describes security holes in a number of popular server software packages and usually specifies which version or release number carries the weakness. Libraries who are just getting started on the Web, or who are taking over control of their own server from a campus computer center, will find this kind of information invaluable in deciding which systems to invest in.

Goncalves also points out specific security flaws in Java and JavaScript and the ways in which these weaknesses could be utilized by malicious parties. Despite the widespread acceptance of these languages, they can contain serious breeches of security (unfortunately, Goncalves does not discuss Active X, which has some even more serious security holes). The weaknesses of CGI (Common Gateway Interface) scripts are also examined in detail, and specific methods for dealing with them are described.

Examples of PERL (Practical Extraction and Report Language) scripts for performing various security procedures are given in their entirety. Again, this is a great help to relatively inexperienced systems people who may have a basic grasp of PERL but are not skilled enough to write useful programs from scratch. The CD-ROM that comes bundled with the book contains shareware versions of several useful security applications such as WebTrends, a utility that helps in monitoring suspicious activity on a Web site, while appendices give annotated lists of a wide variety of software including Web servers, firewall programs,

password testers, system monitors, and patches that fix security problems. The author is also not afraid to make explicit endorsements; at one point he states that from a security standpoint Microsoft Windows NT outperforms UNIX (a statement that many may wish to debate).

Besides the technical issues involved in Web security, Goncalves also addresses the legal issues involved. Legislation continues to trail behind technology, and many of the punishments meted out for Internet crimes seem to be distressingly mild compared to the damage that the criminal may have inflicted. Still, it's important for organizations with a Web presence to know their rights and their ability to bring charges in the rare case when a culprit is nabbed. Goncalves does a good job of not only surveying the current legal situation but also providing contact information for organizations that keep track of the changing nature of Internet law.

Aside from security information, this book provides a lot of good background information on how to set up access to different types of Internet resources through a Web server. Libraries wishing to experiment with virtual reference will find the chapter on Web conferencing particularly interesting. Goncalves discusses several conferencing techniques and packages not only in terms of security, but also in terms of suitability for different sorts of applications. Likewise the chapters on email, FTP (File Transfer Protocol), and newsgroups not only discuss these protocols in terms of security, but also give information on how they work through the Web and on the best ways to set up them up.

This book is written in a popular journalistic style, and the author does not resort to technical language except where necessary. As has already been stated, this is not a security specialist's book, but rather an introduction for readers with some network background who are new to security issues. The practical nature of the advice presented within will be very useful to library systems people who are concerned about the integrity of their Web site.

Matthew M. Benzing is Information Systems Librarian at Rensselaer Polytechnic Institute.

table of contents   ter issues (/lita/publications/archive/ter)

REVIEW OF: Rikk Carey and Gavin Bell. The Annotated VRML 2.0 Reference Manual. Reading, MA: Addison-Wesley Developers Press, 1997.

by David Mattison

Two former employees of Silicon Graphics and principal architects of the VRML (Virtual Reality Modelling Language) 2.0 specification teamed their considerable talents to produce this added-value reference tool for VRML implementors and world creators. While the specification itself is publicly available on the Web, the authors' intimate knowledge and contributions to the development of VRML will assist anyone wishing to gain a deeper understanding of VRML design issues. Extensive design notes, tips, and examples clarify design intentions not readily apparent from the specification itself. The authors warn, nevertheless, that this book is not a VRML tutorial and that their discussion is based on an ideal VRML implementation not necessarily achievable within existing computing environments.

The simplest way to explain VRML, as the authors do, is that it is the three dimensional (3D) equivalent of HTML (Hypertext Markup Language). VRML is not intended to replace HTML or HTTP (Hypertext Transfer Protocol) because one of the design considerations was not to reinvent existing protocols or things better performed outside VRML. Virtual reality modelling on the Web is intended to be scalable so that "it should be theoretically possible for a VRML browser to handle a world distributed across the Internet that contains millions or billions of objects." (p. 4) Like HTML, VRML is not a programming language; both describe the appearance and behavior of their respective objects: text and 3D environments. VRML also serves as a common 3D file exchange format. The authors note that VRML will serve as the foundation for multiuser simulations although the specification does not yet support this level of usage.

The VRML 2.0 specification is expected to be approved and published electronically by the International Standards Organization by the end of 1997. Unlike the somewhat indiscriminate evolution of the hypertext markup language where a standard was agreed upon following intense market competition, VRML's standard seems to be rolling out at a leisurely pace. It's easy to appreciate why this is so since VRML is more complex than HTML. The authors provide in their introduction a fine summary of exactly what VRML is, what it is expected to accomplish, its scalability and integration into almost any graphical computing environment, design factors, and a brief history of VRML from its beginnings at Silicon Graphics in 1989 to the present state of VRML 2.0 nearing ISO approval.

The manual is divided into five chapters followed by eight appendices. An excellent index is included and the book ends with "The VRML Quick Reference"--an odd placement in my opinion for something that might be frequently used. While the differences between VRML 1.0 and 2.0 are discussed throughout the book, the earlier design is not referred to in the index nor is there a table summarizing changes between the two specifications.

Chapters two and three are the heart of the book, with the former covering "Key Concepts," while the latter serves as the "Node Reference." A VRML world is composed of a hierarchical scene graph that consists of entities or nodes. There are 54 node types and 20 field types for use by any one node. New node types beyond the 54 defined in the specification can also be created through a prototype declaration. The fields contain data that define the properties and state of the node as it changes over time through events. Nodes pass data through a route statement, and sensors and scripts determine how events are generated by the user or by the nodes themselves.

The use of Java and JavaScript is detailed in appendices as well as being briefly discussed on page seven. Wherever possible, black and white illustrations are included to clarify the appearance of design issues. The book also includes 17 color plates from a Silicon Graphics application.

The accompanying CD-ROM in HTML format with frames is of great assistance in visualizing how VRML works at the individual component level. The layout is not as pleasing as the printed copy because the "Tips and Design Notes" are not in shaded boxes as they are in the hardcopy. The CD-ROM verson, however, does display in color with "live" examples. Many of the hypertext links in the book are hot links, so you need to pay attention to the message line in your browser window if you are not connected to the Internet.

The contents frame that appears at the top of each of the CD-ROM pages is laid out slightly different than the printed version. Chapter and appendix numbers are not used, and one CD-ROM section titled "References" does not appear at all in the hardcopy. The "Quick Node Reference" on the CD-ROM includes comments on maximum permissible values for fields and events, but this information is not in the book copy. The "Examples" section of the CD-ROM includes links to the examples that can be viewed with a VRML 2.0 compliant browser or authoring software.

In bringing their extensive expertise to this reference work, the authors help put a human face on what is otherwise rather dull and difficult reading. In attempting to follow this work as a novice VRML creator, I felt some topics were not adequately explained. Perhaps the authors assumed the target audience is familiar with 3D graphics rendering, and complex geometries would not need defining. One example is "backface culling" which is applied to certain geometric shapes; the phrase is, however, undefined. One major oversight appears on page 113 where the authors note that only a small number of file formats are supported by VRML; nowhere is there a list of these formats. This work will serve as the definitive reference to the VRML 2.0 draft specification with perhaps a revised edition appearing following ISO approval.

David Mattison (David.Mattison@gems3.gov.bc.ca (mailto:David.Mattison@gems3.gov.bc.ca)) is Reference Archivist at the British Columbia Archives in Victoria, Canada.

table of contents   ter issues (/lita/publications/archive/ter)

About TER