Volume 11, no 5, November 2004

Volume 11, Number 5, November 2004

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

Technology Electronic Reviews (ISSN: 1533-9165) is a periodical copyright © 2004 by the American Library Association.

Contents:

REVIEW OF: Paul Bausch. (2003). *Amazon Hacks*. Sebastopol, CA: O'Reilly.

by Bill Lund

What on earth is there to hack at Amazon? Isn't it just a big bookstore? Interestingly, there are a number of interfaces into the vast data store that comprises the Amazon online retail system. For instance, did you know that you can incorporate purchasing links into Amazon from your

own website and earn a commission on the sales your site referred to Amazon? Did you know that you can link to virtually any image in the Amazon product catalog, selecting the size and format of the image delivered into your website? Did you know that you could control how Amazon views you as a customer, improving the quality of the suggestions that Amazon based on your interests? *Amazon Hacks* provides 100 tips and tools, divided into six chapters, covering roughly: how to better use Amazon to get what you want; how to incorporate Amazon direct links and searches into your own web pages; and how to use the resources of Amazon, such as the huge database of scalable product images and information in your own web context. This book contains everything from simple Amazon user tips to significant coding examples in a variety of languages. Because of the breadth of the offerings, this book may either be considered useful to a wide audience, or trying to do too many things at once.

Amazon Hacks was written by Paul Bausch and published by O'Reilly as a part of the "Hacks" series, which includes, among others, *Google Hacks*, *TiVo Hacks*, *MacOS Hacks*, and *Excel Hacks*. The first question may be, what is a "hack?" The author states: "Among people who write code...the term 'hack' refers to a 'quick-n-dirty' solution to a problem, or a clever way to get something done. And the term 'hacker' is taken very much as a compliment, referring to someone as being creative, having the technical chops to get things done." In this spirit, *Amazon Hacks* provides 100 "quick-n-dirty" solutions to a variety of problems or initiatives that you as a user of Amazon may be interested in.

The scripting languages and examples included in the book are all over the map, including: JavaScript, ActiveX, Windows registry modifications, Perl, PHP, ASP, standard HTML, SOAP, Python, XML, XSL, Microsoft Visual Basic, Microsoft Internet Explorer browser, and the Mozilla browser. In some respects I consider this to be a weakness. Although it is certainly true that each language has its strengths, to require the reader to be conversant in all of these implies a fairly high level of experience. Given that it was beyond the scope of this book to provide background into all of these technologies, the reader is left on his or her own. It would have been interesting for the author to have shared with us why PHP was selected for one example, Perl for another, and ASP for a third. Then, at least, we might be learning of the strengths that recommended each languages' use in the examples. In my opinion it would have been better to have selected a set of technologies, such as those created by Microsoft (Internet Explorer, ActiveX, Windows Registry, ASP) or those sponsored by the open source and standards community (Perl, PHP, HTML) and write the entire book from that perspective. At least then the reader could have been forewarned as to the prerequisite experience the book assumes.

It might be considered a weakness that no CD is included with the book for the thousands of lines of code found in the hacks; however, you can find all of the code examples on-line at http://examples.oreilly.com/amazonhks/ (http://examples.oreilly.com/amazonhks/). Having checked several of the examples, I did find one that did not match the book and was not

functional. Overall, however, the examples were as found in the book. Note also that O'Reilly provides updates and corrections to the book at http://www.oreilly.com/catalog/amazonhks/ (http://www.oreilly.com/catalog/amazonhks/).

Looking at the hacks themselves: Have you ever wanted to incorporate an image from the Amazon catalog into another web page? For example, let's say you're selling an item on eBay and don't want to go to the bother of taking a digital picture and incorporating it into your listing. Hack #5 shows how to pull an image from the Amazon catalog directly into your webpage, changing the size and orientation on the fly. You can even specify whether you prefer JPG or GIF. Let's say you've published a book that is for sale on Amazon and you want to find out how well it is doing. Hack #46 is just the thing. The author explains how to use JungleScan.com to track sales and rankings of books on Amazon. You can either view the overall rankings or select individual items from the entire Amazon catalog to track.

To further enable individuals to integrate Amazon into their own web space, Amazon created a web services application program interface (API) in 2002. These services provide an XML-enabled mechanism to extract data and objects, such as images of products, from Amazon and restructure them within your own web space. For example, you can create your own product catalog, enhancing your website with continuously updated links from Amazon for products that may relate directly to your website's subject. Then, as an Amazon Associate, you may receive a commission on all sales referred from your site. Additionally, there are search terms and sorting criteria that are not available from the standard Amazon site. These are exposed through the API to programmers.

Overall, *Amazon Hacks* is well written, and with the limitations mentioned above, a good buy for anyone interested in managing their Amazon account to greater advantage or using Amazon for personal profit. In addition to being available from the usual libraries and bookstores (including Amazon itself), *Amazon Hacks* is available through O'Reilly's Safari subscription service (not to be confused with the web browser of the same name from Apple Computer). If you haven't checked out Safari on the O'Reilly website (http://safari.oreilly.com (http://www.missingkids.com/cybertip/)), you should. For a yearly or monthly subscription, you will have access to a given number of current books, including *Amazon Hacks*. A very timely and flexible service.

Bill Lund is Assistant to the University Librarian for Information Technology, Harold B. Lee Library, Brigham Young University.

REVIEW OF: Carl Endorf, Eugene Schultz, and Jim Mellander. (2004). *Intrusion Detection & Prevention*. New York: McGraw Hill/Osborne.

by Thomas Raffensperger

Hacking has come a long way from the innocent recreation of technically savvy students to an instrument of vandalism, extortion, and espionage. There has been a concurrently dramatic development in the technologies used to detect and thwart attacks on computer systems. *Intrusion Detection & Prevention* is a guide to Intrusion Detection Systems (IDS) and an introduction to Intrusion Prevention Systems (IPS). Intrusion Detection Systems identify, assess, and report unapproved network activity. Intrusion Prevention Systems not only monitor networks, but take prescribed actions to disrupt unauthorized traffic when it is detected. IDSs are the burglar alarms of network security, while IPSs can actively protect applications and shut down common attacks such as web defacement. These systems are just two components of a complete security strategy that may include other technologies.

IPSs are relatively new compared to IDSs. IDSs have been around since the early 1980's with the most significant development in the field occurring in the late 80's and early 90's. By the late 1990's, IPSs began to emerge as a more active approach to network security. Into this developing field comes *Intrusion Detection & Prevention* by Carl Endorf, Eugene Schultz, and Jim Mellander, as well as four other contributing authors. Endorf is a security analyst in the banking and insurance industries. Schultz and Mellander are principle engineers at Lawrence Berkeley National Laboratory and specialists in incident response.

Perhaps because IPSs are relatively new and not as widely deployed, this book is much more about intrusion detection than prevention. It begins with a 100 page primer on intrusion detection, including a crash course in the Internet Protocol. Experienced network administrators may choose to skip this section, but it does provide a useful review, particularly of header and packet formats. Part II covers IDS and IPS architecture and internals. The architecture chapter shows different approaches to placing sensors within a network and how various elements interact. Chapter 7 on internals reveals the working parts of IDS and IPS systems. This is perhaps the most instructive section of the book for those new to such systems. Part III turns to the more practical aspects of implementation and deployment, highlighting several products, including Internet Security System's RealSecure, Cisco's Secure IDS, Snort (a public-domain, open-source IDS), and NFR Security. While Part III is intended to cover the implementation and fine tuning of these applications, it is more useful in helping systems administrators decide which tool is right for their needs. A similar section including true intrusion prevention systems, such as IntruShield IPS, would be useful, as would a discussion of why organizations have been cautious in deploying IPS (specifically the potential to disrupt legitimate network traffic).

Part IV is the everything else section, touching on a broad range of issues such as data correlation, incident response, and the costs of IDS and IPS. The data correlation chapter discusses the importance of automated or at least structured data analysis to make the most of collected data. Chapter 16 covers the business aspects of IDS and IPS, including deployment costs and vendor selection. The final section also provides a useful overview of a host of human issues related to IDS and IPS, including laws, standards, and policies.

In plain English, with plenty of graphics and tables, *Intrusion Detection & Prevention* is well organized and easy to follow. It strikes a perfect balance between background, theory, and practice to make it an excellent primer for IDS and IPS. The book is refreshingly readable considering the authors' impressive experience in security research and development. It neither assumes too much knowledge, nor is it an "idiot's guide", but is perfectly calibrated for anyone with solid systems administration training. One weakness of the book is that it was written by several contributors and a strong editorial presence is not evident in bringing the chapters together stylistically or ensuring completely consistent content. Overall coherence is achieved however through a well organized section and chapter structure.

Intrusion Detection & Prevention will provide those new to systems administration with an excellent overview of IDSs, including system architecture, forensics and incident response, as well as some basic tools. Chapter 5, for example, provides systems administrators with a simple and essential tool for intrusion detection, tcpdump. More experienced network professionals will find this book a useful reference and a helpful evaluative tool for considering specific IDSs and developing a strategy for deploying such systems. Experienced security administrators may find works with a greater emphasis on specific tools or based on case studies more useful. *Network Intrusion Detection*, 3rd Edition, by Stephen Northcutt, and *Intrusion Signatures and Analysis* by Mark Cooper, Stephen Northcutt, et al., both provide case studies that help network security administrators think strategically and learn from the successes and failures of others.

Despite the disappointing coverage of intrusion prevention systems, *Intrusion Detection & Prevention* is an excellent guide to IDS and a useful and informative resource in security planning.

Thomas Edgar Raffensperger, MLIS, is Library Director, Vermont Community and Technical Colleges.

REVIEW OF: Rachel Singer Gordon. (2003). *The Accidental Systems Librarian*. Medford, N.J.: Information Today.

by Corey Seeman

As a training consultant with Innovative Interfaces, Inc., I have had the opportunity to work with a number of different library types and sizes, and in only a few of those libraries did they have a full-time person serving as the systems librarian. The systems librarian, a product of the last twenty years or so, is the primary contact for all computer-related resources and technology in the library. While larger libraries have systems librarian positions, most libraries in the country do not. Instead, these roles fall to an accidental system librarian, a staff member who assumes the role of the "computer person" in the library. This computer person inevitably has other responsibilities in the library. While many are also catalogers, others who assume the role of systems librarian are library directors, reference librarians, and circulation staff. These people are chosen to lead the systems migration probably for a few reasons, including their basic understanding of computers, their ability to work with others, and, most importantly, their willingness to serve as systems librarian.

Author Rachel Singer Gordon (http://www.lisjobs.com/resume.htm (http://www.missingkids.com/cybertip/)) was such a systems librarian when she assumed the role of Head of Computer Services at the Franklin Park (Illinois) Public Library (1999-2002). Prior to that, she was a reference librarian who started assuming roles with systems-related issues at the library. She has written and given presentations on this subject, and serves as one of the editors of the website - http://www.lisjobs.com (http://www.lisjobs.com/jobseekers/). The genesis of this book was her 2001 article in *Computers in Libraries* entitled "A Course in Accidental Systems Librarianship." Her story is a perfect basis for this book, as she was not trained as a systems librarian, but assumed the responsibilities of one. In this book, she has given people who are embarking on the same journey a roadmap so they can avoid problems and traps in what could be a very stressful position.

A book like this is very timely, as only larger libraries have dedicated systems librarians. Additionally, in today's economic climate, many libraries are forced through hiring freezes and position cuts to rely on other staff members to manage systems, especially in this day and age of electronic information. The likelihood that someone other than a practicing systems librarian will be caring for an ILS (integrated library system) or maintaining computers in a library is very high these days.

As most of us who work with collection development, many computer books have two qualities that limit their long-term retention. First, they are software specific, dealing with the answering of questions on how to perform functions on a particular software system. Second, they are reference books, making them nearly impossible to read from cover to cover. With Gordon's work, we do not have either problem. Rather than produce a time-sensitive reference book

explaining how today's software works in libraries, Gordon provides us with a readable guide that will be relevant for years to come. Furthermore, while it can be used as a reference tool, it can also be read from cover to cover while keeping the interest of the reader.

The book is organized into nine chapters: Systems Librarianship 101, Defining Systems Librarianship, Systems Librarianship 102, Technical Areas You May Need To Master, Organization of Knowledge, Research Techniques, Networking, Instruction Techniques, Independent Study, Administration and Management, and Life Lessons.

In structuring the book this way, Gordon provides the core areas where a new or accidental systems librarian needs to hone his or her skills. Under no pretense to teach everything they need to know about their work, she instead shows a new systems librarian where to go for help, how to interact with others, and how to grasp the core of the problems that are being brought to them. She does this by creating a very readable book that is free of jargon, clearly explaining all terms, and providing excellent reference tools for anyone in this situation. Given the large variety of computer environments in libraries, she does a great job of addressing the computer issues in a relatively generic manner.

While this book is geared towards the new or the accidental systems librarian, it is clear that all systems librarians could find this book useful as a refresher. Among the tools provided in this book are sample forms, tips for managing apparently different jobs simultaneously, and providing advice from not only her experience, but that of other systems librarians who participated in a survey on this subject (2001-2002). Gordon incorporates a number of responses from the survey into this book, offering more than just her personal insight into solving system-related issues. These comments are excellent and provide sage advice for people finding themselves in the position of a systems librarian. Balancing jobs, which is discussed in the book, is very important when one is assuming the role of the systems librarian; you still are required to keep up with your regular job responsibilities. In this day of 24/7 access to information, it is very easy to see how a part-time systems librarian might see that part of their job take over the whole work week.

Each section of the book has a bibliography and a section of web resources. There is also an accompanying website to the book that has all references as hyperlinks (http://www.lisjobs.com/tasl/index.htm (http://www.lisjobs.com/tasl/index.htm)). This site is up to date and has been expanded from the list in the book. A link test showed that there were over 260 links on this web page and that nearly 95% still worked (a very high number for any page of links). In summary, this monograph is a very valuable addition to the professional bookshelf of any library, especially for those that have one (or zero!) person in a systems department.

Reference

Gordon, Rachel Singer. (2001). A course in accidental systems librarianship. *Computers in Libraries, 21(10),* 24-29 .

Corey Seeman is Assistant Dean for Library Systems University, for the University Libraries, University of Toledo in Ohio.

REVIEW OF: Preston Gralla. (2003). *Windows XP Hacks*. Sebastopol, CA: O'Reilly.

by Brian K. Yost

Windows XP Hacks by Preston Gralla is part of the O'Reilly's Hack series. According to the back cover: "O'Reilly's Hacks Series reclaims the term 'hacking' for the good guys--innovators who explore and experiment, unearth shortcuts, create useful tools, and come up with fun things to try on their own." Gralla is successful in sharing many useful hacks that meet this definition.

The 100 included hacks are arranged by topic. The following categories are covered; startup and shutdown; the user interface; Windows Explorer; the web; networking; email; the Registry; basic utilities; applications; graphics and multimedia; system performance and hardware .

A thorough topical index is also included that makes finding particular hacks very easy. Some of my favorite hacks are included e.g., changing the XP startup screen picture, backing up and restoring Outlook Express data and settings, speeding up network browsing, and various registry hacks.

One of the problems I find with books and articles on customizing Windows is that they often depend on third party software (usually freeware or shareware) to perform the function. My expectation is that if it is presented as a Windows hack or trick, I should be able to perform it within Windows. Gralla does depend on third party applications for many of his hacks. However, he usually first presents what can be done within Windows and then offers the third party tool as a way to take the customization further. Gralla presents plenty of customization and tricks that can be done without buying additional software, but he also describes these third party software options when applicable.

Some of the web and networking hacks are made redundant by Windows XP Service Pack 2, such as blocking pop-up windows in Internet Explorer. It is possible that some will no longer work, but most of the hacks will, and will have a relatively long useful life since the next version

of Windows (Longhorn) isn't scheduled to be released until 2006.

Overall, this is a very useful book for Windows XP power users. I recommend this title to any user who would like to customize the Windows XP interface or improve its performance. Some of the tools are also very useful for system administrators, such as the section on using .reg files for making registry changes on multiple computers. This book would also be an excellent addition to a general Windows operating system collection in a public library.

Brian K. Yost is Systems Librarian and Associate Professor at Hope College in Holland, Michigan.

REVIEW OF: Paul Wolfe, Charlie Scott, Mike W. Erwin. (2004). *Anti-Spam Tool Kit*. Emeryville, CA: McGraw-Hill/Osborne.

by Stacey Greenwell

"Refinance today, very very cheap!!" A quick scan of most inboxes today only emphasizes that spam is a growing and serious problem. It has moved beyond simple annoyance, wasting time and money. In the *Anti-Spam Tool Kit*, the authors provide a thoughtful overview of the problem and offer a comprehensive examination of SPAM-fighting tools.

The initial section, "Preparing for the Fight," offers steps for developing a SPAM-fighting strategy, focusing on four schools of thought for dealing with SPAM, from the basics -- traditional techniques like creating client-based rules -- to more advanced techniques of blacklisting or establishing policies on a mailserver. Simple suggestions, such as restricting publication of email addresses on websites, are covered, and multiple resolutions are provided (e.g. specific ways to obscure an email address on an HTML page). In addition to rule-based filtering -- including content analysis, keyword, and pattern matching -- statistical filtering is examined, as well as some methods which have been receiving more press lately, namely challenge/response systems and micropayment systems.

What does one look for in a good anti-spam tool? Stability, interoperability, ease of use, and advanced features are discussed with regard to over 30 anti-spam tools across three platforms. SpamAssassin in particular is covered in depth, with three chapters focusing on its configuration and use. Both the Mac OS and Linux are covered in separate chapters, which is particularly helpful given the exclusive Windows focus of so many manuals.

The bulk of the book is likely most useful for someone running a mail server, or at least someone with administrative control -- someone who creates organizational policies and procedures for email. At the same time, some of the tools discussed are client-based, end-user oriented, and can be very useful. The history and overview of the problem, including a general discussion for how email works, is appropriate for a more general audience. Other useful tips would be beneficial to a general audience, like a detailed discussion of how to read message headers in multiple email clients and follow up with research, such as with SpamCop. Many non-technical readers with a passing interest in the topic will find sections that aren't terribly helpful or applicable, but are clear and likely interesting nonetheless.

The format is quite readable, containing multiple charts and graphs of anti-spam tool features. Step-by-step instructions contain clearly labeled screen shots which are particularly useful for how-tos, such as configuring email client rules. The guide to creating rules is helpful and covers several popular email clients: Eudora, Mozilla, Outlook Express, and Outlook. Sidebars containing additional discussions and examples appear throughout the book.

One gem from this book is the sidebar which lists the specific words used as filtering criteria for the Junk Mail rule in Outlook 2000. This information explains some of the seemingly erratic behavior of the built-in Junk Mail filter. Did you know, for example, that seemingly innocuous phrases in the message body such as "cards accepted" or "removal instructions" will result in mail being marked as junk when using this rule in Outlook 2000?

The closing chapter, "Fighting SPAM defensively," touches on spyware, pop-ups, and one spyware removal tool in particular. The authors are quite correct about the connectedness between SPAM, spyware, and pop-ups. Hopefully a future edition will cover these related problems with the same detail SPAM receives here.

In addition to a glossary, index, and references to additional resources, the *Anti-Spam Tool Kit* includes a CD-ROM. This CD-ROM is a little disappointing; one would expect more than a two page PDF of web links, but by linking to the tools rather than including installers on the CD-ROM, the user is assured of getting the latest version of the tool.

Despite being armed with knowledge and a fleet of anti-SPAM tools, this is no panacea; these tools will not completely eradicate SPAM. The authors warn us that even with all of the tools they employ, nothing is going to be 100% effective. Using this book will at least improve one's chances of having a cleaner, more efficient inbox, and of further understanding this growing problem.

Stacey Greenwell is Desktop Support Librarian for the University of Kentucky Libraries in Lexington, Kentucky.

Click here to take the TER reader survey (http://surveymonkey.com/s.asp?u=17669527561)

About *TER*