Appendix B

Keeping Up

There is always something new in the field of Internet security. With dozens of governments, thousands of companies, and millions of people actively involved in this ongoing research experiment, it is very hard to stay current. True, the basic security issues are largely unchanged from computing in the 1960s, but the details and variations continue, and sometimes are interesting.

This book is a static construct; there is no way for us to update your copy with information on new holes and new tools. You have to assume the responsibility for staying current. How does one keep up to date?

One way, of course, is to buy the next edition of this book. We highly recommend that…

The Internet itself is a useful tool for keeping up. There are a number of security-related newsgroups and mailing lists that you may want to follow.

Another source of information is the hacker community itself. You may want to read *2600 Magazine*, the self-styled “Hacker Quarterly.” Useful online publications include *Phrack*.

You can also monitor *Internet Relay Chat (IRC)* channels, a real-time conferencing system. Some of the “channels” are dedicated to hacking, but participation is not necessarily open to all comers. The signal-to-noise ratio on these systems can be rather low, especially if you don’t like the poor or variant spelling of the “d00dz” in the subculture, or if you aren’t interested in “warez”—stolen PC software—but you can also learn amazing things about how to penetrate some systems.

(Note that IRC access software has often contained back doors and other intentional security holes, as well as the usual buffer overflows and the like.)

If you’re going to participate in some of these forums, you need to make some ethical decisions. Who are you going to claim to be? Would you lie? You may have to prove yourself. Would you contribute sensitive information of your own? You can get remarkably far even if you admit that you are a corporate security person or a cop, especially if the other participants believe that you want information, not criminal convictions. (One friend of ours, who *has* participated in various raids, has been asked by various hackers for his autograph.)

Following are some more mundane sources of information.

B.1 Mailing Lists

This section cites some of the best mailing lists for keeping up with security issues. Obviously, the list is not complete, but there's enough information here to fill any mailbox.

CERT Tools and Advisories The *Computer Emergency Response Team (CERT)* provides tools contributed by the community, as well as their own security advisories. `http://www.cert.org/tech_tips/packet_filtering.html` has guidance on which ports should be blocked.
`http://www.cert.org/`

The *Firewalls* Mailing List The Firewalls mailing list is hosted by the Internet Software Consortium. For subscription details, see
`http://www.isc.org/services/public/lists/firewalls.html`

The *Bugtraq* Mailing List Bugtraq is a security mailing list whose differentiating principle is that it's proper to disclose details of security holes, so that you can assess your own exposure and—perhaps—see how you can fix them yourself. More information is available at:
`http://online.securityfocus.com/archive`
Oddly enough, it requires JavaScript. There is also NTBugtraq, devoted to security issues specific to Windows NT, 2000, and XP:
`http://www.ntbugtraq.com/`

If you think you've found a security hole but are not sure, or are not sure of the implications, you may want to discuss it on vuln-dev.
`http://lists.insecure.org/about/vuln-dev.txt`.

RISKS Forum The *Risks Forum* is a moderated list for discussing dangers to the public resulting from poorly built computer systems. Although not a bug list *per se*, most significant security holes are reported there. RISKS is available as a mailing list and the newgroup *comp.risks* on USENET. Send subscription requests to *risks-request@csl.sri.com*. Excerpts from RISKS appear in *Software Engineering Notes*.
`ftp://ftp.sri.com/risks`

VulnWatch and VulnDiscuss VulnWatch is a mailing list for announcements of security holes. For discussing vulnerabilities in general, as well as for specific questions about particular software, use VulnDiscuss.
`http://www.vulnwatch.org`

One especially useful page lists numerous vendor contacts and security patch archives:
`http://www.vulnwatch.org/links.html`.

Cipher Newsletter The Cipher Newsletter is run by the IEEE Technical Committee on Security and Privacy. To subscribe, send mail to *cipher@issl.iastate.edu* with the subject "subscribe" in the message. To receive only a notification that a new issue is available online, specify "subscribe postcard" in the subject instead. The newsletter contains a very good calendar

of security conferences and calls for papers, important news items, and conference reports. New issues appear about every two months.
`http://www.ieee-security.org/cipher.html`

Cryptogram Bruce Schneier's monthly newsletter containing his musings and other security information. Bruce is quite informative and interesting.
`http://www.counterpane.com/crypto-gram.html`

B.2 Web Resources

We could probably fill a whole book with Web references about security. Instead, we picked some of the best ones. Any omissions are probably linked to from these sites.

slashdot Slashdot has up-to-the-minute news on computers, science, networking, and related information. It is well-read, and Web servers that appear in slashdot are often smothered with queries.
`http://slashdot.org`

SecurityFocus SecurityFocus maintains a portal of security information. They do a good job of keeping the information fresh, and they link to other high-signal security information sites.

`http://www.securityfocus.com/`

SANS A very good summary of major new security problems. Editorial comments are usually quite clueful; the mailing list is especially helpful.
`http://www.sans.org/`

AntiOnline A Web site containing discussion forums and a comprehensive collection of hacker tools, as described in Chapter 6.
`http://www.antionline.com/`

Packet storm A Web site containing many tools for testing the security of a network, including *nessus* and *snort*. Also contains advisories and discussion forums.
`http://packetstormsecurity.nl/`

Insecure.org A Web portal for security vulnerabilities, developments and discussion. Contains current information on security vulnerabilities and patches, mailing lists on various security topics, and vendor-specific links.
`http://www.insecure.org/`

Google This search engine was instrumental in the writing of this book. If you want to find something but don't know where to start, try asking the oracle of our times.
`http://www.google.com/`

B.3 Peoples' Pages

> The problem with folk songs is that they are written by the people.
>
> *An Evening (Wasted) with Tom Lehrer*
> —TOM LEHRER

Many people have good Web pages with links to security resources—too many to list. We've chosen a couple of really good ones. These pages have links to other peoples' pages.

Ron Rivest's links page Ron Rivest is well known within the computer science community for his groundbreaking algorithms work. More broadly, he is famous as the *R* in RSA. Rivest maintains one of the best jump pages for resources in cryptography and security. In fact, it includes a list of other peoples' links pages, so we limit ourselves to his page, and interested parties can start there and browse.
`http://theory.lcs.mit.edu/˜rivest/crypto-security.html`

Peter Gutmann Peter Gutmann is one of the leading practical security researchers. His links page is one of the finest.
`http://www.cs.auckland.ac.nz/˜pgut001/links.html`

B.4 Vendor Security Sites

Many of these vendors have mailing lists to which you can subscribe. In some cases, we included a URL to help you find information on subscribing.

Microsoft This site contains information about the latest security problems, along with patches. If you run Windows, it's a good idea to check back regularly.
`http://www.microsoft.com/security/`

Cisco
`http://www.cisco.com/go/psirt/`

Sun
`http://sunsolve.sun.com/pub-cgi/show.pl.target.security/sec`

Apple
`http://lists.apple.com/mailman/listinfo/security-announce`

Red Hat
`http://www.redhat.com/mailing-lists/redhat-list/`

FreeBSD
`http://www.freebsd.org/security/`

OpenBSD
`http://www.openbsd.org/security.html`

NetBSD
`http://www.netbsd.org/Security/`

B.5 Conferences

These days, it appears that there is a security conference just about every week. The ones we list here are the ones we consider to be the most important. There are some other ones organized by people whose hats are various shades of gray and black; you may or may not enjoy these, depending on your tastes.

Conferences are a great way to meet the leaders in a field, and to keep up with the latest advances and concerns. Most of the following conferences, and many others, provide excellent tutorials to bring novices up to speed. They are usually well worth the time and expense. Hint: don't spend all your time in the sessions; the hallway discussions, and for that matter that bar at night, are great places to learn what's going on.

USENIX Security This conference is about practical systems security. There are usually two tracks—invited talks and technical talks. The hallway track tends to be of extremely high quality, as are the evening *birds of a feather (BoF)* sessions. The conference is held every August in different locations in the U.S.
`http://www.usenix.org/events/`

NDSS The *Internet Society (ISOC) Networks and Distributed Systems Security (NDSS)* conference is similar to the USENIX security conference is scope, but focuses more on security issues related to networking. The conference is single track, and is held every February in San Diego—an additional reason for people from colder climates to attend.
`http://www.isoc.org/isoc/conferences/ndss/`

The Oakland Conference This conference is actually called the IEEE Symposium on Security and Privacy; however, the security community generally refers to this as *the Oakland Conference*. This conference tends to include both theoretical and practical papers. It is an interesting mix of government folks, academic researchers, and industry types.
`http://www.ieee-security.org/TC/SP-Index.html`

ACM CCS The *Association for Computing Machinery (ACM) Computers and Communication Security (CCS)* is another high-quality security conference. It tends to have the broadest scope of all of the security research conferences. It is not uncommon to see a paper about S-box design followed by a paper on penetration testing.
`http://www.acm.org/sigsac/ccs.html`

LISA The USENIX *Large Installation Systems Administration (LISA)* conference is a must for system administrators. Good system administration is a vital part of security, and this con-

ference is the place to be. Many of the papers are extremely good, and the hallway track and the BoFs are invaluable.
`http://www.usenix.org/events/`

BlackHat/DefCon For a view of the seamy underbelly of Internet security, you might want to see what the other side is up to at BlackHat and DefCon. If you can get your boss to pay for BlackHat, you can reserve two more days in your hotel and stay for DefCon for free. It is held in Las Vegas every year, and attended by hats of all colors.
`http://www.blackhat.com/html/`