PART V

Appendixes

CHAPTER A

Security Information Sources

Organizations exist that specialize in Internet security, providing users with bulletins, Web sites, FTP archives, and advice. In addition to the vendors, government-sponsored groups such as national CERTs, and university organizations, such as COAST, can help you in protecting your systems or dealing with intrusions. Appendix B contains a detailed list of useful sites. The following provides a review of the major sites of interest that readers may find useful.

CIAC

The U.S. Department of Energy's Computer Incident Advisory Capability group, the CIAC, was created in 1989 in response to the Internet Worm. It primarily serves the DOE from its Lawrence Livermore National Laboratory site, but it also provides e-mail advisories and an FTP/Web site for anyone on the Internet. The Web site is one of the best security pages, offering advisories, security documents, and FTP links to many significant programs.

- The FTP address is `ftp://ciac.llnl.gov/pub/ciac`.
- The Web address is `http://ciac.llnl.gov`.
- The e-mail address is `ciac@llnl.gov`. (E-mail information is available by sending help to `ciac-listproc@llnl.gov`.)

COAST

Founded by Eugene Spafford, the Purdue University COAST project (Computer Operations, Audit, and Security Technology) is dedicated to improving network security. COAST has an impressive Web site, featuring links to large numbers of security sites. Offering a comprehensive FTP archive, COAST features one of the largest collections of papers and tools on the topic of network security. COAST also issues a newsletter. COAST works closely with major companies and government agencies and has created a number of useful tools and informative studies of network security.

- The FTP address is `ftp://coast.cs.purdue.edu`.
- The Web site is `http://www.cs.purdue.edu/coast/coast.html`.
- The e-mail address is `coast-request@cs.purdue.edu`.

CERT

The U.S. CERT (Computer Emergency Response Team) was founded in 1989 by the U.S. Department of Defense to protect the infrastructure of the Internet. Situated at Carnegie-Mellon University, in Pittsburgh, Pennsylvania, CERT consists of about a dozen employees who respond to reports from Internet users regarding network security, issuing bulletins, notifying vendors, characterizing the state of the Internet from a security standpoint, working with the mass media to publicize and address concerns, and researching solutions to Internet security problems. CERT is frequently mentioned in media reports from the *New York Times* to *Scientific American*.

Some criticize CERT for delaying the release of bulletins; this criticism, however, is unjustified to a certain degree because CERT attempts to ensure that vendors are able to address the vulnerabilities before they announce the hole.

CERT has one of the largest mailing lists for security advisories, with more than 100,000 subscribers. It permits anyone to subscribe. The CERT FTP archive contains a wide range of security programs, as well as every advisory and bulletin that CERT has issued.

The CERT group recommends that you encrypt security information before e-mailing; they support DES, PGP, and PEM. They have a 24-hour hotline at 1-412-268-7090. CERT advisories are posted on `comp.security.announce`.

- The FTP address is `ftp://info.cert.org`.
- The e-mail address is `cert@cert.org`. (You can subscribe by sending a request to `cert-advisory-request@cert.org`.)

Many other countries have also formed CERTs, notably Germany (DFN-CERT) and Australia (AUS-CERT). Visit the FIRST Web site for contact information on these and other CERT groups.

FIRST

The Forum of Incident and Response Security Teams, or FIRST, is a non-profit corporation of representatives from the vendors, universities, national and international government agencies, and large private corporate computer users. A complete list of members (currently 45 groups), along with contact information, is available. CERT redirects requests regarding security problems to the appropriate FIRST member, so that they can address the issue and provide resolution information back to CERT for the CERT advisory or bulletin.

FIRST provides a forum for security response teams to share security information, tools, and practices. FIRST sponsors a yearly week-long meeting of representatives, a mailing list for discussions among members, and a point of contact for Internet users with security concerns.

- The FTP address is `ftp://csrc.ncsl.nist.gov/pub/first`.
- The e-mail address is `first-sec@first.org`.
- The http address is `http://www.first.org/first/`.
- Contact the list at `http://csrc.ncsl.nist.gov/first/team-info/`.

8lgm: Eight Little Green Men

This mailing list sends out advisories and exploit scripts for Unix vulnerabilities. They frequently adhere to full disclosure on security holes, so they are one of the best sources for understanding the source of vulnerabilities.

To subscribe, send the text `subscribe 8lgm-list` to `majordomo@8lgm.org`.

bugtraq

bugtraq is another mailing list that involves detailed discussion of Unix vulnerabilities. The amount of traffic (e-mail) generated by this source is enormous. To subscribe, send the text `subscribe bugtraq` to `listserv@netspace.org`.

Vendors

Most vendors have Web pages and security response teams that can provide assistance in dealing with network vulnerabilities. The FIRST Web page provides contact information, but most vendors typically respond to `security-alert@<vendor-domain>` (for example, `security-alert@hp.com`).

Vendors typically offer free security bulletins to anyone who signs up on the appropriate mailing list, along with a Web/FTP archive of previous bulletins. Contact your vendor for details on subscribing.

Security product vendors usually offer useful Web sites.

- Cygnus offers information on Kerberos at `http://www.cygnus.com/data/cns`.
- TIS offers information on firewalls at `http://www.tis.com`.
- RSA offers information on cryptography at `http://www.rsa.com`.

Others

There are individuals who have created Web sites with links to many security pages. These Web sites are frequently posted to `comp.security.unix` and can be quite helpful in locating new FTP archives, tools, or papers. These come and go, but one interesting site is `http://www.iesd.auc.dk/~johnson/secure.html`.

CHAPTER B

Internet Security References

Table B.1 contains a list of the FTP sites and Web sites that contain Internet security-related programs and files.

Table B.1
Web/FTP Sites

Program	Site
Argus	`ftp://ftp.sei.cmu.edu/pub/argus-1.5`
AT&T Web Sites	`http://www.research.att.com/` `ftp://Research.att.com/dist/internet_security`
Bind (DNS)	`ftp://gatekeeper.dec.com/pub/misc/vixie`
CERN WWW Consortium	`http://www.w3.org`
CERT FTP Archive	`ftp://ftp.cert.org`
CIAC	`ftp://ciac.llnl.gov/pub/ciac` `http://ciac.llnl.gov`
Ckpasswd	`ftp://gatekeeper.dec.com/pub/` `usenet/comp.sources.unix/volume28/ckpasswd`
COAST Project (Purdue University)	`http://www.cs.purdue.edu/coast/coast.html` `ftp://coast.cs.purdue.edu/pub`
Computer Systems Consulting	`http://www.spy.org/`
COPS	`ftp://ftp.cert.org/pub/tools/`cops
Courtney	`ftp://ciac.llnl.gov/pub/ciac` `http://ciac.llnl.gov`
Crack	`ftp://ftp.cert.org/pub/tools/crack`
Cryptography, PGP, and Privacy	`http://draco.centerline.com:8080/~franl/` `crypto.html`
Cygnus Kerberos Information	`http://www.cygnus.com/data/cns`
Cypherpunks	`ftp://ftp.csua.berkeley.edu/pub/cypherpunks` `http://www.csua.berkeley.edu/cypherpunks`
Dan Farmer	`http://www.fish.com/dan.html`
Dartmouth University —Papers, programs	`ftp://dartmouth.edu/pub/security`
DDN Security Bulletins FTP Archive	`ftp://nic.ddn.mil/scc`
Firewall Web Page	`http://www.access.digex.net/~bdboyle/` `firewall.vendor.html`

Program	Site

FIRST	`ftp://csrc.ncsl.nist.gov/pub/first`
	`http://www.first.org/first/`
	`http://csrc.ncsl.nist.gov/first/team-info/`

Fremont	`ftp://ftp.cs.colorado.edu/pub/cs/distribs/fremont`
Gabriel	`http://www.lat.com/gabe.htm`
Greatcircle FTP Archive—Firewall information	`ftp://ftp.greatcircle.com/pub`
httpd	`http://www.ncsa.uiuc.edu`
identd	`ftp://ftp.lysator.liu.se:/pub/ident/servers`
ISS	`http://iss.com/` `ftp://ftp.uunet.net/usenet/comp.sources.misc/volume39/iss/`
Kerberos Information	`ftp://athena-dist.mit.edu/pub/ATHENA`
NEC Security tools—socks, sudo, cops	`ftp://ftp.inoc.dl.nec.com/pub/security`
Netscape	`http://www.netscape.com`

NIST (U.S. National Institute of Standards and Technology)	`ftp://csrc.ncsl.nist.gov`
	`http://cscr.ncsl.nist.gov/`
	`http://www.tansu.com.au/Info/security.html`
	`http://www.nist.gov/`

Opie	`ftp://ftp.nrl.navy.mil/pub/security/nrl-opie`
Perl Source	`ftp://archive.cis.ohio-state.edu/pub/gnu/mirror/perl5.001m.tar.gz`

PGP and IDEA Archives	`ftp://ftp.informatik.uni-hamburg.de/pub/virus/crypt/disk`
	`ftp://ftp.dsi.unimi.it:/pub/security/crypt/code`
	`http://www.ifi.uio.no/~staalesc/PGP/home.html`
	`http://web.mit.edu/network/pgp-form.html`

PGP Documentation	`http://www.pegasus.esprit.ec.org/people/arne/pgp.html`

continues

Table B.1, Continued
Web/FTP Sites

Program	Site
PGP elm	`ftp://ftp.viewlogic.com/pub/elm-2.4pl24pgp2.tar.gz`
PGP Public Key Server	`http://www-swiss.ai.mit.edu/~bal/pks-toplev.html`
RFCs	`ftp://ietf.cnri.reston.va.us`
RSA Data Security, Inc.	`http://www.rsa.com/`
Science Applications International Corporation	`http://mls.saic.com/`
Secure HyperText Transfer Protocol	`ftp://ftp.commerce.net/pubs/standards/drafts/shttp.txt`
Secure Telnet	`ftp://ftp.adfa.oz.au/pub/security/adfa-telnet`
sendmail	`ftp://ftp.cs.berkeley.edu`
SGI IRIX Security Scanner (Securscan)	`ftp://ftp.vis.colostate.edu/pub/irix/security/securscan.tar.gz`
SGI Security Information	`ftp://sgigate.sgi.com/security/`
S/Key	`ftp://thumper.bellcore.com/pub/nmh/skey/`
SNMP FTP Archives	`ftp://ftp.denet.dk/pub/snmp/cmu-snmp` `ftp://lancaster.andrew.cmu.edu/pub/snmp-dist/`

socks	`ftp://ftp.nec.com/pub/security/socks.cstc`
	`http://www.socks.nec.com`
	`ftp://ftp.cup.hp.com/dist/socks`

SRI Computer Science Lab	`http://www.csl.sri.com/`
	`http://www.sri.com/SRI`
	`ftp://ftp.csl.sri.com`

ssh (Secure Shell)	`ftp://ftp.cs.hut.fi:/pub/ssh/` `http://www.cs.hut.fi/ssh`
SSLeay Source	`http://www.psy.uq.oz.au/~ftp/Crypto/`
SSLref Source	`http://www.netscape.com`

SURAnet Security Archive—Alerts, programs	`ftp://ftp.sura.net/pub/security`
tcpdump, libpcap	`http://ciac.llnl.gov`
tcp_wrappers	`ftp://ftp.win.tue.nl:/pub/security/tcp_wrappers_6.3.shar.Z`
Texas A&M University Security Archives	`ftp://ftp.tamu.edu` `ftp://Net.Tamu.edu/pub/security/TAMU`
TIS FTP Archive—firewall programs, information	`ftp://ftp.tis.com/pub`
Tripwire	`ftp://ftp.cs.purdue.edu/pub/spaf/COAST/Tripwire`
VeriSign	`http://www.verisign.com`
ViaCrypt	`http://www.viacrypt.com`
Vince Cate's Security Page—Useful list of pointers to network security sites	`ftp://furmint.nectar.cs.cmu.edu/security/README.html`
Wietse Venema FTP Archive	`ftp://ftp.win.tue.nl:/pub/security`
wu-ftpd	`ftp://wuarchive.wustl.edu`
xinetd	`ftp://ftp.ieunet.ie/pub/security/xinetd-2.14.tar.gz`

The newsgroups shown in table B.2 are an excellent day-to-day source of information for security-minded people of all walks, both novice and expert alike. Investigate them all to start, and stay with the ones you find most useful.

Table B.2
Usenet Newsgroups

Newsgroup	Description
`comp.security.unix`	The primary newsgroup for security
`comp.security.misc`	The second best newsgroup for security
`alt.security`	The third best, though increasing amounts of noise
`sci.crypt`	A lot of theory on cryptography
`alt.2600`	More phone hacking and vending machine breaking

continues

Table B.2, Continued
Usenet Newsgroups

Newsgroup	Description
`comp.security.firewalls`	Discussion of firewalls
`comp.security.announce`	CERT advisories
`alt.security.pgp`	Discussion of PGP
`alt.security.ripem`	Discussion of PEM, little traffic
`comp.protocols.kerberos`	Discussion of Kerberos
`alt.hacker`	Not very useful
`talk.politics.crypto`	Interesting discussions on cryptography