

## Appendix 1 – Resources for Internet Security Information

### 1.1 Web Sites

#### **Project COAST Homepage & Computer Security Archives**

<http://www.cs.purdue.edu/coast/coast.html>

This is a good all-round site for finding security tools such as COPS, Tripwire, SATAN, etc. You can be fairly sure that the source code has not been tampered with, and the Web interface makes it easy to locate what you want. There are also many excellent papers here worth reading.

#### **Spaf's Hotlist**

<http://www.cs.purdue.edu/homes/spaf/hotlists/csec.html>

Dr. Eugene Spafford's computer security hotlist.

#### **CIAC Security Web Site**

<http://ciac.llnl.gov/>

The Livermore Labs security site for government and military sites. They issue alerts similar to CERT alerts. Many of their tools are available to the public, though some are restricted to DoD users.

#### **AUSCERT Information Pages**

<http://www.auscert.org.au/>

AUSCERT is the Australian Computer Emergency Response Team (CERT) team. They have some tools and papers not found at some of the other, American sites, including a very good paper on developing security policies, and a veritable book on security in open systems environments.

#### **8lgm: Security Advisories**

<http://www.8lgm.org>

The "Eight Little Green Men" (or is it "Eight-Legged Groove Machine"?) are a self-appointed group of security vigilantes who publish their own advisory announcements for newly discovered security bugs and problems. In addition to their Web site, they also maintain a mailing list.

#### **Telstra Corporation: Computer and Network Security Reference Index**

<http://www.telstra.com.au/info/security.html>

#### **NIST Computer Security Resource Clearinghouse**

<http://csrc.nist.gov/>

The National Institute of Standards and Technology's computer security web site. This site contains information on DES and the proposed Advanced Encryption standards, the Public Key Infrastructure project, and computer security-related Federal Information Processing Standards and Special Publications.

#### **University of California at Davis Computer Security Research Lab**

<http://seclab.cs.ucdavis.edu/Security.html>

Information from on-going research projects in intrusion detection and auditing.

#### **London School of Economics Computer Security Research Centre**

<http://csrc.lse.ac.uk/csrc/csrchome.htm>

**Institute for Computer and Telecommunications Systems Policy**

<http://www.seas.gwu.edu:80/seas/ictsp/>

Information relevant to legal issues in computing and the "information superhighway".

**World Wide Web Security Issues**

WWW Security FAQ <http://www-genome.wi.mit.edu/WWW/faqs/www-security-faq.html>

Rutgers U. <http://www-ns.rutgers.edu/www-security/index.html>

HotJava <http://java.sun.com/1.0alpha3/doc/security/security.html>

C2 Challenge <http://www.c2.org/hacknetscape/>

CGI Security <http://www.cerf.net/~paulp/cgi-security>

General WWW FAQ <http://www.boutell.com/faq>

CGI FAQ <http://www.best.com/~hedlund/cgi-faq>

**Router and Network Vendor Sites**

<http://www.cisco.com>

<http://www.livingston.com>

<http://www.baynetworks.com>

<http://www.network.com>

<http://www.racal.com/networking.html>

**Firewall Vendor Sites, by product name**

Gauntlet <http://www.tis.com>

NetSP <http://www.ibm.link.ibm.com/oi/ann/alet/294774.html>

Sidewinder <http://www.sctc.com>

Borderware <http://www.border.com>

Firewall-1 <http://www.checkpoint.com>

DEC SEAL <http://www.digital.com>

Centri <http://www.cohesive.com>

PORTUS <http://www.sccsi.com/lsli/lsli.homepage.html>

Eagle <http://www.raptor.com>

Black Hole <http://www.milkyway.com>

InterLock <http://www.ans.net/security.html>

NET1-AccessPlus <http://www.iu.net/n1/>

Ascend <http://www.ascend.com>

**1.2 Ftp Sites**

<ftp.cisco.com> Cisco product info, sample screening rules, etc

<rtfm.mit.edu> MIT archives for USENET newsgroup FAQs

<ftp.greatcircle.com> Firewalls info and archives

<net.tamu.edu> Texas A&M University (TAMU tools)

ftp.uu.net

UUNET archives

### **1.3 Usenet News Groups**

#### **Computer Security**

alt.security	Security issues on computer systems
alt.security.index	Pointers to good stuff in misc.security (Moderated)
comp.risks	Risks to the public from computers & users
comp.security.announce	Announcements from the CERT about security
comp.security.firewalls	Discussion about Internet firewalls
comp.security.misc	Security issues of computers and networks
comp.security.unix	Discussion of Unix security

#### **TCP/IP networking:**

comp.protocols.tcp-ip	TCP and IP network protocols
-----------------------	------------------------------

#### **Telecom:**

comp.dcom.cellular	
comp.dcom.telecom	Telecommunications digest (Moderated)
comp.dcom.telecom.tech	

#### **Communications, vendor-specific:**

comp.dcom.sys.cisco	
comp.dcom.sys.wellfleet	

#### **Packet networks:**

comp.dcom.frame-relay	
comp.dcom.isdn	
comp.dcom.cell-relay	

### **1.4 Mailing Lists**

#### **Firewalls**

Registration Address: Send a message to majordomo@greatcircle.com containing the line "subscribe firewalls user@host". This list is moderated by Brent Chapman, president of Great Circle Associates.

#### **Bugtraq**

To join, send e-mail to [LISTSERV@NETSPACE.ORG](mailto:LISTSERV@NETSPACE.ORG) and, in the text of your message (not the subject line), write: "SUBSCRIBE BUGTRAQ". This is a full-disclosure list moderated by [Aleph1@underground.org](mailto:Aleph1@underground.org).

#### **CERT Advisories**

Registration Address: [cert-advisory-request@cert.org](mailto:cert-advisory-request@cert.org)

#### **CERT Tools**

Reflector Address: [cert-tools@cert.org](mailto:cert-tools@cert.org)

Registration Address: [cert-tools-request@cert.org](mailto:cert-tools-request@cert.org)

**Alert**

Reflector Address: alert@iss.net

Registration Address: request-alert@iss.net

This list is moderated by Christopher Klaus, president of Internet Security Systems, Inc.

**Best of Security**

To join, send e-mail to best-of-security-request@suburbia.net with the following in the body of the message: "subscribe best-of-security". This list is moderated (so to speak) by Julian Assange.

**1.5 Books****Practical Unix and Internet Security, 2<sup>nd</sup> Edition**

Author	Simson Garfinkel and Gene Spafford
Copyright Date	1996
ISBN	1-56592-148-8
Publisher	O'Reilly & Associates, Inc.

---

**Firewalls and Internet Security**

Author	William Cheswick and Steven Bellovin
Publisher	Addison Wesley
Copyright Date	1994
ISBN	0-201-63357-4

---

**Building Internet Firewalls**

Author	Brent Chapman & Elizabeth Zwicky
Publisher	O'Reilly & Associates, Inc.
Copyright Date	1995
ISBN	1-56592-124-0

---

**Actually Useful Internet Security Techniques**

Author	Larry Hughes
Publisher	New Riders Press
Copyright Date	Sep-95
ISBN	1-56205-508-9

---

**Computer Crime: A Crimefighter's Handbook**

Authors	David Icové, Karl Seger and William
Publisher	O'Reilly & Associates, Inc.
Copyright Date	1995
ISBN	1-56592-086-4

---

**Computer Security Basics**

Authors	Deborah Russell & G.T. Gangemi Sr.
Publisher	O'Reilly & Associates, Inc.

---

---

Copyright Date	1991
ISBN	0-937175-71-4

---

**Security in Computing**

Author	Charles P. Pfleeger
Publisher	Prentice Hall
Copyright Date	1989
ISBN	0-13-798943-1.

---

**Network Security: Private Communication in a Public World**

Authors	Charles Kaufman, Radia Perlman, and Michael Speciner
Publisher	Prentice Hall
Copyright	1995
ISBN	0-13-061466-1

---

**Unix System Security**

Author	Rik Farrow
Publisher	Addison Wesley
Copyright Date	1991
ISBN	0-201-57030-0

---

**Unix Security: A Practical Tutorial**

Author	N. Derek Arnold
Publisher	McGraw Hill
Copyright Date	1993

---

**Unix System Security: A Guide for Users and Systems Administrators**

Author	David A. Curry
Publisher	Addison-Wesley
Copyright Date	1992
ISBN	0-201-56327-4

---

**Unix Security for the Organization**

Author	Richard Bryant
Publisher	Sams
Copyright Date	1994
ISBN	0-672-30571-2

---

---

*This list is compiled and maintained by Jody Patilla (jcp@tis.com), a senior security consultant for Trusted Information Systems, in Glenwood, MD.*

