

REVIEW: "Firewalls and Internet Security", William R. Cheswick/Steven M. Bellovin/Aviel D. Rubin

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-04/0405.html>

From: Rob Slade, doting grandpa of Ryan and Trevor (rslade_at_sprint.ca)

Date: 04/25/03

Date: Fri, 25 Apr 2003 15:19:40 GMT

BKFRINSC.RVW 20030321

"Firewalls and Internet Security", William R. Cheswick/Steven M. Bellovin/Aviel D. Rubin, 2003, 0-201-63466-X, U\$49.99/C\$77.99

%A William R. Cheswick ches@cheswick.com

%A Steven M. Bellovin smb@stevebellovin.com

%A Aviel D. Rubin avi@rubin.net

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario M3C 2T8

%D 2003

%G 0-201-63466-X

%I Addison-Wesley Publishing Company

%O U\$49.99/C\$77.99 416-447-5101 fax: 416-443-0948

%O <http://www.amazon.com/exec/obidos/ASIN/020163466X/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/020163466X/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/020163466X/robsladesin03-20>

%P 433 p.

%T "Firewalls and Internet Security: Repelling the Wily Hacker, Second Edition"

As the first work to deal seriously and completely with the topic, the first edition of "Firewalls and Internet Security" was one of those classics that get known only by the last names of the authors, so as not to leave any possibility of confusion with books whose titles may be similar.

When such a long time has elapsed between editions of a work such as this, it is more than possible that the field has moved on far enough that a minor updating of the material is simply not feasible. The authors are quite well aware of the new territory: where useful, the original structure has been retained, but otherwise, the book has essentially been rewritten. A huge undertaking, but the only practical course, in the circumstances.

Part one establishes a starting point. Chapter one, an introduction, presents a number of basic, but worthwhile, security concepts. The operations of various components of the TCP/IP protocol suite are

discussed, with the most serious security vulnerabilities helpfully highlighted, in chapters two (lower layers) and three (upper layers). The authors' thoughts on the security of the Web are amply expressed in the title of chapter four: "The Web: Threat or Menace?"

Part two outlines the threats to networked machines. Chapter five describes a number of different types of attacks. A variety of tools for determining security weaknesses are listed in chapter six, alongside discussions of the relative costs/benefits of disclosure versus security by obscurity.

Part three details security tools and utilities. Chapter seven reviews authentication concepts and techniques. Various network security systems are described in chapter eight.

Part four gets us to firewalls and virtual private networks (VPNs) themselves. Chapter nine outlines the different types of firewalls. Basic filtering concepts are examined in chapter ten. Considerations for constructing and tuning your firewall are in chapter eleven. Tunnelling and VPNs are discussed in chapter twelve.

Part five extends the isolated technology of firewalls into the application of protecting an organization. Network layout, and the implications thereof, is reviewed in chapter thirteen. Chapter fourteen deals with hardening of hosts. Chapter fifteen is a rather terse look at intrusion detection.

Part six is entitled "Lessons Learned." The detection and tracing of "berferd" is described in chapter sixteen, along with the taking of the "CLARK" machine in chapter seventeen. In chapter eighteen, Kerberos and IPSec are used as examples of approaches to security of insecure networks. Chapter nineteen finishes with some ideas for work that yet needs to be done to help with the security of the Internet.

The place of firewalls in regard to network security has broadened considerably in the past decade. This book does reflect that reality. Unfortunately, that breadth of topic has come at the expense of some depth in coverage. The result is a book that is definitely worthwhile as an introduction to the field, but which may no longer be suitable as a working reference. I must admit that, for some time, I have been recommending Chapman and Zwicky (cf. BKBUINFL.RVW) over Cheswick and Bellovin's original text, since "Building Internet Firewalls" seems to have the edge in terms of practicality. Upon reviewing this new edition of the classic, I would have to stick to that recommendation.

copyright Robert M. Slade, 1994, 2003 BKFRINSC.RVW 20030321

--
=====
rslade@sprint.ca rslade@vcn.bc.ca slade@victoria.tc.ca pl@canada.com
"If you do buy a computer, don't turn it on." - Richards' 2nd Law
===== for back issues:

comp.security.misc: REVIEW: "Firewalls and Internet Security", William R. Cheswick/Steven M. Bellovin/Aviel D. Rubin

[Victoria Freenet] site <http://victoria.tc.ca/int-grps/books/techrev/>
or <http://www.victoria.tc.ca/techrev>
or <http://victoria.tc.ca/techrev>

an alternate site has been provided by CuD and NIU at:
<http://sun.soci.niu.edu/~rslade/>

CISSP refs: [Victoria Freenet]mnbkscdd.htm

Security Dict.: [Victoria Freenet]secgloss.htm

Security Educ.: [Victoria Freenet]comseced.htm

Book reviews: [Victoria Freenet]mnbk.htm

[Victoria Freenet]review.htm

Partial/recent: <http://groups.yahoo.com/group/techbooks/>

Security Educ.: <http://groups.yahoo.com/group/comseced/>

Review mailing list: send mail to techbooks-subscribe@egroups.com