Security/Networking

Firewalls and Internet Security, Second Edition

The best-selling first edition of ***Firewalls and Internet Security*** became the bible of Internet security by showing readers how to think about threats and solutions. This completely updated and expanded second edition defines the security problems companies face in today's Internet, identifies the weaknesses of the most popular security technologies, and illustrates the ins and outs of deploying an effective firewall. Readers will learn how to plan and execute a security strategy that allows easy access to Internet services while defeating even the wiliest of hackers.

Firewalls and Internet Security, Second Edition, draws upon the authors' experiences as researchers in the forefront of their field since the beginning of the Internet explosion.

The book begins with an introduction to their philosophy of Internet security. It progresses quickly to a dissection of possible attacks on hosts and networks and describes the tools and techniques used to perpetrate—and prevent—such attacks. The focus then shifts to firewalls and virtual private networks (VPNs), providing a step-by-step guide to firewall deployment. Readers are immersed in the real-world practices of Internet security through a critical examination of problems and practices on today's intranets, as well as discussions of the deployment of a hacking-resistant host and of intrusion detection systems (IDS). The authors scrutinize secure communications over insecure networks and conclude with their predictions about the future of firewalls and Internet security.

The book's appendixes provide an introduction to cryptography and a list of resources (which will also be posted to the book's Web site and updated there regularly) that readers can rely on for tracking further developments in Internet security.

Armed with the authors' hard-won knowledge of how to fight off hackers, readers of ***Firewalls and Internet Security, Second Edition***, can make security decisions that will make the Internet—and their computers—safer.

William R. Cheswick is Chief Scientist at Lumeta Corporation, which explores and maps clients' network infrastructures and finds perimeter leaks. Formerly he was a senior researcher at AT&T Bell Laboratories, where he did pioneering work in the areas of firewall design and implementation, PC viruses, mailers, Internet munitions, and the Plan 9 operating system.

Steven M. Bellovin, one of the creators of Netnews, is a Fellow at AT&T Labs Research. He is a member of the National Academy of Engineering and a frequent participant in National Research Council Activities. He is currently one of the Security Area directors of the Internet Engineering Task Force (IETF).

Aviel D. Rubin (http://avirubin.com) is an Associate Professor in the Computer Science Department at Johns Hopkins University and serves as the Technical Director of their Information Security Institute. He was previously Principal Researcher in the Secure Systems Research Department at AT&T Laboratories and is the author of *White-Hat Security Arsenal* (Addison-Wesley, 2001).

http://www.wilyhacker.com
http://www.awprofessional.com

Text printed on recycled paper

Addison-Wesley
Pearson Education

7 85342 63466 2

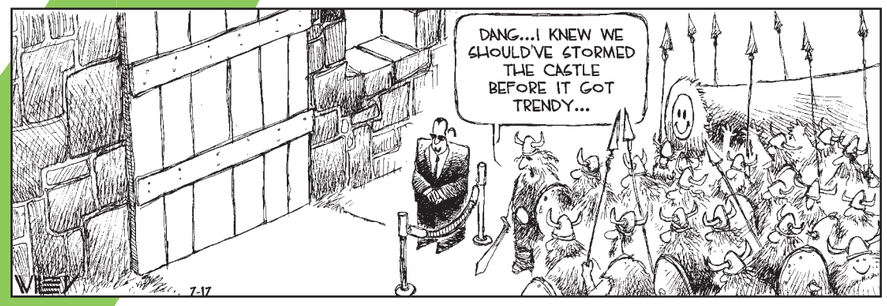
9 780201 634662 54999
ISBN 0-201-63466-X
$49.99 US
$77.99 CANADA

Firewalls and Internet Security
Second Edition
Cheswick
Bellovin
Rubin

Addison
Wesley

Firewalls and Internet Security
Second Edition
Repelling the Wily Hacker

William R. Cheswick
Steven M. Bellovin
Aviel D. Rubin



ADDISON-WESLEY PROFESSIONAL COMPUTING SERIES