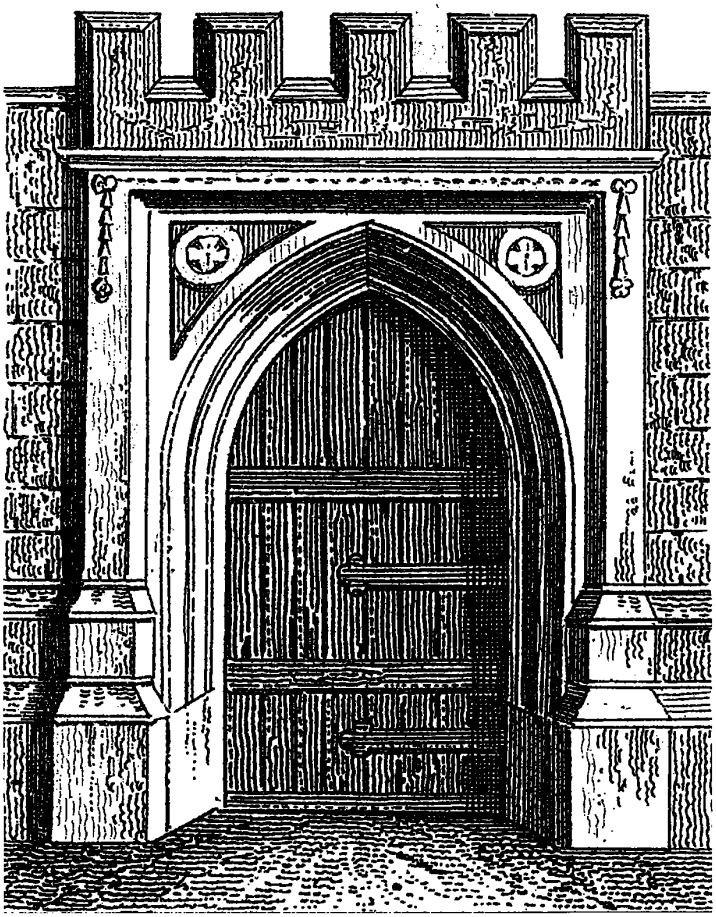
Internet and Web Security

2nd Edition

Covers Unix, Windows NT, and Linux

Building Internet



O REILLY®

Elizabeth D. Zwicky, Simon Cooper
& D. Brent Chapman

Building Internet Firewalls, Second Edition
by Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman

Published by O'Reilly & Associates, Inc., 101 Morris Street, Sebastopol, CA 95472.

Editor: Deborah Russell

Production Editor: Nancy Crumpton

Production Coordinator: Madeleine Newell

Cover Designer: Edie Freedman

Printing History:

April 1995:	First Edition.
November 1995:	Minor corrections.
June 2000:	Second Edition.

Library of Congress Cataloging-in-Publication Data

Zwicky, Elizabeth D.
Building Internet firewalls / Elizabeth D. Zwicky, Simon Cooper & D. Brent Chapman.--
2nd ed. p. cm.
ISBN 1-56592-871-7
1. Computer networks--Security measures. 2. Internet (Computer network)--Security measures. I. Cooper, Simon. II. Chapman, D. Brent. III. Title.

TK5105.59.Z85 2000
005.8--dc21 00-039954

ISBN: 1-56592-871-7 [10/00]
[M]

Preface .....

I. Networ

1. Why Int
What Are
What Are
Who Do
How Can
What Is a
Religious

2. Internet
Secure Se
The Worl
Electronic
File Trans
Remote A
Real-Time
Naming a
Authentic
Administ
Database
Games ..

1

Why Internet Firewalls?

It is scarcely possible to enter a bookstore, read a magazine or a newspaper, or listen to a news broadcast without seeing or hearing something about the Internet in some guise. It's become so popular that no advertisement is complete without a reference to a web page. While nontechnical publications are obsessed with the Internet, the technical publications have moved on and are obsessed with security. It's a logical progression; once the first excitement of having a superhighway in your neighborhood wears off, you're bound to notice that not only does it let you travel, it lets a very large number of strangers show up where you are, and not all of them are people you would have invited.

Both views are true: The Internet is a marvelous technological advance that provides access to information, and the ability to publish information, in revolutionary ways. But it's also a major danger that provides the ability to pollute and destroy information in revolutionary ways. This book is about one way to balance the advantages and the risks—to take part in the Internet while still protecting yourself.

Later in this chapter, we describe different models of security that people have used to protect their data and resources on the Internet. Our emphasis in this book is on the network security model and, in particular, the use of Internet firewalls. A firewall is a form of protection that allows a network to connect to the Internet while maintaining a degree of security. The section later in this chapter called "What is an Internet Firewall?" describes the basics of firewalls and summarizes what they can—and cannot—do to help make your site secure. Before we discuss what you can do with a firewall, though, we want to describe briefly why you need one. What are you protecting on your systems? What types of attacks and attackers are common? What types of security can you use to protect your site?

What Are You Trying to Protect?

A firewall is basically a protective device. If you are building a firewall, the first thing you need to worry about is what you're trying to protect. When you connect to the Internet, you're putting three things at risk:

- Your data: the information you keep on the computers
- Your resources: the computers themselves
- Your reputation

Your Data

Your data has three separate characteristics that need to be protected:

Secrecy
: You might not want other people to know it.

Integrity
: You probably don't want other people to change it.

Availability
: You almost certainly want to be able to use it yourself.

People tend to focus on the risks associated with secrecy, and it's true that those are usually large risks. Many organizations have some of their most important secrets—the designs for their products, financial records, or student records—on their computers. On the other hand, you may find that at your site it is relatively easy to separate the machines containing this kind of highly secret data from the machines that connect to the Internet. (Or you may not; you can't do Internet electronic commerce without having information about orders and money pass through Internet-accessible machines.)

Suppose that you *can* separate your data in this way, and that none of the information that is Internet accessible is secret. In that case, why should you worry about security? Because secrecy isn't the only thing you're trying to protect. You still need to worry about integrity and availability. After all, if your data isn't secret, and if you don't mind its being changed, and if you don't care whether or not anybody can get to it, why are you wasting disk space on it?

Even if your data isn't particularly secret, you'll suffer the consequences if it's destroyed or modified. Some of these consequences have readily calculable costs: if you lose data, you'll have to pay to have it reconstructed; if you were planning to sell that data in some form, you'll have lost sales regardless of whether the data is something you sell directly, the designs from which you build things, or the code for a software product. Intangible costs are also associated with any security

incident. The r
confidence, inv
dence) in your
organization.

Computer se
because dete
find out tha
know. Even
system or da
the intruder
attack is a lc
appear to da
bullet, restor
doesn't appe
yourself, wo
The intruder
making sure

Although th
Chapter 27,
for detecting

Your Reso

Even if you ha
ing system eve
other people a
from this use i
want to charg
puter time anc
they aren't go
your computin

Intruders ofter
their intrusion
argument.

First, it's impc
excess and us
space and hc

incident. The most serious is the loss of confidence (user confidence, customer confidence, investor confidence, staff confidence, student confidence, public confidence) in your systems and data and, consequently, a loss of confidence in your organization.

Has Your Data Been Modified?

Computer security incidents are different from many other types of crimes because detection is unusually difficult. Sometimes, it may take a long time to find out that someone has broken into your site. Sometimes, you'll never know. Even if somebody breaks in but doesn't actually *do* anything to your system or data, you'll probably lose time (hours or days) while you verify that the intruder didn't do anything. In a lot of ways, a brute-force trash-everything attack is a lot easier to deal with than a break-in by somebody who doesn't appear to damage your system. If the intruder trashes everything, you bite the bullet, restore from backups, and get on with your life. But if the intruder doesn't appear to have done anything, you spend a lot of time second-guessing yourself, wondering what he or she might have done to your system or data. The intruder almost certainly has done something—most intruders will start by making sure that they have a way to get back in, before they do anything else.

Although this book is primarily about preventing security incidents, Chapter 27, *Responding to Security Incidents*, supplies some general guidelines for detecting, investigating, and recovering from security incidents.

Your Resources

Even if you have data you don't care about—if you enjoy reinstalling your operating system every week because it exercises the disks, or something like that—if other people are going to use your computers, you probably would like to benefit from this use in some way. Most people want to use their own computers, or they want to charge other people for using them. Even people who give away computer time and disk space usually expect to get good publicity and thanks for it; they aren't going to get it from intruders. You spend good time and money on your computing resources, and it is your right to determine how they are used.

Intruders often argue that they are using only excess resources; as a consequence, their intrusions don't cost their victims anything. There are two problems with this argument.

First, it's impossible for an intruder to determine successfully what resources are excess and use only those. It may look as if your system has oceans of empty disk space and hours of unused computing time; in fact, though, you might be just