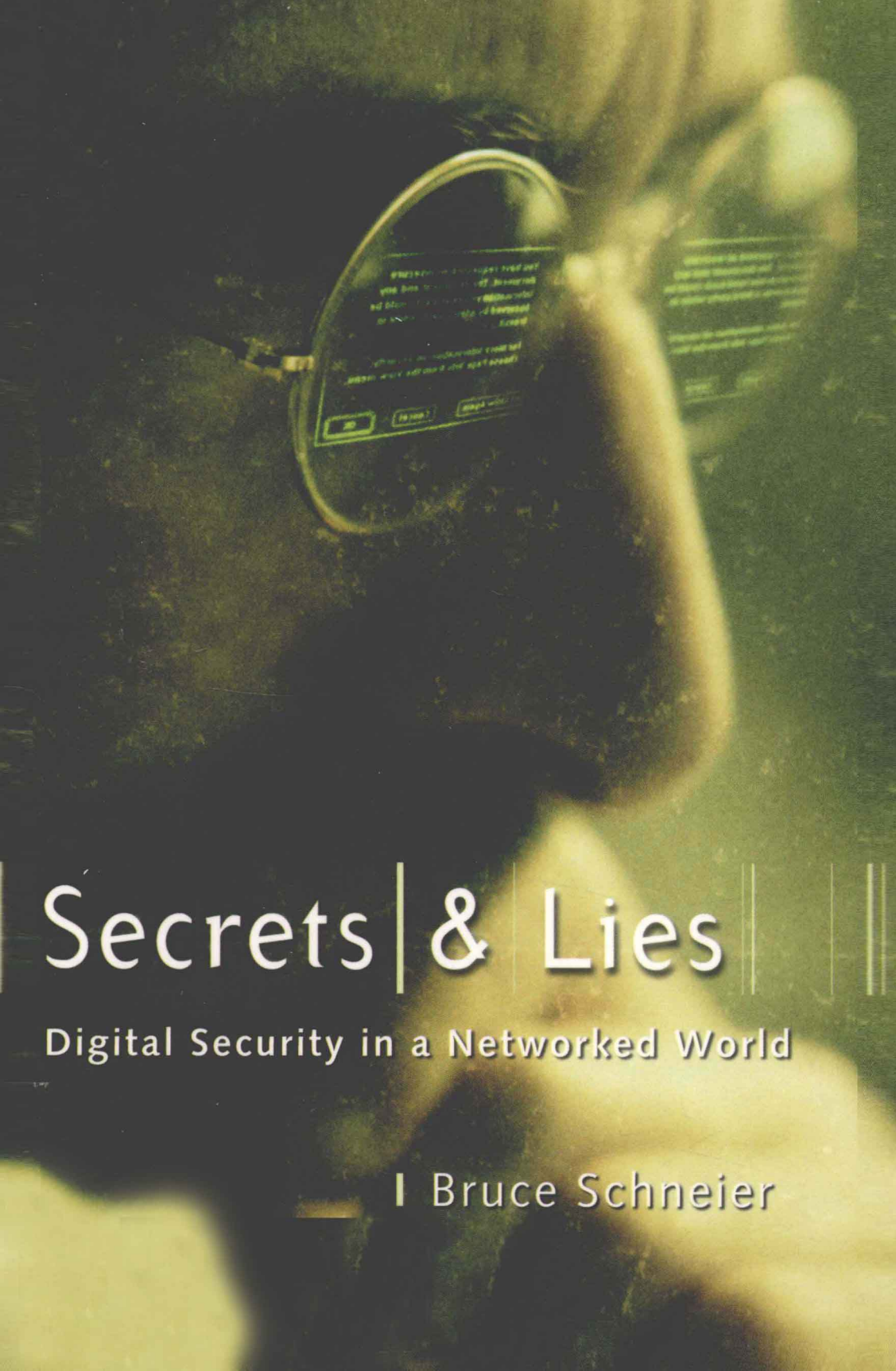
Secrets & Lies
Digital Security in a Networked World
Bruce Schneier

Secrets and Lies

DIGITAL SECURITY IN A NETWORKED WORLD

Bruce Schneier

江苏工业学院图书馆
藏书章

BCA

Secrets and Lies

This edition published 2003
by BCA
by arrangement with John Wiley & Sons, Inc

CN 103996

Publisher: Robert Ipsen
Editor: Carol Long
Associate Editor: Margaret Hendrey
Managing Editor: Micheline Frederick
Associate New Media Editor: Brian Snapp
Text Design & Composition: North Market Street Graphics

Designations used by companies to distinguish their products are often claimed as trademarks. In all instances where John Wiley & Sons, Inc., is aware of a claim, the product names appear in initial capital or ALL CAPITAL LETTERS. Readers, however, should contact the appropriate companies for more complete information regarding trademarks and registration.

Copyright © 2000 by Bruce Schneier. All rights reserved.

Published by John Wiley & Sons, Inc.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4744. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 605 Third Avenue, New York, NY 10158-0012, (212) 850-6011, fax (212) 850-6008, E-Mail: PERMREQ @ WILEY.COM.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in professional services. If professional advice or other expert assistance is required, the services of a competent professional person should be sought.

Printed and bound in Great Britain by Mackays of Chatham Ltd, Chatham, Kent

To Karen: DMASC

此为试读,需要完整PDF请访问: www.ertongbook.com

Preface

I have written this book partly to correct a mistake.

Seven years ago I wrote another book: *Applied Cryptography.* In it I described a mathematical utopia: algorithms that would keep your deepest secrets safe for millennia, protocols that could perform the most fantastical electronic interactions—unregulated gambling, undetectable authentication, anonymous cash—safely and securely. In my vision cryptography was the great technological equalizer; anyone with a cheap (and getting cheaper every year) computer could have the same security as the largest government. In the second edition of the same book, written two years later, I went so far as to write: "It is insufficient to protect ourselves with laws; we need to protect ourselves with mathematics."

It's just not true. Cryptography can't do any of that.

It's not that cryptography has gotten weaker since 1994, or that the things I described in that book are no longer true; it's that cryptography doesn't exist in a vacuum.

Cryptography is a branch of mathematics. And like all mathematics, it involves numbers, equations, and logic. Security, palpable security that you or I might find useful in our lives, involves people: things people know, relationships between people, people and how they relate to machines. Digital security involves computers: complex, unstable, buggy computers.

Mathematics is perfect; reality is subjective. Mathematics is defined;

computers are ornery. Mathematics is logical; people are erratic, capricious, and barely comprehensible.

The error of *Applied Cryptography* is that I didn't talk at all about the context. I talked about cryptography as if it were The Answer™. I was pretty naïve.

The result wasn't pretty. Readers believed that cryptography was a kind of magic security dust that they could sprinkle over their software and make it secure. That they could invoke magic spells like "128-bit key" and "public-key infrastructure." A colleague once told me that the world was full of bad security systems designed by people who read *Applied Cryptography.*

Since writing the book, I have made a living as a cryptography consultant: designing and analyzing security systems. To my initial surprise, I found that the weak points had nothing to do with the mathematics. They were in the hardware, the software, the networks, and the people. Beautiful pieces of mathematics were made irrelevant through bad programming, a lousy operating system, or someone's bad password choice. I learned to look beyond the cryptography, at the entire system, to find weaknesses. I started repeating a couple of sentiments you'll find throughout this book: "Security is a chain; it's only as secure as the weakest link." "Security is a process, not a product."

Any real-world system is a complicated series of interconnections. Security must permeate the system: its components and connections. And in this book I argue that modern systems have so many components and connections—some of them not even known by the systems' designers, implementers, or users—that insecurities always remain. No system is perfect; no technology is The Answer™.

This is obvious to anyone involved in real-world security. In the real world, security involves processes. It involves preventative technologies, but also detection and reaction processes, and an entire forensics system to hunt down and prosecute the guilty. Security is not a product; it itself is a process. And if we're ever going to make our digital systems secure, we're going to have to start building processes.

A few years ago I heard a quotation, and I am going to modify it here: If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

This book is about those security problems, the limitations of technology, and the solutions.

HOW TO READ THIS BOOK

Read this book in order, from beginning to end.

No, really. Many technical books are meant to skim, bounce around in, and use as a reference. This book isn't. This book has a plot; it tells a story. And like any good story, it makes less sense telling it out of order. The chapters build on each other, and you won't buy the ending if you haven't come along on the journey.

Actually, I want you to read the book through once, and then read it through a second time. This book argues that in order to understand the security of a system, you need to look at the entire system—and not at any particular technologies. Security itself is an interconnected system, and it helps to have cursory knowledge of everything before learning more about anything. But two readings is probably too much to ask; forget I mentioned it.

This book has three parts. Part 1 is "The Landscape," and gives context to the rest of the book: who the attackers are, what they want, and what we need to deal with the threats. Part 2 is "Technologies," basically a bunch of chapters describing different security technologies and their limitations. Part 3 is "Strategies": Given the requirements of the landscape and the limitations of the technologies, what do we do now?

I think digital security is about the coolest thing you can work on today, and this book reflects that feeling. It's serious, but fun, too. Enjoy the read.

Acknowledgments

Oodles of people read this book in various stages of completion. I would like to thank Steve Bass, Susan Greenspan, Chris Hall, John Kelsey, and Mudge, who read an early draft of this book. Their comments helped me shape its final tone and scope. I would also like to thank Beth Friedman, who helped with a major edit about halfway through the completion of this book and minor edits throughout the process, and helped keep both the copyeditor and proofreader in line; Karen Cooper, who helped proofread the book; and Raphael Carter, who helped with a major edit toward the end of the process. And I would like to thank Michael Angelo, Ken Ayer, Steve Bass, David Dyer-Bennet, Ed Bennett, Russell Brand, Karen Cooper, David Cowan, Walt Curtis, Dorothy Denning, Carl Ellison, Andrew Fernandez, Gordon Force, Amy Forsyth, Dean Gahlon, Drew Gross, Gregory Guerin, Peter Gutmann, Mark Hardy, Dave Ihnat, Chris Johnston, James Jorasch, Arjen Lenstra, Stuart McClure, Gary McGraw, Doug Merrill, Jeff Moss, Simona Nass, Artimage Nelson, Peter Neumann, Andrew Odlyzko, Doug Price, James Riordan, Bernard Roussely, Tom Rowley, Avi Rubin, Ryan Russell, Adam Shostack, Simon Singh, Jim Wallner, and Elizabeth Zwicky, who read and commented on all or part of the book in its almost-final form. These people did a lot to make the book complete, accurate, and interesting. Any remaining omissions, lingering errors, or residual prolixity are solely my own fault. Open source pundit Eric Raymond has said: "Given enough eyeballs, all bugs are shallow." We'll see if this holds true for books, too.

Secrets and Lies

Contents

此为试读,需要完整PDF请访问: www.ertongbook.com

1

Introduction

During March 2000, I kept a log of security events from various sources. Here are the news highlights:

Someone broke into the business-to-business Web site for SalesGate.com and stole about 3,000 customer records, including credit card numbers and other personal information. He posted some of them on the Internet.

For years, personal information has "leaked" from Web sites (such as Intuit) to advertisers (such as DoubleClick). When visitors used various financial calculators on the Intuit site, a design glitch in the Web site's programming allowed information they entered to be sent to DoubleClick. This happened without the users' knowledge or consent, and (more surprising) without Intuit's knowledge or consent.

Convicted criminal hacker Kevin Mitnick testified before Congress. He told them that social engineering is a major security vulnerability: He can often get passwords and other secrets just by pretending to be someone else and asking.

A Gallup poll showed that a third of online consumers said that they might be less likely to make a purchase from a Web site, in light of recent computer-security events.

Personal data from customers who ordered the PlayStation 2 from the Sony Web site were accidentally leaked to some other customers. (This is actually a rampant problem on all sorts of sites. People try to

check out, only to be presented with the information of another random Web customer.)

Amazon.com pays commissions to third-party Web sites for referrals. Someone found a way to subvert the program that manages this, enabling anyone to channel information to whomever. It is unclear whether Amazon considers this a problem.

The CIA director denied that the United States engages in economic espionage, but did not go on to deny the existence of the massive intelligence-gathering system called ECHELON.

Pierre-Guy Lavoie, 22, was convicted in Quebec of breaking into several Canadian and U.S. government computers. He will serve 12 months in prison.

Japan's Defense Agency delayed deployment of a new defense computer system after it discovered that the software had been developed by the members of the Aum Shinrikyo cult.

A new e-mail worm, called Pretty Park, spread across the Internet. It's a minor modification of one that appeared last year. It spreads automatically, by sending itself to all the addresses listed in a user's Outlook Express program.

Novell and Microsoft continued to exchange barbs about an alleged security bug with Windows 2000's Active Directory. Whether or not this is a real problem depends on what kind of security properties you expect from your directory. (I believe it's a design flaw in Windows, and not a bug.)

Two people in Sicily (Giuseppe Russo and his wife, Sandra Elazar) were arrested after stealing about 1,000 U.S. credit card numbers on the Internet and using them to purchase luxury goods and lottery tickets.

A hacker (actually a bored teenager) known as "Coolio" denied launching massive denial-of-service attacks in February 2000. He admitted to hacking into about 100 sites in the past, including cryptography company RSA Security and a site belonging to the U.S. State Department.

Attackers launched a denial-of-service attack against Microsoft's Israeli Web site.

Jonathan Bosanac, a.k.a. "The Gatsby," was sentenced to 18 months in prison for hacking into three telephone company sites.

The military of Taiwan announced that it discovered more than 7,000 attempts by Chinese hackers to enter the country's security systems. This tantalizing statistic was not elaborated on.

Here are some software vulnerabilities reported during March 2000:

A vulnerability was reported in Microsoft Internet Explorer 5.0 (in Windows 95, 98, NT 4.0, and 2000) that allows an attacker to set up a Web page giving him the ability to execute any program on a visitor's machine.

By modifying the URL, an attacker can completely bypass the authentication mechanisms protecting the remote-management screens of the Axis StarPoint CD-ROM servers.

If an attacker sends the Netscape Enterprise Server 3.6 a certain type of long message, a buffer overflow crashes a particular process. The attacker can then execute arbitrary code remotely on the server.

It is possible to launch some attacks (one denial-of-service attack, and another attack against a CGI script) that Internet Security Systems's RealSecure Network Intrusion Detection software does not detect.

By sending a certain URL to a server running Allaire's ColdFusion product, an attacker can receive an error message giving information about the physical paths to various files.

Omniback is a Hewlett-Packard product that performs system backup routines. An attacker can manipulate the product to cause a denial-of-service attack.

There is a vulnerability in the configuration of Dosemu, the DOS emulator shipped with Corel Linux 1.0, that allows users to execute commands with root privileges.

By manipulating the contents of certain variables, an attacker can exploit a vulnerability in DNSTools 1.0.8 to execute arbitrary code.

SGI has a package called InfoSearch that automatically converts text documentation to HTML Web content. A bug in the CGI script allows attackers to execute commands on the server at the Web server privilege level.

Several vulnerabilities were discovered in the e-mail client The Bat!, allowing an attacker to steal files from users' computers.

Microsoft's Clip Art Gallery lets users download clip art files from the Web. Under certain conditions, a malformed clip art file can let arbitrary code execute on the user's computer.

If you send a long login name and password (even an incorrect one) to BisonWare's FTP Server 3.5, it will crash.

An intruder can crash Windows 95 and 98 computers using specially coded URLs.

Here is a list of the 65 Web sites known to be defaced during the month, as listed at the attrition.org Web site. In this context, "defaced" means that someone broke into the Web site and modified the home page:

Tee Plus; Suede Records; Masan City Hall; The Gallup Organization; Wired Connection; Vanier College; Name Our Child; Mashal Books; Laboratório de Matemática Aplicada da Universidade Federal do Rio de Janeiro; Elite Calendar; Centro de Processamento de Dados do Rio de Janeiro; Parliament of India; United Network for Organ Sharing; UK Jobs; Tennessee State University; St. Louis Metropolitan Sewer District; College of the Siskiyous; Russian Scientific Center for Legal Information, Ministry of Justice; RomTec Plc; Race Lesotho; Monmouth College; University of St. Thomas Library; Int Idea Sweden; Goddard College; Association of EDI Users; Bitstop, Inc; Custom Systems; Classic Amiga; 98 Skate; CU Naked; Korea National University of Education; PlayStation 2; Association for Windows NT System Professionals; K.Net Telecomunicações Ltda.; CyberCT Malaysia; Birmingham Windows NT User Group; Bloem S.A.; Aware, Inc.; Ahmedabad Telephone Online Directory, Ahmedabad Telecom District; Fly Pakistan; Quality Business Solutions; Out; Internet Exposure; Belgium Province de Hainaut; Glen Cove School District; Germantown Academy; Federatie van Wervings en Selectiebureaus; Engineering Export Promotion Council, Ministry of Commerce, India; AntiOnline's AntiCode; Pigman; Lasani; What Online; Weston High School; Vasco Boutique; True Systems; Siemens Italy; Progress Korea; Phase Devices Ltd.; National Treasury Employees Union; National Postal Mail Handlers Union; Metricks; Massachusetts Higher Education Network; The London Institute; Fort Campbell School System; and MaxiDATA Tecnologia e Informatica Ltda.

此为试读,需要完整PDF请访问: www.ertongbook.com