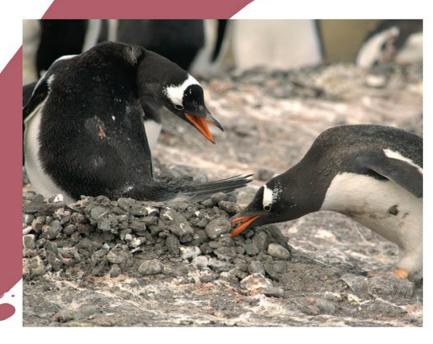
Thinking Security

Stopping Next Year's Hackers



Steven M. Bellovin

Thinking Security

Thinking Security: Stopping Next Year's Hackers

Table of Contents

Contents

Preface

I: Defining the Problem

1 Introduction

- 1.1 Changes
- 1.2 Adapting to Change
- 1.3 Security Analysis
- 1.4 A Few Words on Terminology

2 Thinking About Security

- 2.1 The Security Mindset
- 2.2 Know Your Goals
- 2.3 Security as a Systems Problem
- 2.4 Thinking Like the Enemy

3 Threat Models

- 3.1 Who's Your Enemy?
- 3.2 Classes of Attackers
- 3.3 Advanced Persistent Threats
- 3.4 What's at Risk?
- 3.5 The Legacy Problem

II: Technologies

4 Antivirus Software

- 4.1 Characteristics
- 4.2 The Care and Feeding of Antivirus Software
- 4.3 Is Antivirus Always Needed?
- 4.4 Analysis

5 Firewalls and Intrusion Detection Systems

- 5.1 What Firewalls Don't Do
- 5.2 A Theory of Firewalls
- 5.3 Intrusion Detection Systems
- 5.4 Intrusion Prevention Systems
- 5.5 Extrusion Detection
- 5.6 Analysis



Table of Contents

6 Cryptography and VPNs

- 6.1 Cryptography, the Wonder Drug
- 6.2 Key Distribution
- 6.3 Transport Encryption
- 6.4 Object Encryption
- 6.5 VPNs
- 6.6 Protocol, Algorithm, and Key Size Recommendations
- 6.7 Analysis

7 Passwords and Authentication

- 7.1 Authentication Principles
- 7.2 Passwords
- 7.3 Storing Passwords: Users
- 7.4 Password Compromise
- 7.5 Forgotten Passwords
- 7.6 Biometrics
- 7.7 One-Time Passwords
- 7.8 Cryptographic Authentication
- 7.9 Tokens and Mobile Phones
- 7.10 Single-Sign-On and Federated Authentication
- 7.11 Storing Passwords: Servers
- 7.12 Analysis

8 PKI: Public Key Infrastructures

- 8.1 What's a Certificate?
- 8.2 PKI: Whom Do You Trust?
- 8.3 PKI versus pki
- 8.4 Certificate Expiration and Revocation
- 8.5 Analysis

9 Wireless Access

- 9.1 Wireless Insecurity Myths
- 9.2 Living Connected
- 9.3 Living Disconnected
- 9.4 Smart Phones, Tablets, Toys, and Mobile Phone Access
- 9.5 Analysis

10 Clouds and Virtualization

- 10.1 Distribution and Isolation
- 10.2 Virtual Machines
- 10.3 Sandboxes



Table of Contents

- 10.4 The Cloud
- 10.5 Security Architecture of Cloud Providers
- 10.6 Cloud Computing
- 10.7 Cloud Storage
- 10.8 Analysis

III: Secure Operations

11 Building Secure Systems

- 11.1 Correct Coding
- 11.2 Design Issues
- 11.3 External Links
- 11.4 Trust Patterns
- 11.5 Legacy Systems
- 11.6 Structural Defenses
- 11.7 Security Evaluations

12 Selecting Software

- 12.1 The Quality Problem
- 12.2 Selecting Software Wisely

13 Keeping Software Up to Date

- 13.1 Holes and Patches
- 13.2 The Problem with Patches
- 13.3 How to Patch

14 People

- 14.1 Employees, Training, and Education
- 14.2 Users
- 14.3 Social Engineering
- 14.4 Usability
- 14.5 The Human Element

15 System Administration

- 15.1 Sysadmins: Your Most Important Security Resource
- 15.2 Steering the Right Path
- 15.3 System Administration Tools and Infrastructure
- 15.4 Outsourcing System Administration
- 15.5 The Dark Side Is Powerful

16 Security Process

- 16.1 Planning
- 16.2 Security Policies
- 16.3 Logging and Reporting



Table of Contents

16.4 Incident Response

IV: The Future

17 Case Studies

- 17.1 A Small Medical Practice
- 17.2 An E-Commerce Site
- 17.3 A Cryptographic Weakness
- 17.4 The Internet of Things

18 Doing Security Properly

- 18.1 Obsolescence
- 18.2 New Devices
- 18.3 New Threats
- 18.4 New Defenses
- 18.5 Thinking about Privacy
- 18.6 Putting It All Together

References

Index