INFORMATION SECURITY: PRINCIPLES AND PRACTICE

Preface.

About The Author.

Acknowledgments.

1. Introduction.
1.1 The Cast of Characters.
1.2 Alice's Online Bank.
1.2.1 Confidentiality, Integrity and.
1.2.2 Beyond CIA.
1.3 About This Book.
1.3.1 Cryptography.
1.3.2 Access Control.
1.3.3 Protocols.
1.3.4 Software.
1.4 The People Problem.
1.5 Theory and Practice.
1.6 Problems.

I. CRYPTO.

2. Crypto Basics.
2.1 Introduction.
2.2 How to Speak Crypto.
2.3 Classic Crypto.
2.3.1 Simple Substitution Cipher.
2.3.2 Cryptanalysis of a Simple Substitution.
2.3.3 Definition of Secure.
2.3.4 Double Transposition Cipher.
2.3.5 One-time Pad.
2.3.6 Project VENONA.
2.3.7 Codebook Cipher.
2.3.8 Ciphers of the Election of 1876.
2.4 Modern Crypto History.
2.5 A Taxonomy of Cryptography.
2.6 A Taxonomy of Cryptanalysis.
2.7 Summary.
2.8 Problems.

3. Symmetric Key Crypto.
3.1 Introduction.
3.2 Stream Ciphers.
3.2.1 A5/1.

3.2.2 RC4.
3.3 Block Ciphers.
3.3.1 Feistel Cipher.
3.3.2 DES.
3.3.3 Triple DES.
3.3.4 AES.
3.3.5 Three More Block Ciphers.
3.3.6 TEA.
3.3.7 Block Cipher Modes.
3.4 Integrity.
3.5 Summary.
3.6 Problems.

4. Public Key Crypto.
4.1 Introduction.
4.2 Knapsack.
4.3 RSA.
4.3.1 RSA Example.
4.3.2 Repeated Squaring.
4.3.3 Speeding Up RSA.
4.4 Diffie-Hellman.
4.5 Elliptic Curve Cryptography.
4.5.1 Elliptic Curve Math.
4.5.2 ECC Diffie-Hellman.
4.6 Public Key Notation.
4.7 Uses for Public Key Crypto.
4.7.1 Confidentiality in the Real World.
4.7.2 Signatures and Non-repudiation.
4.7.3 Confidentiality and Non-repudiation.
4.8 Public Key Infrastructure.
4.9 Summary.
4.10 Problems.

5. Hash Functions and Other Topics.
5.1 What is a Hash Function?
5.2 The Birthday Problem.
5.3 Non-cryptographic Hashes.
5.4 Tiger Hash.
5.5 HMAC.
5.6 Uses of Hash Functions.
5.6.1 Online Bids.
5.6.2 Spam Reduction.
5.7 Other Crypto-Related Topics.
5.7.1 Secret Sharing.

- Key Escrow.

5.7.2 Random Numbers.

- Texas Hold 'em Poker.
- Generating Random Bits.

5.7.3 Information Hiding.
5.8 Summary.
5.9 Problems.

6. Advanced Cryptanalysis.
6.1 Introduction.
6.2 Linear and Differential Cryptanalysis.
6.2.1 Quick Review of DES.
6.2.2 Overview of Differential Cryptanalysis.
6.2.3 Overview of Linear Cryptanalysis.
6.2.4 Tiny DES.
6.2.5 Differential Cryptanalysis of TDES.
6.2.6 Linear Cryptanalysis of TDES.
6.2.7 Block Cipher Design.
6.3 Side Channel Attack on RSA.
6.4 Lattice Reduction and the Knapsack.
6.5 Hellman's Time-Memory Tradeo_.
6.5.1 Popcnt.
6.5.2 Cryptanalytic TMTO.
6.5.3 Misbehaving Chains.
6.5.4 Success Probability.
6.6 Summary.
6.7 Problems.

II. ACCESS CONTROL.

7. Authentication.
7.1 Introduction.
7.2 Authentication Methods.
7.3 Passwords.
7.3.1 Keys versus Passwords.
7.3.2 Choosing Passwords.
7.3.3 Attacking Systems via Passwords.
7.3.4 Password Verification.
7.3.5 Math of Password Cracking.
7.3.6 Other Password Issues.
7.4 Biometrics.
7.4.1 Types of Errors.
7.4.2 Biometric Examples.

- Fingerprints.
- Hand Geometry.

- Iris Scan.

7.4.3 Biometric Error Rates.
7.4.4 Biometric Conclusions.
7.5 Something You Have.
7.6 Two-Factor Authentication.
7.7 Single Sign-On and Web Cookies.
7.8 Summary.
7.9 Problems.

8. Authorization.
8.1 Introduction.
8.2 Access Control.
8.2.1 ACLs and Capabilities.
8.2.2 Confused Deputy.
8.3 Multilevel Security Models.
8.3.1 Bell-LaPadula.
8.3.2 Biba's Model.
8.4 Multilateral Security.
8.5 Covert Channel.
8.6 Inference Control.
8.7 CAPTCHA.
8.8 Firewalls.
8.8.1 Packet Filter.
8.8.2 Stateful Packet Filter.
8.8.3 Application Proxy.
8.8.4 Personal Firewall.
8.8.5 Defense in Depth.
8.9 Intrusion Detection.
8.9.1 Signature-based IDS.
8.9.2 Anomaly-based IDS.
8.10 Summary.
8.11 Problems.

III PROTOCOLS.

9. Simple Authentication Protocols.
9.1 Introduction.
9.2 Simple Security Protocols.
9.3 Authentication Protocols.
9.3.1 Authentication Using Symmetric Keys.
9.3.2 Authentication Using Public Keys.
9.3.3 Session Keys.
9.3.4 Perfect Forward Secrecy.
9.3.5 Mutual Authentication, Session Key and PFS.

9.3.6 Timestamps.
9.4 Authentication and TCP.
9.5 Zero Knowledge Proofs.
9.6 The Best Authentication Protocol?
9.7 Summary.
9.8 Problems.

10. Real-World Security Protocols.
10.1 Introduction.
10.2 Secure Socket Layer.
10.2.1 SSL and the Man-in-the-Middle.
10.2.2 SSL Connections.
10.2.3 SSL versus IPSec.
10.3 IPSec.
10.3.1 IKE Phase 1: Digital Signature.
10.3.2 IKE Phase 1: Symmetric Key.
10.3.3 IKE Phase 1: Public Key Encryption.
10.3.4 IPSec Cookies.
10.3.5 IKE Phase 1 Summary.
10.3.6 IKE Phase 2.
10.3.7 IPSec and IP Datagrams.
10.3.8 Transport and Tunnel Modes.
10.3.9 ESP and AH.
10.4 Kerberos.
10.4.1 Kerberized Login.
10.4.2 Kerberos Ticket.
10.4.3 Kerberos Security.
10.5 GSM.
10.5.1 GSM Architecture.
10.5.2 GSM Security Architecture.

- Anonymity.
- Authentication.
- Confidentiality.

10.5.3 GSM Authentication Protocol.
10.5.4 GSM Security Flaws.

- Crypto Flaws.
- Invalid Assumptions.
- SIM Attacks.
- Fake Base Station.

10.5.5 GSM Conclusions.
10.5.6 3GPP.
10.6 Summary.
10.7 Problems.

IV SOFTWARE.

11. Software Flaws and Malware.
11.1 Introduction.
11.2 Software Flaws.
11.2.1 Buffer Overflow.

- Buffer Overflow Example.
- Stack Smashing Prevention.
- Buffer Overflow: The Last Word.

11.2.2 Incomplete Mediation.
11.2.3 Race Conditions.
11.3 Malware.
11.3.1 Brain.
11.3.2 Morris Worm.
11.3.3 Code Red.
11.3.4 SQL Slammer.
11.3.5 Trojan Example.
11.3.6 Malware Detection.

- Signature Detection.
- Change Detection.
- Anomaly Detection.

11.3.7 The Future of Malware.
11.3.8 Cyber Diseases versus Biological Diseases.
11.4 Miscellaneous Software-Based Attacks.
11.4.1 Salami Attacks.
11.4.2 Linearization Attacks.
11.4.3 Time Bombs.
11.4.4 Trusting Software.
11.5 Summary.
11.6 Problems.

12. Insecurity in Software.
12.1 Introduction.
12.2 Software Reverse Engineering.
12.2.1 Anti-disassembly Techniques.
12.2.2 Anti-debugging Techniques.
12.3 Software Tamper-resistance.
12.3.1 Guards. 12.3.2 Obfuscation.
12.3.3 Metamorphism Revisited.
12.4 Digital Rights Management.
12.4.1 What is DRM?
12.4.2 A Real-World DRM System.
12.4.3 DRM for Streaming Media.
12.4.4 DRM for a P2P Application.

12.4.5 DRM in the Enterprise.
12.4.6 DRM Failures.
12.4.7 DRM Conclusions.
12.5 Software Development.
12.5.1 Open versus Closed Source Software.
12.5.2 Finding Flaws.
12.5.3 Other Software Development Issues.
12.6 Summary.
12.7 Problems.

13. Operating Systems and Security.
13.1 Introduction.
13.2 Operating System Security Functions.
13.2.1 Separation.
13.2.2 Memory Protection.
13.2.3 Access Control.
13.3 Trusted Operating System.
13.3.1 MAC, DAC and More.
13.3.2 Trusted Path.
13.3.3 Trusted Computing Base.
13.4 Next Generation Secure Computing Base.
13.4.1 NGSCB Feature Groups.

- Process Isolation.
- Sealed Storage.
- Secure Path.
- Attestation.

13.4.2 NGSCB Compelling Applications.
13.4.3 Criticisms of NGSCB.
13.5 Summary.
13.6 Problems.

Appendices.
A-1 Networking Basics.
A-1.1 Introduction.
A-1.2 The Protocol Stack.
A-1.3 Application Layer.
A-1.4 Transport Layer.
A-1.5 Network Layer.
A-1.6 Link Layer.
A-1.7 Conclusions.
A-2 Math Essentials.
A-2.1 Modular Arithmetic.
A-2.2 Permutations.
A-2.3 Probability.

A-2.4 Linear Algebra.
A-3 DES S-boxes.
Annotated Bibliography.
Index.