



Privacy Protection and Computer Forensics, Second Edition

By Michael Caloyannides

Hardcover / October 2004 /

1580538304

[Link to Publisher](#)

[Link to Amazon](#)

Contents

Introduction

1. Computer Forensics

1.1 What is computer forensics.

1.2 Why is computer forensics of vital interest to you.

1.2.1 *As an employee*

1.2.2 *As an employer or corporate executive*

1.2.3 *As a law enforcement official*

1.2.4 *As an individual*

1.2.5 *As a lawyer for the defense*

1.2.6 *As an insurance company*

1.2.7 *As a user of others' computers*

1.3 If you have done nothing illegal, you have nothing to fear:
not true anywhere!

1.4 Computer forensics

1.4.1 *User rights to privacy.*

1.4.2 *The forensics investigator must know up front*

1.4.3 *Forensics is deceptively simple but requires vast expertise*

1.4.4 *Computer forensics top-level procedure*

1.4.5 *Forensics specifics*

1.4.6 *Digital evidence is often evidence of nothing*

Selected bibliography

2. Locating Your Sensitive Data in Your Computer

2.1 Deleting does not delete—what does.

2.1.1 *General*

2.1.2 *Disk wiping*

2.1.3 *File- and disk-wiping software*

- 2.1.4 *Magnetic microscopy forensic examination of disks*
- 2.2 Where is the sensitive data hiding.
 - 2.2.1 *Cluster tips or slack*
 - 2.2.2 *Free space*
 - 2.2.3 *The swap file*
 - 2.2.4 *Spool and temporary files*
 - 2.2.5 *Forensics on nonmagnetic disks*
 - 2.2.6 *History files*
 - 2.2.7 *Data in the registry files*
 - 2.2.8 *Data from sloppy use of personal encryption software*
 - 2.2.9 *Nonvolatile memory*
- 2.3 The swap file as a source of forensic data
 - 2.3.1 *General*
 - 2.3.2 *Securely wiping the swap file*
- 2.4 The Registry as a source of forensic data
 - 2.4.1 *Why is the Registry a major source of forensic evidence.*
 - 2.4.2 *Where is all this private information hiding in the Registry.*
 - 2.4.3 *Backing up the Registry and restoring a corrupted one*
 - 2.4.4 *Cleaning up sensitive data in the Registry*
- Reference

3.Specialized Forensics Applications

- 3.1 Digital watermarking
- 3.2 The British RIP Act and the US Carnivore (DCS1000)
- Selected bibliography

4.How Can Sensitive Data Be Stolen from One's Computer.

- 4.1 Physical possession of one's computer
- 4.2 Temporary physical access to one's computer
- 4.3 Commercial hardware keystroke loggers
- 4.4 Commercial software keystroke loggers
- 4.5 Going online
 - 4.5.1 *By one's ISP or by anyone having compromised the ISP's security*
 - 4.5.2 *By a legal or an illegal telephone tap*
 - 4.5.3 *By remote Web sites that one accesses*
- 4.6 Spyware in your computer
 - 4.6.1 *By commercial spyware and adware*
- 4.7 van Eck radiation using commercially available systems
 - 4.7.1 *General*
 - 4.7.2 *Protective measures*
 - 4.7.3 *Optical emanations and their interception*
- 4.8 Being on a network, cable modem, or xDSL modem
- 4.9 Other means
- 4.10 Insertion of incriminating data in your computer by others
- 4.11 Security protection steps that don't work well enough
 - 4.11.1 *The fallacy of CMOS password protection*
 - 4.11.2 *The fallacy of password protection offered by popular commercial software*
 - 4.11.3 *The fallacy of protection by hiding files from view*
 - 4.11.4 *The fallacy of protection by hiding data in the slack*
 - 4.11.5 *The fallacy of protection by placing data in normally unused locations of a disk*
 - 4.11.6 *The fallacy of protecting data by repartitioning a disk for a smaller capacity than*

the disk really has

4.11.7 The fallacy of protection through password-protected disk access

4.11.8 The fallacy of protection through the use of booby-trap software

4.11.9 The fallacy that overwriting a file removes all traces of its existence

4.11.10 The fallacy of encryption protection

4.11.11 Other protection fallacies that don't deliver

Selected bibliography

References

5. Why Computer Privacy and Anonymity.

5.1 Anonymity

5.1.1 Practical anonymity

5.2 Privacy

5.2.1 You cannot trust TRUSTe.

5.2.2 Is privacy a right.

5.2.3 The impact of technology on privacy

Selected bibliography

6. Practical Measures For Protecting Sensitive Information

6.1 Installing secure Windows

6.2 Recommended best practices

6.2.1 If using Windows NT

6.2.2 If using Windows 2000

6.2.3 If using Windows XP

6.2.4 Heroic protective measures regardless of the version of Windows

6.2.5 Last but not least

6.3 Additional privacy threats and countermeasures

6.3.1 Individually serial-numbered documents

6.3.2 Online activation and online snooping by software

6.3.3 Microsoft documents that call home

6.3.4 The NetBIOS and other threats from unneeded network services

6.3.5 TCPA/Palladium

6.3.6 The vulnerability of backups

6.4 Protecting sensitive data on hard disks

6.4.1 Full disk encryption

6.4.2 Encrypting disk partitions

Reference

7. Basic Protection from Computer Data Theft Online

7.1 Protection from which of many online threats.

7.2 Installation of Windows for secure online operation

7.3 Online security threats and issues

7.3.1 Web browser hijacking

7.3.2 The romantic e-card and related con schemes

7.3.3 E-mail bombs

7.4 Software to enhance online security

7.4.1 Junkbuster

7.4.2 SurfSecret

7.4.3 Assorted cleaners of browsers

7.5 Basic do's and don'ts

7.5.1 Don'ts

7.5.2 Do's

8. Practical Measures for Online Computer Activities

8.1 Netscape Navigator/Communicator

8.2 Microsoft Internet Explorer

8.3 Desirable e-mail software configuration and modifications

8.3.1 *Free Web-based e-mail offers that require JavaScript: don't!*

8.3.2 *Outlook and Outlook Express*

8.3.3 *Eudora e-mail software*

8.4 Secure e-mail conduct online

8.4.1 *Self-protecting e-mail*

8.4.2 *Accessing e-mail from anywhere on Earth*

8.5 E-mail forensics and traces: the anonymity that isn't

8.5.1 *Tracking suspect e-mail*

8.5.2 *Sending anonymous e-mail: anonymous remailers*

8.5.3 *General network tracing tools*

9. Advanced Protection from Computer Data Theft Online

9.1 Virus/Trojan/worm protection

9.2 Protection from keyloggers

9.2.1 *Protection from keystroke-capturing software*

9.2.2 *Protection from keystroke-capturing hardware*

9.3 Protection from commercial adware/spyware

9.4 Protection from Web bugs: an insidious and far-reaching threat

9.5 Using encrypted connections for content protection

9.6 Using proxy servers for anonymity

9.7 Using encrypted connections to ISPs for content protection

9.7.1 *SSL*

9.8 *SSH*

9.9 The failed promise of peer-to-peer clouds

9.10 Caller ID traps to avoid

9.11 Traps when connecting online from a cellular phone

9.12 Traps when using FTP

9.13 Using instant messaging schemes

9.14 Pitfalls of online banking

9.15 Secure Usenet usage

9.15.1 *Anonymity from other Usenet readers*

9.15.2 *Anonymity from one's in-country ISP*

9.15.3 *Usenet privacy in oppressive regimes*

9.16 Ports to protect from

9.17 Sniffers

9.18 Firewalls

9.18.1 *Personal software-based firewalls*

9.19 Software that calls home

Reference

10. Encryption

10.1 Introduction

10.2 Availability and use of encryption

10.2.1 *Old-fashioned encryption*

10.2.2 *Conventional (symmetric) encryption*

10.2.3 *Public-key encryption*

- 10.2.4 *Elliptic-curve encryption*
- 10.2.5 *Voice encryption online*
- 10.3 Attempts to control against encryption
- 10.4 Legal issues
 - 10.4.1 *Crypto laws around the world*
 - 10.4.2 *Can encryption bans work.*
- 10.5 Societal issues
- 10.6 Technical issues
- 10.7 Countermeasures
- 10.8 State support for encryption
- 10.9 The future of encryption
- 10.10 Quantum cryptography
 - 10.10.1 *Quantum computing*
- 10.11 DNA-based encryption
- 10.12 Comments
- Selected bibliography
- References

- 11. Practical Encryption
 - 11.1 Introduction
 - 11.2 Entire-disk encryption
 - 11.3 Encrypting for e-mail: PGP
 - 11.3.1 *How PGP works*
 - 11.3.2 *Do's and don'ts of PGP installation and use*
 - 11.3.3 *The need for long public keys*
 - 11.3.4 *The man-in-the-middle problem*
 - 11.3.5 *DH or RSA.*
 - 11.3.6 *DSS.*
 - 11.3.7 *Selecting the Symmetric Encryption Algorithm*
 - 11.3.8 *A minor flaw in PGP*
 - 11.3.9 *PGP weaknesses*
 - 11.3.10 *Other uses of PGP*
 - 11.4 Encrypting one's own files: encrypted disk partitions
 - 11.5 Steganography
 - 11.5.1 *Practical considerations in steganography*
 - 11.5.2 *Detecting steganography: steganalysis*
 - 11.5.3 *Other ways that steganography can be detected*
 - 11.5.4 *Recommendations for maintaining privacy through steganography*
 - 11.6 Password cracking
 - 11.7 File integrity authenticity: digital digests
 - 11.8 Emergencies
 - 11.8.1 *Protecting sensitive data from a repressive regime*
 - 11.8.2 *A word of caution*
 - 11.8.3 *Getting discovered as a desirable persona*
 - Selected bibliography
 - References

- 12. Link Encryption: VPNs
 - 12.1 Split tunneling
 - 12.2 IPsec
 - 12.3 Summary
- Selected bibliography

13. Security of Wireless Connectivity: Wi-Fi and Bluetooth

13.1 Background

13.2 The 802.11 technologies

13.2.1 WEP insecurity

13.2.2 War driving and war chalking

13.2.3 Using Wi-Fi while traveling

13.2.4 WPA

13.2.5 Securing 802.11

13.3 Bluetooth wireless link security issues

13.3.1 Bluetooth security threats

13.3.2 Recommended steps for enhancing security of Bluetooth devices

Selected bibliography

14. Other Computer-Related Threats to Privacy

14.1 Commercial GPS devices

14.2 RF ID devices

14.3 Modern vehicles' black boxes

14.4 Cell phones

14.5 Prepaid calling cards

14.6 Credit cards

14.7 Intelligent mail

14.8 Fax machines and telephone answering machines

14.9 Office and home copiers

14.10 Frequent-anything clubs

14.11 Consumer electronics

References

15. Biometrics: Privacy Versus Nonrepudiation

15.1 Are they effective. It depends

15.2 Biometrics can be easily spoofed

15.3 Identification is not synonymous with security

15.4 Societal issues

References

16. Legal Issues

16.1 Software agreements that shift the legal liability to the user

16.2 Cyber-SLAPP suits

16.3 E-mail

16.4 Copyright

16.4.1 U.S. Digital Millennium Copyright Act of 1998

16.4.2 The Uniform Computer Information Transactions Act

16.5 Can one be forced to reveal a decryption key.

16.6 Why is electronic evidence better than paper evidence.

16.7 Civil legal discovery issues

16.8 International policy on computer-related crime

16.9 What is computer crime.

16.10 What can a business do to protect itself.

16.11 Criminal evidence collection issues

16.11.1 Collection

16.11.2 Handling

16.12 Federal guidelines for searching and seizing computers

16.13 Destruction of electronic evidence
16.14 U.S.–European data-privacy disputes
16.15 New international computer crime treaty
16.16 The post–September 11 reality
16.17 The sky is the limit—or is it the courts.
References

About the Author

Index