

Desktop Witness

the do's and don'ts of
personal computer security

Michael A. Caloyannides

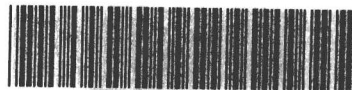
7p309
C165

Desktop Witness

The do's and don'ts of personal computer security

Michael A. Caloyannides

*Senior Fellow
Mitretek Systems
Virginia, USA*



E200201497



JOHN WILEY & SONS, LTD

Copyright © 2002 by John Wiley & Sons Ltd,
Baffins Lane, Chichester,
West Sussex PO19 1UD, England
National 01243 779777
International (+44) 1243 779777
e-mail (for orders and customer service enquiries): cs-books@wiley.co.uk
Visit our Home Page on <http://www.wileyeurope.co.uk>

All Rights Reserved. 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 under the terms of the Copyright, Designs and Patents Act 1988 or under the terms of a licence issued by the Copyright Licensing Agency Ltd, 90 Tottenham Court Road, London, UK W1P 0LP, without the permission in writing of the Publisher with the exception of any material supplied specifically for the purpose of being entered and executed on a computer system for exclusive use by the purchaser of the publication.

Neither the authors nor John Wiley & Sons, Ltd accept any responsibility or liability for loss or damage occasioned to any person or property through using the material, instructions, methods or ideas contained herein, or acting or refraining from acting as a result of such use. The authors and publisher expressly disclaim all implied warranties, including merchantability or fitness for any particular purpose. There will be no duty on the authors or publisher to correct any errors or defects in the software.

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

Michael Caloyannides has asserted his right under the Copyright, Designs and Patents Act 1988 to be identified as the author of this work.

Library of Congress Cataloging-in-Publication Data
(applied for)

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN 0 471 48657 4

Typeset in 10 $\frac{1}{2}$ /12 $\frac{1}{2}$ pt Sabon by Keytec Typesetting, Bridport, Dorset
Printed and bound in Great Britain by Biddles Ltd., Guildford and Kings Lynn
This book is printed on acid-free paper responsibly manufactured from sustainable forestry,
for which at least two trees are planted for each one used for paper production.

Desktop Witness

Dedication

This book is dedicated to my parents, Akylas and Etta, who considered the raising of their children to be their highest priority, and to my two infant children Melody and Brian whom I will not live to see as grown up adults as I am now battling lymphatic cancer. Hopefully, they will carry the torch of individual freedom in a world increasingly opposed to it.

Preface

When asked ‘who are you?’, people in different cultures tend to define themselves fundamentally differently in terms of what their respective culture considers to be most important. In cultures where one’s professional and economic status is most important, people say ‘I am an engineer’, or ‘a priest at St John’s church’, or whatever one’s profession is. In cultures where family ties and ancestry are most important, people say ‘I am John’s son’, or ‘Hsiu’s grandson’. Hardly anywhere does one answer the ‘who are you?’ question by asking ‘in what context?’; societal pressures in most societies force most individuals to have largely one-dimensional personas.

The all too human yearning for security and for acceptance by others often makes some of us internalize and accept our immediate community’s prevailing standards and beliefs as gospel without using any of our own judgment, and viewing with suspicion those that dare question those beliefs. Most in pre WWII Germany accepted Nazism because it was the ‘in’ thing; similarly, most ruthless dictators have a considerable number of followers, and so do most quasi-charismatic leaders of assorted oddball cults even if some of these leaders have mesmerized their followers into committing mass suicide – as has happened time and again.

The yearning by most people to have someone else ‘spoon-feed’ them what is ‘right’ and what is ‘wrong’, and to relieve them of the burden of deciding that for themselves, is, I believe, very strong for most people. It is no surprise, then, that the notion of privacy for others (as opposed to privacy for oneself) is very threatening to many; after all, it implies that someone else may have different views – God forbid – and that privacy may get in the way of the rest of the community knowing that!

For related reasons, citizen privacy is certainly threatening to most any government because it could keep dissent from being identified and being nipped in the bud. Even democratically elected governments that pride themselves in their purported respect for citizen privacy have a catch-all exclusion such as ‘except as lawfully authorized ...’. In short, privacy is OK as long as you believe what the state (or the community) believes. Stated differently, you can choose any color as long as it is the one that is approved.

Having been born and raised in one culture, educated and lived my professional life in another, being married to a wonderful woman from a third culture, and having adopted a child from yet a different culture, I have come to appreciate the fact that a perspective that seems unpalatable to one culture (say, to law enforcers) makes perfectly good sense if seen within the logic framework of a different culture (say, freedom fighters in an oppressive regime). As such, I was not about to write a book preaching any party line, nor a book that is intended solely for one or the other point of view. Instead, this book is intended for anyone who is mature enough to value privacy. Sadly, this is not everyone, although most everyone values his or her own privacy – but not anybody else's.

Although this book deals with some fairly esoteric topics, it is intended to be understandable by anyone with intelligence. Quite simply, this book is for free-thinking, responsible, and mature people who want to write, store, and communicate their ideas with privacy. This includes businesspeople with proprietary documents, physicians with confidential data on patients, philosophers with new ideas, freedom fighters in oppressive regimes, and any person in need of privacy.

This book is for responsible people in need of safeguarding their privacy when using the twenty-first century's primary tool, namely, a computer of some sort. It is *solely* for responsible and mature people, and not for crooks; as with a kitchen knife or a screwdriver, a computer can be used for good and it can be used for evil. This book is emphatically not intended to facilitate the latter.

Gross abuse of anonymity is criminal, unconscionable, unethical, despicable, and shameful. There have been far too many documented cases when individuals' lives have been ruined as a result of anonymous malicious messages to their family, neighbors, employers, and friends. This conduct is positively not what this book is in any way condoning; quite the contrary, such malice should be hunted down and prosecuted.

No sane person is pro-arson or pro-murder, but one should not allow any oppressive regime's self-serving habit of criminalizing every act that it does not like to shape one's own judgment of what is really right or wrong. As an example of some 30 years ago, a military junta in Greece, the birthplace of democracy, banned the study of some ancient Greek philosophers because they talked 'too much' about freedom. Such practice is wrong regardless of what the self-serving laws in the oppressive regime say.

It used to be that the ultimate threat to privacy was some caricature of an authority figure in an oppressive regime, in or out of uniform. It also used to be that just as real a threat was the classical neighborhood 'busybody', that is, the immaturity and intolerance of our neighbors, of our social acquaintances, and of the people that we interfaced with. It was they who would feel threatened enough by our nonconformist views and conduct to consider it their 'obligation' (to whom?) to report to 'the authorities'. Today, conducting ourselves with discretion

is not enough. Technology, such as interception of online traffic, makes the possibility of wholesale surveillance and automated screening not only possible but already in place. Unless one has nothing creative to offer beyond regurgitating the local dogma, one needs effective means of staying out of any oppressive regime's – and even out of one's neighbors – 'radar screens'.

One should also keep in mind that, even under the best of circumstances when one has done nothing wrong, law enforcement databases in even the most technologically advanced country often contain major errors. According to *Wired* reporter Julia Stevens on 11 May 2001 (<http://www.wired.com/news/privacy/0,1848.43743,00.html>), 'when Richard Smith got his FBI file, he learned ... that he had died in 1976 and that he may have been previously married to a woman named Mary ... [and] that he may be known [by] aliases he shares with a couple of convicts doing hard time in Texas'.

Perhaps unwisely, in this book I call a spade a spade, with no deference towards corporations or governments. Inevitably, this candor will offend some corporations and governments. I fully expect this book to be banned in some countries and attempts to be made to discredit it – and me.

In the final analysis, when we lie on our deathbeds we have to seek acceptance by a most critical and unforgiving evaluator of our lives who will see right through any excuse: our own individual conscience.

Michael A. Caloyannides
Washington, DC, January 2002

Acknowledgement

All patents and trademarks are hereby acknowledged as the property of their respective owners.

- stand-alone systems 87–8
- starting clean 82–3
 - hard disk set-up 84
 - installing operating systems 83
 - marking hardware 84
 - memory set-up 84
 - NETBIOS 86
 - online registration of software 85
 - purchasing systems 83
 - RAM-disks 86
 - scheduler 85
 - scrap files 86
 - security patches 85
 - stray magnetic signals 84–5
 - uninterruptable power supply (UPS) 85
 - Visual Basic files 86
 - Windows scripting host 86
- public key encryption 214–15
 - definition 358
- purchasing clean systems 83
- ‘Quicksilver’ 89, 175–6
- RAM-disks 37, 73–4, 86, 94–5, 103
- ‘RealDelete’ 92
- reasonable doubt as a defense 273–5
- ‘RegClean’ 100
- registry 35, 95, 111–12
 - definition 358
 - editing 32–3, 35, 92–3, 112–13
- re-mailers 38, 40
- ‘REPO2000’ 81–2
- resume (curriculum vitae) services, on-line 64–5
- Ricochet wireless telephones 259–60
- ‘Rijandel’ 213, 237
- ‘SafeBack’ 115
- ‘Safeboot’ 138, 139, 140–1
- ‘SafeGuard Easy’ 138
- ‘SafeIt’ 236
- Scandisk utility program 100
- ‘Scorch’ 88, 92
- ‘Scour’ 88
- ‘Scramdisk’ 75, 87, 99, 119–22, 138
- screensavers 54
- ‘Scribble’ 92
- search engines 193–5
- ‘Secret!’ 151
- sectors on a hard drive 76
 - definition 358
 - disowned 77, 81, 96
- ‘Secure Clean’ 88, 91, 100–1
- secure socket layer (SSL) encryption 38, 40, 47, 323–4
 - definition 359
- ‘SecureCRT’ 89
- security, definition 1
- security vulnerabilities
 - adware and spyware 59–64
 - casual snoopers 42–3
 - commercial competitors 51
 - databases 64–5
 - e-mail recipients 51
 - foreign border controls 57–8
 - hard disk evidence 53–4
 - Internet Service Providers (ISPs) 45–9, 154–6
 - national organizations 51–7
 - remote hackers 49–51
 - repair/maintenance personnel 45
 - search engine providers 48–9
 - shared system users 45
 - systems administrator (‘SysAdmin’ or ‘sysop’) 43–5
- September 11 attacks 3–4, 138
- slack at the end of a file 36, 37, 72, 76, 82, 96
- definition 359
- societal cost from lack of privacy 307–11
- South Africa 276–7
- ‘Speak Freely’ 256, 257, 265–70
- ‘Spider’ 181
- ‘SpyAgent Professional’ 128
- ‘Spytech Shadow’ 128
- StarBand satellite telephones 262–3
- steganography 19, 48
 - applicability 239–40
 - considerations 241–2
 - definition 359
 - existing tools 242–3
 - pros and cons 237–9
- ‘Stellar’ 81

- swap file 36, 37, 90–3, 96–7, 101
 - definition 359
 - overwriting procedure 325–9
 - wiping 91–3
- ‘Tauscan’ 137
- TCP/IP, definition 359
- telephony 255
 - anonymized cellphones 264–5
 - anonymized telephones 257–63
 - confidential conversations at a distance 256–7
- terrorism 2–7
- ‘Tiramisu’ 81
- track, definition 359
- ‘Triple-DES’ 213
- trojans 43
- ‘Twofish’ 213, 214
- UK
 - Government use of PGP 228
 - legal framework 25, 45, 275, 276–7
 - employee monitoring 283
 - monitoring 284, 285
 - self-regulation 283–4
 - official justification for computer monitoring 4
- USA
 - legal framework 25, 44, 274, 275, 279
 - 18 USC 1029 act 289
 - 18 USC 1030 act 288–9
 - 18 USC 2252 and 2252A acts 289
 - Digital Millennium Copyright Act (DMCA) 303–4
 - Electronic Communications Privacy Act (ECPA) 286–8
 - employee monitoring 283
 - evidence collected through intrusive technical means 306–7
 - Federal search and seizure 286–92
 - international sweep of DMCA 304–5
 - ‘Patriot Act’ 289–92
 - Privacy Protection Act (PPA) 288
 - security from law enforcement 311–13
 - self-regulation 283–4
 - service provider liability 303–6
 - societal cost 307–11
 - Uniform Computer Information Transactions Act (UCITA) 305–6
 - official justification for computer monitoring 3–4, 6–7, 11–12
- Van Eck radiation 34, 54–7
- virtual memory *see* swap file
- viruses 43
- Visual Basic 86, 144–6
- VPN, definition 359
- Web (World Wide Web), definition 359
- Web bugs 204–7
 - negating 207–9
- ‘Win95pwgrabber’ 125
- ‘Window Washer’ 97, 100
- ‘Windump’ 250
- wiping hard disks 23–4, 32, 77, 95–103
 - definition 359
 - swap file 91–3
- worms 43
- Yahoo! 48–9
- ‘ZapEmpty’ 87
- ‘ZixMail’ 231–4
- ‘ZoneAlarm Pro’ 89, 208

Contents

Preface	xiii
Acknowledgement	xvii
1 The need is very real: author's perspective	1
1.1 But isn't this book helping terrorists? No!	2
1.2 'If you have done nothing wrong, you have nothing to hide'. Not true!	7
1.2.1 The dilemma for law enforcement	13
1.2.2 The Internet undermines regimes' social order	15
2 So you want to encrypt; don't hurt your own interests by so doing	17
2.1 Is encryption the answer to your problem?	20
2.1.1 Encryption algorithms	21
2.2 Common sense is not common	22
2.3 Local laws against encryption	24
2.4 But isn't encryption used by criminals only? No!	26
2.5 Applied psychology	27
3 Protect what and from whom? The answer determines what you should and should not do	31
3.1 Protect what?	31
3.1.1 Protect the content	33
3.1.2 Hiding the 'subject': entry	38
3.1.3 Protecting the information of who communicated with whom	38
3.1.4 Protecting oneself from inferences from observables	41
3.2 Protect from whom?	42
3.2.1 Protecting from casual snooping	42
3.2.2 Protecting from disgruntled or nosy insiders	43
3.2.3 Protecting from the Internet service provider	45
3.2.4 Protecting from a remote hacker	49
3.2.5 Protecting from a commercial competitor	51
3.2.6 Protecting from an untrusted recipient of your e-mail	51
3.2.7 Protecting from overzealous authorities in a repressive regime	51
3.2.8 Protecting from customs agents of foreign repressive regimes at border crossings	57

3.2.9	Protecting from adware and spyware	59
3.2.10	Protecting from worthless 'privacy policies'	64
3.2.11	Protecting from databases where you posted your resume	64
4	Effective protection for computers not connected to networks	67
4.1	Trusting your computer with your life and (relative) freedom	67
4.1.1	File confidentiality in your computer	70
4.1.2	A highly recommended solution	72
4.2	A (readable) tutorial on hard disks	75
4.2.1	The basics	76
4.2.2	EIDE versus SCSI	77
4.2.3	Security aspects of the FDISK command	78
4.2.4	Security aspects of the FORMAT command	79
4.2.5	FAT (file allocation table)	79
4.2.6	FAT32	79
4.2.7	NTFS (new technology file system)	80
4.2.8	Security implications of cluster size	80
4.2.9	Which operating system can read what?	81
4.2.10	Forensics issues	81
4.3	Starting clean	82
4.3.1	Security software	87
4.3.2	Controlling memory bleed: swap file and RAM-disk setting	90
4.4	Secure disk wiping	95
4.5	Password protection is worthless	103
4.6	Office-XP and Windows-XP: don't!	105
4.7	Microphones and cameras in your computer	110
4.8	Windows knows your name	111
4.8.1	Microsoft Word knows and stores your thoughts?	113
4.9	The security problems of backups	114
4.9.1	The problem of making effective backups	114
4.9.2	The problem of protecting the security of backups	116
4.10	Encrypted partitions	118
4.10.1	ScramDisk	119
4.10.2	BestCrypt hidden folder undocumented feature	122
4.10.3	DriveCrypt	124
4.11	Keystroke capturing	125
4.11.1	The threat	125
4.11.2	The countermeasures	133
4.11.3	What if you find your keystrokes <i>are being captured</i> ?	136
4.11.4	How about 'official' keystroke capturing?	136
4.12	The ultimate countermeasure: full disk encryption	138
4.12.1	Technical details	139
4.12.2	Recommendations	140
4.12.3	Biometrics: Do not use unless . . .	141
4.13	Troublesome Microsoft Windows security problems	142
4.13.1	The shell scrap object security problem	142
4.13.2	Other Microsoft Windows vulnerabilities you should fix	144

4.14	Keeping tabs on which programs are running behind your back	149
4.15	Beware devices with infra-red ports	150
4.16	Encryption for PDAs such as the Palm Pilot	150

5	Effective protection for computers connected to the Internet or other networks	153
5.1	Beware of traps	154
5.1.1	Beware of free Internet connectivity offers	154
5.1.2	Beware of Internet software that comes only in a CD ROM	155
5.1.3	Beware of assorted 'security-enhancing services'	156
5.2	Is it what you send or what you receive that matters?	157
5.2.1	ICQ and other instant messengers: Never!	158
5.3	Proxies and maximum online security	160
5.3.1	Basics	160
5.3.2	What are you really trying to do and why?	161
5.3.3	Practical proxy tools	169
5.3.4	Advanced privacy	169
5.4	Remailers	171
5.4.1	Why use them?	171
5.4.2	Private Idaho	174
5.4.3	Jack B. Nymble	175
5.4.4	QuickSilver	175
5.4.5	Vulnerabilities of even sophisticated remailers	176
5.4.6	Gross abuse of remailers and anonymity	177
5.5	Secure and anonymous web browsing	178
5.5.1	Technical issues	180
5.5.2	The fundamental logical problems with all web-based anonymizers	181
5.5.3	Specific web anonymizers worthy of notice	185
5.5.4	So what is the bottom line?	186
5.5.5	Preventing your web browser from contacting select remote sites	187
5.5.6	Cookies	190
5.5.7	Stealth cookies	192
5.5.8	Searching the searcher	193
5.6	Usenet newsgroup security and anonymity	195
5.6.1	Secure Usenet viewing	198
5.6.2	Secure Usenet posting	200
5.7	Web bugs to track e-mail, reading of Usenet posts, and website visits	204
5.7.1	Web bugs and AOL	207
5.7.2	Negating web bugs	207
5.8	Secure e-mail	209
5.8.1	What any encryption software will <i>not</i> do	209
5.8.2	Conventional (symmetric) encryption	213
5.8.3	Public key encryption	214
5.8.4	PGP	215
5.8.5	ZixMail: fine for casual security	231
5.8.6	Easy-to-use anonymizers	234
5.8.7	Safelt and other services	236

5.8.8	Which is really the best algorithm among the five finalists for becoming the advanced encryption standard?	237
5.9	Steganography: hiding in plain view	237
5.9.1	A double-edged sword	237
5.9.2	When would it make sense to use steganography?	240
5.9.3	Do's and don'ts if you must use steganography	240
5.9.4	Using existing steganography tools: <i>not a good idea</i>	242
5.10	Advanced security risks and countermeasures	243
5.10.1	NETBios security risks	243
5.10.2	The RPCSS and DCOM security risks	245
5.10.3	The wireless threat: 802.11b	246
5.10.4	Packet sniffing to defeat keystroke capturers that send captured data through a network connection	248
5.10.5	Peekabooby and M-o-o-t	252
5.10.6	Network sniffing	253
5.11	Excellent websites with current information on PGP	253
5.12	References on cryptography and security	253
5.13	References on digital watermarking	254
6	Encrypted telephony	255
6.1	Confidential conversations in person	255
6.2	Confidential conversations at a distance	256
6.3	Anonymized telephones	257
6.4	Anonymized cellphones	264
6.5	Encrypted telephony over the Internet	265
6.5.1	Demystifying the use of Speak Freely	265
6.5.2	Other voice-encryption software	270
6.5.3	Encrypted voice communications over cellphones	270
7	Legal issues	273
7.1	Reasonable doubt	273
7.2	The impossibility of uniformizing cybercrime laws around the globe	275
7.2.1	South Africa's and other countries' Internet crackdown	276
7.2.2	'Recording' of 'instant messaging'	277
7.3	Attempts to form international cybercrime treaties, and their shortcomings	277
7.4	Computer laws and privacy laws	282
7.4.1	Employee monitoring in the workplace	283
7.4.2	Is industry self-regulation (for privacy) viable?	283
7.4.3	European trends	284
7.5	US federal search and seizure	286
7.5.1	Exactly what are the applicable US laws on computer crime?	286
7.5.2	The Patriot Act and other laws after the 11 September 2001 tragedy	289
7.6	Admissibility of computer-based evidence	292
7.7	Jurisdictional issues	293
7.8	For the law enforcer: arrest or observe?	295
7.9	Legal defense for responsible professionals in oppressive regimes	297

7.9.1	Should you bet your life on the assumption of legal police conduct?	301
7.10	US service provider liability under the Digital Millennium Copyright Act and the death of the Internet for the USA	303
7.10.1	The Digital Millennium Copyright Act is an international matter	304
7.10.2	The Uniform Computer Information Transactions Act	305
7.11	The landmark decision of the US Supreme Court on evidence collected through intrusive technical means	306
7.12	The huge societal costs of excessive lack of privacy for easy law enforcement	307
7.13	Is law enforcement making national information infrastructure more secure or less secure by targeting teenage hackers?	311
8	In conclusion	315
Appendix A		319
A.1	Eudora e-mail reader security fixes	319
Appendix B		323
B.1	Secure socket layer encryption	323
Appendix C		325
C.1	Setting up you Win95/98 computer to overwrite the swap file effectively: a one-time step-by-step procedure	325
Appendix D		331
D.1	Downloading hard-to-find files on the Internet	331
Appendix E		333
E.1	Encryption and hashing algorithms	333
Appendix F		339
F.1	Cleaning after the litter in Internet Explorer, Outlook, and Outlook Express	339
Appendix G		355
G.1	The security flaws of the IEEE 802.11b wireless LAN implementation	355
Glossary		357
Index		360

The Need is Very Real: Author's Perspective

Security is the means by which one makes it difficult for another forcibly to obtain information, whereas privacy is the means by which one makes information unavailable. Privacy and anonymity have been taken for granted in daily life since time started. We buy groceries and movie tickets with cash, we browse at store windows without showing any identification, and we look at newspapers without anyone knowing which particular article we are reading. Lovers have always whispered sweet words in each other's ears in private, and even some formal written and oral communications – such as privileged discussions between lawyer and client – have enjoyed legally sanctioned confidentiality in civilized societies.

This is all changing very rapidly simply because technology makes it easy to break confidentiality. The incentive to violate individuals' privacy exists both in commercial and in government sectors. Commerce has realized the cost-effectiveness of directed advertising to those already known to have an interest in what is being peddled, and has been deploying increasingly sophisticated technical means of identifying who likes what. Repressive governments, which have always feared any dissent, have availed themselves of even more intrusive technologies to create and maintain vast databases about people in order to identify any and all dissent so as to nip it in the bud; sadly, even democratic governments have played up citizens' insecurities and have done the same under the guise of protecting us from each other. One should not forget Montesquieu's words: 'there is no greater tyranny than that which is perpetrated under the shield of law and in the name of justice'. Nor should we forget the words of William Pitt, British Prime Minister, on 18 November 1783: 'Necessity is the plea for every infringement of human freedom; it is the argument of tyrants; it is the creed of slaves'. It is perilous to assume the position that 'I have done nothing wrong, so I am safe'. Holocaust victims had done nothing wrong either but had a lot to fear, and the same is true for numerous executed individuals who have been exonerated post-mortem as a result of DNA testing.

Furthermore, privacy is an essential element of freedom and does not imply any wrongdoing. We shower in private, we try to keep our medical records private, and