

# Contents

About the author . . . . .	xi
Foreword . . . . .	xii
Preface . . . . .	xiv
Acknowledgements . . . . .	xvii
Contact information . . . . .	xx
<b>1 Introduction</b>	<b>1</b>
1.1 Scenario . . . . .	1
1.2 Essential terminology . . . . .	2
1.3 Problems . . . . .	4
1.4 Notation . . . . .	6
<b>2 Ubiquitous computing</b>	<b>8</b>
2.1 Xerox PARC . . . . .	9
2.1.1 Disappearing computing . . . . .	9
2.1.2 Tabs, pads and boards . . . . .	10
2.1.3 Calm technology . . . . .	12
2.2 Norman's Invisible Computer . . . . .	13
2.3 MIT . . . . .	15
2.3.1 Tangible bits . . . . .	15
2.3.2 The WearComp . . . . .	16
2.3.3 Auto-ID . . . . .	21
2.3.4 Oxygen . . . . .	25
2.4 HP's Cooltown . . . . .	26
2.5 ORL/AT&T Labs Cambridge . . . . .	27
2.5.1 The Active Badge . . . . .	28
2.5.2 The Active Floor . . . . .	35
2.5.3 The Active Bat . . . . .	37
2.5.4 TRIP . . . . .	40
2.5.5 PEN . . . . .	43
2.6 Security issues . . . . .	48

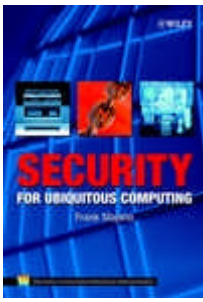
---

2.6.1	The disappearing computer . . . . .	49
2.6.2	The voting button . . . . .	50
2.6.3	The input recognition server . . . . .	50
2.6.4	The Home Medical Advisor . . . . .	51
2.6.5	The Weather and Traffic Display . . . . .	52
2.6.6	The Home Financial Center . . . . .	52
2.6.7	Security versus usability . . . . .	52
2.6.8	The WearCam . . . . .	54
2.6.9	Networked cameras and microphones . . . . .	55
2.6.10	Auto-ID . . . . .	56
2.6.11	The Active Badge and other location systems . . . . .	56
2.6.12	Recording gadgets and other devices that Hollywood dislikes	59
<b>3</b>	<b>Computer security</b>	<b>60</b>
3.1	Confidentiality . . . . .	60
3.1.1	Encryption and decryption . . . . .	61
3.1.2	Security by obscurity (don't) . . . . .	61
3.1.3	Brute force attacks . . . . .	62
3.1.4	The confidentiality amplifier . . . . .	64
3.1.5	Stream and block ciphers . . . . .	65
3.1.6	Public key cryptography . . . . .	66
3.1.7	Hybrid systems . . . . .	67
3.1.8	Other vulnerabilities . . . . .	68
3.2	Integrity . . . . .	69
3.2.1	Independence from confidentiality . . . . .	69
3.2.2	Error-detecting codes . . . . .	70
3.2.3	Hash . . . . .	70
3.2.4	MAC . . . . .	71
3.2.5	Digital signature . . . . .	72
3.2.6	Integrity primitives compared . . . . .	73
3.3	Availability . . . . .	75
3.4	Authentication . . . . .	75
3.4.1	Passwords . . . . .	76
3.4.2	One time passwords . . . . .	77
3.4.3	Challenge-response and man-in-the-middle attacks . . . . .	78
3.5	Security policies . . . . .	82
3.5.1	Setting the goals . . . . .	82
3.5.2	The Bell-LaPadula security policy model . . . . .	83
3.5.3	Beyond multilevel security . . . . .	84

<b>4</b>	<b>Authentication</b>	<b>85</b>
4.1	New preconditions . . . . .	85
4.1.1	The absence of online servers . . . . .	85
4.1.2	Secure Transient Association . . . . .	87
4.2	The Resurrecting Duckling security policy model . . . . .	88
4.2.1	Imprinting and reverse metempsychosis . . . . .	88
4.2.2	Recovery of the imprinting key . . . . .	89
4.2.3	Multilevel souls . . . . .	90
4.2.4	Bootstrapping . . . . .	91
4.2.5	The policy's principles . . . . .	91
4.2.6	Anonymous authentication . . . . .	93
4.2.7	Other uses for the Duckling model . . . . .	94
4.2.8	The computer as a duckling . . . . .	95
4.3	The many ways of being a master . . . . .	98
4.3.1	Human or machine? . . . . .	99
4.3.2	Smart dust . . . . .	99
4.3.3	<i>Mater semper certa</i> . . . . .	100
4.3.4	Further indirection issues . . . . .	102
<b>5</b>	<b>Confidentiality</b>	<b>106</b>
5.1	Cryptographic primitives for peanut processors . . . . .	107
5.1.1	Asymmetric asymmetric cryptosystems . . . . .	107
5.1.2	Maximum rate vs. maximum number of cycles . . . . .	110
5.2	Personal privacy . . . . .	111
5.2.1	The “only dishonest people have things to hide” fallacy . . . . .	111
5.2.2	Leaving traces on shared devices . . . . .	114
5.2.3	Secure disposal vs. encrypted storage . . . . .	118
<b>6</b>	<b>Integrity</b>	<b>123</b>
6.1	Message integrity . . . . .	123
6.1.1	Integrity for point-to-multipoint . . . . .	124
6.1.2	Guy Fawkes . . . . .	125
6.1.3	TESLA . . . . .	126
6.2	Device integrity . . . . .	127
6.2.1	The relationship between integrity and authenticity . . . . .	127
6.2.2	Tamper resistance . . . . .	128
6.2.3	Trusted path . . . . .	131

<b>7</b>	<b>Availability</b>	<b>133</b>
7.1	Threats to the communications channel . . . . .	134
7.1.1	Redefining “denial of service” . . . . .	134
7.1.2	Covert communication techniques . . . . .	135
7.1.3	Speaking to unknowns . . . . .	135
7.1.4	Plutocratic access control . . . . .	136
7.1.5	Cryptographic puzzles . . . . .	137
7.2	Threats to the battery energy . . . . .	138
7.2.1	Peanut devices have limited energy . . . . .	138
7.2.2	Resource reservation . . . . .	140
7.3	Threats from mobile code . . . . .	145
7.3.1	The watchdog timer . . . . .	146
7.3.2	The grenade timer . . . . .	148
7.3.3	Limiting the addressable range . . . . .	150
<b>8</b>	<b>Anonymity</b>	<b>152</b>
8.1	The Cocaine Auction Protocol . . . . .	153
8.1.1	Why a cocaine auction? . . . . .	153
8.1.2	The protocol . . . . .	155
8.1.3	Attacks . . . . .	156
8.2	The anonymity layer . . . . .	160
8.2.1	The dining cryptographers . . . . .	160
8.2.2	Anonymous broadcast based on physics . . . . .	161
8.2.3	A fundamental protocol building block . . . . .	162
8.2.4	The strength (or weakness) of broadcast anonymity . . . . .	164
<b>9</b>	<b>Conclusions</b>	<b>166</b>
<b>A</b>	<b>A short primer on functions</b>	<b>169</b>
A.1	Sets . . . . .	169
A.2	Relations . . . . .	170
A.3	Functions . . . . .	171
A.4	Functions of many arguments . . . . .	173
<b>B</b>	<b>Existing network security solutions</b>	<b>175</b>
B.1	Needham-Schroeder . . . . .	176
B.1.1	The original protocol . . . . .	176
B.1.2	Denning-Sacco . . . . .	177
B.2	Kerberos . . . . .	179
B.3	Public key infrastructures . . . . .	181
B.4	IPSEC . . . . .	184

B.5	SSL/TLS . . . . .	188
B.6	GSM . . . . .	190
B.7	Bluetooth . . . . .	193
B.7.1	System overview . . . . .	193
B.7.2	Security services . . . . .	194
B.7.3	Link keys . . . . .	196
B.8	802.11 . . . . .	200
	<b>Annotated bibliography</b>	<b>204</b>
	<b>Index</b>	<b>244</b>



The book, and this freely available extract, are  
copyright © 2002 by Frank Stajano.  
All rights reserved.

Frank Stajano (University of Cambridge)  
*Security for Ubiquitous Computing*  
John Wiley and Sons, Ltd  
Wiley Series in Communications Networking & Distributed Systems  
ISBN: 0-470-84493-0  
Hardcover; pp. 267 (xx + 247)  
Publication date: 2002-02-12  
RRP: 34.95 GBP (UK); 59 EUR (rest of Europe); 60 USD (USA)

<http://www-lce.eng.cam.ac.uk/~fms27/secubicomp/>