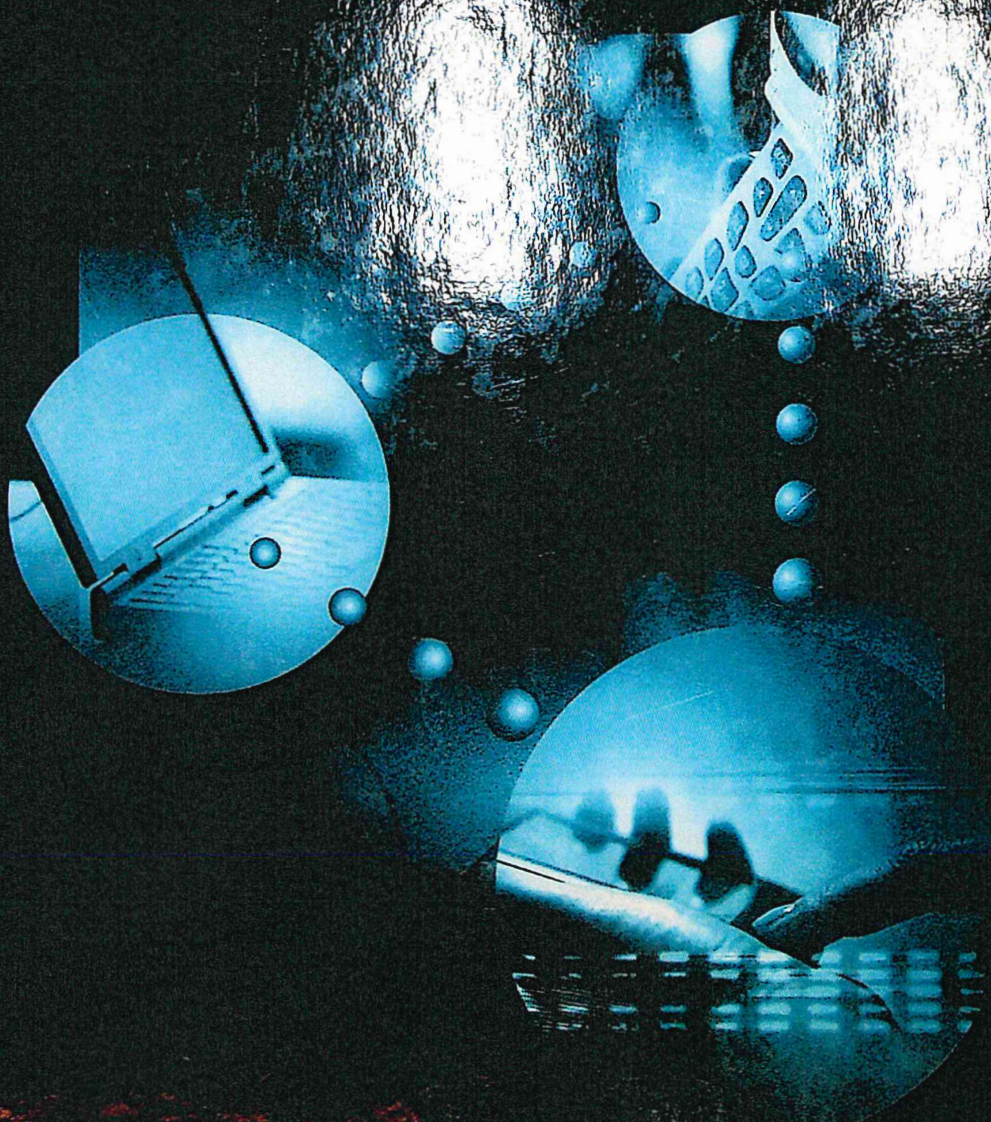


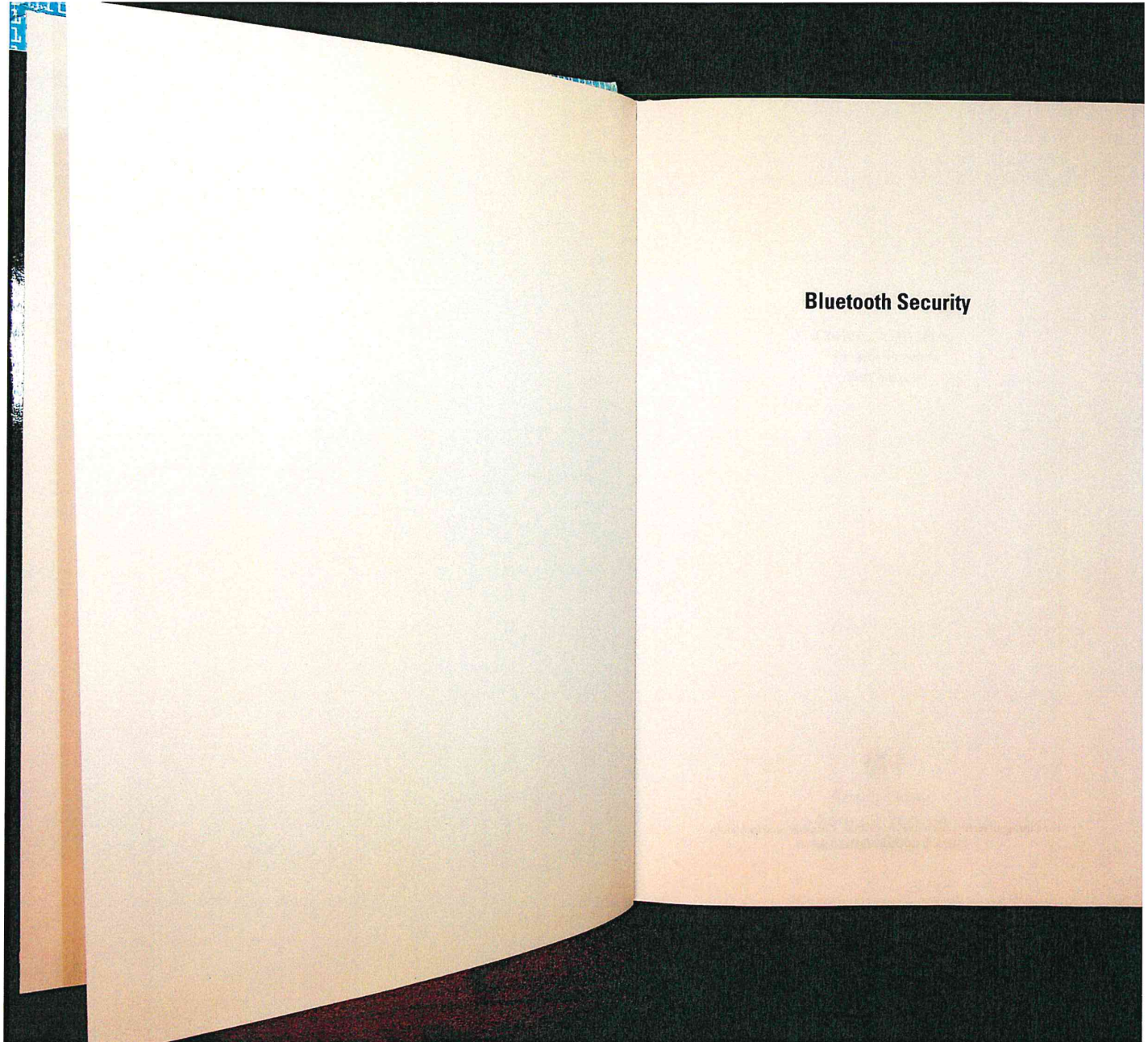
ARTECH HOUSE

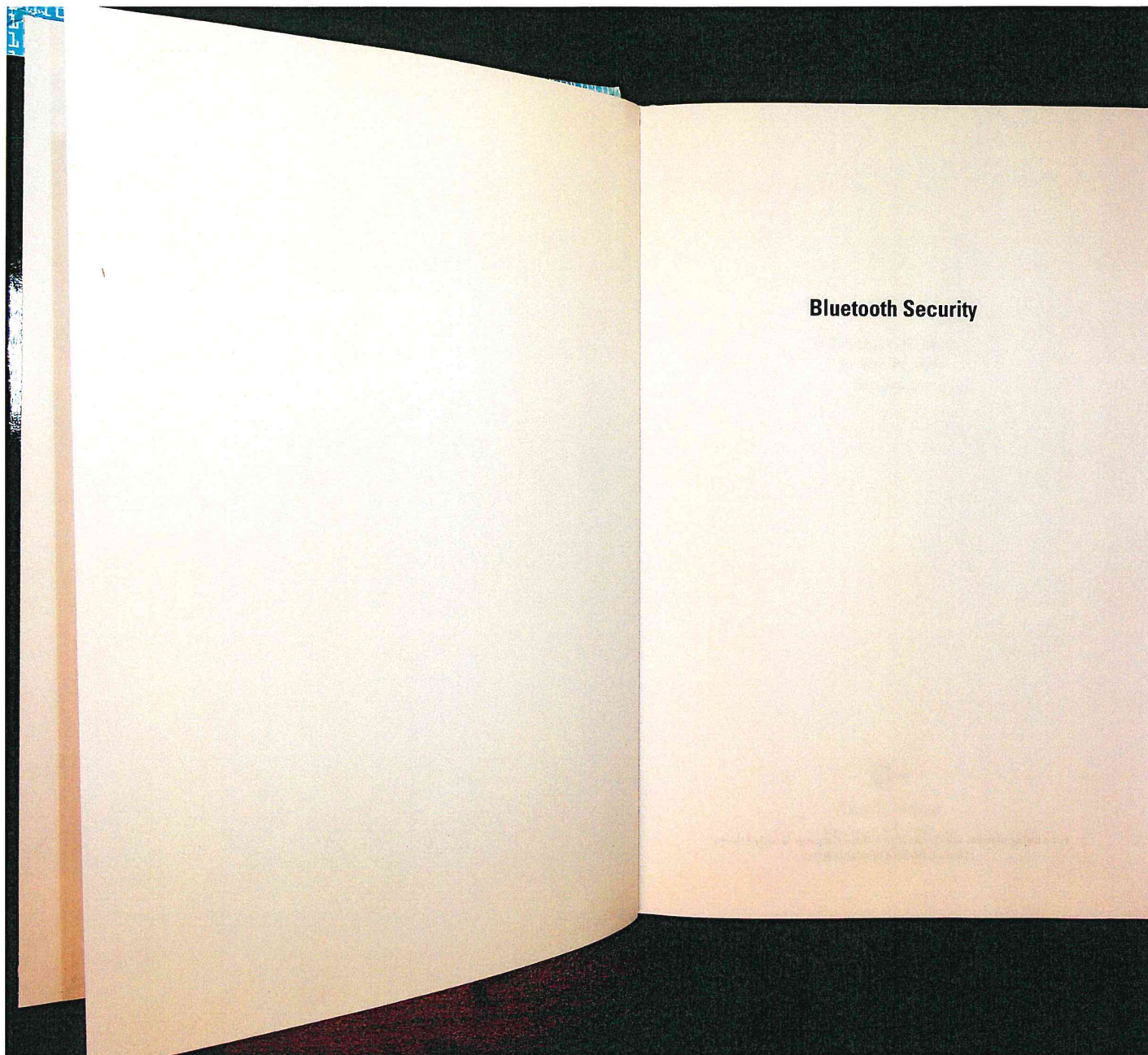
COMPUTER SECURITY SERIES

Bluetooth Security



CHRISTIAN GEHRMANN • JOAKIM PERSSON • BEN SMEETS





For a listing of recent titles in the *Artech House Computer Security Library*,
turn to the back of this book.

Bluetooth Security

Christian Gehrmann
Joakim Persson
Ben Smeets



Artech House
Boston • London
www.artechhouse.com

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the U.S. Library of Congress.

British Library Cataloguing in Publication Data
Gehrman, Christian
Bluetooth security.—(Artech House computing library)
1. Bluetooth technology—Security measures 2. Computer security
I. Title II. Persson, Joakim III. Smeets, Ben
005.8

ISBN 1-58053-504-6
Cover design by Igor Valdman

© 2004 ARTECH HOUSE, INC.
685 Canton Street
Norwood, MA 02062

All rights reserved. Printed and bound in the United States of America. No part of this book may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher.
All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Artech House cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

International Standard Book Number: 1-58053-504-6
10 9 8 7 6 5 4 3 2 1

Contents

Preface	xi
Part I: Bluetooth Security Basics	1
1 Introduction	3
1.1 Bluetooth system basics	3
1.1.1 Background	3
1.1.2 Trade-offs	4
1.1.3 Bluetooth protocol stack	4
1.1.4 Physical layer	6
1.1.5 Baseband	7
1.1.6 Link manager protocol	13
1.1.7 Logical link control and adaptation protocol	15
1.1.8 Host control interface	15
1.1.9 Profiles	17
1.2 Bluetooth security basics	19
1.2.1 User scenarios	19
1.2.2 Notions and terminology	22
References	25

2	Overview of the Bluetooth Security Architecture	27
2.1	Key types	27
2.2	Pairing and user interaction	29
2.3	Authentication	30
2.4	Link privacy	31
2.4.1	Protect the link	32
2.4.2	Encryption algorithm	32
2.4.3	Mode of operation	34
2.4.4	Unicast and broadcast	36
2.5	Communication security policies	37
2.5.1	Security modes	38
2.5.2	Security policy management	42
	References	42
3	Bluetooth Pairing and Key Management	43
3.1	Pairing in Bluetooth	43
3.2	HCI protocol	44
3.3	LM protocol	45
3.4	Baseband events	46
3.4.1	Initialization key generation	47
3.4.2	Unit key generation	47
3.4.3	Combination key generation	49
3.4.4	Authentication	50
3.4.5	Master key generation	52
3.5	User interaction	53
3.6	Cipher key generation	54
3.6.1	Encryption key K_C	55
3.6.2	Constraint key K'_C	57
3.6.3	Payload key K_p	58
3.7	Key databases	58
3.7.1	Unit keys generation requirements	58
3.7.2	Combination key generation requirements	58

3.7.3	Key databases	60
3.7.4	Semipermanent keys for temporary use	63
	References	63
4	Algorithms	65
4.1	Crypto algorithm selection	65
4.1.1	Block ciphers	65
4.1.2	Stream ciphers	66
4.2	SAFER+	67
4.2.1	Authentication algorithm E_1	70
4.2.2	Unit key algorithm E_{21}	71
4.2.3	Initial key algorithm E_{22}	72
4.2.4	Encryption key algorithm E_3	73
4.3	Encryption engine	73
4.4	Ciphering algorithm E_6	74
4.4.1	Initialization	77
4.5	Implementation aspects	79
	References	80
5	Broadcast Encryption	81
5.1	Overview	81
5.2	Preparing for broadcast encryption	82
5.3	Switching to broadcast encryption	83
	References	85
6	Security Policies and Access Control	87
6.1	Objectives	87
6.1.1	Trust relations	88
6.1.2	Security levels	88
6.1.3	Flexibility	89
6.1.4	Implementation considerations	89
6.2	Security manager architecture	90
6.2.1	Overview	90

6.2.2	Device trust level	91
6.2.3	Security level for services	92
6.2.4	Connection setup	92
6.2.5	Database contents and registration procedure	95
	Reference	96
7	Attacks, Strengths, and Weaknesses	97
7.1	Eavesdropping	97
7.2	Impersonation	105
7.3	Pairing	107
7.4	Improper key storage	109
7.4.1	Disclosure of keys	110
7.4.2	Tampering with keys	111
7.4.3	Denial of service	111
7.5	Unit key	112
7.6	Location tracking	113
7.6.1	Bluetooth device address and location tracking	113
7.6.2	Five different types of location tracking attacks	115
7.7	Implementation flaws	116
	References	117
	Part II: Bluetooth Security Enhancements	121
8	Providing Anonymity	123
8.1	Overview of the anonymity mode	123
8.2	Address usage	124
8.2.1	The fixed device address, <i>BD_ADDR_fixed</i>	125
8.2.2	The active device address, <i>BD_ADDR</i>	128
8.2.3	Alias addresses, <i>BD_ADDR_alias</i>	128
8.3	Modes of operation	129
8.4	Inquiry and paging	129
8.4.1	Connectable mode	130
8.4.2	Private connectable mode	

8.4.3	General connectable mode	131
8.5	Alias authentication	131
8.6	Pairing	133
8.7	Anonymity mode LMP commands	133
8.7.1	Address update, LMP <i>active address</i>	134
8.7.2	Alias address exchange, LMP <i>alias address</i>	134
8.7.3	Fixed address exchange, LMP <i>fixed address</i>	135
8.8	Pairing example	136
	References	138
9	Key Management Extensions	139
9.1	Improved pairing	140
9.1.1	Requirements on an improved pairing protocol	140
9.1.2	Improved pairing protocol	141
9.1.3	Implementation aspects and complexity	147
9.2	Higher layer key exchange	149
9.2.1	IEEE 802.1x port-based network access control	150
9.2.2	Higher layer key exchange with EAP TLS	152
9.3	Autonomous trust delegation	154
9.3.1	Security group extension method	154
9.3.2	Public key-based key management	160
9.3.3	Group extension method versus public key method	163
	References	164
10	Security for Bluetooth Applications	167
10.1	Headset	168
10.1.1	Headset security model	168
10.1.2	Pass-key and key management	169
10.1.3	Example	171
10.2	Network access	173
10.2.1	Common access keys	174
10.2.2	Security architecture	175
10.2.3	Network service subscription	175

10.2.4	Initial connection	177
10.2.5	Subsequent access to NAcPs	179
10.3	SIM access	181
10.3.1	The SIM access profile	181
10.3.2	Securing SIM access	182
	References	184
	Glossary	187
	List of Acronyms and Abbreviations	189
	About the Authors	195
	Index	197

Preface

The simple wireless connectivity Bluetooth technology offers is attractive. Therefore, Bluetooth-equipped devices have found their way into quite different environments and are used for a wide range of applications. However, the security aspects must be carefully analyzed in order to decide whether Bluetooth technology indeed provides the right solution for a particular task.

Several books about Bluetooth wireless technology have been written. While these books are excellent at describing the general functionality of Bluetooth devices, they are not particularly detailed when it comes to the security-related aspects of Bluetooth technology. This book is different in this respect, since it is completely devoted to security matters.

The security features that are defined in the specification are thoroughly discussed and described in the book. Moreover, several interesting facts with respect to this are pinpointed. Specifically, both strong and weak points of Bluetooth security are identified. Additionally, we do not limit ourselves to what directly has been written in the specification. We also want to give some insight into how potential risks and security threats will affect deployment of Bluetooth technology.

This book is divided into two parts. Chapters 1 through 7 (Part I) discuss the security functionality defined on the basis of the Bluetooth version 1.2 specification. However, security is not a feature that comes alone in a system. Security only has a meaning in a certain context. Therefore, the first chapter of this book provides an overview of the Bluetooth system. The communication principles and the security-related functions in the system are covered. For the reader not familiar with security concepts and terminology, the notions and terms used in this book are explained. The security-related functions in the Bluetooth

ciphering key derived from the constrained encryption key K'_C . This key is the initial state of the ciphering engine prior to generating the overlay sequence. A summary of the different key types can be found in Table 2.1. More details on the encryption keys is given in Section 2.4.1.

2.2 Pairing and user interaction

As indicated earlier, the pairing of two devices is the procedure by which two devices establish a shared secret that they can use when they meet again. The pairing requires user interaction, for example, the entering of a pass-key.¹ See Figure 2.1(a). The Bluetooth system allows the pass-key to be 128 bits long. Such a large pass-key value would be rather user unfriendly for manual input. However, this feature allows the use of a higher level automated key agreement scheme that can “feed” the agreed pass-key into the pairing procedure. See Figure 2.1(b). The high-level key agreement scheme can be a network or *transport layer security* (TLS) protocol. Examples of such protocols are the Internet Engineering Task Force (IETF) protocols TLS [1] and Internet key exchange (IKE) [2].

There are two kinds of pass-keys in Bluetooth terminology: the *variable* pass-key and the *fixed* pass-key. The first type represents a pass-key that can be arbitrarily chosen at the pairing instance. This requires that some form of user interaction takes place in order to feed the Bluetooth device with the appropriate pass-key value. This interaction is most likely accomplished using a keyboard or numerical keypad. An example of a typical device with a variable pass-key is the mobile phone. In contrast, the fixed pass-key cannot be chosen arbitrarily when it is needed. Instead, a predetermined value must be used. This type of pass-key is used when there is no user interface to input a value to the Bluetooth

Table 2.1
Overview of Key Types

Purpose	Semipermanent		Temporary	
Authentication key generation	Unit key	Combination key	Initialization key	Master key
Ciphering			Encryption key Constrained encryption key	Payload key

1. In the Bluetooth specification, one sometimes uses the term personal identification number (PIN).

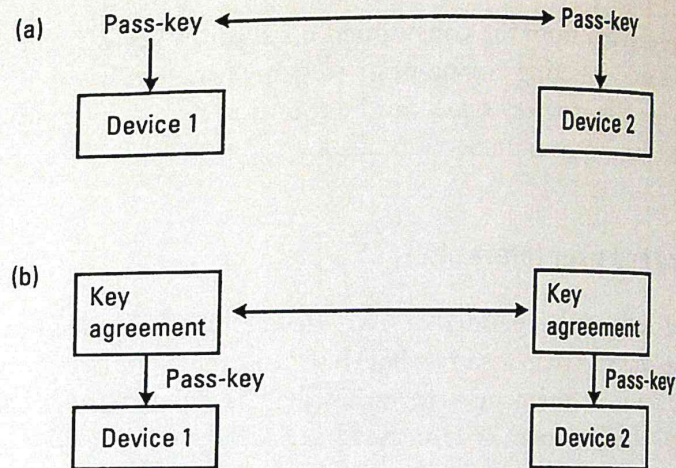


Figure 2.1 (a) Pairing through manual user interaction, and (b) pairing through separate key agreement protocol.

device. Clearly, for a pairing to work, only one device can have a fixed pass-key (unless, of course, both devices happen to have the same fixed pass-key). Examples of devices in need of fixed pass-keys are Bluetooth-enabled mice and headsets. These gadgets come with a factory preset pass-key when delivered to the customer.

Note that a fixed pass-key need not be “fixed” in the sense that it can never be changed. Preferably, the user is allowed to change the fixed pass-key in some way. In some scenarios, a wired connection could be used, for example, by plugging in an external keyboard and changing the pass-key. This is only feasible if it is difficult for anyone but the rightful owner to have physical access to the Bluetooth device in question. More interesting is to allow the change over Bluetooth using an already paired device (equipped with the necessary user interface) over a *secure connection*. This implies that the user connects to the device with a fixed pass-key, authenticates itself, and requests the link to be encrypted before a fresh pass-key value can be sent to the remote device. The new value replaces the old one and becomes the fixed pass-key to use in subsequent pairings. In Chapter 3 we will come back to the details of the pairing procedure.

2.3 Authentication

A Bluetooth device in a connectable state accepts connection requests from other devices. This means that there is a risk that a connectable device is connected to and attacked by a malicious device. Obvious, this can be avoided by never entering a connectable state. On the other hand, that implies that no Bluetooth connections at all can be established. Accordingly, there is a need to

This first-of-its-kind book, written by expert authors who actively contribute to the evolution of Bluetooth specifications, provides an overview and detailed descriptions of all the security functions and features of this standard's latest core release. After categorizing all the security issues involved in ad hoc networking, this hands-on volume explains how to design a highly secure Bluetooth system and implement security enhancements. The book also helps practitioners fully understand the main security risks involved with introducing Bluetooth-based communications in their applications.

This cutting-edge resource covers the most significant attacks on Bluetooth security mechanisms and their implementations, demonstrating how some of these known weaknesses can be avoided with appropriate defensive measures. The book presents concrete examples of how to design security solutions for some Bluetooth applications and how to build on these applications. Professionals find real-world case studies including technical algorithms, mechanisms and protocols, and security architectures. These architectures offer valuable guidelines for use in building Bluetooth and non-Bluetooth-specific security mechanisms.

Christian Gehrman is a senior specialist in security architectures and protocols for Ericsson Mobile Platforms AB. He was formerly the chairman of the Bluetooth SIG Security Expert Group. Dr. Gehrman holds a Ph.D. in information theory and an M.Sc. in electrical engineering from Lund University.

Joakim Persson is a technical manager of new technology in the research department of Ericsson Mobile Platforms AB. He has been playing an active role in the Bluetooth SIG Radio Working Group for many years. Dr. Persson holds a Ph.D. in information theory and an M.Sc. in computer engineering from Lund University.

Ben Smeets is an Ericsson expert in security systems and data compression at Ericsson Mobile Platforms AB. He is also a full professor in digital switching theory at Lund University. Dr. Smeets holds a Docent degree and Ph.D. in digital techniques from Lund University and an M.Sc. in electrical engineering from Eindhoven University of Technology.

