

Iosif I. Androulidakis

Mobile Phone Security and Forensics

A Practical Approach

Second Edition



Springer

Mobile Phone Security and Forensics

Iosif I. Androulidakis

Mobile Phone Security and Forensics

A Practical Approach

Second Edition

 Springer

Iosif I. Androulidakis
Pedini Ioannina
Greece

ISBN 978-3-319-29741-5 ISBN 978-3-319-29742-2 (eBook)
DOI 10.1007/978-3-319-29742-2

Library of Congress Control Number: 2016931614

© Springer International Publishing Switzerland 2016

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

To my parents

Preface

Welcome to the second edition of “Mobile Phone Security and Forensics.” The dominance of mobile phones has continued since the publication of the first version of the book, in an ever-increasing rate. However, while we are enjoying the technological advances that mobile phones offer, we are also facing new security risks coming as a cost of our increasing dependence on the benefits of wireless communications.

The purpose of this book is the same as before: to raise user awareness in regard to security and privacy threats present in the use of mobile phones. It is focused on practical issues and easy to follow examples, skipping theoretical analysis of algorithms and standards. Most sections have been enriched with new material. The book is more geared toward the mobile devices themselves and not the underlying networks, so most of the contents are applicable irrespectively of the “generation” of the network (GSM, 3G, 4G, etc.) to GSM and UMTS alike. The goal is to achieve a balance, including both technical and nontechnical chapters. Amateurs as well as experienced users will benefit from the overview of threats and the valuable practical advice. They will also get to know various tricks affecting the security of their phone. More advanced users will appreciate the technical discussions and will possibly try experimenting with the forensics and mobile phone control techniques presented in the respective chapters.

Chapter 1 gives an introduction to confidentiality, integrity, and availability threats in mobile telephones, providing the background for the rest of the book. In Chap. 2, the results of a large-scale survey and some following ones are presented, placing the user as one of the weakest links in the security landscape. With eavesdropping being one of the most apparent threats, a specific interception technique is examined in Chap. 3, while at the same time the inefficiencies of mobile phones’ graphical user interfaces are highlighted in regard to security. The chapter is further enriched since the previous edition with a discussion regarding software defined radio and other advances in mobile telephony communications interception. Chapter 4 is the more diverse themed chapter of the book covering device and network codes, commands to control the phone, and software and hardware tricks. Software and mobile applications’ security are not extensively covered since they mostly fall in computer security

literature. Chapter 5 is devoted to security in SMS, as a leading service in mobile telephony. Moreover, there is an extended discussion for fighting unsolicited SMS messages (spam). Following, a chapter focusing on the procedures and techniques of forensics reminds us that mobile phones will sooner or later be criminals' preferred target. Concluding the book, Chap. 7 synthesizes the previous chapters and provides a condensed list of practical security advices users should follow.

Closing, I would like to thank my family for all the support and love, my professors in Greece and Slovenia for their mentoring during my studies, and the security researchers all over the world I have met and collaborated with. They are all too many to be listed here but they know who they are! Last, but not least, I would like to thank my editor and all of the members of the Springer team that I collaborated with. With such a good collaboration writing, the second version of the book was a true pleasure. I hope you will enjoy reading it. Writing a book is a hard and long process but thanks to my editor's guidance everything proceeded pleasantly and smoothly.

Ioannina, Greece
October 2015

Iosif I. Androulidakis, Ph.D., Ph.D.

Contents

- 1 Introduction: Confidentiality, Integrity, and Availability Threats in Mobile Phones.** 1
 - 1.1 Introduction 1
 - 1.2 Confidentiality 2
 - 1.3 Integrity 4
 - 1.4 Availability. 7
 - 1.5 Manufacturers’ Responsibilities 10
 - 1.6 Malicious Software and Other Issues 11
 - 1.7 Conclusion 11
 - References. 12
- 2 A Multinational Survey on Users’ Practices, Perceptions, and Awareness Regarding Mobile Phone Security** 15
 - 2.1 Introduction 15
 - 2.2 Methodology 16
 - 2.3 Results 17
 - 2.3.1 In General. 17
 - 2.3.2 Demographics 18
 - 2.3.3 Economics 18
 - 2.3.4 Security-Specific Questions. 20
 - 2.4 Related Work 22
 - 2.5 Conclusion 23
 - References. 26
- 3 Voice, SMS, and Identification Data Interception in GSM.** 29
 - 3.1 Introduction 29
 - 3.2 Practical Setup and Tools. 31
 - 3.3 Implementation 34
 - 3.4 Problem Solution 36
 - 3.4.1 In General. 36

3.4.2	History of the Ciphering Indicator	37
3.4.3	Recent Additions	39
3.4.4	The Actual Situation	39
3.5	Software-Defined Radio and Modified Firmware	43
3.6	Conclusion	44
	References	45
4	Software and Hardware Mobile Phone Tricks	47
4.1	Introduction	47
4.2	Netmonitor	47
4.3	GSM Network Service Codes	48
4.3.1	In General.	48
4.3.2	Forwarding Services	50
4.3.3	Barring Services.	51
4.3.4	Passwords.	51
4.3.5	Calling Line and Caller Identification	52
4.3.6	Call Management.	53
4.4	Mobile Phone Codes	55
4.5	Catalog Tricks	58
4.6	AT Command Set.	59
4.6.1	In General.	59
4.6.2	Identification	60
4.6.3	Call Control	60
4.6.4	Device Control	61
4.6.5	Catalogs	62
4.6.6	SMS	62
4.6.7	SIM Access	66
4.7	Software	66
4.8	Hardware	67
4.9	Conclusion	68
	References	69
5	SMS Security Issues	71
5.1	Introduction	71
5.2	Availability Issues	72
5.3	Confidentiality Issues.	73
5.4	Integrity Issues.	75
5.5	Other Security Issues	77
5.6	SMS Spam	78
5.7	Conclusion	84
	References	84
6	Mobile Phone Forensics	87
6.1	Introduction	87
6.2	Crime and Mobile Phones	88
6.3	The Evidence	89

6.4	Fundamental Questions and Problems	90
6.5	Forensic Procedures	91
6.5.1	Introduction	91
6.5.2	In General.	91
6.5.3	Training and Competence	92
6.5.4	The Analysis Procedure Itself	93
6.5.5	Data Preservation and Isolation from the Network	94
6.5.6	Identification of the Phone.	95
6.5.7	Examination of the SIM Card and the Memory of the Phone	96
6.5.8	Findings Report	97
6.6	The SIM Card	97
6.7	Files Present in SIM Card	99
6.7.1	In General.	99
6.7.2	International Mobile Subscriber Identity.	100
6.7.3	Integrated Circuit Card Identifier.	101
6.7.4	Location Information File and Broadcast Control Channel File.	102
6.7.5	SMS Storage File.	102
6.7.6	Abbreviated Dialing Numbers (Contact List)	104
6.7.7	Last Numbers Dialed (Outgoing Calls)	104
6.8	Device Data	104
6.9	External Memory Dump	106
6.10	External Memory Cards and Computers	107
6.11	Evidence in the Operator's Network	107
6.12	Conclusion	107
	References.	108
7	Conclusion	111
7.1	In General.	111
7.2	Practical Security Advices.	112
	About the Author	115
	Index.	117