

SPRINGER BRIEFS IN
ELECTRICAL AND COMPUTER ENGINEERING

Iosif I. Androulidakis

VoIP and PBX Security and Forensics A Practical Approach

Second Edition

 Springer

SpringerBriefs in Electrical and Computer Engineering

More information about this series at <http://www.springer.com/series/10059>

Iosif I. Androulidakis

VoIP and PBX Security and Forensics

A Practical Approach

Second Edition



Springer

Iosif I. Androulidakis
Pedini Ioannina
Greece

ISSN 2191-8112 ISSN 2191-8120 (electronic)
SpringerBriefs in Electrical and Computer Engineering
ISBN 978-3-319-29720-0 ISBN 978-3-319-29721-7 (eBook)
DOI 10.1007/978-3-319-29721-7

Library of Congress Control Number: 2016934056

© 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

Apart from the public telephone network we all know, there is a parallel private network, consisting of private branch exchanges (PBXs). These are privately owned telephone exchanges that serve the communication needs of a private or public entity making connections among internal telephones and linking them to other users in the public telephone network.

Modern societies rely on telecommunication infrastructure more than ever. PBXs serve Hospitals, Ministries, Police, Army, Banks, Public bodies/authorities, Companies, Industries, and so on. This leads to the assumption that most—if not all—of the nations' vital infrastructures rely on PBXs as well. As such, it is not an exaggeration to state that PBXs are part of a nation's critical infrastructure. The purpose of this second edition of the book, therefore, is to raise user awareness in regard to security and privacy threats present in PBXs, helping both users and administrators safeguard their systems. Moreover, this second edition has an extended coverage on VoIP systems.

It is focused on practical issues and easy-to-follow examples, skipping theoretical analysis of algorithms and standards. The book is more geared towards the telephony as a service and the devices themselves and not the underlying networks, so most of the contents are applicable to PSTN and VoIP alike. The contents are balanced, including both technical and nontechnical chapters. Amateur as well as experienced administrators will benefit from the overview of threats and the valuable practical advice. They will also get to know various issues affecting the security of their PBX while they will also learn the fraudsters' modus operandi. More advanced administrators will appreciate the technical discussions and will possibly try experimenting with the forensics and PBX control techniques presented in the respective chapters.

Chapter 1 gives an introduction to PBXs and the scene, statistics, and involved actors. Confidentiality, integrity, and availability threats are discussed in Chap. 2 providing the background for the highly technical discussion of Chap. 3. Having examined the threats and the technical background, Chap. 4 deals with security. Forensics involving PBXs are covered in Chap. 5. Concluding the book, Chap. 6 synthesizes the previous chapters.

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 with whom I have met and collaborated. There are 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 the members of the Springer team with whom I have collaborated. I hope you will like this book as much as I enjoyed writing it.

Ioannina, Greece
October 2015

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

Contents

1	Introduction	1
1.1	About PBXs.....	1
1.2	PBXs as Critical Infrastructure.....	3
1.3	The Scene	5
1.4	The Players	6
1.5	Conclusion.....	7
	References.....	8
2	Confidentiality, Integrity, and Availability Threats in PBXs	9
2.1	Introduction	9
2.2	Confidentiality	9
2.3	Integrity	14
2.4	Availability	18
2.5	Other Threats.....	21
2.6	Specifically for VoIP	22
2.7	Conclusion.....	23
	References.....	24
3	PBX Technical Details	25
3.1	The PBX Basic Structure	25
3.2	Connection to the Outside World	25
3.3	Distribution Frames-Cabling.....	26
3.4	Physical Parameters.....	26
3.5	PBX Boards and Hardware	29
3.6	PBX Sets	31
3.7	The CPU and the Management Port.....	37
3.8	Software, Administration, and Management Suite and Station	41
3.9	Low Level Tools	43
3.10	Database	44
3.11	Non-predicted Feature Interaction.....	45

- 3.12 The Most Exploited PBX Services..... 46
 - 3.12.1 Direct Inwards System Access (DISA)..... 46
 - 3.12.2 Voice Mail 46
- 3.13 Complementary Systems..... 47
- 3.14 Other Dangerous Points..... 48
- 3.15 On VoIP Security..... 48
- 3.16 On a PBX Malware 50
 - 3.16.1 Start 51
 - 3.16.2 Search for Targets..... 52
 - 3.16.3 Verify the Target Is a PBX 52
 - 3.16.4 Enter-Break into the Target 52
 - 3.16.5 Upload Itself and the Payload 52
 - 3.16.6 Stay Stealth Until the Period of Activation
(Hatch Period)..... 53
 - 3.16.7 Use the Resources Compromised to Find
Other PBXs 53
 - 3.16.8 Activate the Payload..... 53
 - 3.16.9 Delete Itself and Logs 53
- 3.17 Conclusion..... 54
- References..... 54
- 4 PBX Security 55**
 - 4.1 Introduction 55
 - 4.2 Physical Security 55
 - 4.3 Nontechnical Security Issues..... 56
 - 4.4 Technical Security Issues 59
 - 4.4.1 Local and Remote Management..... 59
 - 4.4.2 Settings and Configuration..... 61
 - 4.4.3 Software and Hardware 62
 - 4.4.4 Audits 63
 - 4.4.5 In Conclusion 63
 - 4.5 Direct Inwards System Access (DISA) Security..... 64
 - 4.6 Voice Mail Security 65
 - 4.7 Automated Attendant Security 65
 - 4.8 VoIP Security 66
 - 4.9 Logs..... 68
 - 4.10 The Most Important Tasks..... 69
 - 4.11 Advice for Simple Users 70
 - 4.12 On a Collaborative Project: PRETTY
(PRivatE Telephony SecuriTY) 71
 - 4.12.1 User and System Requirements 71
 - 4.12.2 Research and Development..... 72
 - 4.12.3 Implementation 72
 - 4.12.4 Dissemination of Results..... 72
 - 4.13 Conclusion..... 73
 - References..... 73

- 5 PBX Forensics** 75
 - 5.1 Introduction 75
 - 5.2 Crime and PBXs 75
 - 5.3 The Warning Signs 76
 - 5.4 The Hacker’s Modus Operandi 76
 - 5.5 The Evidence 79
 - 5.6 Fundamental Questions and Problems 80
 - 5.7 Forensic Procedures 81
 - 5.7.1 Introduction 81
 - 5.7.2 In General 82
 - 5.7.3 Training and Competence 83
 - 5.7.4 The Analysis Procedure Itself 83
 - 5.7.5 Data Preservation and Isolation from the Network 84
 - 5.7.6 Identification of the PBX 85
 - 5.7.7 Examining the Evidence 85
 - 5.7.8 Findings Report 86
 - 5.8 Logs 86
 - 5.8.1 In General 86
 - 5.8.2 Commands Log 86
 - 5.8.3 Authentication–Logon Log 88
 - 5.8.4 Alarms Log 89
 - 5.8.5 Calls Log 89
 - 5.9 Real-Time Data 91
 - 5.9.1 In General 91
 - 5.9.2 Equipment Connection 92
 - 5.9.3 Trunk Lines Data 92
 - 5.9.4 Signaling Data 93
 - 5.10 Extensions’ Data 93
 - 5.11 Evidence Stored Outside the PBX 98
 - 5.12 Conclusion 99
 - References 99
- 6 Conclusions** 101
- About the Author** 103