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. Morover, 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 synopsizes 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 Iosif I. Androulidakis, Ph.D., Ph.D.
October 2015

Contents