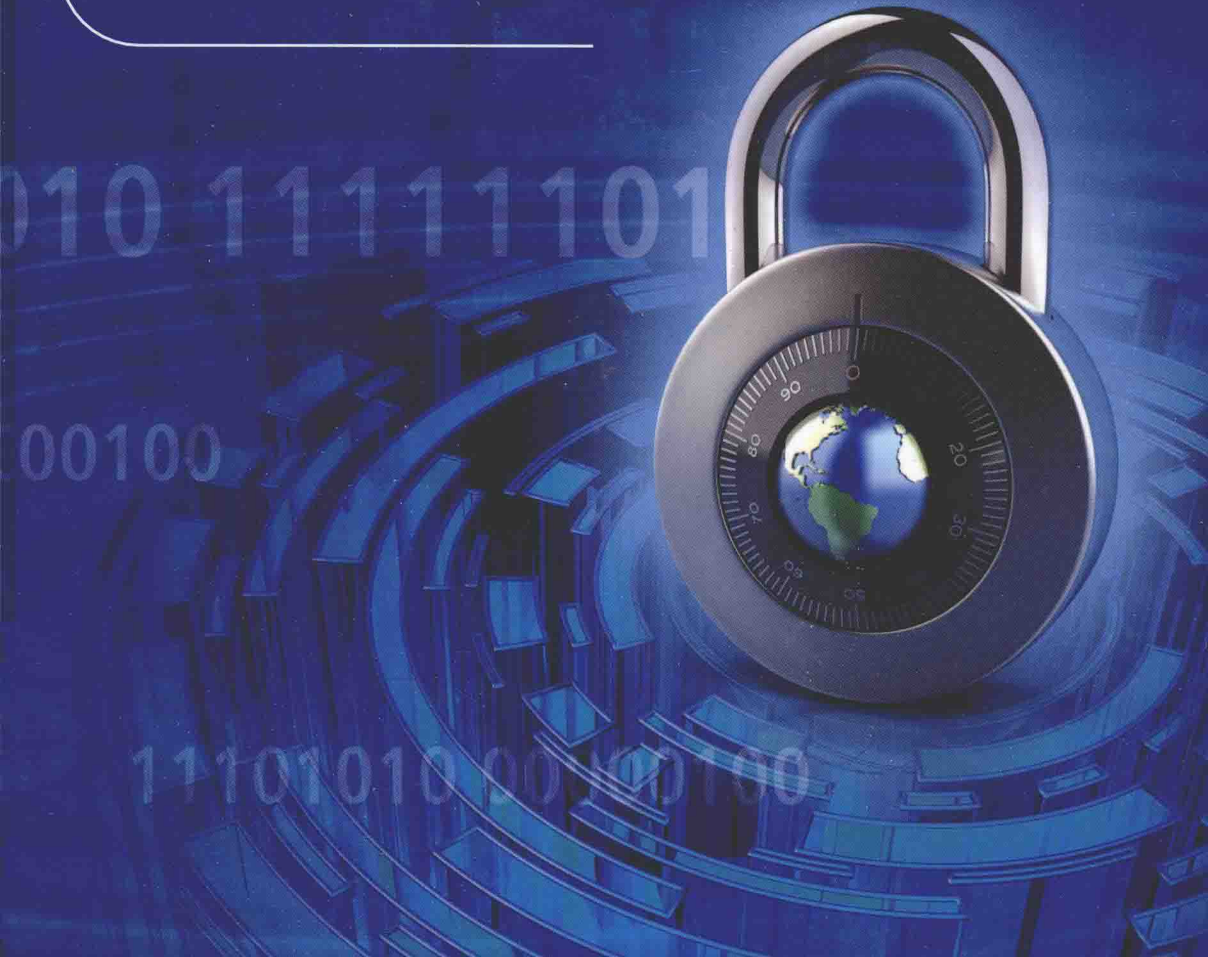
WILEY

Second Edition

LTE Security

Dan Forsberg | Günther Horn
Wolf-Dietrich Moeller | Valtteri Niemi



LTE SECURITY

Second Edition

Dan Forsberg
Poplatek Oy, Finland

Günther Horn
Nokia Siemens Networks, Germany

Wolf-Dietrich Moeller
Nokia Siemens Networks, Germany

Valtteri Niemi
University of Turku and Nokia Corporation, Finland

WILEY
A John Wiley & Sons, Ltd., Publication

This edition first published 2013

Registered office
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at www.wiley.com.

Library of Congress Cataloging-in-Publication Data

LTE security / Gunther Horn ... [et al.]. – 2nd ed.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-118-35558-9 (cloth)
1. Long-Term Evolution (Telecommunications) 2. Global system for mobile communications.
I. Horn, Gunther.
TK5103.48325.L74 2013
621.3845′6–dc23

2012025771

A catalogue record for this book is available from the British Library.

ISBN: 9781118355589

Set in 10/12pt Times by Laserwords Private Limited, Chennai, India
Printed and bound in Singapore by Markono Print Media Pte Ltd

LTE SECURITY

Preface

This is the second edition of the book *LTE Security* whose first edition appeared in the autumn of 2010.

Since 2010, LTE has established itself as the unrivalled mobile broadband technology of the fourth generation (4G), with significant commercial deployments around the world and a fast-growing market. The subject of this book is hence even more relevant than it was at the time of the first edition.

The basic specifications for LTE in general, and LTE security in particular, have proven remarkably stable since their first versions were published in 2008 as part of 3GPP Release 8. Nevertheless, as is quite common in the standardization process, a number of corrections to the LTE security specifications have been agreed since to fix shortcomings that had become apparent during the development and deployment processes.

More importantly, new features have been added to LTE to enhance support for new types of deployment scenarios and applications. From a security point of view, the most important of these additions are the support for relay nodes and for machine-type communications. We therefore devote two new chapters to them.

A number of other new features have been added to LTE security since 2010, one example being the addition of a third family of cryptographic algorithms for LTE. These new features have been added to the chapters that had existed already in the first edition of the book.

This book focuses on LTE security, but also gives a thorough introduction to its predecessors, GSM security and 3G security. The second edition updates the reader on recent developments in these areas. While things were quite calm on the 3G security front, confidence in the strength of some cryptographic algorithms used with GSM has been further eroded by live hacking demonstrations at a number of public events. These developments suggest that it is now time to take those stronger GSM algorithms into use that have already been standardized and are available in products.

Some of the topics mentioned in the last chapter of the first edition that provided an outlook have matured in the meantime and been included in the other chapters of the book. The outlook has been updated accordingly.

Summing up, this second edition includes the following updates with respect to the first edition:

- Two new chapters, on relay nodes and machine-type communications, have been added.

- All enhancements to LTE security specified for 3GPP Releases 10 and 11 have been included.
- All corrections to the specifications up to and including Release 11 and approved by 3GPP by June 2012 have been taken into account as far as they affect the text in the book.
- Major developments since 2010 affecting GSM security and 3G security are explained.
- The last chapter of the book providing an outlook to future developments has been updated.

Foreword to the First Edition

The early to mid-1980s saw the commercial opening across Europe of public-access mobile communications systems. These cellular systems all used analogue technology, but outside of the Nordic countries no attempt was made to standardize the systems – so the technology adopted differed from country to country. Unfortunately, one thing they did have in common was a total absence of adequate security features, which made them open to abuse by criminals, journalists and all manner of opportunists. Users' calls could be eavesdropped on the air using readily available and comparatively inexpensive interception devices, and there were celebrated cases of journalistic invasion of privacy. A well-known example was the 'squidgy' tapes, where mobile telephone calls between members of the British royal family were recorded. Mobile telephone operators and their customers became very concerned.

The operators also had another problem with serious financial consequences. When a mobile phone attempted to connect to a network, the only check made on authenticity was to see that the telephone number and the phone's identity correctly corresponded. These numbers could be intercepted on the air and programmed to new phones creating clones of the original. Clones were used by criminals to run up huge charges for calls which had nothing to do with the legitimate owner. Cloning became very widespread, with criminals placing their 'cloning' equipment in cars parked at airports to capture the numbers from business people announcing their arrival back home to their families. It represented a serious financial problem for operators who ended up covering the charges themselves. The problems caused by lack of security in European analogue systems were a significant factor in accelerating the creation and adoption of GSM.

GSM is a standard for digital mobile communications, designed originally for Europe but now adopted all over the world. Being an international standard it brings economy of scale and competition, and it enables users to roam across borders from one network to another. Being digital it brings transmission efficiency and flexibility, and enables the use of advanced cryptographic security. The security problems of the original analogue systems are addressed in GSM by encryption on the air interface of user traffic, in particular voice calls, and authentication by network operators of their customers on an individual basis whenever they attempt to connect to a network, irrespective of where that network may be. From both a technical and a regulatory perspective, the use of cryptography in GSM was groundbreaking. Initially manufacturers and operators feared it would add too much complexity to the system, and security agencies were concerned that it may be abused by criminals and terror organizations. The legitimate fears and concerns constrained what was possible, especially with the encryption algorithm, which was designed against a philosophy of 'minimum strength to provide adequate security'. Despite this, and the continuing efforts of organized hackers, eavesdropping on the air of GSM calls protected using the original cipher has still to be demonstrated in a real deployment, and with a stronger cipher already available in the wings, any future success will be largely pointless. This doesn't mean that GSM is free from security weaknesses – the ability to attack it using false base stations is very real.

GSM is the first in an evolving family of technologies for mobile communications. The second member of the family is 3G (or UMTS, as it is often referred to in Europe) and the third, and most recent, is LTE EPS to give it its proper title which is used throughout the main body of this book). With each technology evolution the security features have been enhanced to address learning from its predecessor, as well as to accommodate any changes in system architecture or services. The underlying GSM security architecture has proved to be extremely robust, and consequently has remained largely unchanged with the evolving technology family. It has also been adapted for use in other communications systems, including WLAN, IMS and HTTP. It is characterized by authentication data and encryption key generation being confined to a user's home network authentication centre and personal SIM, the two elements where all user-specific static security data is held. Only dynamic and user session-specific security data goes outside these domains.

3G sees the addition to the GSM security features of user authentication of the access network – to complement user authentication by the network, integrity protection of signalling and the prevention of authentication replay. Start and termination of ciphering are moved from the base station further into the network. Of course, the false base station attack is countered. A new suite of cryptographic algorithms based on algorithms open to public scrutiny and analysis is introduced, and changes of regulation governing the export of equipment with cryptographic functionality make their adoption easier for most parts of the world.

LTE heralds the first technology in the family that is entirely packet-switched – so voice security has to be addressed in an entirely different way from GSM and 3G. LTE is a much flatter architecture, with fewer network elements, and is entirely IP-based. Functionality, including security functionality, is migrated to the edge of the network, including encryption functionality which is moved to the edge of the radio network, having been moved from the base station to the radio network controller in the evolution from GSM to 3G. While maintaining compatibility with the security architecture developed for GSM and evolved for 3G, the security functionality has been significantly adapted, enhanced and extended to accommodate the changes that LTE represents, as well as security enhancements motivated by practical experience with 3G. Much of this plays back into 3G itself as new security challenges arise with the advent of femto cells – low-cost end nodes in exposed environments that are not necessarily under the control of the operator of the network to which they are attached.

The book takes the reader through the evolution of security across three generations of mobile, focussing with clarity and rigour on the security of LTE. It is co-authored by a team who continue to be at the heart of the working group in 3GPP responsible for defining the LTE security standards. Their knowledge, expertise and enthusiasm for the subject shine through.

Professor Michael Walker
Chairman of the ETSI Board

Acknowledgements

This book presents the results of research and specification work by many people over an extended period. Our thanks therefore go to all those who helped make Long Term Evolution (LTE) possible through their hard work. In particular, we thank the people working in 3GPP, the standardization body that publishes the LTE specifications, and, especially, the delegates to the 3GPP security working group, SA3, with whom we were working to produce the LTE security specifications over the past years.

We would also like to express our gratitude to our colleagues at Nokia and Nokia Siemens Networks for our longstanding fruitful collaboration. We are particularly indebted to N. Asokan, Wolfgang Bücker, Devaki Chandramouli, Jan-Erik Ekberg, Christian Günther, Silke Holtmanns, Jan Kåll, Raimund Kausl, Rainer Liebhart, Christian Markwart, Kaisa Nyberg, Martin Öttl, Jukka Ranta, Manfred Schäfer, Peter Schneider, Hanns-Jürgen Schwarzbauer, José Manuel Tapia Pérez, Janne Tervonen, Robert Zaus and Dajiang Zhang who helped us improve the book through their invaluable comments.

Finally, we would like to thank the editing team at Wiley whose great work turned our manuscript into a coherent book.

The authors welcome any comments or suggestions for improvements.

Copyright Acknowledgements

The authors would like to include additional thanks and full copyright acknowledgement as requested by the following copyright holders in this book.

Please see the individual figure and table captions and the footnotes to extracts from 3GPP specifications for copyright notices throughout the book.

Contents