国际信息工程先进技术译丛

WILEY

LTE网络安全技术

（原书第2版）

LTE Security (Second edition)

[芬] 丹·福斯伯格（Dan Forsberg）
[德] 冈瑟·霍恩（Günther Horn）
[德] 沃尔夫-迪特里希·穆勒（Wolf-Dietrich Moeller）
[芬] 瓦尔特利·尼米（Valtteri Niemi）
著

白文乐 王月海 刘红 译

机械工业出版社
CHINA MACHINE PRESS

国际信息工程先进技术译丛

LTE 网络安全技术
（原书第 2 版）

［芬］丹·福斯伯格（Dan Forsberg）
［德］冈瑟·霍恩（Günther Horn）
［德］沃尔夫－迪特里希·穆勒（Wolf－Dietrich Moeller）著
［芬］瓦尔特利·尼米（Valtteri Niemi）
白文乐　王月海　刘　红　译

机械工业出版社

本书重点讨论了LTE网络的安全问题，共分16章，每个章节知识点都很丰富，涵盖了蜂窝系统的背景知识、安全概念、GSM安全、3G安全、3G－WLAN互通、EPS安全架构、EPS的认证与密钥协商、信令和数据保护、LTE内的状态转换和移动性安全、EPS加密算法、家庭基站部署的安全性、中继节点安全及MTC（机器类型通信）的安全性问题。

本书的特点是关于工程技术理论与问题的讲解非常多，适合从事移动通信系统及网络安全技术研究的科研工作人员、企业研发人员及工程师阅读，也可作为通信工程与网络安全及相关专业的高年级本科生、研究生和教师的参考用书。

图书在版编目（CIP）数据

LTE网络安全技术：原书第2版/（芬）丹·福斯伯格（Dan Forsberg）等著；白文乐，王月海，刘红译. —北京：机械工业出版社，2019.12
（国际信息工程先进技术译丛）
书名原文：LTE Security（Second edition）
ISBN 978-7-111-64275-6

Ⅰ.①L… Ⅱ.①丹… ②白… ③王… ④刘… Ⅲ.①无线电通信－移动网－安全技术 Ⅳ.①TN929.5

中国版本图书馆CIP数据核字（2019）第268445号

机械工业出版社（北京市百万庄大街22号 邮政编码100037）
策划编辑：江婧婧 责任编辑：江婧婧 朱 林
责任校对：樊钟英 张 征 封面设计：马精明
责任印制：孙 炜
保定市中画美凯印刷有限公司印刷
2020年1月第1版第1次印刷
169mm×239mm·18.5印张·380千字
0 001—2 500册
标准书号：ISBN 978-7-111-64275-6
定价：99.00元

电话服务 网络服务
客服电话：010-88361066 机 工 官 网：www.cmpbook.com
010-88379833 机 工 官 博：weibo.com/cmp1952
010-68326294 金 书 网：www.golden-book.com
封底无防伪标均为盗版 机工教育服务网：www.cmpedu.com

本书特色

LTE预示着通信系统中新技术的来临，即其全部为分组域，所以其对语音安全的解决方式与GSM和3G系统完全不同。LTE具有更加扁平的架构，拥有更少的网络元素，且完全是基于IP的。其功能包括安全加密，都转移到了网络边缘，其中加密功能转移到了无线网络边缘，在GSM到3G的演进过程中均由基站转移到了无线网络控制器中。在保持与GSM、3G系统安全架构兼容的同时，LTE系统中采用了增强的安全功能来适应LTE所带来的改变以及3G系统应用时安全性能的改变。随着家庭基站的引入，这其中的许多改变应用到了3G系统本身，家庭基站是部署在外界的低功耗节点，不需要受到其连接的运营商的控制。

本书将带领读者领略移动通信系统演进过程中安全性能的变化，聚焦LTE安全的清晰与严谨性。

如果您有意写作图书、翻译图书或者有好的外版书推荐，请联系策划编辑江婧婧。
邮箱：jjjblue6268@sina.com
编辑QQ：372205490
电话：010-88379765

关于本书

自2010年以来，LTE凭借其全球范围内广泛的商业部署与业务量的快速增长，已经成为了第四代移动通信技术的主流标准。因此，与本书第1版相比，第2版中所讨论的问题也更为相关。

自2010年以来，许多新的特性已经加入到LTE安全中，一个例子是LTE增加了第三类加密算法。这些新特性已加入本书第1版已存在的章节中。

本书的重点在于LTE安全，但同时也全面介绍了其之前的系统，如GSM和3G。第2版中更新了在这些领域的最新发展。虽然3G安全领域的局面相当平静，但GSM中使用某些加密算法的可信度进一步受到一些公共事件的黑客的侵蚀。这些发展表明，现在是时候将那些更强大的GSM算法加以利用了，这些算法已标准化并可用于产品中。

第1版最后章节中的某些在当时较成熟的内容，如今包含在本书的其他章节中。于是相应章节也进行了更新。

总之，相对于第1版而言，第2版进行了如下更新：

- 增加了全新的两章内容，即中继节点安全与机器类型通信的安全性。
- 已包括为3GPP Release10和11指定的LTE安全性的所有增强。
- 2012年6月3GPP发布的Release11中的修正细则也增加进了本版中。
- 2010年后GSM与3G安全细则的主要发展历程也在本版中做了相应的解释说明。

译者序

网络已成为人们生活中不可或缺的重要元素，不仅人们的生活受到网络的影响而发生改变，其对各行业同样有着广泛的影响。移动网络为大众生活提供便利的同时，其安全隐患问题也随之暴露出来，网络安全已成为人们，乃至国家十分重视的问题。

相对2G、3G网络，LTE（Long Term Evolution，长期演进）呈现扁平化、全IP化两大网络架构的改变，以及高带宽、大数据量的特点，LTE网络将面临数据窃听、假冒欺骗、数据篡改等安全风险，不仅仅会影响到运营商的经济利益，更重要的是会危害到基础网络设施，甚至威胁用户的信息安全。为此华为公司与运营商一直在着力解决LTE网络安全问题，2015年国内首个LTE安全领域行业标准发布并实施，如何不断研究新技术来提供可靠安全的移动大数据网络已经成为一个热点问题，熟悉LTE网络安全架构及工作机理已成为移动网络安全技术工作者所必须掌握的一个技术条件。

本书从基本的网络结构、安全概念及加密概念开始，依次介绍了GSM安全、3G安全、3G－WLAN互通、EPS安全架构、EPS的认证与密钥协商、信令和数据保护、移动性安全、加密算法、互通安全、语音安全、家庭基站部署安全、节点安全等，内容非常全面，技术上以循序渐进的方式描述网络结构发展伴随着安全性能需求的变化而带来新概念、新机制的变化，但又不局限于枯燥的文字描述，而且使用条理清晰的结构图、流程图及表格引导读者理解和领悟LTE安全内涵，就像是在讲一部移动网络安全技术发展史。

对于初学者，本书是一本难得的入门教材，激发您学习移动网络安全基本知识的兴趣，为以后的深入开发奠定扎实的基础。对于网络安全方面的技术工作者，本书是一本深入掌握LTE网络工作安全、互通安全并排除安全故障的启发式指导书，它能够为他们提供技术腾飞的翅膀。相信任何有机会阅读本书的人都会从中受益，并由此跨上一个新的台阶。对于移动网络安全的探索和发现永无止境，面向网络安全的应用开发更是琳琅满目。我们希望通过本书这扇窗，能够引导您进入一个更美好、更安全的信息世界。本书同时也可以作为教材，供网络安全专业教师和学生使用。

本书出版得到北京市自然基金—海淀联合基金重点研究专题项目（L182039）、2019北京高校电子信息类专业群建设项目的资助，张键红教授对本书提出了宝贵的校对意见，在此，一并表示衷心的感谢。鉴于译者水平有限，书中难免存在错漏之处，还望读者谅解并不吝指正。如果读者有什么反馈意见，请发送到邮箱bwlsx1@163.com，我们将不胜感激。

译者

2019年11月于北京

原书第2版前言

这是《LTE网络安全技术》第2版，其第1版于2010年秋出版。

自2010年以来，LTE凭借其全球范围内广泛的商业部署与业务量的快速增长，已经成为了第四代移动通信技术的主流标准。因此，与第1版相比，第2版中所讨论的问题也更为相关。

总体来讲，LTE的规范，特别是LTE安全，在2008年3GPP Release8中首次发布后便基本没有进行过改动。然而，如在标准化过程中很常见的，对LTE安全规范的若干修正已经达成一致，以纠正正在开发和部署过程中出现的明显的缺点。

更重要的是，LTE中已经增加了新的特性来支持新的部署场景和应用。从安全的角度来讲，新的特性中最重要的便是增加了对中继节点和机器类型通信的支持。因此，本书中会增加新的章节来介绍它们。

自2010年以来，许多新的特性已经加入到LTE安全中，一个例子是LTE增加了第三类加密算法。这些新特性已加入本书第1版已存在的章节中。

本书的重点在于LTE安全，但同时也全面介绍了其之前的系统，如GSM和3G。第2版中更新了在这些领域的最新发展。虽然3G安全领域的局面相当平静，但GSM中使用某些加密算法的可信度进一步受到一些公共事件的黑客的侵蚀。

这些发展表明，现在是时候将那些更强大的GSM算法加以利用了，这些算法已标准化并可用于产品中。

第1版最后章节中的某些在当时较成熟的内容，如今包含在本书的其他章节中。于是相应章节也进行了更新。

总之，相对于第1版而言，第2版进行了如下更新：

- 增加了全新的两章内容，即中继节点安全与机器类型通信的安全性。
- 已包括为3GPP Release10和11指定的LTE安全性的所有增强。
- 2012年6月3GPP发布的Release11中的修正细则也增加进了本版中。
- 2010年后GSM与3G安全细则的主要发展历程也在本版中做了相应的解释说明。
- 本书的最后部分展望了未来的发展趋势。

原书第1版序

从20世纪80年代前期到中期拉开了移动通信系统在欧洲的商用序幕。这些蜂窝系统全部都使用模拟电子电路技术，北欧国家也没有将系统标准化，因此在不同国家采用的技术也不尽相同。不幸的是，这些通信系统全部都缺少足够的安全防范措施，这使得它们很容易被个别人滥用。用户的通话很容易遭到简易窃听装备的窃听，现实中有一些著名的新闻侵犯隐私权的案例。基于上述种种事件，移动运营商和用户十分关心通信安全。

运营商同时需要考虑可能造成重大经济损失的另一个问题。当手机想要连接到网络时，基站只会对其手机号与手机标识是否一致进行认证。这些号码很可能在通信过程中遭到拦截并被复制。罪犯用复制手机号的手机能够打大量电话，而这些电话与原合法手机用户一点关系也没有。手机号复制已经成为全球性的问题，罪犯在机场边放置复制设备来截获人们通话时的电话号码。这造成了严重的经济损失，因为最终都是运营商来弥补手机号码复制所造成的损失。在欧洲，模拟移动电话通信系统缺少安全机制的问题加速了GSM的研制与应用。

GSM是数字移动通信标准，以前在欧洲设计，之后应用到全球。其作为国际标准带来了巨大的经济效益与竞争，它使得用户能够在不同国家网络之间漫游通信。GSM作为数字通信系统带来了通信的高效性与灵活性，其中也应用了高级加密算法。之前在模拟通信系统中存在的安全问题在GSM中通过空中接口中的用户流量加密算法得到了很好的解决，尤其是语音通话，而且无论用户连接到何地网络，当地网络都能基于用户基本信息认证用户。从技术和管理角度来看，GSM中应用的加密算法是革命性的。起初，制造商与运营商都担心这会增加系统的复杂性，而安全机构却担心加密算法会被罪犯和恐怖组织滥用。这种忧虑是情有可原的，尤其是对加密算法的担心，因为其在设计之初就违背了“最低限度提供足够安全”的原则。尽管如此，在有组织的黑客的不断“努力”下，使用原始密码保护的GSM电话的安全性需要在实际应用中加以证明，而且随着更强大的密码的使用，黑客们任何未来可能的成功都将毫无意义。但这并不意味着GSM无懈可击——通过使用伪基站攻击它仍是可行的。

GSM是演进移动通信系统家族中的第一代系统。其第二代成员便是3G（或UMTS），第三代成员便是LTE EPS。随着科技的进步，安全机制也随之更新来解决之前系统所存在的问题，同时逐渐适应系统架构或服务的改变。GSM安全架构具有很强的鲁棒性，大部分架构在演进技术家族中保持不变。GSM安全架构也应用于其他通信系统中，包括WLAN、IMS和HTTP，其特点是认证数据和加密密钥生成仅限于用户归属认证中心和SIM卡，所有用户特定的静态安全数据保存在这两

个元素中。只有动态和用户会话安全数据在这些域外。

3G 系统增加了接入网的用户认证——以完成网络端用户认证、通信完整性保护和防止认证重播。加解密的起始和终止从基站端移向了网络端。当然，这抑制了伪基站攻击。基于公共监督和分析的加密算法引入到了 3G 系统中，政府对于具有加密功能设备监管制度的改变，使得它们能够在全世界大多数国家被使用。

LTE 预示着通信系统中新技术的来临，即其全部为分组域，所以其对语音安全的解决方式与 GSM 和 3G 系统完全不同。LTE 具有更加扁平的架构，拥有更少的网络元素，且完全是基于 IP 的。其功能，包括安全加密，都转移到了网络边缘，其中加密功能转移到了无线网络边缘，在 GSM 到 3G 的演进过程中均由基站转移到了无线网络控制器中。在保持与 GSM、3G 系统安全架构兼容的同时，LTE 系统中采用了增强的安全功能来适应 LTE 所带来的改变以及 3G 系统应用时安全性能的改变。随着家庭基站的引入，这其中的许多改变应用到了 3G 系统本身，家庭基站是部署在外界的低功耗节点，不需要受到其连接的运营商的控制。

本书将带领读者领略移动通信系统演进过程中安全性能的变化，聚焦 LTE 安全的清晰与严谨性。本书由在 3GPP 中负责定义 LTE 安全标准的工作组共同编写。他们的学识、专业知识和对工作的热情深深地影响着我。

麦克·沃克教授
ETSI 协会主席

致　谢

本书介绍了许多人在很长一段时间内的研究和规范工作的成果。我们感谢那些通过辛勤工作使得 LTE 成为现实的人们。特别地，我们感谢 3GPP 的工作人员，发布 LTE 规范的标准化组织，特别是 3GPP 安全工作组 SA3 的代表们，在过去的几年中，我们与他们一起完成了 LTE 安全规范的制定。

我们同时要感谢在 Nokia 和 Nokia Siemens 网络工作的同事们，在过去几年中，我们与他们一起努力制定了 LTE 安全规范。我们要特别感谢 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 和 Dajiang Zhang，他们在本书的创作中提供了大量宝贵意见。

最后，我们要感谢 Wiley 公司的编辑团队，他们的努力使得本书成为了现实。

本书作者欢迎大家的批评指正。

版权致谢

作者考虑到本书中包括以下版权持有人的要求，并给予额外的感谢和充分的版权确认。

- ©2009，3GPP™。TS 和 TR 为 ARIB、ATIS CCSA、ETSI、TTA 和 TTC 联合拥有的版权。它们受到进一步修改，因此这里仅供参考，严禁进一步使用。
- ©2010，3GPP™。TS 和 TR 为 ARIB、ATIS CCSA、ETSI、TTA 和 TTC 联合拥有的版权。它们受到进一步修改，因此这里仅供参考，严禁进一步使用。
- ©2010，Nokia 公司。允许在图 2.1、图 3.1、图 3.2、图 3.3、图 6.1、图 6.2、图 6.3、图 7.1 和图 14.1 中使用 Nokia 公司的 UE 图标。
- ©2011，欧洲电信标准协会。进一步使用、更改、抄袭或分发是被严令禁止的。ETSI 标准可从 http：//pda. etsi. org/pda/ 中获得。
- ©2012，3GPP™。TS 和 TR 为 ARIB、ATIS CCSA、ETSI、TTA 和 TTC 联合拥有的版权。它们受到进一步修改，因此这里仅供参考，严禁进一步使用。
- ©2012，GSM 协会GSM™及其证书。保留所有版权。

在本书中，请看从 3GPP 规范中提取的单个图和表格的标题和脚注来获得版权声明。

目　录