



LTE 规模部署中潜在的网络安全风险分析

刘国荣, 刘东鑫, 沈 军, 金华敏

(中国电信股份有限公司广州研究院 广州 510630)

摘 要:近年来,LTE 成为全球通信行业的发展热点。针对 LTE/SAE 的安全特性,对 LTE 规模部署过程中面临的如控制平面拥塞、异常流量攻击、网络融合等各层面的安全风险进行深入分析,并提出相应的安全防护建议。这些安全防护建议包括安全域划分、信令保护、异常流量防护等措施,以期对我国 LTE 规模部署的安全保障提供必要的参考。

关键词: LTE;网络安全;安全管理;信令管理

doi: 10.11959/j.issn.1000-0801.2015269

Analysis on Potential Network Security Risk of LTE Scalable Deployment

Liu Guorong, Liu Dongxin, Shen Jun, Jin Huamin

(Guangzhou Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China)

Abstract: In recent years, the deployment of LTE network has become a hot spot. Based on the introduction of the security design of LTE/SAE, a deep analysis of security risk was made including control plane's congestion, abnormal traffic attack, network convergence which might be brought during the LTE deployment. After that, some solutions were proposed like division of security domain, signaling protection and abnormal traffic protection to provide a security reference for the LTE deployment in China.

Key words: LTE, network security, security management, signaling management

1 LTE/SAE 安全概述

随着移动网络 IP 化、终端智能化及业务开放化、多样化趋势的发展,移动通信网络面临的安全威胁日益严峻,这些威胁包括对无线链路、服务网络和对移动终端的威胁。攻击者可以利用网络协议和系统的弱点,非授权访问和处理敏感数据,或干扰、滥用网络服务,对用户和网络资

源造成损失。

针对 LTE/SAE 网络的主要安全威胁,3GPP 在标准设计之初即制定了基础的安全防护机制,并针对 2G/3G 网络安全的不足,重点对用户身份合法性验证、空口数据加密及完整性保护以及核心网安全保护等方面进行了改进,提升了系统安全性。

LTE/SAE 标准采用了双向认证机制,网络 and 用户分别验

收稿日期:2015-06-16;修回日期:2015-10-10

基金项目:国家高技术研究发展计划(“863”计划)基金资助项目(No.2015AA017205)

Foundation Item: The National High Technology Research and Development Program of China (863 Program) (No. 2015AA017205)

论文引用格式:刘国荣,刘东鑫,沈军等. LTE 规模部署中潜在的网络安全风险分析. 电信科学, 2015269

Liu G R, Liu D X, Shen J, *et al.* Analysis on potential network security risk of LTE scalable deployment. Telecommunications Science, 2015269

证对方的合法性,既可防止非法用户接入网络,又能有效防范假冒网络对用户的威胁。同时,用户标识、密钥等关键信息存储在移动终端独立的安全智能卡中,加解密运算在卡内完成,并采用临时标识等措施对用户标识进行保密处理。

在数据加密和完整性保护方面,网络和终端根据双方加密能力和算法优先级等配置协商产生出加密和完整性保护算法等安全参数,对空中传输信息进行机密性和完整性保护,避免网络控制指令、用户数据被窃听和篡改,同时,采用分层密钥管理体系,移动终端和不同网络实体间推演出多层密钥,实现各网络实体与移动终端通信安全的隔离,进一步提升整个系统的安全性。

在安全算法方面,国际标准化组织 3GPP 采纳了 3 种加密和完整性保护算法作为 LTE 的国际标准:ZUC (中国标准)、SNOW 3G (欧洲标准)和 AES (美国标准)。其中,ZUC 作为我国具有自主知识产权的标准,同时适用于 LTE FDD 和 TD-LTE。

LTE 核心网是全 IP 化的网络,可采用成熟的网络安全机制实施安全防护:如将网络划分为不同的安全域,采用访问控制、网络隔离等技术对不同安全域实施隔离;采用 IPSec 结合双向认证技术,对不同安全域传输的信息提供数据来源认证、机密性和完整性保护;采用容灾备份、负荷均衡和过载控制等机制提升网络的处理能力和可靠性。

2 LTE/SAE 规模部署安全风险

与 2G/3G 网络相比,LTE 安全机制得到了提升,但因其全 IP 化、扁平化的网络结构、控制与承载分离特性以及带宽的提升为新的攻击形式提供了可能,而业务形式的丰富化,特别是语音、实时视频等业务对 QoS (quality of service,服务质量)要求的提升,对网络可靠性、安全性也提出了更高要求。

LTE 规模部署带来安全形势的变化,主要体现在以下方面。

(1)随着业务的迅猛增长,扁平化的网络结构和集中控制方式给信令管理带来很大的挑战,可能产生控制平面拥塞和信令风暴的问题。

在 3G 时代,移动数据业务的快速增长,特别是即时通信等小流量、永远在线应用的广泛使用,使网络信令迅速增长,而智能终端为省电快速休眠的机制,会带来频繁的信令连接重建,给移动网络的信令带来了很大的负荷,曾引发严重的信令风暴问题。

LTE 的规模部署将促使移动数据业务进一步快速增长,信令连接频繁重建的现象不仅继续存在,还可能由于业务的增长、业务模式的变化以及网络架构和信令承载方式的变化而对信令管理带来更大的挑战。

LTE 采用更可靠的承载方式来提升信令可靠性,但也增加了网络负荷,如用于认证、计费、策略管理的 Diameter 信令,采用 TCP/SCTP 承载,需要更多网络交互,以确保可靠传输。同时,LTE 引入了策略管理、在线计费等新的业务模式,导致网络信令量急剧增长。据 Oracle 2014 年发布的 LTE Diameter 信令指数白皮书预测^[1],2013-2018 年,全球 LTE Diameter 信令将以 78% 的年复合平均增长率快速增长。

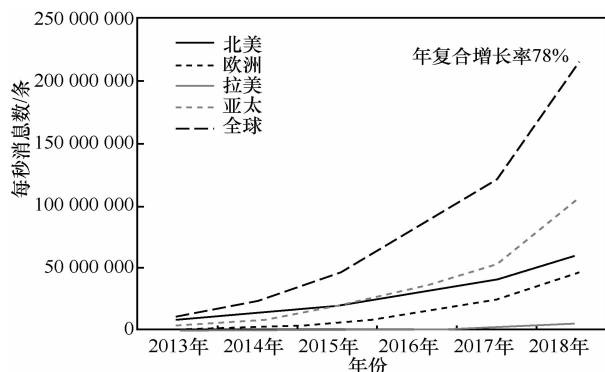


图 1 LTE Diameter 信令增长预测

由于业务增长、业务模式及承载方式的变化,LTE 的信令负荷将是传统语音的数十倍。另一方面,LTE 承载的语音和视频具有很高的 QoS 要求,对 Diameter 信令提出了更严格的要求,需要一个强有力的架构以配合信令和数据流量的激增。

LTE/SAE 扁平化和全 IP 架构的网络设计减少了网络层级,导致 LTE 宏基站和微基站直连到 EPC 时,都会连接到同一个专用的控制面单元 MME,用户通信活动频繁的情况下,单个 MME 所承载的持续性的信令量将保持在很高的负荷,无疑造成了 EPC 承载压力,可能引发控制平面拥塞和信令风暴的问题。同时,其控制与承载分离的架构,使攻击者可能实施针对性的信令攻击,如 attach flood、paging flood、SIP flood 等,不仅加大了检测难度,也增加了信令面故障、威胁网络稳定运行的风险。全 IP 化的网络使移动终端可能成为攻击目标,特别是针对相同网段移动终端的扫描,可能引发局部范围内大量终端同时唤醒,产生信令面的拒绝服务攻击。同一网段终端间通信流量通常不需跨核心网络,可能处于网络攻击检测系统的盲区,给防护带来困难。

(2)家庭基站/小基站的大量部署给核心网络引入新的安全风险,可能成为网络的薄弱点。



LTE 高频段组网空间传播损耗和穿透损耗相比 CDMA 来说会更大,室内深度覆盖成为 LTE 网络部署的重点和难点,特别是建筑密集或人员密集城区宏基站覆盖阴影区域,如家庭、中小企业、宾馆酒店、地下车库、地下商场等。体积小、成本低、接入灵活的 femto 小区、pico 小区等小基站的大量部署,可成为 LTE 室内覆盖的有益补充。

但另一方面,家庭基站/小基站的引入也带来新的安全风险。小基站通过 DSL、LAN、FTTH 等不可信的链路经开放的 IP 网络连接到运营商核心网,核心网络与不可信网络的连接,大大提高了其安全风险。同时,数据在不可信 IP 网络的回传,也增加了数据泄露的风险。根据 LTE 安全机制,为保护用户数据接入安全而提供的加密传输终结于 eNode B, eNode B 与核心网络之间如果不采取额外安全保护措施,数据将以明文回传,因此,不安全的回传网络上的用户数据极易被监听,导致敏感信息的泄露。

小基站的部署位置也使运营商难以保证其物理安全。由于小基站一般分布在公共区域或家庭环境中,特别是机场、酒店、购物中心等公共场所,这些场所的人员构成复杂,更易受到攻击,甚至面临小基站被攻击者控制的风险。一旦攻击者控制了小基站,受控小基站可能被用作无线网络的嗅探器,对驻留在其上的终端执行窃听、假冒等各种攻击,甚至可被用于对运营商核心网络进行攻击,如 DoS (denial of service, 拒绝服务) 攻击等。

(3) 智能终端的普及和移动带宽的不断提升,使智能终端发起攻击的条件进一步成熟,移动僵尸网络和 DDos (distributed denial of service, 分布式拒绝服务) 攻击的威胁将逐步显现。

移动智能终端超越台式 PC 成为第一大互联网访问终端,标志着移动互联网时代的到来,而随着 LTE 网络的规模部署和快速普及、移动带宽的不断提升,移动智能终端的带宽瓶颈不断被突破。Ericsson 移动报告显示^[2],未来几年内,移动手机产生的流量将数倍于移动 PC、平板电脑等终端,成为移动互联网最主要的终端,如图 2 所示。从攻击者的角度看,这些变化使得利用移动智能终端发起各种网络攻击的条件进一步成熟,特别是移动智能终端天然的实时在线性,使得控制智能终端发起 DDos 攻击更加容易、效果也更加明显。

近年,可在移动智能终端发起 DDos 攻击的工具已经出现,甚至可在 Android 官方应用市场 Google Play 下载,典型的如可发起 HTTP post flood 攻击的 AnDOSid、由经典的 PC 端 DDos 攻击工具改写而来 Android 版 LOIC,这类工具在多起实际的 DDos 攻击事件中被检测到单独或与其他攻击工具混合使用,随着移动带宽的不断提升,这类攻击将会不断增加。

通过移动恶意软件的传播创建移动僵尸网络,并通过控制僵尸网络发起 DDos 攻击的现象也已经出现,如用于银行账户攻击的 ZitMo 和用于发送垃圾短信和 DDos 攻击的 Android.DDoS.1.origin。虽然从目前来看,通过复杂的网络互联、接受来自 C&C 的网络命令发起网络攻击的僵尸网络型病毒还在少数,但未来,移动僵尸网络将成为僵尸网络新的发展方向^[3]。

(4) LTE 与 2G/3G/Wi-Fi 等网络的融合,增加了网络攻击的入口和风险,也给用户管理带来挑战。

LTE 发展是渐进式的,与 2G、3G、Wi-Fi 以及 IMS 网络将会长期共存,安全等级不同的网络的混合组网,对兼容性和用户体验的兼顾,增加了攻击入口和安全风险,同时,也给用户管理带来了一定的挑战。

混合组网中不同网络的安全策略、安全防护等级可能并不一致,安全性差的网络不仅自身安全存在问题,而且会影响在它覆盖区域内的其他网络 and 用户。攻击者可通过强制切换,将移动终端引入不同网络实施攻击,如已经完全控制某个系统的攻击者可通过加大基站发射功率,引导其他系统的终端到自己控制的网络,然后通过这个被攻破的系统实施窃听、假冒、篡改等各种攻击;或者生成 RRC 信令,向受控系统的终端发起重配置过程,将移动终端引入选定的小区或网络,大量终端强制切换可导致对目标小区或网络的 DoS 攻击。

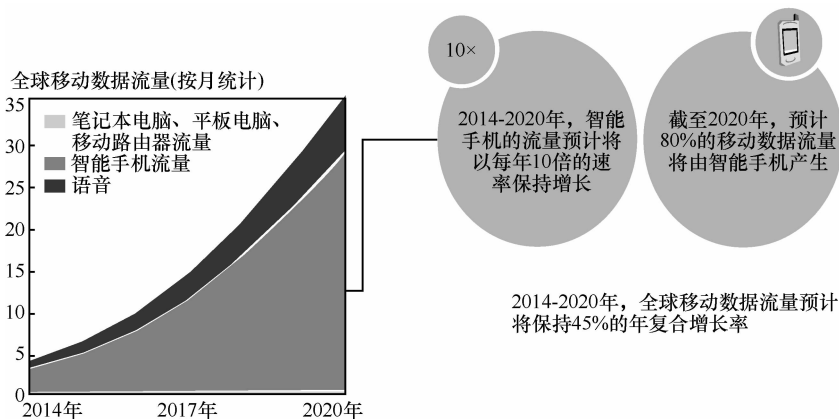


图2 智能手机的流量将成为移动互联网主要数据流量

在用户管理方面,为了实现业务的统一管理,各移动网络将采用同一个号码,用户数据将会分散在不同的网元设备中,这存在以下问题。

- 开户流程复杂。同一个用户的数据将分布在多个网元中,数据本身存在冗余存储,且业务开通管理流程复杂,对同一用户的业务开通要在多点进行,操作流程非常复杂、低效,且难以保证数据的一致性。
- 鉴权重同步问题。同一个用户的鉴权数据将分布在多个网元中,在不同网络间切换时,可能导致鉴权失败,增加终端不能正常服务的风险。

(5) LTE 多元化的业务和应用、海量信息的传输、处理,使攻击更具隐蔽性,大大增加了各类攻击、恶意程序和不良信息监控和防护的难度。

随着移动互联网的快速发展和智能终端的日益普及,互联网上原有的恶意程序传播、远程控制、网络攻击等传统安全威胁向移动互联网快速蔓延。同时,由于移动互联网终端和业务与用户利益密切相关,恶意吸费、信息窃取、诱骗欺诈等恶意的影响和危害更加突出。根据 CNCERT 公布数据统计^[4],2014 年,捕获移动互联网恶意程序样本达 95.1 万个,分别是 2013 年、2012 年、2011 年的 1.35 倍、5.84 倍和 152.19 倍,受感染用户数量达 2 292 万户,较 2013 年的 609 万户用户增长了 3.76 倍,恶意程序继续呈现爆发式增长态势。2005-2014 年移动互联网恶意程序走势如图 3 所示。

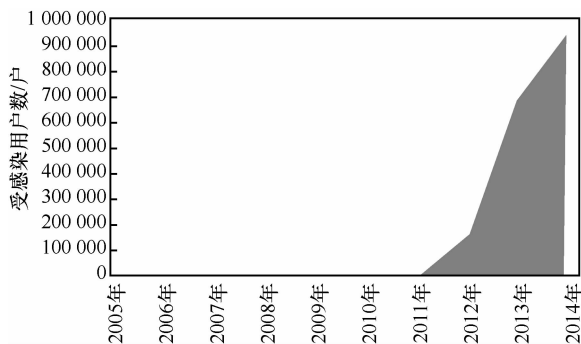


图 3 移动互联网恶意程序走势

随着网上支付类业务的发展、二维码等便捷传播途径的引入,恶意软件呈现强烈的趋利性,手机安全将面临更多的威胁。在信息传播方面,移动互联网已成为一个面向公众的发表、阅读、交互的信息平台,但欺诈、谣言、反动、色情等非法信息也利用移动互联网的便利进行传播。移动互联网的安全问题已经威胁到基础通信网络安全、侵害用

户利益,引起监管部门的高度重视,尤其是恶意程序、不良信息传播,已通过立法、建立监测处置制度和专项行动等机制,加大了治理的力度。

随着 LTE 的规模部署和网络带宽的提升,网络应用将进一步丰富,越来越多的智能终端业务通过各种渠道传播富媒体,网络流量将大幅提升,据 Ericsson 最新发布的移动报告预测,2014-2020 年全球移动数据流量将以每年 45% 的年平均复合增长率快速增长,2020 年流量将达到 2014 年的 10 倍,亚太地区的增长更高达 11 倍。在海量信息中对恶意程序、不良信息的识别发现、监测过滤等,将给管控能力带来严峻挑战。同时,移动互联网业务应用繁多、非标准化协议等问题,使攻击行为更容易隐藏在数量众多的用户请求中,难以被及时发现,这对攻击行为的识别和防治提出了挑战。

(6) LTE 开放化的趋势以及与云计算、物联网等新型应用的广泛结合,将引入更多未知的安全风险。

当前网络正走向 IP 化、融合化、开放化,云计算、物联网等各类新网络和新技术的不断创新给移动互联网带来了新的机遇与挑战。

移动互联网随时随地接入的特性,契合物联网任何时间、任何地点、任何物体互联的要求,成为物联网接入和传输最主要的载体。物联网传感节点数量庞大,在节点密集部署区域,频繁的连接、海量数据的传输可能导致网络拥塞,对网络产生拒绝服务攻击。传感节点由于部署位置和处理能力的限制,是安全性薄弱的环节,节点受控对网络安全将带来更大的挑战。

业务服务逐渐向云计算平台的演进,给网络发展带来了机遇,但云计算强大的计算能力同样吸引了黑客关注,攻击者可以利用云计算能力实施 DDoS 等攻击,甚至将攻击作为一种云服务,降低攻击门槛,给网络安全带来巨大的挑战。

移动互联网时代,运营商的业务平台正在向开放合作、融合创新转变。应用平台开放可能影响到基础网络、基础通信业务的安全稳定运行,影响用户和企业的信息安全和经济利益。与传统手机应用的安全风险相比,开放平台的安全威胁危害程度更深、影响范围更大、查找源头更难。

3 LTE/SAE 规模部署安全防护建议

我国三大运营商均已全面开展 LTE 商用服务,随着其建设规模和服务范围的扩展,LTE 安全防护系统的建设和防护策略的部署至关重要。建议重点从以下几个方面加强



安全防护。

(1)采用安全域划分、边界防护和流量隔离等措施实现不同类系统之间的隔离,控制安全风险的影响范围。

根据网元的功能、安全需求和安全防护等级划分不同的安全域,并在网络边界实施网络隔离和访问控制策略,针对不同安全域实施安全防护策略,如将 LTE/SAE 网络划分为无线接入域、RAN 传输网络域、EPC 核心域、业务网络域和维护域;实施管理面/用户面/控制面隔离,将信令流、OM 数据流和用户面数据流配置到不同 VLAN 中,从而隔离不同平面数据流之间的相互影响;部署安全网关对核心网 EPC 边界进行保护,包括在 eNode B 基站和 EPC 网络之间、EPC 网络与互联网间部署安全网关,开启攻击防范功能,保护 EPC 网络免受外部攻击;对 eNode B 基站实施双向认证,eNode B 基站和安全网关建立 IPSec 隧道,基站的 S1/X2 报文进行加密传输。

(2)构建顽健的信令网络,提升信令网络和控制平面的可靠性和处理能力;优化和完善信令处理流程,减少信令开销、提升用户体验。

从信令网络建设与信令优化两个方面入手,应对信令激增的压力。在信令网络能力建设方面,重点针对 Diameter 信令网、MME pool 的统一规划和建设,提升信令网络和控制平面的可靠性和处理能力。LTE 网络中大量网元之间使用 Diameter 信令互通,DRA 成为构建 LTE 信令网络的关键网元,建议根据漫游业务流量,在全国、大区域或省统一规划建设 DRA,并采用负荷分担、多重路由备份以及拥塞和过负荷处理等机制,充分保障信令网络的高可靠性和高可用性。MME 作为控制平面的核心设备,建议采用 pool 方式组网,pool 内 eNode B 与 MME 实现全互联,达到负载均衡和灾备的目的,并降低局间切换信令。

同时,网络设备应考虑避免不必要的信令交互发生,结合业务特点和用户行为,优化和完善信令处理流程,使网络对业务的处理达到最优;在网络拥塞时,确保高价值业务得到优先处理。如针对寻呼和跟踪区域管理,可采取动态 TA 管理,结合网络状况、用户等级等提供灵活的寻呼策略,在终端用户的寻呼体验和网络资源的消耗上取得平衡,防止寻呼和位置更新产生的信令风暴。

(3)基于 DPI 实施精细化的网络负荷动态管控和 DDoS 流量防护,在保障网络稳定和安全的的基础上,提升用户体验。

建议全网部署网络流量分析系统,在实现精细化的流

量识别的基础上,实施网络负荷的动态管控和攻击识别,及时发现并平抑因网络故障或攻击突发的网络流量异常,保障网络的稳定性和安全性。

针对流量异常对网络可靠性的威胁,可通过实施网络流量动态管控进行防范。基于 DPI 建立用户行为、应用消耗、网络资源间的关系,通过对网络应用的监控和分析,为关键业务与关键用户制定动态的网络带宽控制管理策略,并将策略管控系统与网络状态联动,根据网络拥塞状况、客户等级、业务 QoS 要求等动态调控策略,并利用流量缓存、流量负载均衡等技术来进一步优化网络带宽资源的消耗,实现基于实时网络负荷动态调控的管控策略,达到自动“削峰填谷”的目的,防止系统过载造成的网络不稳定。

针对流量及资源耗尽型攻击,建议基于 DDoS 攻击防御平台和 DPI 系统,采用 NetFlow+DPI 技术实现移动互联网攻击流量监测,并与 PCRF、HSS 联动实施控制,即基于 NetFlow 技术,通过异常流量监控分析系统,实现对 EPC 核心网及承载网络的异常流量实时监控和分析,同时,通过 DPI 与 PCRF、HSS 联动控制,应对智能终端发起的 Syn 扫描等异常流量攻击。

(4)构建移动互联网统一安全管理平台,实现移动互联网安全事件和安全策略统一管理;循序渐进实施不同网络用户数据融合和统一鉴权。

建议在互联网 SOC 平台基础上,构建面向移动互联网的统一安全管理平台,对移动互联网承载网的 CE、防火墙、MME、SAE-GW(SGW)、PDN-GW(PGW)、3G 网络的 PDSN/HSGW 等设备以及异常流量监控系统、DPI 系统进行集中管理,实现对移动互联网异常流量、安全事件集中收集、监控、分析以及安全策略的统一管理。

在用户数据管理方面,分阶段实施用户数据的融合和鉴权统一,如逐步实现用户数据的统一存储和管理,将用户数据存储和业务处理逻辑分离。后端用户数据库通过统一、可扩展的数据模型,提供基于用户各种数据的存储和访问,而前端负责处理来自核心网络的信令逻辑、业务请求等;在此基础上,实现鉴权入口的统一管理和分发,在用户数据集中管理的基础上,由统一的鉴权中心实现认证请求的分发,鉴权功能仍由原相关网元负责;最后,逐步实现鉴权的统一,由统一鉴权中心集成各网络鉴权网元功能,实现用户管理的简化及鉴权流程优化。

(5)研发并应用基于大数据的安全防护等新技术,采用群组认证、接入控制等机制,应对海量数据、海量节点增

长带来的挑战。

针对 LTE 规模部署以及云计算、物联网等应用带来的海量数据的挑战,需要运用大数据等新技术提升安全防护系统的处理能力。如不良信息的检测,可运用 Hadoop 技术,通过并行处理提升系统处理性能;移动互联网恶意程序样本检测,可采用基于云计算的动态沙箱技术,提升检测性能和效果;移动互联网异常流量攻击溯源及攻击路径重演,可在全网流量采集的基础上,采用云计算并行处理技术进行深入关联分析、网络拓扑分析,解决攻击源难以快速准确追溯的难题。

针对 M2M 等物联网海量节点的接入,在节点密集区域,可采用群组认证技术减少频繁连接所引发的认证信令的剧增,降低对控制平面的冲击^[5];或者采用策略认证实施流量自适应的接入控制,在节点身份验证之外,根据其业务属性、业务状态、网络状况等条件对节点接入进行控制,在确保网络稳定的基础上,提升高等级业务和用户的服务质量。

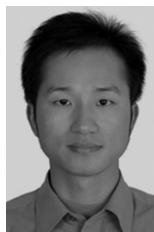
4 结束语

自 2013 年以来,我国的 LTE 发展就进入了快车道,在未来几年内仍将保持迅猛的发展势头。从标准的安全设计来看,相较于 2G/3G 通信标准,3GPP 对 LTE/SAE 网络的安全设计做了较大改进。但是,LTE 的全 IP 化及扁平化的网络结构、控制与承载分离特性和业务形式的丰富化等特性带来一系列的安全风险,给其规模部署带来不可忽视的挑战,同时,LTE 网络以及与云计算、物联网等新型应用的广泛结合,将引入更多未知的安全风险。本文针对 LTE 规模部署中潜在的网络安全风险进行了深入分析,并提出了相应的安全防护建议,以期对我国 LTE 规模部署的安全保障提供必要的参考。

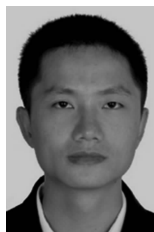
参考文献

- 1 Oracle. LTE Diameter Signaling Index, 3rd Edition. <http://www.oracle.com/us/industries/communications/lte-diameter-signaling-3rd-wp-2331962.pdf>, 2014
- 2 Ericsson Mobility Report. <http://www.ericsson.com/res/docs/2015/ericsson-mobility-report-june-2015.pdf>, 2015
- 3 华为技术有限公司.2013 僵尸网络与 DDoS 攻击专题报告. http://enterprise.huawei.com/topic/AntiDDoS_2013/index.html, 2013
- 4 CNCERT. 2014 年我国互联网网络安全态势报告, 2015
CNCERT. 2014 China's Internet Network Security Situation Report, 2015
- 5 荣星, 江荣, 田立业. 一种适用于物联网的群组接入认证协议. 计算机工程, 2015, 41(3):15~20
Rong X, Jiang R, Tian L Y. A group access authentication protocol for things of internet. Computer Engineering, 2015, 41(3): 15~20

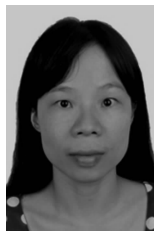
[作者简介]



刘国荣,男,中国电信股份有限公司广州研究院高级工程师,主要研究方向为移动互联网安全、云计算安全。



刘东鑫,男,中国电信股份有限公司广州研究院研究员,主要研究方向为网络与信息安全、大数据安全。



沈军,女,中国电信股份有限公司广州研究院高级工程师,主要研究方向为云计算大数据安全及移动互联网安全。



金华敏,男,中国电信股份有限公司广州研究院云计算研究所副所长,主要研究方向为 IP 网络安全及云计算。