

5G 网络安全研究报告

360 集团

2019 年 3 月 25 日

目 录

一、5G 网络安全特性.....	3
(一) 增强了对用户唯一标志符的隐私保护.....	3
(二) 增强了归属地网络控制力降低了漫游区欺骗风险.....	3
(三) 按需提供数据加密增加了用户面数据完整性保护.....	3
(四) 增强了运营商之间连接的安全性.....	3
(五) 通过选择性拒绝终端接入加强了防物联网 DDoS 攻击的能力.....	4
(六) 冗余传输安全方案兼顾了低时延业务的可靠性和安全性.....	4
二、5G 网络安全挑战.....	4
(一) 短时期内 5G 可能沿用 4G 核心网，5G 的安全特性仍停留在纸面上.....	4
(二) 低时延业务扩大了攻击面.....	5
(三) 大连接业务使 5G 成为黑客攻击的高价值目标.....	5
(四) 网络切片技术使得网络边界模糊.....	5
(五) 伪基站问题仍然存在.....	5
(六) 对用户位置隐私的保护提出更高要求.....	6
三、小结.....	6
附件：关于 360 移动通信安全研究团队.....	8
(一) 研究类工作.....	8
(二) 标准化工作.....	9
(三) 技术攻关工作.....	9

摘要：5G（第五代移动通信技术）时代，移动通信不仅为全世界数十亿人提供高速连接，构建新的互联网形态，更将成为万物互联的新型关键基础设施。工业互联网、车联网、智能电网、智慧城市、军事自组织网络等都将构架在 5G 网络上。5G 安全得到世界各国的高度重视。本报告结合 360 在 5G 网络安全方面的研究，对当前已有的 5G 网络安全研究成果和 3GPP 相关标准进行了梳理。

整体来看，5G 通过增加和改进安全特性，在网络安全上有较大进步。5G 消灭了基于手机用户识别码（IMSI）的用户非法定位威胁，增加了用户数据的完整性保护，有效降低了漫游区欺骗风险，增强了运营商之间连接的安全性，提升了物联网抵御 DDoS 攻击的能力，兼顾了低时延业务的可靠性和安全性。5G 的这些安全特性的设计，对于提高未来网络和应用的安全具有重要作用。但是，其有效性和完备性，需要接受实践的检验。网络安全方案往往是“跟随型”的，需要等待新业务“定型”后，才能提供针对性的解决方案。

从目前的分析来看，5G 安全仍面临着前所未有的更大挑战。短期内 5G 的安全特性难以发挥，并且伪基站问题将长期存在。另一方面，新技术带来新的安全挑战。比如，网络切片技术使得网络边界模糊，5G 对用户位置隐私的保护提出更高要求，低时延业务扩大了网络安全的攻击面，5G

在促进物联网发展的同时，也会成为黑客攻击的重点目标。

为此，5G 的网络安全技术，需要产业界、网络安全企业和政府主管部门共同努力，继续加强研究和应对。

一、 5G 网络安全特性

（一）增强了对用户唯一标志符的隐私保护

5G 中手机的用户唯一标识符 SUPI（传统 3G/4G 中的 IMSI），通过公私钥加密的方式加密为 SUCI，只有运营商可以解密手机的真正的身份信息，因此追踪手机用户的非法追踪设备将失效。

（二）增强了归属地网络控制力降低了漫游区欺骗风险

鉴权过程相比 4G 的鉴权，增强了归属地网络（home network）的控制力，避免了漫游区可能欺骗 home network 的一些风险。

（三）按需提供数据加密增加了用户面数据完整性保护

在 4G 以及之前的系统中，由于完整性保护算法会增加数据处理压力，增大时延，所以一直没有使用，仅仅对控制面数据做了完整性保护。5G 对用户面数据，可按需提供空口到核心网之间的用户面数据加密和完整性保护。

（四）增强了运营商之间连接的安全性

5G 能够避免一些恶意的运营商通过 SS7 公共信道和 Diameter 协议等通道，入侵其他运营商。

（五）通过选择性拒绝终端接入加强了防物联网 DDoS 攻击的能力

恶意物联网设备可以对网络发起分布式拒绝服务攻击（DDoS），消耗接入网接入信令，消耗鉴权请求信令，或者发起大量数据流量造成网络拥塞。为防御这类攻击，5G 设计了一些安全方案可以选择性的拒绝恶意终端的接入。

（六）冗余传输安全方案兼顾了低时延业务的可靠性和安全性

低时延业务为提高传输可靠性，使用了一种冗余传输（redundant transmission）方式，就是在不同的信道上传输两份相同的数据，这可能会使安全算法失效。因此 5G 系统安全组为 redundant transmission 设计了新的安全方案。

二、 5G 网络安全挑战

（一）短时期内 5G 可能沿用 4G 核心网, 5G 的安全特性仍停留在纸面上

由于目前还没有成熟的 5G 核心网产品出现，所以目前的试验网基本采用非独立组网的 Option3 模式。5G 安全功能主要由高层协议实现，这意味着在 5G 核心网没有部署的情况下，很多 5G 安全特性还停留在纸面上。

（二）低时延业务扩大了攻击面

5G 应用场景大致可分为三类，eMBB（大带宽）、uRLLC（低时延通信）和 mMTC（大连接）。其中，4G 网络面临的网络安全问题还将在 eMBB 中延续。

低时延业务（uRLLC）扩大了网络攻击面。针对特殊垂直行业结合，5G 使得以前难以实现的场景变得可行。在安全性方面，uRLLC 会使原来不联网或相对封闭的网络连接到互联网上，这无形中扩大了网络攻击面。

（三）大连接业务使 5G 成为黑客攻击的高价值目标

未来更多的关键基础设施和重要的应用，都会架构在 5G 上。所以 5G 会成为黑客攻击的重点目标，就会有更多黑客研究 5G 的脆弱性。网络安全的本质在于对抗，攻击力量越大，则 5G 就会面临更大的安全挑战。

（四）网络切片技术使得网络边界模糊

网络切片技术的引入，使得网络边界变得十分模糊，以前依赖物理边界防护的安全机制难以得到应用，给 5G 网络安全带来了巨大的挑战。

（五）伪基站问题仍然存在

5G 时代，虽然 IMSI 已经被加密，但解决伪基站问题，仍然面临两大难题。一是广播信号签名体系不统一问题。二

是公共警告消息不能签名加密问题。因此，伪基站在 5G 时代将仍然存在。

（六）对用户位置隐私的保护提出更高要求

5G 时代网络运营商除了可以收集 5G 手机信号强度，还可以收集 WiFi、蓝牙等其他信号的强度用来定位。因此，运营商和第三方业务服务商需要遵守用户隐私保护标准，保护用户隐私数据，是一个重大挑战。

三、 小结

整体来看，5G 通过增加和改进安全特性，在网络安全上有较大进步。5G 消灭了基于手机用户识别码（IMSI）的用户非法定位威胁，增加了用户数据的完整性保护，有效降低了漫游区欺骗风险，增强了运营商之间连接的安全性，提升了物联网抵御 DDoS 攻击的能力，兼顾了低时延业务的可靠性和安全性。5G 的这些安全特性的设计，对于提高未来网络和应用的安全具有重要作用。但是，其有效性和完备性，需要接受实践的检验。网络安全方案往往是“跟随型”的，需要等待新业务“定型”后，才能提供针对性的解决方案。


从目前的分析来看，5G 安全仍面临着前所未有的更大挑战。短期内 5G 的安全特性难以发挥，并且伪基站问题将长期存在。另一方面，新技术带来新的安全挑战。比如，网络切片技术使得网络边界模糊，5G 对用户位置隐私的保护

提出更高要求，低时延业务扩大了网络安全的攻击面，5G在促进物联网发展的同时，也会成为黑客攻击的重点目标。

附件：关于 360 移动通信安全研究团队

360 移动通信安全研究团队，长期从事移动通信安全研究工作。过去 5 年中，取得了一系列国际认可的研究成果。同时，完成了若干个公益性项目，体现了 360 公司的社会责任感。

（一）研究类工作

				
ABOUT WHAT WE DO MEMBERSHIP SER				
Mobile Security Research Hall of Fame				
Welcome to the GSMA Mobile Security Research Hall of Fame.				
The GSMA's Mobile Security Research Hall of Fame lists security vulnerability finders that have made contributions to increasing the security of the mobile industry by submitting disclosures to the GSMA or its members. It is the primary mechanism for the GSMA to recognise and acknowledge the positive impact the finder has had on the mobile industry by following the GSMA's CVD process.				
The Hall of Fame also facilitates the nomination and recognition of other finders that may have made significant discoveries of vulnerabilities to individual GSMA member companies.				
Entry to the Mobile Security Research Hall of Fame is purely optional and is at the discretion of the finder, the GSMA and/or the nominating GSMA member.				
On behalf of the mobile industry, we would like to thank the following people for making a responsible disclosure to us and recognise their contribution to increasing the security of the mobile industry:				
Date	CVD#	Name	Organisation	Link
23/2/2017	0001	Yuwei Zheng, Lin Huang, Haoqi Shan, Jun Li, Qing Yang	Unicorn Team, Radio Security Research Dept., 360 Technology	http://unicom.360.com
19/6/2017	0003	Vladimir Wolstencroft	BAIKE LTD	
19/6/2017	0003	Fredrik Söderlund	Symsoft	http://www.symsoft.com
25/9/2017	0004	Maxime Meyer	Vade Secure Technology, Inc.	http://maximemeyer.com

360 发现并协助修复了全球首个 4G 网络协议漏洞，该漏洞使得攻击者可劫持任意 4G 终端的短信和语音呼叫。此

项工作，使得 360 成为成为首个进入全球移动通讯系统协会（GSMA）移动安全名人堂的安全团队，获得 GSMA 移动安全研究名人堂“CVD#0001”首位漏洞编号。

360 研究了飞蜂窝（Femto cell）基站的安全风险，在 2017 年的 DEFCON 黑客大会发表了议题。360 持续跟踪移动通信网络相关的漏洞发现，跟进分析了 LTE 中间人攻击、LTE 漏洞挖掘工具、基带芯片漏洞等热点问题。

（二）标准化工作

360 公司是唯一一家以中国网络安全公司身份参与 3GPP 标准组织的公司。定期参加 3GPP SA3（系统安全组）的会议，为 5G 通信网络安全的改进与优化发挥其技术优势。2017 年，360 推动了 3GPP 标准中重定向漏洞的修复，该漏洞是 2016 年由独角兽研究团队发现的。

（三）技术攻关工作

从 2014 年开始，独角兽团队联合 360 手机卫士、天眼团队，研究如何打击发送大量垃圾短信的 2G 伪基站。提出在手机侧识别伪基站短信，在云端分析追踪伪基站的位置的解决方案。除了在 APP 层面打击伪基站，独角兽团队还联合 360 手机部门，在基带芯片层面，为 360 手机研发了防伪基站的技术。

2018 年，一种新型的短信验证码劫持方法开始被黑产所

利用，全国各地有若干案件被报道。360 从技术角度破解了该攻击的原理、提出了防御建议，并协助公安机关完成了取证工作，对打击此类网络犯罪发挥了重要作用，得到了公安机关的官方致谢。