信安全,针对机器类终端进行高效的连接设计,在满足小数据信令和数据包传输需求的基础上,确保信令和数据传输的安全性,如隐私保护和完整性保护.

4.5 可信安全

5G 网络为了优化用户体验、提供新型商业模式,将向大量第三方应用开放网络,借此实现网络和第三方应用的互动,并优化网络资源配置.首先,5G 将提供一些网络功能如移动性、会话、QoS 和计费等功能的接口,方便第三方应用独立完成网络基本功能.此外,5G 还将开放 MANO(管理和编排),让第三方服务提供者可以独立实现网络部署、更新和扩容等网络编排能力,最终实现动态地定制网络.以上面向第三方开放的能力都是 5G 网络的基本功能,如果在开放授权过程中出现信任问题,则恶意第三方将通过获得的网络操控能力对整个 5G 网络发起攻击.此外,随着用户(设备)种类增多、网络虚拟化技术的引入,用户、移动网络运营商和基础设施提供商之间的信任问题也比以前的网络更加复杂.

4.6 安全管理

(1) 安全上下文与密钥管理

安全上下文(security context)是网络为设备建立的临时状态信息,其中包括密钥信息和数据承载信息,目的是减少设备在不同状态之间切换时与网络进行相互认证的资源消耗,方便设备快速从空闲状态安全切换到连接状态并安全通信.5G 中,设备移动、设备在不同接入网之间切换均需要考虑安全上下文的迁移和管理,迁移过程中,不同的网络对密码算法的支持情况也不同,涉及算法的重协商、上下文的标识和存储安全.此外,小数据通信模式下,安全上下文受限于设备的计算能力,也需要全新的处理方式.

在密钥管理方面,由于 5G 应用场景丰富,5G 的密钥种类呈现多样化的特点,具体包括专门用于控制平面和用户平面的机密性/完整性保护密钥、用于保护无线通信端信令和消息传输的密钥、用于支持非 3GPP 接入的密钥、用于保证网络切片通信安全的密钥以及用于支持与 LTE 系统后向兼容的密钥,等等.这一系列密钥既需要保持整体系统的统一性,又需要具备一定的独立性,以确保每个部分的安全性互不影响.此外,5G 用户种类多样并包括各种设备,5G 还将提供基于非对称密钥、基于生物信息等的用户身份识别技术.因此,5G 的密钥管理将比 4G 更为复杂,难度也更大.

(2) 安全编排

编排是通过一个中心控制节点来协同业务流程中的各种事件/活动,以达到控制总体的作用.编排的特点是服务可以连接服务,即,一个服务的输出可作为另一个服务的输入,因此能实现服务组合,创造出新的业务模型,最终满足不断变化的市场和用户需求.编排简单来讲是一种自动化的控制理论,在面向服务的架构(SOA)、平台虚拟化、融合的基础设施等领域被广泛使用.5G 在关键技术 SDN 和网络切片中大量使用编排来灵活地提供服务.3GPP 的文档 TR 28.801[41]和 NGMN 的网络服务管理白皮书[42]还就 5G 网络切片管理和编排(MANO)的一些问题进行了研究.管理和编排过程复杂,最基本的安全需求是保证各服务之间共享资源的关联性和一致性.此外,编排决定了网络/特定服务的拓扑结构,编排本身将决定在何处部署安全机制和安全策略.5G 系统需要在编排过程中提供足够的安全保证.

(3) 证书管理

5G 将引入公钥基础设施(public key infrastructure,简称 PKI)来加强用户身份的机密性保护以及网络各节点之间的相互认证.PKI 的引入使得系统必须维护庞大的 CA 系统,一方面对 CA 容量要求高;另一方面,将面临一系列证书管理的开销,如大量并发的证书申请、证书更新、证书撤销等操作.因此,5G 必须加快促进 CA 技术的发展,并将其高效地部署在 5G 系统中.此外,5G 也面临着 PKI 升级换代所带来的安全挑战和影响.

4.7 密码算法

密码算法是保证安全通信的关键组件,LTE 系统采用的一系列对称密码算法包括 SNOW 3G,ZUC[43],AES 等目前均不存在安全性问题,但随着量子计算技术的发展,5G 需要结合未来的发展趋势扩展密钥长度,并考虑算法的量子安全性,因此需要改进提高密码算法的适应性.与此同时,4G 中的大量算法计算代价大,与 5G 绿色节

能的基本要求存在一定的冲突,5G 必须考虑一系列轻量级密码算法.但 3GPP 还建议使用大量的公钥密码算法如 DHIES[44,45]及其 ECC 上的变形 ECIES、基于身份的加密(IBE)[46]和基于属性的加密(ABE)[47],这些算法随着量子计算技术的发展会遇到极大的安全挑战,应尽早做好替代准备工作.

5 5G 安全解决方案

5.1 统一的认证框架

为了解决异构接入技术和设备接入网络的问题,3GPP 在 R15 的文档 33.899[24]中给出了将可扩展认证协议(extensible authentication protocol,简称 EAP)框架,用作 5G 通用认证框架备选方案的具体描述.框架适用于任何类型的订阅者以任何一种 3GPP 定义的接入技术(包括 3G,4G)和非 3GPP 定义的接入技术(包括 WiFi,WiMAX)进行接入网认证.EAP 认证框架由 RFC 3748[48]定义,是一种支持多种认证方法的三方认证框架,框架本身不提供任何安全性,只规定了消息的封装格式,具体的安全目标依赖于使用的认证方法.目前,EAP 支持的认证方法有 EAP-MD5,EAP-OTP,EAP-GTC,EAP-TLS,EAP-SIM 和 EAP-AKA,还包括一些厂商提供的方法和新的建议.在 5G 中,具体的 EAP 协议运行于 UE,AUSF(相当于后端服务器)和 SEAF(相当于前端认证器)之间.

5.2 基于群组的海量IoT设备认证方案

认证数量庞大的 IoT 设备,对确保 5G 安全是一个巨大的挑战.群组认证协议可以一次性认证一组设备,能够有效降低系统的计算、通信和存储代价.目前,5G-ENSURE 给出了一种基于可逆 Hash 树的新型群组 AKA 协议的构造[49].该方案基于树结构存储设备的主密钥,可以一次性认证多个 IoT 设备,并能够动态地在前端认证器的计算量与后端服务器的通信量之间进行调整,可直接部署到现有的通信系统中,且通过形式化工具 ProVerif 的验证,可以提供设备与网络的双向认证、密钥的机密性、设备的隐私性等安全性质.

5.3 丰富的密钥层级架构

3GPP 在文档 TR 33.899[24]中给出了根据 3GPP 对 5G 密钥层级基本要求而整理的两种密钥架构候选方案.两种方案的差别不大,在每种方案中又各自存在两种变形,其中,候选方案 1(包括两种变形)如图 3 所示.

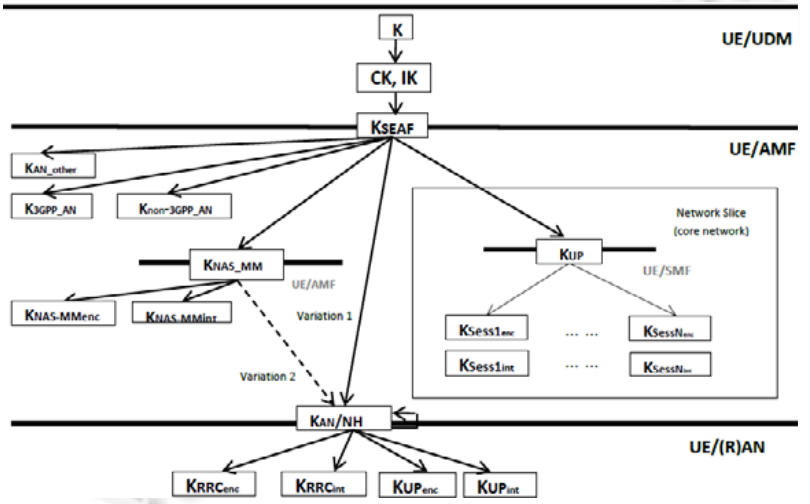

Fig.3 Keyhierarchy of 5G

图 3 5G 密钥层级候选方案

5G 基本延续了 4G 的密钥派生方式,如根密钥 K 为用户(UE)与核心网络的统一认证数据管理(UDM)共享的长期密钥,整个密钥派生系统依赖于这一密钥.密钥层级的第 2 层是加密算法密钥(confidentiality key,简称 CK)和完整性保护算法密钥(integrity key,简称 IK),是为了后向兼容而保留的密钥;在 CK 和 IK 的基础上,密钥层

级的第 3 层为 K_{SEAF},该密钥相当于 LTE 系统的 K_{ASME},主要用于在 UE 和 AMF(接入和移动管理功能)之间进行 UE 的移动管理和会话管理的密钥派生.以 K_{SEAF} 为基础,派生 3 类密钥.

(1) 非接入层移动管理密钥,主要包括 K_{NAS_MM} 以及在此基础上派生的非接入层移动管理加密密钥 $K_{NAS\text{-}MMenc}$ 和完整性保护密钥 $K_{NAS\text{-}MMint}$;

(2) 接入网络密钥 K_{AN}(两种变形体现在该密钥的派生方式上,具体差别见图 3)以及在此基础上派生的 RRC 层加密密钥 K_{RRCenc},RRC 层完整性保护密钥 K_{RRCint},用户平面加密密钥 K_{UPenc} 和用户平面完整性保护密钥 K_{UPint};

(3) 用户向网络切片请求服务时的密钥 K_{UP} 以及在此基础上为每个特定的会话 j(j=1,…,N)派生的会话加密密钥 $K_{Sessjenc}$ 和会话完整性保护密钥 $K_{Sessjint}$.

与 LTE 系统的密钥层级相比,5G 系统的密钥丰富了很多,除了以上的密钥类型,还包括为实现后向兼容而保留的接入网络密钥如 K_{3GPP_AN} 和 $K_{non\text{-}3GPP\_AN}$、为支持一些 3GPP 未考虑的接入网络引入的接入网络密钥 K_{AN_other}.

5.4 基于标识的切片安全隔离

网络切片是5G的重要组件,它使得运营商可以根据不同的市场情景和丰富的需求定制网络,以提供最优的服务.一个网络切片是一系列为特定场景提供通信服务的网络功能的逻辑组合.网络切片本身是一种网络虚拟化技术,因此,不同切片的隔离是切片网络的基本要求.为了实现切片隔离,每个切片被预先配置一个切片 ID,同时,符合网络规范条件的切片安全规则被存放于切片安全服务器(slice security server,简称 SSS)中,用户设备(user equipment,简称 UE)在附着网络时需要提供切片 ID,附着请求到达归属服务器(home subscriber server,简称 HSS)时,由 HSS 根据 SSS 中对应切片的安全配置采取与该切片 ID 对应的安全措施,并选择对应的安全算法,再据此创建 UE 的认证矢量,该认证矢量的计算将绑定切片 ID.通过以上步骤,来实现切片之间的安全隔离.

网络切片本身是一个复杂的系统,切片之间由于共享基础设施或共同协作实现更高级别的功能,使得切片之间的通信安全也至关重要.目前对这个问题的研究仍然处于初级阶段,随着 5G 网络架构的不断完善,这个问题在未来的研究中必将得到合理的解决.

5.5 基于多种身份凭证的隐私保护

网络服务订阅者的隐私在下一代网络中将面临更多安全威胁,3GPP 给出了一些隐私保护解决方案.首先,由于用户在初次访问网络之前的附着阶段还未能与网络协商出任何密钥,其长期身份标识也无法进行任何加密保护.为了避免用户长期身份标识的泄露,5G 网络将为网络核心组件配备公钥,用户在需要向网络中的认证实体发送长期身份标识时,以接收方的公钥对身份标识进行加密,从而保护长期身份信息不遭受敌手的窃听攻击.3GPP 在 TR33.899 中给出的推荐加密方案是 DHIES[44,45]及其 ECC 上的变形 ECIES.此外,3GPP 还给出基于身份的加密(IBE)[46]和基于属性的加密(ABE)[47]的解决方案,直接加密用户的身份标识或者用一个与公共属性绑定的私钥和全局公钥加密身份标识.

5.6 移动边缘计算

移动边缘计算(mobile edge computing,简称 MEC)技术[50]由国际标准组织 ETSI 提出,是在移动网边缘提供 IT 服务环境和云计算能力的技术.MEC 技术的核心思想是:将对带宽和时延要求严格的业务数据的计算、处理和存储推向无线侧,以减少网络操作和服务交付的时延消耗,提高用户的使用体验.目前,3GPP 和 NGMN 均成立了专门的工作组来进行 MEC 的相关研究.MEC 通过对数据包的深度包解析(DPI)[51]来识别业务和用户,并进行差异化的无限资源分配和数据包的时延保证.MEC 服务器可以部署在网络汇聚结点之后,也可以部署在基站内,所有通过基站的数据包都将通过 MEC 服务器的数据包解析,并由 MEC 给出是否进行本地分流的决策,不能本地处理的数据则由 MEC 传递给核心网处理.但目前,MEC 依赖的底层 DPI 技术对 HTTPS 的数据包的解析还不够成熟,而未提交至核心网的数据流量计费功能也存在问题.因此,MEC 技术还存在诸多难点有待解决.各大标准组织正在努力推动 MEC 的标准化工作,并尽可能解决现阶段 MEC 技术引入带来的部署问题,实现从 4G

到 5G 的平滑过渡.

6 小 结

5G 作为新一代移动通信网络基础设施,安全成为支撑其健康发展的关键要素.目前,5G 仍处于初期研究阶段,系统架构和许多关键技术尚未完全确定.因此,5G 带来的安全问题仍然有很多不确定性因素.在 5G 网络的整体架构设计、业务流程、算法和后续标准化工作中,将 5G 的安全需求作为研究重点,有助于整体把握 5G 系统安全要求而避免后期对系统和方案的再调整,最终实现构建更加安全可信的 5G 网络的目标.本文从 5G 的愿景、安全需求、安全框架等角度出发,详细阐述了目前 5G 面临的安全挑战以及关键安全技术.

总体来说,当前国内外针对 5G 安全的研究还不够充分,仍然面临一些亟待解决的问题:(1) 设计灵活可扩展的 5G 安全架构,以满足 5G 支撑的各类新兴的业务模式需求;(2) 提供差异化隐私保护能力,实现对隐私信息保护范围和保护强度的灵活选择;(3) 设计安全高效的密码算法和认证协议,为 5G 网络提供安全基础保障;(4) 实现多层次的切片安全,为 5G 网络不同业务提供安全分级服务;(5) 研究新型的漏洞检测方法,以避免 5G 带来的便利服务为攻击者所恶意利用.

References:

[1] http://www.itu.int/en/ITU-R/information/Pages/default.aspx

[2] http://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/Pages/default.aspx

[3] 3GPP. 3G security, security architecture. Technical Specification, TS 33.102 v12.1.0, 2014.

[4] http://www.3gpp.org

[5] IMT-2020 (5G) Promotion Group. 5G wireless technology architecture. White Paper, 2015 (in Chinese).

[6] IMT-2020 (5G) Promotion Group. 5G network technology architecture. White Paper, 2015 (in Chinese).

[7] ITU-R. IMT-vision-framework and overall objectives of the future development of IMT for 2020 and beyond. Recommendation, ITU-R M.2083-0. 2015. http://www.itu.int/rec/R-REC-M.2083

[8] http://www.3gpp.org/release-14

[9] http://www.3gpp.org/release-15

[10] https://5g-ppp.eu

[11] http://www.ngmn.org/home.html

[12] https://www.gsmaintelligence.com

[13] 5G PPP. View on 5G architecture. White Paper, v 1.0, 2016.

[14] NGMN. NGMN 5G white paper. 2015. http://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2015/NGMN_5G_White_Paper_V1_0.pdf

[15] GSMA Intelligence. Understanding 5G: Perspectives on future technological advancements in mobile. 2014.

[16] IMT-2020 (5G) Promotion Group. 5G vision and requirements. White Paper, 2014 (in Chinese).

[17] IMT-2020 (5G) Promotion Group. 5G concept. White Paper, 2015 (in Chinese).

[18] IMT-2020 (5G) Promotion Group. 5G network architecture design. White Paper, 2016 (in Chinese).

[19] IMT-2020 (5G) Promotion Group. 5G network security requirements and architecture. White Paper, 2017 (in Chinese).

[20] Ericsson. 5G system—Enabling the transformation of industry and society. White Paper, 2017. https://www.ericsson.com/assets/local/publications/white-papers/wp-5g-systems.pdf

[21] Samsung Electronics Co. 5G vision. White Paper, 2015. http://www.samsung.com/global/business-images/insights/2015/Samsung-5G-Vision-2.pdf

[22] Nokia. Now is the time to prepare for 5G. White Paper, 2013.

[23] Huawei Technologies Co. 5G opening up new business opportunities. White Paper, 2016.

[24] 3GPP. Study on the security aspects of the next generation system. Technical Report, TR 33.899 v1.1.0, 2017.

[25] 5G PPP. 5G PPP phase 1 security landscape. 2017. https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf

[26] NGMN. 5G security recommendations (package #1, package #2: networking slicing, package #3: mobile edge computing). White Paper, 2016.

[27] Ericsson. 5G security—Scenarios and solutions. White Paper, 2017.

[28] https://www.ericsson.com/assets/local/publications/white-papers/wp-5g-security.pdf

[29] Nokia. Security challenges and opportunities for 5G mobile networks. White Paper, 2017.

[30] Huawei Technologies Co. 5G security: Forward thinking. White Paper, 2015. http://www.huawei.com/minisite/5g/img/5G_Security_Whitepaper_en.pdf

[31] ETSI. Network functions virtualization (NFV); Terminology for main concepts in NFV. Group Specification, NFV 003 v1.1.1. 2013.

[32] ETSI. Network functions virtualization (NFV); Use cases. Group Specification, NFV 001 v1.1.1. 2013. http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf

[33] ETSI. Network functions virtualization (NFV); Proof of concepts; Framework. Group Specification, NFV-PER 002 v1.1.2. 2014. http://www.etsi.org/deliver/etsi_gs/NFV-PER/001_099/002/01.01.02_60/gs_NFV-PER002v010102p.pdf

[34] Evangelos H, Kostas P, Spyros D, Hadi SJ, David M, Odysseas K. Software-Defined networking (SDN): Layers and architecture terminology. IETF RFC 7426. 2015.

[35] 3GPP. 3GPP system architecture evolution; Security architecture. Technical Specification, TS 33.401 v15.0.0, 2017.

[36] https://en.wikipedia.org/wiki/Orchestration_%28computing%29

[37] Gnther H, Peter S. Towards 5G security. In: Proc. of the 14th IEEE Int'l Conf. on Trust, Security and Privacy in Computing and Communications. Helsinki, 2015. 1165−1170. [doi: 10.1109/Trustcom.2015.499]

[38] 3GPP. Study on architecture for next generation system (release 14). Technical Report, TR 23.799 v14.0.0, 2016.

[39] 5G-Ensure Deliverable D3.5. 5G-PPP security enablers technical roadmap (update). 2016. http://5gensure.eu/sites/default/files/5G-ENSURE_D3.5%205G-PPP%20security%20enablers%20technical%20roadmap%20%28Update%29.pdf

[40] 3GPP. Study on subscriber privacy impact in 3GPP. Technical Report, TR 33.849 v14.0.0, 2016.

[41] 3GPP. Feasibility study on new services and markets technology nnablers—Network operation. Technical Report, TR 22.864 v15.0.0, 2016.

[42] 3GPP. Study on management and orchestration of network slicing for next generation network. Technical Report, TR 28.801 v1.2.0. 2017.

[43] NGMN. 5G network and service management including orchestration. White Paper, v2.12.7. 2017.

[44] 3GPP. Specification of the 3GPP confidentiality and integrity algorithms EEA3 and EIA3, document 4: Design and evaluation reprot. Technical Specification, TR 35.924 v11.0.1, 2012.

[45] Michel A, Mihir B, Phillip R. DHAES: An encryption scheme based on the Diffie-Hellman problem. IACR Cryptology ePrint Archive. 1999. 7.

[46] Michel A, Mihir B, Phillip R. The oracle Diffie-Hellman assumptions and an analysis of DHIES. In: Proc. of the Cryptographers' Track at RSA Conf. San Francisco, 2001. 143−158. [doi: 10.1007/3-540-45353-9_12]

[47] Dan B, Matt F. Identity-Based encryption from the Weil pairing. In: Proc. of the 21st Annual Int'l Cryptology Conf. Santa Barbara, 2001. 213−229. [doi: 10.1007/3-540-44647-8_13]

[48] Amit S, Brent W. Fuzzy identity based encryption. IACR Cryptology ePrint Archive. 2004. 86.

[49] Bernard A, Larry BJ, John VR, James C, Henrik L. Extensible authentication protocol (EAP). IETF RFC 3748, 2004.

[50] Rosario G, Christian G, Markus A, Simon H. A secure group-based AKA protocol for machine-type communications. In: Proc. of the 19th Annual Int'l Conf. on Information Security and Cryptology. Seoul, 2016. 3−27. [doi: 10.1007/978-3-319-53177-9_1]

[51] ETSI. Mobile edge computing—A key technology towards 5G. White Paper, ISBN No. 979-10-92620-08-5. 2015. http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf

[52] https://en.wikipedia.org/wiki/Deep_packet_inspection

附中文参考文献:

[5] IMT-2020(5G)推进组.5G 无线技术架构.白皮书,2015.

[6] IMT-2020(5G)推进组.5G 网络技术架构.白皮书,2015.
[16] IMT-2020(5G)推进组.5G 愿景与需求.白皮书,2014.
[17] IMT-2020(5G)推进组.5G 概念.白皮书,2015.
[18] IMT-2020(5G)推进组.5G 网络架构设计.白皮书,2016.
[19] IMT-2020(5G)推进组.5G 网络安全需求与架构.白皮书,2017.

冯登国(1965－),男,陕西靖边人,博士,研究员,博士生导师,主要研究领域为网络与信息安全,可信计算与信息保障.

徐静(1972－),女,博士,研究员,博士生导师,主要研究领域为应用密码学,安全协议.

兰晓(1990－),女,博士,主要研究领域为安全协议.