5G移动网络安全技术分析

Analysis of Security Technology of 5G Mobile Network

谢振华(中兴通讯股份有限公司,江苏 南京 210012)
Xie Zhenhua(ZTE Corporation,Nanjing 210012,China)

摘　要:
从前几代移动网络到5G移动网络的发展,是从相对封闭走向相对开放的转折,势必会对移动网络的安全形成新的挑战。分析了5G移动网络的核心网、接入网和网间互联在面对新的安全威胁时所用到的技术,如多种接入的统一认证框架、多接入多连接场景的安全、能力开放的安全、切片安全、隐私增强、信令安全增强、按需用户面安全、网间应用层安全边界网关等。

关键词:
5G;移动网络;安全
doi:10.12045/j.issn.1007-3043.2019.04.011
中图分类号:TN915.08
文献标识码:A
文章编号:1007-3043(2019)04-0049-04

Abstract:
It is an initiative transition from closure to opening when the mobile network evolves to 5G. New security threats bring new challenges to the 5G mobile network. It analyzes the security technology of 5G mobile network for the new security threats faced by core network, access network and inter-network interconnection, such as unified authentication framework, security method for multiple NAS connections, security on network capability exposure, security on network slicing, enhanced privacy, enhanced signaling security, on demand UP security, inter-operator security edge protection proxy.

Keywords:
5G; Mobile network; Security

引用格式:谢振华. 5G移动网络安全技术分析[J]. 邮电设计技术,2019(4):49-52.

0 引言

5G移动网络并非是简单的4G移动网络的技术升级,其更重要的进步是更加开放的通信支撑能力,为更广泛的行业应用提供互联互通的网络环境,并最终实现相对统一的多应用互联互通技术平台,打通信息孤岛,实现万物互联。基于这样的目标,势必要求5G网络支持更多样的接入手段,更开放的网络环境,更丰富的应用支撑。

从相对封闭走向相对开放的过程势必会对移动网络的安全带来更多新的挑战。本文分别论述了针对核心网、接入网和网间互联的安全威胁所做的安全提升方面的设计。

收稿日期:2019-02-12

1 5G核心网的相关安全技术

5G移动网络的开放性,首先体现在接入的多样性上。前几代的移动网络仅支持宏蜂窝基站以及家庭基站方式的接入,这些接入方式都是基于3GPP无线制式的。前几代移动网络对于其他接入方式(如Wi-Fi、Cable、有线等)的支持都是十分有限的,基本上采用独立的与接入相关的非3GPP网络来服务使用相应接入方式的用户,再通过网络间的有限交互实现低层次的互通。

5G移动网络针对多制式的接入方式,采用了统一的认证框架(见图1),无论终端用户采用何种制式,5G移动网络都可以使用这个统一的认证框架与终端用户实现相互认证,真正做到了认证的接入无关。

5G移动网络的统一认证框架中,SEAF为安全锚

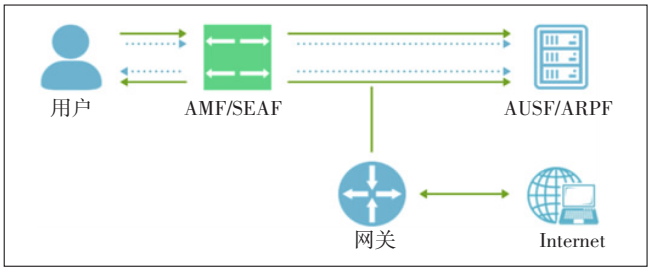

图1　5G统一认证框架示意

点，与4G移动网络中的MME的认证功能相似，而新增的AUSF主要用于支持基于可扩展认证协议（EAP）框架的认证。EAP认证框架是目前所知最能满足5G统一认证需求的方案，它是一个能封装各种认证协议的统一框架，框架本身并不提供安全功能，认证期望取得的安全目标，由所封装的认证协议来实现，它支持多种认证协议，如预共享密钥（EAP-PSK），传输层安全（EAP-TLS），鉴权和密钥协商（EAP-AKA'）等。5G移动网络支持不同制式的接入方式，而不同的接入网使用不同的协议，这意味着5G移动网络需要一个能适配各种认证协议的统一框架，EAP正好能满足这样的应用场景和技术实现的要求。统一认证框架扩展了5G移动网络的认证能力，考虑到5G还将允许垂直行业的设备和网络使用其特有的技术接入，统一认证框架将为满足这一需求提供极大的便利。统一认证框架还能使5G移动网络实现统一的密钥层次体系，进而可实现用户在不同接入网间的无缝切换。

由于支持多接入不仅仅是网络的需求，也是终端的需求，这势必会导致终端与5G核心网间的信令存在多个连接的情况。为了应对这一新增场景，5G核心网需要隔离同一个用户的不同信令连接，以防止其中一个连接上的信息泄露威胁到其他连接上的数据。5G核心网目前采用了简单的多连接共享核心网密钥及算法的方案，为了实现不同连接的安全隔离，不同连接采用不同的密钥流生成参数以及消息校验码生成参数，这样做简化了同步技术，有利于实现移动场景下的无缝多路传输。

5G移动网络的开放性也体现在向第三方开放的网络能力上。5G核心网的各网络功能采用基于业务的架构（SBA——Service Based Architecture），可实现类似于受控的full mesh方式的交互，这区别于前几代的点到点静态网状互联方式，使网络的一些功能可以通过RESTful接口开放给第三方业务或垂直行业。这其中也包括了5G移动网络的安全功能，主要体现在以下几方面：基于网络接入认证向第三方提供业务层的访问认证，即如果业务层与网络层互信，用户在通过网络接入认证后可以直接访问第三方业务，这简化了用户访问业务的认证流程并提高了业务访问效率；基于终端智能卡（如UICC、嵌入式UICC）的安全能力，拓展业务层的认证维度，增强业务认证的安全性。通过网络安全能力开放，可以让第三方应用便捷地使用移动网络的安全能力，从而让第三方业务提供商能有更多的时间和精力专注于具体应用业务逻辑的开发，进而快速、灵活地部署各种新业务，以满足用户不断变化的需求；同时，运营商也通过提供更开放的5G网络能力，拓展全新的业务渠道。网络能力的开放对调用者认证和访问授权提出了更高的要求，因此专门设计了5G移动网络通用API框架（CAPIF——Common API Framework）来保障能力开放的安全，具体如图2所示。

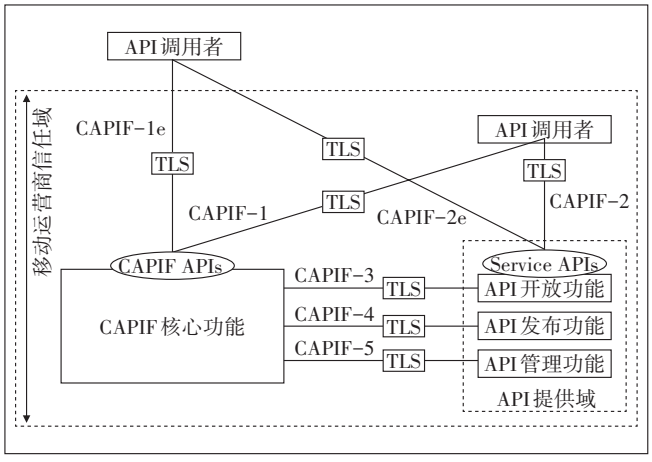

图2　通用API框架功能安全模型示意

5G移动网络能力开放的一种终极手段就是网络切片，即通过虚拟化一个完整的5G移动核心网来定制化地满足特定业务或特定业务提供方的移动通信需求。5G移动网络通过引入网络功能虚拟化（NFV）技术和软件定义网络（SDN）架构，实现了切片化。目前5G移动网络的切片架构分为公共域和切片相关域，如图3所示，切片相关域中主要包括会话管理功能（即SMF）和用户面功能（即UPF）。切片安全机制主要包含3个方面：UE和切片间安全、切片内网络功能与切片外网络功能间的安全、切片内网络功能间的安全。平台技术（即NFV和SDN）本身提供了一定的安全保障，比如SDN控制器防护、虚拟机安全隔离等，此外，5G移动网络主要通过Network Repository功能提供的访问授权机制来确保以上3方面的安全。

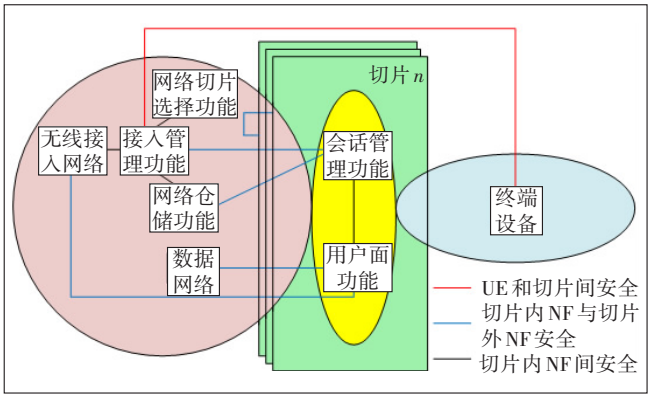

图3　切片安全机制

2 5G接入网的相关安全技术

5G接入网可以是无线接入网也可以是有线接入网，但主要是无线接入网。无线环境是一个开放暴露的环境，因此5G接入网的安全会影响整个5G移动网络。在前几代的移动网络迭代演进过程中，无线接入的安全性已经得到了非常显著的提升，5G移动网络时代则更注重隐私保护、信令安全和用户面数据的安全，因此针对性地设计了增强的隐私保护、增强的信令保护以及增强的用户面数据保护方案。

在隐私安全方面，众所周知，前几代移动网络在初始接入时需要用户在开放的无线环境中以明文方式传递永久用户标识，这一缺陷在早期还并未有明显问题，但随着技术的发展，攻击者的能力也增强了，这一缺陷所带来的风险也变得越来越高。为解决这一问题，5G移动网络采用了非对称加密技术来保护永久用户标识的传递。运营商通过在USIM卡中预先设置归属网的公钥及其他相关信息，使用户终端可以使用归属网的公钥对永久用户标识进行加密保护。用于传输的被保护的永久用户标识（SUCI——Subscription Concealed Identifier）的结构如图4所示，其中Routing indicator用于一个运营商有多个解密功能的情况下标识其使用哪个解密功能来解密SUCI，Protection Scheme Id用于标识加密的机制，其中标准化了2个ECC的加密机制，归属网运营商也可以自定义非标准化的加密机制。

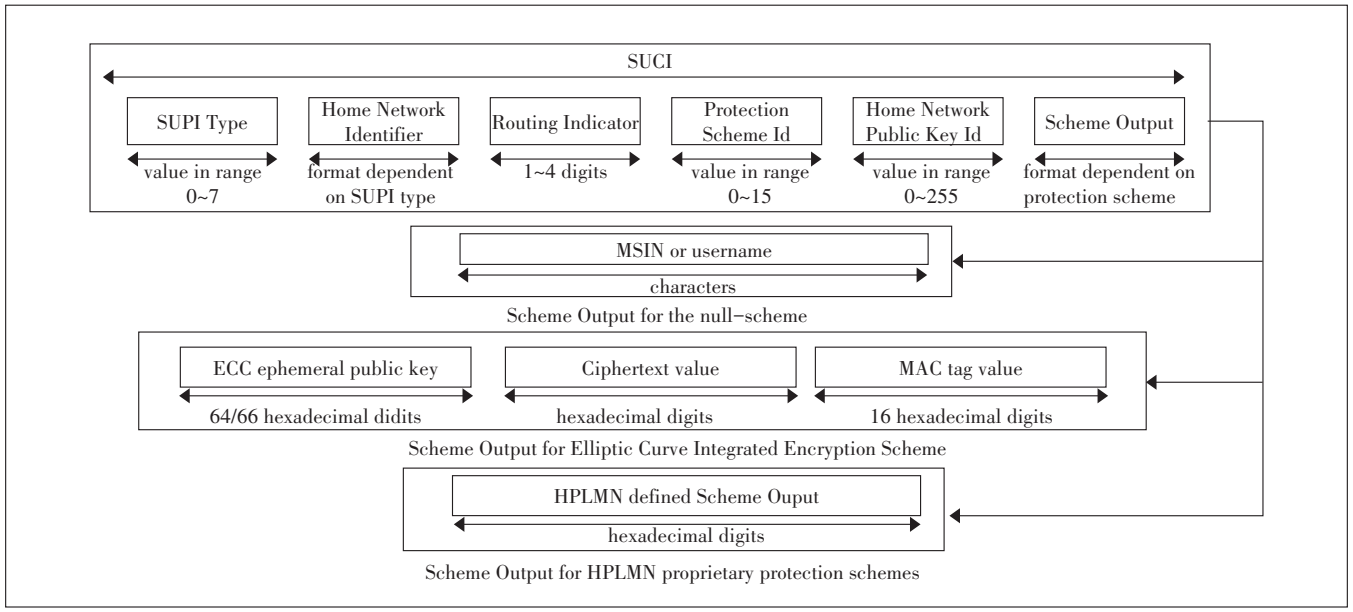

图4　被保护的永久用户标识（SUCI）结构

前几代的移动网络还使用了临时用户标识来保护隐私，但由于标准定义不明确，导致在实际使用中存在不更新临时用户标识的情况，相当于把临时用户标识当成半永久用户标识在使用，导致在开放的无线环境中可以方便地跟踪用户。3GPP标准组织针对这种情况明确了5G移动网络在注册、业务发起过程中必须刷新临时用户标识。

在信令保护方面，前几代的移动网络在终端从空闲态向网络发起业务时，发送的初始信令都是用的明文。随着数据分析技术的进步，这些在开放无线环境中传输的信息存在泄露用户隐私、用户习惯、用户业务类型等安全风险。在5G移动网络时代，为了增强安

全性，减少信息在开放的无线环境中暴露的风险，设计了加密传输初始信令的机制，除了与建立安全连接有关的信息可以明文传递外，其他信息一律加密传输，加密使用的密钥等信息基于本次或之前的安全建立过程协商而来。

5G时代既有移动互联网终端（主要为5G手机），也有海量的物联网终端，在用户数据保护方面，其安全需求不再是一致和单一的，而是按需而定的。5G移动网络可以按需决定是否在用户面使用加密和完保的安全措施，从而使无线安全的适用性更强。

3 5G移动网络网间的相关安全技术

前几代的移动网络设计虽然也考虑了网间安全，网间信令协议从完全没有安全策略的7号信令到Diameter协议，网间安全在理论层面有了显著的提升，但实际部署上，传输网络运营商大多没有启用安全保护，毕竟传输网络运营商不在3GPP的约束范围内。

在沿用以往已经成熟的网间信令传输运营模式的基础上，5G移动网络为了加强信令的安全性，专门设计了安全边界保护网关（SEPP——Security Edge Protection Proxy）来保障应用层的安全，这样即使传输层没有启用安全机制，信令中的敏感信息仍旧是安全的。图5为网间信令保护的示意图，其中cSEPP为消费者SEPP，即信令发送方的SEPP，pSEPP为提供者SEPP，即信令接收方的SEPP，c/pIPX为传输层的传输运营商信令转发设备。

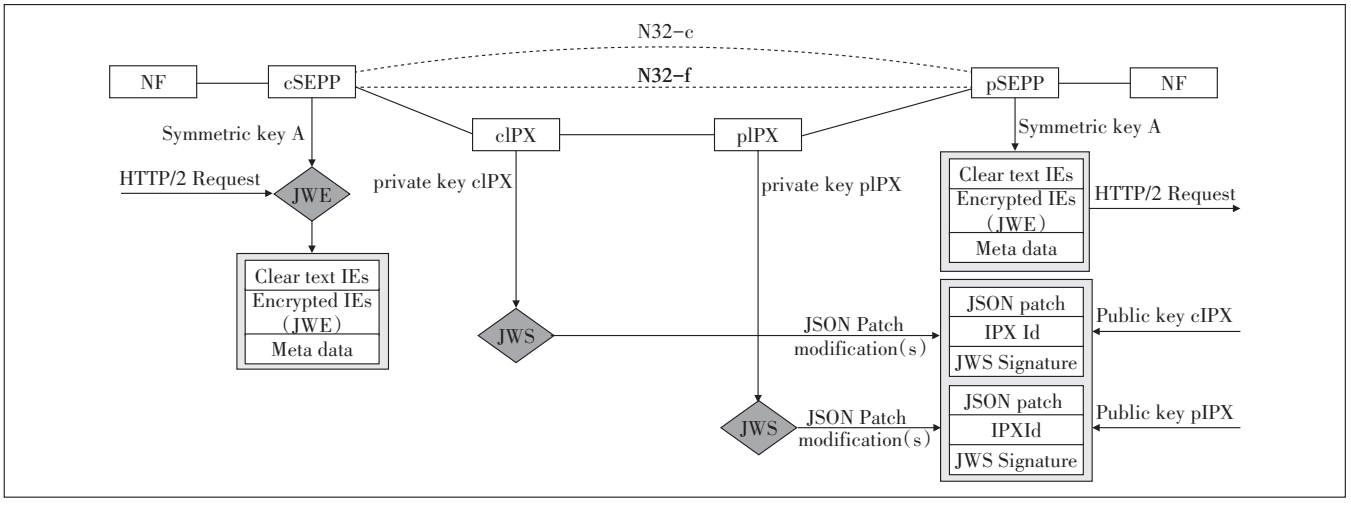

图5　5G移动网络网间信令保护示意图

4 结束语

5G移动网络标准的设计工作虽然目前尚处于初始阶段，但从中已经可以看出5G网络的明显的开放特性。2019年将启动5G移动网络的新版本标准设计，新版本标准将更突出物联网业务支持、高可靠低时延业务支持、垂直业务支持等，更好地支持类似物联、车联、在线游戏、企业网等应用。相信随着标准的不断演进，5G移动网络的开放性将更加突出、网络的安全性也将更加牢固。

参考文献：

[1] Study on Architecture for Next Generation System：3GPP TR 23.799 [S/OL]. [2019-01-22]. ftp://ftp.3gpp.org/Specs/.

[2] System architecture for the 5G System；Stage 2：3GPP TS 23.501 [S/OL]. [2019-01-22]. ftp://ftp.3gpp.org/Specs/.

[3] Procedures for the 5G System；Stage 2：3GPP TS 23.502 [S/OL]. [2019-01-22]. ftp://ftp.3gpp.org/Specs/.

[4] Study on the security aspects of the next generation system：3GPP TR 33.899 [S/OL]. [2019-01-22]. ftp://ftp.3gpp.org/Specs/.

[5] Security architecture and procedures for 5G system：3GPP TS 33.501 [S/OL]. [2019-01-22]. ftp://ftp.3gpp.org/Specs/.

[6] Study on Enhancement of Network Slicing：3GPP TR 23.740 [S/OL]. [2019-01-22]. ftp://ftp.3gpp.org/Specs/.

作者简介：

谢振华，长期致力于3GPP标准技术研究与标准方案推进工作，目前主要从事3GPP安全标准技术研究工作。