RESTful API 在 5G 应用场景中的安全威胁研究

张奕鸣 刘彩霞 刘树新
(中国人民解放军战略支援部队信息工程大学 河南 郑州 450002)

摘 要 针对 5G 核心网络引入的 RESTful API 服务化关键技术,研究其安全威胁。梳理 5G 网络服务化架构和 RESTful API 应用方法,从四个方面分析 RESTful API 在 5G 应用场景中存在的安全问题以及可能引入的安全威胁,并针对每类安全威胁提出安全防护机制。

关键词 5G 服务化架构 RESTful API 安全威胁

中图分类号 TP309.2 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2023.02.049

SECURITY THREATS OF RESTFUL API IN 5G APPLICATION SCENARIOS

Zhang Yiming Liu Caixia Liu Shuxin
(*PLA Strategic Support Force Information Engineering University, Zhengzhou 450002, Henan, China*)

Abstract For the key technologies of RESTful API service introduced by 5G core network, we study its security threats. The 5G network service architecture and RESTful API application methods were sorted out. We analyzed the security problems and possible security threats of RESTful API in 5G application scenarios from four aspects, and proposed a security protection mechanism for each type of security threat.

Keywords 5G Service-based architecture RESTful API Security threats

0 引 言

5G 网络为了满足增强移动宽带、超高可靠超低延迟通信和大规模机器类通信[1]等应用场景的业务需求,引入了毫米波、超密集组网、大规模多输入多输出、软件定义网络、网络功能虚拟化、基于服务化架构(SBA)等新技术和新机制[2-3]。同时,互联网开放和共享的一些优势技术也被 5G 技术标准采用,其中 RESTful API 作为 5G SBA 架构实现的一种关键技术被 3GPP 纳入 5G 标准[4-5]。

REST(Representational State Transfer)是互联网络应用程序的一种设计理念与开发方式,其概念是 Roy Thomas Fielding 在 2000 年所发表的论文中提出的[6],Fielding 在论文第 6 节中详细描述了如何在互联网中使用统一资源标识符(URI)、超文本传输协议(HTTP)和不同数据表示格式实现 REST,满足 REST 开发方式的 API 则被称为 RESTful API。当前,RESTful API 已经在 Web 服务和物联网等场景得到成熟应用。

RESTful API 在 Web 服务和物联网应用场景中已经发现面临诸多安全问题,如:(1) 由于 Web 服务的大连接特性和物联网终端处理能力受限特性使得 RESTful API 在这两种场景中面临 DDoS 攻击威胁;(2) RESTful API 的身份验证机制导致其面临中间人攻击威胁;(3) 针对 RESTful API 输入参数的注入攻击威胁;(4) 由于 RESTful API 使用 XML、JSON 等序列化方法传输请求和响应数据,使得攻击者利用 XML 和 JSON 自身漏洞对 RESTful API 发起攻击等。

针对 RESTful API 在 Web 服务与物联网应用场景中的安全威胁,业界也开展了一些安全增强机制研究。文献[7]提出基于 ID 的身份验证算法,利用 URI 实现客户端与服务器的轻量身份验证,解决 REST 的无状态特性带来的复杂身份验证问题。文献[8]提出一种 REST 安全协议,采用数字证书、消息签名、消息对称加密方法为 RESTful API 消息提供机密性、完整性和不可抵赖性保护。文献[9]提出一种一次性令牌机制,每个 REST Web 请求都携带唯一的不易伪造的一次性令牌,令牌中包含时间戳,并限制合法访问的时间窗

收稿日期:2020-07-08。国家科技重大专项(2018ZX03002002)。**张奕鸣**,硕士,主研领域:移动通信安全,网络空间安全。**刘彩霞**,研究员。**刘树新**,助理研究员。

口,降低 REST Web 服务遭受中间人攻击与劫持攻击的风险。文献[10]引入了 RE-CHECKER 框架分析软件定义网络控制器中的 RESTful 服务的漏洞。文献[11]提出了一种基于 RESTful API 的体系结构保护物联网设备安全,物联网中间件使用 RESTful API 对终端进行身份验证后下发令牌,并将持有令牌的终端生成的数据上传至云服务器等。

由于 5G 网络面向海量连接和大规模通信应用场景,网络功能(NF)间存在身份验证机制,控制平面 NF 间数据传输使用 JSON 编码,故 RESTful API 在 5G 场景中也可能面临相似的安全威胁。此外,RESTful API 在 5G 网络应用场景的特殊应用需求,也会引入新的安全威胁。

本文首先介绍 5G 核心网 SBA 架构,在此基础上,介绍了 REST 的特点和 SBA 架构中应用 RESTful API 的具体流程,从 DDoS 攻击、JSON 安全威胁、中间人攻击、注入攻击四个角度分析了 RESTful API 在 5G SBA 架构中可能存在的安全威胁,最后,分别基于 RESTful API 请求频率控制、JSON 防护、令牌改进、参数检查四个方面给出了在 5G 应用场景针对四类威胁的安全防护方案,为增强 RESTful API 在 5G 核心网的应用安全提供参考。

1　5G 核心网 SBA 架构与 RESTful API

3GPP 定义了 5G 网络的架构,如图 1 所示[12],定义了 NF 之间交互的两种表示方法,分别是基于服务表示和参考点表示。图 1 中 5G 网络架构可以分为两部分,分别是用户平面与控制平面,虚线下方为用户平面,虚线上方为控制平面。5G 网络中控制平面 NF 之间通过基于服务的表示进行交互,例如接入管理功能(AMF)通过 Namf 为其他控制平面的 NF 提供服务,参考点表示应用于用户平面 NF 之间的交互,例如接入网((R)AN)通过参考点 N3 与用户平面功能(UPF)进行交互,控制平面与用户平面之间的交互同样使用参考点表示,参考点分别是 N1、N2、N4。

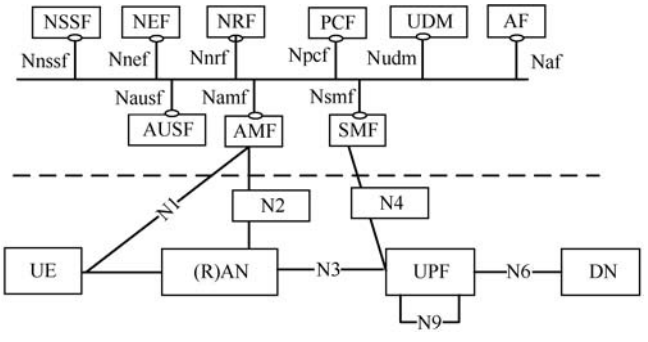

图 1　5G 网络架构

3GPP 定义的基于服务表示方法以基于服务接口(SBI)作为实现,3GPP 对 SBI 的协议栈进行了定义[13]。SBI 协议栈自底向上在网络层协议采用 IP,传输层协议采用 TCP,应用层协议采用 HTTP/2.0,采用 JSON 作为序列化方法,采用 OpenAPI3.0 作为接口描述语言,采用 REST 作为 API 开发方式[14]。RESTful API 有以下几个主要特点:(1) RESTful API 的开发采用客户端-服务器的设计架构;(2) RESTful API 的无状态性,即服务器不保存客户端的信息,客户端发送的每一个请求都需要包含所有必需的状态信息;(3) 服务器中的所有资源采用 URI 进行标识,资源可以是文字、图片、音频、视频、服务等;(4) 资源的表示形式根据客户端的需要进行转换,例如服务器可向客户端发送 XML、JSON、TXT 等类型的数据;(5) 客户端对资源所进行的操作使用 HTTP 方法实现,查询操作采用 GET 方法,新增操作采用 POST 方法,修改更新操作采用 PUT 或 PATCH 方法,删除操作采用 DELETE 方法。

RESTful API 设计方案减少了 5G 网络控制平面 NF 之间的耦合度和依赖性,符合 5G 网络服务化的理念,此外,电信运营商可以使用 RESTful API 将不同地理位置和不同类型的 NF 组合到网络切片中,实现 5G 网络的云化、虚拟化和按需部署。

以 AMF 通过服务发现请求访问 NRF 并使用 SMF 服务为例,阐述 RESTful API 应用流程,为了便于说明,例中应用场景为非漫游。在此场景中,AMF 为 NF 服务消费者,SMF 为 NF 服务生产者,NRF 为授权服务器。NF 之间交互如图 2 所示。

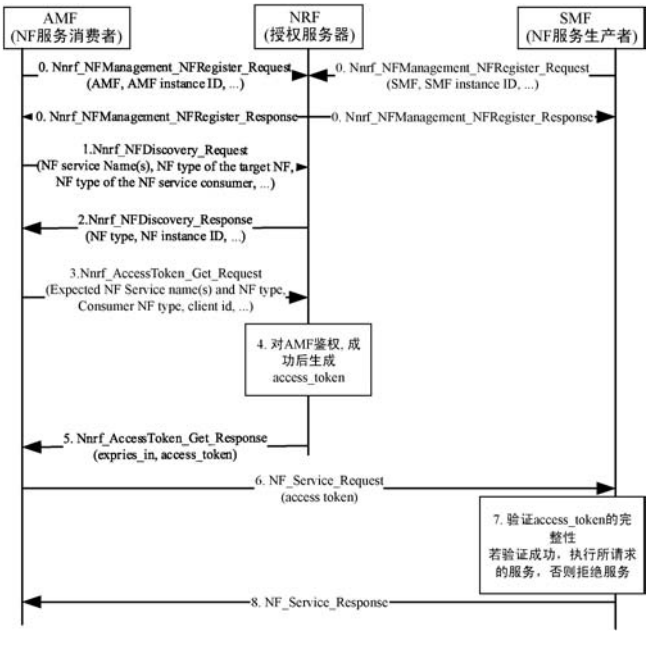

图 2　AMF-NRF-SMF 交互

5G 核心网 NF 服务访问授权采用 OAuth2.0 框架,

5G 核心网控制平面中的 NF 服务消费者通过 RESTful API 请求使用 NF 服务生产者的服务须经过 NRF 授权且 NF 服务消费者与 NRF 之间授权的方式是 OAuth2.0 框架的 Client Credentials,即 NF 服务消费者和 NF 服务生产者首先须要在 NRF 中注册,注册完成后 NF 服务消费者使用 Nnrf_NFDiscovery_Request 请求获取 NRF 中已注册的 NF 服务生产者信息,然后 NF 服务消费者使用 Nnrf_AccessToken_GET_Request 向 NRF 请求访问令牌,NRF 对 NF 服务消费者进行鉴权,若通过鉴权,则向 NF 服务消费者下发访问令牌,NF 服务消费者需要将访问令牌与服务请求一同发送至 NF 服务生产者,NF 服务生产者验证令牌完整性后执行服务。根据 RFC 6749[15]和 3GPP 的定义[16],5G 核心网控制平面的 NF 在 OAuth2.0 框架中的角色如下:(1) NRF 为 Authorization server;(2) NF 服务消费者为 Client;(3) NF 服务生产者为 Resource server。

2 5G 核心网 Restful API 安全威胁

RESTful API 的无状态特性提高了服务器可扩展性,服务器可以以此为基础实现负载均衡,减轻流量压力;RESTful API 使用 URI 标识服务器资源,简化了资源的发现过程;客户端使用已有 HTTP 协议的方法对资源进行操作,提高了 RESTful API 的兼容性,这些优势使 RESTful API 在现代软件架构设计中越来越重要。但与此同时引入了因 RESTful API 设计漏洞而产生的安全威胁。分布式拒绝服务(DDoS)攻击尤为普遍和显著,其本质是攻击者利用与受害主机的资源不对称特性,控制 5G 网络中不同位置的多台假冒 NF 同时对受害 NF 发起恶意请求,导致受害 NF 资源耗尽,无法为合法 NF 提供正常服务[17]。JSON 是 5G 核心网 SBI 协议栈中的序列化方法,即通过 RESTful API 发送请求和响应数据的编码方式是 JSON,故其安全漏洞会成为攻击者通过 RESTful API 攻击 5G 网络的途径。中间人攻击是 5G 网络安全威胁中一个重要部分,攻击者可以建立中间人监听访问令牌从而非法请求服务。RESTful API 的输入参数会受到注入攻击的威胁,注入攻击的根本原因是系统对用户的输入验证不足,可以根据输入内容分类为以 SQL 语句作为输入的 SQL 注入[18]、以系统无法处理的错误数据作为输入的错误数据注入[19]、以恶意可执行代码作为输入的恶意代码注入等。5G 核心网 RESTful API 安全威胁如图 3 所示,以下对安全威胁进行详细说明。

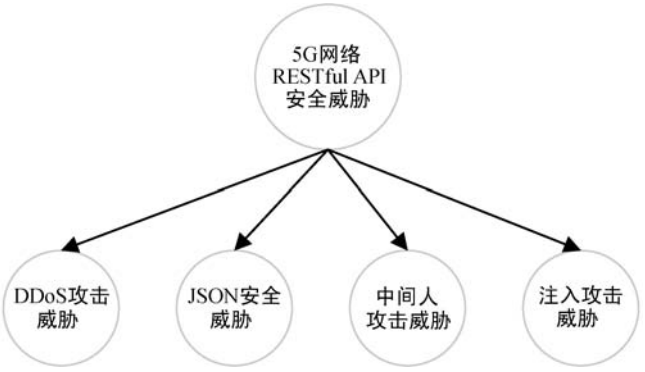

图 3 5G 核心网 RESTful API 安全威胁

2.1 DDoS 攻击威胁

在 5G 核心网中,假设攻击者控制多台假冒 NF 在多个 PLMN 中的 NRF 中进行注册,注册完成后同时请求同一个 PLMN 中 NRF 的同一个服务 RESTful API,如图 4 所示,若该受害 NRF 的 RESTful API 运行需要消耗较多资源,例如服务发现 RESTful API,则受害 NRF 可能会由于本身资源的耗尽而无法为合法 NF 提供正常服务。

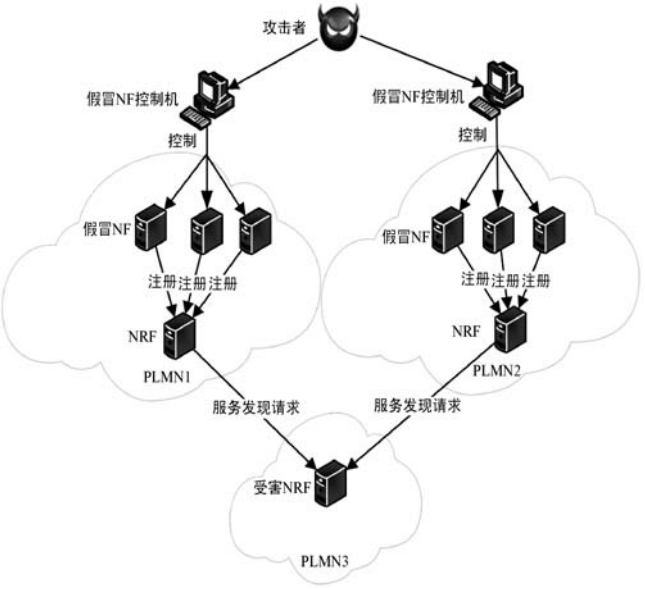

图 4 DDoS 攻击

2.2 JSON 安全威胁

利用当前最新发现的 JSON 漏洞 CVE-2020-10663,攻击者可以在 5G 网络 NF 的 JSON 解析器中创建恶意对象。3GPP 规定了当前 5G 核心网控制面中 PLMN 之间 JSON 消息数据传输由 SEPP 和 IPX 进行保护[16],SEPP 使用 JWE[21]对 JSON 数据进行机密性和完整性保护,IPX 使用 JWS[22]对修改后 JSON 数据进行数字签名,如图 5 所示。但在同一个 PLMN 核心网内控制平面 NF 之间 JSON 数据传输并没有受到保护,在 SBI 协议栈中是否采用 TLS 仍在讨论中[23]。如果不使用 TLS 机制,攻击者可以通过监听和嗅探等方式获取

JSON 数据,若 JSON 数据中包含地理位置、身份标识等用户敏感信息,则会危害用户隐私。即使使用 TLS 机制,攻击者可以将伪造的 TLS 证书安装在 PLMN 的核心网中,从而使用攻击者的公钥对所有数据包进行加密,并使用攻击者的私钥(由伪造的 TLS 证书提供)对其进行解密[24]。因此,攻击者可以读取所有加密的 JSON 数据。

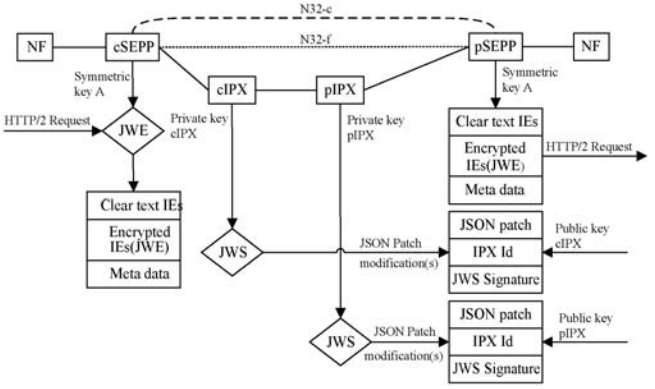

图 5　PLMN 间 JSON 消息保护

2.3　中间人攻击威胁

上文举例说明了 5G 核心网中 AMF 使用 RESTful API 在 NRF 中注册并获取访问令牌进而请求 SMF 服务。如果攻击者在 AMF 和 NRF 之间插入非法的监听设备,如图 6 所示,NRF 对 AMF 鉴权成功后,会将访问令牌通过 Nnrf_AccessToken_Get_Response 消息发送至 AMF,此时若攻击者通过监听设备获取到了 AMF 的访问令牌,则攻击者可以控制假冒 AMF 携带访问令牌使用 SMF 的服务而不被检测到,若 NRF 下发的是敏感服务的访问令牌,例如 AMF 的获取用户地理位置的服务,则攻击者可以获取到用户的地理位置进而追踪用户。

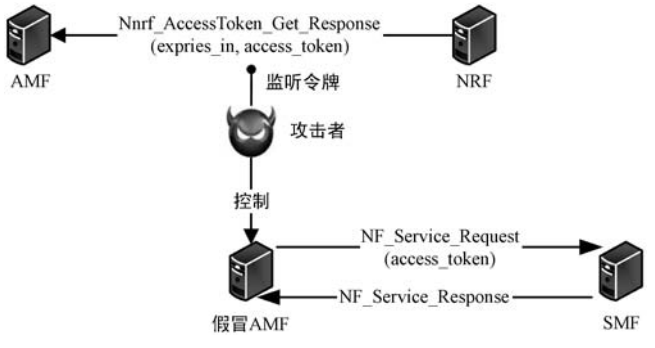

图 6　中间人攻击

2.4　注入攻击威胁

在 5G 核心网中攻击者可以利用某些 NF 没有对 RESTful API 的输入参数进行严格检查的漏洞,在 RESTful API 的输入参数中注入恶意数据从而获取敏感信息。试想,攻击者通过中间人攻击获取到特定 NF 服务(例如 AMF 的 Namf_MT 服务)访问令牌后,使用访问令牌所规定权限范围之外的 NF 服务(例如 AMF 的 Namf_Location 服务)构造恶意请求,攻击者将恶意请求与访问令牌一同发送至 NF 服务生产者端,由于访问令牌是合法的,若 NF 服务生产者没有严格检查令牌中权限范围参数与请求服务是否匹配,则 NF 服务生产者会执行攻击者的恶意请求,这可能导致用户的敏感信息被窃取,若攻击者构造的恶意请求包含 NF 服务生产者无法处理的越界参数,则可能导致其崩溃,如图 7 所示。

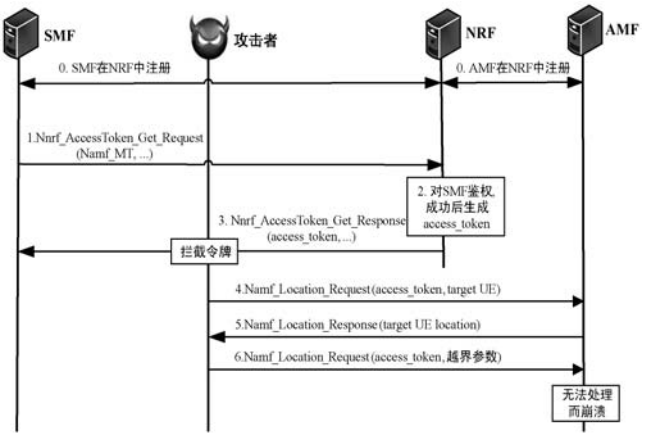

图 7　注入攻击

3　5G 核心网 RESTful API 安全防护机制

针对上文分析的 RESTful API 在 5G 核心网存在的安全威胁,基于业界对 RESTful API 在 Web 与物联网安全研究方法,本文结合 5G 网络 SBA 架构特点,对四类安全威胁提出了对应的安全防护机制。

3.1　DDoS 攻击威胁防护机制

针对上文分析的 DDoS 攻击威胁,NF 服务生产者应对来自同一个令牌的 RESTful API 请求频率做出相应的限制,可以根据 RESTful API 所占用资源的不同进行等级划分,对占用资源高的 RESTful API 请求频率设定更严格的阈值,对资源占用低的 RESTful API 请求频率设定较为宽松的阈值。若单位时间内来自同一个令牌的请求超过 RESTful API 请求频率阈值,则 NF 服务生产者使用 HTTP 状态码“429 Too Many Requests”作为响应且拒绝执行服务,如图 8 所示。此外,NRF 可加入防火墙机制,依据 NF 服务请求内容(例如恶意源 IP 地址、恶意 NF ID、未知 PLMN ID 等)划分出恶意 NF 服务消费者,过滤恶意 NF 服务消费者的请求,降低 NF 服务生产者 RESTful API 滥用风险。

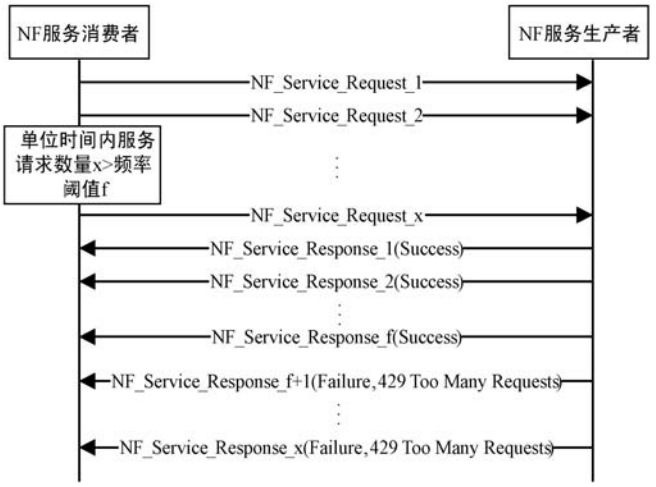

图 8 RESTful API 请求频率限制

3.2 JSON 安全威胁防护机制

针对上文分析的 JSON 安全威胁,5G 核心网 NF 应具备对第三方功能进行细粒度快速升级的能力,若有 JSON 漏洞被挖掘,则 5G 核心网应能够对所有使用 JSON 功能的 NF 进行快速升级,安装 JSON 漏洞补丁。此外,同一 PLMN 核心网内 NF 间 JSON 数据传输应使用 JWE[21] 进行保护,JWE 可以同时保护 JSON 数据的机密性和完整性,防止攻击者获取到用户的敏感数据,如图 9 所示。

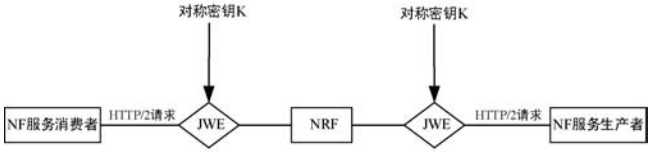

图 9 JSON 防护

3.3 中间人攻击威胁防护机制

针对上文分析的中间人攻击威胁,即攻击者获取到 NRF 发送至 NF 服务消费者的访问令牌,从而携带访问令牌使用 NF 服务生产者的服务。提出一种改进访问令牌的安全机制,如图 10 所示。NF 服务消费者请求访问令牌之前,生成随机数 R 并使用散列算法计算随机数的散列值 H,将 H 与散列算法名称 $\text{Hash}_{\text{name}}$ 连同访问令牌请求一同发送至 NRF。NRF 对 NF 服务消费者鉴权成功后,将散列值 H 与散列算法名称 $\text{Hash}_{\text{name}}$ 放入访问令牌中发送至 NF 服务消费者,当 NF 服务消费者向 NF 服务生产者请求服务时,将随机数 R 与访问令牌一同发送至 NF 生产者,NF 服务生产者成功验证访问令牌完整性后,将散列值 H 与散列算法名称 $\text{Hash}_{\text{name}}$ 取出,使用相同散列算法计算 R 的散列值 H',若散列值 H' 与 H 相同,则允许 NF 服务消费者使用服务,并将服务响应返回至 NF 服务消费者,否则拒绝提供服务。

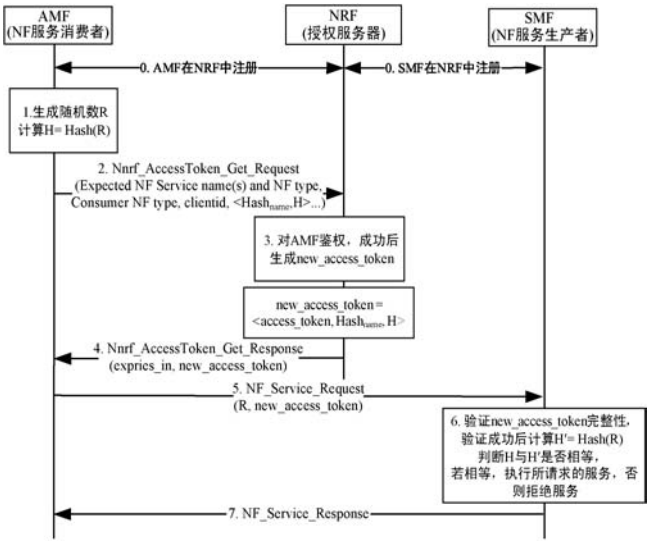

图 10 改进访问令牌

通过改进令牌的安全机制,攻击者即使获取到 NRF 向 NF 服务消费者下发的访问令牌,由于无法获知 NF 服务消费者生成的随机数 R,故无法使用 NF 服务生产者的服务。

3.4 注入攻击威胁防护机制

针对上文分析的注入攻击威胁,NF 服务生产者验证 NF 服务消费者访问令牌完整性的同时,应严格检查 NF 服务消费者请求 RESTful API 中输入参数是否与令牌保持一致或者是否存在安全威胁。例如检查 NF 服务消费者请求 RESTful API 访问资源的权限是否在令牌所规定权限之内,验证 RESTful API 输入的参数数量、类型、长度、数值是否在 NF 服务生产者所允许范围之内。若 NF 服务消费者请求的访问权限超过了访问令牌权限范围或 NF 服务消费者输入参数越界,则 NF 服务生产者应拒绝 NF 服务消费者的服务请求并返回错误消息,如图 11 所示。

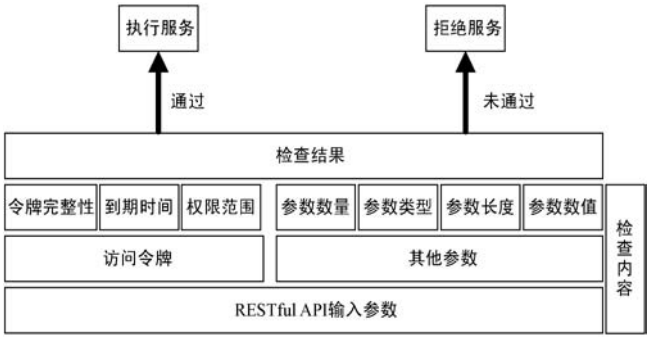

图 11 RESTful API 检查机制

4 结 语

5G 网络将内生安全作为重要的设计理念之一,因此 5G 网络在设计之初必须全面考虑可能存在的安全

威胁。针对 RESTful API 在 5G 应用场景中相关安全研究较少的不足,本文在梳理 5G 网络服务化架构与 RESTful API 应用方法的基础上,分析了 5G 网络 RESTful API 的 4 种主要安全威胁,包括 DDOS 攻击威胁、JSON 安全威胁、中间人攻击威胁和注入攻击威胁,并提出了相应的安全防护机制,为 5G 网络的发展完善提供了参考。未来将会针对 5G 服务化架构相关协议和应用场景安全做进一步研究。

参 考 文 献

[1] Series M. IMT Vision-Framework and overall objectives of the future development of IMT for 2020 and beyond [EB/OL]. [2023 - 01 - 11]. http://www. itu. int/rec/R-REC-M. 2083.

[2] Andrews J G, Buzzi S, Choi W, et al. What will 5G be? [J]. IEEE Journal on selected areas in communications, 2014, 32(6): 1065 - 1082.

[3] Ji X, Huang K, Jin L, et al. Overview of 5G security technology[J]. Science China Information Sciences, 2018, 61(8): 081301.

[4] 3GPP. Principles and guidelines for services definition:3GPP TS 29. 501[S].

[5] Mayer G. RESTful APIs for the 5G service based architecture[J]. Journal of ICT Standardization,2018,6(1):101 - 116.

[6] Fielding R T, Taylor R N. Architectural styles and the design of network-based software architectures[M]. Irvine: University of California, 2000.

[7] Lee S, Jo J Y, Kim Y. Method for secure RESTful web service[C]//2015 IEEE/ACIS 14th International Conference on Computer and Information Science(ICIS). IEEE, 2015: 77 - 81.

[8] Serme G, de Oliveira A S, Massiera J, et al. Enabling message security for RESTful services[C]//2012 IEEE 19th International Conference on Web Services. IEEE,2012:114 - 121.

[9] Huang X W, Hsieh C Y, Wu C H, et al. A token-based user authentication mechanism for data exchange in RESTful API[C]//2015 18th International Conference on Network-Based Information Systems. IEEE, 2015: 601 - 606.

[10] Woo S, Lee S, Kim J, et al. Re-checker: Towards secure restful service in software-defined networking [C]//2018 IEEE Conference on Network Function Virtualization and Software Defined Networks(NFV-SDN). IEEE,2018:1 - 5.

[11] Garg H, Dave M. Securing IoT devices and securelyconnecting the dots using rest API and middleware[C]//2019 4th International Conference on Internet of Things: Smart Innovation and Usages(IoT-SIU). IEEE, 2019: 1 - 6.

[12] 3GPP. System architecture for the 5G System(5GS):3GPP TS 23. 501[S].

[13] 3GPP. Technical realization of service based architecture: 3GPP TS 29. 500[S].

[14] 聂衡,赵慧玲,毛聪杰.5G 核心网关键技术研究[J]. 移动通信,2019,43(1):2 - 6.

[15] Hardt D. IETF RFC 6749: The OAuth 2. 0 Authorization Framework[EB/OL]. [2023 - 01 - 11]. https://datatracker. ietf. org/doc/html/rfc6749.

[16] 3GPP. Security architecture and procedures for 5G system [S]. 3GPP TS33. 501,2019.

[17] 陈飞,毕小红,王晶晶,等. DDoS 攻击防御技术发展综述[J]. 网络与信息安全学报,2017,3(10):16 - 24.

[18] Alwan Z S, Younis M F. Detection and prevention of SQL injection attack: A survey[J]. International Journal of Computer Science and Mobile Computing, 2017, 6(8): 5 - 17.

[19] Liu Y, Ning P, Reiter M K. False data injection attacks against state estimation in electric power grids [J]. ACM Transactions on Information and System Security(TISSEC), 2011, 14(1): 1 - 33.

[20] Jones M, Hildebrand J. JSON web encryption(JWE)[EB/OL]. [2023 - 01 - 11]. https://www. rfc-editor. org/rfc/pdfrfc/rfc7516. txt. pdf.

[21] Jones M, Bradley J, Sakimura N. JSON web signature (JWS)[EB/OL]. [2023 - 01 - 11]. https://www. rfc-editor. org/rfc/rfc7515.

[22] Hu X, Liu C, Liu S, et al. Signalling security analysis: Is HTTP/2 secure in 5G core network? [C]//2018 10th International Conference on Wireless Communications and Signal Processing(WCSP). IEEE, 2018: 1 - 6.

[23] Patni P, Iyer K, Sarode R, et al. Man-in-the-middle attack in HTTP/2[C]//2017 International Conference on Intelligent Computing and Control(I2C2). IEEE, 2017: 1 - 6.

(上接第 229 页)

[24] Duan S,Zhao H, Zhou J,et al. Syntax-aware transformer encoder for neural machine translation[C]//2019 International Conference on Asian Language Processing(IALP),2019.

[25] Zhang Z, Wu Y, Zhou J, et al. SG-Net: Syntax-guided machine reading comprehension[C]//Proceedings of the 34th AAAI Conference on Artificial Intelligence(AAAI 2020), 2020.

[26] 刘雄,张宇,张伟男,等. 基于依存句法分析的复合事实型问句分解方法[J]. 中文信息学报,2017(3):140 - 146.

[27] Vaswani A, Shazeer N, Parmar N, et al. Attention is all you need[C]//Proceedings of the 31st International Conference on Neural Information Processing Systems. ACM, 2017.