基于零信任架构的5G核心网安全改进研究

Research on Security Improvement of 5G Core Network Based on Zero Trust Architecture

刘建华(中兴通讯股份有限公司,江苏 南京 210012)
Liu Jianhua(ZTE Corporation,Nanjing 210012,China)

摘 要:
5G网络物理边界日益模糊和难以固化,以边界防护为中心的传统安全架构凸显出巨大局限性,无法做到安全能力按需部署、动态配置和有效防护。通过分析5G网络安全现状,给出了单包授权、网络功能信任评分等7个潜在方向作为5G核心网安全设计的零信任增强。研究表明,通过上述方法,把安全能力沉浸到5G网络每个节点,将有助于提高5G核心网的安全性。

关键词:
零信任;5G核心网;单包授权;信任评分
doi:10.12045/j.issn.1007-3043.2020.09.015
文章编号:1007-3043(2020)09-0075-04
中图分类号:TN915
文献标识码:A
开放科学(资源服务)标识码(OSID):

Abstract:
Aiming at the increasingly blurred and difficult-to-solidify physical boundaries of 5G networks, the traditional security architecture centered on border protection highlights huge limitations and cannot achieve security capabilities on-demand deployment, dynamic configuration, and effective protection. By analyzing the current status of 5G network security, seven potential directions such as single-package authorization and network function trust scoring, are given as the zero-trust enhancement directions in the 5G core network security design. Researches show that immersing security capabilities into each node of the 5G network through the above methods will help improve the security of the 5G core network.

Keywords:
Zero trust;5G core network;Single-package authorization;Trust score

引用格式:刘建华. 基于零信任架构的5G核心网安全改进研究[J]. 邮电设计技术,2020(9):75-78.

1 零信任安全架构

1.1 变化的安全边界

传统网络安全基于“边界防护”模型构建,企业关键数字资产位于内网中,默认内网比外网更安全,安全建设重点在于隔离内外网的防火墙等安全设备,以抵御来自外部的安全威胁。

云计算、5G垂直行业、边缘计算等多个场景中,数据资产位置动态变更、按需迁移,网络物理边界日益模糊,难以固化。以边界防护为中心的传统安全架构凸显出巨大局限性,无法做到安全能力按需部署、动态配置和有效防护。

安全实践需要新的安全方法论来指导,以保护云化基础架构,实现安全与行业应用的深度融合。零信任安全架构针对传统网络安全架构的局限性提出了新的解决思路。

1.2 核心理念

零信任网络(ZTN)安全架构由研究机构Forrester在2010年提出,其核心思想为“Never Trust, Always Verify”,即打破物理边界防护的局限性,不再默认信任物理安全边界内外部的任何用户、设备或者系统、应用,以身份认证作为核心,将认证和授权作为访问控制

收稿日期:2020-07-30

的基础。

零信任网络要求：无论用户和资源位置，都要确保所有资源访问的安全；记录和检查所有流量；执行最小权限原则。

1.3 发展与实践

Gartner将零信任列为Top 10安全技术之一，并预测2022年80%的开放应用会使用零信任产品；零信任架构也成为了分析机构、安全厂家和大型企业的安全研究热点。

a）CSA云安全联盟的软件定义边界（SDP）。SDP架构可以认为是实施零信任架构的最佳实践指导：对设备和用户进行强认证，对网络连接进行加密；执行最小特权原则，严格按照白名单模型进行访问控制。

b）美国NIST的零信任安全草案。2019年9月发布，认为零信任架构是一种端到端的网络安全体系。零信任架构提供了相关概念、思路和组件关系的集合，旨在消除在信息系统和服务中实施精准访问策略的不确定性。

c）Google BeyondCorp。BeyondCorp作为Google的安全访问平台，利用持续验证的思路，帮助员工访问内部资源。在该系统中，应用被分为若干可信任级别，设备信息和用户信息通过规则引擎验证和综合判定后确定可访问的内容。

d）Microsoft Azure。利用机器学习、实时评估引擎、组织策略等对用户、终端、位置和设备等进行综合判断，实现持续自适应地访问多个资源，Azure可以在cloud、SaaS等多个层面构建完整的零信任系统。

2 5G核心网安全从零开始

2.1 5GC安全概况

5G核心网相对之前的2G/3G/4G网络，对多种接入制式采用统一认证，服务化实体间支持双向认证；引入HTTP/2作为核心网控制面的互通协议，并通过OAuth和HTTPS等机制来实现授权与流量安全；NF之间通过NRF实现访问控制；提供了服务化网元的API接口规范。

2.1.1 双向认证

EAP-AKA'和5G-AKA 2种认证方案，可以实现用户和网络间的双向认证：用户5G卡集成了4G的双向鉴权特性，实现了卡对网络的认证，一定程度上防止黑客或者伪基站对用户的攻击；网络对用户进行认证，确保只有合法开户的终端才能够接入5G网络。

在5G核心网中，AUSF提供5G-AKA、EAP-AKA'认证方式；UDM为AUSF提供基础鉴权向量；UDR存储用户标识、鉴权认证数据等。5G鉴权过程增强了归属网的控制，防止拜访网中可能存在的欺诈。

服务化架构中，在服务提供方NF Producer和消费者NF consumer之间，NF同时支持客户端和服务端证书，和其他NF通信时可以互相验证对方身份，确保NF间通信安全。

2.1.2 流量安全

在5GC服务化架构中，TLS作为基本的安全协议为信令流量提供机密性、抗重放攻击和完整性保护。

在同一个PLMN内，NF间和NF与NRF间都可以根据需要启用TLS功能；如果部署了SCP，各NF/NRF和SCP间也可以按需启用TLS功能。

在不同PLMN间，通过部署SEPP来保障信令流量安全性，cSEPP和pSEPP间使用JWE和JWS机制保障流量安全传输；PLMN内的NF和SEPP间可启用TLS。

2.1.3 互访控制

NRF支持NF的注册登记、状态监测等，实现网络功能服务自动化管理、选择和可扩展。同时基于运营商配置策略，通过NRF可以控制NF间的互通策略。

例如当某2个NF不在同一个切片中时，NRF比较NASSI和NSI ID等信息进行授权判断，某个切片的NF consumer将无法获取另外一个切片内的NF访问权限。

2.1.4 API防护

在3GPP中，对每个NF可以对外提供的API接口都进行了详细规定，NF不会提供协议规定之外的API服务。

CAPIF被用来设计保证5G网络对外北向API的安全性，API调用者、CAPIF和服务API提供者之间都通过TLS来保障安全性，同时考虑了这些API的监控、记录和审计等安全功能。

2.2 零信任理念，拓展5G安全设计

5GC安全协议在设计时并没有刻意参考零信任架构，但实际上作为移动通信网安全架构，3GPP的安全设计和零信任存在一定的非严格映射关系。

a）身份认证：UDM/UDR存储终端的身份信息，提供终端接入网络时的IAM功能；NRF通过证书实现对NF身份的校验认证。

b）访问授权：NRF可以看作类似策略引擎，基于NF身份认证结果、运营商策略、网络切片等信息集中控制各NF间的互访关系，并通过OAuth 2.0完成服务

授权。

c）流量安全性：TLS广泛应用于PLMN内各NF间、运营商互通等场景，提供控制面流量的安全防护。

d）最小服务集：NF/NRF等5GC网元仅针对规定的API提供服务。

根据零信任架构的核心观点，5GC内外网的安全威胁级别是一致的：5G会广泛应用于工业互联网、物联网等业务场景，部署环境复杂；在多个厂家互操作、某些NF在不安全环境部署、安全协议实现理解有差异、特定情况下NF被恶意感染等多个特殊场景中，信任域内的5G NF也一样面临风险。因此可以使用零信任架构的设计理念对5G安全协议进一步增强。

2.2.1 单包授权机制

CSA SDP架构采用单包授权机制（SPA）来提供启动通信安全防护，服务提供方的端口号在SPA授权之前不对请求方开启任何服务，强制要求先认证后连接。SPA优点是可以做到服务隐藏和按需开启，减小攻击面，同时有助于抵御DDoS攻击。

NF Consumer在正式发起TLS通信前，可以向策略服务器（可以是NRF等）发送SPA预认证报文，NRF通知NF Producer为该Consumer打开对应的定制安全规则，允许该NF Consumer作为客户端进行连接，该安全规则可以基于IPtable等状态防火墙机制实现，在SPA完成之前，NF Producer上防火墙规则默认为All Deny。这样的预认证实现了防火墙规则的动态开关，避免了知名端口的滥用。SPA机制可以作为5GC TLS的增强而非替代。

2.2.2 异常流量监控

获取和分析网络流量是迈向零信任架构的第1步，通过非侵入式的长期记录和分析网络流量，可以进行流量分类、感知通信模式变化和分析可能的攻击模式。该功能在IT中广泛使用，例如在AWS Web服务中的网络流量日志记录功能可以帮助管理员了解和分析数据包流量。

5GC在HTTPS加密流量情况下，也要提供对应的流量监控功能：在Indirect模式下，SCP作为HTTPS的转发节点，可以提供对应的流量监控、异常告警、日志记录和安全审计功能，并通过API方式提供服务，供管理节点查询或连接安全态势感知系统；在Direct模式下，各NF/NRF要具备类似的功能并以API方式提供这些安全能力。

例如当一个Access Token被多个NF使用、向同一个NF发起多个连接时，该目标NF应该进行告警，告知管理员该Access Token可能已泄露和发生了中间人攻击。

2.2.3 API安全防护

API作为网络攻击的一个典型载体，存在安全风险。一些重大API攻击在IT领域也经常发生，恶意攻击者可以利用系统弱点篡改API参数、实现Cookie篡改、注入恶意内容、发送无效参数以浪费服务器资源，造成业务中断。

5GC能力均通过RESTFul API方式对外提供，除了在开发API时要遵守业界最佳开发实践外，也需要嵌入对应的API防护功能。按照层次化纵深防御理念，Indirect通信下的SCP和NF2个层级、Direct下的各NF都要具备相应的API防护能力：实现API安全策略的预设，可以监视、分析和限制API的调用，发生API异常调用时进行告警。

2.2.4 网络功能评分

在零信任网络中，访问控制策略和信任应该是动态变化的，可以基于设备、用户和环境的多源环境数据计算出来。零信任网络建议持续监控参与者的网络活动，并持续更新其信任评分，将此评分作为授权策略判定的依据。这种模糊性的度量机制考虑了用户网络行为的变化，可以用于防御未知威胁。

5GC在提供对应服务时，应考虑引入类似的评分机制，以防止对端NF加载完成并通过可信验证后的网络攻击行为，该攻击行为可能是在NF运行期间被攻击者渗入植入恶意软件，也可能是软件设计不严谨导致的漏洞。NF根据对端NF的运行时间、流量和网络行为逐渐积累其信任积分，并根据攻击类型的严重等级扣减积分，这样既避免了偶尔突发异常造成的误判导致业务中断，也做到了攻击持续发生时的恶意NF隔离。

2.2.5 主动授权撤销

授权验证是IT安全实践中验证用户信任等级的常见手段。零信任架构中控制平面可以依赖授权验证来对数据平面进行有效干预，当信任等级波动时，可以更改授权判定，及时撤销授权。

在RFC 7009中定义了OAuth 2.0中的Token撤销机制，允许客户端向授权服务器发起Token撤销请求，通知服务器端对应的Token不再有效，从而阻止未到生命周期的Token被滥用的可能性。

5GC的SBA采用OAuth 2.0作为认证和授权的机

制。当SIEM或者其他安全等控制面系统判定某个NF为恶意/被攻击NF需要被隔离时，需要NRF具备主动撤销恶意/被攻击NF Token的能力，在对应Token生命周期到之前取消该NF的访问能力。

当前5G安全协议尚不具备类似的授权撤销机制，可以考虑作为后续的安全优化方向。

2.2.6 数据面防护

零信任网络默认所有网络实体间都不具备信任关系，因此要提供流量安全机制确保资源访问安全。在5G网络中，用户面的加密和完保机制可能不是默认开启的，需要核心网进行策略指示；随着UPF的下沉部署，UPF到DN网络间的流量也需要进行安全防护。

在关键垂直行业应用中，针对关键网络切片，核心网应设置策略指示空口数据强制启用加密和完保，以确保空口媒体面流量安全；UPF也需要根据切片和自身环境部署的安全态势，内置安全功能，通过防火墙为用户提供状态安全过滤，利用IPSEC功能建立到DN网络的安全隧道以提供设备间的全流量安全传输。

3GPP安全协议规定了通过SEPP为PLMN间的控制面流量提供安全防护；对于媒体面数据，如果采用回归属地策略，这些媒体面数据也要提供安全防护以确保其安全传输。

2.2.7 持续性检测

零信任架构要求在认证授权后的整个安全过程中，进行持续安全检测，随时评估安全状况的变化。MITRE ATT&CK框架可以协助构建和改善安全检测和响应机制。

ATT&CK根据真实的观察数据描述和分类攻击行为，创建了一个网络攻击中使用的已知攻击战术/技术知识库并提供了相应的应用场景。防护方借此可以站在攻击者视角，重新审视自己的网络安全工具，评估现有的安全防护能力。

高级威胁防御方面，可以使用APT设备监控5GC的HTTPS流量、管理面流量和关键垂直行业的流量，如果发生高级威胁行为，则进行告警。ATT&CK有助于APT设备了解最新的攻击者战术思路和入侵技术新特征，开发新攻击检测方法和更新防控措施建议，提升APT的威胁检测能力；对照ATT&CK，APT设备可以检查自身对于业界主流攻击方式的覆盖程度。

安全防御能力方面，可以利用ATT&CK进行对抗演习，测试和验证防御方案是否生效。例如在试验网5GC中生成一个恶意NF对其他NF进行渗透和横向移动，检测5GC中安全手段有效性；基于虚拟化架构，加入恶意VM，对Hypervisor发起渗透攻击，并向其他VM进行横向移动，以实现防御手段检测的目的。防御者根据对抗结果有针对性地评估与改进防御手段。

2.3 其他

基于区块链智能合约来构建多方可信关系、利用基于身份的密码体制/无证书密码体系等新机制来减少对PKI的依赖等安全议题在业界都有热烈讨论，这些研究也可考虑用来加强5GC网络的安全性。

3 总结展望

以“Never Trust，Always Verify”为核心思想的零信任安全架构成为了业界研究热点，移动通信5G核心网安全架构也引入了基于HTTPS的SBA架构作为通信基础。针对当前5G核心网安全防护手段，借鉴零信任的基本理念及业界当前实践经验，将单包授权、网络功能信任评分等7个潜在方向作为5G核心网安全设计的增强改进方向。如何将安全能力沉浸到5GC中的每个节点，并实现细粒度安全控制和自适应安全评估与改进会是一个持续的安全研究课题。

参考文献：

[1] 埃文吉尔曼，道格巴斯. 零信任网络在不可信网络中构建安全系统[M]. 北京：人民邮电出版社，2019.

[2] Gartner. Market Guide for Zero Trust Network Access [EB/OL]. [2020-04-29]. https://www.gartner.com/doc/3912802.

[3] CSA大中华区SDP工作组. 软件定义边界(SDP)安全架构技术指南[EB/OL].[2020-04-29]. https://www.c-csa.cn/html/1549.html.

[4] NIST. Zero Trust Architecture (2nd Draft)[EB/OL].[2020-04-29]. https://csrc.nist.gov/publications/detail/sp/800-207/draft.

[5] 杨宁，刘梓溪，李婷婷. Kubernetes下零信任安全架构分析[EB/OL]. [2020-04-23]. https://www.kubernetes.org.cn/6356.html.

[6] 李鑫. Hyperledger Fabric技术内幕架构设计与实现原理[M]. 北京：机械工业出版社，2019.

[7] 程朝辉. 基于标准算法的高效无证书密码系统[EB/OL].[2020-04-09]. https://olymtech.net/news/business/2019-12-09-01.html.

作者简介：

刘建华，安全系统架构师，硕士，拥有CISSP证书，主要从事移动通信核心网的产品架构设计和产品安全治理工作。