



NFV 中虚拟化网络功能生命周期安全管理措施

苏坚,肖子玉

(中国移动通信集团设计院有限公司,北京 100080)

摘要:网络功能虚拟化的动态特性需要引入灵活可靠、能够实现自动化快速部署和资源弹性可扩展的嵌入式安全防护体系,要求安全技术和安全策略能够在 VNF 整个生命周期进行安全管理。描述了从 VNF 实例化、运行到退役的安全历程,并针对网络运营商需要在 VNF 生命周期关注的相应动态和静态安全策略进行分析探讨。

关键词: NFV; VNF; 生命周期; 安全管理

中图分类号: TP915.08

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016291

VNF lifecycle security management measures in NFV

SU Jian, XIAO Ziyu

China Mobile Group Design Institute Co., Ltd., Beijing 100080, China

Abstract: The dynamic feature of NFV demands that security technologies, policies, processes and practices were embedded in the genetic fabric of VNF. The VNF security management lifecycle represented the security processes spanning from VNF platform guidance, to VNF instantiation, operation and retirement. It was intended to represent a process view of VNF security and process guidance.

Key words: NFV, VNF, lifecycle, security management

1 引言

网络功能虚拟化(NFV)将网络服务与硬件设施解耦,网络服务能够以软件形式部署于通用硬件之上,为网络服务的设计、部署和管理带来更大的灵活性,不再受到专用设备或网络拓扑结构的限制。NFV 技术颠覆了传统电信封闭专用平台的思想,同时引入灵活的弹性资源管理理念。ETSI 提出的 NFV 技术架构主要由 3 个域构成: NFV 基础设施(NFV infrastructure, NFVI)、虚拟化网络功能(virtualized network function, VNF)和 NFV 管理与业务编排(management and orchestration, MANO)。其中, NFVI 构成基

础设施的硬件资源(服务器、存储、网络)及虚拟化实例, VNF 是网元功能的软件实现,运行于 NFVI 之上, NFVI 包括可用于计算、存储的网络硬件资源和相应的虚拟化资源,用来托管和连接虚拟功能,支持 VNF 的资源调用^[1]。NFV MANO 在 NFV 框架中集中了所有 NFV 相关的管理功能,实现对 NFVI 和 VNF 的管理,通过管理虚拟化的硬件/软件资源,实现包括网络业务编排功能在内的 VNF 生命周期管理。

VNF 是 NFV 根据租户的性能需求,通过动态地调整计算和存储资源,为不同租户创建的网络功能虚拟化实例,一个 VNF 是一个网络功能的虚拟化的实例,这些网络



功能可以共同形成一个网络服务,根据不同架构部署在一个或多个虚拟机上。NFV 的生命周期通过网络功能虚拟化实例进行描述^[2]。VNF 生命周期如图 1 所示。

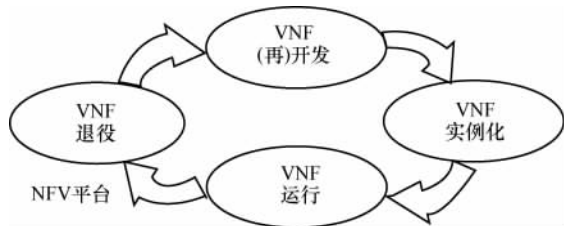


图 1 VNF 生命周期

NFV 生命周期描述从 VNF 实例化、运行到退役的全过程,NFV 的灵活部署极大提升了网络运维管理效率。同时,动态网络部署也为网络安全带来全新挑战。虚拟化网络的安全是一个过程而不是一个状态,安全管理将深度融合为网络管理的一部分,需要更加智能和灵活地进行分析、识别和响应。

作为一个基于软件的网络部署方案,NFV 最大的优势之一便是其实现运维流程自动化的能力,涵盖从部署到监控、伸缩、故障恢复、升级,直至退出整个 VNF 生命周期。研究表明,这种自动化能力将使得运营商在某些情况下能缩减超过 50% 的运维成本^[3]。然而传统的安全部署模式在管理性、伸缩性、业务快速升级等方面已无法满足 NFV 的安全要求,需要引入灵活可靠、能够实现自动化快速部署和资源弹性可扩展的嵌入式安全防护体系。网络运营商需要在 NFV 的全生命周期配置相应的静态和动态安全策略,进行入侵检测、安全评估、快速的威胁应对以及修复漏洞。图 2 描述来自 ETSI 的 NFV 安全管理过程。

2 NFV 安全威胁概述

除了传统网络架构中面对的安全风险,新架构的部署和新业务的引入还会带来新的风险。NFV 可能面临的典型安全威胁及应对措施包括以下方面。

- 外部攻击:与传统电信网络架构类似,NFV 同样面临着物理环境中存在的安全风险,如洪泛攻击、DDoS 攻击等,会导致网络或数据的可用性、私密性和完整性损失。对此可通过传统的防恶意软件、漏

洞屏蔽等解决方案在虚拟化环境中应用来保护应用程序和系统安全。

- 内部攻击:传统的网络安全设备如物理探针无法查看虚拟机内部通信,这些通信流量对标准的网络安全控制来说是不可见的,因而无法对它们进行监控或内嵌封堵。对此需要确保与创建 VNF 直接相关的资源,包括硬件平台、软件平台和服务平台的安全性,通过物理资源和虚拟资源、数据和控制分组的感知以防范来自虚拟机内部的攻击。
- 动态防护:NfV 中虚拟化网络功能从实例化、运行直到退役都处于动态的生命周期中,这使得管理员在配置静态的一致安全策略变得异常困难。对此,需要在网络部署的同时建立起全方位的解决方案,该方案不应局限于传统保护方式,而应该嵌入 NFV 的全生命周期,使 NFV 在更“危险”的网络环境中仍然确保“电信级”安全网络。

其中,内部攻击和动态防护是 NFV 带来的新的安全问题,因此,对于 NFV 平台以及整个 VNF 生命周期内有预见性的安全管理成为应对此类威胁的重要手段。NFV 平台能够方便地创建、移动和撤销 VNF。当需要新的服务的时候,可以创建新的 VNF 或者提取已有的 VNF 模板,然后根据需要进行设置。随着需求的增加,可以克隆 VNF 或动态地为 VNF 分配额外的资源;同样,随着需求的减少,可以撤销 VNF 的设置或动态地减少 VNF 当前的资源。VNF 的实例化(创建)、运行(移动)和退役(销毁)过程构成了 VNF 的生命周期。VNF 在生命周期的每一个步骤都会受到安全威胁。当开始创建新的 VNF 时,重要的是要保证 VNF 安全启动;当克隆虚拟机镜像和移动虚拟机的时候,重要的是动态过程管理保持新加入资源的安全性和运行中的 VNF 处于稳定状态;在 VNF 退役阶段,重要的是对于销毁 VNF 和防止闲置的 VNF 数据蔓延成为未知威胁的攻击目标。

3 NFV 平台安全措施

NFV 通过为不同租户创建不同的 VNF 以支持多租户,并且能够根据租户的性能需求,动态地调整分配给这些 VNF 计算和存储资源,实现租户 VNF 功能和性能的按



图 2 NFV 安全管理过程

需分配。作为创建 VNF 的平台, NFV 需要确保与创建 VNF 直接相关的资源, 包括硬件平台、软件平台和服务平台的安全性, 通过物理资源和虚拟资源、数据和控制分组的感知以防范来自虚拟机内部的攻击。

3.1 硬件资源和应用在虚拟环境中的感知

在 NFV 部署时, 需要周密规划物理和虚拟资源接口, 以确保虚拟机和 VNF 的工作负载具有适当的可见性。在“可虚拟第三代架构的规范化条件”中定义了虚拟化环境的 3 个特征: 对等、资源控制和效率。对等意味着一个运行于虚拟机管理器的程序, 其行为应与直接运行于等价物理机上的同程序的行为完全一致, 同一“虚拟化”环境中运行的应用程序不会互相干扰^[4]。对等保证了操作系统和虚拟机内执行的应用程序不会被同一虚拟机管理器主机上运行的其他虚拟机的程序以及运行这些程序的软硬件操作所干扰。为实现对等, 虚拟机管理器将分离虚拟机正在运行的硬件计算环境中的大部分物理和软件特性, 这些特性包括物理 BIOS 和虚拟机管理器的版本信息、物理组件的位置和排列(如 CPU、存储)以及各种虚拟化伪影(如主机到虚拟机物理地址转换信息)等。

虚拟抽象、私密性、安全性和外部管理等原因会限制工作负载在物理和虚拟运行环境中可见, 然而在现网场景中, 可信平台模块(TPM)或硬件安全模块(HSM)以及合法拦截等场景可能需要工作负载可见。因此, NFV 中 VNF 生命周期中应考虑物理资源和虚拟资源的负载呈现问题, 谨慎确定对工作负载提取或可见性的要求, 并明确可见规则和可见 API。此外, NFV 内部的 VNFC 虚拟化运行过程同样需要进行隐藏, 建议 NFV 部署应基于安全要求对虚拟机管理器和 NFVI 组件进行适当的安全隔离。

虚拟机自省(virtual machine introspection, VMI)技术通过在目标虚拟机外部获取虚拟机底层状态数据(CPU 寄存器、I/O 控制器寄存器、内存、大容量存储设备以及虚拟 BIOS 等), 可以在安全虚拟机中有效地监控或干预其内部运行状态。虚拟机管理器完全了解每个 guest OS 的当前状态, 同时与被监控系统相隔离^[5], 包括管理自省和进程自省在内的虚拟机管理器自省可导致保密性、完整性和可用性的风险。自省可以通过直接或间接的方法查看或修改与 NFV 相关的操作状态信息。获得操作状态信息可能导致任意读取或写入内存、存储、密钥库和其他 NFV 操作相关内容。虚拟机管理器管理模式使具有完全访问权限的系统资源管理员、超级用户等可查看并更改 NFV 中的私钥、对称

密钥、密码、系统配置、知识产权及其他资源。基于内省的更改和登录、日志和警报可以伪装恶意访问、意外修改、漏洞和管理失误。同样, 类似的特权进程也具有自省功能。由于管理和进程自省的使用允许不受限制的访问和修改, 使得 NFV 生态系统存在风险。

此外, 现有的虚拟机自省研究多数是在虚拟机管理器安全可靠的前提下开展的, 但是, 虚拟机管理器是管理资源分配的系统软件, 随着其功能的增多, 代码安全漏洞频繁出现。由于部分虚拟机自省技术的底层状态数据获取及传递等工作需借助虚拟机管理器才可以顺利完成, 因此应通过尽量简化虚拟机管理器的设计等方式增强虚拟机管理器的安全性, 使虚拟机自省技术可以稳定地发挥作用^[6]。

3.2 数据和控制分组在虚拟环境中的感知

为了实现终端用户智能, 需要能够关联用户平面和控制平面数据, 关联分析可以基于用户 IP 地址、IMSI 地址、用户设备、应用、位置、应用所消耗的带宽等有用信息。这些分析还可以帮助运营商跟踪网络使用、用户动态、发现网络异常, 例如在控制面或数据面的恶意软件和 DDoS 相关攻击。在非虚拟化环境中许多网元接口暴露, 因此传统的有源和无源探针可用于数据面和控制面中的监控、深度分组检测(DPI)的功能和关联分析。例如, 使用无源探针, 可以监控 VoLTE 控制消息, 如 EPC 和 SIP 的 GTP-C、S1-C, 跟踪端到端会话呼叫建立和终止等。这些探针同样还可以捕获用户面的数据分组进行协议分析和深度数据分组分析, 如 GTP-U。在控制面和数据面消息的帮助下, 这些探针不仅可以提供网络和用户 KPI, 还能够帮助定位影响到移动用户、移动承载的安全冲击。

然而, 在 NFV 环境中, 这些接口或者被经过组装的垂直“功能竖井”所隐藏, 或者由同一虚拟机内部或不同虚拟机之间堆叠成栈(例如不通过 IP 接口, 而是通过虚拟 socket 连接), 从而难以通过物理探针来探测所需数据。在某些情况下, 设备商尝试通过非 3GPP 标准优化某些接口的处理功耗和减少信令时延。因此, 此类情况下采集数据需要新的解决方案。

虚拟探针(vTap)和前端处理器可以有多种形式, 虚拟前端(vFEP)的部署方案取决于 VNF 在网络中的部署方式。宏观来看, 虚拟探针的选择性过滤和转发功能需要作为服务链的一部分在 NFV 服务编排时考虑, 因此当 NFV 根据 scale-out/scale-in 改变模块或扩展/暂停时, 虚拟探针都需要部署在合适的位置。下面几个用例场景描述了虚拟



探针如何在这些场景中使用。

在一种部署场景中,一个NFV运行在一个或多个专用刀片上,类似于虚拟私有云。在这个场景中,所有的NFV内部通信通过交换机结构完成。例如,多个VNF既可以运行在不同的刀片上,也可以运行在相同的刀片上。虚拟探针可以选择过滤流数据并且将数据复制到另一个作为虚拟前端运行的虚拟机,完成第一层选择过滤功能。虚拟前端形成第二层数据采集,完成采集器/协议优化工具/预处理器/聚合器前端任务。虚拟前端可以是单独的虚拟机,也可以是根据性能/处理能力的要求分布于不同机箱中的多个虚拟机。

在第二种部署场景中,不使用3GPP定义的协议作为VNF之间的通信,而是使用设备商私有协议或内存共享(shared memory)协议或本地数据库来优化VNF间通信。只有当这些系统需要与其他设备商的设备进行互操作时,系统才会使用标准接口。例如,一些虚拟EPC厂商在MME和HSS通信时使用非标准接口而不是基于DIAMETER的S6a接口,但在与外部HSS通信时,这些MME使用标准的Diameter协议,使用优化的协议可以减少信令开销。在这些场景中,通过使用普通的虚拟探针采集数据分组来分析和检测网络中的特定异常十分困难。在这种情况下,设备商需要向虚拟前端提供设备的API完成3GPP标准化协议的转换或通过网元管理系统(EMS),或通过其他方式提供虚拟前端所需的元数据(meta data),通过执行推/拉(push/pull)机制或订阅/通知机制可以将相关的控制和数据信息送至虚拟前端。

4 VNF实例化阶段的安全措施

4.1 措施一:安全启动

VNF安全启动依赖于本地认证、远程认证、属性、真实性、配置管理、证书、密钥、数字签名、特定硬件功能等多重保障,安全启动过程需要确认硬件、固件、虚拟机管理器和操作系统的有效性。

VNF安全启动是NFV特有的安全和信任机制,类似于微软定义的预启动加载机制UEFI,默认情况下,UEFI固件只会加载那些被签名的引导程序,这个功能被称为安全引导(secure boot)或可信引导(trusted boot),在缺少安全引导功能的传统PC机上,恶意的后门程序可以加载自身,进而伪装成一个引导程序,BIOS就会在启动的时候加载后门程序,这样它就可以躲过操作系统。安全引导只会

引导受信程序,拒绝引导那些未被UEFI密钥签名的操作系统,这是针对特定问题的具体解决方案。微软公司的安全引导与NFV并无特别关联,NFV旨在保护初始化的相关方法称为安全引导。NFV所要面对的主要问题是共享基础设施(包括虚拟机管理器)的VNF在编排过程中的特定需求,例如基础设施的独享或分享、anti-affinity功能(保持虚拟机互相独立)。

VNF安全启动可以确保VNFC的启动过程完全处于可测的安全路径。在VNF中,VNFC启动过程的安全路径保障需要由基础设施层延伸至虚拟机管理器层。在VNF环境下,安全的启动步骤依次为:硬件、虚拟机管理器和平台、VNFC虚拟化容器、VNFC操作系统、VNFC应用、用于VNFC的部署状态。而在实际操作中,由于启动可能产生预期之外的结果,因此并非绝对安全。对于无法确保安全启动的情况,可以预配置如下处理策略:

- 拒绝开机;
- 允许启动,但减少权限;
- 允许引导,但限制对其他实体、网络的访问;
- 允许引导,同时标记为需进一步调查。

4.2 措施二:身份认证

NFV的引入在涉及AAA平台认证时带来新的安全问题,使用当前身份和记账的实体至少分布在两个层面——网络基础设施(识别租客)和网络功能(识别实际用户)。在端到端虚拟网络架构中(如VNFAaaS、VNPaaS等),身份堆叠可以在多个层发生,任何类型的横向和纵向组合(集成)模式,都需要解决与身份相关的问题。基本的AAA架构利用特定的租客基础设施识别一般租客身份或在虚拟网络中代表用户的租客身份,当前AAA机制假设没有唯一的ID、唯一的决策和执行点、唯一的策略级别和唯一的记账基础设施,为了在不影响某些NFV增强能力(如伸缩性、灵活性和回弹性)的情况下实现AAA认证,就必须利用严格的隧道分离。因此,认证、授权和计费可能存在以下风险:

- 在认证过程中,即使不打算调用某些身份属性,用户的相关隐私信息也面临暴露的风险;
- 在某个特定层级将不可验证的无关ID打包导致授权风险(权限扩大漏洞);
- 需同时按使用基础设施的虚拟化应用和网络租户的粒度要求在基础设施层所有计费点执行计费。

为了解决认证中的隐私问题,生成、生效和交换ID令

牌的机制需要在多层多租户环境验证用户的属性。涉及属性交换的授权过程需要可用的策略路由和构造方法,该方法不仅适用于用户和租户,亦需适用于 VNF 部署单元。属性交换要求目前的云 AuthN/AuthZ 技术(如 keystone 梯形校正)和网络技术(主要是基于 RADIUS 和 Diameter)构造一致。属性交换可以借鉴云计算中的联合身份的方案。联合身份意味着将一个人的电子身份、属性以及个人信息进行打包,然后将其存储在多个身份管理系统中。联合身份是一个跨多个身份管理系统存储用户信息的虚拟集合。身份联合的最终目的在于使一个域的用户能够更为安全、简便地访问另一个域中的数据或系统,且无须多余的用户管理。这一目标要求所有涉及的系统使用相同的协议,以实现最大的互操作性^[6]。联合身份认证过程如图 3 所示。

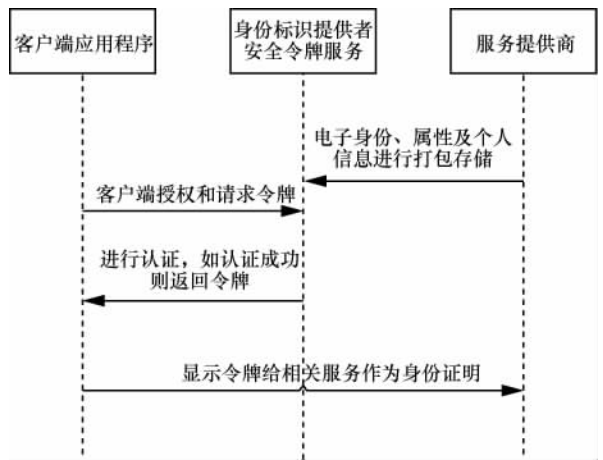


图 3 联合身份认证过程

4.3 措施三:可信计算

虚拟化的可信平台模块 (vTPM) 是可信平台模块 (TPM) 虚拟化解决方案之一,它使得在虚拟化环境里每一个虚拟机都能获得完整的可信计算功能。当使用物理 TPM 受限时,亟需虚拟化 TPM 对测量、证书和机密进行安全存储。

在 NFV 建构中,在物理硬件层之上运行虚拟机管理器,负责抽象底层的硬件资源并为上层的虚拟机提供虚拟资源,包括计算、存储资源等。管理员可通过最先创建的虚拟机进程管理用户虚拟机,包括创建、关闭、迁移等,同时具有访问物理 I/O 的权限,并同客户虚拟机进行交互。客户虚拟机被创建时由管理员使用配置程序与最先创建的(管理)虚拟机直接对话。

根据 Xen 的 vTPM 架构,vTPM 的完整功能由 vTPM 管

理者与 vTPM 实例协同完成,每一个 vTPM 实例都支持 TPM1.2 标准,并有独立的 EK,需要可信计算能力的虚拟机必须与一个独立的 vTPM 实例相关联。通过服务器端 TPM 驱动给每条 TPM 命令包上添加 4 bit 的 vTPM 实例标识的手段使得用户虚拟机与 vTPM 一一对应,这样客户虚拟机无法通过伪造命令包来与 vTPM 进行通信。在客户虚拟机被休眠或被迁移时,与它关联的 vTPM 也一起被休眠或被迁移,这是为了能够保留已存在的完整性度量结果,避免了运行在一个新的环境下需要重新完整性度量的复杂性。因此这需要 vTPM 在转移时不能被修改或复制。vTPM 原型系统还设计了一种特权 vTPM 实例,它能够产生或管理子 vTPM 实例(子 vTPM 实例能够继承父 vTPM 的特殊权利),提供加解密,生成对称密钥,负责迁移 vTPM 的非对称密钥等功能,目的是迁移 vTPM 实例时能够加密 vTPM 实例的状态^[7]。图 4 描绘了将 vTPM 引入 NFV 的部署架构。

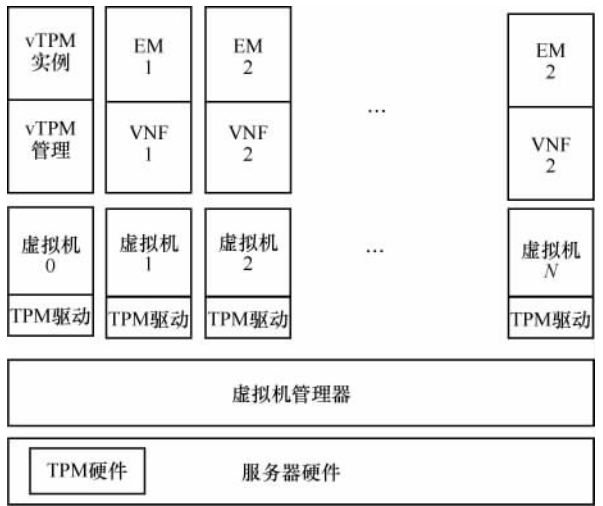


图 4 vTPM 引入 NFV 的部署架构

5 VNF 运行阶段的安全措施

VNF 生命周期事件包括 VNF/VNFC 愈合、VNFC 伸缩等,如果向一个运行中的 VNFC 加入新的资源,分配内存、解除分配、添加 LUN 卷以及任何底层基础设施的改变都需要 VNF 的基础设施操作,需要相关措施确保 VNF 安全运行。

5.1 措施一:控制和授权

实例化的 VNFC 虚拟机构成特定 VNF,虚拟机的最终控制由 MANO 及其相连的虚拟机管理器协同实现。在一



些 VNF 生命周期运行阶段,需要在移动、销毁、加入组件、主机升级等操作前通知相关 VNFC。针对 VNF 类型可以采用不同方案,例如,所有的控制通过主 VNFC 与 VNF 管理器通信,通过 VNF 管理器控制一组或特定的 VNFC,控制也可以由其他功能实体实现。

在所有这些方法中,基于角色的访问控制(RBAC)或基于属性的访问控制(ABAC)适用于大多数部署。基于属性的访问控制能够解决复杂系统中的细粒度访问控制和大规模用户动态扩展问题,基于角色的访问控制虽然没有实现动态分配权限和细粒度的访问控制,却可以通过“角色”建立起用户和资源的关系,极大简化权限的分配问题^[8]。对于两种访问控制方式,访问可根据基于密码证书的身份认证进行授权。操作的实际授权既可以通过用于 VNFC 信任链的实体(诸如 AAA 服务器),也可以向 VNFC 提供足够的信息使其作出关于授权的决策。

5.2 措施二:动态模式管理

动态模式管理包括信任方的网络准备和存储准备。在网络准备时,一旦 VNFC 设置可信的初始 root,该 VNF 便可以与这个可信的初始 root 联系并接受密钥,但作为可信的初始 root 的实体可能无法信任该 VNFC,需要通过 MANO 及其相连的虚拟机管理器实现协同,经过协同,该实体可以唯一地识别 VNFC,知道安全启动是否完成,控制可信的初始 root 和 VNFC 之间的所有通信,与证书和密钥提供者定义信任关系以确认身份和 VNFC 的信任,并且可以作为中间人,保证可信的初始 root 以及在整个生命周期动态的信任管理。同时,MANO 及其相连的虚拟机管理器协同控制特定 VNFC 访问的存储,而另一实体很可能也对同一存储写访问并提供密钥对,访问受保护的证书存储应受到严格控制。

在 VNF 运行阶段,崩溃的管理和恢复应该作为 VNF 动态模式管理的重要部分。错误的软件、硬件、配置、管理和电源事件将对 VNF 产生影响,甚至导致崩溃。VNF 崩溃事件将导致相关部件处于未知或意外状态并导致安全问题。需要事先进行编排应对可能发生的崩溃事件,可以预配置如下处理策略:

- (1)是否将崩溃恢复,并尽快还原可用性作为首要目标;
- (2)是否将收集信息分析崩溃事件作为首要目标;
- (3)如何在崩溃发生后安全保存私人信息(例如密钥和密码),随后进行报告和分析;

(4)根据崩溃是否涉及外部影响(例如 DoS 攻击),判断是否需要尽快缓解并恢复服务;

(5)事件信息是否涉及机密的硬件、虚拟机管理器、VNF、操作系统、应用程序和用户状态。

6 VNF 退役阶段的安全措施

VNF 退役主要包括 license 退役和可靠的数据清除。license 退役是指包括数字版权管理(DRM)的 license 从运行和暂停到 VNF 注销的过程。

VNF 退役的安全措施主要针对可靠的数据清除。有 3 种类型的内存或存储最有可能在 VNFC 退役后保留数据。

(1)虚拟机管理器平台上的 RAM。当一个虚拟机从一个虚拟机管理器删除、销毁或迁移,虚拟机管理器负责确保所有被释放的 RAM 由另一个虚拟机在重新使用前数据擦除,这是虚拟机管理器平台的标准功能。

(2)虚拟机管理器平台的“本地存储”。通常由于相关的性能问题 VNFC 应避免使用 SWAP 空间,如果使用则虚拟机管理器平台需确保它在由另一个虚拟机重新使用前擦拭干净;为保证更短的访问时间,应优选本地存储数据,虚拟机管理器平台同样需确保它在由另一个虚拟机重新使用前擦拭干净。

(3)远离虚拟机管理器平台的“远程存储”。由于远程存储可能用于经过迁移的虚拟机(单个虚拟机管理器只具有其本地的上下文信息)或用于不同 VNF 的长期存储数据,虚拟机管理器无法擦除或根本没有擦除远程存储的权限。在这种情况下,最佳方式是 VNFM 通过与 VIM 和其他 MANO 组件协商进行远程存储的数据清除。

以上 3 种典型存储的数据清除是基于虚拟机管理器具有直接访问本地存储的假设,如果部署穿越(pass-through)技术允许托管的虚拟机(和 VNFC)直接访问硬件或接口,则需优选用于远程存储的擦除技术。

在未配置或故障的情况下,需要人工进行数据擦除操作以确保 VNF 的安全退役。虽然 RAM 是临时性的,但在特殊情况下仍然有可能通过访问这些数据进行攻击,减少此类攻击最好通过对 NFV 基础设施的物理访问的限制。

7 结束语

由于 NFV 网络基于软件构建,在灵活部署和动态扩展的同时也给网络本身和其上加载的业务带来新的安全

挑战。安全问题是 NFV 部署提出的重要注意事项,软件比之前管理更多的网络功能,应该重新思考传统的保护机制并使之不断发展变化。NFV 是创造自动化网络的第一步^[9]。本质上 NFV 是一种循环部署的绿色网络,服务提供商需要围绕 NFV 中虚拟化网络功能生命周期完善安全管理策略,主动解决在实施过程中的安全问题,构建一种灵活的、透明的网络,既能满足更灵活的网络部署,提供更高效的网络服务,同时保证网络和信息的安全性。

参考文献:

- [1] 孙彪. 核心网虚拟化 NFV 技术在虚拟运营 MVNO 应用探讨[J]. 移动通信, 2016, 40(9): 9-12.
SUN B. Discussion on core network NFV technology application in MVNO[J]. Mobile Communications, 2016, 40(9): 9-12.
- [2] ETSI. Network functions virtualisation (NFV); NFV security; security and trust guidance: GS NFV-SEC 003(V1.1.1)[S]. 2014.
- [3] ANDREAS L. OpenStack 需要提升五个方面以支持 NFV [J]. 技术前沿, 2015(10).
ANDREAS L. To improve OpenStack to support NFV [J]. Technology Frontier, 2015(10).
- [4] POPEK G J, GOLDBERG R P. Formal requirements for virtualizable third generation architectures [J]. ACM Sigops Operating Systems Review, 1974, 17(7): 412-421.
- [5] 李保琿, 徐克付, 张鹏, 等. 虚拟机自省技术研究与应用进展[J]. 软件学报, 2016, 27(6): 1384-1401.
LI B H, XU K F, ZHANG P, et al. Research and application progress of virtual machine introspection technology[J]. Journal of Software, 2016, 27(6): 1384-1401.
- [6] 周君平, 孔德新, 付伟, 等. 云服务中跨安全域的联合身份认证技术分析[J]. 信息安全与通信保密, 2012(11): 89-90.
ZHOU J P, KONG D X, FU W, et al. Analysis of federation identity authentication across security domains in cloud service[J]. China Information Security, 2012(11): 89-90.
- [7] 王含章. 可信云计算平台模型的研究及其改进[D]. 合肥: 中国科学技术大学, 2011.
WANG H Z. Research and evolution on module of trust cloud computing platform[D]. Hefei: University of Science and Technology of China, 2011.
- [8] 何新新, 纪阳. 基于 RBAC 框架实现 ABAC [J]. 中国科技论文在线, 2013(10).
HE X X, JI Y. The achievement of ABAC based on the framework of RBAC [J]. China Science and Technology Papers Online, 2013(10).
- [9] DILIP P. Building a secure DNS architecture for NFV [J]. Lightreading, 2016.

[作者简介]



苏坚(1984-),男,中国移动通信集团设计院有限公司高级咨询设计师、工程师,主要研究方向为 5G 架构演进、移动核心网网络安全、SDN/NFV 安全 and 信息安全等。



肖子玉(1969-),女,中国移动通信集团设计院有限公司教授级高级工程师,中国通信学会高级会员,美国北卡罗来纳州立大学访问学者,主要研究方向为移动通信核心网、5G、NFV、IMS、网络安全和信息安全等。