



NFV 安全需求及应对策略

郭志斌¹, 陈扬帆², 刘露¹

(1. 中国联合网络通信有限公司研究院, 北京 100032;

2. 中国联合网络通信集团有限公司, 北京 100033)

摘要: 云计算技术的快速发展不仅带来了高速运算的便利, 也埋下了很多不安全因素。欧洲电信标准化协会 (European Telecommunications Standards Institute, ETSI) 指出虚拟化安全问题成为电信运营商和企业明年将面临的大问题。针对 NFV 架构中的安全技术进行研究, 指出安全对 NFV 技术的重要性, 分析管理支持设施的可用性及安全启动相关问题, 并总结了 NFV 的软件安全隐患, 通过不断完善 NFV 安全技术使得云计算环境可以更加安全有序地发展。

关键词: NFV; 安全; VFN

中图分类号: TP918.91

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016100

NFV security requirements and strategies

GUO Zhibin¹, CHEN Yangfan², LIU Lu¹

1. Research Institute, China United Network Communications Group Co., Ltd., Beijing 100032, China

2. China United Network Communications Co., Ltd., Beijing 100032, China

Abstract: Rapid development of cloud computing technology not only brings the convenience of high-speed computing, but also buries a lot of unsafe factors. European Telecommunications Standards Institute (ETSI) pointed out that the problem of virtualization security would become a major problem for telecom operators and enterprises in the next year. The NFV architecture security technology was researched, the importance of the safety was pointed out, the facilities of availability management and startup related safety problems were analyzed, and the NFV software security risks was summarized too. Through continuous improvement of NFV security technology makes cloud computing environment can be more secure and orderly development.

Key words: NFV, security, VFN

1 引言

传统的网络设备都是将网络功能与特定的硬件设备集成为专用网元。相比之下, NFV 就是在 x86 等通用硬件设备上运行的软件管理模块, 通过软硬件解耦及功能抽象, 利用虚拟化技术控制对硬件设备的访问, 使网络功能

不再依赖于硬件设备, 网络资源可以根据实际业务需求进行自动部署、弹性伸缩、故障隔离和灵活共享等, 从而降低网络昂贵的设备成本, 加快新业务的开发和部署。

虚拟化技术在电信运营商和企业领域已得到了广泛应用, 但欧洲电信标准化协会 (European Telecommunications Standards Institute, ETSI) 指出虚拟化安全问题 (主要指软件



定义网络(SDN)和网络功能虚拟化(NFV)将成为电信运营商和企业明年面临的大问题。ETSI同时表示,该问题或将成为电信运营商的新机遇,运营商可以通过敏捷的虚拟网络,实现数据整合及分析,从而更好地保护网络安全。ETSI召开专题专家讨论会议,指出当前NFV世界面临的安全挑战,并提出相关建议,同时也将成立NFV ISG(Network Functions Virtualization Industry Specification Group)安全工作组,该工作组由来自政府机构、厂商和运营商的专家组成,将更好地解决NFV面临的安全挑战

2 安全对NFV的重要性

NFV利用虚拟化技术,通过标准x86服务器运行防火墙、IPS(intrusion prevention system)等网络安全业务,让网络不再依赖于专用硬件,从而使云安全体系的安全业务能够“弹性扩展”、“快速交付”、“统一部署”,并解决传统安全部署时的“拓扑依赖”问题。下面对NFV架构中的安全威胁场景进行分析。

2.1 表面威胁

与已知的一般虚拟化威胁或网络威胁相比,表面威胁只关注针对NFV的特定威胁,如图1所示。通过适当的基础设施保护,NFV可以通过改善网络功能固有的安全属性真正提供安全保障。

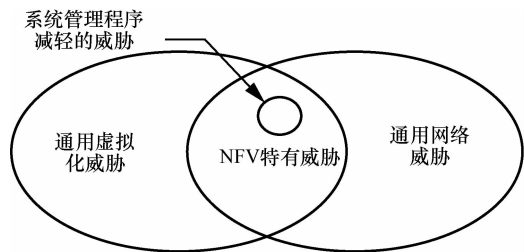


图1 NFV表面威胁的虚拟化

由于VNF(virtualized network function)只是一个运行在虚拟机上的网络功能,由VNF组成的网络的所有安全威胁包括:

- 所有一般虚拟化威胁(例如内存泄露、中断隔离);
- 在虚拟化之前的物理网络功能系统的特定威胁(如泛洪攻击、路由安全);
- 虚拟化技术与网络结合带来的新威胁。

考虑到虚拟化的主要安全优势:管理器(hypervisor)可以使用hypervisor自省和其他技术减轻甚至消除其他非虚拟网络功能的固有威胁。

因此NFV技术虽然由于虚拟化导致了新的威胁,但也迎来了新的机遇。通过确保NFV基础设施安全,尽可能地减小两个集合之间的交集,从而减少新的安全威胁,也可以运用适当的基于管理程序的安全技术,双管齐下提升NFV网络安全性。

2.2 攻击识别

识别攻击者主要通过攻击手段、攻击动机以及攻击时机。引入NFV对这些已存在的动机没有太大的影响,但确实改变了黑客利用漏洞的手段和时机,在某种程度上取决于攻击者在NFV供应链中与其他组织在技术和合约中的关系。因此,需要针对各类组织或个人按照合约等级进行NFV技术供应。NFV供应链中的主要元素包括终端客户、网络运营商、基础设施运营商、虚拟运营商和设备管理者等。

最初的攻击目的可能会局限于以下几类:

- 来自更高层面的攻击,如终端客户攻击其网络运营商或其他运营商;
- 来自相同层面的攻击,如网络运营商通过共享基础设施以获取竞争对手的信息,或者终端客户滥用其网络服务来攻击另一个终端客户;
- 来自内部攻击,例如网络运营商内部心怀不满的员工。

NFV环境中也存在知识产权相关威胁。不同的NFV功能提供商希望保护运行的专有算法、图像、配置文件和签名。为了保护运行在同一个平台的各个供应商的知识产权,需要减少逆向工程和边际信道攻击。

为了让从机更加信任主机服务,可以利用现有技术使客户存储自己信任的密钥并且在主机电脑的防伪模块做有限处理。鉴于有限的内存、处理能力和I/O资源,从机的计算功能不可能隐瞒于主机。另一种方法是局部同态加密技术,使某些没有太多开销的特定功能得到扩展(例如从机可以要求主机服务通过加密数据搜索加密的搜索词,并且返回一个加密的结果。因此,即使是主机处理器也不能清楚地获取到这些数据)。从单一的特定功能扩展到任何功能,需要使用完全同态加密。

3 管理支持设施的可用性

不管是否使用NFV,带外管理基础设施要求能够远程管理任何大型计算或网络基础设施的部署。这将确保即使在计算或网络基础设施已经崩溃的情况下,访问管理仍然可用。否则,管理系统将无法远程重启故障应对服务,

包括修复坏掉的操作系统或加载认证密钥、操作系统许可密钥和其他基本配置。

理想地,MANO(management and orchestration)、处理刀片的管理端口、交换机和存储控制器应该在物理上独立连接到其配置状态。本地访问配置状态的存储/缓存以及对这些基本但至关重要的资源的必要访问控制也是如此。无论是否使用 NFV,上述要求同样适用于日常日志数据的通信信道和管理系统以及需要管理员远程手动诊断和解决的问题。否则配置错误的警报通知可能不会传达到管理系统,从而通知管理员。

不管是否使用 NFV,上述所有的可用性和安全性之间的权衡同样适用。然而,NFV 也带来了一些额外的挑战。作为一个系统管理程序启动时,它需要网络访问记录自己的配置,包括软件许可和安全密钥。问题是如果管理程序的网络连接是依赖于运行在管理程序顶层的网络功能,或者依赖于另一个管理程序,就有可能带来电源故障。如果允许管理器连接同一物理独立的管理网络去管理硬件,这样问题才会得到解决。当一个虚拟转发功能启动时,同样的问题也会出现。网络访问自己的配置可能依赖于第二个虚拟转发功能的连接,而第二个虚拟转发功能又取决于与第一个虚拟转发功能连接的配置。这样虚拟化进程访问物理上独立的管理网络会更不安全。传统应用程序虚拟化与网络功能虚拟化之间的重排顺序的依赖性如图 2 所示。

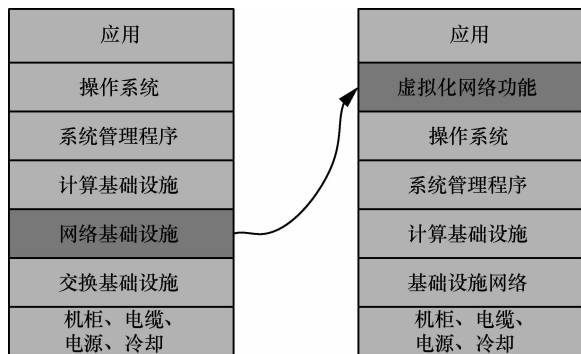


图 2 传统应用程序虚拟化(左)与网络功能虚拟化(右)之间的重排顺序的依赖性

4 NFV 的安全启动

在所有的主机部署场景中,特别是在用户侧,网络运营商必须充分信任其主机提供商的虚拟化平台,并在其上运行 VNF,平台也同样希望能够检测 VNF 是否真实。这就

是安全启动(secure boot)问题。

安全启动包括验证以及确保完整启动的技术和方法。启动完整性验证可以调用大量的认证因素,包括本地认证、远程认证、归属、真实性、配置管理、证书、密钥、数字签名和特定硬件特性。安全启动进程包括硬件(专用加速硬件以及通用进程)、固件程序、操作系统镜像以及安全凭据等保证因素。通过选择适当的因素保证所需的验证等级。

在初装和后续使用 VNF 时还有一个受关注的领域是 VNF 软件验证。这样的验证确保在认证和加载时,代码加载到真实的以及没有被篡改的 VNF 执行环境。虽然已建立的信任基础可以用来衡量 VNF 是否正常,然而这仍然是一个需要进一步研究和发展的领域。

安全启动技术可以防止根包和重置攻击,检测对 BIOS(和它的配置)未经授权的更改、启动顺序、hypervisor、操作系统及其配置。因此,基于硬件启动的已知配置是否可信可以确定主机启动是否正常。虽然目前市面上的服务器可以支持这项技术,但是至今仍未真正实现广泛应用。采用 UEFI(unified extensible firmware interface)架构的 UEFI 安全启动包括签名检测(如签署加密摘要)或者所有 UEFI 模块加载散列值。如果签名检测失败,那么就停止启动。也可以在管理员的控制下,通过控制台手动批准启动。

还有其他类型的安全问题会受到事故的影响,尤其是服务的可用性。一个 VNF 组件实例事故或者该实例与另一个实体之间的路由故障都会影响可用性。在这种情况下,VNF 管理者需要确定问题的可能原因,并且和 NFV 基础设施管理者合作去解决问题。这可能需要创建一个新的 VNF 组件实例(或一组实例),完成实体之间数据分组的重路由或实体之间新路由的创建。还可能重新配置 VNF 组件实例,或者重建 VNF 管理节点和其他实例之间的信任关系。在某些情况下,一个事故可能会对特定的 VNF 实例造成致命的影响。由此看出在某些情况下,VNF 管理者会联系其他实体采取行动。所需的识别这些行动的信息来自两组数据:VNF 组件部署和配置策略;VNF 组件实例的运行状态。为了让 VNF 管理者识别出需要从事故中安全清理的操作,需要的信息不仅仅是发生事故之前和之后瞬间的状态,还有特定的组件是否需要清理操作、需要清理哪些操作以及清理的迫切性。这些 VNF 管理者提供的操作信息将由 VNF 描述符表示。



5 NFV 的软件安全隐患

常见的软件安全隐患有 3 种:设计漏洞、安装漏洞和配置漏洞。软件安全隐患可能存在于任何软件中,包括在定制硬件设备(称为非 NFV 之后)和 NFV 上编译等。

- 人们希望 VNF 可以在商用软件和硬件上运行。这使得攻击者和防御者联合起来,但目前尚不清楚这使系统更容易攻击还是更容易防护。考虑到攻击者只需要发现一个安全隐患,而防御者必须找到并修复所有安全隐患,故可知这种联合对防御者的帮助更大。事实上,许多漏洞检测已经实现自动化,并且添加到互联网上的新应用的第一位使用者通常不是人类,而是搜索机器人、恶意扫描和开发工具。
- NFV 采用云安全技术将个人虚拟应用分离。网络功能可以提供关键的网络基础设施,从攻击者的角度看,相比于个人虚拟应用,这是一个更具价值的目标。因此,在考虑虚拟技术适用于保护关键网络基础设施之前,需要对其进行重新评估。例如,攻击者利用底层商用虚拟基础软件的一个漏洞,将一个虚拟 BGP(border gateway protocol)路由器控制,可能会利用受害者的网络地址发送广播信息以占用网络流量。这可能会造成大范围的服务崩溃或严重的数据丢失。如果不攻击网络基础设施,这种攻击很难实施。一经确认,软件漏洞可以通过安全补丁修复,而硬件漏洞修复的代价更大。然而,安全补丁并不是万能的。

由于软件可以面市之后再进行特色拓展、漏洞修复和安全更新,其更新频率比硬件高很多。更短的软件更新周期使得每次 VNF 的更新或底层计算设备的更新不会为了测试安全漏洞而不计代价,所以需要定义安全软件更新程序。

6 结束语

目前,云技术针对与安全相关的漏洞已经有了一个强大而稳健的设计方案。NFV 看似没有增加新的功能,却显著改变了对潜在攻击的影响。建立自动化、虚拟化、可动态

弹性伸缩的云安全防护体系已经是大势所趋,伴随着 NFV 安全技术的不断发展,可以使得云计算环境可以更加安全有序地健康发展。

参考文献:

- [1] NFV whitepaper #1 [EB/OL].(2013-11-13)[2015-12-20]. http://portal.etsi.org/NFV/NFV_White_Paper.pdf.
- [2] NFV whitepaper #2 [EB/OL].(2013-11-13)[2015-12-20]. http://portal.etsi.org/NFV/NFV_White_Paper2.pdf.
- [3] ETSI GS NFV 001 network functions virtualisation (NFV)[EB/OL].(2013-11-13)[2015-12-20]. http://docbox.etsi.org/ISG/NFV/Open/Published/gs_NFV001v010101p.pdf.
- [4] Xen home page [EB/OL]. (2014-03-20) [2015-12-20]. <http://www.xenproject.org/>.
- [5] KVM home page [EB/OL]. (2014-03-20)[2015-12-20]. http://www.linux-kvm.org/page/Main_Page.

[作者简介]



郭志斌(1981-),男,中国联合网络通信有限公司研究院云计算实验室标准组组长、工程师,主要研究方向为云计算管理、云服务市场规划和云计算标准化等。



陈扬帆(1975-),男,中国联合网络通信集团有限公司产品创新部副总经理,主要研究方向为运营商业务、运营商发展与互联网企业的关系等。



刘露(1984-),女,中国联合网络通信有限公司研究院工程师,主要研究方向为云计算服务质量管理及标准化等。