随着《网络安全法》的深度落地和等级保护进入2.0时代，网络安全得到了各单位的高度重视，防护水平有了显著提升，但我们仍要清楚地认识到网络安全面临的严峻挑战。做好网络安全工作，管理层面需要明确一把手责任制，由上而下全面推动，明确单位、部门和人员的安全职责，筹建安全管理和安全审计专职部门，形成基于安全责任主体且能以业务板块为考核单元的安全绩效机制，真正做到谁主管谁负责，谁运营谁负责。技术层面，在做好传统安全工作基础上，要重视云、大数据、移动互联网、物联网和工控等新技术应用的安全规划和防护，要培养网络安全人才，加速自主可控的网络安全技术研究和相关产品研发，同时融合各项先进技术和产品，不断优化网络安全应急管理和服务水平。

——北京中安国发信息技术研究院院长张胜生

基于虚拟化的电信云网络安全解决方案

方琰崴，陈亚权

（中兴通讯股份有限公司，江苏 南京 210012）

【摘　要】 针对NFVI、VNF、MANO等构成电信云网络的关键组件，提出了安全解决方案，介绍了安全启动和增强Hypervisor、数据安全、虚拟机生命周期、用户个人隐私保护、统一接入门户和控制节点认证、安全加固、日志集中审计和资源安全回收协同等关键技术，最后结合虚拟化电信云网络发展和国内运营商的网络特点，提出了安全部署的策略建议。

【关键词】 网络功能虚拟化；安全解决方案；安全部署策略

doi:10.3969/j.issn.1006-1010.2018.12.001　中图分类号：TN929.5　文献标志码：A　文章编号：1006-1010(2018)12-0001-07

引用格式：方琰崴,陈亚权. 基于虚拟化的电信云网络安全解决方案[J]. 移动通信, 2018,42(12): 1-7.

Security Solution to Cloud Core Network Based on NFV

FANG Yanwei, CHEN Yaquan

(ZTE Corporation, Nanjing 210012, China)

[Abstract] Based on the key technologies such as NFVI, VNF and MANO which constitutes telecommunication cloud networks, a security solution was proposed in this paper. Specifically, the key technologies such as safe start, enhanced Hypervisor, data security, virtualized machine life cycle, user privacy protection, unified access portal and control node authentication, security reinforcement, log centralized audit and resource safe recovery coordination were introduced. Finally, considering both the development of virtualized telecommunication cloud networks and the characteristics of domestic operators, the strategic suggestion on security deployment was presented.

[Key words] NFV; security solution; security deployment strategy

1　NFV电信云网络面临的安全挑战

随着M-ICT（Mobile Information and Communication Technology，移动信息通信技术）时代的到来，基于

收稿日期：2018-04-17

视频、虚拟现实、大数据以及万物互联的消费者体验产品越来越丰富，移动用户数和数据流量的快速增长，对网络设备的容量和性能提出了更高的要求。NFV（Network Function Virtualization，网络功能虚拟化）使软硬件解耦，即通过使用虚拟化技术，使得X86等通用硬件可以承载电信功能软件，维护也更加便利，从而大幅降低电信运营商的CAPEX（Capital Expenditure，资本支出）和OPEX（Operating Expense，维护支出）。NFV以运行在X86服务器上的网元功能软件化方式实现了软硬件解耦，以硬件资源池化的方式实现了资源共享，解决了电信网元烟囱式建设的难题。NFV作为一种先进的、颠覆性的技术，可以使电信运营商的网络架构更加开放，业务部署更佳灵活，但是在NFV架构下，为实现各层面的互操作性，NFV组件之间必须具备开放性，这将带来组件交互的开放性安全风险。和传统网络相比，NFV增加了MANO（Management and Orchestration，管理和编排）和Hypervisor（管理程序），新网元及虚拟化平台的引入也面临安全性方面的挑战。

在NFVI（Network Function Virtualization Infrastructure，网络功能虚拟化基础设施）中，由于VM（Virtual Machine，虚拟机）共享物理资源，存在资源竞争关系，同时也会存在安全边界缺失或者模糊化的问题。虚拟化软件采用开源软件，引入了安全风险。在VNF（Virtual Network Function，虚拟网络功能）网元中，由于网元功能软件化，软件面对DDoS（Distributed Denial of Service，分布式拒绝服务）攻击时，物理网元的处理性能更为有限。VNF在生命周期内会自动化创建、迁移、缩扩容、终止，VM在网络中的位置是流动的，增加了信息暴露的可能性。而MANO是NFV系统的大脑，是新引入的网元，如果安全应对不当将带来系统性风险。NFV架构中还引入了很多标准接口，比如VIM（Virtualized Infrastructure Management，虚拟化基础设施管理器）的API、MANO组件之间的互通接口，接口的开放会带来通信安全风险。

安全是电信网络的基本需求之一，必须采用有效的安全举措消除NFV系统中存在的安全风险，才能切实保障虚拟化电信云网络系统的安全运行。

2 NFV系统安全解决方案架构

在构建电信云网络之初，运营商需要基于ETSI NFV架构以全方位的视角审视NFV系统面临的安全威胁，构建无“安全盲区”的NFV系统，打造具有立体安全防护体系的NFV系统。

CSA（Cloud Security Alliance）是致力于云计算安全领域的国际权威组织，CSA发布了一系列云计算安全规范并形成了业界标准。电信运营商需要以CSA规范作为NFV产品安全方法论，按照业界最佳安全实践组建电信网络的各个组件。在NFV产品生命周期内，在各阶段建立云安全检查点，把通过云安全检查点作为该环节关闭的必要条件，否则禁止执行下一个环节。运营商必须从物理安全、NFVI安全、VNF安全、MANO安全和公用安全方面制定一系列的安全举措，形成如图1所示的NFV安全解决方案架构。

3 NFVI安全架构和关键技术

可靠的NFVI安全架构能够满足NFVI层面的安全增强需求，为NFV多租户网络提供SECaaS（Security as a Service，安全即服务）。电信运营商必须采用电信级操作系统作为NFV的Host OS，并针对云安全进行优化，在安全加固方面需要考虑采取多项关键技术。

3.1 NFVI组网安全

组网安全技术是保障网络安全的重要的手段之一，如图2所示，安全的组网部署可以实现VNF组件之间、基础设施及VNF业务之间的网络隔离。

（1）基础设施网络平面。基础设施网络分成云管理网络、存储网络、业务网络和带外管理网络，四类网络必须进行物理隔离。前三类网络在服务器上部署独立的物理网卡，接入到不同的Leaf交换机，机箱的带外管理口接入到带外管理交换机形成独立的带外管理网。

（2）基于SDN（Software Designed Network，软件定义网络）的网络安全业务链。利用SDN网络业务灵活编排的特性，根据用户安全需求设计安全业务模板，为NFV多租户安全地提供SECaaS能力。NFVO加载安全模板，系统自动执行模板定义的安全服务和

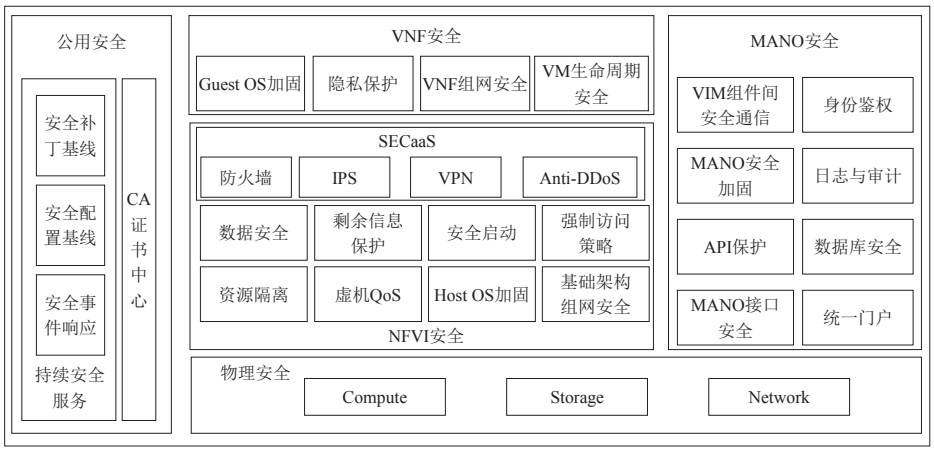

图1　NFV安全解决方案架构

安全策略，SDN控制器将租户流量引入到不同的安全服务中。

3.2 安全启动和增强的Hypervisor

TPM（Trusted Platform Module，可信平台模块）是一种基于硬件的安全启动方案，保证上电时BIOS、操作系统及应用程序的安全性。TPM采用密钥对，在服务器上加载的操作系统或者硬件驱动程序都必须通过公钥的认证，需要加载的软件必须用对应的私钥进行签名，否则服务器拒绝加载。电信云网络平台必须基于TPM实现安全启动可信根，提供从底层硬件至上层虚拟机应用的完整可信启动链条。各层次的TPM客户端从TPM服务器获取安全策略，Guest OS与Host OS应用软件分别根据相应安全策略经过内核可信度量之后向可信服务器进行安全确认，提供可信服务。为用户提供可信任认证机制，有助于发现、阻止非法应用的加载及访问，能够保证系统的安全。

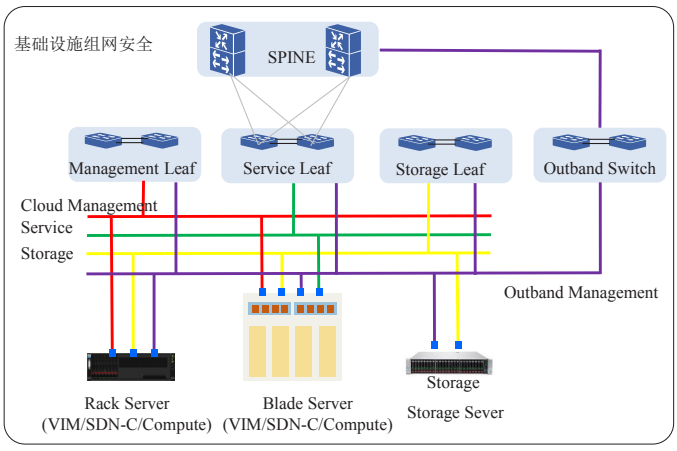

图2　NFVI安全组网架构

电信云网络中需要部署增强的Hypervisor安全特性，包括虚拟机之间资源的隔离和指令的隔离。云平台提供CPU隔离、内存隔离、网络隔离和存储隔离，保证虚拟机的资源独立及信息安全，并提供Guest/Host的指令空间隔离，防止某个虚拟机运行在高特权模式下威胁到另一个虚拟机的情况发生。

同时，电信云网络还需要对虚拟机VM进行一系列QoS保障，虚拟机的CPU、内存、网络I/O、存储I/O资源都设置上限、下限及优先级，既能开展普通业务，也能保证关键业务的运行。为了使虚拟机避免逃逸攻击的威胁，云平台提供了良好的虚拟机资源隔离机制，通过认证机制保证共享资源的组件是可信的。

3.3 数据安全

数据安全是信息安全的基石，运营商需要采取一系列举措确保用户的数据安全。

电信云网络平台提供密码管理功能，管理租户的密码生命周期和访问控制权限，账号密码需要符合复杂度管理要求，并使用MD5（Message Digest Algorith5，消息摘要算法第五版）进行加密保存。电信云网络平台在传输

用户密码时，使用HTTPS安全连接，防止用户密码在传输中泄露。

电信云网络平台必须具备存储加密功能，将虚拟机数据写入磁盘之前对其进行加密，保证用户数据的隐私性。块存储中的卷在挂载到主机上时对其进行加密，再将加密后的块设备提供给虚拟机使用。

如图3所示，数据存储加密业务流程可以分为六个步骤：

第一步：Nova为用户虚拟机申请存储卷挂载；

第二步：Cinder接收请求创建存储卷并挂载到物理主机；

第三步：物理主机通过安全通道向密钥管理服务器获取密钥；

第四步：利用密钥和卷加密器（提供加密算法）对存储进行加密；

第五步：将加密卷信息更新到VM的配置文件中；

第六步：将加密卷挂载给用户虚拟机使用。

电信运营商还需要部署镜像签名功能。这是因为虚机镜像在传输过程中可能会被篡改，修改过的镜像文件可能包含恶意代码，通过如图4所示的镜像签名和签名校验功能，用户在引导镜像之前可以验证该镜像是否被恶意修改。

4 VNF安全方案和关键技术

VNF是电信网元的功能逻辑实现，是NFV系统的

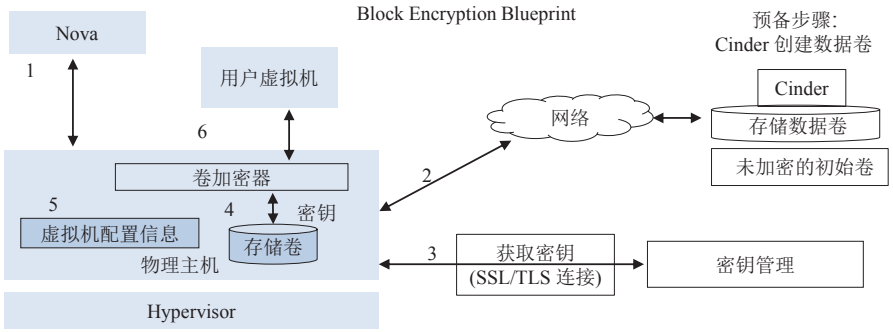

图3　数据存储加密业务流程

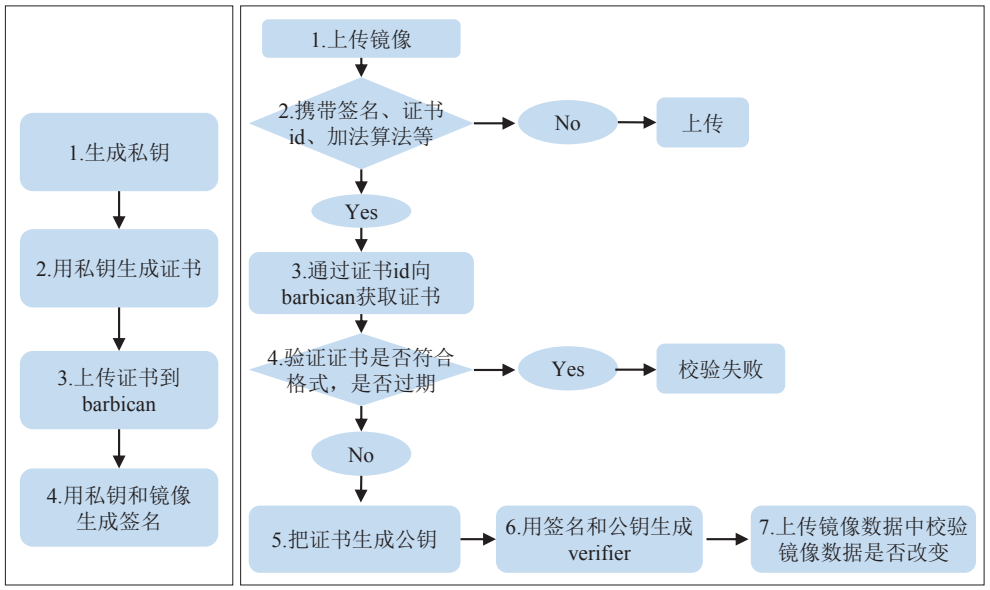

图4　镜像签名和签名校验功能

核心信息资产，其安全性至关重要，必须为VNF设计可信的安全方案，保证VNF整个生命周期及业务流程的安全性。

4.1 业务组网

业务组网安全能够简单有效地保障VNF的安全性，首先要考虑业务网络隔离。VNF网络包括VNF内部互通网络、VNF外部互通网络。内部互通网络细分成管理平面、控制平面及媒体平面；外部互通网络细分成信令互通网络平面、媒体互通网络平面、管理互通网络平面，如VNF有计费接口，还有计费互通网络平面。VNFC（Virtualised Network Function Component，虚拟化的网络功能模块组件）的每个互通网络平面都有一个专用的虚拟网口，通过vSwitch或者SR-IOV（Single Root I/O Virtualization，单根I/O虚拟化）连接到外部物理网络。

根据VNF的安全风险等级，将VNF划分成多个安全域，跨越安全域的VNF间互通流量需经过防火墙隔离，安全域内VNF之间的互通不需要经过防火墙。以虚拟化核心网为例，典型VNF安全域设置如表1所示：

表1　虚拟化核心网的VNF安全域设置

安全域	VNF	说明
安全暴露域	S-PGW/GGSN/ePDG、Gi DNS、SFC	直接面向Internet，安全风险最高
非暴露域	SGSN/MME、Gn/Gp DNS、UDC FE、PCRF、CS Core、IMS、RCS	不直接面向Internet，但有与域外其他VNF交互的需求，安全风险次之
敏感数据域	UDC BE、CG	存有敏感数据，安全等级高
管理域	NFVO、VNFM、EMS	NFV管理节点，安全等级高

4.2 虚拟机生命周期

完备的VM安全贯穿整个虚拟机的生命周期，体现在生命周期的各个阶段：在VNF模板中，NFV需采用数字签名及MD5等，支持NSD（Network Service Descriptor，网络服务描述符）、VNFD（Virtualized Network Function Descriptor，虚拟化网络功能描述符）在注册、加载、更新时的完整性验证和来源鉴权。通过VNF的安全需求，设计亲和、反亲和原则，限制携带敏感数据的VNF与具有外部访问接口的VNF共用物理服务器。而VM的镜像、快照必须存储在安全的路径下，采取存储加密功能，防止被非法授权访问后出现恶意篡改行为。VM镜像包应支持在注册、加载、更新时的完整性校验。在VM迁移过程中，为防止敏感信息泄露，VM的移动性应限制在特定的安全域内，不建议VM跨越安全域迁移。需要为VM移动性部署逻辑独立的承载网络，还可通过制作快照并加密的方式保护VM敏感信息。而当VM被终止后，VM原来占用的物理内存和存储资源可能会被重新分配给其他VM，这些资源必须被彻底清除。

4.3 个人隐私保护

完整的用户个人隐私保护解决方案如图5所示，可以采取两种匿名化的处理方式。

第一种是不可逆匿名处理方式。通过散列将包含隐私字段的文件、功能以散列后的结果显示。不可逆匿名化处理之后，个人隐私信息均不可读、不可逆，这有效地保护了个人隐私。这种匿名化方式常用于故障定位、性能统计、数据查询等，并不需要标识用户身份。

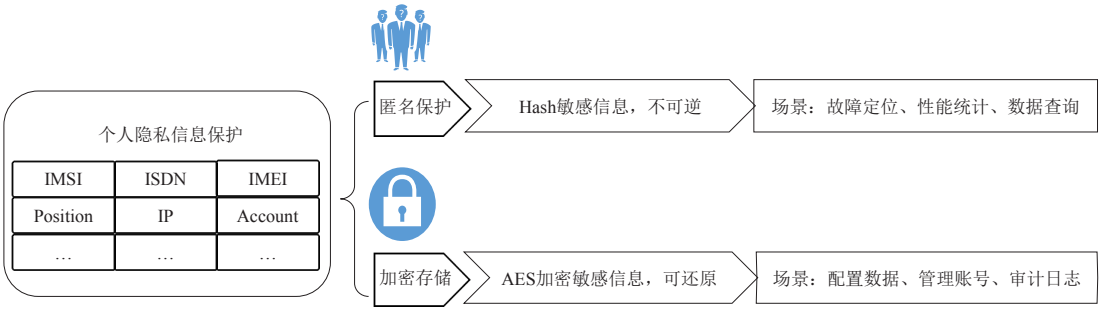

图5　用户个人隐私保护方案

第二种是可逆的匿名化方式。通过AES（Advanced Encryption Standard，高级加密标准）或其他加密算法进行匿名化，将包含个人隐私的字段、文件信息以公钥形式加密，以密文显示，授权人员可以用私钥解密后获取隐私信息。这种匿名化方式常用于数据配置、账号管理、日志审计等需要还原数据或可以回溯数据的功能。

5 MANO安全加固和关键技术

MANO是NFV的管控节点，电信运营商必须针对MANO制定安全解决方案，防范全局性系统安全风险。

5.1 统一接入门户和控制节点认证

为提高NFV的整体安全性，应实现NFV系统的统一认证、单点登录及日志操作。运营商有必要采用反向代理，提供集中账号管理，建立基于唯一身份标识的全局实名制管理。通过集中访问控制和细粒度的命令级授权策略，基于最小权限原则，实现集中有序的运维操作管理。通过集中安全审计，对用户从登录到退出的全程操作行为进行审计，监控用户对目标设备的所有敏感操作，聚焦关键事件，能够及时发现安全事件的预警。

云控制节点以多种方式认证用户，一旦认证成功，用户可以获取Openstack组件服务，以此来保证组件之间的接口调用安全，避免相关接口被非授权的人员调用。云控制节点对外提供服务的API接口均采用安全的数据传输协议。云控制节点的组件之间通信采用消息队列机制并承载在数据传输协议之上，保证通信的完整性和加密性。云控制节点必须对使用的数据库设置复杂的帐户及口令，记录数据库的操作日志，设置数据库安全白名单，拒绝匿名访问等。

5.2 NFVO、VNFM安全加固

在MANO内部，可以对NFVO（Network Function Virtualization Orchestrator，网络功能虚拟化编排）、VNFM（Virtual Network Function Manager，虚拟化网络功能管理器）进行多项安全加固。

（1）虚拟机安全：NFVO、VNFM基于虚拟机方式部署，以仅满足该服务器基本业务可正常运行为目的，对Guest OS进行最小化定制，限制操作系统开放的端口、访问权限和运行服务，实现可信赖的云安全管理节点。

（2）端到端安全：NFVO、VNFM验证操作员的权限，决定是否允许该操作员进行操作。NFVO、VNFM收到来自VNF的弹性请求时，验证请求方的身份，只允许处理来自合法身份的请求。

（3）接口交互安全：NFVO、VNFM与客户端通信采用SSH、SFTP及HTTPS等安全通信机制；NFVO、VNFM、VIM之间采用基于HTTPS的REST接口交互；VNFM与VNF之间采用基于HTTPS的REST接口或者SSH交互。

（4）镜像存储安全：NFVO、VNFM的镜像文件存储在安全的环境中。

5.3 日志集中审计和资源安全回收协同

集中采集及分析NFV系统中各节点的日志，运维人员能够实时了解系统的安全事件和运行状况。在日志采集和存储中，可以收集并存储NFV系统产生的操作类日志、安全类日志和系统类日志，全面记录系统运行状况。转储日志实现自动压缩和加密，减小日志存储空间并提供安全的存储机制。将旧的日志备份到指定的存储空间，以支持更长时间的日志存储和系统灾难性故障的快速恢复。在会话审计和分析中，可以按照日志级别、关键字等设置审计策略，对多个单设备的策略按照一定的逻辑关系组合为一个更加复杂的审计关联策略，并以会话为单位，通过条件查询进行定位，条件查询支持多种关键字组合。

当VNF组件崩溃或者VM迁移时，NFV系统确保待回收的资源不被非授权的应用或人员利用，因此VIM及VNFM要配合，对VM的资源进行安全回收，包括CPU、内存、网络和存储。VIM或VNFM发起与资源回收场景相关的操作，删除虚拟机、VM迁移或者重生，释放计算节点的CPU资源和RAM资源，更新控制节点可用CPU核数和RAM空间，并自动删除镜像文件，释放磁盘空间，更新控制节点可用磁盘空间，自动将VF网卡的MAC地址及VLAN重置，将其置为初始状态，最后擦除VM原有内存及存储。

6 电信云网络安全部署建议

运营商需要建立安全增强保障体系，并深入到日常运维工作中。

由于基于虚拟化NFV的电信云网络构建在数据中心上，而数据中心是电信云网络核心资产，电信运营商必须建立物理安保措施实现物理访问控制，建立准入、授权、监控、隔离、审计、演练等一系列规范化的安全制度。通过物理分区管理，设立运维区、测试区，设置完备的监控体系，严格限制对运维区的物理访问。建立物理安全应急预案和物理安全审计制度，定期输出物理安全审计报告，改进安全风险点。完备的管理是系统安全解决方案的根本。

电信云网络的NFV架构基于分层解耦架构的开放平台，NFV模型各组件之间至少有9个接口，一旦出现具有安全威胁的匿名接口调用，很有可能引发安全雪崩。因此，运营商运维团队需要部署CA（Certificate Authority）中心保证各个节点的身份可靠性。CA中心是管理、签发安全凭证和密钥的网络机构，CA可以向EMS/VNF/MANO以及Host主机颁发证书，拥有证书后，NFV系统的任何API调用均可保证其身份的有效性。VNF北向接口由于历史原因，使用鉴权授权方式进行身份认证，不需要使用证书来证明其身份。

在日常运营中，运营商的运营维护团队还可以利用漏洞扫描工具执行安全漏洞扫描，及时发现NFV系统是否存在CVE（Common Vulnerabilities & Exposures，公共漏洞和暴露）漏洞。在日常运营中，通过不断的安全累积更新，外部事件触发或内部定期扫描，才能够建立NFV系统安全漏洞加固基线并不断更新。同时，由于通用操作系统、数据库、中间件、虚拟化管理器，运营商的运营维护团队还可以利用配置核查工具，优化NFV各组件的配置项，形成NFV产品安全配置加固基线，有效地降低安全风险发生的概率。

在日常运营维护中，电信运营商要建立OMSIRT（Operation and Maintenance Security Incident Response Team，操作维护安全事件响应团队），这是专门负责接收供应商安全相关漏洞的应急响应组织，提供全局处理的解决方案，其职责包括：响应和处理供应商提交的安全事件，响应和处理行业协会公布的安全事件，制定运营商公司信息安全事件管理策略和安全事件处理方案，分析系统软件提供商和专业安全厂商发布的漏洞及补丁等。

7 结束语

基于NFV虚拟化的电信云网络跟传统网络相比，其更加复杂、更加开放、更加灵活，为电信网络IT化提供了技术基础。而同时，NFV系统也带来了更多的安全风险，给NFV商用网络造成了潜在的危害和挑战。电信运营商需要基于ETSI NFV架构，全面审视NFV中潜在的安全威胁，形成多维度、纵深的安全防护方案，封堵NFV系统中的安全漏洞。在日常的运维中，建立专业的网络安全服务团队，组建可持续发展的电信网络安全服务保障体系，为电信云网络安全保驾护航。

参考文献：

[1] 方琰崴. 中兴通讯云化核心网vCN助运营商网络变革[J]. 通信世界, 2018(2): 20-21

[2] ETSI GS NFV 001. Network Functions Virtualisation (NFV); Use Cases[S]. 2016.

[3] ETSI GS NFV 002. Network Functions Virtualisation (NFV); Architectural Framework[S]. 2016.

[4] ETSI GS NFV 003. Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV[S]. 2016.

[5] ETSI GS NFV 004. Network Functions Virtualisation (NFV); Virtualisation Requirements[S]. 2016.

[6] ETSI GS NFV-INF 001. Network Functions Virtualisation; Infrastructure Overview[S]. 2016.

[7] ETSI GS NFV-MAN 001. Network Functions Virtualisation (NFV); Management and Orchestration[S]. 2016.

[8] 朱建军,方琰崴. 电信运营商云化数据中心及关键技术研究[J]. 中国新通信, 2018(6): 57-58.

[9] ETSI GS NFV-SWA 001. Network Functions Virtualisation (NFV); Virtual Network Function Architecture[S]. 2016.

[10] ETSI GS NFV-INF 003. Network Functions

（下转第 13 页）

代, 2017(10): 1.
[2] 工业和信息化部. 中国区块链技术和应用发展白皮书[S]. 2016.
[3] 张偲. 区块链技术原理、应用及建议[J]. 软件, 2016, 37(11): 51-54.
[4] 华为技术有限公司. 华为区块链白皮书[Z]. 2018.
[5] 彭力. 物联网技术概论[M]. 北京: 北京航空航天大学出版社, 2011.★

作者简介

黄泽源：工程师，硕士毕业于中山大学，现任职于中国电信股份有限公司广州研究院，从事企业物联网产品以及物联网安全前沿技术研究工作。

孔勇平：工程师，硕士毕业于华南理工大学，现任职于中国电信股份有限公司广州研究院，从事移动互联网领域的LBS产品研发、区块链技术、物联网安全业务研究工作。

张会炎：工程师，硕士毕业于重庆大学，现任职于中国电信股份有限公司广州研究院，从事企业物联网平台以及物联网安全研究工作。

（上接第 7 页）

Virtualisation (NFV); Infrastructure; Compute Domain[S]. 2016.
[11] ETSI GS NFV-INF 004. Network Functions Virtualisation (NFV); Infrastructure; Hypervisor Domain[S]. 2016.
[12] ETSI GS NFV-INF 005. Network Functions Virtualisation (NFV); Infrastructure; Network Domain[S]. 2016.
[13] 方琰崴. 面向云化的电信运营转型方案、关键技术和发展策略[J]. 信息通信技术, 2018(2): 58-65.★

作者简介

方琰崴：高级工程师，硕士毕业于南京航空航天大学信息学院数字通信专业，现任中兴通讯股份有限公司电信云与核心网产品线产品规划总工、产品市场总监，发表论文二十余篇，获多项专利，研究方向为电信云与核心网的组网和关键技术。

陈亚权：学士毕业于江苏理工学院计算机科学与技术专业，现任中兴通讯股份有限公司电信云与核心网产品线产品规划总工，研究方向为5G核心网的规划。