ACCEPTED FROM OPEN CALL

NFV: Security Threats and Best Practices

Shankar Lal, Tarik Taleb, and Ashutosh Dutta

Network function virtualization (NFV) yields numerous benefits, particularly the possibility of cost-efficient transition of telco hardware functionalities on the software platform to break the vendor lock-in problem. These benefits come at the price of some security flaws. Indeed, with NFV, virtual mobile networks become vulnerable to a number of security threats.

ABSTRACT

Network function virtualization (NFV) yields numerous benefits, particularly the possibility of a cost-efficient transition of telco hardware functionalities on the software platform to break the vendor lock-in problem. These benefits come at the price of some security flaws. Indeed, with NFV, virtual mobile networks become vulnerable to a number of security threats. These threats can be leveraged using some available mitigation techniques and also through other emerging solutions. This article presents critical security threats that exist in the NFV infrastructure, proposes best security practices to protect against them.

INTRODUCTION

The telecommunication infrastructure is experiencing great structural changes in the way it used to be deployed, thanks to emerging technologies such as network functions virtualization (NFV). NFV is a great development in the process of network evolution which uses modern virtualization platforms and commercial of-the-shelf (COTS) hardware to deploy network functions for mobile networks. It has undoubtedly a significant impact on network operations. An important contribution of NFV is to turn network functions, which traditionally rely on hardware appliances, into software modules such as network firewalls and gateway routers/switches.

Traditional network functions are coupled with underlying dedicated hardware, which are, in turn, vendor propriety. When it comes to scaling the network, the deployment of new network functions and services becomes increasingly cumbersome and expensive. It is also difficult to provision them when there is dynamic network traffic and constantly changing requirements. NFV defines a promising approach to overcome these problems, enabling easy and fast network function deployment [1, 2]. In comparison with traditional network infrastructures, NFV delivers the following promises among others:

- Lowering the cost of ownership by moving network functions from dedicated boxes into virtual resources (i.e., virtual machines, VMs or containers).
- Enabling fast and cost-efficient deployment of network functions for better service agility.
- Supporting agile and flexible deployment of network functions along with their lifecycle management.
- Reducing energy consumption.

Contrary to common belief, NFV does not depend on software defined networking (SDN) and can be implemented stand-alone. SDN and NFV are complementary to each other and bring significant advantages when used together. NFV can bring the benefits of virtualizing SDN controllers and thus allowing dynamic mobility of SDN controllers to desired locations. SDN can bring value to NFV allowing dynamic network connectivity by programming the network to be optimal based on network traffic monitoring and analysis [1]. Some practical examples of VNF are vRouters, vFirewalls, virtual content delivery servers, vIPS/vIDS, vDNS servers, and virtual VPN servers.

In this article, we review the security challenges that pose threats to NFVI. We explain the ways by which these security attacks can be carried out on NFVI. Based on the severity of these security attacks, we propose some best security practices to cope with these attacks. The rest of this article is organized as follows. We list the gains and pains of adopting NFV. This section also explains the security implications of adopting NFVI and also the opportunities arising to build a secure and vibrant NFVI-based ecosystem. We present some related work and ongoing research projects. We briefly discuss the ETSI NFV architecture. We discuss the main security risks associated with NFVI and highlight the most popular security attacks that can be executed on NFVI. We propose best security practices that should be followed to protect against these attacks. We further discuss the open security challenges. Finally, the article concludes.

GAINS AND PAINS OF NFVI

NFV provides the means to install new network functions on demand without needing any installation of new hardware equipment. For example, a mobile operator can run any software-based network function in a specific format of virtual resources (e.g., VMs or containers) at any time. This certainly enables agile networking and cost-effective deployment of network functions. By enabling these features, NFV promises a decrease in time to market for network functions through software-based services and facilitating custom deployment of services based on customer's requirements.

Security in NFV raises important concerns about its adaptability in the underlying telecommunication infrastructure. It largely impacts the system resiliency [16] as well as the overall quality of the offered services [17]. Some of these security concerns apply to the key architectural components of NFV infrastructure such as virtual infrastructure manager (VIM). Hypervisor is the main element of VIM and is already under various

Digital Object Identifier:
10.1109/MCOM.2017.1600899

Shankar Lal is with Nokia Bell Labs/Aalto University; Tarik Taleb is with Sejong University/Aalto University; Ashutosh Dutta is with AT&T.

security attacks such as VM/guest OS manipulation and data exfiltration/destruction. Therefore, when the hypervisor is compromised, other vulnerabilities can arise exponentially. Since NFV delivers software enabled automated provisioning of network functions, it can also open security vulnerabilities such as automated network configuration exploits, orchestration exploits, malicious misconfiguration, and SDN controller exploits. Due to the elastic and flexible nature of NFVI elements, some security attacks can also become amplified. One type of such an attack is called a DNS amplification attack, which is discussed in a later section. In addition, VNFs are likely to be provided by many different vendors, which can possibly result in interoperability issues causing security loopholes in the infrastructure [3].

In addition to these security risks, the flexible and scalable nature of NFV helps to improve the incident response time, provides better resiliency against distributed denial of service (DDoS) attacks and enables on-demand firewalling and intrusion detection/prevention systems (IDS/IPS) to block or reroute malicious traffic. Figure 1 depicts an example of an attack on NFVI. In the envisioned scenario, the mobility management entity (MME) is virtualized and the orchestrator is capable of instantiating new vMME instances on demand. In this scenario, an attacker could create a botnet army by infecting many mobile devices with a "remote-reboot" malware, enabling the attacker to instruct the malware to reboot all devices at the same time (step 1 in Fig. 1). The simultaneous rebooting of all devices causes excessive "malicious" attach requests and results in a signaling storm (step 2 in Fig. 1), putting vMME under DDoS attack. In response to the attack, the orchestrator may instantiate a new VM to scale-out the vMME function to sustain the surge in the signaling traffic and to ensure service availability while the attack is being investigated (step 3 in Fig. 1).

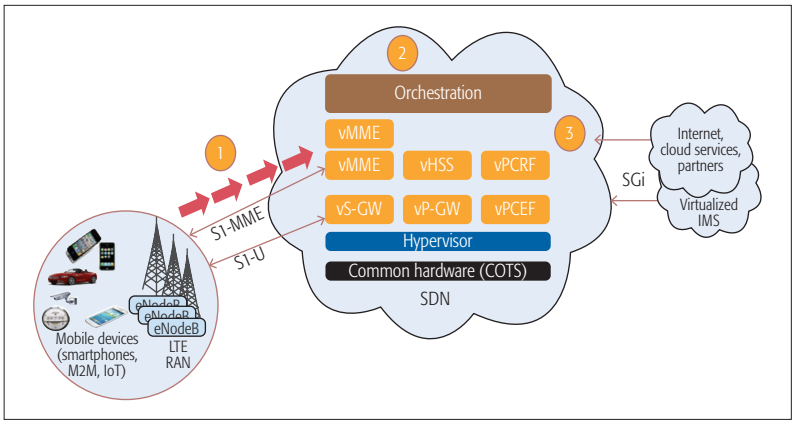

Figure 1. NFVI- DDoS resiliency.

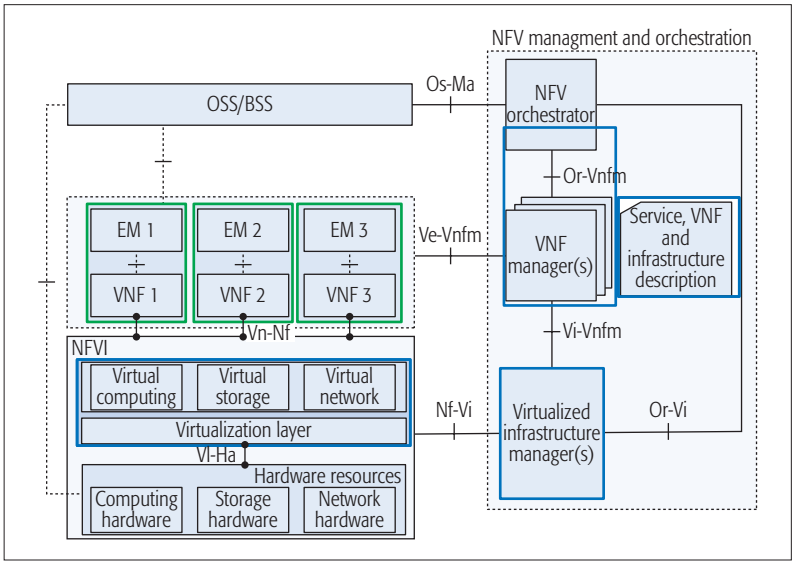

Figure 2. The ETSI NFVI reference architecture.

Related Work and Ongoing Projects

Security concerns have been raised in [4] where the authors identified security challenges in managing security of virtual appliances in cloud service provider's infrastructure along with the introduction of additional entities such as orchestrators which can be vulnerable to security threats. The authors in [5] presented two security risks that need to be taken care of during NFV design. The first is the isolation and protection of two network functions from different subscribers. The second is the security and resiliency of physical and virtual resources of NFVI. In [6], the authors provided a security framework for virtualized networks based on the use of a root trusted module.

There are a number of ongoing research projects in the NFV security domain aiming to provide security and resiliency of the NFV infrastructure. The European H2020 Arcadia project[1] has the objectives of detecting, exploring, and understanding security events in NFVI by service chain performance analytics to detect anomalistic behavior of the network functions. The 5G Ensure project[2] envisions securing future 5G networks that will rely on NFVI. It aims at developing security enablers consisting of privacy, trust, and virtualization isolation functions for 5G networks. OPNFV, an open source project from the Linux Foundation[3], has a dedicated security group working on vulnerability management to develop network security functions for NFV.

Brief Overview of NFV Infrastructure

NFVI provides the infrastructure that consists of all the hardware and software resources that are required to deploy VNFs. Figure 2 shows the NFVI reference architecture as defined by the European telecommunications standards institute (ETSI). The hardware resources consist of compute, storage, and network elements that basically provide the processing, storage, and connectivity capabilities to VNFs through a virtualization layer. The virtualization layer provides an abstraction to the hardware resources and enables the software to use the virtualized infrastructure instead. Examples of the virtualization layer are the hypervisor and container based virtualization solutions such as Docker. Beyond the NFVI, the NFVI architectural framework also includes the following functional building blocks [7].

Virtual Network Functions: VNFs are software packages that can implement the network functions using the infrastructure provided by NFVI. Virtualizing the network functions reduces hardware usage, improves the scalability, and reduces

[1] http://www.arcadia-framework.eu

[2] http://www.5gensure.eu

[3] https://wiki.opnfv.org/display/security/Security+Home

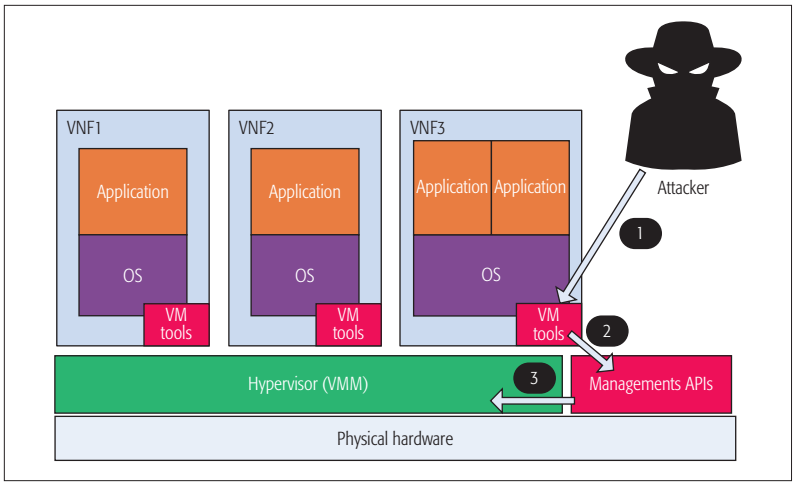

Figure 3. A VM escape attack scenario.

implementation costs. This enables easy upgrades, reduced power consumption, and equally reduced maintenance.

NFV Orchestrator: Responsible for onboarding the new network services and their lifecycle (e.g., instantiation, scaling in and out, performance measurement, and termination). The NFV orchestrator also performs global resource management and authorization to resource requests in the NFV.

VNF Manager(s): In charge of lifecycle management of VNFs from instantiating, updating, scaling, and terminating, and also performing other functions that are necessary for the entire VNF lifecycle. It also performs coordination and event reporting to other NFVI components.

Virtual Infrastructure Manager(s) (VIM): The VIM functionality includes controlling and managing the interaction of VNFs with NFVI. Basically, it performs resource management, which involves management and allocation of NFVI resources such as compute, storage, and network resources to VNFs. It also analyzes the performance of NFVI and logs if there is any fault information. Other functions of VIM involve collecting and forwarding performance and measurement events.

Additionally, there exists a VNF descriptor (VNFD) in the NFV management and orchestration stack, which is a VNF deployment template and contains descriptions regarding VNF operational and deployment requirements.

Security Risks Associated with NFV

VNFs run over virtual resources such as VMs. The security threats associated with VNFs are the combination of the security threats on physical networking and on virtualization technologies where NFV specific threats emerge when the two sets of threats intersect each other [8]. In the following, we discuss the potential security risks associated with NFVI, considering some potential attack scenarios.

Isolation Failure Risk

Here, we consider the case when an attacker manages to break into a hypervisor by compromising some VNFs running over it. This attack can impose great risk once successfully carried out. This is called a VM escape attack and is depicted in Fig. 3. In this attack scenerio, the attacker first compromises one VNF by gaining access to its operating system (step 1 in Fig. 3). Using tools and VNF network connectivity with the cloud management network, the attacker gains access to the hypervisor management API (step 2 in Fig. 3) and then the attacker breaks into the hypervisor to cause great impact (step 3 in Fig. 3). These attacks are possible due to the improper isolation between hypervisors and VNFs. A practical example of this attack could be launched by an application, running in a VNF and sending crafted network packets in order to exploit heap overflow with a compromised virtualization process and resulting in the execution of arbitrary code on the hypervisor to gain access to the host.

In another attack scenario, a VNF may orchestrate other VNFs, which can be achieved by granting the VNF API access to the virtualization infrastructure to instantiate new VNFs. The API can be misused by an attacker who can break in by compromising the VNF and gaining full access to all infrastructure resources [9].

Network Topology Validation and Implementation Failure

Using NFV, virtual networking components (e.g., virtual routers and virtual networks) can be easily created. Quick and dynamic service decisions can result in human error when a virtual router is created and used to interconnect virtual networks without the use of any firewall. Compared to physical network appliance deployments, the dynamicity of virtual network appliances and its connectivity can lead to improper separation between the network and its subnets. Using the above mentioned VM escape attack, an attacker can compromise virtual firewalls to restrict firewall functionality while allowing enough access to carry out the attack. In a similar attack scenario, an attacker may acquire knowledge about a multi-site network infrastructure using the elastic nature of NFVI. Effectively, an attacker can trigger the VNF instantiation or migration in another NFVI point of presence with lower security protection (i.e., without any IDS/IPS/deep packet inspection (DPI) capabilities) [9].

Regulatory Compliance Failure

Attacks aiming to place and migrate workload outside the legal boundaries were not possible using traditional infrastructure. Using NFV, violation of regulatory policies and laws becomes possible by moving one VNF from a legal location to another illegal location, as depicted in Fig. 4. The consequences of violating regulatory policies can be in the form of a complete banning of service and/or exerting a financial penalty, which may be the original intention of the attacker to harm the service provider. One possible attack scenario can be when an attacker exploits the insecure VNF API to dump the records of personal data from the database to violate user privacy.

Denial of Service Protection Failure

DoS attacks may be directed to virtual networks or VNFs' public interfaces to exhaust network resources and impact service availability. A huge volume of traffic from a compromised VNF can be generated and sent to other VNFs that would be running on the same hypervisor or even on different hypervisors. Similarly, some VNF applications

can consume high CPU, hard disk, and memory resources in order to exhaust the hypervisor [9]. In this vein, Fig. 5 depicts one practical scenario of DNS amplification attack. In this scenario, a NFVI infrastructure hosts a virtual DNS server as a component of a virtual evolved packet core (vEPC). The NFVI orchestrator is able to deploy additional virtual DNS servers if the traffic load increases. An attacker may spoof IP addresses of a number of victims and launches a high number of malicious DNS queries using the spoofed IP addresses (step 1 in Fig. 5). In response to such an attack, the orchestrator will instantiate new VMs to scale-out the vDNS function to accommodate more queries (step 2 in Fig. 5). Accordingly, multiple recursive DNS servers will respond to the victims that will ultimately receive amplified DNS query responses (step 3 in Fig. 5), which can result in its service disruption or unavailability.

Security Logs Troubleshooting Failure

In this security attack, compromised VNFs can generate a huge amount of logs on the hypervisor, making it difficult to analyze logs from other VNFs, especially when the initial entries in the log files are deleted. There is also risk when the infrastructure logs are leaked, which consequently enables cross relating of logs from one VNF operator with another to extract sensitive information [10].

Malicious Insider

These risks are classified as internal security risks and are caused by vicious actions of internal administrators. In one attack scenario, a malicious administrator takes the memory dump of a user's VM. Since the malicious administrator has the root access to the hypervisor and by using a search operation, he can extract the user ID, passwords, and SSH keys from the memory dump, which in turn violates user privacy and data confidentiality. In a second attack scenario, an internal attacker may extract a user's data from the hard-drive volume, managed by the cloud storage devices. To execute this attack, the attacker first creates a backup copy of the VM drive and then uses open source tools, such as kpartx and vgscan, to extract sensitive data from it [11].

NFV Best Security Practices

In this section, we shed light on best security practices that should be followed in order to achieve reasonably better security protection against the above mentioned threats in a NFV environment. It should be noted that these practices do not guarantee foolproof security of NFVI, but will provide better resiliency against these threats.

Boot Integrity Measurement Leveraging TPM

Using trusted platform module (TPM) as a hardware root of trust, the measurement of system sensitive components such as platform firmware, BIOS, bootloader, OS kernel, and other system components can be securely stored and verified. The platform measurement can only be taken when the system is reset or rebooted; there is no way to write the new platform measurement in TPM during the system run-time. The validation of the platform measurements can be performed by TPM's launch control policy (LCP) or through the remote attestation server [12]

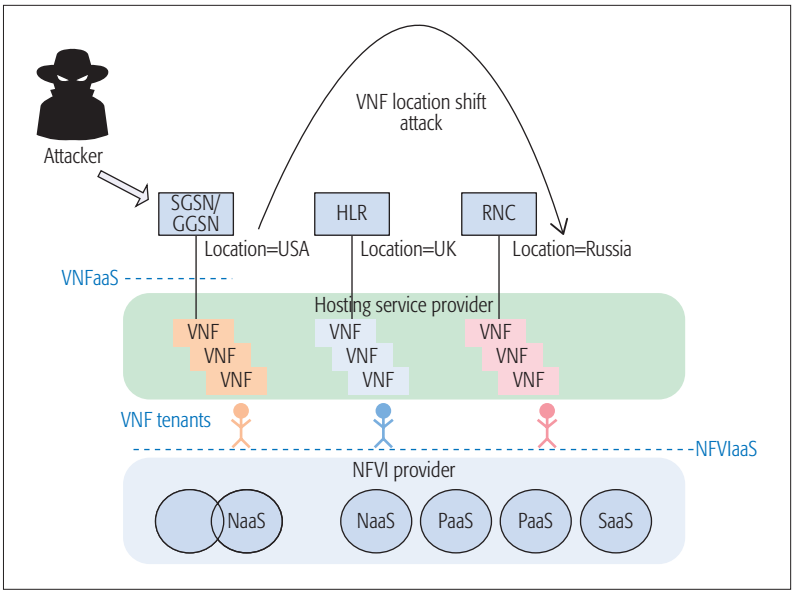

Figure 4. VNF location shift attack.

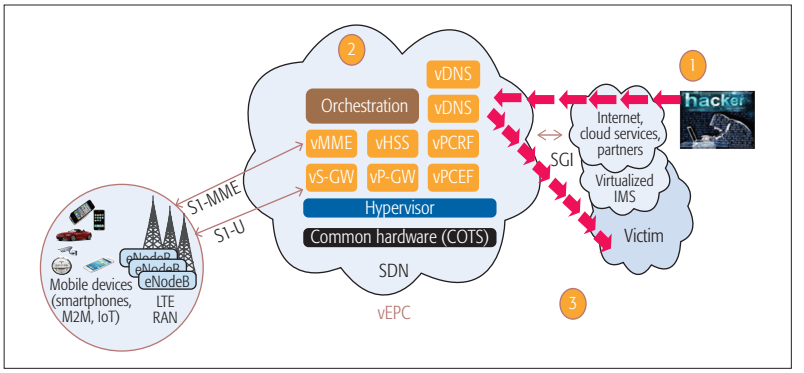

Figure 5. DNS amplification attack.

Hypervisor And Virtual Network Security

The hypervisor enables virtualization between underlying hardware and VMs. Virtual networks in the cloud use SDN to enable connectivity among VMs and also with outside networks. Security of these elements is a must in order to protect the whole infrastructure [15]. One of the security best practices is to keep the hypervisor up-to-date by regularly applying the released security patches. Failure to do that would result in exposure to security risks in the future. Another best practice is to disable all services that are not in use. For example, SSH and remote access service may not be needed all the time; therefore, it would be a good idea to enable these services only when needed [13]. Cloud administrators are the gatekeepers of the whole infrastructure and their accounts are the keys. It should be mandated to secure admin accounts by applying a strong password policy along with strictly following an organization's security guidelines.

Security Zoning

To prevent a VM from impacting other VMs or hosts, it is a good practice to separate VM traffic and management traffic. This will prevent attacks by VMs tearing into the management infrastructure. It is also a good idea to separate the VLAN traffic into groups and disable all other VLANs

To prevent a VM from impacting other VMs or hosts, it is a good practice to separate VM traffic and management traffic. This ill prevent attacks by VMs tearing into management infrastructure. It is also a good idea to separate the VLAN traffic into groups and disable all other VLANs that are not in use.

that are not in use. Likewise, VMs of similar functionalities can be grouped into specific zones and their traffic should be isolated. Each zone can be protected using access control policies and a dedicated firewall based on its needed security level. One example of such zones is a demilitarized zone (DMZ) [13, 15].

Linux Kernel Security

In virtualized platforms, the kernel of the host systems is a highly important component that provides isolation between the applications. The SELinux module, developed by the National Security Agency (NSA), is implemented in Kernel and provides robust isolation between the tenants when virtualization technology is used over the host. Secure virtualization (sVirt) is a new form of SELinux, developed to integrate mandatory access control security with Linux based hypervisors. sVirt provides isolation between VM processes and data files. Beyond these tools, other kernel hardening tools can be useful to secure the Linux kernel. A notable example is hidepd, which can be used to prevent unauthorized users from seeing other users' process information. Another example is GRSecurity, which provides protection against attacks on corrupted memory [10].

Hypervisor Introspection

Hypervisor introspection can be used to scrutinize software running inside VMs to find abnormal activities. It acts as a host-based IDS that has access to the states of all VMs, so that the root kit and boot kit inside VMs cannot hide easily. Using introspection capabilities, the hypervisor's functionalities are enhanced, enabling it, among other things, to monitor network traffic, access files in storage, and read memory execution. Hypervisor introspection APIs are powerful tools to perform deep VM analysis and potentially increase VM security. However, they can also be used as an exploit that makes it possible to break and bypass the isolation between VMs and the hypervisor. LibVMI is the library for hypervisor introspection for various platforms, implemented in C language with Python bindings. It gives the hypervisor the means to perform deep inspection of VMs (e.g., memory checking, vCPU register inspection, and recording trapping events) [14].

Encrypting VNF Volume/Swap Areas

Virtual volume disks associated with VNFs may contain sensitive data. Therefore, they need to be protected. The best practice to secure the VNF volume is by encrypting them and storing the cryptographic keys at safe locations. The TPM module can also be used to securely store these keys. In addition, the hypervisor should be configured to securely wipe out the virtual volume disks in the event a VNF is crashed or intentionally destroyed to prevent it from unauthorized access [6]. VM swapping is a memory management technique used to move memory segments from the main memory to disk, which is used as a secondary memory in order to increase system performance in case the system runs out of memory. These transferred memory segments can contain sensitive information such as passwords and certificates. They can be stored on the disk and remain persistent even after system reboot. This enables an attack scenario whereby a VM swap is copied and investigated to retrieve any useful information. One way to avoid this kind of attack is to encrypt VM swap areas. Linux based tools such as dm-crypt can be used for this purpose [10].

VNF Image Signing

It is easy to tamper with VNF images. It requires only a few seconds to insert some malware into a VNF image file while it is being uploaded to an image database or being transferred from an image database to a compute node. Luckily, VNF images can be cryptographically signed and verified during launch time. This can be achieved by setting up some signing authority and modifying the hypervisor configuration to verify an image's signature before they are launched [9].

Security Management and Orchestration

One best practice consists of designing a NFV orchestrator incorporating security and trust requirements of the NFVI. The orchestration and management of security functions requires integration by enabling interaction among the security orchestrator, the VNF manager, and the element management systems (EMS). This type of protection can be achieved by setting scaling boundaries in the VNFD or network service descriptor (NSD), for example, and having the NFVO enforce these restrictions to protect from attacks such as a DNS amplification attack.

Remote Attestation

The remote attestation technique can be used to remotely verify the trust status of a NFV platform. The concept is based on boot integrity measurement leveraging TPM, as mentioned earlier. Remote attestation can be provided as a service, and may be used by either the platform owner or a consumer to verify if the platform has booted in a trusted manner [12]. Practical implementations of the remote attestation service include the open cloud integrity tool (openCIT), an open source software hosted on GitHub.

Table 1 provides a summary of the security risks associated with NFVI as discussed above, and lists the targets of these risks along with possible mitigation techniques.

Open Security Challenges

Despite the best practices describe above, there are still open security challenges that are yet to be addressed. One of the security challenges is to define the standard interface in the ETSI NFV architecture to deploy virtual security functions to react to various threats in real time. Such functionalities should be able to communicate with the orchestration modules and follow the provided instructions. Another challenge is to securely manage and monitor VNFs by maintaining their configuration and state information during migration. This can be difficult to perform due to the dynamicity and elasticity of VNF operations in cloud environments. Another challenge is to perform the trust management between different vendors who build NFV hardware and software. The challenge is to efficiently manage the trust chain among vendors and provide trustiness of the final VNF products.

At the moment, attestation technologies only

provide the boot time attestation. This does not guarantee run time modification or prevent tampering with the system's critical components, and such modification would only be detected when the system is rebooted. Run time attestation is still an open research area that needs to be explored further. There is also a strong need to develop a comprehensive security architecture to take care of these security challenges in NFVI. To achieve these goals, network operators and vendors need to work together to form a vibrant security ecosystem. New standards, testbeds, and proofs of concept would serve as a catalyst for securing the NFV infrastructure. The services in this new virtualized environment are rapidly evolving, and in turn create new opportunities for innovation.

Conclusion

NFV undoubtedly provides great benefits for telecom service providers in terms of cost efficiency and dynamic service deployability. However, it is extremely necessary to understand the security implications for these benefits. It is essential to know the difference between general cloud computing infrastructure and NFV infrastructure and its needs and requirements. Previous studies presented analysis on security threats that exist in cloud computing along with mitigation techniques. It is equally required that similar studies have to be carried out for security in NFVI. Indeed, NFVI hosts highly sensitive workloads, and accordingly needs to be highly secured and protected. In this article, we identified security attacks on NFVI. We also presented best security practices to protect against these attacks. Admittedly, security in NFVI is still in its infancy, and there are still many open security challenges to tackle. This defines one of the future research directions of the authors. Future work also includes putting into practice the proposed solutions by means of implementations and experimental testbed setups.

Acknowledgement

This article is issued within the research activities of the Finnish Dimecc Cyber Trust Program. It was also partially supported by the ANASTACIA project, which has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 731558, and from the Swiss State Secretariat for Education, Research and Innovation. The authors would like to thank Dr. Ian Oliver from Nokia Bell Labs Finland and Deon Ogle and Shawn Hiemstra from AT&T, for useful discussions.

	Security risk	Target	Best practices
1	Compromised hypervisor	Platform	Separation of VM and management traffic, regular hypervisor patching
2	Isolation failure	Platform/VNFs	Hypervisor introspection, security zoning
3	Platform integrity	Platform	TPM boot integrity, remote attestation
4	DDoS attack	VNFs	Flexible VNF strategic deployment to defend against DDoS
5	Malicious insider	VNFs	Volume/swap encryption, VNF image signing, strict operational practices
6	Regularity compliance failure	VNFs	Geo-tagging using remote attestation

Table 1. NFVI security risks and best practices.

References

[1] T. Taleb *et al.*, "EASE: EPC as a Service to Ease Mobile Core Network," *IEEE Network*, vol. 29, no. 2, Mar. 2015, pp. 78–88.
[2] T. Taleb, "Towards Carrier Cloud: Potential, Challenges, & Solutions," *IEEE Wireless Commun.*, vol. 21, no. 3, June 2014. pp. 80–91.
[3] W. Yang and C. Fung. "A Survey on Security in Network Functions Virtualization," *2016 IEEE NetSoft Conf. and Wksps. (NetSoft)*, 2016.
[4] B. Han *et al.*, "Network Function Virtualization: Challenges and Opportunities for Innovations," *IEEE Commun. Mag.*, vol. 53, no. 2, 2015, pp. 90–97.
[5] R. Mijumbi *et al.* "Network Function Virtualization: State-of-the-Art and Research Challenges," *IEEE Commun. Surveys & Tutorials*, vol. 18, no. 1, 2015, pp. 236–62.
[6] Z. Yan *et al.*, "A Security and Trust Framework for Virtualized Networks and Software-Defined Networking," *Security and Communication Networks*, 2015.
[7] ETSI Group Specifications: Network Functions Virtualization (NFV); Architectural Framework.
[8] ETSI Published Specifications ETSI GS NFV-SEC 001 V1.1.1: Network Functions Virtualisation (NFV); NFV Security; Problem Statement
[9] Building Secure Telco clouds, Nokia white paper
[10] NFV Security in Practice Series — 9 Top Security Impacting Choices ALCATEL-LUCENT Bell Labs WHITE PAPER
[11] F. Rocha and M. Correia. "Lucy in the Sky Without Diamonds: Stealing Confidential Data in the Cloud," *2011 IEEE/IFIP 41st Int'l. Conf. Dependable Systems and Networks Wksps. (DSN-W)*, 2011.
[12] ETSI GS NFV-SEC 009 Network Functions Virtualisation (NFV); NFV Security; Report on Use Cases and Technical Approaches for Multi-Layer Host Administration, page 34.
[13] R. L. Krutz and R. D. Vines, *Cloud Security: A comprehensive Guide to Secure Cloud Computing*, Wiley Publishing, 2010.
[14] T. Garfinkel and M. Rosenblum. "A Virtual Machine Introspection Based Architecture for Intrusion Detection," NDSS, vol. 3. 2003.
[15] ETSI Published Specifications ETSI GS NFV-SEC 002: Network Functions Virtualisation (NFV); NFV Security; Cataloguing Security Features in Management Software.
[16] T. Taleb, A. Ksentini, and B. Sericola, "On Service Resilience in Cloud-Native 5G Mobile Systems," *IEEE JSAC*, vol. 34, no. 3, Mar. 2016. pp. 483–96.
[17] T. Taleb and Y. Hadjadj-Aoul, "QoS2: A Framework for Integrating Quality of Security with Quality of Service," *Wiley J. Security & Communication Networks*, vol. 5, no. 12, Dec. 2012. pp. 1462–70.

Biographies

Shankar Lal (shankar.lal@aalto.fi) received his B.E degree in electronics enginerring and M.Sc. degree in communication engineering-networking technology from Mehran University, Jamshoro, Pakistan and Aalto University, Espoo, Finland in 2008 and 2015, respectively. He is currently pursuing a doctoral degree at Aalto University, Espoo, Finland since May 2016. He has also been working with Nokia Bell Labs, Finland (previously Nokia Networks) as a research assistant since November 2014. Prior to his work at Nokia, he worked as an IT security engineer at Sapphire Consulting Services in Karachi, Pakistan for three and a half years. His main research interests revolve around security and integrity of NFV components, trusted telco cloud, secure placement of NFV MANO elements, and platform security leveraging the TPM module.

Tarik Taleb [S'04, M'05, SM'10] (tarik.taleb@aalto.fi) received his B.E. degree (with distinction) in information engineering, and M.Sc. and Ph.D. degrees in information science from Tohoku University, Sendai, Japan, in 2001, 2003, and 2005, respectively. He is a professor with the School of Electrical Engineering, Aalto University, Finland. He was a senior researcher and 3GPP standardization expert with NEC Europe Ltd. He was then leading the NEC Europe Labs Team, working on research and development projects on carrier cloud platforms. Prior to his work at NEC, he worked as an assistant professor at the Graduate School of Information Sciences, Tohoku University. His current research interests include architectural enhancements to mobile core networks, mobile cloud networking, mobile multimedia streaming, and social media networking. He has also

been directly engaged in the development and standardization of the evolved packet system as a member of 3GPP's System Architecture Working Group. He is an IEEE Communications Society (ComSoc) Distinguished Lecturer. He is a board member of the IEEE ComSoc Standardization Program Development Board. He is serving as the Chair of the Wireless Communications Technical Committee, the largest in IEEE ComSoC. He founded and has been the General Chair of the IEEE Workshop on Telecommunications Standards: From Research to Standards, which is a successful event that received the "Best Workshop Award" from IEEE ComSoC. He is/was on the editorial board of *IEEE Transactions on Wireless Communications*, *IEEE Wireless Communications Magazine*, *IEEE Transactions on Vehicular Technology*, *IEEE Communications Surveys and Tutorials*, and a number of Wiley journals. He has received many awards, including the IEEE ComSoc Asia Pacific Best Young Researcher Award in June 2009. Some of his research work has also received Best Paper Awards at prestigious conferences.

ASHUTOSH DUTTA [SM] (ad5939@att.com) is currently Lead Member of Technical Staff at AT&T's Chief Security Office in Middletown, New Jersey. His career, spanning more than 30 years, includes Director of Technology Security at AT&T, CTO of Wireless at cybersecurity company NIKSUN, Inc., Senior Scientist at Telcordia Research, Director of the Central Research Facility at Columbia University, adjunct faculty at NJIT, and computer engineer with TATA Motors. He has more than 90 conference and journal publications, three book chapters, and 30 issued patents. He is co-author of the book *Mobility Protocols and Handover Optimization: Design, Evaluation and Application*, published by IEEE and John & Wiley, that was recently translated into Chinese. An active IEEE and ACM volunteer, he served as the chair for IEEE Princeton/Central Jersey Section, Industry Relation Chair for Region 1 and MGA, Pre-University Coordinator for IEEE MGA, and vice chair of Education Society Chapter of PCJS. He co-founded the IEEE STEM conference (ISEC) and helped implement EPICS (Engineering Projects in Community Service) projects in several high schools. He currently serves as the Director of Industry Outreach for the IEEE Communications Society and is the co-lead for the IEEE 5G initiative. He was the recipient of the prestigious 2009 IEEE MGA Leadership Award and the 2010 IEEE-USA Professional Leadership Award. He obtained his B.S. in electrical engineering from NIT Rourkela, India, an M.S. in computer science from NJIT, and a Ph.D. in electrical engineering from Columbia University under the supervision of Prof. Henning Schulzrinne. He is a senior member of ACM.