NFV : Security Threats and Best Practices

Bhargavi Mohan

November 9, 2018

Abstract

This study gives an account of the critical security threats present in the NFV architecture , introduces some of the best security practices to avoid them.

1 Introduction

NFV is indeed a significant invention in the networking evolution and its applications have valuable outcomes in the network operations. Network functions that rely on hardware appliances can now rely on software modules such as network firewalls and gateway routers/switches. NFV offers a lot of advantages to avoid problems caused by traditional approaches. NFV doesn't depend on SDN and can be implemented standalone.This article explains the how the security challenges that are hazardous to NFVI could be executed.Depending on the severity of attacks, suitable security practices have been proposed.

2 Related Work and Ongoing Projects

The study in [2] identifies challenges in managing security of virtual appliances in cloud service provider's infrastructure. The study in [5] presents two security risks,one is : two network functions from different subscribers has to be isolated and protected. second is:security and strength of physical and virtual resources of NFVI. The study in [9] provides a security framework for virtualized network based on the use of root trusted module.

2.1 Ongoing Research

- The European H2020 Arcadia project [1]
- The 5G Ensure project 2 [2]
- OPNFV, an open source project from the Linux Foundation 3 [3]

[1] http://www.arcadia-frame-work.eu
[2] http://www.5gensure.eu
[3] https://wiki.opnfv.org/display/security/Security+Home

3 Security Risks Associated with NFV

Isolation Failure Risk: Firstly, the attacker gains access to the OS of one VNF and then gains access to the hypervisor management interface through VM tools. Finally the attacker hijacks the hypervisor to cause a colossal effect.Another attack scenario where the API access of the VNF is given to the virtualization infrastructure to orchestrate other VNFs. The API could be tainted and gains full access to all the infrastructure resources [8].

Network Topology Validation and Implementation Failure: When a virtual router is created and used to interconnect virtual network without using firewall, it could sometimes be erroneous. Using the VM escape attack, an attacker can compromise virtual firewalls delimiting the firewall features thus creating a chance for a hijack. Due to NFVI being extremely flexible , an attacker may achieve knowledge about a multisite network infrastructure where the VNF instantiation or migration in another NFVI Pop without DPI capabilities can be generated.

Regulatory Compliance Failure: Relocating one VNF from a legal location to an illegal location is now possible using NFVs regulatory policies and laws. The attack scenario can be when an attacker leaks the VNF API to discard the personal data from database to breach user privacy.

Denial of Service Protection Failure: In this attack scenario,a NFVI manages a virtual DNS server as an element of a vEPC. An attacker may fake IP addresses of a number of victims and sends a huge number of DNS queries. In response to this , the orchestrator will arrange additional virtual DNS servers to take in more queries. Ultimately multiple DNS servers reponds to the victims with huge responses thus resulting in service disruption/unavailability.

Security Logs Troubleshooting Failure: Massive amount of logs on the hypervisor is created by compromising VNFs which makes it hard to inspect logs from other VNFs particularly when the early entries in the log files are deleted. There are chances that sensitive data can be extracted when the infrastructure logs are exposed from one VNF operator to another.

Malicious Insider: This is the internal security risk where an admin maliciously takes the memory dump of any user's VM. Root access to the hypervisor is an advantage to the admin who can access the user ID , password and SSH keys. Also, an attacker can take a copy of the user's VM drive and uses tools as kpartx and vgscan, to extract sensitive data [7].

4 NFV Best Security Practices

Boot Integrity Measurement Leveraging TPM: By using TPM, sensitive components such as platform firmware, bootloader, OS kernal and other components can be safely stored and verified. The platform measurement can only be done when the system is rebooted and not during system run-time.

Hypervisor And Virtual Network Security: Security of VMs is a must to safeguard the entire infrastructure [6]. Keeping the hypervisor updated on regular basis by applying the released security patches is a good way to go. Disabling the unwanted services and enabling them as and when needed is a good idea[4].Strong passwords to admin accounts should be mandated.

Security Zoning: Keeping the VM traffic from not interfering with other VMs or hosts is a good practice, also better to seperate the VLAN traffic into groups and disable all useless VLANs.Organizing similar featured VMs into specific zones and isolating their traffic is required. Zone example : demilitarized zone (DMZ) [4, 6].

Linux Kernel Security: Kernel being a prominent component of the host in virtualized platform, provides isolation between the applications. hidepd - is used to prevent unauthorized users from seeing other user's process information.GRSecurity - provides protection against attacks on corrupted memory [3].

Hypervisor Introspection: Software running inside VMs need to be carefully examined to find abnormalities using hypervisor introspection. Powerful tools to execute deep VM analysis are hypervisor introspection APIs which also scales up the VM security.LibVMI - is a library for hypervisor introspection , helps hypervisor to enforce deep inspection of VMs [1].

Encrypting VNF Volume /Swap Areas: Virtualized volume disks with confidential data have to be protected. Encrypting these disks with cryptographic keys at safe locations is the best practice. When a VNF is crashed, hypervisor should be configured in a way to safely wipe out the virtual volume disks to avoid unauthorized access [9]. VM swapping is movement of memory segments from main memory to disk to increase system performance. VM swapped areas should be encrypted using tools like dm-crypt [3].

VNF Image Signing: Some malware can be inserted into a VNF image file to vary the information while it is being uploaded to image database. Hence VNF images should be cryptographically signed during uploads. Setting up signing authority and changing hypervisor configuration to verify image's signature is a good practice [8].

Security Management and Orchestration: Involves designing an NFV orchestrator characterizing security requirements of the NFVI

Remote Attestation: This technique is based on boot integrity measurement leveraging TPM, this can be provided as a service to check if the platform boots as expected [6].

5 Open Security Challenges

There exists open security challenges that are yet to be addressed. Virtual security function to address threats in real time requires a standard interface in the NFV architecture. Monitoring VNFs by handling their configuration during migration is hard to attain due to the flexibility of VNF operations in cloud environments. Dynamic attestation is still an ongoing research.

6 Conclusion

This study gives an awareness about the absolute necessity to understand all the security threats that is posed to the NFVI. The best practices to follow are discussed to remain protected against these attacks. There are a few more open security challenges that has to be dealt which is a part of the future research.

References

[1] Tal Garfinkel, Mendel Rosenblum, et al. A virtual machine introspection based architecture for intrusion detection. In *Ndss*, volume 3, pages 191–206, 2003.

[2] Bo Han, Vijay Gopalakrishnan, Lusheng Ji, and Seungjoon Lee. Network function virtualization: Challenges and opportunities for innovations. *IEEE Communications Magazine*, 53(2):90–97, 2015.

[3] NFV Security in Practice Series. - 9 top security impacting choices alcatel-lucent bell labs white paper.

[4] Ronald L Krutz and Russell Dean Vines. *Cloud security: A comprehensive guide to secure cloud computing*. Wiley Publishing, 2010.

[5] Rashid Mijumbi, Joan Serrat, Juan-Luis Gorricho, Niels Bouten, Filip De Turck, and Raouf Boutaba. Network function virtualization: State-of-the-art and research challenges. *IEEE Communications Surveys & Tutorials*, 18(1):236–262, 2016.

[6] ETSI Published Specifications ETSI GS NFV-SEC 002: Net. work functions virtualisation (nfv); nfv security; cataloguing security features in management software.

[7] Francisco Rocha and Miguel Correia. Lucy in the sky without diamonds: Stealing confidential data in the cloud. In *Dependable Systems and Networks Workshops (DSN-W), 2011 IEEE/IFIP 41st International Conference on*, pages 129–134. IEEE, 2011.

[8] Nokia white paper. Building secure telco clouds.

[9] Zheng Yan, Peng Zhang, and Athanasios V Vasilakos. A security and trust framework for virtualized networks and software-defined networking. *Security and communication networks*, 9(16):3059–3069, 2016.