A Misuse Pattern for Distributed Denial-of-Service Attack in Network Function Virtualization

ABDULRAHMAN K. ALNAIM, Florida Atlantic University
AHMED M. ALWAKEEL, Florida Atlantic University
EDUARDO B. FERNANDEZ, Florida Atlantic University

Network Function Virtualization (NFV) takes advantage of cloud-based virtualization to offer scalable and flexible network functions such as switches, routers, load balancers, and domain name systems (DNSs). These virtualized network functions (VNFs) are considered better solutions than hardware-based network functions (NFs) as their resources can be dynamically increased upon consumer requests. While their usefulness can't be denied, they also have some security implications; VNFs have a large attack surface and can be used by attackers to jeopardize the NFV environment. We present here a misuse pattern for distributed denial-of-service (DDoS) attacks in NFV. DDoS is a malicious attempt to make the service unavailable for legitimate users by flooding system servers with a high volume of requests. Misuse patterns describe how the attack is performed from the point of view of the attacker; they also define the environment where the attack is performed, what security mechanisms are needed as countermeasures to stop it, and how to find forensic information to trace the attack once it happens. This pattern is part of an ongoing catalog of misuse patterns we aim to build for the diagrams of NFV systems. Our audience are system designers, system architects, and security professionals who are interested in building a secure NFV system.

Categories and Subject Descriptors: D.2.11 [Software Engineering] Software Architectures–Patterns;

General Terms: Design

Additional Key Words and Phrases: cloud computing, network function virtualization (NFV), distributed denial-of-service attack, hypervisor, misuse patterns, security reference architecture

ACM Reference Format:

Alnaim, A. K., Alwakeel, A. M. & Fernandez, E. B. (2019). (2019). A Misuse pattern for distributed denial-of-service attack in network function virtualization. In *Proceedings of the 26th PLoP'19*, October 7-10, Ottawa, Ontario, Canada. 10 pages.

1. INTRODUCTION

The telecommunication industry is having a new shift in its infrastructure and network service delivery. In the traditional network infrastructure, telecommunication service providers (TSPs) are required to deploy physical proprietary equipment for every network function, which introduces high installation costs and restrictions when scaling up/down the network. But this is not the case with NFV. Network Function Virtualization uses clouds to virtualize the network functions that may be chained together to build a communication service. This ensures the provision of a shared, scalable, and energy-efficient network environment.

The European Telecommunications Standards Institute (ETSI) has developed a reference architecture (RA) framework for NFV that consists of three main components as shown in fig.1 (ETSI, 2014). First, it uses virtualized network functions (VNFs), that are software implementations of network functions. Second, NFV management and orchestration (MANO), that covers the lifecycle management and orchestration of NFV resources, and consists of three parts; the Orchestrator, responsible for managing the lifecycle of network services; the VNF Manager, responsible for VNFs lifecycle management; and the Virtualized Infrastructure Manager (VIM), which is responsible

Authors' addresses: A. K. Alnaim (corresponding author), Dept. of Computer and Electrical Eng. and Computer Science, Florida Atlantic University, 777 Glades Rd., Boca Raton, FL33431, USA; email: aalnaim2017@fau.edu; A. M. Alwakeel, Dept. of Computer and Electrical Eng. and Computer Science, Florida Atlantic University, 777 Glades Rd., Boca Raton, FL33431, USA; email: aalwakeel2013@fau.edu; E. B. Fernandez, Dept. of Computer and Electrical Eng. and Computer Science, Florida Atlantic University, 777 Glades Rd., Boca Raton, FL33431, USA; email: fernande@fau.edu

Function Virtualization Infrastructure (NFVI), which comprises all the hardware and software components to support the execution of the virtualized network functions. The NFVI also contains the hypervisor, which resides within the virtual machine environment. The hypervisor is a collection of software modules that provides virtualization of hardware resources and creates virtual machines (VMs) to be run on a single physical server (ETSI, 2015).

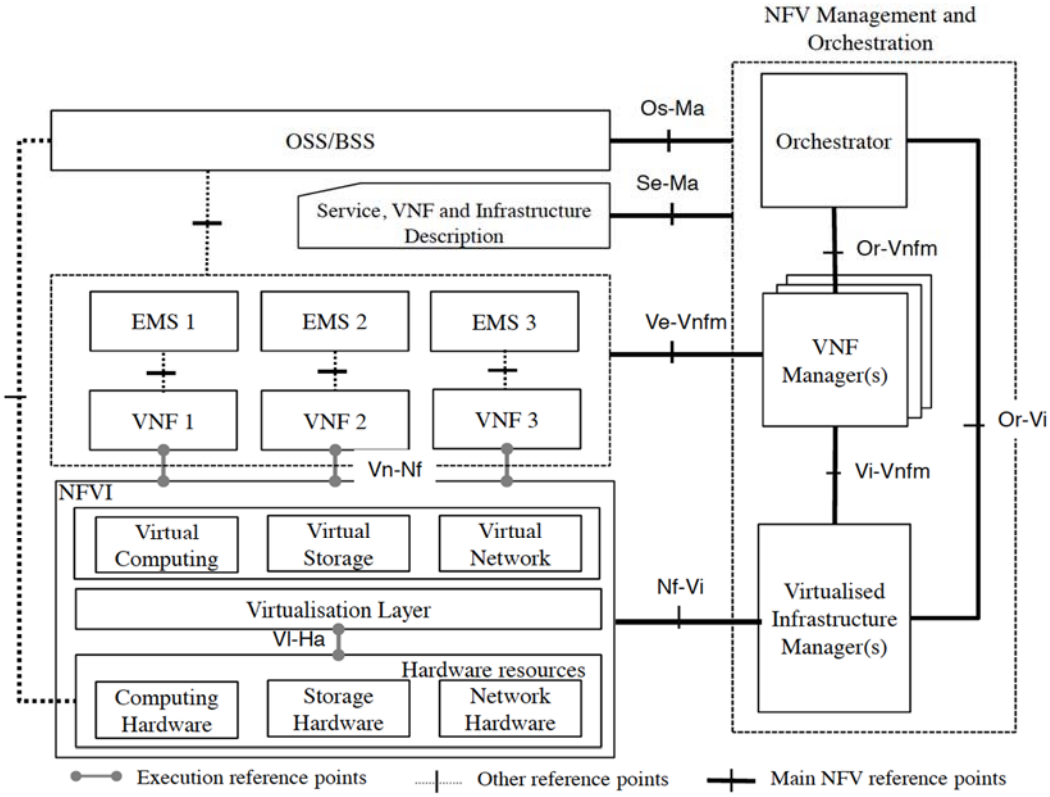

Fig. 1: NFV reference architecture framework of ETSI (ETSI, 2014)

Despite the advantages that NFV provides, it introduces several security threats and challenges. We have surveyed the main security threats and attacks of NFV and the possible countermeasures to mitigate these threats (Alwakeel, Alnaim, & Fernandez, 2018). Our approach was to categorize the threats based on the NFV vulnerabilities. In previous work, we showed how some of the identified threats may lead to several misuses of information and described two of them using misuse patterns, Privilege Escalation (Alnaim, Alwakeel, & Fernandez, 2019b), and VM Escape (Alnaim, Alwakeel, & Fernandez, 2019a). Misuse patterns describe, from the point of view of an attacker, a generic way of performing an attack that takes advantage of the specific vulnerabilities of some environment or context (Fernandez, 2013). They also define the environment where the attack is performed, what security mechanisms are needed as countermeasures to stop it, and how to find forensic information to trace the attack once it happens.

In this paper, we use misuse patterns to describe denial-of-service (DoS) attack in NFV. DoS/DDoS is a type of attack that affects the service availability (misuse) of the legitimate users of a network by flooding it with useless traffic. In NFV, it can be performed in different forms, for example, a compromised VNF can generate multiple resource requests that will make other VNFs running on the same hypervisor to starve for resources, or a malicious VNF application can consume high CPU and memory seeking to exhaust the hypervisor resources. Here, we show a possible scenario of DDoS (threat) based on a Domain Name Server (DNS) amplification attack. The DNS amplification

attack is a reflection-based volumetric DDoS attack that leverages DNS resolvers, which are servers that store DNS name-servers and manage DNS requests for all users in a network, to overwhelm the victim's servers or network with a huge volume of malicious requests hogging the resources and making the service inaccessible for legitimate users. To perform this attack, attackers use a botnet, which is a group of infected devices called bots, that sends User Datagram Protocol (UDP) packets to DNS resolvers with spoofed IP addresses (Cloudflare, n.d.). The spoofed addresses point to the real IP addresses of the victims. The DNS resolvers will then respond to the spoofed IP addresses, and in turn the victims will receive amplified responses that overwhelm their servers resulting in a denial-of-service. Attackers take advantage of the UDP packets as they do not require a handshake which allows the receiver to accept the request before it is sent. UDP Packets are designed to be sent without confirmation from the receiver, which makes them ideal for attackers to send their malicious packets. The reason why the UDP is still used today is because it is vital for time-sensitive communications such as voice and video communications (Cloudflare, n.d.).

This NFV DDoS misuse pattern is part of an ongoing catalog that could be used by security professionals, system designers, and system architects to consider security aspects when building an NFV system. Also, we are building a Reference Architecture (RA) for NFV. By adding these misuse patterns to it and their corresponding defenses we can obtain a Security Reference Architecture (SRA). Fig. 2 shows a pattern diagram that describes the misuse patterns that have been added to the RA: misuse pattern using Privilege Escalation (Alnaim et al., 2019b), and using VM Escape (Alnaim et al., 2019a), and the pattern in this paper.

Section 2 presents a misuse pattern for DDoS in NFV based on DNS amplification attack. We end with conclusions and future work in section 3. We added appendix 1 at the end of the paper includes the template we use for misuse patterns (Fernandez, 2013). We also added a list of all acronyms we used in appendix 2, and a glossary in appendix 3.

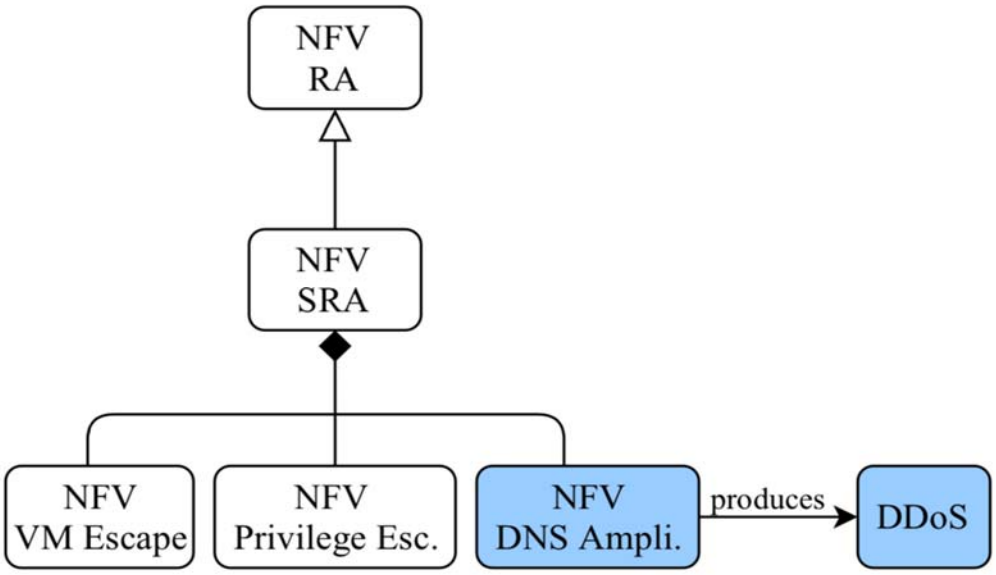

Fig. 2. Pattern diagram for misuse patterns in NFV

2. DISTRIBUTED DENIAL-OF-SERVICE ATTACK IN NFV USING DNS AMPLIFICATION

Intent

An attacker intends to exhaust network resources and impact service availability to legitimate users by sending a huge number of requests from a DNS.

2.2 Context

NFV providers offer elastic and scalable network services for their consumers, and they can dynamically spawn additional resources (Virtual Machines) to accommodate consumers network requests. However, these resources, even if large, could be limited.

2.3 Problem

How can an attacker flood a target (a network service of an NFV consumer) with a large number of DNS requests consuming most of its resources, e.g., bandwidth, thus achieving a DDoS attack?

The attack can be performed by exploiting the following vulnerabilities:

1. NFV is a recent technology and its security infrastructure has not been tested enough in the wild, which raises the possibility that vulnerabilities may lead to several threats including the denial of service threat.
2. The urgency to adopt NFV services may have let NFV providers to focus more on profits without hardening the security of its infrastructure including the DNS server configurations (SecurityTrails, 2018).
3. The network service is hosted on a shared environment running on top of VMs; if a VNF is compromised due to misconfiguration, malware infection, or by exploiting a vulnerability in an old version of software running on it, a huge amount of traffic can be generated from the compromised VNF and sent to other co-resident VNFs running on the same hypervisor or even on different hypervisors, or to DNSs (Huang, Chowdhary, & Pisharody, 2018).
4. The NFV environment provides network functions with a higher degree of flexibility and configuration than traditional architectures; therefore, it has more ways to misconfigure the network functions, which increases the attack surface and opens new avenues to compromise the system (Pillaipakam, 2016).
5. The elasticity of the NFV environment enables network resources to rapidly scale up or down. In case of the DNS amplification DDoS attack, attackers can take advantage of that to amplify the attack when multiple vDNSs will be created due to the traffic load and will produce a huge number of DNS replies to the victim. This scenario is possible in NFV environment and we demonstrate it in the later sections.
6. Domain Name Systems, especially public DNSs, are designed to respond to any request where attacker can turn small DNS requests into a much larger payloads. Attackers can leverage this amplification effect to launch a DDoS attack.

2.4 Solution

The attack is possible when the attacker floods the network resources with a large number of DNS requests using spoofed IP addresses. First, we assume the attacker has a botnet of infected devices (Syed, Fernandez, & Moreno, 2018), and a list of victims' IP addresses. The attacker spoofs the IP addresses of victims' machines and uses the botnet, which is controlled by the command and control server, to launch a large number of malicious DNS requests (UDP packets). These requests are sent to a VNF (a vDNS). The orchestrator realizes the traffic load on the vDNS is above the normal threshold, and in turn the hypervisor initiates new VMs to scale-out additional vDNSs to accommodate more requests. This elastic and scalable nature of NFV will make multiple vDNS recursively respond to the victims, and in effect will receive amplified DNS responses, which can ultimately result in service disruption for the victims' web servers. This practical scenario is described by (Lal, Taleb, & Dutta, 2017) and it is possible in any system, including NFV.

2.4.1 Structure

Fig. 3 shows a class diagram for distributed denial-of-service attack in NFV, showing the units compromised by this attack. The **Command and Control Server (CC)** is a centralized management platform controlled by the attacker used for orchestrating the attack. **Botnet** is a network of attacking machines, which the attacker uses to launch a high number of malicious DNS requests that contain spoofed IP addresses matching the victims' IP addresses. The **NFV**

Consumer accesses the **VNF** functions using their **APIs**. The **vDNS** is one of the VNF functions. The **Hypervisor** controls the **VMI Repository** that stores **VM Images** (VMIs), creates **VMs**, and manages the **NFVI resources** necessary to provide network services. Each VM is created using a VMI, and VMs can contain several VNFs. Once a VM is launched, the Hypervisor assigns resources to it. The **Orchestrator** is a management and orchestration (MANO) unit that has several roles, one of them is monitoring the NFVI resources.

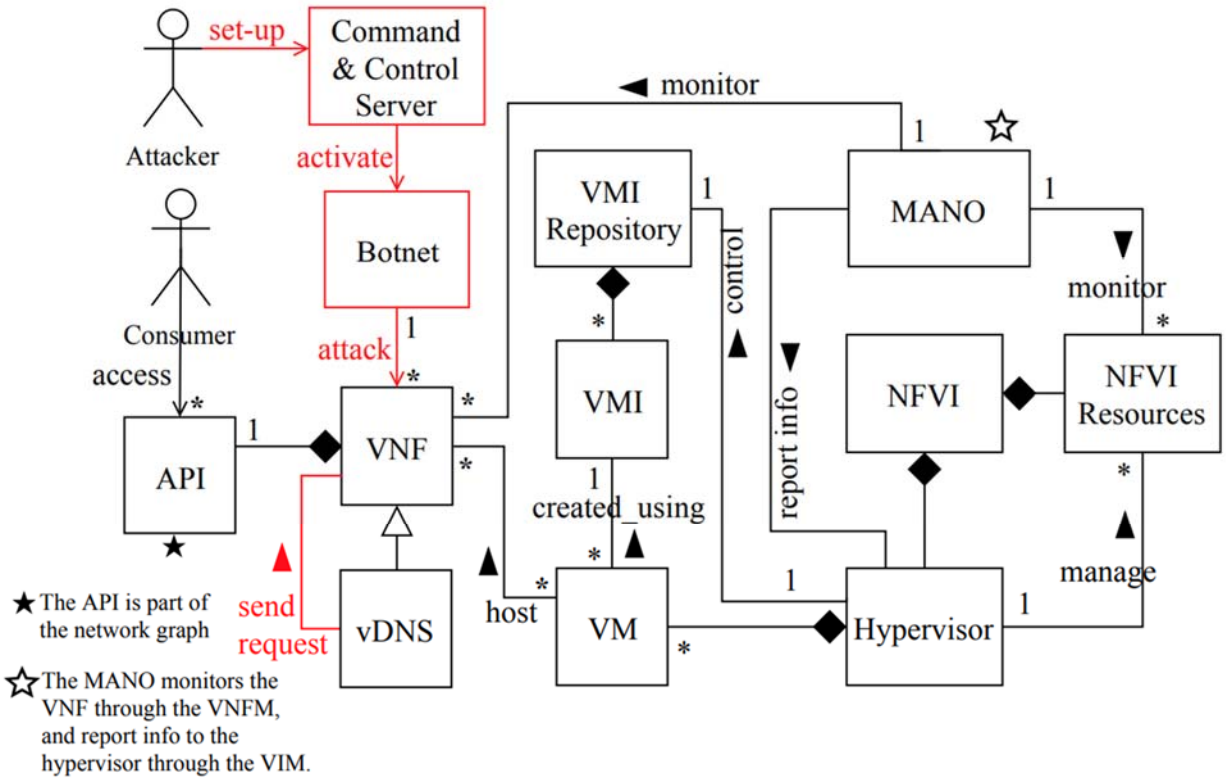

Fig. 3. Class diagram for distributed denial-of-service attack in NFV

2.4.2 Dynamics

Distributed denial-of-service attack in NFV using DNS amplification attack (Fig. 4).

Summary: An attacker uses spoofed IP addresses to send a large number of DNS requests to vDNSs, that in turn send amplified responses to victims, resulting in service unavailability or disruption.

Actor: Attacker

Precondition: The attacker controls a botnet of infected devices and a list of victims' IP addresses.

Description:

1. The attacker first sets up the command and control server (CC) and activates it.
2. Through the command and control server, the attacker sends attack commands to the botnet to launch a high number of DNS requests to a vDNS.
3. Meanwhile, the orchestrator is monitoring the VNF and realizes that the traffic load is higher than the normal threshold, and reports it to the hypervisor.
4. As a response to the high traffic load on the vDNS, the hypervisor initiates additional VMs to scale-up additional vDNSs to accommodate more requests.
5. Accordingly, amplified DNS requests are recursively sent to the victims' web servers, which results in service unavailability or disruption.

Postcondition: Victims' VNFs will be disrupted or become unavailable.

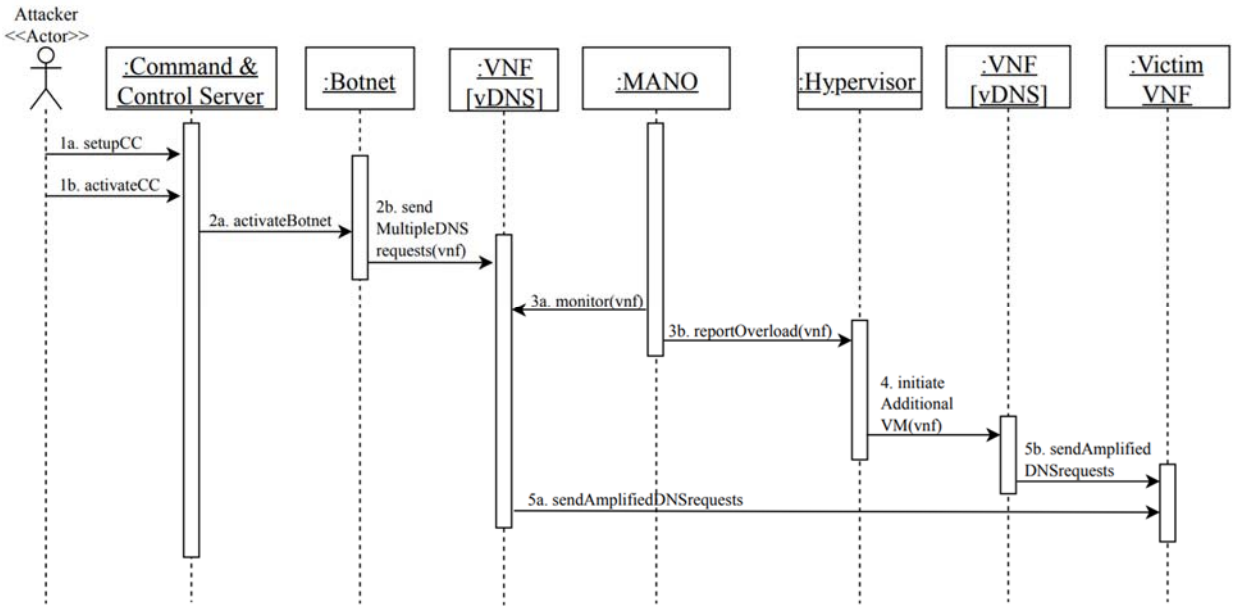

Fig. 4. Sequence diagram for distributed denial-of-service attack in NFV using DNS amplification attack

2.5 Consequences

A successful attack may lead to the following consequences:

1. The network service would be disrupted from legitimate NFV consumers thereby disrupting their operations and web servers.
2. Generally, NFV providers provide network services in a form of subscription-as-a-service business model; the DDoS attacks bring financial losses for NFV providers as NFV consumers will not be able to use the network services during and after the attack.
3. The attacker may be a competitor in the network service market and would try to damage the reputation of the NFV provider as its service has been disrupted and as a consequence it will appear to have security isolation issues.
4. NFV providers may face poblems if the attack leads to making the service unavailable and they would fail to comply with their service level agreement.

2.6 Forensics

1. As long as the attacker uses spoofed IP addresses to perform the DDoS attack, the vDNS will receive the victims' IP addresses, and it might not possible to trace back the attacker in this case.
2. Network traffic analysis may help NFV providers to detect the anomalies in network traffic. The results of these analysis can be used in the future as evidence for future attacks.

2.7 Countermeasures

The attack can be prevented or mitigated using the following countermeasures:

1. NFV providers should use network discovery and automation tools that determine improperly configured network functions and identify potential problems (Pillaipakam, 2016).
2. Apply network behavior analysis tools that monitor network traffic and detect anomalies of high volume of traffic on the network. This measure would just detect the attack, not stop it.
3. Apply packet filtering tools, such as ingress filtering that prevents suspicious inbound traffic from entering the network by examining their source headers, and egress filtering that examines traffics exiting the network and ensures those packets have legitimate source headers. This prevent someone within the network to send malicious traffics using a spoofed IP address (Bass, 2019; Ferguson & Senie, 2000).

4. Spoofed IP addresses normally bypass the basic security mechanisms that rely on IP blacklisting, thus, NFV providers may use Deep Packet Inspection (DPI) that performs analysis of the complete packet headers rather than just the source of the IP addresses (Imperva, n.d.).
5. Using other methods and mechanisms that aim to mitigate and detect the distributed denial-of-service attacks such as (Ahmed, Kim, & Park, 2017), (Tegeler, Fu, Vigna, & Kruegel, 2012), and (Huistra, 2013).
6. If the attack is localized and affects a few VMs they could be shut down.

2.8 Known Uses

Upon until now, there is no DDoS attack in NFV systems known in the literature, but some attacks have happened in cloud and Internet-of-Things (IoT) systems. Therefore, the attack could be possible in NFV systems as long as they are implemented using cloud computing. The following are known attack incidents of DDoS:

1. A major amplification DDoS attack on Memcashed servers with a hit of 1.7 Tbps against undisclosed US service providers (Higgins, 2018).
2. Domain Name Service provider Dyn was hit with a 1.2 Tbps DDoS attack (Schneier, 2016).
3. In September 2016, the website KrebsonSecurity.com was a target of a massive DDoS with traffic hit approximately 665 Gbps (Krebs, 16AD).

2.9 Related Patterns

1. A misuse pattern for DDoS in IoT (Syed et al., 2018): describes a possible scenario of a DDoS attack in an IoT environment.
2. A misuse pattern for NFV-based on Privilege Escalation (Alnaim et al., 2019b): describes a possible scenario of VM privilege escalation threat in NFV environment.
3. A misuse pattern for compromising VMs via virtual machine escape in NFV (Alnaim et al., 2019a): shows how a weak isolation between the hypervisor and its VMs may lead the a VM to escape from the hypervisor control in NFV environment.
4. NFV Virtual Machine Environment (Alnaim, Alwakeel, & Fernandez, 2019c): describes the environment where VMs are created and managed for the purpose of NFV.
5. A pattern for Network Function Virtualization (Fernandez & Hamid, 2015): presents the overall NFV architecture that shows how to create network services using cloud Software-as-a-Service (SaaS) and the general advantages and disadvantages of NFV.

3. CONCLUSIONS AND FUTURE WORK

NFV is a new paradigm that leverages cloud computing and virtualization technologies to offer scalable, isolated, cost and energy efficient network service. These network services are built in software and offered as services. To ensure secure NFV systems, it is important to understand their possible threats.

There are several threats that can jeopardize and slow down the adoption of NFV (Alwakeel et al., 2018). We have presented one of them as a form of misuse pattern, which is a denial-of-service threat. We showed how attackers can take advantage of a botnet to send a high volume of DNS requests to slow or shut-down the victims' web servers.

Our future goal is to build a partial catalog of misuse patterns for NFV system, which is considered the first step toward building a security reference architecture for NFV. The validation of our misuse patterns is not possible in practice because no incidents on NFV systems are known, so our validation is based on defining possible scenarios.

ACKNOWLEDGMENTS

We thank our shepherd Dr. Peng Zhang and Prof. Michael Weiss for their useful comments that helped improve this paper. The participants in the PLoP 2019 Writers' Workshop (Alla Zakurdaeva, Lina Garces, Heil Harrison, Rafael Papa, and Hind Milhem) made valuable comments.

REFERENCES

Ahmed, M. E., Kim, H., & Park, M. (2017). Mitigating DNS query-based DDoS attacks with machine learning on software-defined networking. In *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)* (pp. 11–16). IEEE. https://doi.org/10.1109/MILCOM.2017.8170802

Alnaim, A. K., Alwakeel, A. M., & Fernandez, E. B. (2019a). A Misuse Pattern for Compromising VMs via Virtual Machine Escape in NFV. In *The 14th International Conference on Availability, Reliability and Security (ARES 2019)*. Canterbury, UK.

Alnaim, A. K., Alwakeel, A. M., & Fernandez, E. B. (2019b). A Misuse Pattern for NFV based on Privilege Escalation. In *Proceedings of the 8th Asian Conference on Pattern Languages of Programs*. Tokyo, Japan.

Alnaim, A. K., Alwakeel, A. M., & Fernandez, E. B. (2019c). A Pattern for an NFV Virtual Machine Environment. In *Proceedings of the 13th annual IEEE international systems conference 2019*. Orlando, Florida.

Alwakeel, A. M., Alnaim, A. K., & Fernandez, E. B. (2018). A Survey of Network Function Virtualization Security. In *SoutheastCon 2018* (pp. 1–8). IEEE. https://doi.org/10.1109/SECON.2018.8479121

Bass, S. H. (2019). *Spoofed IP Address Distributed Denial of Service Attacks: Defense-in-Depth*. Retrieved from https://www.sans.org/reading-room/whitepapers/threats/spoofed-ip-address-distributed-denial-service-attacks-defense-in-depth-469

Cloudflare. (n.d.). DNS Amplification DDoS Attack. Retrieved August 9, 2019, from https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/

ETSI. (2014). *GS NFV 002 - V1.2.1 - Network Functions Virtualisation (NFV); Architectural Framework*. Retrieved from https://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf

ETSI. (2015). *GS NFV-INF 004 - V1.1.1 - Network Functions Virtualisation (NFV); Infrastructure; Hypervisor Domain*. Retrieved from https://www.etsi.org/deliver/etsi_gs/NFV-INF/001_099/004/01.01.01_60/gs_nfv-inf004v010101p.pdf

Ferguson, P., & Senie, D. (2000). *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*. https://doi.org/10.17487/rfc2827

Fernandez, E. B. (2013). *Security patterns in practice : designing secure architectures using software patterns*. J. Wiley & Sons, 2013.

Fernandez, E. B., & Hamid, B. (2015). A pattern for network functions virtualization. In *Proceedings of the 20th European Conference on Pattern Languages of Programs* (p. 47).

Higgins, K. (2018). DDoS Amped Up: DNS, Memcached Attacks Rise. Retrieved May 17, 2019, from https://www.darkreading.com/cloud/ddos-amped-up-dns-memcached-attacks-rise/d/d-id/1332041

Huang, D., Chowdhary, A., & Pisharody, S. (2018). *Software-Defined networking and security: from theory to practice*. CRC Press.

Huistra, D. (2013). Detecting Reflection Attacks in DNS Flows. Retrieved from https://www.semanticscholar.org/paper/Detecting-Reflection-Attacks-in-DNS-Flows-Huistra/4ad824537f212f70e25e4cbab55498f5a8e43942

Imperva. (n.d.). IP Spoofing. Retrieved May 17, 2019, from https://www.imperva.com/learn/application-security/ip-spoofing/

Krebs, B. (16AD). KrebsOnSecurity Hit With Record DDoS. Retrieved May 17, 2019, from https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos./

Lal, S., Taleb, T., & Dutta, A. (2017). NFV: Security Threats and Best Practices. *IEEE Communications Magazine*, *55*(8), 211–217. https://doi.org/10.1109/MCOM.2017.1600899

Pillaipakam, D. (2016). Building a Secure DNS Architecture for NFV | Light Reading. Retrieved from https://www.lightreading.com/nfv/nfv-strategies/building-a-secure-dns-architecture-for-nfv/a/d-id/720711

Schneier, B. (2016). Lessons From the Dyn DDoS Attack. Retrieved May 17, 2019, from https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html

SecurityTrails. (2018). 8 tips to prevent DNS attacks. Retrieved from https://securitytrails.com/blog/8-tips-to-prevent-dns-attacks

Syed, M. H., Fernandez, E. B., & Moreno, J. (2018). A misuse Pattern for DDoS in the IoT. In *Proceedings of the 23rd European Conference on Pattern Languages of Programs - EuroPLoP '18* (pp. 1–5). New York, New York, USA: ACM Press. https://doi.org/10.1145/3282308.3282343

Tegeler, F., Fu, X., Vigna, G., & Kruegel, C. (2012). BotFinder: Finding Bots in Network Traffic Without Deep Packet Inspection. In *Proceedings of the 8th international conference on Emerging networking experiments and technologies - CoNEXT '12* (p. 349). New York, New York, USA: ACM Press. https://doi.org/10.1145/2413176.2413217

APPENDIX

1- TEMPLATE FOR MISUSE PATTERNS (FERNANDEZ, 2013)

In this section, we show the template used in this paper to describe the misuse pattern.

Name

The name of the misuse pattern should correspond to the generic name given to the specific type of threat in standard attack repositories.

Intent
A short description of the intended purpose of the pattern (what problem it solves for an attacker).

Context
It describes the generic environment including the conditions under which the attack may occur. This may include minimal defenses present in the system as well as standard vulnerabilities of the system.

Problem
From an attacker's perspective, the problem is how to find a way to attack the system. The forces indicate what factors may be required in order to accomplish the attack and in what way; for example, which vulnerabilities can be exploited.

Solution
This section describes the solution of the attacker's problem, i.e., how the attack can reach its objectives and the expected results of the attack. UML class diagrams show the system units involved in the attack. Sequence or collaboration diagrams show the exchange of messages needed to accomplish the attack.

Structure (where to look for evidence, targets)
The pattern should indicate in the UML class diagram the role of all components that are involved in the attack. From a forensic viewpoint, this section describes what information can be obtained at each stage tracing back the attack and what can be deduced from this data.

Dynamics
The pattern should include sequence or collaboration diagrams to show the exchange of messages needed to accomplish the attack.

Consequences for the attacker
Discusses the benefits and drawbacks of a threat pattern from the attacker's viewpoint. The enumeration includes good and bad aspects and should match the forces.

Forensics
From a forensic viewpoint, this section describes what information can be obtained at each stage tracing back the attack. It also may indicates what additional information should be collected at the involved units to improve forensic analysis

Countermeasures
Describes the security measures necessary in order to stop, mitigate, or trace this type of attack. This implies an enumeration of which security patterns or other practical measures are effective against this attack.

Known uses
List of the security incidents where the attack has already occurred.

Related Patterns
Discusses other misuse patterns with different objectives but performed in a similar way or with similar objectives but performed in a different way.

2- ACRONYMS

CC	Command and Control Server
DDoS	Distributed Denial-of-Service
DNS	Domain name server
vDNS	virtual Domain name server
DoS	Denial-of-Service
DPI	Deep Packet Inspection
ETSI	The European Telecommunications Standards Institute
IoT	Internet of Thinks
MANO	Management and Orchestration
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
POSA	Pattern Oriented Software Architecture
RA	Reference Architecture
SaaS	Software-as-a-Service
SRA	Security Reference Architecture
TSP	Telecommunication Service Provider
UDP	User Datagram Protocol
VIM	Virtualization Infrastructure Manager
VM	Virtual Machine
VMI	Virtual Machine Image
VNF	Virtual Network Function

3- GLOSSARY

DNS	A hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet that translates human readable domain names to machine readable IP addresses.
DoS	A cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.
NFV	The service to be provided to the user to provide virtual network services.
NFVI	One of the NFV components where the physical resources are used to build virtual network services.
RA	A generic and abstract software architecture used to understand, analyze, and design complex systems at the highest level of abstraction. It specifies system components, their functionalities, and their mutual interactions, but it does not contain implementation details.
TSP	A telecommunications service provider is a type of communication service provider that provides networking solution.
	MANO An NFV unit takes care of controlling and managing the NFV system.
VM	An emulation of a computer system and its functionality.
VIM	One of MANO functional block that manages and controls the infrastructure in NVF systems.
VNF	Are virtual implementations of network functions.