INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2019, VOL. 65, NO. 4, PP. 571-577
Manuscript received September 26, 2019; revised September, 2019. DOI: 10.24425/ijet.2019.129814

Network Topology Mutation as Moving Target Defense for Corporate Networks

Mariusz Rawski

***Abstract*—The paper introduces a topology mutation – the novel concept in Moving Target Defense (MTD). MTD is a new technique that represents a significant shift in cyber defense. Traditional cybersecurity techniques have primarily focused on the passive defense of static networks only. In MTD approach cyber attackers are confused by making the attack surface dynamic, and thus harder to probe and infiltrate. The emergence of Network Functions Virtualization (NFV) and Software-Defined Networking (SDN) technology has opened up new possibilities in network architecture management. The application of combined NFV and SDN technologies provides a unique platform for implementing MTD techniques for securing the network infrastructure by morphing the logical view of the network topology.**

***Keywords*—Cybersecurity, MTD, SDN, NFV**

I. Introduction

FROM the cyber attacker's perspective, a network attack is intendent to locate and analyze the targeted system and to find out the existence of vulnerability in network resources. Every such a vulnerability opens cyber-threat vector (attack vector) and makes security operations more complex. The totality of all vulnerabilities in a system forms the attack surface. After attack vectors are identified, attackers take intrusive actions to gain access to the system resources.

An adversary who conducts cyber-attacks frequently follows this methodology, performing an extensive survey of their target organization. This integrated, end-to-end process is described as a cyber kill-chain, a widely accepted, multistage segmental type intrusive model proposed by Lockheed Martin cooperation in [1].

Most computer networks have the static nature. This gives an attacker great advantage – time. Adversaries are able to perform network reconnaissance and identify vulnerabilities, which can be exploited by identifying potential targets and their vulnerabilities [2]. An insider adversary may use highly effective scanning strategies for network reconnaissance. By probing networked environments an attacker is able to identify hosts and open ports and map their topology to find known and zero-day vulnerabilities to perform further attack manoeuvres. In fact, previous studies have shown that entire topologies can be precisely mapped with *traceroute* provided enough probing points are used [3].

Moving Target Defense (MTD) has emerged as a solution to deal with security issues associated with the static nature of computer networks. This is one of the most promising trends in cyber defense. In this approach cyber attackers are confused by making the attack surface dynamic, and thus harder to probe and infiltrate. It represents a significant shift in the cyber defense, which has primarily focused on the passive defense of static networks. In the past few years, MTD developed rapidly and a large number of concepts and approaches have been proposed. In [4] an overview of different cyber moving-target techniques, their threat models, and technical details are presented.

The ways to design, build and operate networks have changed with the emergence of Network Functions Virtualization (NFV) and Software-Defined Networking (SDN) technology. These trends are transforming network management and make it possible to propose new sophisticated MTD-based techniques. Together, SDN and NFV technologies are making it easier to provision network resources, enabling greater network flexibility, dynamic network deployment with fast instantiation, support for Commercial-Off-The-Shelf (COTS) hardware and significant cost savings. These technologies allow creating virtualized network architectures (built of physical and virtual network components), that can be shaped and changed according to the needs.

The paper discusses the application of the NFV and the SDN technology to provide a unique platform for implementing the novel MTD technique – topology mutation. The concept is based on creating virtualized network architecture, that is morphed in time by dynamic introduction of virtual components and rearranging logical structure of the network.

II. Preliminary Information

A. Software-Defined Networking

The Software-Defined Networking (SDN) is a networking technology developed in 2008. SDN is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services. The control plane is logically centralized (in small scale implementations a single SDN controller is in use) and the control plane entity, i.e. the SDN Controller, is a software entity. The data planes entities can be hardware or software-based ones. The OpenFlow protocol is a foundational element for building SDN solutions, since it provides the basic interaction between the data plane and control plane.

B. Network Functions Virtualization

Network Function Virtualization (NFV) is a term used to represent the implementation of data-plane network functions in software, that is executed on commodity hosts [5]. It allows for

The work has been partly supported by The Polish National Centre for Research and Development under project No. CYBERSECIDENT/381219/ll/NCBR/2018.

The Author is with Warsaw University of Technology, Institute of Telecommunications, Poland (e-mail: m.rawski@tele.pw.edu.pl)

dynamic deployment of networking solutions that are made in software. NFV is designed to consolidate and deliver the networking components needed to support an infrastructure totally independent from hardware. These components include virtual compute, storage and network functions. NFV utilizes standard IT virtualization technologies that run on off-the-shelf hardware like commodity servers. It is applicable to any data plane processing or control plane function in both wired and wireless network infrastructures. The architectural components of NFV are Network Function Virtualization Infrastructure (NFVI) and Network Functions (NFs). NFVI consists of hardware (a single computer or a compute cluster), and framework software, which offers functions that are commonly required by NFs, such as NF placement, dynamic scaling, etc. Data-plane network functions considered for software implementation in commodity hosts range from basic packet forwarding (i.e. Open vSwitch – OVS) to complex middlebox functions such as intrusion detection and prevention systems. When NFs are executed on Virtual Machines (VMs), they are referred to as Virtual Network Functions (VNFs).

C. NFV management and network orchestration

NFV changes the way networks are managed. The management role is performed by NFV management and network orchestration (MANO) framework. NFV MANO is a concept developed by a working group within the European Telecommunications Standards Institute (ETSI). Its responsible for the management and orchestration of all resources in a virtualized environment including compute, networking, storage, and virtual machine (VM) resources. The main focus of NFV MANO is to allow flexible on-boarding of network components.

NFV MANO is broken up into three functional blocks:

- NFV Orchestrator – controls on-boarding of new VNF; manages VNF lifecycle and global resources; validates NFVI resource requests,
- VNF Manager – supervises lifecycle management of VNF instances; coordinates configuration and event reporting between NFVI and Element/Network Management Systems.
- Virtualized Infrastructure Manager (VIM) – controls and manages the NFVI compute, storage, and network resources.

III. Related Work

A. Moving Target Defense

From the cyber security perspective, the system can be described using the concept of the attack surface [6] and exploration surface [7] (Fig. 1a). The exploration surface is a space that attacker must explore or recon to determine the configuration of the target system before launching the actual attack. While the attack surface is formed by all of the different points, where an attacker could get into a system and is a concept to indicate the exploitable components in a system.

Creating a more secure system usually is achieved by hardening it, i.e. closing unused ports, removing unneeded software or using the most current versions of software. This reduces the attack surface (Fig. 1b). The more advanced hardening techniques modify the attack surface at runtime in response to recognized threads, identified by intrusion detection systems (IDS), and reactively launch automated responses (Fig. 1c). The effectiveness of advanced hardening techniques is limited by the large number of false alarms from the IDS that can disrupt normal system operations. In addition, these techniques are ineffective against new and zero-day attacks.

Instead of focusing on reducing the attack surface, MTD approaches seek to enlarge the exploration surface and move the attack surface at runtime to force the attacker to re-explore the exploration surface (Fig. 1d). The goal of an MTD techniques is to eliminate the attacker's asymmetric advantage of time by deploying proactive mechanisms.

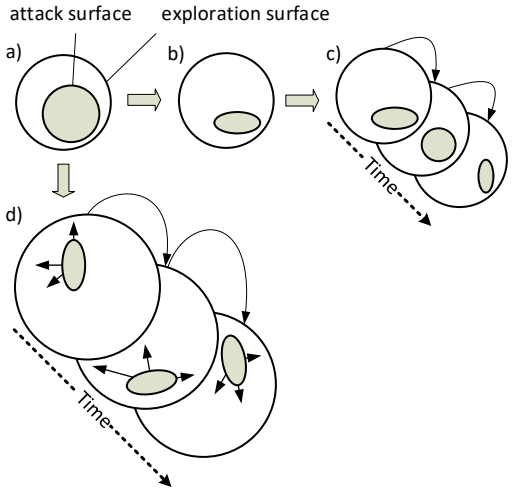

Fig. 1. Demonstration of MTD concept

Moving Target Defense is one of the most effective defense strategies to increase the attackers' costs. The concept of MTD was proposed at first at the U.S. National Cyber Leap Year Summit in 2009. MTD has been defined as an approach that enables creating, analyzing, evaluating and deploying mechanisms and strategies, that are diverse and that continually shift and change over time to increase complexity and cost for attackers, limit the exposure of vulnerabilities and opportunities for attack, and increase system resiliency. A cyber MTD technique refers to any technique that attempts to defend a system and increase the complexity of cyber-attacks by making the system less homogeneous, static, or deterministic [8]. A comprehensive survey of cyber MTD techniques have been presented in [4].

B. The Dynamic Networks

The Dynamic Networks are one of five categories of MTD techniques [4]. Methods belonging to Dynamic Network MTD (DN-MTD) strive to break the static nature of a network by adding uncertainties and pursuing frequent changes of network states which make it harder for attackers to obtain the network states for launching attacks. The network-based MTD includes techniques that dynamically vary network aspects of a distributed computer network system. Any aspect providing network connectivity and enabling system transactions across multiple computing platforms is a candidate for MTD techniques.

Example techniques included in this class are dynamic IP address assignment and/or port randomization [9] [10], host and rout mutation [11], protocol-obfuscation techniques [12] and proxy-location randomization [13]. The fundamental idea for

these techniques is periodically changing the structure of the network an adversary must use to access resources or data in the protected computer network system

C. The SDN/NFV-based MTD

In modern approaches NFV and SDN are commonly used together, however, they are different and serve different goals [14]. NFV aims at moving network services (switches, firewalls, IDS, etc.) away from dedicated hardware into a virtualized environment. SDN separates the network's control and forwarding planes, thus enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications. When SDN is combined with NFV, SDN's centralized management can forward traffic from one network device to another, while NFV allows network device function (routing control, security or monitoring) to run on a VM or a container located in network server. Software Defined Networking and Network Function Virtualization provide excellent opportunities to implement MTD mechanisms efficiently.

The combination of these techniques has been used in [15] to propose SDN/NFV-based moving target DDoS defense mechanism using multiple fuzzy systems and a proxy virtual network function (VNF) to achieve DDoS detection and mitigation. In [16] virtual shadow networks through NFV have been proposed to be used when implementing MTD mechanisms via route mutation. The idea was to dynamically change the routes for specific reconnaissance packets, so that attackers cannot be able to identify the actual network topologies for potential DDoS attacks, while enabling the defender to store potential attacker's information through a forensics feature. Another MTD method that uses SDN and NFV has been proposed in [17]. To implement additional defenses against penetration attack the decoy chains are deploy in the network for changing the attack. The SHIELD framework [18] applies NFV/SDN for virtualization and dynamic placement of virtualized security functions in the network. In combination with Big Data analytics it allows for real-time incident detection and mitigation.

IV. Network Topology Mutation

A. Virtualized network

The methods proposed in literature so far use NFV to extend the existing network with additional elements (honey networks, security functions) and SDN to dynamically change the routes for selected traffic identified as malicious or to provide Security-as-a-Service.

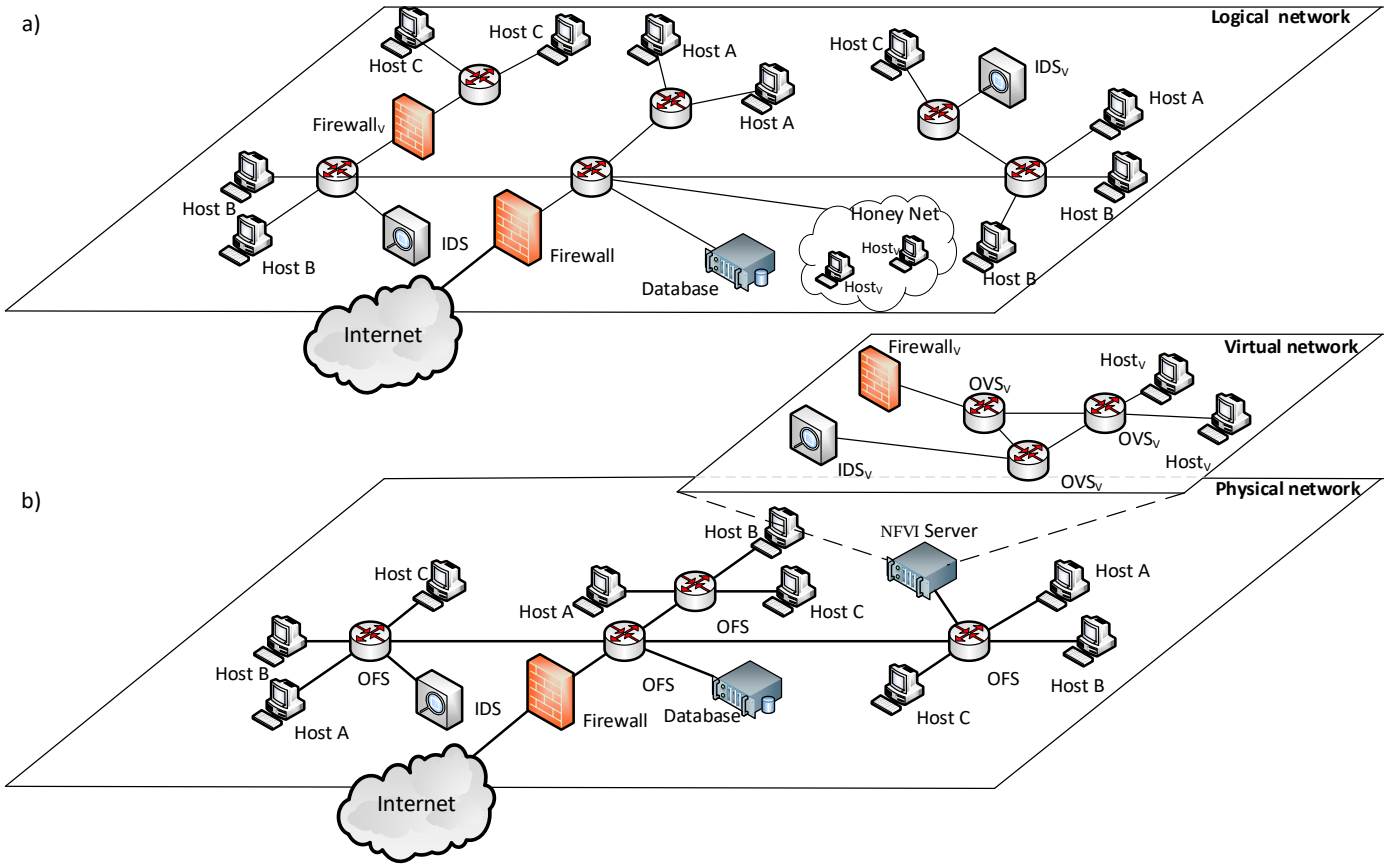

Fig. 2. Application of SDN/NFV to create virtualized network: a) logical network topology, b) corresponding physical and virtual components of the network

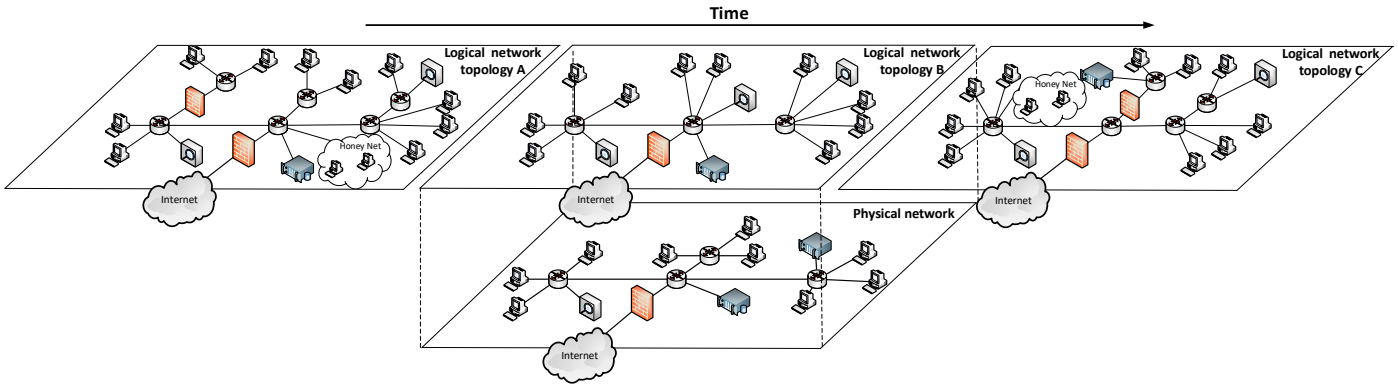

Fig. 3. Using virtualized network to change topology over time

However these technologies allow creating virtualized network architectures (built of physical and virtual network components), that can be shaped and changed according to the needs. If network is expanded with a dedicated server running software for deployment, scaling, and management of virtualized network functions to introduce NFVI infrastructure, it allows creating virtualized network (Fig. 2b). NFVI allows creating virtual network elements in form of VNFs and SDN mechanisms make it possible to integrate these elements into a network. This creates logical topology of the network, that can be flexibly shaped (Fig. 2a).

Application of NFV management and orchestration mechanisms allows to automate the process of moving from one virtualized network instance (logical network) to another. This makes it possible to implement completely new MTD technique that is based on changing virtualized network over time, by moving from one logical network topology to another (Fig. 3).

B. *Overview of the concept*

The general concept of the network topology mutation system is presented in Fig. 4. The system consists of four key components:

- **Virtualized Network (VN)** – the concept assumes that the protected network is virtualized, i.e. is SDN-capable and equipped with NFVI,
- **Network Topology Management (NTM)** – responsible for automated logical topology reconfiguration according to provided specification,
- **Network Monitoring (NM)** – collects and analyzes network status information,
- **Topology Mutation Control (TMC)** – decides about changes in logical topology and when the change will be performed.

1) *Virtualized Network*

Virtualized network consists of physical components, such as hosts, servers, SDN network switching elements. It also contains a dedicated NFVI, that allows to deploy and manage virtualized NFs. There are many solution available, that can be used to achieve NFVI functionality: commercial (i.e. Cisco NFV Infrastructure, VMware vCloud NFV virtualization platform), as well opensource (OpenStack, Kubernetes). NFVI is controlled by NTM module to instantiate VNFs necessary to create desired logical network topology (Fig. 2b). SDN network switching elements are controlled by SDN Controller to provide required connectivity.

2) *Network Topology Management*

NTM is composed of SDN Controller and NFV Management and Orchestration (MANO). NTM module's role is to reconfigure logical topology of VN according to provided topology description. The description of the logical topology can be provided for example in Topology and Orchestration Specification for Cloud Applications (TOSCA). TOSCA is an open-source language used to describe the relationships and dependencies between services and applications that reside on a cloud computing platform.

MANO is responsible for instantiation of VNFs required to create desired topology. This mechanism is based on three Managers:

- Virtualized Infrastructure Manager (VIM) – manages life cycle of virtual resources in an NFVI domain; it creates, maintains and tears down virtual machines (VMs) from physical resources in an NFVI domain, keeps inventory of VMs associated with physical resources, is responsible for performance and fault management of hardware, software and virtual resources, keeps north bound APIs and exposes physical and virtual resources to other management systems,
- VNF Manager (VNFM) – manages life cycle of VNFs, it creates, maintains and terminates VNF instances (installed on the VMs created and managed by VIM), is responsible for the FCAPS of VNFs, scales up/down VNFs (scaling up/down of CPU usage),
- NFV Orchestrator (VNFO) – coordinates, authorizes, releases and engages NFVI resources by controlling the VIMs through their north bound APIs, creates end to end service among different VNFs

SDN Controller is responsible for configuring SDN switching elements (physical and virtual) to direct network flows in such a way, that physical and virtual parts of the network are integrated to form desired logical topology.

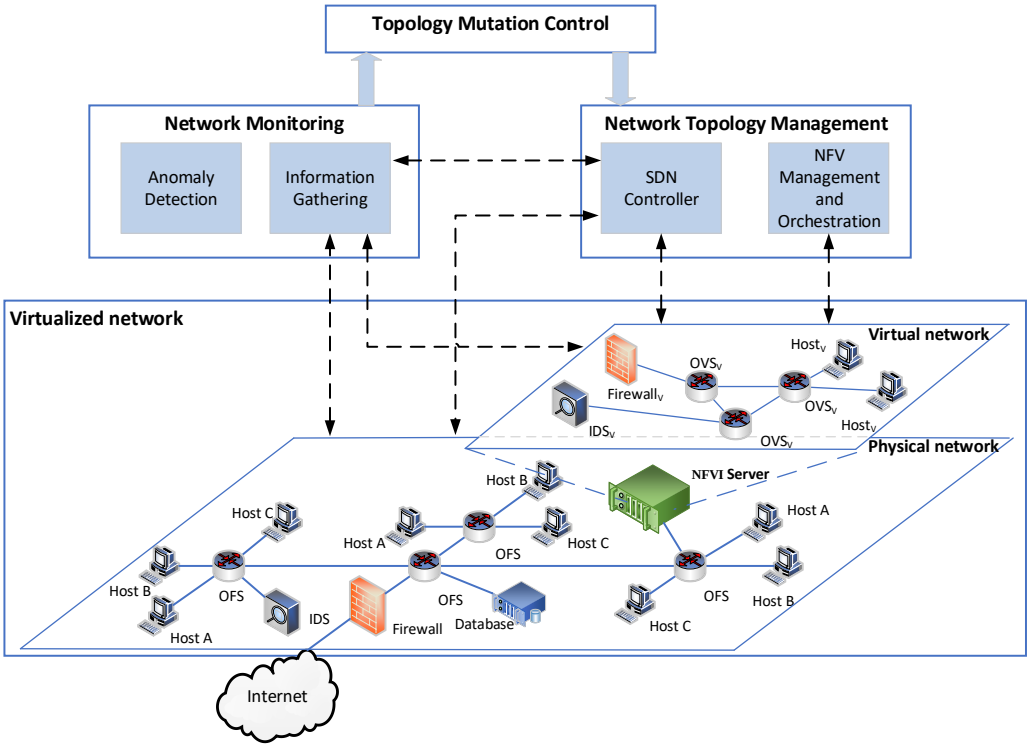

Fig. 4. Schematic representation of network topology mutation system

3) Network Monitoring

NM collects from the network information, that can be used to asses security level. The information can be gathered from network security elements (physical or virtual), such as IDS, firewalls, system log analyzers, as well as from SDN Controller, that can provide information about network flows. This data is then used by anomaly detection algorithms to identify suspicious activity. A number of techniques, such as machine learning or data mining, can be used to support network monitoring.

4) Topology Mutation Control

TMC is responsible for selecting new network logical topology and generating topology specification required by NTM. The logical topology can be changed periodically or can be triggered by NM. TMC may select next logical topology from the set of precomputed configuration or generate one as response to thread identified by NM.

V. MTD Using Network Topology Mutation

A. Threat Model

According to a cyber kill-chain model, adversaries start an attack on a computer network by collecting as much information about the network as they can. Attackers identify the vulnerable elements of the network and then they connect to those vulnerable hosts and send attack payloads. Therefore, we considered the threat from reconnaissance phase for both direct and indirect attacks. We consider insider adversaries who have placed themselves in the network (on one or more hosts), using techniques such as social engineering, exploiting zero-day vulnerabilities, via drive by downloads or by manual infection.

The proposed solution aims at creating a dynamic and variable network with logical topology changing over time, so as to make reconnaissance attacks on a target system much more complex and costly for attackers. We assume, that an attacker can scan a network and monitor the network traffic to acquire topology knowledge. Moreover, the adversary can eavesdrop network packets.

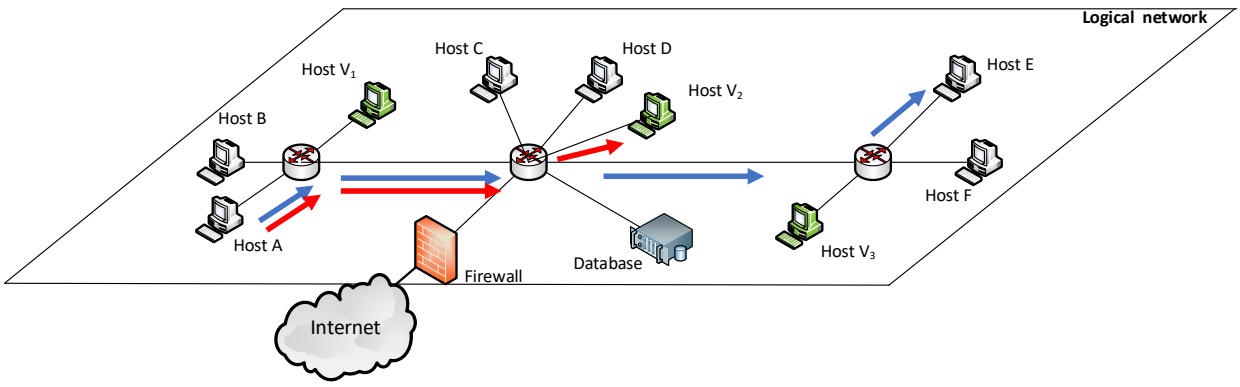

Fig. 5. Logical topology LT$_1$

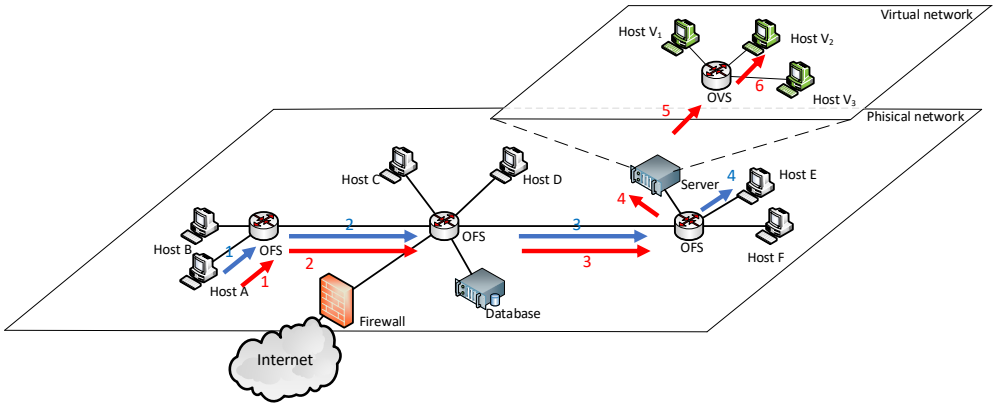

Fig. 6. Virtualized network configuration for LT_1

B. *MTD Strategies*

Topology mutation system (TMS) allows implementing wide range of MTD strategies. Simple one are based on introduction virtual components in form of Honeypots or more complex Honey Nets. Fig. 5 presents the logical topology LT_1 of a network, where 3 virtual Honeypots have been introduced.

To achieve this TMS has to create virtual hosts and virtual OVS switch in virtual part of the network. Appropriate flow rules have to be installed by SDN Controller at switches (physical and virtual). This can be done in a proactive approach, where the controller installs flow rules in advance for every host at every switch as the network gets configured. Fig. 6 shows the configuration of virtualized network to achieve logical topology LT_1.

More complex scenarios may involve deeper rearrangement of the network topology. Fig. 7 presents the logical topology LT_2 of a network, where except that 3 virtual Honeypots and a virtual firewall were added, network segments have been rearranged. For example host E previously belonging to the segment of the network containing host F now has been moved to segment containing host A. Moreover hosts C, D and virtual host V_2 have ben placed behind the firewall.

To achieve this, appropriate NVFs have to instantiated using NFVI infrastructure and flow rules have to be installed by SDN Controller at switches (Fig. 8). However, to imitate topology LT_2, TMS system must assign different network views to all nodes in a network. Network view is how a network looks from the perspective of given network node. This can be done by appropriate handling protocols used for network discovery (i.e. ARP, ICMP) by SDN switches and SDN Controller.

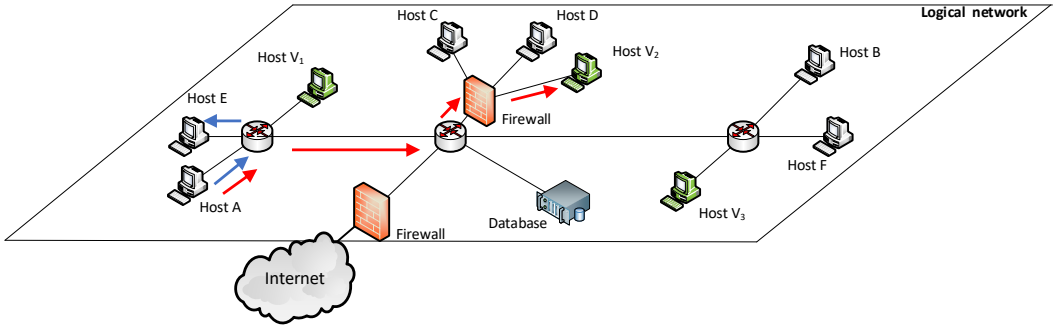

Fig. 7. Logical topology LT_2

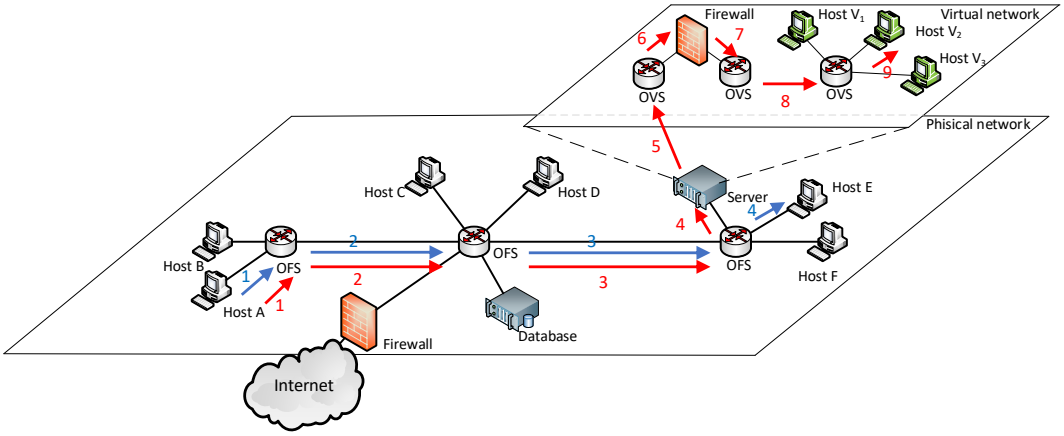

Fig. 8. Virtualized network configuration for LT_2

MTD strategies implemented using presented approach may assume periodic changes in logical topology, where next topology configuration is selected from a set of precomputed configuration. The frequency of changes may depend on a security level indicated by the network monitoring subsystem. Frequent changes will confuse an attacker performing reconnaissance of the network.

More sophisticated strategies may involve rearrangement of a logical network topology triggered by NM as a response to anomaly detected in the network. Logical network topology may be configured according to more detailed information about network security state. This may include introduction of additional virtual network security elements, such as IDS or firewalls, into network segments indicated by NM as being the source of suspicious traffic or activity.

CONCLUSION

The paper presents the novel concept of Moving Target Defense – topology mutation. Modern technologies, such as SDN, NFV and MANO provide sufficient functionalities to implemented proposed concept. There are commercial, as well as opensource solutions available, that may be used to create the described MTD system. A deception approach based on presented concept is outlined as a defense strategy against network reconnaissance. The topology mutation opens up the possibility to implement very sophisticated defense and deception strategies.

REFERENCES

[1] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Proc. 6th Int. Conf. Inf. Warf. Secur.*, 2011.

[2] S. A. Shaikh, H. Chivers, P. Nobles, J. A. Clark, and H. Chen, "Network reconnaissance," *Netw. Secur.*, 2008.

[3] N. Spring, R. Mahajan, D. Wetherall, and T. Anderson, "Measuring ISP Topologies With Rocketfuel," *IEEE/ACM Trans. Netw.*, 2004.

[4] B. C. Ward *et al.*, "Survey of Cyber Moving Targets Second Edition," 2018.

[5] M. Veeraraghavan, T. Sato, M. Buchanan, R. Rahimi, S. Okamoto, and N. Yamanaka, "Network Function Virtualization: A Survey," *IEICE Trans. Commun.*, vol. E100.B, no. 11, pp. 1978–1991, 2017.

[6] P. K. Manadhata and J. M. Wing, "An Attack Surface Metric," *IEEE Trans. Softw. Eng.*, vol. 37, no. 3, pp. 371–386, May 2011.

[7] R. Zhuang, S. A. DeLoach, and X. Ou, "Towards a Theory of Moving Target Defense," *Proc. First ACM Work. Mov. Target Def. - MTD '14*, pp. 31–40, 2014.

[8] "NITRD's Cyber Security and Information Assurance Interagency Working Group (CSIA IWG)." [Online]. Available: https://www.nitrd.gov/cybersecurity/. [Accessed: 04-Apr-2019].

[9] S. Achleitner, T. F. La Porta, P. McDaniel, S. Sugrim, S. V Krishnamurthy, and R. Chadha, "Deceiving Network Reconnaissance Using SDN-Based Virtual Topologies," *IEEE Trans. Netw. Serv. Manag.*, vol. 14, no. 4, pp. 1098–1112, Dec. 2017.

[10] E. Al-Shaer, Q. Duan, and J. H. Jafarian, "Random Host Mutation for Moving Target Defense," Springer, Berlin, Heidelberg, 2013, pp. 310–327.

[11] Q. Duan, E. Al-Shaer, and H. Jafarian, "Efficient random route mutation considering flow and network constraints," *2013 IEEE Conf. Commun. Netw. Secur. CNS 2013*, pp. 260–268, 2013.

[12] D. Kewley, R. Fink, J. Lowry, and M. Dean, "Dynamic approaches to thwart adversary intelligence gathering," in *Proceedings DARPA Information Survivability Conference and Exposition II. DISCEX'01*, vol. 1, pp. 176–185.

[13] Q. Jia, K. Sun, and A. Stavrou, "MOTAG: Moving target defense against internet denial of service attacks," in *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, 2013.

[14] D. Huang, A. Chowdhary, and S. Pisharody, "SDN and NFV," in *Software-Defined Networking and Security*, First edition. | Boca Raton, FL : CRC Press/Taylor & Francis Group, 2018. | Series: Data-enabled engineering: CRC Press, 2018, pp. 81–108.

[15] C.-C. Liu, B.-S. Huang, C.-W. Tseng, Y.-T. Yang, and L.-D. Chou, "SDN/NFV-Based Moving Target DDoS Defense Mechanism," 2019, pp. 548–556.

[16] A. Aydeger, N. Saputro, and K. Akkaya, "A moving target defense and network forensics framework for ISP networks using SDN and NFV," *Futur. Gener. Comput. Syst.*, vol. 94, pp. 496–509, May 2019.

[17] Q. Zhao, C. Zhang, and Z. Zhao, "A decoy chain deployment method based on SDN and NFV against penetration attack.," *PLoS One*, vol. 12, no. 12, p. e0189095, 2017.

[18] G. Gardikis *et al.*, "SHIELD: A novel NFV-based cybersecurity framework," in *2017 IEEE Conference on Network Softwarization: Softwarization Sustaining a Hyper-Connected World: en Route to 5G, NetSoft 2017*, 2017.