# Virtualizing and Utilizing Network Security Functions for Securing Software Defined Infrastructure

Hongxin Hu[†], Gail-Joon Ahn[‡]
[†]Clemson University [‡]Arizona State University

## 1 Introduction

In traditional networks, network security functions, such as firewall and IDS/IPS, are generally implemented on vendor proprietary appliances or *middleboxes*. However, middleboxes usually lack a general programming interface, and their flexibility and versatility are also very limited. On the other hand, traditional hardware-based security functions feature *fixed* location and capacity, since they are often placed at fixed network entry points and have a constant capacity with respect to the maximum amount of traffic they can process. Such a nature of hardware-based security functions renders them awkward in protecting emerging Software Defined Infrastructure (SDI), which enables *programmable* and *virtualizable* environments. First, the perimeter of a network in virtualized environments becomes fluid, as VMs and applications may span across racks within a data center and across multiple data centers, and they are often migrated for the purpose of flexible resource management and optimization. Second, VMs and applications in cloud today can elastically scale to handle workload variations. This requires that the network security functions protecting them must scale in a similar fashion. Third, traditional network security functions are often large appliances that protect entire security zones/domains. However, in programmatic and virtualized environments, service providers need to instantiate smaller, dedicated virtual security functions tailored to protect specific security zones/domains. In addition, traditional hardware-based security appliances often work *individually* with *static* configuration. However, SDI envisions a *multi-domain* and *multi-tenant* Software Defined Exchange (SDX) infrastructure, which requires *interoperable*, *dynamic* and *reconfigurable* network security functions.

To address above security challenges and requirements introduced by emerging SDI, we propose a new security framework, Network Security Function Virtualization (NSFV), which virtualizes and utilizes network security functions to secure SDI. NSFV enables following secure features for protecting SDI: (1) ***Security Elasticity***. Based on Network Function Virtualization (NFV) technique, NSFV implements network security functions as software instance (a.k.a *virtual* network security function) that can be quickly instantiated and elastically scaled to deal with attack traffic variations toward flexible and on-demand placement of virtual network security functions. To achieve safe, efficient and optimal elasticity control, NSFV will address a number of key challenges with respect to *safe migration*, *semantic consistency*, *correct flow update*, and *optimal provision* in virtual security function control. (2) ***Security Automation***. NSFV virtualizes three types of network security functions: (i) attack prevention functions (e.g. firewalls and IPS); (ii) attack detection functions (e.g. IDS, scan and DDoS detector); and (iii) attack capturing function (e.g. honeypot). In particular, NSFV provides a centralized security function controller to enable *dynamic interoperation* and *automatic reconfiguration* of virtual security functions. For example, virtual honeypots can capture attacks, learn and generate attackers' patterns, and then send the patterns to virtual IDSs. Virtual IDSs can then reconfigure their detectors based on the new or updated attack patterns. When virtual IDSs detect malicious behaviors, they can either redirect malicious traffic to virtual honeypots for further monitor or notify virtual firewalls to update their configuration and block traffic. Moreover, NSFV will address more comprehensive interoperation of security functions with respect to multi-domain and multi-tenant SDX infrastructure. (3) ***Security as a Service (SaaS)***. NSFV provides virtual network security functions as services that can be automatically provisioned and dynamically migrated based on real-time security requirements. Especially, a high-level service-oriented security language will be investigated to enable users to readily specify security requirements, and defined security service chains and interoperation based on SDI/SDX abstraction.

Both Clemson University (CU) and Arizona State University (ASU) are building up campus-wide research computing infrastructures. For example, CU has Clemson NextNet and is part of a consortium of universities to build CloudLab. ASU has also built ASU Science DMZ. Both SDN and NFV will play a vital role to establish such critical research/educational infrastructures. Our research effort will focus on security and robustness challenges of such SDN-NFV centric infrastructures.

## 2 Preliminary Work

We have introduced a *FlowGuard* framework for building robust firewalls for Software-Defined Networks (SDNs) [1]. We also presented a stateful forwarding abstraction for SDN data plane [2] and integrated it with NFV [3]. Most recently, we proposed VNGuard, which is an NFV/SDN combination framework for provisioning and managing virtual firewalls [4], leveraging CloudLab as our testbed platform.

## 3 Team Member

Dr. **Hongxin Hu**, from Clemson University, has worked on a couple of projects related to SDN and NFV security. He is especially working on building various virtual network security functions including virtual firewalls and virtual IDSs. He just started organizing an ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization (http://honeynet.asu.edu/sdnnfvsec2016/). Dr. **Kuang-Ching Wang** is the Networking CTO of Clemson University. He is leading an NSF's CC-NIE project called Clemson NextNet and as a Co-PI for NSF CloudLab project. Dr. **Gail-Joon Ahn**, from Arizona State University, has been working on various areas related to network and system security. He is currently serving on the Research Computing (RC) committee at ASU, which has SDN deployed with OpenDaylight & OpenFlow (Linux Foundation) currently. He also serves as a general chair of ACM SDN-NFV Security'16 workshop.

All team members wish to be reimbursed to attend this NSF SDI workshop.

## References

[1] H. Hu, W. Han, G. Ahn and Z. Zhao, "FlowGuard: Building Robust Firewalls for Software-Defined Networks," in *HotSDN'14*.
[2] S. Zhu, J. Bi, C. Sun, C. Wu and H. Hu, "SDPA: Enhancing Stateful Forwarding for Software-Defined Networking ," in *ICNP'15*.
[3] J. Bi, S. Zhu, G. Yao, C. Sun and H. Hu, "Supporting Virtualized Network Functions with Stateful Data Plane Abstraction ," *IEEE Network*, 2015.
[4] J. Deng, H. Hu, H. Li, Z. Pan, KC. Wang, G. Ahn, J. Bi and Y. Park, "VNGuard: An NFV/SDN Combination Framework for Provisioning and Managing Virtual Firewalls," in *NFV-SDN'15*.