COLLEGE OF ENGINEERING AND COMPUTER SCIENCE
FLORIDA ATLANTIC UNIVERSITY

Announces the Ph.D. Dissertation Defense of

Abdulrahman K. Alnaim

for the degree of Doctor of Philosophy (Ph.D.)

"Towards a Security Reference Architecture for Network Function Virtualization"

February 27, 2020, 12:00 A.M.
Engineering East, Room 405
777 Glades Road
Boca Raton, FL

DEPARTMENT:
Computer and Electrical Engineering & Computer Science

ADVISOR:
Eduardo B. Fernandez, Ph.D.

PH.D. SUPERVISORY COMMITTEE:
Mohammad Ilyas, Ph.D.,
Shihong Huang, Ph.D.
Imadeldin Mahgoub, Ph.D.

ABSTRACT OF DISSERTATION
Towards a Security Reference Architecture for Network Function Virtualization

Network Function Virtualization (NFV) is an emerging technology that transforms legacy hardware-based network infrastructure into software-based virtualized networks. Instead of using dedicated hardware and network equipment, NFV relies on cloud and virtualization technologies to deliver network services to its users. These virtualized network services are considered better solutions than hardware-based network functions because their resources can be dynamically increased upon the consumer's request. While their usefulness can't be denied, they also have some security implications. In complex systems like NFV, the threats can come from a variety of domains due to it containing both the hardware and the virtualize entities in its infrastructure. Also, since it relies on software, the network service in NFV can be manipulated by external entities like third-party providers or consumers. This leads the NFV to have a larger attack surface than the traditional network infrastructure. In addition to its own threats, NFV also inherits security threats from its underlying cloud infrastructure. Therefore, to design a secure NFV system and utilize its full potential, we must have a good understanding of its underlying architecture and its possible security threats. Up until now, only imprecise models of this architecture existed. We try to improve this situation by using architectural modeling to describe and analyze the threats to NFV. Architectural modeling using Patterns and Reference Architectures (RAs) applies abstraction, which helps to reduce the complexity of NFV systems by defining their components at their highest level. The literature lacks attempts to implement this approach to analyze NFV threats. We started by enumerating the possible threats that may jeopardize the NFV system. Then, we performed an analysis of the threats to identify the possible misuses that could be performed from them. These threats are realized in the form of misuse patterns that show how an attack is performed from the point of view of attackers. Some of the most important threats are privilege escalation, virtual machine escape, and distributed denial-of-service. We used a reference architecture of NFV to determine where to add security mechanisms in order to mitigate the identified threats. This produces our ultimate goal, which is building a security reference architecture for NFV.

BIOGRAPHICAL SKETCH
Born in Alahsa, Saudi Arabia
B.S., King Faisal University, Alahsa, Eastern Region, Saudi Arabia, 2011
M.S., Nova Southeastern University, Davie, Florida, USA, 2014
Ph.D., Florida Atlantic University, Boca Raton, Florida, 2020

CONCERNING PERIOD OF PREPARATION
& QUALIFYING EXAMINATION

Time in Preparation: 2016 - 2020

Qualifying Examination Passed: Spring 2017

Published Papers:

1. A. K. Alnaim, A. M. Alwakeel, and E. B. Fernandez, "A Pattern for an NFV Virtual Machine Environment," in *Proceedings of the 13th Annual IEEE International Systems Conference 2019*, 2019.

2. A. K. Alnaim, A. M. Alwakeel, and E. B. Fernandez, "Threats Against the Virtual Machine Environment of NFV," in *2nd International Conference on Computer Applications and Information Security, ICCAIS 2019*, 2019.

3. A. K. Alnaim, A. M. Alwakeel, and E. B. Fernandez, "A Misuse Pattern for NFV based on Privilege Escalation," in *Proceedings of the 8th Asian Conference on Pattern Languages of Programs*, 2019.

4. A. K. Alnaim, A. M. Alwakeel, and E. B. Fernandez, "A Misuse Pattern for Compromising VMs via Virtual Machine Escape in NFV," in *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019)*, 2019.

5. A. K. Alnaim, A. M. Alwakeel, and E. B. Fernandez, "A Misuse Pattern for Distributed Denial-of-Service Attack in Network Function Virtualization," in *In Proceedings of the 26th PLoP'19*, 2019.

6. A. K. Alnaim, A. M. Alwakeel, and E. B. Fernandez, "Towards a Security Reference Architecture for Network Function Virtualization," 2020. (Submitted).

7. A. M. Alwakeel, A. K. Alnaim, and E. B. Fernandez, "A Survey of Network Function Virtualization Security," in *IEEE SoutheastCon 2018*, 2018, doi: 10.1109/SECON.2018.8479121.

8. A. M. Alwakeel, A. K. Alnaim, and E. B. Fernandez, "Analysis of threats and countermeasures in NFV use cases," in *SysCon 2019 - 13th Annual IEEE International Systems Conference, Proceedings*, 2019, pp. 1–6.

9. A. M. Alwakeel, A. K. Alnaim, and E. B. Fernandez, "Toward a Reference Architecture for NFV," in *2nd International Conference on Computer Applications and Information Security, ICCAIS 2019*, 2019.

10. A. M. Alwakeel, A. K. Alnaim, and E. B. Fernandez, "A Pattern for Network Function Virtualization Infrastructure (NFVI)," in *In Proceedings of the 26th PLoP'19*, 2019.

11. A. M. Alwakeel, A. K. Alnaim, and E. B. Fernandez, "A Pattern for a Virtual Network Function (VNF)," in *The 14th International Conference on Availability, Reliability and Security (ARES 2019)*, 2019.

12. A. M. Alwakeel, A. K. Alnaim, and E. B. Fernandez, "A Pattern for NFV Management and Orchestration (MANO)," in *Proceedings of the 8th Asian Conference on Pattern Languages of Programs*, 2019.