# Seunghyeon Lee (이승현)

KAIST, 291, Daehak-ro, Yuseung-gu, Daejeon, 34141, South Korea
E seunghyeon AT kaist.ac.kr
www.nss.kaist.ac.kr / www.sdnsecurity.org

## Summary

Seunghyeon Lee is currently a Ph.D. student at SoC (School of Computing) at KAIST, where he is working with Dr. Seungwon Shin at NSS (Network and System Security Laboratory). He is primarily interested in the area of network security including an SDN (Software-Defined Networking) and a network debugging.

## Education

**Korea Advanced Institute of Science and Technology (KAIST)** **Mar 2015 - Present**

Ph.D. student, School of Computing (Advisor: Dr. Seungwon Shin)

**Korea Advanced Institute of Science and Technology (KAIST)** **Mar 2013 - Feb 2015**

Master of Science in Engineering - Information Security (Advisor: Dr. Brent Byunghoon Kang)
(Thesis title: sCARF: Collaborative Response Framework for Reducing Threat Semantic Gap)

**Chungnam National University** **Mar 2007 - Feb 2013**

Bachelor of Science in Computer Science

## Publication

**(DSN) Dependable Systems and Networks 2017** **Jun 2017**

Title: Athena: A Framework for Scalable Anomaly Detection in Software-Defined Networks [paper]
(Acceptance ratio 22.2%=49/220)
Authors: **Seunghyeon Lee**, Jinwoo Kim, Seungwon Shin, Phillip Porras, Vinod Yegneswaran

**(SCN) Security and Communication Networks 2015** **Oct 2015**

Title: Vulnerabilities of Network OS and Mitigation with State-based Permission System [paper]
Authors: Jiseong Noh, **Seunghyeon Lee**, Jaehyun Park, Seungwon Shin, Brent Byunghoon Kang

**(SOSR) ACM SIGCOMM Symposium on SDN Research 2015** **Jun 2015**

Title: A playground for Software-defined Networking Security (Demo) [paper]
Authors: **Seunghyeon Lee**, Chanhee Lee, Hyeonseong Jo, Jinwoo Kim, Seungsoo Lee, Jaehyun Nam, Taejune Park, Changhoon Yoon, Yeonkeun Kim, Heedo Kang, and Seungwon Shin

## Software Release

**Athena** **Jun 2017**

The network anomaly detection framework in SDN networks [Link]

## Projects

**Institute for Information & communications Technology Promotion (IITP), South Korea**
**Jun 2015 - Present**

Global SDN/NFV Open-Source Software Core Module/Function Development

**Korea Institute of Science and Technology Information (KISTI)** **Mar 2015 - Nov 2016**

Research in distributed control plane clustering and network virtualization for SDN

**National IT Industry Promotion Agency, South Korea** **Dec 2014 - May 2015**

Development of SDN/OpenFlow based network security framework and service

**Agency for Defense Development, South Korea (ADD)** **Mar 2014 - Feb 2015**

Technical Consulting on the Test & Evaluation Methodology for Cyber-security Technologies

## Awards

**Graduate Summa cum laude, Computer Science Department in CNU** **Feb 2013**

Graduated first class honor

**2nd prize at 1st Test Of Practical Competency in IT(TOPCIT) competition** **Oct 2012**

TOPCIT evaluates the basic core knowledge to solve the problems in accordance with the requirements needed to perform the IT task successfully.

## Work experience

**International Fellow** **Jun 2016 - Sep 2016**

(Internet Security Group, Computing Science Laboratory, Supervisor: Phillip Porras)
SRI International - The Athena project

**Research Observer** **Dec 2015 - Mar 2016**

(Internet Security Group, Computing Science Laboratory, Supervisor: Phillip Porras)
SRI International - The Athena project

## Activities

**Manager** **Mar 2015 - Present**

SDNSecurity.org (www.sdnsecurity.org)

**Teaching Assistant** **Mar 2016 - Jun 2016**

IS521 - Cyber Attack & Response I

**Teaching Assistant** **Mar 2015 - Jun 2015**

IS539 - Network Security

**Teaching Assistant** **Mar 2014 - Jun 2014**

IS511 - Information Security

## Talks

**Open Networking Foundation (ONF)** **Jun 2016**

Member Work Day - Athena framework

## Patents

**Domestic (Submitted)** **Apr 2016**

METHOD, APPARATUS AND COMPUTER PROGRAM FOR NETWORK ANOMALY DETECTION IN DISTRIBUTED SOFTWARE DEFINED NETWORKING ENVIRONMENT)
Authors: Seungwon Shin, **Seunghyeon Lee**, Jinwoo Kim

## References

**Dr. Seungwon Shin (E: claude@kaist.ac.kr)**

Assistant Professor, School of Computing, KAIST

**Dr. Brent Byunghoon Kang (E: brentkang@kaist.ac.kr)**

Associate Professor, School of Computing, KAIST

## Bio long ver (NetSoft 16)

Seunghyeon Lee is currently a Ph.D. student at SoC (School of Computing) at KAIST, where he is working with Dr. Seungwon Shin at NSS (Network and System Security Laboratory). He is primarily interested in the area of network security including SDN (Software-Defined Networking). He is currently leading Athena project, which is a collaborative project with Computer Science Laboratory in SRI International to design and develop an anomaly detection framework for SDN environment. Besides, he has initially built up SDNSecurity.org, which has provided useful resources related to SDN security, and he has demonstrated it as "A playground for Software-defined Networking Security" at SOSR by Open Networking Summit 2015.

## Research Interests (SRI Intern resume)

He is primarily interested in the area of network security including SDN (Software-Defined Networking). He is currently leading the Athena project to design and develop a large-scale network anomaly detection and monitoring framework for SDN environment. The Athena prototype provides a development environment for a scalable network analysis and systemizes SDN-specific network features including well-defined APIs to create an analysis application on SDN.

As an extension of the Athena framework, he is planning for the following future research topics:

- **Athena Switch (Athena feature extension)**: Although the Athena prototype systemizes network features with SDN`s characteristics, it is not sufficient to provide various network features such as information about the packet and session information per flows. To overcome the limitation of the Athena features, he is planning to design and implement the *Athena switch* to collect useful and fine-grained network features including packet-level features and flow-level features through a packet inspection, and a stateful session monitoring.
- **Athena Script Language:** The Athena framework provides a set of high-level APIs, which enables a developer to create an anomaly detection application with well-defined functionalities. Although a

developer makes an application with its usability, a non-security expert still has a problem to implement an anomaly detection application due to lack of preliminary bits of knowledge (e.g., Programming experiences, understanding of network features). To address the usability issue for the non-security expert, he is planning to design the *Athena Script Language,* which is a script language to initiate and define functions on the Athena without the preliminary knowledge.