CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

KAIST

IEEE NetSoft 2016 Tutorial Proposal

Title of Tutorial: Software Defined Network Security – In Practice

Tutorial Length: ½ Day

Outline of the Tutorial:

In this tutorial we provide a comprehensive overview of the state of Software Defined Network (SDN) Security. The tutorial will be presented in clearly defined sections, outlined as follows:

Part 1: Introduction – The state of SDN Security (25 mins)

This section will introduce results of a survey on SDN security considering both security issues in SDN and network security enhancements using SDN [1].

Speaker: SSH

Part 2: Attacks and Vulnerabilities in SDN (45 mins)

This section will focus on the identification of specific attacks and vulnerabilities in SDN. Using demonstration videos and animations, a range of attack scenarios will be demonstrated. Specifically, the vulnerabilities in each of the three layers of SDN: the control plane, the data plane, and the application plane (along with the control channel), will be revealed. The demonstration videos will show the attacks against a real SDN testbed with popular open-source SDN controller implementations and OpenFlow-enabled switches.

Speakers: SSH, CY, SL

Part 3: Solutions to Security Issues in SDN (35 mins)

This section introduces some of the proposed solutions to the attacks identified in Part 2. Solutions will be referenced from [1] and additional, recent proposals.

Speakers: SSH, CY, SL

Part 4: Controller Security (40 mins)

This section focusses on SDN controller security with a presentation of the requirements for secure, robust, and resilient control followed by presentation of the features of Secure Mode ONOS as designed by KAIST in collaboration with ON.LAB and SRI International.

Speakers: SSH, CY, SL

Part 5: Network Security Enhancements using SDN (40 mins)

This section introduces security features and applications that have been developed to exploit the characteristics of SDN for increased network security. An SDN traffic monitoring and threat analysis application will be demonstrated and discussed.

Speaker: SSH

Part 6: Conclusion – Future SDN Security (25 mins)

In this final section, the tutorial contents will be reviewed and the future of SDN security research and development will be discussed.

Speaker: SSH

The emphasis of the tutorial is on the state-of-the-art in SDN Security and the teaching material will include implementation results and demonstrations of open-source tools as developed by CSIT and KAIST.

The timing breakdown of the tutorial includes allowance for short breaks and Q&A.

Links to the presentation slides and the open-source tools will be provided to the participants.

Tutorial Speaker(s):

Speaker 1:

Dr. Sandra Scott-Hayward (SSH)

Centre for Secure Information Technologies (CSIT), Queen's University Belfast, Northern Ireland

Email: s.scott-hayward@qub.ac.uk

Dr. Sandra Scott-Hayward, CEng CISSP CEH OCSA, is a Senior Research Engineer in the Network Security research group at the Centre for Secure Information Technologies (CSIT), Queen's University Belfast. She has experience in both research and industry, having worked as a Systems Engineer and Engineering Group Leader with Airbus before returning to complete her Ph.D. at Queen's University Belfast. At CSIT, Sandra leads research and development of network security architectures and security functions for SDN. Sandra is a Research Associate of the Open Networking Foundation (ONF) and Vice-Chair of the ONF Security Working Group. She received an Outstanding Technical Contributor Award from the ONF in February 2015. Sandra has been invited to present her research on SDN Security at events globally (Ethernet Technology Summit 2014 (Santa Clara), Open Tech Ireland SDN Gathering 2014 (Dublin), SDN & NFV 2015 (London), SDN & OpenFlow World Congress 2015 (Dusseldorf), Open Networking Korea 2015 (Seoul).

Lecturing Experience: 6 years

Speaker 2:

Changhoon Yoon (CY)

School of Computing, Korea Advanced Institute of Science and Technology (KAIST), South Korea

Email: chyoon87@kaist.ac.kr

Changhoon Yoon is a PhD student at KAIST (School of Computing) in South Korea. He is working with Dr. Seungwon Shin at the Network and System Security Laboratory, and his research interests primarily lie in the area of network security including SDN and Network Function Virtualization (NFV) security. He is currently leading the Security-Mode ONOS project, which is a collaborative project with the researchers from ON.LAB and SRI International to design and implement a security extension for ONOS. He is also participating in other SDN security projects, such as an SDN WAN security project. In addition, he has presented “Security vulnerabilities in open-source SDN controllers” at the Open Networking Foundation Member Workday Event in September 2015. Changhoon has published several research papers on SDN security in major journals and a workshop.

Speaker 3:

Seunghyeon Lee (SL)

School of Computing, Korea Advanced Institute of Science and Technology (KAIST), South Korea

Email: coksm1963@kaist.ac.kr

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. He is currently leading the Athena project, which is a collaborative project with the Computer Science Laboratory at SRI International to design and develop an anomaly detection framework for SDN environments. In addition, he has created SDNSecurity.org, which has provided useful resources related to SDN security, and he has demonstrated “A playground for Software-defined Networking Security” [2] at SOSR at the Open Networking Summit 2015.

Importance and Timeliness of the Tutorial:

It is clear that SDN, in one form or another, is the future of networking. The academic community and networking industry members have been exploring new commercial applications for SDN based technologies for the past 5-8 years. As early-stage deployments have evolved from the data center to enterprise and towards wide area network design, the focus of SDN development has similarly evolved from data path design to distributed network control and external application integration. With this evolution, there has been an increasing focus on SDN security, particularly over the past 18 months.

SDN security applications can powerfully exploit the characteristics of SDN to increase the security of the network. At the same time, vulnerabilities in the SDN framework must be understood and mitigated in order to protect the network. In the course of research at CSIT and KAIST, and collaboration with industrial partners, solutions to SDN security challenges have been explored and developed.

SDN Security is a key topic in 2016. It is our belief that this tutorial provides a valuable insight into the domain of SDN Security and will appeal to the combined audience of researchers and industry participants at IEEE NetSoft 2016.

Intended Audience:

This tutorial is intended for researchers, students, and those in industry interested in learning about the security aspects of SDN.

Prior history of tutorial presentation:

Aspects of this tutorial have previously been presented at the COINS Summer School 2015:

Link https://coinsrs.no/coins-summer-school-2015/

Delta (previously POSEIDON) has been demonstrated at Open Networking Summit 2015:

Links http://opennetsummit.org/2015-archive/sosr/demo-abstracts/

References

[1] Scott-Hayward, Sandra, Sriram Natarajan, and Sakir Sezer. "A survey of security in software defined networks." *IEEE Communications Surveys & Tutorials*, July 2015.

[2] Lee, Seunghyeun et al. “A Playground for Software-Defined Networking Security.” *ACM SIGCOMM Symposium on Software Defined Networking Research - Demos 2015* - http://opennetsummit.org/wp-content/themes/ONS/files/sosr-demos/sosr-demos15-final3.pdf