Hyunwoo Lee

Address	Lawson 2142U, Purdue University, West Lafayette, 47906 IN
Nationality	Korean
Email	lee3816@purdue.edu
Home Page	`https://hw5773.github.io`
Github	`https://github.com/hw5773`

Education

2015-2020 M.S./Ph.D integrated Course in Dept. of Computer Science and Engineering, Seoul National University (*Advisor: Ted "Taekyoung" Kwon*)

2004-2011 B.S. in Dept. of Computer Science and Engineering, Seoul National University

Career

2020- Postdoc Research Associate Department of Computer Science, Purdue University (*Advisor: Elisa Bertino and Ninghui Li*)

Research Interests

- **Security of multi-party communications**
  My research aims to design/implement secure protocols for sessions where multi-parties are involved. For example, We consider extending Transport Layer Security (TLS) or Public Key Infrastructure (PKI) to make application middleboxes function over encrypted sessions without sharing private keys.
- **Security of distributed systems (Content Delivery Network/Edge Computing Platforms)**
  Many web services are running over the third-party distributed systems such as content delivery networks (CDNs), where services are delegation-based with a large attack surface. We are conducting research to leverage Trusted Execution Environments (TEEs) such as Intel SGX or ARM TrustZone with designing remote attestation protocols on the platforms.
- **Measurement study of security in the Internet**
  The security of Internet is getting important and many security protocols such as the TLS protocol, are proposed and deployed. We are investigating how well TLS 1.3 is deployed on the third-party platforms such as CDNs or web hosting platforms.
- **Formalization of security properties and verification of the security protocol executions**
  Many security protocols are designed based on their security goals. To guarantee the security of the protocols, their goals should be formalized and their execution should be verified. We are reviewing security of multi-party protocols with a security verification tool, TAMARIN.

Key Achievements

- **Enabling application middleboxes function in-between TLS endpoints**
  1) Objective: The wide deployment of TLS disables application middleboxes such as web application firewalls in-between endpoints.
  2) Approach: We design the X.509 extension for middleboxes and the TLS extension to securely introduce/audit middleboxes in TLS sessions, while formally proving the protocol by leveraging the secure verification tool.
  3) Related Achievements:
  ○ Paper) maTLS: How to Make TLS middlebox-aware? (NDSS '19)
  ○ Poster) A Trustworthy Middlebox-aware Networking Architecture (NSDI '18)
  ○ Award) Best Research Award (Open Tech Talk at Samsung Security Tech Forum (SSTF) '19)

List of Publications

2021

Analyzing Spatial Differences in the TLS Security of Delegated Web Services
Joonhee Lee, **Hyunwoo Lee**, Jongheon Jeong, Doowon Kim, and Taekyoung “Ted” Kwon
The 16th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2021)
Hong Kong, China, June 2021 (Virtual)

TLS 1.3 in Practice: How TLS 1.3 Contributes to the Internet
Hyunwoo Lee, Doowon Kim, and Yonghwi Kwon
The Web Conference 2021 (TheWebConf 2021, formerly WWW),
Ljublijana, Slovenia, April 2021 (Virtual)

2019

mqTLS: Toward Secure MQTT Communication with an Untrusted Broker
Hyunwoo Lee, Junghwan Lim, and Ted “Taekyoung” Kwon
The 10th International Conference on ICT Convergence (ICTC ’19),
Jeju Island, Korea, October 2019

Proactive SDN-based Load Balancing for Datacenter Network (Poster)
Minhyeok Kang, **Hyunwoo Lee**, Junghwan Song, and Ted “Taekyoung” Kwon
The 14th International Conference on Future Internet Technologies (CFI ’19),
Phuket, Thailand, August 2019

D2TLS: Delegation-based DTLS for Cloud-based IoT Services
Eunsang Cho, Minkyung Park, **Hyunwoo Lee**, Junhyeok Choi, and Ted “Taekyoung” Kwon
2019 ACM/IEEE Fourth International Conference on Internet-of-Things Design and Implementation (IoTDI ’19), Montreal, Canada, April 2019

maTLS: How to Make TLS middlebox-aware?
Hyunwoo Lee, Zach Smith, Junghwan Lim, Gyeongjae Choi, Selin Chun,
Taejoong Chung, and Ted “Taekyoung” Kwon
In Proceedings of the Network and Distributed System Security Symposium (NDSS ’19),
San Diego, USA, February 2019

A Multi-Interface Mobility Support Socket Library for Edge Computing (Korean)
Junghwan Lim, **Hyunwoo Lee**, and Ted “Taekyoung” Kwon
Korea Information and Communication Society (KICS) Conference Winter 2019,
Pyeongchang, Gangwon-do, January 2019

2018

A Trustworthy Middlebox-aware Networking Architecture (Poster)
Hyunwoo Lee, Zach Smith, Selin Chun, and Ted “Taekyoung” Kwon
15th USENIX Symposium on Networked Systems Design and Implementation (NSDI ’18),
Renton, USA, April 2018

An Application and Analysis on TLS extension with Compressed Certificate (Korean)
Hyunwoo Lee, Younghyun Kim, Eunsang Cho, and Ted “Taekyoung” Kwon
Korea Information and Communication Society (KICS) Conference Winter 2018,
Jeongsun-gun, Gangwon-do, January 2018

2017

A Preliminary Study on Disaster Waste Detection and Volume Estimation based on 3D Spatial Information
Hyungtaeck Yoo, **Hyunwoo Lee**, Seokho Chi, Bon-Gang Hwang
2017 International Workshop on Computing in Civil Engineering (IWCCE 2017)

2016

Position Estimation of Robotic Mobile Nodes in Wireless Testbed using GENI
Ahmed Abdelhadi, Felipe Rechia, Arvind Narayanan, Thiago Teixeira, Ricardo Lent,
Driss Benhaddou, **Hyunwoo Lee**, T. Charles Clancy
Systems Conference (SysCon 2016)

2015 **Enabling SDN Experimentation with Wired and Wireless Resources: The SmartFIRE facility**
Kostas Choumas, Thanasis Korakis, **Hyunwoo Lee**, Donghyun Kim, Junho Suh
Ted “Taekyoung” Kwon, Pedro Martinez-Julia, Antonio Skarmeta, Taewan You, Loic Baron
Serge Fdida , and JongWon Kim
6th EAI International Conference on Cloud Computing (Cloudcomp 2015)

ICN-OMF: A Control, Management Framework for Information-Centric Network Testbed
Hyunwoo Lee, Donghyun Kim, Junho Suh, Ted ”Taekyoung” Kwon
International Conference on Information Networking (ICOIN 2015)

Awards

2019 **Ph D. Fellowship Award**
December 20 from Naver Corporation

Best Research Award
August 20 in Open Tech Talk at Samsung Security Tech Forum (SSTF) 2019

Seminar Talk

2019 **Toward Trustworthy Middlebox-aware Secure Architecture**
August 20 in Open Tech Talk at Samsung Security Tech Forum (SSTF) 2019
`https://research.samsung.com/sstf`

maTLS: How to Make TLS middlebox-aware?
March 13 at Security and Trust of Software Systems (SaToSS) in University of Luxembourg
`http://satoss.uni.lu/seminars/srm/`

Research Projects

Mar 2019 – Nov 2019 **Analysis on the distributed internet infrastructure**
Researcher (*funded by ETRI*)

This project aims to review the systems for the distributed internet

- I analyzed a decentralized identifier for the distributed internet.
- I surveyed digital identity schemes including Blockstack or Sovrin.

Related Technologies: Blockchain, Decentrailized Identifier (DID), Blockstack, Sovrin, etc.

Oct 2016 – Aug 2020 **Developing high-performance programming environments and computing systems**
System Designer / System Programmer (*funded by NRF*)

This project aims to develop super high-performance computing system.

- I designed a hybrid approach for a congestion control mechanism between HPC computation nodes.
- I am managing an experiment to compare the above approach with a centralized congestion control mechanism based on software defined networking (SDN) concepts and a distributed congestion control mechanism based on the equal-cost multi-path routing (ECMP) over the priority-based flow control (PFC).
- I am developing a pluggable Linux kernel module to balance the traffic loads at the endpoints leveraging the ECMP.

Related Technologies: High Performance Computing, Remote Direct Memory Access (RDMA), Software Defined Networking (SDN), TCP/IP Networking, Loseless Network, Congestion Control, Switch Configuration, Linux Kernel Module Development (C)

May 2016 – Aug 2020 **Versatile Network System Architecture for Multi-dimensional Diversity**
Project Manager (Lab.) / System Designer / System Programmer (*funded by IITP*)

This project aims to design a network architecture to cover diversity, such as interfaces, services, and resources, in the edge network.

- I am a project manager of this project in our lab.
- I designed a flexible identifier structure, called the Flex ID, used in the edge network to provide trustworthiness of entities, mobility/multicasting support, and in-networking caching.
- I designed a protocol for service/content discovery based on Flex ID.
- I designed and implemented a socket module for the name (Flex ID) based routing.

Related Technologies: Edge/Cloud Computing, Software Defined Network, TCP/IP Networking, Trustworthiness, Mobility, Multicasting, In-network caching, Linux Kernel Module Development (C)

Jan 2016 – Mar 2016 **Consultation on the Mash-up API for the IoT Platform Improvement**
Researcher (*funded by JC Square Inc.*)

This project aims to consult the mash-up API and security issues to improve the IoT platform.

- I proposed to deploy the OAuth system for authorizing the apps to access IoT devices.

Related Technologies: Internet of Things, Authentication, Authorization, OAuth

Jul 2015 – Dec 2015 **Study on Future Internet Architectures focusing on Security**
Researcher (*funded by KIISE*)

This project aims to survey diverse future Internet architectures, such as the content centric networking (CCN), focusing on their security aspects.

- I summarized the trends on the security aspects in the future Internet architecture.

Related Technologies: eXpressive Internet Architecture (XIA), Mobility First (MF), Named Data Networking (NDN)

Jul 2015 –
Dec 2015

Development of Network Security Acceleration for Next-generation Low-power SoC
Developer (*funded by Samsung Electronics*)

This project aims to secure the communication sessions with low-power SoCs.

- I developed our offloading based DTLS extension over TI CC3200.
- I evaluated our scheme and analyzed the data.

Related Technologies: OpenSSL, WolfSSL, Transport Layer Security, Datagram Transport Layer Security, Internet of Things, Energia, RedBearLab CC3200 Board, Beagle Bone Black, ODROID, C, Python

Sep 2014
Dec 2015

SmartFIRE: Enabling SDN Experiments in Wireless Testbeds exploiting Future Internet Infrastructures in South Korea and Europe
Project Manager (Lab) / Researcher / Developer (*funded by MSIP*)

This project aims to secure the communication sessions with low-power SoCs.

- I managed a plan of the project in our lab.
- I designed a testbed for information-centric networking based on the OMF framework.
- I implemented a virtual machine based ICN-testbed.

Related Technologies: Information-Centric Networking (ICN), KVM, GRE-tunneling, Ruby, Python, Bash shell script

Oct 2014 –
Dec 2014

Research on the Manageable IP-based Secure Architecture
Developer (*funded by SKT*)

This project aims to design and implement the light-weight authentication and authorization regarding IoT devices.

- I implemented our certificate-less authentication protocol on the Raspberry Pi.
- I evaluated our scheme and analyzed the result.

Related Technologies: Certificate-Less Public Key Cryptography (CL-PKC), OpenSSL, Raspberry Pi, C, Python

Patents

2019

Network System and Method for Performing Message Security Thereof (Pending / Korea)
Ted “Taekyoung” Kwon, **Hyunwoo Lee**, Myungchul Kwak, Hyeonmin Lee, Junghwan Lim, Yoojung Shin
(Application No. 10-2019-0156578)

Communication Method and Apparatus for Supporting Diverse Interface, Mobility, and Multicasting using Integrated Flat ID (Pending / PCT)
Ted “Taekyoung” Kwon, **Hyunwoo Lee**, Myungchul Kwak, Hyeonmin Lee, Junghwan Lim, Yoojung Shin, Gyeongjae Choi
(Application No. PCT/KR2019/016640)

2018

Communication Method and Apparatus for Supporting Diverse Interface, Mobility,

and Multicasting using Integrated Flat ID (Pending / Korea)
Ted “Taekyoung” Kwon, **Hyunwoo Lee**, Myungchul Kwak, Hyeonmin Lee, Junghwan Lim, Yoojung Shin, Gyeongjae Choi
(Application No. 10-2018-0160970)

2017 **Integrated ID based Communication Method and System (Registered / Korea)**
Ted “Taekyoung” Kwon, **Hyunwoo Lee**, Hyeonmin Lee, Dongjun Lee, Hyunchul Oh
(Application No. 10-2017-0159700)

Waste Volume Calculation Method and Waste Volume Calculation System (Pending / Korea)
Seokho Chi, Hyungtaeck Yoo, **Hyunwoo Lee**
(Application No. 10-2017-0020084)

2016 **Method and System for Estimating the Generation of Disaster Waste using Unmanned Aerial Vehicle (UAV) (Pending / Korea)**
Seokho Chi, Hyungtaeck Yoo, **Hyunwoo Lee**
(Application No. 10-2016-0181527)

Systems and Methods that Support an Integrated Identity (Pending / Korea)
Ted “Taekyoung” Kwon, Myungchul Kwak, **Hyunwoo Lee**, Hyeonmin Lee
(Application No. 10-2016-0158686)

Certification

- **Engineer Information Security**
  Certified by Korea Internet & Security Agency on December 27, 2013
  (Qualification Number: 13202000151A)

- **Oracle Certified Professional, Java SE 6 Programmer**
  Certified by Oracle on December 27, 2013

- **Engineer Information Processing**
  Certified by Human Resources Development Service of Korea on June 1, 2009
  (Qualification Number: 09201021824B)

- **Craftsman Computer Graphics Operation**
  Certified by Human Resources Development Service of Korea on October 8, 2001
  (Qualification Number: 01403071984N)

Technical Skills

- **Programing Languages**: C/C++, Java, Python, Ruby, PHP, Go

- **Operating Systems**: Linux (Ubuntu), Windows, Energia, Contiki, Android

- **Cryptography Libraries**: OpenSSL, BoringSSL, WolfSSL, Relic Toolkit, MbedTLS

- **System on Chips**: Raspberry Pi (1, 3B), Beagle Bone Black, RedBearLab CC3200 Board, ODROID

- **Web Server Development**: nginx

- **Browser Development**: Chromium

- **Database**: MySQL

- **Framework**: Flask

- **Trusted Execution Environment**: Intel SGX, ARM TrustZone, OP-TEE