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 to establish sessions where multi-parties are involved. To this end, I have worked on on Transport Layer Security (TLS) extensions, Public Key Infrastructure (PKI) extensions, or searchable encryption to make application middleboxes function over encrypted sessions without sharing private keys.
- **Security of distributed systems (content delivery network/edge computing platforms)**
  Many 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. I do research in applying Trusted Execution Environments (TEEs) such as Intel SGX or ARM TrustZone to secure such platforms.
- **Measurement study of security in the Internet**
  The growing importance of security in the Internet introduces many security protocols such as TLS or IPSec in practice. I did research on how well TLS 1.3 is deployed on the third-party platforms such as CDNs or web hosting platforms. I also designed a possible downgrade attack due to the distributed system and analyzed its feasibility against the real-world platforms.
- **Formal verification of security of protocol executions**
  Many security protocols are designed to achieve their security goals. Formal methods are useful to analyze the security of the protocols or to identify possible vulnerabilities. I am doing research on security of mobile network protocols (e.g., Voice over WiFi) and multi-party protocols (e.g., TLS extensions for middleboxes and blockchain lightning protocols) with a security verification tool.
- **Lightweight security protocol for Internet-of-Things**
  Some Internet-of-Things (IoT) devices have lack of capabilities to execute security protocols based on asymmetric cryptography. We designed and implemented the lightweight DTLS protocol by delegating heavy computation to a high-end security agent.
- **Intrusion detection systems for Internet-of-Things with machine learning algorithms**
  My research aims to design/implement intrusion detection systems (IDSes) for Internet-of-Things (IoT) with machine learning algorithms. I am applying the state-of-the-art deep learning techniques to secure IoT networks and to enhance the accuracy of the systems.

Key Achievements

- **Enabling application middleboxes function in end-to-end security sessions**

1) Objective: The wide deployment of TLS disables application middleboxes such as web application firewalls in-between endpoints. I am working on enabling middleboxes function alongside TLS protocol.
2) Approach: I designed 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)

- **Measurement study of TLS 1.3 in the Internet**
1) Objective: The new version of the TLS protocol is designed and deployed in practice. I evaluated whether the TLS 1.3 protocol was well deployed as intended and found any possible attacks.
2) Approach: I collected the dataset of TLS 1.3 handshakes for over one year (temporal) and from multiple sources (spatial) to analyze the TLS 1.3 protocol in diverse aspects. Also, I designed a possible TLS downgrade attack and evaluated its feasibility in the wild.
3) Related Achievements:
○ Paper) TLS 1.3 in Practice: How TLS 1.3 Contributes to the Internet (WWW '21)
○ Paper) Analyzing Spatial Differences in the TLS Security of Delegated Web Services (AsiaCCS '21)

- **Security verification for protocol execution**
1) Objective: Security protocols have their own goals called security properties. I verified whether the properties are guaranteed or not on security protocols including Voice over WiFi (VoWiFi), TLS extensions for middleboxes, and the lightning protocol
2) Approach: I used verification tools (e.g., Tamarin) and model checkers (e.g., nuXmv) for this purpose. I modeled protocols and verified them based on properties extracted from specifications
3) Related Achievements:
○ Paper) VWAnalyzer: A Systematic Security Analysis Framework for the Voice over WiFi Protocol (AsiaCCS '22) (to appear)
○ Paper) Modelling Agent-Skipping Attacks in Message Forwarding Protocols (arXiv)

- **Security for Internet-of-Things**
1) Objective: Due to lack of capabilities, IoT devices become the weakest point of the network and require security guarantees.
2) Approach: We designed the lightweight DTLS protocol for IoT devices. Furthermore, to guarantee end-to-end security on the MQTT protocol, I extended the standard TLS protocol to include the MQTT broker in-between publishers and subscribers. I also wrote the book chapter about IDS for IoT devices, which will be published soon.
3) Related Achievements:
○ Paper) D2TLS: Delegation-based DTLS for Cloud-based IoT Services (IoTDI '19)
○ Paper) mqTLS: Toward Secure MQTT Communication with an Untrusted Broker (ICTC '19)
○ Book Chapter) Intrusion Detection Systems for IoT in *IoT for Defense and National Security* (to appear)

Publications

2022 **VWAnalyzer: A Systematic Security Analysis Framework for the Voice over WiFi Protocol**
Hyunwoo Lee, Imtiaz Karim, Ninghui Li, and Elisa Bertino
The 17th ACM ASIA Conference on Computer and Communications Security (AsiaCCS 2022)
Nagasaki, Japan, June 2022

Modelling Agent-Skipping Attacks in Message Forwarding Protocols
Zach Smith, Hugo Jonker, Sjouke Mauw, and **Hyunwoo Lee**
arXiv (2201.08686)

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 (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/`

Patents

2019 **Network System and Method for Performing Message Security Thereof (Registered / 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)

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)