

I am a postdoctoral researcher at Seoul National University. My research interests lie in network security, especially, DNS and Email security. I have published five papers, three of which were published in top-tier conferences including USENIX Security and The Web Conference (formerly WWW). Also, I have participated in (or led) more than ten research projects with institutions such as Virginia Tech, Rochester Institute of Technology, University of Twente, KAIST, SIDN Labs, NLnet Labs, etc. I have covered a variety of techniques in my research, such as DNS, DNS security (e.g., DNSSEC, DoT, DoH), SMTP, Email security (e.g., STARTTLS), PKI, DANE, TLS, IoT, and edge computing.

## RESEARCH INTERESTS

My research interests lie in the field of **network security**, with a focus on identifying security issues in network systems and designing practical solutions to address them. In my research, I often utilize network measurements to identify potential security problems.

My current research focuses on areas including (but not limited to) DNS security, email security, and Transport Layer Security (TLS). Additionally, I am interested in improving existing security protocols from a practical standpoint.

### ◦ Security of DNS

The Domain Name System (DNS) was originally designed without any security features. While DNSSEC was introduced 20 years ago to guarantee the integrity of DNS messages, its deployment ratio remains very low (only 7%). As a result, the vast majority of DNS messages in the real world are still vulnerable to integrity attacks, such as DNS cache poisoning attacks. To address this challenge, my research investigates a practical and deployable solution for ensuring the integrity of DNS messages by leveraging PKIX certificates

### ◦ Security of Email

My research aims to address security problems in the email system. Particularly, Simple Mail Transfer Protocol (SMTP) was designed without any security mechanisms. As a result, there is no authentication of a sender and no encryption of email contents. Although STARTTLS was proposed as a solution, it is vulnerable to downgrade attacks, which presents a critical problem. To mitigate this issue, my research focuses on developing solutions to prevent downgrade attacks.

### ◦ Transport Layer Security (TLS)

TLS requires one more round-trip to establish a secure session between a client and a server and it can degrade the user experience. To address the issue, I conducted research to design a novel technique that leverages DNS to publish a server's cryptographic information for the TLS handshake. This approach allows a client to fetch a server's IP address and Z-data simultaneously, enabling encrypted data transmission with a 0-RTT delay. This work is the first to use DNS to reduce network latency in the TLS handshake.

Furthermore, I am researching the adoption of the DANE protocol in the Web ecosystem. The current Web infrastructure relies on the CA-based PKI model, which has been criticized due to the vulnerabilities of CAs, such as being compromised and issuing fraudulent certificates to attackers. The DANE protocol enables authentication of communication peers without CAs, but it is currently only used for email transmission. I am investigating how the Web ecosystem can adopt the DANE protocol for secure communication.

## EDUCATION

**Ph.D., Computer Science and Engineering**, *Seoul National University*, (Seoul, South Korea) **Mar 2016 — Feb 2022**

- [Dissertation] "Understanding the DANE Ecosystem in Email: How Is It Deployed and Managed?"
- [Advisors] *Prof. Taekyoung "Ted" Kwon (Seoul National University)* and *Prof. Taejoong "Tijay" Chung (Virginia Tech)*

**B.S., Computer Science and Engineering**, *Seoul National University*, (Seoul, South Korea) **Mar 2011 — Feb 2016**  
**Visiting Student, Information Technology**, *Uppsala University*, (Uppsala, Sweden) **Fall 2014**

## PROFESSIONAL EXPERIENCE

**Postdoctoral Researcher**, Network Convergence and Security Lab **Apr 2022 — Present**  
*Seoul National University* *Seoul, South Korea*

- [Web and DANE] Study how the Web ecosystem will be changed if the Web adopts the DANE protocol (Achievement - Grant).
- [STARTTLS] Investigate how to prevent STARTTLS downgrade attacks.
- [DNS and TLS] Analyze how DNS can be exploited to reduce the TLS handshake time (Achievement - Publication [C4]).
- [DNS and PKIX] Study how we can guarantee the integrity of DNS records using PKIX certificates (Achievement - Publication [I-D]).

**Research Assistant**, Network Convergence and Security Lab  
Seoul National University

**Mar 2016 — Feb 2022**  
Seoul, South Korea

- [Email and DANE] Measured how DANE is deployed in the SMTP ecosystem (Achievements - Publications [C2, P1]).
- [Email and DANE] Investigated the underlying reasons for the DANE mismanagement (Achievement - Publication [C3]).

**Visiting Student**, The Center for Cybersecurity  
Rochester Institute of Technology

**May 2019 — Aug 2019**  
Rochester, NY, United States

- [Email and DANE] Analyzed DANE to measure its deployment in the real-world (Achievements - Publications [C2, P1]).

## PUBLICATIONS

- [C4] ZTLS: A DNS-based Approach to Zero Round Trip in TLS handshake (To appear) **TheWebConf'23**  
Sangwon Lim, **Hyeonmin Lee**, Hyunsoo Kim, Hyunwoo Lee, and Ted "Taekyoung" Kwon  
*In Proceedings of the ACM Web Conference 2023*, Austin, United States, Apr 2023
- [C3] Under the Hood of DANE mismanagement in SMTP **USENIX Security'22**  
**Hyeonmin Lee**, Md. Ishtiaq Ashiq, Moritz Müller, Roland van Rijswijk-Deij, Taekyoung "Ted" Kwon, Taejoong Chung  
*In Proceedings of the 31st USENIX Security Symposium*, Boston, United States, Aug 2022
- [C2] A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email **USENIX Security'20**  
**Hyeonmin Lee**, Aniketh Gireesh, Roland van Rijswijk-Deij, Taekyoung "Ted" Kwon, Taejoong Chung  
*In Proceedings of the 29th USENIX Security Symposium*, Boston, United States, Aug 2020
- [C1] Development of Cellular Core Network Enabling Network Function Virtualization **JCCI'18**  
**Hyeonmin Lee**, Junghwan Song  
*The 28th Joint Conference on Communication and Information*, Yeosu, Korea, May 2018
- [J1] TwinPeaks: An Approach for Certificateless Public Key Distribution for the Internet and Internet of Things **Computer Networks**  
Eunsang Cho, Jeongnyeo Kim, Minkyung Park, **Hyeonmin Lee**, Chorom Hamm, Soobin Park, Sungmin Sohn, Minhyeok Kang, Ted "Taekyoung" Kwon  
*Elsevier Computer Networks (SCI-E)*
- [P1] A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email **USENIX Security'22**  
**Hyeonmin Lee**, Md. Ishtiaq Ashiq, Moritz Müller, Roland van Rijswijk-Deij, Taekyoung "Ted" Kwon, Taejoong Chung  
*Poster Session in the 31st USENIX Security Symposium*, Boston, United States, Aug 2022
- [I-D] DNSSEC Extension by Using PKIX Certificates **Internet-Draft**  
**Hyeonmin Lee**, Taekyoung Kwon  
*Active Internet-Draft*, March 2023

## GRANTS

- A Study for the Future-oriented DANE-based Web Architecture to Solve Problems in the Current TLS-based Web Ecosystem**  
Primary Investigator, System Designer **Sep 2022 — Aug 2023**  
(Funded by *Post-Doctoral Domestic and Overseas Training Program - National Research Foundation of Korea*, ₩60,000,000 ≈ \$46,000)
- [Project Goal] Currently, the DANE protocol is mainly used for SMTP server authentication in mail transfers. In this research, I study how the Web ecosystem will be changed if the Web adopts the DANE protocol for communication peer authentication.
  - [Keywords] Web, Transport Layer Security (TLS), Authentication, DANE.

## RESEARCH PROJECT EXPERIENCE (SELECTED)

- System Designer/ Programmer** **Aug 2022 — Present**  
Research on Secure DNS and Privacy aware Packet Filtering Technology  
(Funded by *Samsung Electronics*)
- [Project Goal] This project aims to design a secure DNS environment for mobile devices, which includes analyzing the performance of DoT/DoH in the mobile environment, designing a packet filtering mechanism based on DNS packets.
  - [Keywords] Domain Name System (DNS), DNS over TLS (DoT), DNS over HTTPS (DoH), Packet filtering.
  - [Role] I investigate a way to filter packets using DNS packets and implement it on BIND9.
- Project Manager/System Designer/Programmer** **Mar 2021 — Nov 2021**  
Abnormal Detection and Forensic Techniques using IoT Network Traffic Analysis  
(Funded by *Korea Institute of Information Security & Cryptology (KIISC)*)
- [Project Goal] This project aims to develop a system that detects anomalies (or attacks) in IoT networks and generates evidence for digital forensics by collecting IoT network traffic.
  - [Keywords] IoT network, Network security, Machine learning, Abnormal detection.

- [Role] I analyzed IoT network traffic to distinguish abnormal traffic from normal ones using an autoencoder.

## Project Manager

Mar 2020 — Dec 2020

## System Designer/ Programmer

Apr 2016 — Mar 2020

Versatile Network System Architecture for Multi-dimensional Diversity

(Funded by *Institute for Information and Communication Technology Promotion (IITP)*)

- [Project Goal] This project aims to design a network architecture that covers diverse network devices, services, or resources, especially, in the edge network (Related achievements - Patent [1, 2, 3]).
- [Keywords] Edge/Cloud computing, Mobility, In-network caching, Trustworthiness.
- [Role] I devised/tested a naming system that can effectively express diverse network devices, services, or resources in the edge network. Also, I implemented an ID resolver that handles the mapping between IDs and resources such as ID allocation or mobility handling.

## PATENTS

### • Method for Performing Mutual Authentication in Communication using Locator ID Separation Protocol, Apparatus, and System for Performing the Same

Ted “Taekyoung” Kwon, **Hyeonmin Lee**, Hyunwoo Lee

- Registration No. 10-2476081
- South Korea, Dec 2022

### • Network System and Method for Performing Message Security Thereof

Ted “Taekyoung” Kwon, Hyunwoo Lee, Myungchul Kwak, **Hyeonmin Lee**, Junghwan Lim, Yoojung Shin

- Registration No. 10-2265611
- South Korea, Jun 2021

### • Communication Method Based on Integrated Flat ID and System

Ted “Taekyoung” Kwon, Hyunwoo Lee, Myungchul Kwak, **Hyeonmin Lee**, Dongjun Lee, Hyunchul Oh

- Registration No. 10-2023115
- South Korea, Sep 2019

## AWARDS & FELLOWSHIPS

Seoul National University Alumni Association Scholarship

Aug 2018

Exchange Student Program to Uppsala University (Information Technology)

Fall 2014

## TALKS & PRESENTATIONS

DNS-OARC 40, Online, “Guaranteeing the integrity of DNS records using PKIX Certificates”

Feb 2023

APNIC Blog, Online post, “Under the hood of DANE mismanagement in SMTP”

Sep 2022

USENIX Security Symposium, Boston, “Under the Hood of DANE Mismanagement in SMTP”

Aug 2022

USENIX Security Symposium, Online, “A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email”

Aug 2020

## SKILLS

### Tools and Languages

Python (proficient), C/C++, Java, Go, Spark, Hadoop, Git,  $\text{\LaTeX}$ , Linux OS

### Knowledge Background

DNS, DNS Security (i.e., DNSSEC, DoT, DoH), SMTP, Email Security (i.e., STARTTLS), PKI, DANE, TLS, IoT, Edge computing

### Communication

English, Korean (native)

## MISCELLANEOUS

### Expert Research Personnel (military service)

Mar 2019 — Feb 2022

Seoul National University, Seoul, South Korea

Expert Research Personnel is a form of alternative military service (a combination of military service with the Ph.D. program) in which the service is fulfilled by carrying out research on technology. During the service, I participated in or led several research projects at Network Convergence and Security Lab, SNU. (I had not been involved in any military research project.)

## REFERENCES

### Taekyoung “Ted” Kwon ([tkkwon@snu.ac.kr](mailto:tkkwon@snu.ac.kr))

- Professor, Department of Computer Science and Engineering, Seoul National University, Seoul, South Korea

### Taejoong (Tijay) Chung ([tijay@vt.edu](mailto:tijay@vt.edu))

- Assistant Professor, Department of Computer Science, Virginia Tech, Blacksburg, VA, United States

## RESEARCH PROJECT EXPERIENCE (COMPLETE LIST)

---

### **A Study for the Future-oriented DANE-based Web Architecture to Solve Problems in the Current TLS-based Web Ecosystem**

Primary Investigator Sep 2022 — Present  
(Funded by *Post-Doctoral Domestic and Overseas Training Program - National Research Foundation of Korea*, ₩60,000,000 ≈ \$46,000)

- [Project Goal] Currently, DANE is only used with SMTP (for mail transfer). In this research, I study how the Web ecosystem will be changed if the Web adopts the DANE protocol for communication peer authentication.
- [Role] Primary Investigator / System Designer

### **Research on Secure DNS and Privacy aware Packet Filtering Technology**

Aug 2022 — Present

(Funded by *Samsung Electronics*)

- [Project Goal] This project aims to design a secure DNS environment for mobile devices, which includes analyzing the performance of DoT/DoH in the mobile environment, designing a packet filtering mechanism based on DNS packets.
- [Role] System Designer / Programmer

### **Research on Traceability for Data Stability on Cloud-edge Lifecycle**

Apr 2020 — Dec 2021

(Funded by *Institute for Information and Communication Technology Promotion (IITP)*)

- [Project Goal] This project aims to develop a technology that ensures the stability and traceability of cloud data by leveraging Trusted Execution Environment (TEE).
- [Role] Programmer

### **Abnormal Detection and Forensic Techniques using IoT Network Traffic Analysis**

Mar 2021 — Nov 2021

(Funded by *Korea Institute of Information Security & Cryptology (KIISC)*)

- [Project Goal] This project aims to develop a system that detects anomalies (or attacks) in IoT networks and generates evidence for digital forensics by collecting IoT network traffic.
- [Role] Project Manager (Lab.) / System Designer / Programmer

**Versatile Network System Architecture for Multi-dimensional Diversity** This project aims to design a network architecture that covers diverse network devices, services, or resources, especially, in the edge network. Apr 2016 — Dec 2020

(Funded by *Institute for Information and Communication Technology Promotion (IITP)*)

- [Project Goal] This project aims to design a network architecture that covers diverse network devices, services, or resources, especially, in the edge network.
- [Role] Project Manager (Lab.) / System Designer / Programmer

### **Research on GPU Acceleration for Fully Homomorphic Encryption**

Feb 2020 — Nov 2020

(Funded by *Korea Institute of Information Security & Cryptology (KIISC)*)

- [Project Goal] This project aims to accelerate Fully Homomorphic Encryption (FHE) techniques using GPUs, including research that reduces CPU-GPU interaction and CPU-to-GPU memory dependencies.
- [Role] Programmer

### **Research on Distributed Web Structure and Counterplan**

Aug 2019 — Nov 2019

(Funded by *Korea Internet and Security Agency (KISA)*)

- [Project Goal] The project aims to analyze trends in the Distributed Web and draw a blueprint for applying it to the domestic web ecosystem.
- [Role] Researcher

### **Research on Trust and Security Scheme for Interconnection of Heterogeneous Networks**

Sep 2018 — Nov 2018

(Funded by *Electronics and Telecommunications Research Institute (ETRI)*)

- [Project Goal] The purpose of this task is to analyze the authentication and networking methods of diverse IoT products and to propose a new framework to solve problems arising in heterogeneous network environments.
- [Role] Researcher

### **Research and Development of Open 5G Reference Model**

Aug 2016 — Feb 2019

(Funded by *Giga KOREA Foundation*)

- [Project Goal] This project aims to develop an open-source 5G reference model and implement a simulator to test it.
- [Role] System Designer / Programmer

### **Development of Network Security Acceleration for Next-generation Low-power SoC**

Jul 2015 — Dec 2015

(Funded by *Samsung Electronics*)

- [Project Goal] This project aims to design a system that reduces the overhead of the TLS handshake through a delegation in communications among low-power devices.
- [Role] Programmer