min0921110@gmail.com

Hyeonmin Lee

Network Security Researcher

hyeonminlee1110
hyeonmin-lee.github.io/

I'm a postdoctoral researcher at Seoul National University. My research interests lie in network security. I've participated in (or led) diverse network security projects with institutions such as Virginia Tech (VT), Rochester Institute of Technology (RIT), University of Twente, KAIST, SIDN Labs, NLnet Labs, etc. Also, I've performed large-scale network measurement research to analyze network security *in practice*.

Research Interests

I'm interested in solving security problems in the real world. And the current interests lie in the security of DNS and Email:
(1) How can we solve the security problems that DNS and Email have?
(2) Also, How can we solve other network problems by leveraging DNS or Email protocols?

- **Security of Email**
  My research aims to solve security problems in the email system. Especially, SMTP has no security mechanism in its initial design. Thus, there are no authentication of a sender and no encryption of email contents. To solve this problem, STARTTLS was proposed, but it has a critical problem – vulnerable to downgrade attacks. I do research to mitigate this problem.
- **Security of DNS**
  DNS was also designed without any security features and DNSSEC was introduced 20 years ago to guarantee the integrity of DNS messages. However, DNSSEC shows a very low deployment ratio (7%), thus, the vast majority of DNS messages in the real world are still vulnerable to integrity attacks like DNS cache poisoning attacks. To solve the challenge, I investigate a practical and deployable way to guarantee the integrity of DNS messages by leveraging PKIX certificates.
- **Leveraging DNS or Email protocols to solve other network problems**
  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 challenge, I designed a novel technique that publishes a server's cryptographic information for the TLS handshake as DNS records. A client can fetch a server's IP address and Z-data simultaneously and sends encrypted data with a 0-RTT delay. This work is the first approach that leverages DNS to reduce network latency in the TLS handshake.

  Also, I do research about applying the DANE protocol to the Web ecosystem. The current Web works based on the CA-based PKI model but it has been criticized due to the vulnerabilities that CAs have — CAs have been compromised and issued fraudulent certificates to attackers. DANE protocol was proposed to authenticate communication peers without CAs, but currently, it is only used for mail transmission. Thus, I investigate how the Web ecosystem can adopt the DANE protocol.

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?"
- [Supervisors] 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 **Apr 2022 — Present**
Seoul National University *Seoul, South Korea*

- [Web and DANE] Study how the Web ecosystem will be changed if the Web adopts DANE protocol (Achievement - Grant).
- [STARTTLS] Investigate how to prevent STARTTLS downgrade attacks.
- [DNS and TLS] Analyze how DNS can be exploited to reduce 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 **Mar 2016 — Feb 2022**
Seoul National University *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 Researcher **May 2019 — Aug 2019**
Rochester Institute of Technology *Rochester, USA*

- [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 Sep 2022 — Aug 2023
(Funded by *Post-Doctoral Domestic and Overseas Training Program - National Research Foundation of Korea*, ₩60,000,000 ≈ $46,000)

- [Research 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 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'm investigating a way to filter packets using DNS packets and implementing it on BIND9.

Project Manager **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'm investigating a way to filter packets using the information in DNS messages and implementing it on BIND9.

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, LaTeX
Quantitative Research Network Security, DNS Security (i.e., DNSSEC, DoT, DoH), Email Security (i.e., SMTP, STARTTLS), Public Key Infrastructure (PKI), Transport Layer Security (TLS), Internet of Things (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)
- Professor, Department of Computer Science and Engineering, Seoul National University, Seoul, South Korea

Taejoong (Tijay) Chung (tijay@vt.edu)
- Assistant Professor, Department of Computer Science, Virginia Tech, Blacksburg, VA, United States

Research Project Experience (Complete List)

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