

Kangkook Jee

Computer Science Dept., University of Texas at Dallas
800 West Campbell Road, EC-31 Richardson, TX 75080

✉ kangkook.jee@utdallas.edu | 🏠 kangkookjee.io

Research Statement

Dr. Kangkook Jee has been an Assistant Professor in the Computer Science Department at the University of Texas at Dallas since 2019. Dr. Jee earned his doctorate in Computer Science from Columbia University under the supervision of Prof. Angelos D. Keromytis. Before joining UT Dallas, he spent five years at NEC Laboratories America as a security researcher, tackling a diverse set of real-world security problems. Throughout his academic career, he has published over 50 academic papers and has been awarded patents addressing research challenges in computer systems, cybersecurity, and machine learning domains. Dr. Jee's current research interests primarily span across three thrusts of (1) system provenance, (2) reversing and decompilation of high-level dynamic languages, and (3) safety and security of small satellites in Low Earth Orbit (LEO).

Advanced Security with system provenance: Dr. Jee's system provenance research extends a comprehensive and fine-grained system event collection framework deployed in real-world environments, such as research servers and administrative computers. Dr. Jee's group is among the few research groups capable of collecting and generating system provenance datasets through a mature data collection and analysis framework. Dr. Jee's research typically utilizes two distinct data collection infrastructures: one for benign networks and another for malicious networks. Dozens of hosts from real-world environments constantly report their system call-level events to the data collection backends. Concurrently, hosts from malicious testbed environments run the latest malware samples and advanced attack vectors to capture the behavioral specifics of contemporary attacker tactics. Over the last four years, the system provenance datasets have amassed over 40 TB of data from both benign and malicious environments.

Reversing and decompilation of HDLs. Software products and malware payloads are increasingly packaged in High-level Dynamic Languages (HDLs) bytecode representation to (1) reduce development efforts, (2) support memory safety, and (3) seamlessly support heterogeneous architectures and diverse execution environments. Many HDLs compile their programs into specific bytecode formats that are compatible with and run on different computing models, such as stack-based VMs. This shift from traditional software development and deployment scenarios, which focused exclusively on compiling regular binaries into the underlying machine code, marks a significant trend. Despite this transition, there is a notable lack of proper support for reversing and decompilation toolchains within the community. For instance, there is no fully functioning decompiler for Python; the most advanced decompiler available offers only partial support for Python 3.8, even though the language's latest official release is version 3.12.

Security and Safety of Small Satellites in LEO. Security and Safety of Small Satellites: Dr. Jee's research delves into the security and safety concerns associated with small satellites, which are becoming increasingly prevalent occupants of LEO due to innovations in affordable rocket boosters and advancements in smaller, more powerful microelectronics (ME) technologies.

His involvement in space security research began with an industry collaboration with IBM Space, leading to the launch of the Endurance CubeSat for science and community outreach purposes. With two years of comprehensive experience in planning, preparation, launch, and post-launch operations, Dr. Jee has established a solid foundation in space security research. This experience has facilitated the acquisition of an NSF grant focused on Space CyberInfrastructure and enabled his active participation in conference presentations within the space research community. Given his unique expertise in the space domain, Dr. Jee has been a pivotal technical panelist at the NSF SaTC workshop, leading sessions on the future of cybersecurity education.

Education

Ph.D. in Computer Science

COLUMBIA UNIVERSITY

New York, USA

2016

- Ph.D. Thesis: "On Efficiency and Accuracy of Data Flow Tracking Systems"
- Academic Advisor: Angelos D. Keromytis

M.Phil. in Computer Science

COLUMBIA UNIVERSITY

New York, USA

2012

M.Sc. in Computer Science

COLUMBIA UNIVERSITY

New York, USA

2007

B.S. in Mathematics & Computer Science

KOREA UNIVERSITY

Seoul, South Korea

Mar 2000

Work Experience

University of Texas, at Dallas

ASSISTANT PROFESSOR, COMPUTER SCIENCE DEPARTMENT

Richardson, TX

Aug 2019 - Present

NEC Laboratories America

RESEARCHER, COMPUTER SECURITY DEPARTMENT

Princeton, NJ

Sep 2014 - Jul 2019

IBM Korea

ADVANCED TECHNICAL SUPPORT STAFF

Seoul, South Korea

Mar. 2001 - Aug. 2006

18 Medical Company, 8th U.S. Army

INFORMATION MANAGEMENT STAFF

Seoul, South Korea

Jan 1997 - Mar 1999

Publications

CONFERENCE PUBLICATIONS

- C1 K. Mukherjee, J. D. Wiedemeier, Q. Wang, J. Kamimura, J. Rhee, J. Wei, Z. Li, X. Yu, L. Tang, J. Gui, **K. Jee** "ProvIoT: Detecting Stealthy Attacks in IoT through Federated Edge-Cloud Security". International Conference on Applied Cryptography and Network Security (ACNS), Mar 2024.
- C2 Z. Zhen, Y. Chen, M. Kantarcioglu, Y. Gel, **K. Jee** "United We Stand, Divided We Fall: Networks to Graph (N2G) Abstraction for Robust Graph Classification under Graph Label Corruption". In Learning on Graphs Conference (LOG), Dec 2023.
- C3 C. Wang, Y. Zhou, **K. Jee**, M. Kantarcioglu, "An Investigation on the Fragility of Graph Neural Networks: The Impact of Node Feature Modification on Graph Classification Accuracy". IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Nov 2023
- C4 K Mukherjee, J Wiedemeier, T Wang, J Wei, M Kim, M Kantarcioglu, **K Jee** "Evading Provenance-Based ML Detectors with Adversarial System Actions". In Proceedings of the USENIX Security Symposium, Anaheim CA, August 2023.
- C5 H. Kim, S. Kim, J. Lee, **K. Jee**, S. Cha "Reassembly is Hard: A Reflection on Challenges and Strategies". In Proceedings of the USENIX Security Symposium, Anaheim CA, August 2023.
- C6 **K. Jee**, M. Lee, O. Daescu, M. Quevedo-Lopez "A Hands-on Oriented Workforce Development Framework for Space Cyber-Infrastructure (CI)". In Proceedings of ISS Research Development Conference (ISSRDC), Aug. 2023
- C7 P. Fang, P. Gao, C. Liu, E. Ayday, **K. Jee**, T. Wang, Y. Ye, Z. Liu, X. Xiao "Back-Propagating System Dependency Impact for Attack Investigation". In Proceedings of the USENIX Security Symposium, Boston MA, August 2022.
- C8 P. Fei, Z. Li, Z. Wang, X. Yu, D. Li, **K. Jee** Kulkarni, P. Mittal "SEAL: Storage-efficient Causality Analysis on Enterprise Logs with Query-friendly Compression". In Proceedings of the USENIX Security Symposium, Vancouver, BC, August 2021.
- C9 Y. Li, Z. Wu, H. Wang, K. Sun, Z. Li, **K. Jee**, J. Rhee, H. Chen "Utrack: Enterprise User Tracking Based on OS-Level Audit Logs". In Proceedings of ACM Conference on Data and Application Security and Privacy (CODASPY), April 2021.
- C10 W. U. Hassan, D. Li, **K. Jee**, X. Yu, K. Zou, D. Wang, Z. Chen, Z. Li, J. Rhee, J. Gui, A. Bates "This is Why We Can't Cache Nice Things: Lightning-Fast Threat Hunting using Suspicion-Based Hierarchical Storage". In Proceedings of Annual Computer Security Applications Conference (ACSAC), December 2020
- C11 Y. Sun, **K. Jee**, S. Sivakorn, Z. Li, C. Lumezanu, L. Kort-Parn, Z. Wu, J. Rhee, C. Kim, M. Chiang, P. Mittal "Detecting Malware Injection with Program-DNS Behavior". In Proceedings of The European Conference on Security and Privacy (EuroS&P), Genova Italy, September 2020

- C12 G. Ayoade, K. Akbar, Pracheta S., Yang G., Agarwal A., **K. Jee**, L. Khan, A. Singhai “Evolving Advanced Persistent Threat Detection using Provenance Graph and Metric Learning”. in IEEE Conference on Communications and Network Security (CNS), Avignon, France, 2020
- C13 J, D. Li, Z. Chen, J. Rhee, X. Xiao, M. Zhang, **K. Jee**, Z. Li, and H. Chen “APTrace: A Responsive System for Agile Enterprise Level Causality Analysis,” In Proceedings of the IEEE International Conference on Data Engineering (ICDE), Dallas, TX, May 2020
- C14 J. Gui, D. Li, Z. Chen, J. Rhee, X. Xiao, M. Zhang, **K. Jee**, Z. Li, and H. Chen “APTrace: A Responsive System for Agile Enterprise Level Causality Analysis,” In Proceedings of the IEEE International Conference on Data Engineering (ICDE), Dallas, TX, May 2020
- C15 Q. Wang, W. U. Hassan, D. Li, **K. Jee**, X. Yu, K. Zou, J. Rhee, Z. Chen, W. Cheng, C. A. Gunter, and H. Chen, “You Are What You Do: Hunting Stealthy Malware via Data Provenance Analysis,” In Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA, 2020.
- C16 S. Sivakorn , **K. Jee**, Y. Sun, L. Kort-Parn, Z. Li, C. Lumezanu, Z. Wu, L. Tang, D. Li “Countering Malicious Processes with Endpoint DNS Monitoring”. In Proceedings of The Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 2019
- C17 W. U. Hassan, S. Guo, D. Li, Z. Chen, **K. Jee**, Z. Li, A. Bates “NoDoze: Combatting Threat Alert Fatigue with Automated Provenance Triage”. In Proceedings of The Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 2019
- C18 Y. Tang, D. Li, Z. Li, M. Zhang, **K. Jee**, Z. Wu, J. Rhee, X. Xiao, F. Xu, Q. Li “NodeMerge: Template Based Efficient Data Reduction For Big-Data Causality Analysis”. In Proceedings of the 25th ACM Conference on Computer and Communications Security (CCS), Toronto, Canada, November 2018.
- C19 P. Gao, X. Xiao, D. Li, Z. Li, **K. Jee**, Z. Wu, C. Kim, S. R. Kulkarni, P. Mittal “SAQL: A Stream-based Query System for Real-Time Abnormal System Behavior Detection”. in Proceedings of the USENIX Security Symposium, August 2018, Baltimore, MD, August 2018.
- C20 P. Gao, X. Xiao, Z. Li, **K. Jee**, F. Xu, S. R. Kulkarni, P. Mittal “AIQL: Enabling Efficient Attack Investigation from System Monitoring Data”. In Proceedings of Usenix Annual Technical Conference (ATC), Boston, MA, June 2018.
- C21 Y. Liu, M. Zhang, D. Li, **K. Jee**, Z. Li, Z. Wu, J. Rhee, P. Mittal “Towards a Timely Causality Analysis for Enterprise Security” In Proceedings of The Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 2018
- C22 Z. Xu, Z. Wu, Z. Li, **K. Jee**, J. Rhee, X. Xiao, F. Xu, H. Wang, G. Jiang “High fidelity data reduction for big data security dependency analyses” In Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS), Vienna, Austria, November 2016.
- C23 M. Pomonis, T. Petsios, **K. Jee**, M. Polychronakis, A. D. Keromytis “IntFlow: improving the accuracy of arithmetic error detection using information flow tracking” In Proceedings of Annual Computer Security Applications Conference (ACSAC), New Orleans, LA, December 2014.
- C24 **K. Jee**, V. P. Kemerlis, A. D. Keromytis and G. Portokalidis “ShadowReplica: Efficient Parallelization of Dynamic Data Flow Tracking” In Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS), Berlin, Germany, November 2018.
- C25 V. P. Kemerlis, G. Portokalidis, **K. Jee**, and A. D. Keromytis “libdft: Practical Dynamic Data Flow Tracking for Commodity System” In Proceedings of 8th Annual International Conference on Virtual Execution Environments (VEE), London, UK, March 2012.
- C26 **K. Jee**, G. Portokalidis, V. P. Kemerlis, S. Ghosh, D. I. August, and A. D. Keromytis “A General Approach for Efficiently Accelerating Software-based Dynamic Data Flow Tracking on Commodity Hardware” In Proceedings of The Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 2012
- C27 **K. Jee**, S. Sidiroglou-Douskos, A. Stavrou, and A. D. Keromytis. “An Adversarial Evaluation of Network Signaling and Control Mechanisms” In Proceedings of the 13th International Conference on Information Security and Cryptology (ICISC), Seoul, South Korea, December 2010.

JOURNALS

- B1 K. Hayashi, **K. Jee**, O. Lascu, H. Pienaar, S. Schreitmueller, T. Tarquinio, J. Thompson “AIX 5L Practical performance and tuning guide” published by IBM Press books, ISBN-0738491799 , March 2005

DEMO PAPERS

- D1 P. Gao, X. Xiao, D. Li, **K. Jee**, H. Chen, S. Kulkarni, and P. Mittal, “*Querying Streaming System Monitoring Data for Enterprise System Anomaly Detection.*” Presented at the IEEE International Conference on Data Engineering (ICDE), Dallas TX, May 2020.
- D2 P. Gao, X. Xiao, Z. Li, **K. Jee**, F. Xu, S. R. Kulkarni, P. Mittal “*A Query System for Efficiently Investigating Complex Attack Behaviors for Enterprise Security.*” Presented at the International Conference on Very Large Data Bases (VLDB), Los Angeles, CA, August 2019.

BOOKS

- B1 K. Hayashi, **K. Jee**, O. Lascu, H. Pienaar, S. Schreitmueller, T. Tarquinio, J. Thompson “*AIX 5L Practical performance and tuning guide*” published by IBM Press books, ISBN-0738491799 , March 2005

Proposal and Funding

CURRENT

- F1 NSF 2321117: CyberTraining: Pilot: CyberTraining for Space CI in Low Earth Orbit (LEO)
PI, 11/1/23 - 10/31/25, Current budget \$299,999
- F2 NSF 2331424: EAGER: Privacy Preserving Synthetic Graph Generation for System Provenance
PI, 10/1/23 - 9/30/25, Current budget \$250,003

PENDING (SUBMITTED)

- F1 : Developing technology for analyzing satellite attack surface and detecting vulnerabilities in networks and firmware
Submitted to IITP, South Korea 4/1/24 - 3/31/28, Current budget \$700,000

PAST AWARDED

- F1 UT System: VA Apprenticeship: Cybersecurity Testbed Environment for Workforce Development
PI, 2/1/22 - 1/31/23, Current budget \$120,000

Patents

PATENTS

- P1 Confidential machine learning with program compartmentalization.
CH Kim, J Rhee, **K Jee**, LI Zhichun US Patent 11,423,142 issued on Aug 2022.
- P2 Graphics processing unit accelerated trusted execution environment.
CH Kim, J Rhee, **K Jee**, LI Zhichun, A Ahmad, H Chen US Patent 11,295,008 issued on Apr 2022.
- P3 Real-time threat alert forensic analysis
D Li, **K Jee**, LI Zhichun, Z Chen, X Yu US Patent 11,275,832 issued on Dec 2020.
- P4 User-added-value-based ransomware detection and prevention.
Z Wu, Y Li, J Rhee, **K Jee**, Z Li, J Kamimura, LA Tang, Z Chen US Patent 11,223,649 issued on Jan 2022.
- P5 Automated threat alert triage via data provenance.
D Li, **K Jee**, Z Chen, LI Zhichun, WU Hassan US Patent 11,194,906 issued on Dec 2021.
- P6 Inter-application dependency analysis for improving computer system threat detection D Li,**K Jee** , Z Chen, LA Tang, LI Zhichun US Patent 11,030,308 issued on Jun 2021.
- P7 Template based data reduction for commercial data mining.
D Li,**K Jee** , LI Zhichun, M Zhang, Z Wu US Patent 11,030,157 issued on Jun 2021.
- P8 Host behavior and network analytics based automotive secure gateway.
J Rhee, H Li, HAO Shuai, CH Kim, Z Wu, LI Zhichun, **K Jee**, L Korts-Parn US Patent 10,931,635 issued on Feb 2021.
- P9 Automated software safeness categorization with installation lineage and hybrid information sources
J Rhee, Z Wu, L Korts-Parn, **K Jee**, LI Zhichun, O Setayeshfar US Patent 10,929,539 issued on Feb 2021.

- P10 Path-based program lineage inference analysis.
J Rhee, Z Wu, L Korts-Parn, **K Jee**, LI Zhichun, O Setayeshfar US Patent 10,853,487 issued on Dec 2020.
- P11 Template based data reduction for security related information flow data.
D Li, **K Jee**, LI Zhichun, M Zhang, Z Wu US Patent 10,733,149 issued on Feb 2020.
- P12 Automated blackbox inference of external origin user behavior Z Wu, J Rhee, J Yuseok, LI Zhichun, **K Jee**, G Jiang US Patent 10,572,661 issued on Feb 2020.
- P13 Host level detect mechanism for malicious DNS activities **K Jee**, LI Zhichun, G Jiang, L Korts-Parn, Z Wu, Y Sun, J Rhee US Patent 10,574,674 issued on Feb 2020.
- P14 Blackbox program privilege flow analysis with inferred program behavior context J Rhee, J Yuseok, LI Zhichun, **K Jee**, Z Wu, G Jiang US Patent 10,505,962 issued on Dec 2019.
- P15 Fine-grained analysis and prevention of invalid privilege transitions.
J. Rhee, Y. Jeon, Z. Li, **K Jee**, Z. Wu, and G. Jiang. US Patent 10,402,564 issued on Sep 2019.
- P16 Extraction and comparison of hybrid program binary.
J. Rhee, Z. Li, Z. Wu, **K. Jee**, and G. Jiang. US Patent 10,289,843 issued on May 2019.

Teaching

CS4459: Cyber Attack and Defense Laboratory (CANDL)

Dallas, TX

UNIVERSITY OF TEXAS AT DALLAS

Spring 2023 - 2021

The CANDL is a hands-on security lab course that teaches a broad range of offensive and defensive techniques for computer systems. Specifically, the course consists of eight units featuring hands-on labs in a CTF format in binary reversing and pwning techniques, covering topics from introductory (e.g., stack overflow, shellcode) and intermediate levels (e.g., ROP, format string vulnerabilities) and advanced topics (e.g., heap exploits). The course also covers vulnerability analysis, exploit development, patching vulnerabilities, bug hunting etc.

CS4301: Cyber Attack and Defense Laboratory (CANDL)

Dallas, TX

UNIVERSITY OF TEXAS AT DALLAS

Spring 2021 - 2023

First launched in Spring 2021 as a 3-credit hour, special topic course, the CS4301 has attracted many undergraduates over three years. The course teaches offensive and defensive techniques for computer systems, covering introductory to intermediate binary reversing and exploitation techniques, including vulnerability analysis, exploit development, and bug hunting. It features eight units of hands-on labs with CTF-style challenges Starting Spring 2024, we will expand this hands-on binary reversing and hacking course, incorporating CTF challenges, to a four-credit hour, security elective (CS4459).

CS6332: System Security and Binary Code Analysis

Dallas, TX

UNIVERSITY OF TEXAS AT DALLAS

Fall 2019 - present

CS6332, a graduate-level course, focuses on the fundamental principles of recent system security research, emphasizing the software execution stack in various system architectures, including desktops, servers, and IoT devices. It examines the impact of system characteristics on security across hardware architectures like x86, AMD64, and ARM, and discusses securing software execution layers, such as code generation pipelines, process-level virtualization, and container environments. The course also tackles the challenges of code generation, deployment, and reversing, especially regarding dynamic language interpreters

CS7301: Advanced topics in System Security

Dallas, TX

UNIVERSITY OF TEXAS AT DALLAS

Spring 2020

The graduate-level, special-topic course comprises three parts. The first offers a historical and principled overview of notable attacks and their defenses, reviewing key static and dynamic techniques used in defense strategies. The second part explores cutting-edge topics in system security research, covering provenance analysis, the Internet of Things (IoT), and Industrial Control Systems/Cyber-Physical Systems (ICS/CPS), to understand and extend traditional methods to new challenges. Finally, we examine machine learning's role in solving modern system security problems.

Introduction to Programming (COMSW3101-003)

NY, New York

COLUMBIA UNIVERSITY

Fall 2013

- Designed and taught a course, Programming with Python as a graduate research assistant (Enrollment: 14, rating 4.5/5.0)

Student Advising

The University of Texas at Dallas

PH.D. STUDENTS

- Kunal Mukherjee, 2019 Fall ~
- Joshua D. Weidemeier, 2022 Fall ~
- Jaehyun Park, 2023 Fall ~

MASTER STUDENTS

- Albert Shouh-Cherng Jean, 2024 Spring ~
- Nick D. Baker, post-graduation appointment: Amazon Web Service (Spring 2023)
- Jonathan Yu, post-graduation appointment: American Airline (Fall 2022 ~ Spring 2023)
JSUGRA: Jonsson School Undergraduate Research Award (Spring 2023)
- Jerry Teng, (Fall 2021 ~ Spring 2023)
- James A. Wei, post-graduation appointment: Livermore National Lab (Summer 2021 ~ Fall 2022)
- Henry H. Wang, post-graduation appointment: Microsoft (Fall 2019 ~ Spring 2021)

UNDERGRADUATE STUDENTS

- Logan S. Cheung, (Summer 2022, Spring 2024~)
Clark Summer Research Scholar (Summer 2022)
- Elliot M. Tarbet, (Spring 2023 ~ Spring 2024)
- Anthony T. Maranto, post-graduation appointment: Dell (Summer 2021~ Spring 2022)
- Guangze Zu, post-graduation appointment: Meta (Spring 2022)
- David J. Wank, (Spring 2021 ~ Spring 2023)
JSUGRA: Jonsson School Undergraduate Research Award (Spring 2022)

Columbia University

STUDENTS ADVISING

- Fall 2013: Marios Pomonis, Theofilos Petsios (Ph.D. candidates at Columbia University)
Project: Arithmetic error detection using information flow tracking with compiler-assisted program instrumentation.
- Spring 2013: Daniel Song (MS student at Columbia University, currently a Ph.D. candidate at Rice University)
Project: A comparison study of Dynamic Binary Instrumentation (DBI) frameworks
- Fall 2012: Mengqi Zhang (MS student Columbia University, currently a software engineer at Facebook)
Project: Compiler (LLVM) assisted program instrumentation and hardening

NEC Labs America

INTERN ADVISING

- Summer 2019: Qi Wang (Ph.D. candidate at UIUC).
Project: SplitBrain: Edge-Cloud Collaborative Security for IoT.
- Summer 2018: Qi Wang (Ph.D. candidate at UIUC).
Project: End-point Detection and Response for IoT Devices.
- Summer 2017: Suphanee Sivakorn (Ph.D. candidate at Columbia University).
Project: System to Detect Malicious Processes with End-point DNS Monitoring.
- Summer 2016: Yixin Sun (Ph.D. candidate at Princeton University).
Project: Analyzing Program DNS Behavior under Malware Injection.
- Summer 2015: Yasser Shalabi (Ph.D. candidate at UIUC).
Project: Fast and efficient system event collection from Linux kernel.

Service

NSF PANEL

- Review Panelist** NSF SaTC, Jan 2024, Virtual
- Technical Panelist** NSF SaTC EDU Workshop, Nov 2023, Dallas TX
- Invited Participant** NSF SaTC Vision 2.0 Workshop, Mar 2023, Dallas TX
- Review Panelist** NSF IIS, Mar 2020, Virtual

TECHNICAL PROGRAM COMMITTEE MEMBER

- Usenix Security 2024** Program Committee Member
- ISC 2023** Program Committee Member
- WISA 2021** Program Committee Member
- ToPP 2021** Program Committee Member
- ACSAC 2020** Cloud Security Session Chair
- ICDE 2020** Ph.D forum Session Chair
- SiMLA 2020** Security in Machine Learning and its Applications
- ISC 2016** International Conference on Information Security Conference

Talks

INVITED TALKS

Feb 2023	“Enhancing System Provenance through Efficient Fine-Grained Data Flow Tracking”	<i>AWS security seminar, Virtual</i>
Jul 2022	“Hardware Safety and Security in Space Environments”	<i>SKKU, Suwon, South Korea</i>
Jul 2022	“Machine Learning Security for System Provenance Research”	<i>AI Sec Workshop, Hongcheon, South Korea</i>
Sept 2021	“Data Driven Approach for System Security”	<i>Korea University, Seoul South Korea</i>
July 2021	“Data Driven Approach for System Security”	<i>Soongsil University, Seoul South Korea</i>
Apr 2019	“Finding Flow: Connecting the Dots to Disclose Attacker Trails”	<i>NSR (National Security Research Institute), Daejeon, South Korea</i>
Apr 2019	“Finding Flow: Connecting the Dots to Disclose Attacker Trails”	<i>KAIST, Daejeon, South Korea</i>
Apr 2019	“Finding Flow: Connecting the Dots to Disclose Attacker Trails”	<i>SKKU, Suwon, South Korea</i>
Dec 2018	“Research Challenges and Opportunities in End-point Detection and Response (EDR)”	<i>Security & Privacy PIC Seminar Series, IBM Watson Research</i>
Oct 2013	“ShadowReplica: Efficient Parallelization of Dynamic Data Flow Tracking”	<i>Security Group Seminar, Stevens Institute of Technology</i>
Jun 2012	“A General Approach for Efficiently Accelerating Software-based Dynamic Data Flow Tracking on Commodity Hardware”	<i>IBM PL Day, IBM T. J. Watson Research Center</i>
Mar 2011	“A General Approach for Efficiently Accelerating Software-based Dynamic Data Flow Tracking on Commodity Hardware”	<i>Liberty Group Seminar, Princeton University</i>

CONFERENCE PRESENTATIONS

Aug 2023	“A Hands-on Oriented Workforce Development Framework for Space Cyber-Infrastructure (CI)”	<i>ISSRDC, Seattle WA</i>
Feb 2019	“Countering Malicious Processes with Process-DNS Association”	<i>NDSS, San Diego, CA</i>
Nov 2018	“NodeMerge: Template Based Efficient Data Reduction For Big-Data Causality Analysis”	<i>ACM CCS, Toronto, Canada</i>
Nov 2013	“ShadowReplica: Efficient Parallelization of Dynamic Data Flow Tracking”	<i>ACM CCS, Berlin, Germany</i>
Feb 2012	“A General Approach for Efficiently Accelerating Software-based Dynamic Data Flow Tracking on Commodity Hardware”	<i>NDSS, San Diego, USA</i>
Dec 2010	“An Adversarial Evaluation of Network Signaling and Control Mechanisms”	<i>ICISC, Seoul, South Korea</i>

Honors & Awards

May 2022	Teaching Award , Eric Johnson school of Computer Science and Engineering	<i>Richardson, TX</i>
May 2021	Service Award , Computer Science Department, UT Dallas	<i>Richardson, TX</i>
Mar 2020	IEEE Big Data Security Junior Research Award , IEEE Big Data Security, 2020	<i>Baltimore, USA</i>
Aug 2016	CEATEC Award, Innovation for better society , CEATEC Japan CPS/IoT Exhibition	<i>Tokyo, Japan</i>
2014	2nd Place CyberSecurity for the Next Generation 2014: Americas Round , Kaspersky lab	<i>Washington, DC</i>
2008-2014	Graduate Fellowship , Graduate Research Assistantship (GRA), Columbia University	<i>New York, USA</i>
2003-2005	IBM top-talented group (resource pool for future executives) , IBM Korea	<i>Seoul, South Korea</i>
2005	Employee education program with full tuition support , IBM Korea	<i>Seoul, South Korea</i>
2004	IBM Stock option (500 stocks) , IBM Korea	<i>Seoul, South Korea</i>
2000	Army Commendation Medal , 8th U.S. Army	<i>Seoul, South Korea</i>

Service

NSF PANEL

Review Panelist NSF SaTC, Jan 2024, Virtual
Technical Panelist NSF SaTC EDU Workshop, Nov 2023, Dallas TX
Review Panelist NSF IIS, Mar 2020, Virtual

TECHNICAL PROGRAM COMMITTEE MEMBER

Usenix Security 2024 Program Committee Member
ISC 2023 Program Committee Member
WISA 2021 Program Committee Member
ToPP 2021 Program Committee Member
ACSAC 2020 Cloud Security Session Chair
ICDE 2020 Ph.D forum Session Chair
SiMLA 2020 Security in Machine Learning and its Applications
ISC 2016 International Conference on Information Security Conference