Kangkook **Jee**

Assistant professor · Security Researcher

800 W. Campbell Rd. Richardson, TX 75080

(+1) 972-883-3863 | kangkook.jee@utdallas.edu | https://kangkookjee.io | jikk | kangkook.jee

Research Interests

Dr. Jee has primarily focused on the following three research areas: First, system provenance research, which involves implementing fine-grained data collection to establish large-scale datasets and conducting various analysis studies to combat stealthy attack vectors by advanced adversaries. Second, the safety and security of spacecraft, primarily due to the ever-increasing number of satellite launches and overcrowded satellites in Low Earth Orbit (LEO). Lastly, the challenges surrounding the disassembly and decompilation of binaries at different levels. In particular, Dr. Jee is highly interested in scaling reverse engineering processes, which are known to be highly customized and therefore expensive, while providing a certain level of accuracy guarantee.

Education

Ph.D. in Computer Science — *New York, USA*

Columbia University — *2016*

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

M.Phil. in Computer Science — *New York, USA*

Columbia University — *2012*

M.Sc. in Computer Science — *New York, USA*

Columbia University — *2007*

B.S. in Mathematics & Computer Science — *Seoul, South Korea*

Korea University — *Mar 2000*

Publications

Conference Publications

C1 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.

C2 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.

C3 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.

C4 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.

C5 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.

C6 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

C7 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

C8 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

C9 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

C10 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

C11 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.

C12 S. Sivakorn , **K. Jee**, Y. Sun, L. Kort-Parn, Z. Li, C. Lumezanu, Z. Wu, L. Tang, D. Li *"Countering Malicious Processes with End-point DNS Monitoring"*. In Proceedings of The Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 2019

C13 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

C14 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.

C15 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.

C16 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.

C17 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

C18 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.

C19 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.

C20 **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.

C21 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.

C22 **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

C23 **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 Angelos, 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

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 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.

P3 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.

P4 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.

P5 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.

P6 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.

P7 Graphics processing unit accelerated trusted execution environment.
CH Kim, J Rhee, **K Jee**, LI Zhichun, A Ahmad, H Chen US Patent App. 16/787,610 issued on Aug 2020

P8 Real-time threat alert forensic analysis
D Li, **K Jee**, LI Zhichun, Z Chen, X Yu US Patent App. 16/781,366 issued on Aug 2020

P9 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 Aug 2020

P10 Confidential machine learning with program compartmentalization.
CH Kim, J Rhee, **K Jee**, LI Zhichun US Patent App. 16/693,710 issued on Jun 2020

P11 Blackbox program privilege flow analysis with inferred program behavior context.
J. Rhee, Y. Jeon, L. I. Zhichun, **K. Jee**, Z. Wu, and G. Jiang. US Patent App. 10/505,962 issued on Dec 2019.

P12 User-added-value-based ransomware detection and prevention.
Z. Wu, Y. Li, J. Rhee, **K. Jee**, Z. Li, J. Kamimura, L. Tang, and Z. Chen. US Patent App. 16/379,024 issued on Nov 2019.

P13 Fine-grained analysis and prevention of invalid privilege transitions.
J. Rhee, Y. Jeon, Z. Li, K. Jee, Z. Wu, and G. Jiang. US Patent App. 15/623,589 issued on Sep 2019.

P14 Extraction and comparison of hybrid program binary.
J. Rhee, Z. Li, Z. Wu, **K. Jee**, and G. Jiang. US Patent App. 15/479,928 issued on May 2019.

P15 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 App. 16/146,166 issued on Apr 2019.

P16 Inter-application dependency analysis for improving computer system threat detection.
D Li, **K Jee**, Z Chen, LA Tang, LI Zhichun. US Patent App. 16/006,164 issued on Feb 2019.

P17 Path-based program lineage inference analysis.
J Rhee, Z Wu, L Korts-Parn, **K Jee**, LI Zhichun, O Setayeshfar. US Patent App. 16/039,993 issued on Feb 2019.

P18 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 App. 16/040,086 issued on Feb 2019.

P19 Timely causality analysis in homogeneous enterprise hosts.
M Zhang, **K Jee**, Z Li, D Li, Z Wu, J Rhee. US Patent 15/972,911 issued on Nov 2018.

P20 Template based data reduction for security related information flow.
data. D Li, **K Jee**, Z Wu, M Zhang, Z Li. US Patent 15/979,512 issued on Nov 2018.

P21 Template based data reduction for commercial data mining.
D Li, **K Jee**, Z Wu, M Zhang, Z Li. US Patent 15/979,514 issued on Nov 2018.

P22 Blackbox Program Privilege Flow Analysis with Inferred Program Behavior.
Context. J Rhee, Y Jeon, Z LI, **K Jee**, Z Wu, G Jiang. US Patent 15/623,538 issued on Feb 2018.

P23 Fine-Grained Analysis and Prevention of Invalid Privilege Transitions.
J Rhee, Y Jeon, Z LI, **K Jee**, Z Wu, G Jiang. US Patent 15/623,589 issued on Feb 2018.

P24 Automated blackbox inference of external origin user behavior.
Z Wu, J Rhee, Y Jeon, Z Li, **K Jee**, G Jiang. US Patent 15/652,796 issued on Feb 2018.

P25 Host level detect mechanism for malicious dns activities.
K Jee, Z LI, G Jiang, L Korts-Parn, Z Wu, Y Sun, J Rhee. US Patent 15/644,018 issued on Jan 2018.

P26 Extraction and comparison of hybrid program binary features.
J Rhee, Z Li, Z Wu, **K Jee**, G Jiang. US Patent 15/479,928 issued on Oct 2017.

P27 High Fidelity Data Reduction for System Dependency Analysis.
Z Wu, Z Li, J Rhee, F Xu, G Jiang, **K Jee**, X Xiao, Z Xu. US Patent 15/416,346 issued on Aug 2017.

P28 Intrusion Detection Using Efficient System Dependency Analysis.
Z Wu, Z Li, J Rhee, F Xu, G Jiang, **K Jee**, X Xiao, Z Xu, J Rhee. US Patent 15/416,462 issued on Aug 2017.

Teaching

Cyber Attacks and Defense Laboratory (cs4301)

Dallas, TX

University of Texas at Dallas

Spring 2023 - 2021

This course aims to teach a wide spectrum of offensive and defensive techniques for computer systems. In particular, the course will cover introductory (e.g., stack overflow, shellcode) to intermediary level (e.g., heap exploits) binary reversing and pwning techniques, which include vulnerability analysis, exploit development, patching vulnerabilities, bug hunting, etc. The course comprises of eight units of hands-on labs with Capture-The-Flag (CTF) style challenges.

Advanced topics in System Security (cs7301)

Dallas, TX

University of Texas at Dallas

Spring 2020

This is a graduate-level course that mainly comprises three parts. The first part of the course will give a historical and principled overview of prominent attacks and their corresponding defensive measures. The course will review leading static and dynamic techniques that have been widely used in various defense approaches. The second part of the course will introduce emerging, frontier topics in system security research. We will cover various domains of provenance analysis, IoT, and ICS/CPS systems to learn how traditional approaches can be applied and further extended to new challenges. Lastly, the course will see how machine learning-based approaches can be applied to solve system security problems.

System Security and Binary Analysis (cs6332)

Dallas, TX

University of Texas at Dallas

Fall 2022 - 2019

The course aims to deliver the fundamental/overarching principles of the latest system security research for the layered components of software execution stack, reviewing different system architectures for desktops, servers, and embedded IoT devices.

Introduction to Programming (COMSW3101-003)

NY, New York

Columbia University

Fall 2013

- Designed and taught a course, Programming with Python (Students: 14)

Teaching Assistant

NY, New York

Columbia University

2010-2012

- Spring 2012: Teaching Assistant (TA) for Artificial Intelligence (COMSW4701)
- Fall 2010: Teaching Assistant (TA) for Introduction to Programming (COMS3157)

Student Advising

The University of Texas at Dallas

Ph.D. students

- Takemaru Kadoi: 2023 Spring ∼
- Joshua D. Weidemeier: 2022 Fall ∼
- Tianhao Wang: 2022 Spring ∼
- Kunal Mukherjee: 2019 Fall ∼

The University of Texas at Dallas

Master and undergraduate students

- Nick D. Baker, now at Amazon Web Service (2023 Spring)
- Jonathan Yu, now at American Airline (2022 Fall 2023 Spring)
  JSUGRA: Jonsson School Undergraduate Research Award (2023 Spring)
- Anthony T. Maranto, now at Dell (2021 Summer 2022 Spring)
- Jerry Teng, (2021 Fall 2023 Spring)
- Guangze Zu, now at Meta (2022 Spring)
- James A. Wei, now at Livermore National Lab (2021 Summer 2022 Fall)
- David J. Wank, (2021 Spring)
  JSUGRA: Jonsson School Undergraduate Research Award (2022 Spring)
- Henry H. Wang, now at Microsoft (2019 Fall 2021 Spring)

Columbia University

Students advising

- Fall 2012: Mengqi Zhang (MS student Columbia University, currently a software engineer at Facebook)
  Project: Compiler (LLVM) assisted program instrumentation and hardening
- 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 2013: Marios Pomonis, Theofilos Petsios (Ph.D. candidates at Columbia University)
  Project: Arithmetic error detection using information flow tracking with compiler-assisted program instrumentation.

NEC Labs America

Intern Advising

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

Talks

Invited Talks

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

Conference Presentations

Feb 2019	"Countering Malicious Processes with Process-DNS Association"	*NDSS, Sand Diego, USA*
Nov 2018	"NodeMerge: Template Based Efficient Data Reduction For Big-Data Causality Analysis"	*ACM CCS, Toronto, Canada*
Nov 2013	"ShadowReplica: Efficient Parallelization of Dynamic Data Flow Tracking"	*ACM CCS, Berlin, Germany*
Feb 2012	"A General Approach for Efficiently Accelerating Software-based Dynamic Data Flow Tracking on Commodity Hardware"	*NDSS, San Diego, USA*

Dec 2010 "An Adversarial Evaluation of Network Signaling and Control Mechanisms" *ICISC, Seoul, South Korea*

Honors & Awards

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

Service

NSF Panel

III-SMALL-IX-ENG Panelist The Information & Intelligent Systems Division (IIS), Mar 2020

Technical Program Committee Member

ISC 2023 International Conference on Information Security Conference
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