**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 byte-code 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**

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

**M.Phil. in Computer Science**

**COLUMBIA UNIVERSITY**

**M.Sc. in Computer Science**

**COLUMBIA UNIVERSITY**
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


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


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


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


JOURNALS

**DEMO PAPERS**


**Books**


---

**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.  

P2 Graphics processing unit accelerated trusted execution environment.  

P3 Real-time threat alert forensic analysis  

P4 User-added-value-based ransomware detection and prevention.  

P5 Automated threat alert triage via data provenance.  

P6 Inter-application dependency analysis for improving computer system threat detection  

P7 Template based data reduction for commercial data mining.  

P8 Host behavior and network analytics based automotive secure gateway.  

P9 Automated software safeness categorization with installation lineage and hybrid information sources  
Path-based program lineage inference analysis.  

Template based data reduction for security related information flow data.  


Fine-grained analysis and prevention of invalid privilege transitions.  

Extraction and comparison of hybrid program binary.  

---

**Teaching**

**CS4459: Cyber Attack and Defense Laboratory (CANDL)**  
**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 pwnning 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)**  
**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**  
**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**  
**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)
Columbia University
- 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.
  Project: End-point Detection and Response for IoT Devices.
  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”  
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

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**
Aug 2023  “A Hands-on Oriented Workforce Development Framework for Space Cyber-Infrastructure (CI)”  
ISSRDC, Seattle WA

Feb 2019  “Countering Malicious Processes with Process-DNS Association”  
NDSS, San Diego, CA

Nov 2018  “NodeMerge: Template Based Efficient Data Reduction For Big-Data Causality Analysis”  
ACM CCS, Toronto, Canada

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

Baltimore, USA

Aug 2016  CEATEC Award, Innovation for better society, CEATEC Japan CPS/IoT Exhibition  
Tokyo, Japan

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

Review Panelist  NSF SaTC, Jan 2024, Virtual

Technical Panelist  NSF SaTC EDU Workshop, Nov 2023, Dallas TX

Review Panelist  NSF IIIS, 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