Kangkook Jee

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

kangkook.jee@utdallas.edu | kangkookjee.io | jikk | kangkook-jee-2172bb6 | 0000-0003-3797-4637 | KangkooK Jee

Research Summary

Dr. Jee's research advances the **trustworthy understanding and verification of software artifacts**: recovering high-level representations from binaries and bytecode, verifying and repairing the result, and reasoning about software provenance. The flagship of this agenda, **PyLingual**, is at once a peer-reviewed research contribution and an influential software platform. Its core results appeared at the IEEE Symposium on Security and Privacy (S&P) 2025, with practitioner-facing presentations at Black Hat USA and PyCon US and a tutorial at PLDI 2025. Just as importantly, PyLingual has become community infrastructure: it is integrated into the **FLARE-VM** and **REMnux** reverse-engineering distributions, has processed roughly 510,000 Python bytecode samples through its public service since 2023, and is a go-to decompiler for malware analysts and reverse engineers. This dual standing, scholarly and operational, gives the work direct relevance to malware analysis, reverse engineering, and software assurance for national-defense systems. Complementary threads include system-provenance attack investigation, provenance-driven intrusion detection, and verified binary rewriting. A growing second thread extends this assurance lens to the safety and security of COTS components and small-satellite systems in low Earth orbit, relevant to resilient space-based defense capability, supported by NSF CyberTraining funding and the UT Dallas Small Satellite Workshop series.

Research Highlights

- PyLingual at IEEE Symposium on Security & Privacy (S&P), 2025; ACM PLDI Tutorial on PyLingual, 2025; Black Hat USA, 2024; PyCon US, 2024
- PyLingual integrated into **FLARE-VM** and **REMnux**
- Space security endeavor; NSF CyberTraining grant awarded; established and hosted the Small Satellite Workshop (2024, 2025, and 2026), satworkshop.syssec.org; launched a 6U CubeSat destined for LEO in collaboration with IBM Space
- 17 U.S. patents (granted, pending, and provisional)
- Multi-million-dollar funded research portfolio
- ACNS 2026 Program Committee Co-Chair

Education

Ph.D. in Computer Science — *New York, USA*
Columbia University — *May 2016*
Ph.D. Thesis: "On Efficiency and Accuracy of Data Flow Tracking Systems" advised by professor Angelos D. Keromytis

M.Phil. in Computer Science — *New York, USA*
Columbia University — *May 2012*

M.Sc. in Computer Science — *New York, USA*
Columbia University — *Feb 2008*

B.S. in Mathematics & Computer Science — *Seoul, South Korea*
Korea University — *Feb 2000*

Work Experience

University of Texas, at Dallas — *Richardson, TX*
Associate professor, Computer Science Department — *Sep 2026 –*
Assistant professor, Computer Science Department — *Aug 2019 – Aug 2026*

NEC Laboratories America — *Princeton, NJ*
Researcher, Computer Security Department — *Sep 2014 – Jul 2019*

IBM Korea — *Seoul, South Korea*
Advanced technical support staff — *Mar 2001 – Aug 2006*

18 Medical Company, 8th U.S. Army *Seoul, South Korea*

Information management staff *Jan 1997 – Mar 1999*

Publications

Conference Publications

C1 S. Klancher, J. Flores, J. Wiedemeier, M. Kantarcioglu, **K. Jee** *"The Consequences of Benchmark Scarcity in Provenance-Based Intrusion Detection"*. **Network and Distributed System Security Symposium (NDSS)**, Feb 2027

C2 J. Wiedemeier, S. Klancher, J. Flores, M. Zheng, J. Park, SK Cha, **K. Jee** *"Walking the Last Mile: Studying Decompiler Output Correction in Practice"*. **ACM Conference on Computer and Communications Security (CCS)** 2025

C3 B. Thuraisingham, **K. Jee**, L. Khan *"An Education Program for Data Driven Security with Machine Learning Applications"*. IEEE Conference on Big Data Security on Cloud (BigDataSecurity) 2025

C4 J. Wiedemeier, E. Tarbet, M. Zheng, S. Ko, J. Ouyang, S.K. Cha, **K. Jee** *"PYLINGUAL: Toward Perfect Decompilation of Evolving High-Level Languages"*. **IEEE Symposium on Security and Privacy (S&P)** 2025

C5 J. Wiedemeier, E. Tarbet, M. Zheng, J. Teng, X. Liu, M. Kim, J. Ouyang, S.K. Cha, **K. Jee** *"PYLINGUAL: A Python Decompilation Framework for Evolving Python Versions"*. BlackHat USA, Aug 2024

C6 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.

C7 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.

C8 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

C9 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.

C10 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.

C11 **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

C12 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.

C13 P. Fei, Z. Li, Z. Wang, X. Yu, D. Li, **K. Jee**, S. 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.

C14 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.

C15 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

C16 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

C17 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

C18 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

C19 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.

C20 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

C21 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

C22 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.

C23 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.

C24 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.

C25 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

C26 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.

C27 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.

C28 **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 2013.

C29 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.

C30 **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

C31 **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.

Manuscripts Under Review

U1 K. Mukherjee, J. Wiedemeier, T. Wang, F. Chen, M. Kim, M. Kantarcioglu, **K. Jee** *"Robust Explanation of GNN-based IDS for System Provenance with Graph Structural Features"*. Under review, **Network and Distributed System Security Symposium (NDSS)**, San Diego, CA, 2026.

U2 T. Wang, S. Klancher, K. Mukherjee, J. Wiedemeier, F. Chen, M. Kantarcioglu, **K. Jee** *"PROVCREATOR: Synthesizing Graphs with Text Attributes"*. Under review, Neural Information Processing Systems (NeurIPS), 2026 (preprint: arXiv:2507.20967).

Preprints & Technical Reports

R1 K. Mukherjee, J. Wiedemeier, T. Wang, M. Kim, F. Chen, M. Kantarcioglu, **K. Jee** *"Interpreting GNN-based IDS Detections Using Provenance Graph Structural Features"*. CoRR, abs/2306.00934, 2023.

Journals

J1 A. Akbar, Y. Wang, G. Ayoade, A. Singhal, L. Khan, B. Thuraisingham, **K. Jee** *"Advanced Persistent Threat Detection using Data Provenance and Metric Learning"* published by Transaction on Dependable and Secure Computing IEEE, October 2022

Tutorials

T1 J. Wiedemeier, SK Cha, and **K. Jee** *"Tutorial: Perfect Decompilation of Python Bytecode with PyLingual"* Presented at the **ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)**, Seoul South Korea, June 2025.

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

Proposal and Funding

Current

F1 **[KISTI]** Collaborative Research on AI-Driven Vulnerability Discovery and Automated Security Analysis
PI, 7/1/26 ~ 6/30/29, Current budget $350,000

F2 **[NSF]** CyberAI SFS: Training Next Generation AI-Proficient Cybersecurity Workforce at UT Dallas
Co-PI, 8/1/26 ~ 7/31/29, Current budget $1,999,998

F3 **[USDOT]** TRaCR: National Center for Transportation Cyber Security
Co-PI, 10/1/23 ~ 5/31/29, Current budget $1,036,000

F4 **[NIST]** UT Dallas Center for Secure and Trustworthy Artificial Intelligence (Award #24012811)
Co-PI, 8/1/24 ~ 7/31/26, Current budget $962,930

Pending (Under Review)

F1 **[NSA]** Secure LLMs and Agentic AI: A Unified Framework for Defense Against Adversarial Attacks
Co-PI, 7/1/26 ~ 6/30/29, Current budget $300,000

F2 **[NSA]** Toward a Generative AI-Driven Agentic Decompiler
Co-PI, 7/1/26 ~ 6/30/29, Current budget $300,000

F3 **[NSF]** SaTC:CORE:Small: A New Decompilation Paradigm for High-Level Languages
PI, 5/1/25 ~ 4/30/28, Current budget $596,297

Past Awarded

F1 **[USAFRL]** Building Robust AI Systems
Co-PI, 8/20/24 ~ 8/19/27, Current budget $398,248

F2 **[NSF]** CyberTraining: Pilot: CyberTraining for Space CI in Low Earth Orbit (LEO) (Award #2321117)
PI, 11/1/23 ~ 10/31/25, Current budget $299,999

F3 **[NSF]** EAGER: Privacy Preserving Synthetic Graph Generation for System Provenance (Award #2331424)
PI, 10/1/23 ~ 9/30/25, Current budget $250,003

F4 **[UT System]** VA Apprenticeship: Cybersecurity Testbed Environment for Workforce Development
PI, 2/1/22 ~ 1/31/23, Current budget $120,000

F5 **[NSF]** REU Site: Software Safety and Reliability: Research, Practice, and Innovation
Co-PI, 3/1/21 ~ 2/29/24, Current budget $404,772

F6 **[Cisco]** Gift for Research for Error Resilience AI
Co-PI, 9/30/22 ~, Current budget $85,500

F7 **[Amazon]** Gift for Research FAI
Co-PI, 1/1/20 ~, Current budget $37,923

Patents

Patents

P1 System and Method for Machine Learning Assisted Computer Object Code Decompilation, Repair, and Verification.
K. Jee, et al. U.S. Provisional Patent Application No. 63/999,450 (Attorney Docket No. 24023P1), filed Mar 2026. Covers (1) a verification-driven decompilation framework and (2) post-decompilation verification and repair. *First patent filing arising from research conducted at UT Dallas.*

P2 Confidential machine learning with program compartmentalization.
CH Kim, J Rhee, **K Jee**, LI Zhichun US Patent 11,423,142 issued on Aug 2022.

P3 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.

P4 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.

P5 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.

P6 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.

P7 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.

P8 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.

P9 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.

P10 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.

P11 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.

P12 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.

P13 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.

P14 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.

P15 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.

P16 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.

P17 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.

Software

PyLingual: A Decompilation Framework for Evolving High-Level Languages *2023 – present*

A research artifact and openly available platform for decompiling Python bytecode across evolving language versions. PyLingual pairs learning-based statement translation with mechanical control-flow reconstruction and a bytecode-level equivalence check, and is widely used in malware analysis and reverse engineering.

- Website: pylingual.io | Source: github.com/syssec-utd/pylingual
- Distributed with the **FLARE-VM** (Mandiant/Google, merged Mar 2026) and **REMnux** reverse-engineering platforms
- Community adoption by malware analysts and reverse engineers worldwide
- Public web service since Nov 2023: ∼510,000 PYC samples processed to date, with 500 to 1,000 samples uploaded daily

Teaching

CS4459: Cyber Attack and Defense Laboratory (CANDL) *Dallas, TX*

University of Texas at Dallas *Spring 2024 – present*

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.*

CS6332: System Security and Binary Code Analysis *Dallas, TX*

University of Texas at Dallas *Fall 2019* – present

The CS6332, a graduate-level system security 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)

Course Evaluations

Year	Term	Course	Title	Rating
2019	Fall	CS6332.001	System Security and Malware Code Analysis	4.56 / 5.00
2020	Spring	CS7301.001	Recent Advances in Computing: Advanced Topics, System Security	N/A
2020	Fall	CS6332.001	System Security and Malware Code Analysis	2.50 / 5.00
2021	Spring	CS4301.001	Special Topic: Cybersecurity Attacks and Defenses Laboratory	4.81 / 5.00
2021	Fall	CS6332.001	System Security and Malware Code Analysis	4.40 / 5.00
2022	Spring	CS4301.001	Special Topic: Cybersecurity Attacks and Defenses Laboratory	4.73 / 5.00
2022	Fall	CS6332.001	System Security and Binary Code Analysis	4.60 / 5.00
2023	Spring	CS4301.001	Special Topic: Cybersecurity Attacks and Defenses Laboratory	4.55 / 5.00
2023	Fall	CS6332.001	System Security and Binary Code Analysis	4.63 / 5.00
2024	Spring	CS4459.001	Cybersecurity Attacks and Defenses Laboratory	4.94 / 5.00
2024	Fall	CS6332.001	System Security and Binary Code Analysis	4.75 / 5.00
2025	Spring	CS4459.001	Cybersecurity Attacks and Defenses Laboratory	4.90 / 5.00
2025	Fall	CS6332.001	System Security and Binary Code Analysis	4.69 / 5.00
2026	Spring	CS4459.001	Cybersecurity Attacks and Defenses Laboratory	4.95 / 5.00

Ratings reflect the “Overall, the instructor was excellent” item (5.00 scale).

Student Advising

The University of Texas at Dallas

Ph.D. Alumni

- Kunal Mukherjee, 2019 Fall ∼ 2024 Fall
  Thesis: IoT Integration, Adversarial Attacks, and Threat Explanations in Provenance-based Intrusion Detection Systems
  Post-graduation appointment: Post doctorate research at Virginia Tech.
- Joshua D. Wiedemeier (McDermott Graduate Fellow), 2022 Fall ∼ 2026 Spring
  Thesis: PyLingual and the Benign Blindspot: Revisiting Dataset Construction in Malware Detection
  Post-graduation appointment: EOG Resources.

The University of Texas at Dallas

Ph.D. students

- Joel J. Flores (McDermott Graduate Fellow), 2024 Fall ∼
  Research Project: PyLingual and PYC Malware Analysis.
- Simon Klancher (McDermott Graduate Fellow), 2025 Fall ∼
  Research Project: Data-driven Security with System Provenance.
- Max Zheng (McDermott Graduate Fellow; NSF Graduate Fellowship Recipient), 2025 Fall ∼
  Research Project: Formal Verification of Static Binary Rewriter.

Master students

- Caleb Krause, 2026 Spring ∼
  EVM decompilation research.
- Jordan Flimpter, 2024 Summer ∼ 2024 Fall
  PyLingual UI design enhancement and stabilization.
- Albert Shouh-Cherng Jean,
  post-graduation appointment: Charles Schwab (2024 Spring)
  PyLingual code edit and patching interface design.
- Nick D. Baker,
  post-graduation appointment: Amazon Web Services (Spring 2023)
  GNN modeling pipeline design and implementation for system provenance dataset.
- Jonathan Yu, post-graduation appointment: American Airlines (Fall 2022 ∼ Spring 2023)
  DARPA TC dataset analysis and schema translation.
  JSUGRA: Jonsson School Undergraduate Research Award (Spring 2023)
- Jerry Teng, post-graduation appointment: Flatiron Health (Fall 2021 ∼ Spring 2023)
  Python dataset collection and establishment for NLP model training.
- James A. Wei, post-graduation appointment: Lawrence Livermore National Laboratory (Summer 2021 ∼ Fall 2022)
  System provenance research; Adversarial attack study on provenance-based intrusion detection system (PIDS).
- Anthony T. Maranto, post-graduation appointment: Dell (Summer 2021 ∼ Spring 2022)
  Python decompilation research; Established the core/initial foundation for PyLingual framework.
- Henry H. Wang, post-graduation appointment: Microsoft (Fall 2019 ∼ Spring 2021)
  IoT/SCADA firmware analysis research; Initial effort on launching Cyber-Attack And Defense Laboratory (CANDL) class.

Undergraduate students

- Serhan Doganay, (Summer 2026)
  Data collection agent design and implementation for system provenance.
- Tanner Raley, (Summer 2026)
  EVM decompilation research; space security research.
- Nicholas Gover, (Summer 2026)
  Data collection agent design and implementation for system provenance.
- Henry Harrison, (Summer 2026)
  PyLingual open source maintainer; Decompilation improvement research.
- Ronald Dang, (Summer 2024)
  RF communication research; 1st Small satellite workshop.
- Daniel Angel, (Fall 2023)
  RF communication research with UHF/VHF antennas.
- Elliot M. Tarbet, (Spring 2023 ∼ Spring 2024)
  PyLingual open source maintainer; Decompilation improvement research.
- Guangze Zu, post-graduation appointment: Meta (Spring 2022)
  PyLingual open source maintainer; Decompilation improvement research.
- 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.

Talks

Invited Talks

Jul 2025	"PyLingual: Toward Perfect Decompilation of Evolving High-Level Languages", Nanjing University	*Nanjing, China*
Jun 2025	"PyLingual: Toward Perfect Decompilation of Evolving High-Level Languages", SKKU	*Suwon, South Korea*
Jun 2025	"PyLingual: Toward Perfect Decompilation of Evolving High-Level Languages" NSR	*Daejon, South Korea*
Mar 2025	"Safety and Security of the Emerging Space Era", CNU	*Daejon, South Korea*
Jun 2025	"PyLingual: Toward Perfect Decompilation of Evolving High-Level Languages", KISTI	*Daejon, South Korea*
Jun 2025	"PyLingual: Toward Perfect Decompilation of Evolving High-Level Languages", ETRI	*Daejon, South Korea*
Mar 2025	"Hardware Safety and Security in Space Environments", ETRI	*Daejon, South Korea*
Dec 2024	"PyLingual: Toward Perfect Decompilation of Evolving High-Level Languages", KAIST	*Daejon, South Korea*
May 2024	"There and Back Again: Reverse Engineering Python Binaries", PyCon US 2024	*Pittsburgh, PA*
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	*Daejeon*
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	*New York, NY*
Oct 2013	"ShadowReplica: Efficient Parallelization of Dynamic Data Flow Tracking" Security Group Seminar, Stevens Institute of Technology	*Hoboken, NJ*
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	*New York, NY*
Mar 2011	"A General Approach for Efficiently Accelerating Software-based Dynamic Data Flow Tracking on Commodity Hardware", Liberty Group Seminar, Princeton University	*Princeton, NJ*

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", Internet Society NDSS	*Sand Diego, CA*
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", Internet Society NDSS	*San Diego, CA*
Dec 2010	"An Adversarial Evaluation of Network Signaling and Control Mechanisms", IEEE ICISC	*Seoul, South Korea*

Honors & Awards

2026	**Tenure awarded; promotion to Associate Professor (effective Aug 2026),** Computer Science Department, UT Dallas	*Richardson, TX*
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*
May 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*
2000	**Army Commendation Medal,** 8th U.S. Army	*Seoul, South Korea*

Service

Professional Service

Technical Program Committee Co-chair 26th Applied Cryptography and Network Security (ACNS) 2026
Program Committee Member ACM CCS 2024, 2025, 2026; USENIX Security 2024, 2025, 2026; ISC 2016, 2023, 2025; WISA 2021
Session Chair ACSAC 2020 (Cloud Security); ICDE 2019 (Ph.D. Symposium Chair)
Journal / Conference Reviews ACM TOPS (TOPS-2023-03-0040, "System Auditing for Real-Time Systems", Feb 2023); IEEE T-IFS (T-IFS-17867-2024.R1, "LTRDetector: Exploring Long-Term Relationship for Advanced Persistent Threats Detection")

NSF Panels

Review Panelist NSF IIS, Mar 2020; NSF SaTC:Core, Mar 2024; NSF SaTC2.0:Res, Jun 2025
Technical Panelist NSF SaTC EDU Workshop, Nov 2023, Dallas TX
Invited Participant NSF SaTC Vision 2.0 Workshop, Mar 2023, Dallas TX

University & Departmental Service

Student Club Mentoring Computer Security Group (CSG) advisor (2020 – present); K5UTD advisor (2024 – present)
CTF Competition Coaching NSA Codebreaker Challenge (8th nationwide, 2021; 4th nationwide, 2022); CSG CTF team (2025: 24th national, 165th worldwide; 2024: 26th national, 201st worldwide)
Outreach 2nd Small Satellite Workshop at UTD, Jul 2025 (NSF #23011291; 18 participants); 1st Small Satellite Workshop at UTD, Jun 2024 (NSF #23011291; 19 participants); Cybersecurity curriculum development for the Department of Veterans Affairs (UT System / IBM)
Departmental Committees Admission Committee (2019 – present); Publicity Committee (2019 – present); Graduate Curriculum Committee (2022 – present); Ad-hoc QE Committee (2022)

Ph.D. Dissertation Committees

- Mestan Firat Celiktug (UT Dallas) — Enhancing Privacy and Security in Distributed Data Analytics using Statistical Learning, Fall 2025
- Kunal Mukherjee (UT Dallas) — IoT Integration, Adversarial Attacks, and Threat Explanations in Provenance-based Intrusion Detection Systems, Nov 2024
- Hyungseok Kim (KAIST) — Towards Reliable Reassembly of Modern Binaries, Dec 2023
- Harsh Desai (UT Dallas) — Using Public and Private Blockchains for Secure Data Sharing and Analysis, May 2022
- Imrul Anindya (UT Dallas) — Understanding and Mitigating Privacy Risks Raised By Record Linkage, Nov 2020
- Qi Wang (UIUC) — Securing Emerging IoT Systems through Systematic Analysis and Design, Nov 2019

Master's Dissertation Committees

- Jungwoo Lee (KAIST) — Fuzzing Python Interpreter Using Type-Aware Bytecode Mutation, Dec 2024
- Myeong-Geun Shin (KAIST) — Prov-DFT: Mitigating Dependency Explosion with Information Flow Analysis, Dec 2021

Qualifying-Exam (QE) Committees

- Md Nazmus Sakib (UT Dallas) — A Survey of Security, Privacy, and Defense Mechanisms in Large Language Models, Aug 2025
- Ilan Buzzetti (UT Dallas) — Bit-Vector Proof Automation For Coq: Towards Automated, Bottom-up Software Verification, Jun 2025
- Joshua Wiedemeier (UT Dallas) — Survey of Provenance-based IDS, Jun 2024