Chung Hwan Kim
Assistant Professor of Computer Science
University of Texas at Dallas
800 W. Campbell Road
Richardson, TX 75080

Email: chungkim@utdallas.edu
URL: https://chungkim.io
Phone: 972-883-3551
Fax: 972-883-2399

I Education

Ph.D.	2017	Purdue University	West Lafayette, IN	Computer Science
		Advisors: Prof. Dongyan Xu and Prof. Xiangyu Zhang		
M.S.	2012	University of Utah	Salt Lake City, UT	Computer Science
B.S.	2008	Sunmoon University	South Korea	Computer & Information Sciences

II Employment History

Assistant Professor	Department of Computer Science Department of Electrical & Computer Engineering (by courtesy) University of Texas at Dallas, Richardson, TX	08/2020–present
Researcher	Computer Security Department NEC Labs, Princeton, NJ	08/2017–07/2020
Research Intern	Software Platform, CTO LG Electronics, South Korea	06/2015–07/2015
Research Intern	Autonomic Management Department NEC Labs, Princeton, NJ	05/2013–08/2013
Research Assistant	Department of Computer Science Purdue University, West Lafayette, IN	08/2012–08/2017
Research Assistant	Flux Research Group, School of Computing University of Utah, Salt Lake City, UT	01/2011–08/2012

III Honors and Awards

1. NSF CAREER Award, 2025.
2. UT Dallas New Faculty Research Symposium Grant Award, 2021.
3. Top 10 Finalist, CSAW Best Applied Research Paper Award, 2018.
4. Chungnam Provincial Government Global Scholarship ($80k for 2 years), 08/2010–08/2012.
5. Grand Prize, Capstone Design Fair 2007, Innovation Center for Engineering Education, Sunmoon University, 2007.

IV Scholarly and Creative Activities

A Refereed Publications and Submitted Articles

A.1 Summary Statistics

Years	**Full Paper Publications in Tier-1 Venues**									**Other Selective Venues**		
	USENIX Security	CCS	NDSS	ASPLOS	FSE	ASE	SIGMETRICS	WWW	TDSC	SOCC	EuroS&P	ACSAC
08/2020–present	2	1	2	1		1				2		
Before UT Dallas	2		2		1		1	1	1		1	3

- **26** peer-reviewed publications (all with $\leq$29% acceptance rate).
- **15** full paper publications in **tier-1 venues** and **6** in other **selective venues**.

A.2 Conference Proceedings

[c1] Minkyung Park, Zelun Kong, Dave (Jing) Tian, Z. Berkay Celik, and Chung Hwan Kim, DNN Latency Sequencing: Extracting DNN Architectures from Intel SGX Enclaves with Single-Stepping Attacks, in *Proceedings in the 33rd Network and Distributed System Security Symposium (NDSS 2026)* (San Diego, CA, 2026).

[c2] Sudharssan Mohan, Kyeongseok Yang, Zelun Kong, Yonghwi Kwon, Junghwan Rhee, Tyler Summers, Hongjun Choi, Heejo Lee, and Chung Hwan Kim, IMUFUZZER: Resilience-based Discovery of Signal Injection Attacks on Robotic Aerial Vehicles, in *Proceedings of the 40th IEEE/ACM International Conference on Automated Software Engineering (ASE 2025)* (Seoul, South Korea, 2025).

[c3] Zelun Kong, Minkyung Park, Le Guan, Ning Zhang, and Chung Hwan Kim, TZ-DATASHIELD: Automated Data Protection for Embedded Systems via Data-Flow-Based Compartmentalization, in *Proceedings of the 32nd Network and Distributed System Security Symposium (NDSS 2025)* (San Diego, CA, 2025).

[c4] Ali Ahad, Gang Wang, Chung Hwan Kim, Suman Jana, Zhiqiang Lin, and Yonghwi Kwon, FreePart: Hardening Data Processing Software via Framework-based Partitioning and Isolation, in *Proceedings of the 29th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2024)* (San Diego, CA, 2024).

[c5] Xiaolong Wu, Dave (Jing) Tian, and Chung Hwan Kim, Building GPU TEEs using CPU Secure Enclaves with GEVisor, in *Proceedings of the 14th ACM Symposium on Cloud Computing (SOCC 2023)* (Santa Cruz, CA, 2023).

[c6] Md Shihabul Islam, Mahmoud Zamani, Chung Hwan Kim, Latifur Khan, and Kevin Hamlen, Confidential Execution of Deep Learning Inference at the Untrusted Edge with ARM TrustZone, in *Proceedings of the 13th ACM Conference on Data and Application Security and Privacy (CODASPY 2023)* (Charlotte, NC, 2023).

[c7] Seulbae Kim, Major Liu, Junghwan "John" Rhee, Yuseok Jeon, Yonghwi Kwon, and Chung Hwan Kim, DriveFuzz: Discovering Autonomous Driving Bugs through Driving Quality-Guided Fuzzing, in *Proceedings of the 29th ACM Conference on Computer and Communications Security (CCS 2022)* (Los Angeles, CA, 2022).

[c8] Kyeongseok Yang*, Sudharssan Mohan*, Yonghwi Kwon, Heejo Lee, and Chung Hwan Kim, Poster: Automated Discovery of Sensor Spoofing Attacks on Robotic Vehicles, in *Proceedings of the 29th ACM Conference on Computer and Communications Security (CCS 2022)* (Los Angeles, CA, 2022) *Equal contribution.

[c9] Taegyu Kim, Vireshwar Kumar, Junghwan "John" Rhee, Jizhou Chen, Kyungtae Kim, Chung Hwan Kim, Dongyan Xu, and Dave (Jing) Tian, PASAN: Detecting Peripheral Access Concurrency Bugs within Bare-metal Embedded Applications, in *Proceedings of the 30th USENIX Security Symposium (USENIX Security 2021)* (Virtual Event, 2021).

[c10] Omid Setayeshfar, Junghwan "John" Rhee, Chung Hwan Kim, and Kyu Hyung Lee, Find My Sloths: Automated Comparative Analysis of How Real Enterprise Computers Keep Up with the Software Update Races, in *Proceedings of the 18th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2021)* (Virtual Event, 2021).

[c11] Kyungtae Kim, Chung Hwan Kim, Junghwan "John" Rhee, Xiao Yu, Haifeng Chen, Dave (Jing) Tian, and Byoungyoung Lee, Vessels: Efficient and Scalable Deep Learning

Prediction on Trusted Processors, in *Proceedings of the 11th ACM Symposium on Cloud Computing (SOCC 2020)* (Virtual Event, 2020).

[c12] Yixin Sun, Kangkook Jee, Suphannee Sivakorn, Zhichun Li, Cristian Lumezanu, Lauri Korts-Pärn, Zhenyu Wu, Junghwan Rhee, Chung Hwan Kim, Mung Chiang, and Prateek Mittal, Detecting Malware Injection with Program-DNS Behavior, in *Proceedings of the 5th IEEE European Symposium on Security and Privacy (EuroS&P 2020)* (Virtual Event, 2020).

[c13] Taegyu Kim, Chung Hwan Kim, Altay Ozen, Fan Fei, Zhan Tu, Xiangyu Zhang, Xinyan Deng, Dave (Jing) Tian, and Dongyan Xu, From Control Model to Program: Investigating Robotic Aerial Vehicle Accidents with MAYDAY, in *Proceedings of the 29th USENIX Security Symposium (USENIX Security 2020)* (Virtual Event, 2020).

[c14] Kyungtae Kim, Dae R. Jeong, Chung Hwan Kim, Yeongjin Jang, Insik Shin, and Byoungyoung Lee, HFL: Hybrid Fuzzing on the Linux Kernel, in *Proceedings of the 27th Network and Distributed System Security Symposium (NDSS 2020)* (San Diego, CA, 2020).

[c15] Jiaping Gui, Xusheng Xiao, Ding Li, Chung Hwan Kim, and Haifeng Chen, Progressive Processing of System Behavioral Query, in *Proceedings of the 35th Annual Computer Security Applications Conference (ACSAC 2019)* (San Juan, PR, 2019).

[c16] Taegyu Kim, Chung Hwan Kim, Junghwan Rhee, Fan Fei, Zhan Tu, Gregory Walkup, Xiangyu Zhang, Xinyan Deng, and Dongyan Xu, RVFuzzer: Finding Input Validation Bugs in Robotic Vehicles through Control-Guided Testing, in *Proceedings of the 28th USENIX Security Symposium (USENIX Security 2019)* (Santa Clara, CA, 2019).

[c17] Yuseok Jeon, Junghwan Rhee, Chung Hwan Kim, Zhichun Li, Mathias Payer, Byoungyoung Lee, and Zhenyu Wu, PoLPer: Process-Aware Restriction of Over-Privileged Setuid Calls in Legacy Applications, in *Proceedings of the 9th ACM Conference on Data and Application Security and Privacy (CODASPY 2019)* (Dallas, TX, 2019).

[c18] Peng Gao, Xusheng Xiao, Ding Li, Zhichun Li, Kangkook Jee, Zhenyu Wu, Chung Hwan Kim, Sanjeev R. Kulkarni, and Prateek Mittal, SAQL: A Stream-based Query System for Real-Time Abnormal System Behavior Detection, in *Proceedings of the 27th USENIX Security Symposium (USENIX Security 2018)* (Baltimore, MD, 2018).

[c19] Chung Hwan Kim, Taegyu Kim, Hongjun Choi, Zhongshu Gu, Xiangyu Zhang, and Dongyan Xu, Securing Real-Time Microcontroller Systems through Customized Memory View Switching, in *Proceedings of the 25th Network and Distributed System Security Symposium (NDSS 2018)* (San Diego, CA, 2018).

[c20] Taegyu Kim, Chung Hwan Kim, Hongjun Choi, Yonghwi Kwon, Xiangyu Zhang, and Dongyan Xu, RevARM: Cross-Platform ARM Binary Instrumentation for Security Applications, in *Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC 2017)* (Orlando, FL, 2017).

[c21] Kyungtae Kim, I Luk Kim, Chung Hwan Kim, Yonghwi Kwon, Yunhui Zheng, Xiangyu Zhang, and Dongyan Xu, J-Force: Forced Execution on JavaScript, in *Proceedings of the 26th International World Wide Web Conference (WWW 2017)* (Perth, WA, Australia, 2017).

[c22] Chung Hwan Kim, Junghwan Rhee, Kyu Hyung Lee, Xiangyu Zhang, and Dongyan Xu, PerfGuard: Binary-Centric Application Performance Monitoring in Production Environments, in *Proceedings of the 24th ACM SIGSOFT International Symposium on Foundations of Software Engineering (FSE 2016)* (Seattle, WA, 2016).

[c23] Shiqing Ma, Kyu Hyung Lee, Chung Hwan Kim, Junghwan Rhee, Xiangyu Zhang, and

Dongyan Xu, Accurate, Low Cost and Instrumentation-Free Security Audit Logging for Windows, in *Proceedings of the 31st Annual Computer Security Applications Conference (ACSAC 2015)* (Los Angeles, CA, 2015).

[c24] Chung Hwan Kim, Sungjin Park, Junghwan Rhee, Jong-Jin Won, Taisook Han, and Dongyan Xu, CAFE: A Virtualization-Based Approach to Protecting Sensitive Cloud Application Logic Confidentiality, in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2015)* (Singapore, 2015).

[c25] Chung Hwan Kim, Junghwan Rhee, Hui Zhang, Nipun Arora, Guofei Jiang, Xiangyu Zhang, and Dongyan Xu, IntroPerf: Transparent Context-sensitive Multi-layer Performance Inference Using System Stack Traces, in *Proceedings of the 2014 ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2014)* (Austin, TX, 2014).

A.3 Journal Articles

[j1] Sungjin Park, Chung Hwan Kim, Junghwan Rhee, Jong-Jin Won, Taisook Han, and Dongyan Xu, CAFE: A Virtualization-Based Approach to Protecting Sensitive Cloud Application Logic Confidentiality, IEEE Transactions on Dependable and Secure Computing (TDSC) **17**, 10.1109/tdsc.2018.2817545 (2020).

A.4 Thesis

[b1] Chung Hwan Kim, *Protecting Production Systems from Performance Anomalies*, Ph.D. thesis (2017).

A.5 Other Refereed Materials

[i1] Md Nazmus Sakib, Seungmok Kim, Zelun Kong, Seulbae Kim, Kyu Hyung Lee, Heejo Lee, and Chung Hwan Kim, Poster: Deterministic Replay and Debugging for Robotic Systems, in *39th Annual Computer Security Applications Conference (ACSAC 2023)* (Austin, TX, 2023).

[i2] Major Liu, Seulbae Kim, Seungmok Kim, Congzhou Li, and Chung Hwan Kim, AutoInsight: A Comprehensive Testing and Analysis Platform for Autonomous Driving Systems, in *Fed Supernova 2021* (Austin, TX, 2021).

[i3] Anton Burtsev, David Johnson, Chung Hwan Kim, Mike Hibler, Eric Eide, and John Regehr, *XenTT: Deterministic Systems Analysis in Xen*, Tech. Rep. (XenSummit North America 2012, San Diego, CA, 2012).

[i4] Chung Hwan Kim, *Iterative Backtracking via Deterministic Virtual Machine Replay and Virtual Machine Introspection*, Tech. Rep. (University of Utah, 2012) Master's Project Report.

B Other Publications and Creative Products

B.1 Patents

[p1] Chung Hwan Kim, Junghwan Rhee, Xiao Yu, LuAn Tang, Haifeng Chen, and Kyungtae Kim, Efficient and Scalable Enclave Protection for Machine Learning Programs (2023), US 20210081122 A1, Granted 02/2023.

[p2] Chung Hwan Kim, Junghwan Rhee, Kangkook Jee, and Zhichun Li, Confidential Machine Learning with Program Compartmentalization and SGX (2022), US 11423142 B2, Granted 08/2022.

[p3] Chung Hwan Kim, Junghwan Rhee, Kangkook Jee, Zhichun Li, and Adil Ahmad, Graphics Processing Unit Accelerated Trusted Execution Environment (2022), US 20200257794 A1, Granted 04/2022.

[p4] Junghwan Rhee, Ziqiao Zhou, Lu-An Tang, Zhengzhang Chen, Chung Hwan Kim, and Zhichun Li, Protocol-Independent Anomaly Detection (2022), US 20200059484 A1, Granted 04/2022.

[p5] Junghwan Rhee, Hongyu Li, Shuai Hao, Chung Hwan Kim, Zhenyu Wu, Zhichun Li, Kangkook Jee, and Lauri Korts-Pärn, Host Behavior and Network Analytics Based Automotive Secure Gateway (2021), US 10931635 B2, Granted 02/2021.

[p6] Junghwan Rhee, Hui Zhang, Nipun Arora, Guofei Jiang, and Chung Hwan Kim, Transparent Performance Inference of Whole Software Layers and Context-Sensitive Performance Debugging (2016), US 9367428 B2, Granted 06/2016.

[p7] Chung Hwan Kim, Jeong Bae Lee, and Yoon Young Park, Apparatus and Method For Software Security (A Secure, Platform-Independent Process Execution Model) (2011), KR 1020090056092, Granted 12/2011.

B.2 Software Artifacts

1. **dls**: an attack framework to extract DNN architectures from enclaves with single-stepping attacks [c1], 2025
   https://gitlab.com/s3lab-code/public/dls.
2. **imufuzzer**: a resilience-guided fuzzing framework for discovering signal injection attacks on robotic aerial vehicles [c2], 2025
   https://gitlab.com/s3lab-code/public/imufuzzer.
3. **tz-datashield**: a compartmentalization framework for protecting sensitive data in embedded systems with ARM TrustZone [c3], 2024
   https://gitlab.com/s3lab-code/public/tzds.
4. **s3overleaf**: my research group's private OverLeaf website (https://overleaf.s3lab.io), 2024
   https://gitlab.com/s3lab-code/public/s3overleaf.
5. **t-slices**: a confidential deep learning inference framework for edge devices [c6], 2024
   https://gitlab.com/s3lab-code/public/tslices.
6. **drivefuzz**: a feedback-driven fuzzing framework for autonomous driving systems [c7], 2022
   https://gitlab.com/s3lab-code/public/drivefuzz.
7. **s3web**: my research group's website (https://www.s3lab.io), 2020
   https://gitlab.com/s3lab-code/public/s3web.
8. **vmprobes**: a virtual machine introspection tool for Xen [i4] (now part of Stackdb), 2011
   https://gitlab.com/chungkim/vmprobes.
9. **dbtgpu**: GPU-accelerated dynamic binary translation for fixed-size instructions, 2011
   https://gitlab.com/chungkim/dbtgpu.
10. **gmsgr**: an instant messaging server and client for GNOME desktop environment, 2007
    https://gitlab.com/chungkim/gmsgr.
11. **peshield**: a secure process loader for Windows NT [p7], 2006
    https://gitlab.com/chungkim/peshield.

C Invited Talks

1. **Securing Robotic Systems: From Autonomous Vehicles to On-Device Machine Learning**
   RTST (07/2025).
2. **Hardening Embedded Systems through Compartmentalization and Isolation**
   Hanyang University ERICA (06/2025), POSTECH (06/2025), KAIST (06/2025), Seoul National University (06/2025), Hanwha Systems (07/2025).
3. **An End-to-End Infrastructure for Confidential Machine Learning**
   Yonsei University (06/2025).
4. **Fuzzing Autonomous Vehicles**
   Hyundai Motor Group (08/2023), Bayless (06/2023), Sungkyunkwan University (06/2023).
5. **Data-Generation Aspects of Fuzzing of Self-Driving Systems**
   2nd Annual Workshop on Future Automotive Research Datasets (11/2022).
6. **Cyber Meets Physical: Cross-Domain Fuzzing for Autonomous Vehicle Security**
   13th International Conference on Information and Communication Technology Convergence (10/2022).
7. **Cyber Meets Physical: Finding and Eliminating Vulnerabilities in Autonomous Vehicles**
   8th Zhejiang University CSE Graduate International Summer School (8/2022).
8. **Securing Autonomous Vehicles through Software Testing and Analysis**
   21st KOCSEA Technical Symposium (11/2021).
9. **Confidential Deep Learning on Trusted Processors**
   Korea University (05/2021).
10. **Securing Robotic Vehicles: A Cross-Layer Approach**
    Soongsil University (07/2021), Soonchunhyang University (07/2021), POSTECH (05/2021), Hanyang University ERICA (04/2021), UNIST (03/2021), Sunmoon University (03/2021), Korea University (02/2021).
11. **A Cross-Layer Approach to Robotic Vehicle Controller Security**
    UT Dallas (03/2020), University of Central Florida (02/2020), Virginia Tech (02/2020), CISPA (02/2020), Oregon State University (02/2020).
12. **Securing Real-Time Microcontroller Systems through Customized Memory View Switching**
    18th KOCSEA Technical Symposium (11/2018), 25th Network and Distributed System Security Symposium (02/2018).
13. **Protecting Production Systems from Software Anomalies**
    University of Delaware (03/2017), University of Texas at San Antonio (02/2017).

D Proposal and Grant Activities

D.1 Grants Awarded

$1.86M is awarded in total, out of which my share is **$1.19M**.

1. **NCAE-C: Course Material Contribution Stipend**
   Agency/Company: National Security Agency
   Program: National Centers of Academic Excellence in Cybersecurity Curriculum Task Force
   Total Amount: $5K
   Senior Personnel: Chung Hwan Kim (Sole PI)
   Project Period: 01/2026–03/2026

2. **CAREER: A Cross-Domain Approach to Improving the Attack Resilience of Robotic Systems**
   Agency/Company: National Science Foundation
   Program: Faculty Early Career Development Program
   Total Amount: $531K
   Senior Personnel: Chung Hwan Kim (Sole PI)
   Project Period: 08/2025–08/2030
3. **National Center for Transportation Cybersecurity and Resiliency (TraCR)**
   Agency/Company: Department of Transportation
   Total Amount: $688K (UT Dallas share) – Lead: Clemson University
   Senior Personnel: Bhavani Thuraisingham (PI), Latifur Khan (Co-PI), Chung Hwan Kim (Co-PI), Kevin Hamlen (Senior Personnel)
   Project Period: 01/2025–12/2025
   Share: $55K (8%)
4. **Research for Vulnerability Analysis Methods and Evaluation of a Secure Real-Time Operating System**
   Agency/Company: Hanwha Systems
   Total Amount: $180K
   Senior Personnel: Chung Hwan Kim (Sole PI)
   Project Period: 12/2024–11/2026
5. **UT Dallas Seed Program for Interdisciplinary Research**
   Agency/Company: University of Texas at Dallas Office of Research and Innovation
   Total Amount: $60K
   Senior Personnel: Chung Hwan Kim (PI), Tyler Summers (Co-PI)
   Project Period: 06/2024–05/2025
   Share: $40K (67%)
6. **Verification of Cyber-Physical Threat Detection and Response Model**
   Agency/Company: Korea Agency for Defense Development
   Total Amount: $260K (amended from $370 during project period)
   Senior Personnel: Chung Hwan Kim (Sole PI)
   Project Period: 07/2023–01/2026
7. **Telemetry Analytics to Secure Cloud Computing**
   Agency/Company: Sandia National Laboratories
   Total Amount: $44K
   Senior Personnel: Chung Hwan Kim (Sole PI)
   Project Period: 12/2022–09/2023
8. **Ministry of Science and ICT Research Grant (Gift)**
   Agency/Company: Korea Ministry of Science and ICT
   Total Amount: $5K
   Senior Personnel: Chung Hwan Kim (Sole PI)
   Award Date: 10/2021
9. **UT Dallas New Faculty Research Symposium Grant Award**
   Agency/Company: University of Texas at Dallas Office of Research
   Total Amount: $25K
   Senior Personnel: Chung Hwan Kim (PI), Kanad Basu (Co-PI)

Project Period: 06/2021–05/2022
Share: $20K (80%)

10. **From Device to Cloud: An End-to-End Framework for Trusted Edge Computing for IIoT Security**
    Agency/Company: Texas A&M Engineering Experiment Station
    Total Amount: $120K (including $60K cost share)
    Senior Personnel: Bhavani Thuraisingham (PI), Latifur Khan (Co-PI), Chung Hwan Kim (Senior Personnel)
    Project Period: 01/2021–12/2021
    Share: $49K (40%)

E Societal Impacts

E.1 Press Releases

1. **CAREER Awards Boost Studies in Robot Security, Drug Development**
   UT Dallas News Center (09/2025)
2. **Bug Hunting in Self-Driving Cars**
   Georgia Tech College of Computing News (11/2022).
3. **Increasing Smart Factory Cybersecurity using Trusted Execution Environments**
   Industrial Cybersecurity Pulse (06/2022), Texas A&M Engineering Experiment Station (05/2022).
4. **Spring 2021 Seed Grant Winners**
   UT Dallas Office of Research and Innovation (05/2021).
5. **Follow Your Curiosity**
   10th Anniversary Journal of Chungnam Association of Scholarship (07/2010).

E.2 Software Bug and Vulnerability Reports

1. **PX4 Drone Autopilot**
   PX4-Autopilot-5643 (10/2016), PX4-Autopilot-5644 (10/2016), PX4-Autopilot-5645 (10/2016), PX4-NuttX-84 (10/2016).

V Teaching

A Organized Courses and Seminars

Course Number	Course Title	Semesters (Enrollments)
CS/SE 4348	Operating Systems Concepts	Fall 2025 (77), Fall 2024 (80), Fall 2023 (75), Fall 2022 (72)
CS 6324	Information Security	Spring 2025 (75), Spring 2024 (67), Spring 2023 (66), Spring 2022 (63), Spring 2021 (60)
CS 6301	Special Topics in Computer Science–Security of CPS & IoT Systems	Fall 2021 (11), Fall 2020 (6)
Non-Credit	Software & Systems Security Seminar	Fall 2025 (7), Spring 2025 (7), Fall 2024 (6), Summer 2024 (6), Spring 2024 (12), Summer 2023 (10), Summer 2022 (8), Spring 2021 (16)

B Individual Student Guidance

B.1 Ph.D. Students

1. **Jaehyun Park**
   Summer 2025-present
   Status: Ph.D. post-qualifier
2. **Ruoyu Xu**
   Spring 2025-present
   Status: Ph.D. pre-qualifier
3. **Sai Tharun Reddy Mulka**
   Spring 2024-present
   Status: Ph.D. post-qualifier
4. **Mary Grace Dhooghe**
   Summer 2023-present
   Status: Ph.D. post-qualifier, co-advised with Bhavani Thuraisingham
5. **Sudharssan Mohan**
   Fall 2021–present
   Publications: [c2, c8]
   Status: Ph.D. post-qualifier
6. **Zelun Kong**
   Fall 2021–present
   Publications: [c1, c2, c3, i1]
   Status: Ph.D. post-qualifier
7. **Md Nazmus Sakib**
   Fall 2023-Summer 2024
   Publications: [i1]
   Status: Currently advised by Latifur Khan
8. **Md Shihabul Islam**
   Fall 2020–Spring 2024
   Publications: [c6]
   Status: Ph.D. 2024 in Computer Science, co-advised with Latifur Khan
   First Employment: **Data Security Technologies**

B.2 Masters Students

1. **Swathi Kote**
   Spring 2024
   Status: M.S. 2025 in Computer Science
   First Employment: **Nokia**
2. **Nate Simmons**
   Spring 2024
   Status: M.S. 2025 in Computer Science
3. **Shiven Pandya**
   Spring 2023
   Status: M.S. 2023 in Computer Science
   First Employment: **Dell Technologies**
4. **Major Liu**

Fall 2021–Spring 2023
Publications: [c7, i2]
Status: M.S. 2023 in Computer Science

5. **Ishpreet Bhasin**
Summer 2021–Fall 2022
Status: M.S. 2022 in Computer Science
First Employment: **Enable Medicine**
6. **Benjamin Stark**
Summer 2021–Spring 2022
Status: M.S. 2022 in Computer Science
First Employment: **Los Alamos National Laboratory**
7. **Alex Armstrong**
Fall 2021–Spring 2022
Status: M.S. 2022 in Computer Science
First Employment: **Lawrence Livermore National Laboratory**
8. **Cindy Chang**
Fall 2021
Status: M.S. 2021 in Computer Science
First Employment: **FedEx**
9. **Vasuki Shankar**
Spring 2021–Fall 2021
Status: M.S. 2021 in Computer Engineering
First Employment: **Nvidia**
10. **Deeprangshu Pal**
Spring 2021
Status: M.S. 2022 in Computer Science
First Employment: **Samsung Electronics America**

B.3 Undergraduate Students

1. **Pablo Collantes**
Spring 2025–present
Status: expected B.E. 2027 in Computer Science
Remark: UT Dallas 2025 REU Summer Program scholarship winner
2. **Conner Replogle**
Fall 2024–Spring 2025
Status: expected B.E. 2027 in Computer Science
3. **Benjamin Carroll**
Summer 2023–Spring 2024
Status: expected B.S. 2027 in Computer Science
4. **Veer Shah**
Summer 2023–Spring 2024
Status: expected B.S. 2027 in Computer Science
5. **Vishvak Bandi**
Fall 2020–Fall 2021
Status: B.S. 2023 in Computer Science

First Employment: **JPMorgan Chase & Co.**

B.4 Postdoctoral Associates and Visiting Scholars

1. **Minkyung Park**
   Fall 2023–present
   Publications: [c1, c3]
   Status: Postdoctoral associate
2. **Ahrim Cho**
   Fall 2021–Spring 2022
   Status: Visiting scholar from Korea Ministry of Science and ICT

B.5 Thesis or Dissertation Committee

1. Xian Wang, Ph.D. Dissertation, "Empirical Analysis to Enhance Security of Information Platforms," 09/2025
2. Saquib Irtiza, Ph.D. Dissertation, "Low Resource AI Security: Novel Frameworks for Network Protection Vulnerability Detection and Language Model," 07/2025
3. Md Shihabul Islam, Ph.D. Dissertation, "Confidential Computing with Trusted Execution Environments," 04/2024
4. Zachary J. Patterson, Ph.D. Dissertation, "Toward Applying Variability-Oblivious Static Analyses to Software Product Lines," 07/2023
5. Xujiang Zhao, Ph.D. Dissertation, "Multidimensional Uncertainty Quantification for Deep Neural Networks," 06/2022

B.6 Ph.D. Qualifying Exam Committee

1. Md Nazmus Sakib, QE Format: Systematic Review, 08/2025
2. Jaehyun Park, QE Format: Systematic Review, 07/2025
3. Sai Tharun Reddy Mulka, QE Format: Systematic Review, 05/2025
4. Meah Tahmeed Ahmed, QE Format: Systematic Review, 05/2025
5. Sudharssan Mohan, QE Format: Research Questions, 12/2024

B.7 Students Outside UT Dallas

1. **Xiaolong Wu**
   Fall 2021–Fall 2023
   Publications: [c5]
   Status: Ph.D. student at Purdue, advised by Dave (Jing) Tian
2. **Kyeongseok Yang**
   Spring 2021–Fall 2023
   Publications: [c2, c8]
   Status: Ph.D. student at Korea Univ., advised by Heejo Lee
3. **Choongin Lee**
   Spring 2021–Fall 2023
   Status: Ph.D. student at Korea Univ., advised by Heejo Lee
4. **Yeonseok Jang**
   Spring 2021–Spring 2023
   Status: M.S. 2023 in Computer Science from Korea Univ., co-advised with Heejo Lee
   First Employment: **Hyundai Motors (Cyber Security Lab)**
5. **Seungmok Kim**
   Spring 2021–Summer 2022

Publications: [i1, i2]
Status: M.S. 2022 in Computer Science from Korea Univ., co-advised with Heejo Lee
First Employment: **LIG Nex1 (Unmanned Systems Lab)**

B.8 Students Mentored Before UT Dallas

1. **Seulbae Kim**
   Publications: [c7]
   Status: Ph.D. 2023 in Computer Science from Georgia Tech
   First Employment: **Assistant Professor at POSTECH**
   Remark: Research intern at NEC Labs in Summer 2020
2. **Cody Holliday**
   Status: M.S. 2021 in Computer Science from Oregon State
   First Employment: **Jedox GmbH**
   Remark: Research intern at NEC Labs in Spring 2020
3. **Kyungtae Kim**
   Publications: [c11, p1]
   Status: Ph.D. 2022 in Computer Science from Purdue
   First Employment: **Assistant Professor at Dartmouth**
   Remark: Research intern at NEC Labs in Summer 2019
4. **Adil Ahmad**
   Publications: [p3]
   Status: Ph.D. 2022 in Computer Science from Purdue
   First Employment: **Assistant Professor at Arizona State**
   Remark: Research intern at NEC Labs in Summer 2018
5. **Taegyu Kim**
   Fall 2017–Fall 2019
   Publications: [c9, c13, c16, c20]
   Status: Ph.D. 2021 in Electrical & Computer Engineering from Purdue
   First Employment: **Assistant Professor at Penn State (IST)**

VI Service

A Professional Contributions

A.1 Organizing Committee

1. Posters and WIPs Co-Chair, *Annual Computer Security Applications Conference (ACSAC)*, 2023.
2. Publication Chair, *IEEE Secure Development Conference (SecDev)*, 2021.

A.2 Program Committee

1. *ACM Conference on Computer and Communications Security (CCS)*, 2026.
2. *USENIX Security Symposium (USENIX Security)*, 2025–2026.
3. *Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2020, 2025–2026.
4. *International Workshop on Software Engineering for Autonomous Driving Systems (SE4ADS)*, 2025.
5. *European Symposium on Research in Computer Security (ESORICS)*, 2024.
6. *ISOC Symposium on Vehicle Security and Privacy (VehicleSec)*, 2023–2025.

7. *IEEE Workshop on the Internet of Safe Things (SafeThings)*, 2022, 2024.
8. *International Conference on Distributed Computing Systems (ICDCS)*, 2021–2023.
9. *International Workshop on Automotive and Autonomous Vehicle Security (AutoSec)*, 2022.
10. *World Conference on Information Security Applications (WISA)*, 2021.
11. *Network and Distributed System Security Symposium (NDSS)*, 2019.

A.3 Artifact Evaluation Committee

1. *ACM Symposium on Operating Systems Principles (SOSP)*, 2019.

A.4 Journal Referee

1. *ACM Transactions on Cyber-Physical Systems (TCPS)*, 2023.
2. *IEEE Transactions on Mobile Computing (TMC)*, 2020.
3. *IEEE Transactions on Networking (TNET)*, 2018.
4. *IEEE Transactions on Information Forensics and Security (TIFS)*, 2015.
5. *IEEE Transactions on Services Computing (TSC)*, 2015.

A.5 External Reviewer

1. *IEEE Symposium on Security and Privacy (S&P)*, 2015, 2021.
2. *Network and Distributed System Security Symposium (NDSS)*, 2015, 2017–2018.
3. *USENIX Security Symposium (USENIX Security)*, 2018.
4. *ACM Conference on Computer and Communications Security (CCS)*, 2016.
5. *Workshop on Internet of Things Security and Privacy (IoT S&P)*, 2017.
6. *Annual Computer Security Applications Conference (ACSAC)*, 2014, 2016.
7. *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2016.
8. *ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, 2016.
9. *International Symposium on Research in Attacks, Intrusions, and Defenses (RAID)*, 2016.
10. *IEEE Conference on Communications and Network Security (CNS)*, 2016.
11. *ACM International Symposium on the Foundations of Software Engineering (FSE)*, 2016.
12. *International Symposium on Software Testing and Analysis (ISSTA)*, 2016–2017.
13. *ACM Cloud Computing Security Workshop (CCSW)*, 2014.

A.6 Memberships in Professional Societies

1. Member, *Association for Computing Machinery (ACM)*.
2. Member, *The Advanced Computing Systems Association (USENIX)*.
3. Member, *Institute of Electrical and Electronics Engineers (IEEE)*.
4. Member, *Korean Computer Scientists and Engineers Association in America (KOCSEA)*.
5. Member, *Korean-American Scientists and Engineers Association (KSEA)*.

B Public and Community Service

1. Faculty Mentor, *Clark Summer Research Program* for incoming freshmen students, 2023.
2. Faculty Member, *UT Dallas CS K-12 Outreach Summer Camp* for K-12 students, 2022.
3. Program Host, *CAST STEM Bridge Summer Camp* for K-12 students, 2022.

C Institute Contributions

1. *BS in Cybersecurity, Technology, and Policy (BS CTP) Curriculum Committee*, Department of Computer Science, Spring 2025–present.
2. Observer/Observee, *Collegial Teaching Observation by Peers (CTOP)*, Department of Computer Science, Spring 2025.
3. Faculty Member, *Center for Smart Mobility (COSMO)*, Spring 2022–present.

4. *CS 4485 (Senior Design) Faculty Mentor*, Department of Computer Science, Spring 2022-Spring 2023, Fall 2024-Spring 2025.
5. *Graduate Student Admissions Committee*, Department of Computer Science, Fall 2020–present.
6. Faculty Member, *Cyber Security Research and Education Institute (CSI)*, Fall 2020–present.