

# Hyungsub Kim

✉ [hk145@iu.edu](mailto:hk145@iu.edu)  
📄 [kimhyungsub.github.io](https://kimhyungsub.github.io)

Assistant Professor  
Department of Computer Science  
Indiana University, Bloomington, IN, USA

## Research Interests

I am a system security researcher. I develop *program analysis* and *formal method* techniques to tackle security threats in systems. My research is best represented by my extensive work on robotic vehicles (RVs). I was working on automatically finding logic bugs, patching them, and verifying the patches in RV control software. In addition, I was uncovering the root causes and formulating countermeasures against physical sensor attacks that target RVs. Currently, my efforts are dedicated to developing *formal methods* to address cyber and physical attacks against various cyber-physical systems, including vehicles, satellites, implantable medical devices, and industrial control systems.

## Education

- 2018–2023 **PhD in Computer Science, *Purdue University***, IN, USA.
  - Thesis: "Defeating Cyber and Physical Attacks in Robotic Vehicles" [\[PDF\]](#)
  - Advisors: Professor Dongyan Xu, Antonio Bianchi, Z. Berkay Celik
- 2013–2015 **M.S. in Computer Science and Engineering, *POSTECH***, Pohang, South Korea.
  - Thesis: "Privacy Threats in HTML5 Geolocation API: Case Studies and Countermeasures" [\[PDF\]](#)
  - Advisor: Professor Jong Kim
- 2011–2013 **B.S. in School of Computer Science, *University of Seoul***, Seoul, South Korea.

## Employment History

- Aug. 2024 – present **Assistant Professor, Indiana University**, Bloomington, Indiana, USA.
- Jan. 2024 – Jul. 2024 **Postdoctoral Researcher, Purdue University**, West Lafayette, Indiana, USA.
- 2015–2018 **Researcher, 3rd R&D Institute (Intelligence, Surveillance and Reconnaissance), Agency for Defense Development (ADD)**, DaeJeon, South Korea.
- 2007–2009 **Auxiliary Policeman, Gwangju Seobu Police Station, Gwangju Metropolitan Police Agency**, Gwangju, South Korea.  
Mandatory military service

## Publications

★ **First-author publications in top security conferences [4]:** (1) S&P'24, (2) USENIX Security'23, (3) S&P'22, (4) NDSS'21

### Conference Papers

- [1] **RVSPEC: Cyber-Physical Interplay Graphs for Formal Specification of Robotic Vehicle Control Software**  
Chaoqi Zhang, Minhyun Cho, Inseok Hwang, **Hyungsub Kim**  
In the Proceedings of the IEEE International Conference on Robotics and Automation (**ICRA 2026**), Vienna, Austria, June 1-5, 2026.  
(acceptance rate: 1882/4947=38.04%)

- [2] **Automated Discovery of Semantic Attacks in Multi-Robot Navigation Systems** [PDF]  
Doguhan Yeke, Kartik Anand Pant, Muslum Ozgur Ozmen, Hyungsub Kim, James Goppert, Inseok Hwang, Antonio Bianchi, Z. Berkay Celik  
In the Proceedings of the 34th USENIX Security Symposium (**USENIX Security 2025**), Seattle, Washington, USA, August 13-15, 2025.  
(acceptance rate:  $407/2385=17.06\%$ )
- [3] **Intent-aware Fuzzing for Android Hardened Application** [PDF]  
Seongyun Jeong, Minseong Choi, Haehyun Cho, Seokwoo Choi, Hyungsub Kim, Yuseok Jeon  
In the Proceedings of the 32nd ACM Conference on Computer and Communications Security (**CCS 2025**), Taipei, Taiwan, October 13-17, 2025.  
(acceptance rate:  $316/2278=13.9\%$ )
- [4] ★ **A Systematic Study of Physical Sensor Attack Hardness** [PDF]  
Hyungsub Kim, Rwitam Bandyopadhyay, Muslum Ozgur Ozmen, Z. Berkay Celik, Antonio Bianchi, Yongdae Kim, Dongyan Xu  
In the Proceedings of the 45th IEEE Symposium on Security and Privacy (**S&P 2024**), San Francisco, California, USA, May 20-23, 2024.  
(acceptance rate:  $261/1463=17.8\%$ )
- [5] **Discovering Adversarial Driving Maneuvers against Autonomous Vehicles** [PDF] [Slide]  
Ruoyu Song, Muslum Ozgur Ozmen, Hyungsub Kim, Raymond Muller, Z. Berkay Celik, Antonio Bianchi  
In the Proceedings of the 32nd USENIX Security Symposium (**USENIX Security 2023**), Anaheim, California, USA, August 9-11, 2023.  
(acceptance rate:  $442/1444=29.2\%$ )
- [6] ★ **PatchVerif: Discovering Faulty Patches in Robotic Vehicles** [PDF] [Slide]  
Hyungsub Kim, Muslum Ozgur Ozmen, Z. Berkay Celik, Antonio Bianchi, Dongyan Xu  
In the Proceedings of the 32nd USENIX Security Symposium (**USENIX Security 2023**), Anaheim, California, USA, August 9-11, 2023.  
(acceptance rate:  $442/1444=29.2\%$ )
- [7] ★ **PGPATCH: Policy-Guided Logic Bug Patching for Robotic Vehicles** [PDF] [Slide]  
Hyungsub Kim, Muslum Ozgur Ozmen, Z. Berkay Celik, Antonio Bianchi, Dongyan Xu  
In the Proceedings of the 43rd IEEE Symposium on Security and Privacy (**S&P 2022**), San Francisco, California, USA, May 23-26, 2022.  
(acceptance rate:  $147/1012=14.5\%$ )
- [8] **M2MON: Building an MMIO-based Security Reference Monitor for Unmanned Vehicles** [PDF] [Slide]  
Arslan Khan, Hyungsub Kim, Byoungyoung Lee, Dongyan Xu, Antonio Bianchi, Dave (Jing) Tian  
In the Proceedings of the 30th USENIX Security Symposium (**USENIX Security 2021**), Vancouver, British Columbia, Canada, August 11-13, 2021.  
(acceptance rate:  $246/1316=18.7\%$ )
- [9] ★ **PGFUZZ: Policy-Guided Fuzzing for Robotic Vehicles** [PDF] [Slide]  
Hyungsub Kim, Muslum Ozgur Ozmen, Antonio Bianchi, Z. Berkay Celik, Dongyan Xu  
In the Proceedings of the 28th Network and Distributed System Security Symposium (**NDSS 2021**), San Diego, California, USA, February 21-24, 2021.  
(acceptance rate:  $87/573=15.2\%$ )
- [10] **Inferring Browser Activity and Status Through Remote Monitoring of Storage Usage** [PDF] [Slide]  
Hyungsub Kim, Sangho Lee, and Jong Kim  
In the Proceedings of the 32nd Annual Computer Security Applications Conference (**ACSAC 2016**), Los Angeles, California, USA, December 5-9, 2016.  
(acceptance rate:  $48/210=22.8\%$ )
- [11] **Identifying Cross-origin Resource Status Using Application Cache** [PDF] [Slide]  
Sangho Lee, Hyungsub Kim, and Jong Kim  
In the Proceedings of the 22nd Network and Distributed System Security Symposium (**NDSS 2015**), San Diego, California, USA, February 8-11, 2015.  
(acceptance rate:  $50/302=16.6\%$ )

- [12] **Exploring and mitigating privacy threats of HTML5 geolocation API** [\[PDF\]](#) [\[Slide\]](#)  
**Hyungsub Kim**, Sangho Lee, and Jong Kim  
In the Proceedings of the 30th Annual Computer Security Applications Conference (**ACSAC 2014**), New Orleans, Louisiana, USA, December 8-12, 2014.  
(acceptance rate: 47/236=19.9%)

### Short Paper

- [1] **Short: Rethinking Secure Pairing in Drone Swarms** [\[PDF\]](#)  
Muslum Ozgur Ozmen, Habiba Farrukh, **Hyungsub Kim**, Antonio Bianchi, Z. Berkay Celik  
In the Proceedings of the Inaugural ISOC Symposium on Vehicle Security and Privacy (**VehicleSec 2023**), San Diego, California, USA, February 27, 2023.

### Workshop/Demo/Poster Papers

- [1] **Poster: A Multi-Agent Framework for Formal Specification of Robotic Vehicle Control Software** [\[PDF\]](#)  
Chaoqi Zhang, **Hyungsub Kim**  
The 3rd USENIX Symposium on Vehicle Security and Privacy (**VehicleSec 2025**), Seattle, Washington, USA, August 11, 2025.
- [2] **Demo: Discovering Faulty Patches in Robotic Vehicle Control Software** [\[PDF\]](#)  
**Hyungsub Kim**, Muslum Ozgur Ozmen, Z. Berkay Celik, Antonio Bianchi, Dongyan Xu  
In the Proceedings of the Inaugural ISOC Symposium on Vehicle Security and Privacy (**VehicleSec 2023**), San Diego, California, USA, February 27, 2023.
- [3] **Demo: Policy-based Discovery and Patching of Logic Bugs in Robotic Vehicles** [\[PDF\]](#)  
**Hyungsub Kim**, Muslum Ozgur Ozmen, Antonio Bianchi, Z. Berkay Celik, Dongyan Xu  
In the Proceedings of the 4th International Workshop on Automotive and Autonomous Vehicle Security (**AutoSec 2022**), San Diego, California, USA, April 24, 2022.

### Dissertation/Thesis

- [1] **Defeating Cyber and Physical Attacks in Robotic Vehicles** [\[PDF\]](#)  
PhD dissertation, Department of Computer Science, Purdue University, 2023.
- [2] **Privacy Threats in HTML5 Geolocation API: Case Studies and Countermeasures** [\[PDF\]](#)  
Master's Thesis, Department of Computer Science and Engineering, POSTECH, 2015.

### Interdisciplinary Work

- [1] **Community-based death preparation and education: A scoping review** [\[PDF\]](#)  
Sungwon Park, Hyungkyung Kim, Min Kyeong Jang, Hyungsub Kim, Rebecca Raszewski & Ardith Z. Doorenbos  
Death Studies, March 11, 2022.

---

### Grants

- Jan. 2026 – Children's Heart Foundation - Fontan Pump: Wireless Charge and Control System Development  
Dec. 2027 \$200,000, percentage under my control: 25%
- Sep. 2024 – DARPA - Faithful Integration and Reverse-engineering and Emulation (FIRE),  
Jan. 2026 Subcontract from Purdue University,  
Indiana University share: \$130,000, percentage under my control: 100%

---

### Talks

- [1] **Defeating Cyber and Physical Attacks in Robotic Vehicles**, *The Center for Connected and Automated Transportation (CCAT) cybersecurity working group meeting, February 9, 2026*, [\[Link\]](#).

- [2] **A Systematic Study of Physical Sensor Attack Hardness**, *KOCSEA Technical Symposium 2025, Las Vegas, Nevada, USA, November 8, 2025*, [\[Link\]](#).
- [3] **Generic Large Language Model (GLLM) in Cybersecurity**, *as a Panelist at CAE Cybersecurity Community Symposium, Charleston, South Carolina, USA, April 8, 2025*, [\[Link\]](#).
- [4] **Simulating Cyber-Physical Vulnerabilities**, *DARPA - Faithful Integration and Reverse-engineering and Emulation (FIRE) Quarterly Review, Philadelphia, Pennsylvania, USA, March 19, 2025*.
- [5] **Modeling and Simulating Cyber-Physical Vulnerabilities**, *DARPA - Faithful Integration and Reverse-engineering and Emulation (FIRE) Workshop 3, Philadelphia, Pennsylvania, USA, March 17-18, 2025*.
- [6] **Modeling and Simulating Cyber-Physical Vulnerabilities**, *DARPA - Faithful Integration and Reverse-engineering and Emulation (FIRE) Workshop 2, Orlando, Florida, USA, January 22-23, 2025*.
- [7] **Software Supply Chain Security**, *as a Panelist at CAE Special Topics Workshop on Software Supply Chain Security, St. Louis, Missouri, USA, October 9, 2024*.
- [8] **Sensor Modeling and Physical Sensor Attack Simulations**, *DARPA - Faithful Integration and Reverse-engineering and Emulation (FIRE) Quarterly Review, Melbourne, Florida, USA, September 17, 2024*.
- [9] **Defeating Cyber and Physical Attacks in Robotic Vehicles**,  
*Sejong University, Seoul, Korea, August 29, 2024*  
*National Security Research Institute, Daejeon, Korea, July 5, 2024*  
*KAIST, Daejeon, Korea, July 4, 2024*  
*POSTECH, Pohang, Korea, July 3, 2024*  
*Korea University, Seoul, Korea, July 2, 2024*  
*Agency for Defense Development, Daejeon, Korea, June 24, 2024*  
*UNIST, Ulsan, Korea, April 1, 2024*  
*Indiana University Bloomington, Indiana, USA, March 26, 2024*  
*Arizona State University, Tempe, Arizona, USA, March 1, 2024*  
*Georgia State University, Atlanta, Georgia, USA, February 8, 2024*  
*University of Maryland, College Park, Maryland, USA, January 30, 2024*  
*CISPA Helmholtz Center for Information Security, Saarbrücken, Germany, January 23, 2024*  
*New Jersey Institute of Technology, Newark, NJ, USA, January 19, 2024*  
*University of California, Santa Barbara, California, USA, January 16, 2024*  
*University of Florida, Gainesville, FL, USA, January 10, 2024*  
*Washington University in St. Louis, Missouri, USA, December 15, 2023*  
*University of Illinois at Urbana-Champaign, Illinois, USA, December 1, 2023*  
*Purdue University, Indiana, USA, November 28, 2023 (PhD dissertation defense)*  
*Indiana University Bloomington, Indiana, USA, November 17, 2023*  
*Georgia Institute of Technology, Atlanta, Georgia, USA, October 18, 2023*.
- [10] **Cyber-physical Vulnerability Analysis**, *DARPA - Faithful Integration and Reverse-engineering and Emulation (FIRE) Quarterly Review, Tempe, Arizona, USA, May 29, 2024*.
- [11] **A Systematic Study of Physical Sensor Attack Hardness**, *45th IEEE Symposium on Security and Privacy (S&P 2024), San Francisco, California, USA, May 21, 2024*.
- [12] **PatchVerif: Discovering Faulty Patches in Robotic Vehicles**, *32nd USENIX Security Symposium, Anaheim, California, USA, August 10, 2023*.
- [13] **Defeating Logic Bugs in Robotic Vehicles**,  
*POSTECH, Pohang, Korea, June 1, 2023*  
*UNIST, Ulsan, Korea, May 31, 2023*  
*Ohio State University, Columbus, Ohio, USA, February 17, 2023*  
*Purdue University, West Lafayette, Indiana, USA, November 18, 2022 (preliminary examination)*  
*New York University Abu Dhabi, UAE, November 10, 2022*.
- [14] **Logic Bug-Finding and Patching Tools**, *2nd Technology Innovation Institute (TII) Annual SSRC Research Partners Summit, Abu Dhabi, UAE, November 8, 2022*.
- [15] **PGPATCH: Policy-Guided Logic Bug Patching for Robotic Vehicles**, *43rd IEEE Symposium on Security and Privacy (S&P), San Francisco, California, USA, May 25, 2022*.

- [16] **PGFUZZ: Policy-Guided Fuzzing for Robotic Vehicles**, *28th Network and Distributed System Security Symposium (NDSS)*, San Diego, California, USA, February 24, 2021.
- [17] **Inferring Browser Activity and Status Through Remote Monitoring of Storage Usage**, *32nd Annual Computer Security Applications Conference (ACSAC)*, Los Angeles, California, USA, December 8, 2016.
- [18] **Exploring and Mitigating Privacy Threats of HTML5 Geolocation API**, *30th Annual Computer Security Applications Conference (ACSAC)*, New Orleans, Louisiana, USA, December 11, 2014.
- [19] **I Know the Shortened URLs You Clicked on Twitter: Inference Attack using Public Click Analytics and Twitter Metadata**, *Workshop among Asian Information Security Labs (WAIS)*, Shanghai, China, Jan 10, 2014.

---

## Fellowships, Awards, and Honors

**Best Poster Award**, Midwest Security Workshop (MSW) 2025. [\[Link\]](#)

☆ **Distinguished Reviewer Award**, ISOC Network and Distributed System Security Symposium (NDSS) 2025.

☆ **Outstanding Reviewer Award**, ISOC Symposium on Vehicle Security and Privacy (VehicleSec) 2024.

☆ **Noteworthy Reviewer**, International Symposium on Research in Attacks, Intrusions and Defenses (RAID) 2023. [\[Link\]](#)

☆ **CPS Rising Stars**, CPS-VO@National Science Foundation (NSF) 2023. [\[Link\]](#)

☆ **Outstanding Reviewer Award**, ISOC Symposium on Vehicle Security and Privacy (VehicleSec) 2023.

**IEEE S&P Student Travel Grant** (US\$1,300), San Francisco, California, USA, May, 2022.

**CCS Student Conference Grant**, Virtual Conference, November, 2021.

☆ **Ross Fellowship**, Purdue University Graduate School, 2018.

**ACSAC Student Conferenceship Award** (US\$1,200), New Orleans, Louisiana, USA, December, 2014.

**Best Student Presentation Award**, POSTECH CSE Student Workshop, 2014.

**Semester High Honors**, 2011 and 2012 2nd semester, University of Seoul.

**Semester High Honors**, 2007 2nd semester, Chonnam National University.

**Ministry of Commerce, Industry and Energy grand prize** (US\$2,600), high school competitions in the field of computer science, 2004.

---

## Professional Services

### Research Grant Panelist

2026 National Science Foundation (NSF) Review Panel

### Organizing Committee

2027 ISOC Network and Distributed System Security Symposium (NDSS), Publication Chair [\[Link\]](#)

2026 ISOC Network and Distributed System Security Symposium (NDSS), Publication Chair [\[Link\]](#)

2026 USENIX Vehicle Security and Privacy (VehicleSec), **General Chair** [\[Link\]](#)

2025 ISOC Network and Distributed System Security Symposium (NDSS), Publication Chair [\[Link\]](#)

2025 USENIX Vehicle Security and Privacy (VehicleSec), Publicity Chair [\[Link\]](#)

2025 Midwest Security Workshop (MSW), **Organizing Chair** [\[Link\]](#)

2024 ISOC Symposium on Vehicle Security and Privacy (VehicleSec), Travel Grant Chair [\[Link\]](#)

2024 Midwest Security Workshop (MSW), Organizing Committee [\[Link\]](#)

2023 ISOC Symposium on Vehicle Security and Privacy (VehicleSec), Travel Grant Chair [\[Link\]](#)

## Program Committee (PC)

- 2027 IEEE Symposium on Security and Privacy (S&P)
  
- 2026 IEEE Symposium on Security and Privacy (S&P)
- 2026 ACM Conference on Computer and Communications Security (CCS)
- 2026 Network and Distributed System Security Symposium (NDSS)
- 2026 ISOC Workshop on Security and Privacy in Standardized IoT (SDIoTSec)
  
- 2025 IEEE Symposium on Security and Privacy (S&P)
- 2025 Network and Distributed System Security Symposium (NDSS)
- 2025 Annual Computer Security Applications Conference (ACSAC)
- 2025 International Symposium on Research in Attacks, Intrusions and Defenses (RAID)
- 2025 IEEE European Symposium on Security and Privacy (EuroS&P)
- 2025 ISOC Workshop on Security and Privacy in Standardized IoT (SDIoTSec)
  
- 2024 International Symposium on Research in Attacks, Intrusions and Defenses (RAID)
- 2024 IEEE European Symposium on Security and Privacy (EuroS&P)
- 2024 ACM ASIA Conference on Computer and Communications Security (ASIACCS)
- 2024 International Conference on Applied Cryptography and Network Security (ACNS)
- 2024 ISOC Symposium on Vehicle Security and Privacy (VehicleSec)
- 2024 IEEE/ACM Workshop on the Internet of Safe Things (SafeThings)
  
- 2023 European Symposium on Research in Computer Security (ESORICS)
- 2023 International Symposium on Research in Attacks, Intrusions and Defenses (RAID)
- 2023 ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)
- 2023 ISOC Symposium on Vehicle Security and Privacy (VehicleSec)
- 2023 Workshop of Designing Security for the Web (SecWeb)

## Artifact Evaluation Committee (AEC)

- 2023 USENIX Security Symposium
- 2023 ACM Conference on Computer and Communications Security (CCS)
- 2023 European Conference on Computer Systems (EuroSys)
- 2023 ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)
- 2023 USENIX Workshop on Offensive Technologies (WOOT)
  
- 2022 USENIX Security Symposium
- 2022 Annual Computer Security Applications Conference (ACSAC)

## Journal Reviewer

- 2024 IEEE Transactions on Information Forensics and Security (T-IFS)
- 2023 IEEE Transactions on Dependable and Secure Computing (TDSC)
- 2023 IEEE Transactions on Information Forensics and Security (T-IFS)

## Sub-reviewer/External Reviewer

- 2024 IEEE Symposium on Security and Privacy (S&P)

- 2024 Network and Distributed System Security Symposium (NDSS)
- 2023 USENIX Security Symposium
- 2023 Network and Distributed System Security Symposium (NDSS)
- 2023 Security and Privacy in Communication Networks (SecureComm)
- 2022 IEEE Symposium on Security and Privacy (S&P)
- 2022 USENIX Security Symposium
- 2022 Network and Distributed System Security Symposium (NDSS)
- 2022 ACM ASIA Conference on Computer and Communications Security (ASIACCS)
- 2022 Workshop on Automotive and Autonomous Vehicle Security (AutoSec)
- 2021 IEEE Symposium on Security and Privacy (S&P)
- 2021 Network and Distributed System Security Symposium (NDSS)
- 2021 Annual Computer Security Applications Conference (ACSAC)
- 2021 ACM ASIA Conference on Computer and Communications Security (ASIACCS)
- 2021 European Symposium on Research in Computer Security (ESORICS)
- 2020 Dependable Systems and Networks (DSN)
- 2020 Security and Privacy in Communication Networks (SecureComm)
- 2014 World Conference on Information Security Applications (WISA)

### Session Chair

- 2025 "Cyber-Physical Systems" Session, Annual Computer Security Applications Conference (ACSAC)
- 2025 "Autonomous Vehicle Security" Session, USENIX Symposium on Vehicle Security and Privacy (VehicleSec)
- 2025 "Electromagnetic Attacks" Session, ISOC Network and Distributed System Security Symposium (NDSS)
- 2024 "Side and Covert Channels" Session, IEEE/ACM Workshop on the Internet of Safe Things (SafeThings)
- 2024 "Firewall and IDS" Session, ISOC Symposium on Vehicle Security and Privacy (VehicleSec)
- 2023 "Autonomous Driving Security" Session, ISOC Symposium on Vehicle Security and Privacy (VehicleSec)
- 2022 "Robotic Vehicles Security" Session, Workshop on Automotive and Autonomous Vehicle Security (AutoSec)

### Volunteering

- 2014 Participating in the international World Wide Web Conference (WWW) as a volunteer, April, 7-11, Seoul, South Korea.
  - o Helped organization and progress of the conference

---

## Student Mentoring

### PhD

- Fall 2026 - **Sikandar Mehmood Abbasi**
  - Now o PhD student at Indiana University
  - o Project: Security for Robotic Vehicles
- Fall 2026 - **Muhammad Anser Sohaib**
  - Now o PhD student at Indiana University
  - o Project: Security for Robotic Vehicles

## Master

- Spring 2025 **Rajay Ravikumar**
- Master student at Indiana University
  - Project: Security for Robotic Vehicles
- Fall 2024 **Luke Harris**
- Master student at Indiana University
  - Project: Breaking Authentications in Vehicles
  - Job: Federal Deposit Insurance Corporation (FDIC)

## Undergraduate

- Spring 2026 - **Suhita Anubha**  
Now
- Undergraduate student at Indiana University
  - Project: Physical Sensor Attacks
- Spring 2026 - **Abhi Chaddha**  
Now
- Undergraduate student at Indiana University
  - Project: Robotic Vehicle Security
- Fall 2024 **Anthony Grego**
- Undergraduate student at Indiana University
  - Project: Robotic Vehicle Security
- Fall 2024 **Thomas Goeyardi**
- Undergraduate student at Indiana University
  - Project: Robotic Vehicle Security
- Fall 2024 **Maryanne McGlone**
- Undergraduate student at Indiana University
  - Project: Autonomous Vehicle Security

## Research Intern

- Fall 2025 **Kyoungmin Roh**
- Research Intern
  - Student at Dankook University
- Spring 2025 **Insup Lee** [[Homepage](#)]
- Research Intern
  - Student at Korea University
- Spring 2025 **Ho-Jin Choi**
- Research Intern
  - Student at Sogang University
- Spring 2025 **Ho Jun Lee**
- Research Intern
  - Student at Purdue University
- Spring 2025 **Md Rayhanul Islam**
- Research Intern
  - Student at University of Connecticut

Spring 2025 **Jewook Park**  
○ Research Intern  
○ Student at Georgia Tech

### At Purdue University

Fall 2021 - **Ruoyu Song**  
Spring 2024 ○ Ph.D. student at Purdue University  
○ Project: Discovering Adversarial Driving Maneuvers against Autonomous Vehicles (paper published at **USENIX Security'23** [\[PDF\]](#))

Fall 2022 - **Rwitam Bandyopadhyay**  
Spring 2023 ○ Master student at Purdue University  
○ Current employment: Amazon  
○ Project: A Systematic Study of Physical Sensor Attack Hardness (paper published at **IEEE S&P'24** [\[PDF\]](#))

Fall 2023 - **Faaz Masood Memon**  
Spring 2024 ○ Undergraduate student at Purdue University  
○ Project: Drone fail-safe algorithms

---

## Teaching

### Lecturer

2026 Spring **Systems and Protocol Security and Information Assurance** (INFO/CSCI-B 433), Indiana University, Bloomington, IN, USA [\[Syllabus\]](#) [Number of students: 92]

2025 Fall **Topics in Systems: Cyber-Physical Systems Security** (CSCI-B 649), Indiana University, Bloomington, IN, USA [\[Syllabus\]](#) [Number of students: 5]

2025 Spring **Systems and Protocol Security and Information Assurance** (CSCI-B 547 & INFO-I 533), In-Person Class, Indiana University, Bloomington, IN, USA [\[Syllabus\]](#) [Number of students: 7]

2025 Spring **Systems and Protocol Security and Information Assurance** (CSCI-B 547 & INFO-I 533), Online Class, Indiana University, Bloomington, IN, USA [Number of students: 57]

2024 Fall **Security for Networked Systems** (CSCI-B 544 & INFO-I 520), Indiana University, Bloomington, IN, USA [\[Syllabus\]](#) [Number of students: 17]

### Guest Lecturer

2023 Fall Topic: Defeating Logic bugs in Robotic Vehicles, Software Security (CS 490) Purdue University, West Lafayette, IN, USA [\[Slide\]](#)

2022 Fall Topic: Static Analysis, Software Security (CS 490) Purdue University, West Lafayette, IN, USA [\[Slide\]](#)

2022 Spring Topic: Program Analysis for IoT/CPS (Dynamic, Static Analysis, and Symbolic Execution), IoT/CPS Security (CS 590) Purdue University, West Lafayette, IN, USA [\[Slide\]](#)

## Teaching Assistant (TA)

- 2019 Fall **Teaching assistant** Problem Solving And Object-Oriented Programming (CS180) and Data Structures And Algorithms (CS251), Purdue University, West Lafayette, IN, the USA.
- Assignment and project development.
- 2014 Fall **Teaching assistant** Software Design Methods (CSED332), POSTECH, Pohang, South Korea.
- Planned, taught, and graded course term project assignments about implementing a database-management system (DBMS).

---

## University Activities

### PhD Dissertation Committee

- Spring 2026 **Anesu Chaora**
- Director of IT at Indiana University

### PhD Qualifying Exam Committee

- Spring 2026 **Andrew Meighan**
- PhD student in the Department of Intelligent Systems Engineering at Indiana University
- Spring 2025 **Hassan Jardali**
- PhD student in the Department of Intelligent Systems Engineering at Indiana University

### PhD Research Committee

- Spring 2026 -  
Now **Andrew Meighan**
- PhD student in the Department of Intelligent Systems Engineering at Indiana University
- Spring 2025 -  
Spring 2026 **Anesu Chaora**
- Director of IT at Indiana University

---

## Engagement, Diversity, and Outreach Activities

### Services for College

- 2025 Research presentation for undergraduate students, Luddy Graduate Admissions Coffee & Conversations, April 3, Indiana University, Bloomington, Indiana, USA.
- 2024 - Now Hosting the Cybersecurity Reading Group at the Luddy School, Indiana University, Bloomington, Indiana, USA.
- 2024 Research presentation for incoming undergraduate researchers, Luddy Student Research Fair, August 27, Indiana University, Bloomington, Indiana, USA.

### Services for Department

- 2025-2026 Faculty search committee, Indiana University, Bloomington, Indiana, USA.
- 2024-2026 Graduate education committee, Indiana University, Bloomington, Indiana, USA.
- 2024-2026 Master student admission committee, Indiana University, Bloomington, Indiana, USA.
- 2023 "Discovering Faulty Patches in Robotic Vehicles", Prospective PhD Visit Day Poster Session, March 23, Purdue University, West Lafayette, Indiana, USA.

---

## Reported Vulnerabilities

- August, 2023 **115 bugs in ArduPilot and PX4**, discovered by PatchVerif, [\[Link\]](#).
- February, 2021 **207 bugs in ArduPilot, PX4, and Paparazzi**, discovered by PGFuzz, [\[Link\]](#).
- March, 2020 **ArduPilot Bug #13815**, Checking min/max angular position of mount, [\[Link\]](#).
- March, 2020 **ArduPilot Bug #13811**, Drone crash when repeating flip mode, [\[Link\]](#).
- July, 2018 **ArduPilot Bug #8783**, NULL pointer dereference, [\[Link\]](#).
- June, 2018 **ArduPilot Bug #8644**, Memory leak, [\[Link\]](#).
- June, 2018 **ArduPilot Bug #8642**, Memory leak, [\[Link\]](#).
- June, 2018 **ArduPilot Bug #8641**, NULL pointer dereference, [\[Link\]](#).
- June, 2018 **ArduPilot Bug #8640**, Resource leak, [\[Link\]](#).

---

Last updated: April 24, 2026