Hyungsub Kim

✉ hk145@iu.edu
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. Currently, my efforts are dedicated to uncovering the root causes and formulating countermeasures against physical sensor attacks that target RVs.

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] ★ **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
Accepted to the 45th IEEE Symposium on Security and Privacy (**S&P**), San Francisco, California, USA, May 20-23, 2024.
(acceptance rate: 261/1463=17.8%)

[2] **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**), Anaheim, California, USA, August 9-11, 2023.
(acceptance rate: 442/1444=29.2%)

[3] ★ **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**), Anaheim, California, USA, August 9-11, 2023.
(acceptance rate: 442/1444=29.2%)

[4] ★ **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**), San Francisco, California, USA, May 23-26, 2022.
(acceptance rate: 147/1012=14.5%)

[5] **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**), Vancouver, British Columbia, Canada, August 11-13, 2021.
(acceptance rate: 246/1316=18.7%)

[6] ★ **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**), San Diego, California, USA, February 21-24, 2021.
(acceptance rate: 87/573=15.2%)

[7] **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**), Los Angeles, California, USA, December 5-9, 2016.
(acceptance rate: 48/210=22.8%)

[8] **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**), San Diego, California, USA, February 8-11, 2015.
(acceptance rate: 50/302=16.6%)

[9] **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**), 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**), San Diego, California, USA, February 27, 2023.

Workshop/Demo Papers

[1] **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**), San Diego, California, USA, February 27, 2023.

[2] **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**), 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

2024-2025 DARPA - Faithful Integration and Reverse-engineering and Emulation (FIRE),
Subcontract from Purdue University,
Indiana University share: $\$100,000$, percentage under my control: 100%

Talks

[1] **Modeling and Simulating Cyber-Physical Vulnerabilities**, *DARPA - Faithful Integration and Reverse-engineering and Emulation (FIRE) Workshop 2, Orlando, Florida, USA, January 22-23, 2025.*

[2] **Software Supply Chain Security**, *CAE Special Topics Workshop on Software Supply Chain Security, St. Louis, Missouri, USA, October 9, 2024.*

[3] **Sensor Modeling and Physical Sensor Attack Simulations**, *DARPA - Faithful Integration and Reverse-engineering and Emulation (FIRE) Quarterly Review, Melbourne, Florida, USA, September 17, 2024.*

[4] **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.

[5] **Cyber-physical Vulnerability Analysis**, *DARPA - Faithful Integration and Reverse-engineering and Emulation (FIRE) Quarterly Review, Tempe, Arizona, USA, May 29, 2024.*

[6] **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.*

[7] **PatchVerif: Discovering Faulty Patches in Robotic Vehicles**, *32nd USENIX Security Symposium, Anaheim, California, USA, August 10, 2023.*

[8] **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.

[9] **Logic Bug-Finding and Patching Tools**, *2nd Technology Innovation Institute (TII) Annual SSRC Research Partners Summit, Abu Dhabi, UAE, November 8, 2022.*

[10] **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.*

[11] **PGFUZZ: Policy-Guided Fuzzing for Robotic Vehicles**, *28th Network and Distributed System Security Symposium (NDSS), San Diego, California, USA, February 24, 2021.*

[12] **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.*

[13] **Exploring and Mitigating Privacy Threats of HTML5 Geolocation API**, *30th Annual Computer Security Applications Conference (ACSAC), New Orleans, Louisiana, USA, December 11, 2014.*

Fellowships, Awards, and Honors

☆**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

Organizing Committee

2025 ISOC Network and Distributed System Security Symposium (NDSS), Publication Chair
2025 USENIX Vehicle Security and Privacy (VehicleSec), Publicity Chair
2023-2024 ISOC Symposium on Vehicle Security and Privacy (VehicleSec), Travel Grant Chair
2025 Midwest Security Workshop (MSW), Organizing Chair
2024 Midwest Security Workshop (MSW), Organizing Committee

Program Committee (PC)

2025 IEEE Symposium on Security and Privacy (S&P)
2025 Network and Distributed System Security Symposium (NDSS)

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

Artifact Evaluation Committee (AEC)

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

Journal Reviewer

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

Sub-reviewer/External Reviewer

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

Session Chair

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.
- Helped organization and progress of the conference

Engagement, Diversity, and Outreach Activities

Services for College

2024 Research presentation for incoming undergraduate researchers, Luddy Student Research Fair, August 27, Indiana University, Bloomington, Indiana, USA.

Services for Department

2024-2025 Graduate education committee, Indiana University, Bloomington, Indiana, USA.

2024-2025 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.

Teaching

Lecturer

2025 Fall Cyber-Physical Systems Security, Indiana University, Bloomington, IN, USA

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

2024 Fall Security for Networked Systems (CSCI-B 544 & INFO-I 520), Indiana University, Bloomington, IN, USA [Syllabus] [Number of students: 16]

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, teached, and graded course term project assignments about implementing a database-management system (DBMS).

Student Mentoring

At Indiana University

Fall 2024 - Now
Chaoqi Zhang [Homepage]
- PhD student at Indiana University
- Project: Security for Robotic Vehicles (ongoing)

Spring 2025 - Now
Rajay Ravikumar
- Master student at Indiana University
- Project: Security for Robotic Vehicles (ongoing)

Fall 2024
Luke Harris
- Master student at Indiana University
- Project: Breaking Authentications in Vehicles

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

At Purdue University

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

Fall 2022 - Spring 2023
Rwitam Bandyopadhyay
- 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 - Spring 2024
Faaiz Masood Memon
- Undergraduate student at Purdue University
- Project: Drone fail-safe algorithms

Reported Vulnerabilities

August, 2023 **115 bugs in ArduPilot and PX4**, *discovered by PatchVerif*.
February, 2021 **207 bugs in ArduPilot, PX4, and Paparazzi**, *discovered by PGFuzz*.
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.