Hyungsub Kim

+1-765-337-5981
kim2956@purdue.edu
kimhyungsub.github.io

Research Interests

I am a system security researcher. I develop program analysis 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. I am on the academic job market in Fall 2023 and Spring 2024.

Education

2018–2023 **PhD in Computer Science**, ***Purdue University***, IN, the USA, *GPA – .*

2013–2015 **M.S. in Computer Science and Engineering**, ***POSTECH***, Pohang, South Korea, *GPA – 3.8/4.3*.
- Thesis: "Privacy Threats in HTML5 Geolocation API: Case Studies and Countermeasures"

2011–2013 **B.S. in School of Computer Science**, ***University of Seoul***, Seoul, South Korea, *GPA – 4.15/4.5*.

2005–2011 **Major in Mathematics**, ***Chonnam National University***, Gwangju, South Korea, *GPA – 3.27/4.5*.

2002–2005 **Major in Information Processing**, ***Pyeongchon Information Industry High School***, Anyang, South Korea.

Employment History

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: TBA)

[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**
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.

Talks

[1] **Defeating Cyber and Physical Attacks in Robotic Vehicles**, *Washington University in St. Louis, Missouri, USA, December 15, 2023*.

[2] **Defeating Cyber and Physical Attacks in Robotic Vehicles**, *University of Illinois at Urbana-Champaign, Illinois, USA, December 1, 2023*.

[3] **Defeating Cyber and Physical Attacks in Robotic Vehicles**, *Purdue University, Indiana, USA, November 28, 2023*, PhD dissertation defense.

[4] **Defeating Cyber and Physical Attacks in Robotic Vehicles**, *Indiana University Bloomington, Indiana, USA, November 17, 2023*.

[5] **Defeating Cyber and Physical Attacks in Robotic Vehicles**, *Georgia Institute of Technology, Atlanta, Georgia, USA, October 18, 2023*.

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

[7] **Defeating Logic Bugs in Robotic Vehicles**, *POSTECH, Pohang, Korea, June 1, 2023*.

[8] **Defeating Logic Bugs in Robotic Vehicles**, *UNIST, Ulsan, Korea, May 31, 2023*.

[9] **Defeating Logic Bugs in Robotic Vehicles**, *Ohio State University, Columbus, Ohio, USA, February 17, 2023*.

[10] **Defeating Logic Bugs in Robotic Vehicles**, *Purdue University, West Lafayette, Indiana, USA, November 18, 2022*, preliminary examination.

[11] **Defeating Logic Bugs in Robotic Vehicles**, *New York University Abu Dhabi, UAE, November 10, 2022*.

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

[13] **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*.

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

[15] **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*.

[16] **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

☆**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

2023-2024 ISOC Symposium on Vehicle Security and Privacy (VehicleSec) Travel Grant Chair

Program Committee (PC)

2024 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 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)
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 IEEE Transactions on Information Forensics and Security (T-IFS)

Sub-reviewer/External Reviewer

2021-2022, 2024 IEEE Symposium on Security and Privacy (Oakland)
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

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

University Services

Services for Department

2023 "Discovering Faulty Patches in Robotic Vehicles", Prospective PhD Visit Day Poster Session, March 23, Purdue University, West Lafayette, Indiana, USA.

Teaching Experience

Guest Lecturer

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

2022 Fall Topic: Static Analysis, Software Security (CS 490) Purdue University, West Lafayette, IN, USA

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

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).

Mentoring Experience

2021 - Now **Ruoyu Song**

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

2023 - Now **Shidong Pan**

- Co-supervised with Dr. Kisub Kim at Singapore Management University
- Ph.D. student at Australian National University
- Project: Privacy issues with drones (ongoing)

2023 - Now **Faaiz Masood Memon**
- Undergraduate student at Purdue University
- Project: Drone fail-safe algorithms (ongoing)

2023 - Now **Rwitam Bandyopadhyay**
- Amazon
- Project: A Systematic Study of Physical Sensor Attack Hardness (paper published at **IEEE S&P'24** [PDF])

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.

References

[1] **Dr. Dongyan Xu**
Professor
Purdue University
E-mail: dxu@purdue.edu

[2] **Dr. Sukarno Mertoguno**
Research Professor
Georgia Institute of Technology
E-mail: karno@gatech.edu

[3] **Dr. Antonio Bianchi**
Assistant professor
Purdue University
E-mail: antoniob@purdue.edu

[4] **Dr. Z. Berkay Celik**
Assistant professor
Purdue University
E-mail: zcelik@purdue.edu