Hyungsub Kim

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

Research Interests

My research interests are all aspects of computer security including Cyber-Physical Systems security, systems security, and web security. In particular, I am working on automatically finding logic bugs, patching them, and verifying the patches.

Education

2018–Present **PhD student 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.

Publications

Conference Papers

[1] **PatchVerif: Discovering Faulty Patches in Robotic Vehicles**
Hyungsub Kim, Muslum Ozgur Ozmen, Z. Berkay Celik, Antonio Bianchi, Dongyan Xu
In the Proceedings of the 32nd USENIX Security Symposium (**USENIX**), Anaheim, California, USA, August 9-11, 2023.

[2] **PGPATCH: Policy-Guided Logic Bug Patching for Robotic Vehicles**
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.

[3] **M2MON: Building an MMIO-based Security Reference Monitor for Unmanned Vehicles**
Arslan Khan, **Hyungsub Kim**, Byoungyoung Lee, Dongyan Xu, Antonio Bianchi, Dave (Jing) Tian
In the Proceedings of the 30th USENIX Security Symposium (**USENIX**), Vancouver, British Columbia, Canada, August 11-13, 2021.

[4] **PGFUZZ: Policy-Guided Fuzzing for Robotic Vehicles**
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.

[5] **Inferring Browser Activity and Status Through Remote Monitoring of Storage Usage**
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.

[6] **Identifying Cross-origin Resource Status Using Application Cache**
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.

[7] **Exploring and mitigating privacy threats of HTML5 geolocation API**
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.

Workshop Papers

[1] **Demo: Policy-based Discovery and Patching of Logic Bugs in Robotic Vehicles**
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.

Thesis

[1] **Privacy Threats in HTML5 Geolocation API: Case Studies and Countermeasures**
Master's Thesis, Department of Computer Science and Engineering, POSTECH, 2015.

Employment History

2015–2018 **Researcher**, *3rd R&D Institute (Intelligence, Surveillance and Reconnaissance)*, **Agency for Defense Development** (**ADD**), DaeJeon, South Korea.

2013–2015 **Research Assistant**, *High Performance Computing Laboratory*, **Pohang University of Science and Technology** (**POSTECH**), Pohang, South Korea.
Supervisor: Prof. Jong Kim

2013 **Research Assistant**, *Software Engineering Lab*, **POSTECH**, Pohang, South Korea.
Supervisor: Prof. Kyo-Chul Kang

2012–2013 **Research Assistant**, *Software Engineering Lab*, **University of Seoul**, Seoul, South Korea.
Supervisor: Prof. Byung-jeong Lee

2007–2009 **Auxiliary Policeman**, *Gwangju Seobu Police Station*, **Gwangju Metropolitan Police Agency**, Gwangju, South Korea.
Mandatory military service

2006–2007 **Research Assistant**, *Environmental Systems Engineering Lab*, **Gwangju Institute of Science and Technology**, Gwangju, South Korea.
Supervisor: Prof. Joon Ha Kim

Research Projects

2017–2018 **Automatic Video-based Target Detection and Classification**, *Agency for Defense Development (ADD)*.
- researched target classification, localization, and detection by using deep learning such as Convolutional Neural Networks (CNNs)

2015–2017 **Real-time Target Geo-positioning on multiple Videos**, *Agency for Defense Development (ADD)*.
- developed image matching algorithms for highly oblique Full Motion Videos (1080p, 30Hz)

2014–2015 **Context-aware Unified IoT Platform for Security and Privacy**, *Samsung*.
- invented anti-fingerprinting methods for IoT security

2014–2015 **Resilient Cyber-Physical Systems Research**, *Ministry of Science, ICT and Future Planning (MSIP)*.
- researched new attack and error models for Cyber-Physical Systems (CPS)

2013 **Next Generation Web Browser**, *Samsung*.
- implemented fine-grained sandboxing for a next generation web browser

Honors and Awards

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.

Technical Experiences

2014 ACSAC paper, **developed fine-grained permission and location models, and by inspecting the location sensitivity of each web page.** JAVA, Android

2013 Advanced Operating System, **modified Linux kernel to support I/O alignment for solid-state drives (SSD).** C

Technical Skills

Programming Languages

- C, C++, C#, JAVA, Python, TensorFlow, MATLAB, JavaScript, HTML (good)
- Shell scripts (Bash and PowerShell), SQL, Maple, LaTeX (intermediate)

Miscellaneous Availabilities

- Linux, GDB, SubVersion/Git

Teaching Experience

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).

Talks

[1] **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.*

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

[3] **Inferring Browser Activity and Status Through Remote Monitoring of Storage Usage**, *32nd Annual Computer Security Applications Conference (ACSAC), Los Angeles, California, USA, Dec 8, 2016.*

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

[5] **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.*

Activities

Artifact Evaluation Committee (AEC)

2022 USENIX Security Symposium

2022 Annual Computer Security Applications Conference (ACSAC)

Sub-reviewer

2021, 2022 IEEE Symposium on Security and Privacy (Oakland)
2021-2023 Network and Distributed System Security Symposium (NDSS)
2022 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 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

2022 Robotic Vehicles Security in Workshop on Automotive and Autonomous Vehicle Security (AutoSec)

Professional Activities

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

Service to Community

2006–2007 Volunteering at free tutoring for poor students at middle school, Gwangju, South Korea.
- 6 hours per week of volunteer service to the community through teaching underprivileged students

Extracurricular Activities

2005–2007 Literature dicussion club, Chonnam National University, Gwangju, South Korea.
- Wrote one poetry per week, discussed opions on the poetry, and applied lessons to real life

2002–2004 Computer science club, Pyeongchon Information Industry High School, Anyang, South Korea.
- Studied programming languages (C and C++), data structures, and algorithms for computer science competitions

Reported Vulnerabilities

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.