

HONGJUN CHOI

Assistant Professor
Electrical Engineering and Computer Science (EECS)
DGIST

RESEARCH INTERESTS

I am interested in **software and systems security** broadly. In particular, my research focuses on improving **security and reliability of autonomous cyber-physical systems (CPS)**, such as self-driving cars and drones, through various techniques and interdisciplinary knowledge, including program analysis, search-based software engineering, control theory, robotics, and AI/machine learning.

EDUCATION

Purdue University, West Lafayette, IN August 2022
Ph.D. in Department of Computer Science
Advisor: Xiangyu Zhang

POSTECH, Pohang, South Korea February 2008
M.S. in Computer Science and Engineering
Co-advisor: Sungje Hong and Jong Kim

Kyungpook National University, Daegu, South Korea February 2006
B.S. in Computer Science and Engineering

WORK EXPERIENCE

DGIST Sep 2022 - Current
Assistant Professor, Cyber-Physical Security (CPSec) Lab.

Purdue University Jan 2014 - Aug 2022
Research Assistant: Systems and Software Security / Software Engineering

HPC Lab, Pohang University of Science and Technology (POSTECH) Sep 2012 - Feb 2013
Researcher: researched on mobile security and privacy

Ubiquitous Computing Lab (UCL), IBM Jun 2011 - Oct 2011
Staff Software Engineer: managed enterprise customer projects for a mobile service platform - SPoSA (Smartphone-oriented Service Architecture)

Korea Software Solutions Lab (KSSL), IBM Jan 2008 - May 2011
Software Engineer: developed and tested enterprise software - CoreSCMS (Smart cards Management System), BOAPM (Business-Oriented Application Performance Monitoring)

Center for Mobile Embedded Software Technology (CMEST), POSTECH Mar 2006 - Dec 2007
Research Assistant: researched on mobile embedded security, including RFID security, digital right management, IPTV key management

Republic of Korea Army, Daejeon, South Korea Jun 2000 - Aug 2002
Military Service: Sergeant, Honorable Discharge (26 months)

PUBLICATION

- 4 papers ([2]★[4]★[7]★[8]) in top-tier security conferences (Top 4: IEEE S&P, CCS, USENIX Security, NDSS)
- 1 paper ([3]) in top-tier software engineering conferences (Top 4: ICSE, FSE, ASE, ISSTA)
- 1 paper ([1]) in top-tier AI/computer vision conference (ECCV)
- 2 papers ([5]★[9]) in selective security conferences (RAID, ACSAC)
- 1 paper ([6]) in a selective software engineering conference (CGO)

★ indicates first author

Conferences

- [1] **Physical Attack on Monocular Depth Estimation in Autonomous Driving with Optimal Adversarial Patches.**
Zhiyuan Cheng, James Liang, **Hongjun Choi**, Guanhong Tao, Zhiwen Cao, Dongfang Liu, and Xiangyu Zhang.
In *Proceedings of the 17th European Conference on Computer Vision (ECCV 2022)*, Tel-Aviv, Israel, 2022.
- [2] **RVPLAYER: Robotic Vehicle Forensics by Replay with What-if Reasoning.**
Hongjun Choi, Zhiyuan Cheng, and Xiangyu Zhang.
In *Proceedings of the Network and Distributed System Security Symposium (NDSS 2022)*, San Diego, CA, 2022 (Acceptance Rate: 14.0%, 53/377).
- [3] **PhysFrame: Type Checking Physical Frames of Reference for Robotic Systems.**
Sayali Kate, Michael Chinn, **Hongjun Choi**, Xiangyu Zhang, and Sebastian Elbaum.
In *Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2021)*, Virtual, 2021 (Acceptance Rate: 24.5%, 97/396).
- [4] **Cyber-Physical Inconsistency Vulnerability Identification for Safety Checks in Robotic Vehicles.**
Hongjun Choi, Sayali Kate, Yousra Aafer, Xiangyu Zhang, and Dongyan Xu.
In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS 2020)*, Orlando, USA, November 2020 (Acceptance Rate: 16.9% 121/715).
- [5] **Software-based Realtime Recovery from Sensor Attacks on Robotic Vehicles.**
Hongjun Choi, Sayali Kate, Yousra Aafer, Xiangyu Zhang, and Dongyan Xu.
In *Proceedings of the 23rd USENIX International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020)*, Donostia / San Sebastian, Spain, October 2020 (Acceptance Rate: 25.6%, 31/121).
- [6] **White-box Program Tuning.**
Wen-Chuan Lee, Yingqi Liu, Peng Liu, Shiqing Ma, **Hongjun Choi**, Xiangyu Zhang, and Rajiv Gupta.
In *Proceedings of 2019 IEEE/ACM International Symposium on Code Generation and Optimization (CGO 2019)*, Washington DC, USA, 2019 (Acceptance Rate: 31%, 27/69).
- [7] **Detecting Attacks against Robotic Vehicles: A Control Invariant Approach.**
Hongjun Choi, Wen-Chuan Lee, Yousra Aafer, Fan Fei, Zhan Tu, Xiangyu Zhang, Dongyan Xu, and Xinyan Deng.
In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS 2018)*, Toronto, Canada, November 2018 (Acceptance Rate: 16.6%, 134/809).
- [8] **Securing Real-Time Microcontroller Systems through Customized Memory View Switching.**
Chung Hwan Kim, Taegy Kim, **Hongjun Choi**, Zhongshu Gu, Byoungyoung Lee, Xiangyu Zhang, and Dongyan Xu.
In *Proceedings of the 25th Network and Distributed System Security Symposium (NDSS 2018)*, San Diego, CA, 2018 (Acceptance Rate: 21.5%, 71/331).
- [9] **RevARM: A Platform-agnostic ARM Binary Rewriter for Security Applications.**
Taegy Kim, Chung Hwan Kim, **Hongjun Choi**, Yonghwi Kwon, Brendan Saltaformaggio, Xiangyu Zhang, and Dongyan Xu.
In *Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC 2017)*, San Juan, PR, 2017 (Acceptance Rate: 19.7%, 48/244).

- [10] **Eavesdropping on Fine-grained User Activities within Smartphone Apps over Encrypted Network traffic.**
Brendan Saltaformaggio, Hongjun Choi, Kristen Johnson, Yonghwi Kwon, Qi Zhang, Xiangyu Zhang, Dongyan Xu, and John Qian.
In *10th USENIX Workshop on Offensive Technologies (WOOT'16)*, Austin, TX, 2016 (Acceptance Rate: 47.7%, 21/44).
- [11] **Reducing IPTV Channel Zapping Time based on Viewer's Surfing Behavior and Preference.**
Yuna Kim, Jae Keun Park, Hongjun Choi, Sangho Lee, Heejin Park, Jong Kim, Zino Lee, and Kwangil Ko.
In *2008 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting*, pages 1–6. IEEE, 2008 (Acceptance Rate: 37.1%, 52/140).
- [12] **Secure and Efficient Offline RFID Authentication for Anti-counterfeiting.**
Hongjun Choi, Sungje Hong, and Jong Kim.
In *Proceeding of the 2nd International Conference on Ubiquitous Information Technologies & Applications (ICUT 2nd)*, Bali, Indonesia, December, 2007 (Acceptance Rate: 29.9%, 118/394).
- [13] **Distributing ID-based Public Key Management based on Clustering in MANET.**
Hongjun Choi, Sungje Hong, and Jong Kim.
In *Proceedings of the Korean Information Science Society Conference*, Busan, Korea, October, 2006. Korean Institute of Information Scientists and Engineers (KIISE).
- [14] **Detection of Worm Generated by Polymorphic Engine.**
Ki-Hun Lee, Seung-Ick Lee, Hongjun Choi, Yu-Na Kim, Sung-Je Hong, and Jong Kim.
In *Proceedings of the Korean Information Science Society Conference*. Korean Institute of Information Scientists and Engineers (KIISE), October, 2006.

Technical Reports

- [15] **Automated Differential Testing for Energy-Efficient Control Software.**
Hongjun Choi, Bruce V Nguyen, Sayali Kate, Xiangyu Zhang, and Dongyan Xu. Technical report. Center for Education and Research Information Assurance and Security (CERIAS), Purdue. 2018.

Patents

- [16] **Off-line Authentication Method of Preventing Fabrication of Genuine Products,**
Hongjun Choi, Jong Kim, and Sungje Hong. 2009. Korea Patent No: 10-0917177-000.

TEACHING EXPERIENCE

Instructor, Special Topics in Cyber-Physical Systems (CPS) - CPS Security (IC899 at DGIST), Spring 2022

Guest Instructor, IoT/CPS Security (CS 59200-ICS at Purdue), Fall 2022

Teaching Assistant, Systems Programming (CS252 at Purdue), Spring 2017

Teaching Assistant, Computer Security (CS6035 at POSTECH), Fall 2006

ACADEMIC SERVICES

Program Committee

USENIX Security Symposium (SECURITY), Artifact Evaluation Committee, 2022

IEEE Symposium on Security and Privacy (IEEE S&P), Shadow PC, 2021

IEEE Conference on Dependable and Secure Computing (IEEE DSC), Program Committee, 2022

External Reviewer

ACM Conference on Computer and Communications Security (CCS), 2020,2019,2016,2015
USENIX Security Symposium (SECURITY), 2022, 2021, 2018
Conference on Data and application security and privacy (CODASPY), 2021
IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2015
IEEE Secure Development Conference (SecDev), 2017
Engineering Secure Software and Systems (ESSOS), 2017
ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE), 2022, 2020, 2018, 2016
International Conference on Software Engineering (ICSE), 2022, 2020, 2017
Automated Software Engineering (ASE), 2020, 2018
International Symposium on Software Testing and Analysis (ISSTA), 2017

Journal Reviewer

IEEE Internet of Things Journal, 2020

HONORS AND AWARDS

Rising Star, CPS Rising Stars Workshop 2022 (sponsored by NSF and UVA)

Network and Distributed System Security Symposium (NDSS) Student Grant, 2022
ACM Conference on Computer and Communications Security Student Conference Grant, 2021
IEEE Symposium on Security and Privacy Student Travel Grant, 2021
USENIX Security '20 Student Grant, 2020
Academic Performance Scholarship (Full-funded), Dongbu Cultural Foundation, S. Korea, 2004, 2005
Academic Excellence Scholarship, Kyungpook National University, S. Korea, 2002, 2003

TALKS AND PRESENTATIONS

RVPLAYER: Robotic Vehicle Forensics by Replay with What-if Reasoning

The Network and Distributed System Security Symposium, San Diego, April 2022

Towards Secure and Reliable Robotic Vehicles with Holistic Modeling and Program Analysis

CISPA Helmholtz Center for Information Security, Virtual, March 2022

Attack-resilient Control for Robotic Vehicles

Cheongju University, Virtual, Feb 2021

Cyber-physical Inconsistency Vulnerability Identification for Safety Checks in Robotic Vehicles

ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, Nov 2020

Software-based Realtime Recovery from Sensor Attacks on Robotic Vehicles

The 23rd USENIX International Symposium on Research in Attacks, Intrusions and Defenses, Virtual Event, Oct 2020

Detecting Attacks Against Robotic Vehicles: A Control Invariant Approach

ACM SIGSAC Conference on Computer and Communications Security, Toronto, Canada, Nov 2018

Automated Differential Testing for Energy-Efficient Control Software

The Office of Naval Research (ONR) Naval Enterprise Partnership Teaming with Universities for National Excellence (NEPTUNE) Meeting II, MIT, Cambridge MA, May 2017

Towards Vetted Sensing and Control System Firmware and Software

The Office of Naval Research (ONR) Naval Enterprise Partnership Teaming with Universities for National Excellence (NEPTUNE) Meeting I, University of California, Davis, CA, Nov 2016

LIST OF REFERENCES

Available upon a request.