Taegyu **Kim**

PH.D.

305 N. University St., West Lafayette, Indiana 47907, USA

tgkim@purdue.edu | tgkim.gitlab.io

Research Interests

Robotic Vehicle Security, Systems Security, and Program Analysis

Education

Purdue University — *West Lafayette, IN, USA*

PH.D. IN ELECTRICAL AND COMPUTER ENGINEERING — *Aug. 2015 - May 2021*

- Advisors: Dongyan Xu and Dave Tian (in Computer Science)

KAIST (Korea Advanced Institute of Science and Technology) — *Daejeon, South Korea*

M.S. IN ELECTRICAL ENGINEERING — *Mar. 2013 - Feb. 2015*

- Advisor: Kyu Ho Park

Kwangwoon University — *Seoul, South Korea*

B.S. IN ELECTRONICS AND COMMUNICATIONS ENGINEERING — *Mar. 2005 - Feb. 2013*

- GPA: 4.35/4.5 (Top Rank)

Work Experience

Assistant Professor, Pennsylvania State University — *Starting from Jan. 2022*

- College of Information Sciences and Technology

State College, PA, USA

Postdoctoral Researcher, Purdue University — *May 2021 - Dec. 2021*

- Department of Computer Science (Host: Dongyan Xu and Dave (Jing) Tian)

West Lafayette, IN, USA

Conference Publications

PASAN: Detecting Peripheral Access Concurrency Bugs within Bare-metal Embedded Applications — *Aug. 2021*

Taegyu Kim, Vireshwar Kumar, Junghwan Rhee, Jizhou Chen, Kyungtae Kim, Chung Hwan Kim, Dongyan Xu, Dave (Jing) Tian

Proceedings of the 30th USENIX Security Symposium (USENIX Security'21)

Accepted to appear

From Control Model to Program: Investigating Robotic Aerial Vehicle Accidents with MAYDAY — *Aug. 2020*

Taegyu Kim, Chung Hwan Kim, Altay Ozen, Fan Fei, Zhan Tu, Xiangyu Zhang, Xinyan Deng, Dave (Jing) Tian, Dongyan Xu

Proceedings of the 29th USENIX Security Symposium (USENIX Security'20)

Acceptance rate: 16.1%

RVFuzzer: Finding Input Validation Bugs in Robotic Vehicles through Control-Guided Testing — *Aug. 2019*

Taegyu Kim, Chung Hwan Kim, Junghwan Rhee, Fan Fei, Zhan Tu, Gregory Walkup, Xiangyu Zhang, Xinyan Deng, Dongyan Xu

Proceedings of the 28th USENIX Security Symposium (USENIX Security'19)

Acceptance rate: 15.7%

Securing Real-Time Microcontroller Systems through Customized Memory View Switching — *Feb. 2018*

Chung Hwan Kim, **Taegyu Kim**, Hongjun Choi, Zhongshu Gu, Byoungyoung Lee, Xiangyu Zhang, Dongyan Xu

Proceedings of the 25th Network and Distributed System Security Symposium (NDSS'18)

Acceptance rate: 21.0%

Cross-Layer Retrofitting of UAVs Against Cyber-Physical Attacks *May. 2018*
Fan Fei, Zhan Tu, Ruikun Yu, **Taegyu Kim**, Xiangyu Zhang, Dongyan Xu, Xinyan Deng
Proceedings of the IEEE International Conference on Robotics and Automation (ICRA'18)
Acceptance rate: 40.6%

RevARM: A Platform-Agnostic ARM Binary Rewriter for Security Applications *Dec. 2017*
Taegyu Kim, Chung Hwan Kim, Hongjun Choi, Yonghwi Kwon, Brendan Saltaformaggio, Xiangyu Zhang, Dongyan Xu
Proceedings of the Annual Computer Security Applications Conference (ACSAC'17)
Acceptance rate: 19.7%

Malfinder: Accelerated Malware Classification System through Filtering on Manycore System *Feb. 2015*
Taegyu Kim, Woomin Hwang, Chulmin Kim, Dong-Jae Shin, Ki-Woong Park, Kyu Ho Park
Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP'15)

I-Filter: Identical Structured Control Flow String Filter for Accelerated Malware Variant Classification *Aug. 2014*
Taegyu Kim, Woomin Hwang, Ki-Woong Park, Kyu Ho Park
Proceedings of the International Symposium on Biometrics and Security Technologies (ISBAST'14)

Journal Publications

Learning from the Ones that Got Away: Detecting New Forms of Phishing Attacks *Nov. 2018*
Christopher N. Gutierrez, **Taegyu Kim**, Raffaele D. Corte, Jeffrey Avery, Saurabh Bagchi, Dan Goldwasser, Marcello Cinque
IEEE Transactions on Dependable and Secure Computing (TDSC) Vol.15, Issue 6, pp.988-1001

MalCore: Toward a Practical Malware Identication System Enhanced with Manycore Technology *Jan. 2016*
Taegyu Kim, Ki-Woong Park
Information Systems Security and Privacy in Communications in Computer and Information Science, Vol.576, pp.31-48

Patents

The Device for Analyzing a Malware based on Similarity *Sep. 2015*
Taegyu Kim, Woomin Hwang, Kyu Ho Park
South Korea, No. 1020150096061 (granted)

Honors & Awards

Purdue ECE Fellowship *West Lafayette, IN, USA*
$6,000 over one year awarded by Purdue University *2015*

Presentations

From Control Model to Program: Investigating Robotic Aerial Vehicle Accidents with MAYDAY *Virtual Conference*
USENIX Security Symposium *Aug. 2020*

RVFuzzer: Finding Input Validation Bugs in Robotic Vehicles through Control-Guided Testing *Santa Clara, CA*
USENIX Security Symposium *Aug. 2019*

Control-Guided Program Bug Investigation and Discovery *Philadelphia, PA*
ONR RHIMES PI meeting *Mar. 2019*

RevARM: A Platform-Agnostic ARM Binary Rewriter for Security Applications *Orlando, FL*
Annual Computer Security Applications Conference *Dec. 2017*

Teaching Experience

Guest Instructor — *University of Texas at Dallas*

CS 6301, Security of CPS & IoT Systems — *Nov. 2020*

- Lectured on the state-of-the-art research trend and future project direction in non-traditional system fuzzing including cyber-physical systems

Guest Instructor — *Purdue University*

CS 590, IoT/CPS Security — *Feb. 2020*

- Lectured on the state-of-the-art research trend and future project direction in cyber-physical system fuzzing and investigation

Teaching Assistant — *KAIST*

CC 522, Introduction to Instruments — *Aug. 2014 - Dec. 2015*

Student Mentoring Experience

Jizhou Chen (Undergraduate Student from Purdue University) — *May. 2019 - Present*

- Research topic: peripheral device driver vulnerability detection on embedded systems using the compiler-level analysis
- Research topic: robotic vehicle firmware hardening using the binary analysis technique

William Wang (Undergraduate Student from University of California, Los Angeles) — *June. 2020 - Present*

- Research topic: securing robotic aerial vehicle communication while imposing low overhead

Sungwoo Kim (Undergraduate Student from Kwangwoon University) — *Sep. 2020 - Feb. 2021*

- Research topic: securing controller area network (CAN) communication using on a binary program analysis technique

Gisu Yeo (Undergraduate Student from Pusan National University) — *Oct. 2020 - Jan. 2021*

- Research topic: securing controller area network (CAN) communication using on a binary program analysis technique

Professional Services

Technical Program Committee

- ACM ASIA Conference on Computer and Communications Security (ASIACCS), 2021, 2022
- Workshop on Binary Analysis Research (BAR), 2021
- International Workshop on Automotive and Autonomous Vehicle Security (AutoSec), 2021
- EAI International Conference on Security and Privacy in Communication Networks (SecureComm), 2020

Journal Reviewer

- IEEE Transactions on Dependable and Secure Computing (TDSC), 2021

Artifact Evaluation Committee

- USENIX Security Symposium (USENIX Security), 2021

Sub-reviewer

- USENIX Security Symposium (USENIX Security), 2020, 2021
- Network and Distributed System Security Symposium (NDSS), 2019, 2021
- IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2020
- IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), 2020