Taegyu **Kim**

PH.D CANDIDATE

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

tgkim@purdue.edu

Education

Purdue University — *West Lafayette, IN, USA*

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

- Co-advised: 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)

Research Interests

Cyber-Physical System Security, IoT Security, Embedded System Security, and Program Analysis

Skills

Programming C/C++, Python, Assembly (x86, ARM), Verilog, Java, Matlab, MySQL, R

Tool LLVM, IDA Pro, GDB, CUDA

Languages Korean, English, Japanese

Conference Publications

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%

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%

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: 21.5%

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)

Nominee for Best Student Paper Award

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)
Best Paper Award

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*

Best Paper Award *Kuala Lumpur, Malaysia*
Large-scale malware classification speed acceleration without the loss of accuracy (ISBAST '14) *2014*

Talk and Presentation

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, NJ*
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*

Work Experience

FRIENDS Lab, Purdue University *West Lafayette, IN, USA*
Research Assistant *Jan. 2016 - Present*
- Researching on cyber-physical system security
- Mainly focusing on fuzzing and investigation on security attacks against unmanned vehicle based on program analysis techniques and control theory

CORE Lab, KAIST *Daejeon, South Korea*
Research Assistant *Mar. 2013 - Feb. 2015*
- Developed high-performance malware variant classification and detection system using control flow information
- Utilized the efficient memory management technique which is the part of the MN-MATE project for high performance

Military Service *Hongcheon, South Korea*

Sergeant *Oct. 2006 - Oct. 2008*

- Served in the national army for two years

Teaching Experience

KAIST *Daejeon, South Korea*

Teaching Assistant *Aug. 2014 - Dec. 2015*

- CC522, Introduction to Instruments

Advising Experience

Student Mentoring *Purdue University*

Jizhou Chen (Undergraduate Student) *May. 2019 - Present*

Researching on embedded/cyber-physical system security projects to detect vulnerabilities based on program analysis techniques at both binary and compiler level.

Professional Services

External Reviewer

- Network and Distributed System Security Symposium (NDSS), 2019
- USENIX Security Symposium (USENIX Security), 2020