Chung Hwan Kim

800 W Campbell Rd, MS EC31
Richardson, TX 75080

Assistant Professor
University of Texas at Dallas

chungkim@utdallas.edu
https://chungkim.io

Research Interests

Cyber-Physical Systems Security, **Systems Security**, **Software Security and Reliability**.

Education

08/2012–08/2017 | **Purdue University** ..... West Lafayette, IN
08/2017 | Ph.D. in Computer Science
Co-advised: Dongyan Xu and Xiangyu Zhang

08/2010–08/2012 | **University of Utah** ..... Salt Lake City, UT
08/2012 | M.Sc. in Computer Science
Co-advised: John Regehr and Eric Eide

03/2001–06/2008 | **Sunmoon University** ..... Asan, Chungnam, Korea
08/2008 | B.Sc. in Computer and Information Sciences

Work Experience

08/2020–present | **University of Texas at Dallas** ..... Richardson, TX
Assistant Professor, Department of Computer Science

08/2017–07/2020 | **NEC Labs America** ..... Princeton, NJ
Researcher, Computer Security Department

08/2012–08/2017 | **Purdue University** ..... West Lafayette, IN
Research Assistant, Lab FRIENDS

06/2015–07/2015 | **LG Electronics** ..... Seoul, Korea
Research Intern, Software Platform Team, CTO

05/2013–08/2013 | **NEC Labs America** ..... Princeton, NJ
Research Intern, Autonomic Management Department

01/2011–08/2012 | **University of Utah** ..... Salt Lake City, UT
Research Assistant, Flux Research Group

Publications

[**c1**] **Vessels: Efficient and Scalable Deep Learning Prediction on Trusted Processors.**
Kyungtae Kim, **Chung Hwan Kim**, Junghwan Rhee, Xiao Yu, Haifeng Chen, Dave (Jing) Tian, Byoungyoung Lee.
In *Proceedings of the 11th ACM Symposium on Cloud Computing (SOCC 2020).*
Virtual Event, October 2020.

[**c2**] **Detecting Malware Injection with Program-DNS Behavior.**
Yixin Sun, Kangkook Jee, Suphannee Sivakorn, Zhichun Li, Cristian Lumezanu, Lauri Korts-Pärn, Zhenyu Wu, Junghwan Rhee, **Chung Hwan Kim**, Mung Chiang, Prateek Mittal.
In *Proceedings of the 5th IEEE European Symposium on Security and Privacy (EuroS&P 2020).*
Virtual Event, September 2020.

[c3] **From Control Model to Program: Investigating Robotic Aerial Vehicle Accidents with Mayday.**
Taegyu Kim, **Chung Hwan Kim**, Altay Ozen, Fan Fei, Zhan Tu, Xiangyu Zhang, Xinyan Deng, Dave (Jing) Tian, Dongyan Xu.
In *Proceedings of the 29th USENIX Security Symposium (Security 2020).*
Virtual Event, August 2020.

[j4] **CAFE: A Virtualization-Based Approach to Protecting Sensitive Cloud Application Logic Confidentiality.**
Sungjin Park, **Chung Hwan Kim**, Junghwan Rhee, Jongjin Won, Taisook Han, Dongyan Xu.
IEEE Transactions on Dependable and Secure Computing (TDSC),
11(7), July-August 2020.

[c5] **HFL: Hybrid Fuzzing on the Linux Kernel.**
Kyungtae Kim, Dae R. Jeong, **Chung Hwan Kim**, Yeongjin Jang, Insik Shin, Byoungyoung Lee.
In *Proceedings of the 27th Network and Distributed System Security Symposium (NDSS 2020).*
San Diego, CA, February 2020.

[c6] **Progressive Processing of System Behavioral Query.**
Jiaping Gui, Xusheng Xiao, Ding Li, **Chung Hwan Kim**, Haifeng Chen.
In *Proceedings of the 35th Annual Computer Security Applications Conference (ACSAC 2019).*
San Juan, PR, December 2019.

[c7] **RVFuzzer: Finding Input Validation Bugs in Robotic Vehicles through Control-Guided Testing.**
Taegyu Kim, **Chung Hwan Kim**, Junghwan Rhee, Fan Fei, Zhan Tu, Gregory Walkup, Xiangyu Zhang, Xinyan Deng, Dongyan Xu.
In *Proceedings of the 28th USENIX Security Symposium (Security 2019).*
Santa Clara, CA, July 2019.

[c8] **PoLPer: Process-Aware Restriction of Over-Privileged Setuid Calls in Legacy Applications.**
Yuseok Jeon, Junghwan Rhee, **Chung Hwan Kim**, Zhichun Li, Mathias Payer, Byungyoung Lee, Zhenyu Wu.
In *Proceedings of the 9th ACM Conference on Data and Application Security and Privacy (CODASPY 2019).*
Dallas, TX, March 2019.

[c9] **SAQL: A Stream-based Query System for Real-Time Abnormal System Behavior Detection.**
Peng Gao, Xusheng Xiao, Ding Li, Zhichun Li, Kangkook Jee, Zhenyu Wu, **Chung Hwan Kim**, Sanjeev R. Kulkarni, Prateek Mittal.
In *Proceedings of the 27th USENIX Security Symposium (Security 2018).*
Baltimore, MD, August 2018.
* Top 10 Finalist for CSAW Best Applied Research Paper Award.

[c10] **Securing Real-Time Microcontroller Systems through Customized Memory View Switching.**
Chung Hwan Kim, Taegyu Kim, Hongjun Choi, Zhongshu Gu, Byoungyoung Lee, Xiangyu Zhang, Dongyan Xu.
In *Proceedings of the 25th Network and Distributed System Security Symposium (NDSS 2018).*
San Diego, CA, February 2018.

[c11] **RevARM: A Platform-Agnostic ARM Binary Rewriter for Security Applications.**
Taegyu Kim, **Chung Hwan Kim**, Hongjun Choi, Yonghwi Kwon, Brendan Saltaformaggio, Xiangyu Zhang, Dongyan Xu.
In *Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC 2017).*
Orlando, FL, December 2017.

[c12] **J-Force: Forced Execution on JavaScript.**
Kyungtae Kim, I Luk Kim, **Chung Hwan Kim**, Yonghwi Kwon, Yunhui Zheng, Xiangyu Zhang, Dongyan Xu.
In *Proceedings of the 26th International World Wide Web Conference (WWW 2017).*
Perth, WA, Australia, April 2017.

[c13] **PerfGuard: Binary-Centric Application Performance Monitoring in Production Environments.**
Chung Hwan Kim, Junghwan Rhee, Kyu Hyung Lee, Xiangyu Zhang, Dongyan Xu.
In *Proceedings of the 24th ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE 2016)*,
Seattle, WA, November 2016.

[c14] **Accurate, Low Cost and Instrumentation-Free Security Audit Logging for Windows.**
Shiqing Ma, Kyu Hyung Lee, **Chung Hwan Kim**, Junghwan Rhee, Xiangyu Zhang, Dongyan Xu.
In *Proceedings of the 31st Annual Computer Security Applications Conference (ACSAC 2015)*,
Los Angeles, CA, December 2015.

[c15] **CAFE: A Virtualization-Based Approach to Protecting Sensitive Cloud Application Logic Confidentiality.**
Chung Hwan Kim, Sungjin Park, Junghwan Rhee, Jongjin Won, Taisook Han, Dongyan Xu.
In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2015)*,
Singapore, April 2015.

[c16] **IntroPerf: Transparent Context-Sensitive Multi-Layer Performance Inference using System Stack Traces.**
Chung Hwan Kim, Junghwan Rhee, Hui Zhang, Nipun Arora, Guofei Jiang, Xiangyu Zhang, Dongyan Xu.
In *Proceedings of the 2014 ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2014)*,
Austin, TX, June 2014.

Patents

[p1] **Graphics Processing Unit Acceleration for Secure Enclaves.**
Chung Hwan Kim, Junghwan Rhee, Kangkook Jee, Zhichun Li, Adil Ahmad.
US 20200257794 A1, Filed February 2020.

[p2] **Confidential Machine Learning with Program Compartmentalization and SGX.**
Chung Hwan Kim, Junghwan Rhee, Kangkook Jee, Zhichun Li.
US 20200184070 A1, Filed November 2019.

[p3] **Protocol-Independent Deep Learning Based Anomaly Detection for OT Network.**
Junghwan Rhee, Ziqiao Zhou, Lu-An Tang, Zhengzhang Chen, **Chung Hwan Kim**, Zhichun Li.
US 20200059484 A1, Filed August 2019.

[p4] **Host Behavior and Network Analytics Based Automotive Secure Gateway.**
Junghwan Rhee, Hongyu Li, Shuai Hao, **Chung Hwan Kim**, Zhenyu Wu, Zhichun Li, Kangkook Jee, Lauri Korts-Parn.
US 20190104108 A1, Filed September 2018.

[p5] **Transparent Performance Inference of Whole Software Layers and Context-Sensitive Performance Debugging.**
Junghwan Rhee, Hui Zhang, Nipun Arora, Guofei Jiang, **Chung Hwan Kim.**
US 9367428 B2, Granted June 2016.

[p6] **Apparatus and Method For Software Security: A Secure, Platform-Independent Process Execution Model.**
Chung Hwan Kim, Jeong Bae Lee, Yoon Young Park.
KR 1020090056092, Granted December 2011.

Posters

[o1] **IntroPerf: Transparent Context-Sensitive Multi-Layer Performance Inference using System Stack Traces.**
Chung Hwan Kim, Junghwan Rhee, Hui Zhang, Nipun Arora, Guofei Jiang, Xiangyu Zhang, Dongyan Xu.
2014 ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2014),
Austin, TX, June 2014.

[o2] **KMAG: VMM-level Malware Detection via Kernel Data Access Profiling.**
Chung Hwan Kim, Dannie Stanley, Rick Porter, Dongyan Xu.
14th Annual CERIAS Information Security Symposium (CERIAS 2013),
West Lafayette, IN, April 2013.

[o3] **Accelerating Dynamic Binary Translation with GPUs.**
Chung Hwan Kim, Srikanth Manikarnike, Vaibhav Sharma, Eric Eide, Robert Ricci.
University of Utah School of Computing Research Day 2011,
Salt Lake City, UT, March 2011.

Technical Reports

[t1] **XenTT: Deterministic Systems Analysis in Xen.**
Anton Burtsev, David Johnson, **Chung Hwan Kim**, Mike Hibler, Eric Eide, John Regehr.
XenSummit North America 2012,
San Diego, CA, August 2012.

[t2] **Iterative Backtracking via Deterministic Virtual Machine Replay and Virtual Machine Introspection.**
Chung Hwan Kim.
Master's Project Report,
Salt Lake City, UT, August 2012.

Talks and Presentations

03/2020 **University of Texas at Dallas** ..... Richardson, TX
A Cross-Layer Approach to Robotic Vehicle Controller Security.

02/2020 **University of Central Florida** ..... Orlando, FL
A Cross-Layer Approach to Robotic Vehicle Controller Security.

02/2020 **Virginia Polytechnic Institute and State University** ..... Blacksburg, VA
A Cross-Layer Approach to Robotic Vehicle Controller Security.

02/2020 **CISPA Helmholtz Center for Information Security** ..... Saarbrücken, Germany
A Cross-Layer Approach to Robotic Vehicle Controller Security.

02/2020 **Oregon State University** ..... Corvallis, OR
A Cross-Layer Approach to Robotic Vehicle Controller Security.

11/2018 **KOCSEA Technical Symposium** ..... Mountain View, CA
Securing Real-Time Microcontroller Systems through Customized Memory View Switching.

02/2018 **Network and Distributed System Security Symposium** ..... San Diego, CA
Securing Real-Time Microcontroller Systems through Customized Memory View Switching.

03/2017 **University of Delaware** ..... Newark, DE
Protecting Production Systems from Software Anomalies.

02/2017 **NEC Labs America** ..... Princeton, NJ
Building Reliable and Secure Production Systems through Program Introspection.

02/2017 **University of Texas at San Antonio** ..... San Antonio, TX
Protecting Production Systems from Software Anomalies.

11/2016 **ACM SIGSOFT International Symposium on the Foundations of Software Engineering** ..... Seattle, WA
PerfGuard: Binary-Centric Application Performance Monitoring in Production Environments.

07/2015 **LG Electronics** ..... Seoul, Korea
Toward Reliable Software via System Level Introspection.

09/2009 **World IT Show 2009** ..... Seoul, Korea
Kernel Trace Toolkit for Embedded Linux Systems.

06/2008 **World IT Show 2008** ..... Seoul, Korea
Embedded System Prototyping (demo).

Awards and Honors

10/2018 **Top 10 Finalist.**
CSAW Best Applied Research Paper Award.

08/2010–08/2012 **Chungnam Provincial Government Global Scholarship.**
$80k for 2 years of Master's study.

11/2007 **Grand Prize.**
Capstone Design Fair 2007, Innovation Center for Engineering Education, Sunmoon University.

02/2007 **Learning Excellence Award.**
BIT Computer Advanced Windows Developer Course (1-year course).

08/2006–08/2008 **Sunmoon University Scholarships.**
Merit-based scholarships.

Student Travel Grants.
09/2016 SIGSOFT CAPS for attending the 24th ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE 2016).
07/2016 25th USENIX Security Symposium (Security 2016).
05/2014 2014 ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2014).
10/2011 23rd ACM Symposium on Operating Systems Principles (SOSP 2011).
02/2011 8th USENIX Symposium on Networked Systems Design and Implementation (NSDI 2011).
09/2010 9th USENIX Symposium on Operating Systems Design and Implementation (OSDI 2010).

Teaching Experience

Spring 2021 **Instructor.** University of Texas at Dallas ..... Richardson, TX
CS 6324: Information Security (link).

Fall 2020 **Instructor.** University of Texas at Dallas ..... Richardson, TX
CS 6301.007: Special Topics in Computer Science - Security of CPS & IoT Systems (link).

Spring 2017 | **Guest Instructor.** Purdue University ..... West Lafayette, IN
CS503: Operating Systems (link).

Fall 2016 | **Guest Instructor.** Purdue University ..... West Lafayette, IN
CS527: Software Security (link).

Student Supervision

05/2020–08/2020 | **Research Intern.** Seulbae Kim (Ph.D., Georgia Institute of Technology, expected 2023).
Researched on a summer intern project to build a fuzzing system for self-driving cars.

01/2020–03/2020 | **Research Intern.** Cody Holliday (M.S., Oregon State University, expected 2021).
Researched on a spring intern project to enable secure authentication of USB devices.

05/2019–08/2019 | **Research Intern.** Kyungtae Kim (Ph.D., Purdue University, expected 2021).
Researched on a summer intern project to build an efficient and scalable deep learning system with Intel SGX [c1].

05/2018–08/2018 | **Research Intern.** Adil Ahmad (Ph.D., Purdue University, expected 2021).
Researched on a summer intern project to enable confidential GPU-acceleration on trusted processors [p1].

08/2016–05/2020 | **Graduate Student.** Taegyu Kim (Ph.D., Purdue University, expected 2021).
Researched on the security enhancement of robotic vehicles through "control-aware" testing [c7], analysis [c3], and binary instrumentation [c11].

08/2016–12/2016 | **Undergraduate Student.** Brian Hays (B.Sc., Purdue University, graduated 2017).
Contributed to a cyber-physical systems security project [c10] finding several vulnerabilities in the firmware of a robotic vehicle system.

Academic Services

Program Committee.
2020 | Dependable Systems and Networks (DSN).
2019 | Network and Distributed System Security Symposium (NDSS).
Total 18 reviews and served as a session chair.

Artifact Evaluation Committee.
2019 | ACM Symposium on Operating Systems Principles (SOSP).

Journal Reviewer.
2020 | IEEE Transactions on Mobile Computing (TMC).
2018 | IEEE Transactions on Networking (TNET).
2015 | IEEE Transactions on Information Forensics and Security (TIFS).
2015 | IEEE Transactions on Services Computing (TSC).
Total 7 reviews.

	External Reviewer.
2015, 2021	IEEE Symposium on Security and Privacy (S&P).
2015, 2017–2018	Network and Distributed System Security Symposium (NDSS).
2018	USENIX Security Symposium (Security).
2016	ACM Conference on Computer and Communications Security (CCS).
2017	Workshop on Internet of Things Security and Privacy (IoT S&P).
2014, 2016	Annual Computer Security Applications Conference (ACSAC).
2016	IEEE/IFIP International Conference on Dependable Systems and Networks (DSN).
2016	ACM Symposium on Information, Computer and Communications Security (ASIACCS).
2016	International Symposium on Research in Attacks, Intrusions, and Defenses (RAID).
2016	IEEE Conference on Communications and Network Security (CNS).
2016	ACM International Symposium on the Foundations of Software Engineering (FSE).
2016–2017	International Symposium on Software Testing and Analysis (ISSTA).
2014	ACM Cloud Computing Security Workshop (CCSW).
	Total 28 reviews.
	Conference Volunteer.
10/2011	Symposium on Operating Systems Principles (SOSP).
	Check-in desk and scribing for sessions.

Open Source Software

07/2011–08/2012	**vmprobes** [t1, t2]: A virtual machine introspection tool for Xen, now part of Stackdb (code).
03/2011–06/2011	**dbtgpu** [o3]: A solution to accelerate dynamic binary translation for fixed size instructions using CUDA (code).
11/2006–10/2009	**PE Shield** [p6]: A secure process loader for Windows NT (code).
09/2007–12/2007	**G Messenger**: An instant messaging server and client for Linux (code).

Reported Vulnerabilities

10/2016	PX4 Pro Autopilot Bug #5645: NULL pointer dereference in sched_note_switch (link).
10/2016	PX4 Pro Autopilot Bug #5644: NULL pointer dereference in sched_note_stop (link).
10/2016	PX4 Pro Autopilot Bug #5643: Stack overflow possible in mixer_multirotor.cpp (link).
10/2016	NuttX RTOS Bug #84: Buffer overrun possible in NuttShell (~~link~~).

Press Releases

07/2010	10th Anniversary Journal of Chungnam Association of Scholarship Subject: *Follow your curiosity.*