

Kangkook Jee

Princeton NJ, 08540

☎ (+1) 201 390 3931 | ✉ kjee@nec-labs.com | 🏠 <http://kangkookjee.github.io> | 📱 jikk

Research Interests

Experienced researcher with a demonstrated history of working for both industry and research. My skills and research areas span the general system and software security areas also include operating systems, compiler technologies, binary analysis and privacy.

Education

Ph.D. in Computer Science

COLUMBIA UNIVERSITY

New York, USA

Jan 2008 - Aug 2014

- Ph.D. Thesis: "On Efficiency and Accuracy of Data Flow Tracking Systems"
- Academic Advisor: Angelos D. Keromytis

M.Phil. in Computer Science

COLUMBIA UNIVERSITY

New York, USA

Jun 2012

M.Sc. in Computer Science

COLUMBIA UNIVERSITY

New York, USA

Dec 2007

B.S. in Mathematics & Computer Science

KOREA UNIVERSITY

Seoul, South Korea

Mar 2000

Work Experiences

NEC Laboratories America

RESEARCHER, COMPUTER SECURITY DEPARTMENT

Princeton, NJ

Sep 2014 - Present

- Designed and implemented end-point security solutions for enterprise computers, IoT devices, Automobiles, and ICS devices. The solutions collect and process large-scale system event stream to support ML-based anomaly detection and forensic analysis.
- In charge of assessing mitigating security risk. Designed and implemented attack scenarios.
- Worked on various system security projects that include building security profile for each program based on its DNS queries, protecting machine learning logics using hardware primitives (e.g., Intel SGX, ARM TrustZone), and so forth.

NOTABLE PROJECT EXPERIENCES AND ACHIEVEMENTS

Jan 2004 - Dec 2004

- Autonomic Security Intelligence (ASI): Designed and implemented data collection component implementation for Linux, OSX. Evaluated and assessed enterprise security risks. Designed several attack scenarios.
- End-host Protection for ICS infrastructure: **Project lead**, designed and proposed security and safety solutions to major ICS vendors.
- End-point Detection and Response Solution for IoT devices: **Project lead**. Designed and proposed end-point security solution for IoT devices. Currently, leading and collaborating business units to deliver product release candidate.
- Secure GateWay for Automotive: Assessed security risks for connected cars. Designed and developed attack scenarios.

IBM Korea

ADVANCED SOFTWARE ENGINEER

Seoul, South Korea

Jul. 2004 - Aug. 2006.

- Advanced technical resource to handle critical projects or customer issues. Covered various IBM technologies; AIX operating system, IBM Java Virtual Machine (JVM), and high availability solutions.
- **Technical lead** for KEB (Korean Exchange Bank) downsizing project: The world's first reference case that downgraded the core banking system of major bank from mainframe to Unix system (IBM AIX).

SOFTWARE SPECIALIST

Mar. 2001 - Jul. 2004

- System engineer AIX operating systems and IBM's high availability solutions.

18 Medical Company, 8th U.S. Army

INFORMATION MANAGEMENT STAFF

Seoul, South Korea

Jan 1997 - Mar 1999

- IT infrastructure administrator for 121 general hospital Yongsan U.S. army garrison, South Korea.

Talks

CONFERENCE TALKS

Nov 2013	“ShadowReplica: Efficient Parallelization of Dynamic Data Flow Tracking”	ACM CCS, Berlin, Germany
Feb 2012	“A General Approach for Efficiently Accelerating Software-based Dynamic Data Flow Tracking on Commodity Hardware”	NDSS, San Diego, USA
Dec 2010	“An Adversarial Evaluation of Network Signaling and Control Mechanisms”	ICISC, Seoul, South Korea

INVITED TALKS

Oct 2013	“ShadowReplica: Efficient Parallelization of Dynamic Data Flow Tracking”	Security Group Seminar, Stevens Institute of Technology
Jun 2012	“A General Approach for Efficiently Accelerating Software-based Dynamic Data Flow Tracking on Commodity Hardware”	IBM PL Day, IBM T. J. Watson Research Center
Mar 2011	“A General Approach for Efficiently Accelerating Software-based Dynamic Data Flow Tracking on Commodity Hardware”	Liberty Group Seminar, Princeton University

Skills

Programming	C/C++, Python, Go, Assembly, SQL, Javascript
Technologies	LLVM, Intel PIN, Metasploit, Cuckoo
Languages	Korean (<i>Native</i>) English (<i>Proficient</i>) Japanese (<i>Elementary proficiency</i>)

Honors & Awards

2016	CEATEC Award, Innovation for better society , CEATEC Japan CPS/IoT Exhibition	Tokyo, Japan
2008-2014	Fellowship , Graduate Research Assistantship (GRA), Columbia University	New York, USA
2003-2005	IBM top-talented group (resource pool for future executives) , IBM Korea	Seoul, South Korea
2005	Employee education program with full tuition support , IBM Korea	Seoul, South Korea
2004	IBM Stock option (500 stocks) , IBM Korea	Seoul, South Korea
2000	Army Commendation Medal , 8th U.S. Army	Seoul, South Korea

Service

TECHNICAL PROGRAM COMMITTEE MEMBER

ISC 2016 International Conference on Information Security Conference

EXTERNAL REVIEWER

CCS	ACM Conference on Computer and Communications Security: 2012, 2013, 2014
NDSS	International Workshop on Security: 2015
INFOCOM	IEEE International Conference on Computer Communications: 2015
RAID	International Symposium on Research in Attacks, Intrusions and Defenses: 2014, 2015
ACNS	Applied Cryptography and Network Security: 2015
CSET	USENIX Workshop on Cyber Security Experimentation and Test: 2011
CANS	International Conference on Cryptology And Network Security: 2011
ICS	International Conference on Information Security Conference: 2011
IWSEC	International Workshop on Security: 2013

Teaching

Introduction to Programming (COMSW3101-003)

COLUMBIA UNIVERSITY

New York, USA

Fall 2013

- Designed and taught a course that teaches Programming with Python (Students: 14, Course evaluation: 4.45 / 5.0)

Teaching Assistant

COLUMBIA UNIVERSITY

New York, USA

2010-2012

- Spring 2012: Teaching Assistant (TA) for Artificial Intelligence (COMSW4701)
- Fall 2010: Teaching Assistant (TA) for Introduction to Programming (COMS3157)

Student Advising

Intern Advising

NEC LABS AMERICA

- Summer 2015: Yasser Shalabi (Ph.d candidate at UIUC).
Project: Fast and efficient system event collection from Linux kernel.
- Summer 2016: Yixin Sun (Ph.d candidate at Princeton University).
Project: Analyzing Program DNS Behavior under Malware Injection.
- Summer 2017: Suphanee Sivakorn (Ph.d candidate at Columbia University).
Project: System to Detect Malicious Processes with End-point DNS Monitoring.
- Summer 2018: Qi Wang (Ph.d candidate at UIUC).
Project: End-point Detection and Response for IoT Devices.

Student Mentoring

COLUMBIA UNIVERSITY

- Fall 2012: Mengqi Zhang (MS student Columbia University, currently software engineer at Facebook)
Project: Compiler (LLVM) assisted program instrumentation and hardening
- Spring 2013: Daniel Song (MS student at Columbia University, currently Ph.d candidate at Columbia University)
Project: Comparison study of Dynamic Binary Instrumentation (DBI) frameworks
- Fall 2013: Marios Pomonis, Theofilos Petsios (Ph.d candidates at Columbia University)
Project: Arithmetic error detection using information flow tracking with compiler assisted program instrumentation.

Publications

CONFERENCE PUBLICATIONS

- C1 Y. Tang, D. Li, Z. Li, M. Zhang, **K. Jee**, Z. Wu, J. Rhee, X. Xiao, F. Xu, Q. Li “NodeMerge: Template Based Efficient Data Reduction For Big-Data Causality Analysis”. In Proceedings of the 25th ACM Conference on Computer and Communications Security (CCS), Toronto, Canada, November 2018.
- C2 P. Gao, X. Xiao, D. Li, Z. Li, **K. Jee**, Z. Wu, C. Kim, S. R. Kulkarni, P. Mittal “SAQL: A Stream-based Query System for Real-Time Abnormal System Behavior Detection”. in Proceedings of the USENIX Security Symposium, August 2018, Baltimore, MD, August 2018.
- C3 P. Gao, X. Xiao, Z. Li, **K. Jee**, F. Xu, S. R. Kulkarni, P. Mittal “AIQL: Enabling Efficient Attack Investigation from System Monitoring Data”. In Proceedings of Usenix Annual Technical Conference (ATC), Boston, MA, June 2018.
- C4 Y. Liu, M. Zhang, D. Li, **K. Jee**, Z. Li, Z. Wu, J. Rhee, P. Mittal “Towards a Timely Causality Analysis for Enterprise Security” In Proceedings of The Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 2018
- C5 Z. Xu, Z. Wu, Z. Li, **K. Jee**, J. Rhee, X. Xiao, F. Xu, H. Wang, G. Jiang “High fidelity data reduction for big data security dependency analyses” In Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS), Vienna, Austria, November 2016.
- C6 M. Pomonis, T. Petsios, **K. Jee**, M. Polychronakis, A. D. Keromytis “IntFlow: improving the accuracy of arithmetic error detection using information flow tracking” In Proceedings of Annual Computer Security Applications Conference (ACSAC), New Orleans, LA, December 2014.
- C7 **K. Jee**, V. P. Kemerlis, A. D. Keromytis and G. Portokalidis “ShadowReplica: Efficient Parallelization of Dynamic Data Flow Tracking” In Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS), Berlin, Germany, November 2018.
- C8 V. P. Kemerlis, G. Portokalidis, **K. Jee**, and A. D. Keromytis “libdft: Practical Dynamic Data Flow Tracking for Commodity System” In Proceedings of 8th Annual International Conference on Virtual Execution Environments (VEE), London, UK, March

2012.

- C9 **K. Jee**, G. Portokalidis, V. P. Kemerlis, S. Ghosh, D. I. August, and A. D. Keromytis “A General Approach for Efficiently Accelerating Software-based Dynamic Data Flow Tracking on Commodity Hardware” In Proceedings of The Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 2012
- C10 **K. Jee**, S. Sidiroglou-Douskos, A. Stavrou, and A. D. Keromytis. “An Adversarial Evaluation of Network Signaling and Control Mechanisms” In Proceedings of the 13th International Conference on Information Security and Cryptology (ICISC), Seoul, South Korea, December 2010.
- C11 Y. Sun, **K. Jee**, S. Sivakorn, Z. Li, C. Lumezanu, Z. Wu, L. Kort-Parn, J. Rhee, C. Kim, M. Chiang, P. Mittal “You are What You Query: Program DNS Behavior under Malware Injection” *Under review*
- C12 S. Sivakorn, **K. Jee**, Y. Sun, L. Kort-Parn, Z. Li, Z. Wu, C. Lumezanu, L. Tang, D. Li “PDNS: Countering Malicious Processes with End-point DNS Monitoring” *Under review*
- C13 H. Zhang, L. Tang, J. Gao, Z. Chen, B. Zong, **K. Jee** and Z. Li “On Discovering Advanced Persistent Threats from Enterprise Monitoring Logs” *Under review*
- C14 Y Li, Z Wu, H. Wang, K. Sun, Z. Li, **K. Jee** and J. Rhee “ UTrack: User Tracking in an Enterprise Network Based on OS-Level Audit Logs” *Under review*
- C15 W. U. Hassan, S. Guo, D. Li, Z. Chen, **K. Jee**, Z. Li and A. Bates “NoDoze: Combatting Threat Alert Fatigue with Automated Provenance Triage” *Under review*

Books

- B1 K. Hayashi, **K. Jee**, O. Lascu, H. Pienaar, S. Schreitmueller, T. Tarquinio, J. Thompson “AIX5L Practical performance and tuning guide” published by IBM Press books, ISBN-0738491799 , March 2005

Patents

- P1 High Fidelity Data Reduction for System Dependency Analysis Z Wu, Z Li, J Rhee, F Xu, G Jiang, **K Jee**, X Xiao, Z Xu US Patent App. 15/416,346
- P2 Intrusion Detection Using Efficient System Dependency Analysis Z Wu, Z Li, J Rhee, F Xu, G Jiang, **K Jee**, X Xiao, Z Xu, J Rhee US Patent App. 15/416,462
- P3 Extraction and comparison of hybrid program binary features J Rhee, Z Li, Z Wu, **K Jee**, G Jiang US Patent App. 15/479,928
- P4 Blackbox Program Privilege Flow Analysis with Inferred Program Behavior Context J Rhee, Y Jeon, Z LI, **K Jee**, Z Wu, G Jiang US Patent App. 15/623,538
- P5 Fine-Grained Analysis and Prevention of Invalid Privilege Transitions J Rhee, Y Jeon, Z LI, **K Jee**, Z Wu, G Jiang US Patent App. 15/623,589
- P6 Host level detect mechanism for malicious dns activities **K Jee**, Z LI, G Jiang, L Korts-Parn, Z Wu, Y Sun, J Rhee US Patent App. 15/644,018
- P7 Automated blackbox inference of external origin user behavior Z Wu, J Rhee, Y Jeon, Z Li, **K Jee**, G Jiang US Patent App. 15/652,796
- P8 (Patent pending) Path-based program lineage inference analysis L Korts-Parn, J Rhee, K Jee, Z Li, Z Wu, O Setayeshfar US Patent App. 16/039,993
- P9 (Patent pending) Inter-application dependency analysis for improving computer system threat detection D Li, **K Jee**, Z Li, Z Chen, L Tang US Patent App. 16/006,164
- P10 (Patent pending) Timely causality analysis in homogeneous enterprise hosts J Rhee, **K Jee**, Z Li, D Li, Z Wu, M Zhang US Patent App. 15/972,911
- P11 (Patent pending) Template based data reduction for security related information flow data **K Jee**, Z Wu, M Zhang, D Li, Z Li US Patent App. PCT/US18/32938
- P12 (Patent pending) Inter-application dependency analysis for improving computer system threat detection D Li, **K Jee**, Z Li, Z Chen, L Tang US Patent App. 16/006,164
- P13 (Patent pending) Automated software safeness categorization with installation lineage and hybrid information sources L Korts-Parn, Z Li, **K Jee**, J Rhee, O Setayeshfar, Z Wu US Patent App. PCT/US18/43405
- P14 (Patent pending) Host behavior and network analytics based automotive secure gateway L Korts-Parn, Z Wu, Z Li, **K Jee**, C H Kim, J Rhee, H Li, S Hao US Patent App. 62/660,319

Reference

Dr. Angelos D. Keromytis
Program Manager, DARPA
Arlington, VA
phone: available on request
e-mail: available on request

Professor Salvatore S. Stolfo
Professor Columbia University
New York, NY
phone: available on request
e-mail: available on request

Professor Junfeng Yang
Associate Professor Columbia University
New York, NY
phone: available on request
e-mail: available on request

Dr. Geoff Jiang
Vice President, Technology
Ant Financial
Hangzhou, Zhejiang, China
phone: available on request
e-mail: available on request