Kangkook Jee

4 Independence Way Suite 200, Princeton NJ, 08540

☎ 201 390 3931 | ✉ kjee@nec-labs.com | kangkookjee.github.io | jikk

Research Interests

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

Education

Ph.D. in Computer Science *New York, USA*
Columbia University *2016*

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

M.Phil. in Computer Science *New York, USA*
Columbia University *2012*

M.Sc. in Computer Science *New York, USA*
Columbia University *2007*

B.S. in Mathematics & Computer Science *Seoul, South Korea*
Korea University *Mar 2000*

Work Expierence

NEC Laboratories America *Princeton, NJ*
Researcher, Computer Security Department *Sep 2014 - Present*

- Autonomic Security Intelligence (ASI): Designed and implemented data collection component implementation for Linux, OSX. Evaluated and assessed enterprise security risks. Designed several attack scenarios. Data collection components are written in C/C++ and the backend components are implemented using Java.
- End-host Protection for ICS infrastructure: *Project lead*. designed and proposed security and safety solutions to major ICS vendors. The solution is for Windows system and written in C++/Java languages. The demo cases and penetration scenarios are written using Golang.
- End-point Detection and Response Solution for IoT devices: *Project lead*. Designed and proposed end-point security solution for IoT devices which is written in C++ and Java. Currently, leading a six member team to deliver product release candidate.
- Secure GateWay for Automotive: Assessed security risks for connected cars. Designed and developed attack scenarios using Python.
- 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 a 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.

IBM Korea *Seoul, South Korea*
Advanced software engineer *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 a 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 *Seoul, South Korea*

INFORMATION MANAGEMENT STAFF *Jan 1997 - Mar 1999*

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

Publications

CONFERENCE PUBLICATIONS

C1 S. Sivakorn , **K. Jee**, Y. Sun, L. Kort-Parn, Z. Li, C. Lumezanu, Z. Wu, L. Tang, D. Li *"Countering Malicious Processes with Endpoint DNS Monitoring"*. In Proceedings of The Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 2019

C2 W. U. Hassan, S. Guo, D. Li, Z. Chen, **K. Jee**, Z. Li, A. Bates *"NoDoze: Combatting Threat Alert Fatigue with Automated Provenance Triage"*. In Proceedings of The Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 2019

C3 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.

C4 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.

C5 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.

C6 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

C7 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.

C8 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.

C9 **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.

C10 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.

C11 **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

C12 **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.

UNDER SUBMISSION

C1 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*

C2 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*

C3 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*

C4 J. Gui, D. Li, Z. Li, **K. Jee**, J. Rhee, Z. Wu, Z. Chen, M. Zhang, X. Xiao "APTrace: An Responsive System for Agile Enterprise Level Causality Analysis" *Under review*

C5 S. Wang, Z. Chen, D. Li, X. Yu, J. Gui, L. Tang, **K. Jee**, H. Chen, Z. Li "Detecting Unexpected Programs in Execution Environment of Web Services via Deep Graph Neural Networks" *Under review*

C6 P. Fang, Peng Gao, C. Liu, **K. Jee**, T. Wang, W. Shim, X. Xiao "Reptracker: Towards Automatic Attack Investigation via Weighted Causality Analysis" *Under review*

Books

B1 K. Hayashi, **K. Jee**, O. Lascu, H. Pienaar, S. Schreitmueller, T. Tarquinio, J. Thompson *"AIX 5L Practical performance and tuning guide"* published by IBM Press books, ISBN-0738491799 , March 2005

Patents

Approved Patents

P1 Timely causality analysis in homogeneous enterprise hosts. M Zhang, **K Jee**, Z Li, D Li, Z Wu, J Rhee,. US Patent 15/972,911, issued on Nov 2018.

P2 Template based data reduction for security related information flow data. D Li, **K Jee**, Z Wu, M Zhang, Z Li. US Patent 15/979,512, issued on Nov 2018.

P3 Template based data reduction for commercial data mining. D Li, **K Jee**, Z Wu, M Zhang, Z Li. US Patent 15/979,514, issued on Nov 2018.

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 15/623,538, issued on Feb 2018.

P5 Fine-Grained Analysis and Prevention of Invalid Privilege Transitions. J Rhee, Y Jeon, Z LI, **K Jee**, Z Wu, G Jiang. US Patent 15/623,589, issued on Feb 2018.

P6 Automated blackbox inference of external origin user behavior. Z Wu, J Rhee, Y Jeon, Z Li, **K Jee**, G Jiang. US Patent 15/652,796 , issued on Feb 2018.

P7 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 15/644,018 , issued on Jan 2018.

P8 Extraction and comparison of hybrid program binary features. J Rhee, Z Li, Z Wu, **K Jee**, G Jiang. US Patent 15/479,928, issued on Oct 2017.

P9 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 15/416,346 Issued on Aug 2017

P10 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 15/416,462, issued on Aug 2017

Pending Patents

P1 (Patent pending) Path-based program lineage inference analysis. L Korts-Parn, J Rhee, K Jee, Z Li, Z Wu, O Setayeshfar. US Patent 16/039,993

P2 (Patent pending) Inter-application dependency analysis for improving computer system threat detection. D Li, **K Jee**, Z Li, Z Chen, L Tang. US Patent 16/006,164

P3 (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 PCT/US18/43405

P4 (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 62/660,319

Teaching

Introduction to Programming (COMSW3101-003) *New York, USA*

Columbia University *Fall 2013*

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

Teaching Assistant *New York, USA*

Columbia University *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 Rice 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.

Talks

Conference Presentations

Nov 2018	"NodeMerge: Template Based Efficient Data Reduction For Big-Data Causality Analysis"	*ACM CCS, Toronto, Canada*
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

Dec 2018	"Research Challenges and Opportunities in End-point Detection and Response (EDR)"	*Security & Privacy PIC Seminar Series, IBM Watson Research*
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*

Honors & Awards

2016	**CEATEC Award, Innovation for better society**, CEATEC Japan CPS/IoT Exhibition	*Tokyo, Japan*
2014	**2nd Place CyberSecurity for the Next Generation 2014: Americas Round**, Kaspersky lab	*Washington, DC*
2008-2014	**Graduate 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

Reference

Prof. Angelos D. Keromytis
John H. Weitnauer Jr. Endowed Chair Professor
Georgia Institute of Technology
Atlanta, GA
e-mail: angelos@gatech.edu

Dr. Geoff Jiang
Vice President, GM of Technology
Ant Financial
Hangzhou, Zhejiang, China
e-mail: geoff.jiang@yahoo.com

Prof. Georgios Portokalidis
Assistant Professor
Stevens Institute of Technology
Hoboken, NJ
e-mail: gportoka@stevens.edu

Prof. Salvatore J. Stolfo
Professor
Columbia University
New York, NY
e-mail: sal@cs.columbia.edu

Prof. Michalis Polychronakis
Assistant Professor
Stony Brook University
Stony Brook, NY
e-mail: mikepo@cs.stonybrook.edu