Kangkook Jee

Computer Science Dept.,University of Texas at Dallas
800 West Campbell Road, EC-31 Richardson, TX 75080
kangkook.jee@utdallas.edu | kangkookjee.github.io

Research Interests

My research areas spans the general system and network security areas on the basis of operating system, compiler, binary analysis techniques. I am also interested in and have experiences in security research on different domains that include automotive, and Internet of Thing (IoT), critical infrastructure with ICS and SCADA systems.

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

Univesrity of Texas, at Dallas — *Richardson, TX*
Assistant professor, Computer Science Department — *Aug 2019 - Present*

NEC Laboratories America — *Princeton, NJ*
Researcher, Computer Security Department — *Sep 2014 - Jul 2019*

IBM Korea — *Seoul, South Korea*
Advanced technical support staff — *Mar. 2001 - Aug. 2006*

18 Medical Company, 8th U.S. Army — *Seoul, South Korea*
Information management staff — *Jan 1997 - Mar 1999*

Publications

Conference Publications

C1 J. Gui, D. Li, Z. Chen, J. Rhee, X. Xiao, M. Zhang, **K. Jee**, Z. Li, and H. Chen, *"APTrace: A Responsive System for Agile Enterprise Level Causality Analysis,"* In Proceedings of the IEEE International Conference on Data Engineering (ICDE), Dallas, TX, 2020

C2 Q. Wang, W. U. Hassan, D. Li, **K. Jee**, X. Yu, K. Zou, J. Rhee, Z. Chen, W. Cheng, C. A. Gunter, and H. Chen, *"You Are What You Do: Hunting Stealthy Malware via Data Provenance Analysis,"* In Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA, 2020.

C3 S. Sivakorn , **K. Jee**, Y. Sun, L. Kort-Parn, Z. Li, C. Lumezanu, Z. Wu, L. Tang, D. Li *"Countering Malicious Processes with End-point DNS Monitoring"*. In Proceedings of The Network and Distributed System Security Symposium (NDSS), San Diego, CA,

February 2019

C4 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

C5 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.

C6 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.

C7 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.

C8 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

C9 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.

C10 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.

C11 **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.

C12 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.

C13 **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

C14 **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.

Demo papers

D1 P. Gao, X. Xiao, D. Li, **K. Jee**, H. Chen, S. Kulkarni, and P. Mittal, *"Querying Streaming System Monitoring Data for Enterprise System Anomaly Detection."* Presented at the IEEE International Conference on Data Engineering (ICDE), Dallas TX, May 2020.

D2 P. Gao, X. Xiao, Z. Li, **K. Jee**, F. Xu, S. R. Kulkarni, P. Mittal *"A Query System for Efficiently Investigating Complex Attack Behaviors for Enterprise Security."* Presented at the International Conference on Very Large Data Bases (VLDB), Los Angelos, CA, August 2019.

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

Patents

P1 Blackbox program privilege flow analysis with inferred program behavior context.
J. Rhee, Y. Jeon, L. I. Zhichun, **K. Jee**, Z. Wu, and G. Jiang. US Patent App. 10/505,962 issued on Dec 2019.

P2 User-added-value-based ransomware detection and prevention.
Z. Wu, Y. Li, J. Rhee, **K. Jee**, Z. Li, J. Kamimura, L. Tang, and Z. Chen. US Patent App. 16/379,024 issued on Nov 2019.

P3 Fine-grained analysis and prevention of invalid privilege transitions.
J. Rhee, Y. Jeon, Z. Li, K. Jee, Z. Wu, and G. Jiang. US Patent App. 15/623,589 issued on Sep 2019.

P4 Extraction and comparison of hybrid program binary.
J. Rhee, Z. Li, Z. Wu, **K. Jee**, and G. Jiang. US Patent App. 15/479,928 issued on May 2019.

P5 Host behavior and network analytics based automotive secure gateway.
J Rhee, H Li, Hao Shuai, CH Kim, Z Wu, LI Zhichun, **K Jee**, L Korts-Parn. US Patent App. 16/146,166 issued on Apr 2019.

P6 Inter-application dependency analysis for improving computer system threat detection.
D Li, **K Jee**, Z Chen, LA Tang, LI Zhichun. US Patent App. 16/006,164 issued on Feb 2019.

P7 Path-based program lineage inference analysis.
J Rhee, Z Wu, L Korts-Parn, **K Jee**, LI Zhichun, O Setayeshfar. US Patent App. 16/039,993 issued on Feb 2019.

P8 Automated software safeness categorization with installation lineage and hybrid information sources.
J Rhee, Z Wu, L Korts-Parn, **K Jee**, LI Zhichun, O Setayeshfar. US Patent App. 16/040,086 issued on Feb 2019.

P9 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.

P10 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.

P11 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.

P12 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.

P13 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.

P14 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.

P15 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.

P16 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.

P17 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.

P18 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.

Teaching

Advanced topics in System Security (7301.005) *Dallas, TX*
University of Texas at Dallas *Spring 2020*

Malware and Binary Analysis (cs6301.005) *Dallas, TX*
University of Texas at Dallas *Fall 2019*

Introduction to Programming (COMSW3101-003) *NY, New York*
Columbia University *Fall 2013*

- Designed and taught a course, Programming with Python (Students: 14)

Teaching Assistant *NY, New York*

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.
- Summer 2019: Qi Wang (Ph.D candidate at UIUC).
  Project: SplitBrain: Edge-Cloud Collaborative Security for IoT.

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

Feb 2019	"Countering Malicious Processes with Process-DNS Association"	*NDSS, Sand Diego, USA*
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

Apr 2019	"Finding Flow: Connecting the Dots to Disclose Attacker Trails"	*NSR (National Security Research Institute), Daejon, South Korea*
Apr 2019	"Finding Flow: Connecting the Dots to Disclose Attacker Trails"	*KAIST, Daejon, South Korea*
Apr 2019	"Finding Flow: Connecting the Dots to Disclose Attacker Trails"	*SKKU, Suwon, South Korea*
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

NSF Panel

III-SMALL-IX-ENG Panelist The Information & Intelligent Systems Division (IIS), Mar 2020

Technical Program Committee Member

SiMLA 2020 Security in Machine Learning and its Applications
ISC 2016 International Conference on Information Security Conference