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 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.

Demos

D1 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"*. In Proceedings of 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

Approved Patents

P1 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

P2 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

P3 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

P4 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

P5 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.

P6 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.

P7 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.

P8 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.

P9 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.

P10 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.

P11 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.

P12 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.

P13 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

P14 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

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.
- 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

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

Research Experience

Researcher, NEC Laboratories America, Sep 2014 - Present.

Protection of Machine Learning Algorithm with Hardware Assistance (Mar 2018 - Present): To protect the privacy of ML algorithms, I co-designed the ML platform that runs the algorithm inside Intel SGX and encrypts the channel for GPU communication.

Application White-listing with Binary Triage (Mar 2018 - Present): I proposed and work on a white-listing solution that dynamically updates the reputation of application binary considering new metrics related to the trustworthiness of the binary.

End-point Detection and Response for IoT devices (Sep 2017 - Present): In this project, we develop an EDR solution for IoT devices. To minimize the interference to the operation of IoT device, our approach only remains minimal workload to IoT devices and offload the rest to the cloud to protect IoT deployment with ML-based anomaly detection and support for forensic analysis.

Enterprise security solution for ML detection and forensic support (Sep 2014 - Aug 2017): Autonomous Security intelligence (ASI) is an award-winning security solution that monitors and collects system activities from a large number of end-hosts to support ML-based anomaly detection and forensic analysis. I designed and developed auditing components for different end-hosts (Linux, OS X, IoT platforms). I was mainly in charge of the threat intelligence and the analysis the latest attack trend.

Research Assistant, Columbia University, Sep 2008 - Aug 2014.

IntFlow (Jun 2012 - Jul 2012): IntFlow is a compiler extension which uses static data-flow analysis to report integer errors, taking into account common developer practices to reduce false positives. IntFlow achieves 89% reduction in false positives compared to the Clang-based Integer Overflow Checker (IOC).

ShadowReplica, (Jan 2012 - June 2013): ShadowReplica accelerates DFT and other shadow memory-based analyses, by decoupling analysis from execution and utilizing spare CPU cores to run them in parallel. DFT is run in parallel by a shadow thread that is spawned for each application thread, and the two communicate using a shared data structure. We avoid the problems suffered by previous approaches, by introducing an offline application analysis phase that utilizes both static and dynamic analysis approaches to generate optimized code for decoupling execution and implementing DFT, while it also minimizes the amount of information needed for communication between two threads.

Taint Flow Algebra (TFA), (Jan 2010 - Dec 2011): To improve the efficiency of DFT, our approach separates the program logic from the corresponding tracking logic, extracting the semantics of the latter and abstracting them using an intermediate representation(IR) of Taint Flow Algebra. We then apply optimization techniques to eliminate redundant tracking logic and minimize interference with the target program.

libdft, (Jan 2010 - Dec 2011): Dynamic data flow tracking (DFT) deals with tagging and tracking data of interest as they propagate during program execution. We presented libdft, a dynamic DFT framework that unlike previous work is at once fast, reusable, and works with commodity software and hardware. libdft provides an API for building DFT-enabled tools that work on unmodified binaries, running on common operating systems and hardware, thus facilitating research and rapid prototyping.

Evaluation of control plane mechanisms in propagating security updates, (June 2008 - July 2010) The project measured and evaluated the reliability and performance trade-offs for a variety of control channel mechanisms that are suitable for coordinating large-scale collaborative defenses when under attack. Our results show that the performance and reliability characteristics change drastically when one evaluates the systems under attack by a sophisticated and targeted adversary.