Kyuhong **Park**

GRADUATE RESEARCH ASSISTANT

756 W Peachtree St NW, Atlanta, GA 30308

☎ (+1) 206-445-9661 | ✉ kpark302@gatech.edu | 🏠 https://pb2bee.github.io/ | https://github.com/pb2bee | in
https://www.linkedin.com/in/davidkpark302/

Summary

Interests: **Malware, Programming Analysis, System Security.**

Kyuhong Park is a Ph.D student in computer science at Georgia Tech (2016 Fall) and is working with Professor Wenke Lee and Professor Taesoo Kim. His research focuses on building a robust malware analysis framework using static and dynamic programming analysis to 1) identify and trigger hidden malicious behaviors and 2) build defense mechanisms against malware. He is also interested in operating system security, especially building security and fault-tolerance mechanisms on an embedded and a cyber physical system.

Research Experience

Hybrid (static and dynamic) malware binary rewriting for Penetration testing. *Atlanta, GA*

GEORGIA INSTITUTE OF TECHNOLOGY, GRADUATE RESEARCH ASSISTANT *Dec, 2019 - Current*

- Developing a hybrid binary rewriting framework to build a modified malware in raw binary from real malware.
- With dynamic binary instrumentation tool and programming analysis, collecting binary information from dynamic and static, and mapping the information to correctly modify the malware binary.
- Performing penetration testing or network security evaluation with rewritten malware binary without harming in the given system, but using real malware.

Identifying Behavior Dispatchers for Malware Analysis. *Atlanta, GA*

GEORGIA INSTITUTE OF TECHNOLOGY, GRADUATE RESEARCH ASSISTANT *Aug, 2018 - Dec. 2019*

- Developed an automatic analysis system to identify triggering conditions on malware such as C&C server logic and anti-virus software awareness by leveraging on dispatching patterns.
- Implement detection methods using the two unique pattern identification to assist in behavior exposure with our tailored concolic-execution engine for malware and dispatcher clone detection.
- Applied our tool to analyze 3,943 real-world malware samples.

A collaborative malware analysis and experimentation framework. *Atlanta, GA*

GEORGIA INSTITUTE OF TECHNOLOGY, GRADUATE RESEARCH ASSISTANT *Aug, 2016 - Aug. 2018*

- Developed automatic reconstruction of reproducible environment of malware such as C&C server logic.
- Implement neutralizing targeted malicious behavior of the malware through static and dynamic analysis, and autonomous and active containment of the network stack that isolates the environment.
- Built a fully shareable architecture; analysts can share not only the data such as pcap and traces, but also sharing running environment.
- Collaboration with Lockheed Martin Security Research.

Attack Tolerance in Hard Real-Time systems. *Atlanta, GA*

GEORGIA INSTITUTE OF TECHNOLOGY, GRADUATE RESEARCH ASSISTANT *May. 2015 - Aug. 2016*

- Designed the foundations, principles, and techniques for building attack tolerance on mission-critical cyber physical systems, such as UAV and drone vehicle.
- Developed software and system diversification techniques for operational system and subsystems to ensure that an attack is detected early and the system is resilient against cyber attacks.
- Implement efficient and robust detection and tolerance features under the constraints of a real-time system.

Publication

DeepReflect: Discovering Malicious Functionality through Binary Reconstruction *San Francisco, CA*

USENIX SECURITY SYMPOSIUM (USENIX 2021) *August. 2021*

- DeepReflect, tool for localizing and identifying malware components within a malicious binary. We use an unsupervised deep neural network in a novel way, and classify the components through a semi-supervised cluster analysis, where analysts incrementally provide labels during their daily work flow. The tool is practical since it requires no data labeling to train the localization model, and minimal/noninvasive labeling to train the classifier incrementally.
- Evan Downing, Kyuhong Park, Yisroel Mirsky and Wenke Lee

BDHunter: Identifying Behavior Dispatchers for Malware Analysis *Hong kong, China*

ACM ASIA CONFERENCE ON COMPUTER AND COMMUNICATION SECURITY (ASIACCS 2021) *June. 2021*

- BDHunter is a system that identifies dispatchers in order to discover hidden malicious behaviors. The system takes advantage of the observation that a dispatcher compares one input with a set of different discrete values in order to find the best routine to achieve malicious actions. We also demonstrate the utility of BDHunter's results by revealing hidden malicious behaviors through concolic-execution engine.
- Kyuhong Park, Burak Sahin, Yongheng Chen, Jisheng Zhao, Evan Downing, Hong Hu and Wenke Lee

Augmenting Cyber Assessment through Dynamic Malware Analysis

Orlando, FL

I/ITSEC 2019 *Dec. 2019*

- This paper describe an approach on how dynamic malware analysis capability can help design a system with better cyber resiliency against existing and emerging advanced persistent threats (APT). With understanding the capability, we build a simulation enviroment to thoroughtly test and evalutate its "what-if" cyber defensive postures relative to threats that have not been launched in the real world
- Ambrose Kam, Charles Johnson-Bey, Michael Nance, Wenke Lee, Kyuhong Park and Carter Yagemann

Teaching Experience

CS 8803 - System and Network Defenses, Georgia Institute of Technology

Atlanta, GA

Graduate Teaching Assistant *Spring. 2020 - Current*

- Performing analysis malware with dynamic binary instrumentation tools and programming analysis tools by guiding methods. Exposing behaviors as much as possible and observing them to build defense mechanism to catch the malware.

CS 6262 - Network Security, Georgia Institute of Technology

Atlanta, GA

Graduate Teaching Assistant *Fall. 2016 - Current*

- In-depth analysis of real malware with programming analysis. Implementing triggering logic in a fake C2 server and interacting the server with malware to expose hidden behaviors.

CS 3210 - Design Operating Systems, Georgia Institute of Technology

Atlanta, GA

Graduate Teaching Assistant *Spring. 2016*

- Operating systems concepts, including multi-threading, scheduling, synchronization, communication, and access control.

Work Experience

Computer Emergency Response Team, R.O.K Army Headquaters.

Seoul, S.Korea

Security Expert *Nov. 2007 - Sep. 2009*

- Lead malware analyst, targeting virus, worm and botnet.
- Develop distributed AV system in Army system.

Education

Georgia Institute of Technology

Atlanta, GA

Ph.D. in Computer Science, School of Computer Science *Aug. 2016 - Current*

- Advisors: Prof. Wenke Lee and Prof. Taesoo Kim.
- Specialty: Information Security

Georgia Institute of Technology

Atlanta, GA

M.S. in Computer Science, School of Computer Science *May. 2015 - Aug. 2018*

- Specialty: Computing Systems and Information Security.

Georgia Institute of Technology

Atlanta, GA

B.S. in Computer Science, School of Computer Science *Jan. 2012 - Dec. 2014*

- Specialty: Computing Systems and Network.

Honors & Awards

2012	**Highest Honor**, Georgia Institute of Technology	*Atlanta, GA*
2008	**2nd Award**, Military Hacking & Defense Competition Final	*Seoul, South Korea*

Writing

CyBoK - MMALWARE KNOWLEDGE AREA

www.cybog.org

Writer *Jan. 2019 - PRESENT*

- In-depth understanding of Malware and Attack Technologies.

Programming Languages

Advanced	C, Python
Knowledgeable	C++, ruby, C#