Kyuhong **Park**

Security Researcher · Malware Analyst

756 W Peachtree St NW, Atlanta, GA 30308

https://www.linkedin.com/in/davidkpark302/

Summary

Interests: **Malware analysis, System Security.**

Current graduate research assistant in the Institute for Information Security& Privacy (IISP) at Georgia Tech. 5+ years experience specializing in automatic malware analysis framework development and malware reverse engineering using static and dynamic analysis to 1) identify and trigger hidden malicious behaviors and 2) build defense mechanisms against malware.

Work Experience

Hybrid malware binary rewriting framework for Penetration testing

Atlanta, GA

Georgia Institute of Technology — *Dec, 2019 - Current*

- As a project lead, collaborating with Cisco Research Team to develop a hybrid binary rewriting framework to generate rewritten x86 and x86-64 malware that semi-automatically exposes hidden malicious behaviors from real malware.
- Performing penetration testing at system and network security evaluation with rewritten malware binary.
- Providing safety environment on top of Emulation-base malware sandbox(Qiling) and DynamoRIO inside a virtual machine while performing penetration. By hijacking and monitoring write-related API calls through the safety environment, pentesting can be conducted without harming the given system.
- On top of DynamoRIO, IDA Pro, and BinaryNinja, collecting binary information, mapping the information to hidden malicious behaviors, and correctly modify the malware binary to trigger them for penetration testing purpose.

Identifying Behavior Dispatchers for Malware Analysis

Atlanta, GA

Georgia Institute of Technology — *Aug, 2018 - Dec. 2019*

- As a project lead, developed automatic detection platform to identify triggering conditions on PE and ELF malware such as C&C logics and Anti-virus software awareness by leveraging on dispatching pattern.
- Utilizing DynamoRIO, IDA Pro, and BinaryNinja, developed bridges using the pattern identification to assist in malicious behavior exposure with dynamic analysis engine for malware and malware triage.
- Applied 3,943 real-world malware samples on the tool to evaluate effectiveness of identifying the pattern, and reverse engineered them to verify the findings.

A collaborative malware analysis and experimentation framework

Atlanta, GA

Georgia Institute of Technology — *Aug, 2016 - Aug. 2018*

- As a project lead, worked with Lockheed Martin Security Research Team to develop automatic reconstructable and reproducible malware analysis environment using Vagrant, VM and Git.
- Implemented neutralizing targeted malicious behaviors in active containment of the network stack that isolates the environment.
- Built a detection mechanism of XOR-based cryptographic algorithms and obfuscated codes.

Attack Tolerance in Hard Real-Time systems

Atlanta, GA

Georgia Institute of Technology — *May. 2015 - Aug. 2016*

- Designed the foundations, principles, and techniques for building attack tolerant 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.
- Implemented efficient and robust detection and tolerance features under the constraints of real-time linux system.

Skills

DevOps	AWS, Docker, Vagrant
Disassembler and Debugger	BinaryNinja, IDA Pro, Ghidra, x64dbg, WinDBG, GDB
Programming	Python, C, C++, LaTeX

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.

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.

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

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.

Extracurricular Activity

CyBoK - MALWARE KNOWLEDGE AREA

www.cybog.org

Writer *Jan. 2019 - PRESENT*

- In-depth understanding of Malware and Attack Technologies.