HYUNGJOON KOO

kevin.koo@skku.edu • https://dandylife.net/blog

Assistant Professor, Sungkyunkwan University, *Department of Computer Science and Engineering, College of Computing and Informatics* Feb 2021 – Present

EDUCATION

Postdoc., Georgia Tech, *School of Computer Science, College of Computing* Jun 2019 – Dec 2020
- Adviser: Taesoo Kim (Systems Software & Security Lab)
- Research Area: Software Security, Artificial Intelligence for Security

Ph.D., Stony Brook University, *Department of Computer Science* Aug 2013 – May 2019
- Adviser: Michalis Polychronakis (Hexlab)
- Research Area: Binary Protection, Software Diversification against Code Reuse Attacks
- Thesis: Practical Software Specialization against Code Reuse Attacks

M.Sc., Korea University, *Information Management and Security* Mar 2008 – Feb 2010
- Adviser: Sangjin Lee (Digital Forensic Lab)
- Thesis: Pre-detection Model for Trusted Insider's Leaks and Manipulation from a Forensic Perspective

B.Sc., Hanyang University, *Industrial Engineering* Mar 1998 – Aug 2005
- Graduated with College Honors Cum Laude

PUBLICATIONS

- IoTivity Packet Parser for Encrypted Messages in Internet of Things Hyeonah Jung, **Hyungjoon Koo**, and Jaehoon (Paul) Jeong. *In the 24th International Conference on Advanced Communications Technology (ICACT '22)*
- A Look Back on a Function Identification Problem **Hyungjoon Koo**, Soyeon Park, and Taesoo Kim. *In the 37th Annual Computer Security Applications Conference (ACSAC '21)*
- Software Watermarking via a Binary Function Relocation Honggoo Kang, Yonghwi Kwon, Sangjin Lee and **Hyungjoon Koo**. *In the 37th Annual Computer Security Applications Conference (ACSAC '21)*
- Slimium: Debloating the Chromium Browser with Feature Subsetting, Chenxiong Qian, **Hyungjoon Koo**, Changseok Oh, Taesoo Kim, and Wenke Lee. *In the 27th ACM Conference on Computer and Communications Security (CCS '20)*
- Configuration-Driven Software Debloating, **Hyungjoon Koo**, Seyedhamed Ghavamnia, and Michalis Polychronakis. *In the 12th European Workshop on Systems Security (EuroSec)*, 2019
- Compiler-assisted Code Randomization, **Hyungjoon Koo**, Yaohui Chen, Long Lu, Vasileios P. Kemerlis, and Michalis Polychronakis. *In the 39th IEEE Symposium on Security & Privacy (S&P)*, 2018
  Top 10 Finalist, Cyber Security Awareness Week (CSAW), 2018
- Defeating Zombie Gadgets by Re-randomizing Code Upon Disclosure, Micah Morton, **Hyungjoon Koo**, Forrest Li, Kevin Z. Snow, Michalis Polychronakis, and Fabian Monrose. *In the 9th International Symposium on Engineering Secure Software and Systems (ESSoS)*, 2017
- The Politics of Routing: Investigating the Relationship between AS Connectivity and Internet Freedom, Rachee Singh, **Hyungjoon Koo**, Najmehalsadat Miramirkhani, Fahimeh Mirhaj, Leman Akoglu, and Phillipa Gill. *In the 6th USENIX Workshop on Free and Open Communications on the Internet (FOCI)*, 2016
- Return to the Zombie Gadgets: Undermining Destructive Code Reads via Code-Inference Attacks, Kevin Z. Snow, Roman Rogowski, Jan Werner, **Hyungjoon Koo**, Fabian Monrose, and Michalis Polychronakis. *In the 37th IEEE Symposium on Security & Privacy (S&P)*, 2016
- Juggling the Gadgets: Binary-level Code Randomization using Instruction Displacement, **Hyungjoon Koo** and Michalis Polychronakis. *In the 11th ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2016
- Identifying Traffic Differentiation in Mobile Networks, Arash Molavi Kakhki, Abbas Razaghpanah, Anke Li, **Hyungjoon Koo**, Rajeshkumar Golani, David Choffnes, Phillipa Gill, and Alan Mislove. *In the 15th ACM Internet Measurement Conference (IMC)*, 2015

WORK EXPERIENCE

Research Assistant, *Stony Brook University* May 2014 – May 2019
- System / Software Security (Michalis Polychronakis)
- Traffic Differentiation / Internet Censorship (Philipa Gill)

Intern, *Fujitsu Laboratories of America* Jun 2018 – Aug 2018

- Fuzzing and concolic execution

Teaching Assistant, *Stony Brook University* Aug 2013 – Dec 2017

- [CSE102] Introduction to Web Design and Programming (Ahmad Esmaili), Fall 2013
- [CSE130] Introduction to Programming in C (Ahmad Esmaili), Fall 2013
- [CSE312] Legal, Social, and Ethical Issues in Information Systems (Robert Johnson), Spring 2014
- [CSE408] Network Security (Robert Johnson), Spring 2014
- [CSE508] Network Security for Graduates (Michalis Polychronakis), Fall 2017

Intern, *Fujitsu Laboratories of America* Jun 2016 – Aug 2016

- Automated binary hardening

Lecturer Mar 2013 – Jul 2013

- Security Essentials, Korea Productivity Center, July 2013
- Network Security for Rwanda government officials, KISA, Mar 2013

Security Researcher, *Shinhan Bank* Jul 2011 – Sep 2012

- Review, deployment, and operation on Advanced Persistent Threat (a.k.a APT) products
- Discovery and analysis on new breed of on-the-fly cyber attacks over company network
- Cryptographic module maintenance for critical customers' information
- Up-to-date anti-virus engine deployment to protect 24/7 ATM banking
- Security review for brand-new banking services to comply related regulations

Assistant Manager, *Samsung SDS* Jan 2006 – Jul 2011

- Policy establishment and deployment to decrease botnet activities over company network
- Leading the project to design Security History Information Management System for web apps
- Penetration testing on Sri-Lanka's Government Network project
- Incident response against web/network based attacks
- Review security COTS products including web app firewall and source code analysis solution.
- Performing in-house IT audits

PROFESSIONAL ACTIVITIES

Invited Talks

- Software Protection via Code Randomization, University of Tennessee (Nov. 2020)
- Practical Software Specialization against Code Reuse Attacks, Sungkyunkwan University and KAIST (Feb. 2019)
- Practical Software Hardening against Code Reuse Attacks, Georgia Tech (Nov. 2018)
- Software Hardening with Code Diversification, CS Colloquium at SUNY Korea (Jun. 2018), Korea University and Samsung Research (May 2018)
- Software Hardening, Cyber Symposium by the Stony Brook Computing Society (Apr. 2018)
- Elaborate Attacks with Existing Tools, National Computing & Information Agency (May 2013)
- Anonymizing Yourself with Tor, Korea Internet & Security Agency (Apr. 2013)

Committee / (External) Review Services

- IEEE Security & Privacy Magazine (S&P, 2019-21)
- NYU's CSAW '21 Program Committee (2021)
- NYU's CSAW '20 Program Committee (2020)
- Frontiers of Information Technology & Electronic Engineering (FITEE, 2020)
- International Journal of Information Security (IJIS, 2020)
- The Network and Distributed System Security Symposium (NDSS, 2020)
- NYU's CSAW '19 Program Committee (2019)
- IEEE Access (2019)
- IEEE/ACM Transactions on Networking (TON, 2019)

Translation of Technical Books/Articles into Korean

- Gray Hat C# (ISBN: 1593277598, 2018)
- Logging and Log Management (ISBN: 1597496359, 2014)
- Practical Malware Analysis (ISBN: 1593272901, 2013)
- Malware Analyst's Cookbook and DVD (ISBN: 0470613033, 2011)
- Cryptography Engineering (ISBN: 0470474246, 2010)
- OWASP Top10, SANS Top20 and ISM Top10 (2007, 2010)

Grant/Participation

- International Symposium on Research in Attacks, Intrusions, and Defenses in Crete (Sep 2018)
- ACM Asia Conference on Computer & Communications Security in Incheon (Jun 2018)
- NSF Cybersecurity TTP Workshop in New York (Apr 2018)
- Student Grant for the 26th USENIX Security Symposium in Vancouver (Aug 2017)

Poster Presentation

- CSAW ’18 North America Applied Research Competition (Nov 2018)
- Young Faculty Award Meeting, DARPA Conference Center (Jul 2018)

Write-ups

- Keychain Analysis for Mac OS X, Kyeongsik Lee and **Hyungjoon Koo** (2013)
- Hunting OS X Rootkit in Memory, Kyeongsik Lee, Jinkook Kim, and **Hyungjoon Koo** (2013)
- A Guidebook for Building and Operating CERT by KISA (2007)

CERTIFICATIONS

- EnCE (EnCase® Certified Examiner), Guidance Software (2010)
- CHFI (Computer Hacking Forensic Investigator), EC-Council (2010)
- RHCT (Red Hat Certified Technician), RedHat (2009)
- CC (Common Criteria Evaluation), NCSC (2009)
- GCIH (Certified Incident Handler), GIAC (2008)
- CISA (Certified Information Systems Auditor), ISACA (2008)
- CISSP (Certified Information Systems Security Professional), (ISC)2 (2008)
- SIS (Specialist for Information Security), KISA (2007)
- CCNA (Cisco Certified Network Associate), Cisco (2006)

SKILLS Python, C/C++, Binary Analysis (IDA, radare), Reversing, Shell Programming, R, LaTeX