HYUNGJOON KOO

kevin.koo@skku.edu • https://kevinkoo001.github.io

Associate Professor, Sungkyunkwan University, *Department of Computer Science and Engineering, College of Computing and Informatics* Sep 2024 – Present

Assistant Professor, Sungkyunkwan University, *Department of Computer Science and Engineering, College of Computing and Informatics* Feb 2021 – Aug 2024

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

CONFERENCES

Note that [*] represents either the first author or the (co-) corresponding author.
- Evaluating the Effectiveness and Robustness of Visual Similarity-based Phishing Detection Models (To appear), Fujiao Ji, Kiho Lee, **Hyungjoon Koo**, Wenhao You, Euijin Choo, Hyoungshick Kim, and Doowon Kim, *International Symposium on Foundations and Practice of Security (FPS 2024)*, 2025
- An Empirical Study of Black-box based Membership Inference Attacks on a Real-World Dataset, Yujeong Kwon, Simon S. Woo, and **Hyungjoon Koo**, *International Symposium on Foundations and Practice of Security (FPS 2024)*, 2024 [*]
- R2I: A Relative Readability Metric for Decompiled Code, Haeun Eom, Dohee Kim, Sori Lim, **Hyungjoon Koo**, and Sungjae Hwang, *In the ACM International Conference on the Foundations of Software Engineering (FSE '24)*, 2024 [*]
- BinAdapter: Leveraging Continual Learning for Inferring Function Symbol Names in a Binary (To appear), Nozima Murodova and **Hyungjoon Koo**, *In Proceedings of the 19th ACM ASIA Conference on Computer and Communications Security (ASIACCS '24)*, 2024 [*]
- BENZENE: A Practical Root Cause Analysis System with an Under-Constrained State Mutation, Younggi Park, Hwiwon Lee, Jinho Jung, **Hyungjoon Koo**, and Huy Kang Kim, *In the 45th IEEE Symposium on Security & Privacy (S&P '24)*, 2024 (*Distinguished Paper Award*) [*]
- A Transformer-based Function Symbol Name Inference Model from an Assembly Language for Binary Reversing, Hyunjin Kim, Jinyeong Bak, Kyunghyun Cho, and **Hyungjoon Koo**, *In the 18th ACM Asia Conference on Computer and Communications Security (ASIACCS '23)*, 2023 [*]
- SmartMark: Software Watermarking Scheme for Smart Contracts, Taeyoung Kim, Yunhee Jang, Chanjong Lee, **Hyungjoon Koo**, and Hyoungshick Kim, *In the 45th IEEE/ACM International Conference on Software Engineering (ICSE '23)*, 2023 [*]
- Practical Binary Code Similarity Detection with BERT-based Transferable Similarity Learning, Sunwoo Ahn, Seonggwan Ahn, **Hyungjoon Koo**, and Yunheung Paek, *In the 38th Annual Computer Security Applications Conference (ACSAC '22)*, 2022 [*]
- DeView: Confining Progressive Web Applications by Debloating Web APIs, ChangSeok Oh, Sangho Lee, Chenxiong Qian, **Hyungjoon Koo**, and Wenke Lee, *In the 38th Annual Computer Security Applications Conference (ACSAC '22)*, 2022 [*]
- 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)*, 2022 [*]
- 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)*, 2021 [*]

- 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)*, 2021 [*]
- 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)*, 2020
- 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 '18)*, 2018
  Top 10 Finalist, Cyber Security Awareness Week (CSAW '18), 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 '17)*, 2017
- 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 '16)*, 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 '16)*, 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 '15)*, 2015

JOURNALS

Note that [*] represents either the first author or the (co-)corresponding author.

- ToolPhet: Inference of Compiler Provenance from Stripped Binaries with Emerging Compilation Toolchains, Nozima Murodova Hohyeon Jang, and **Hyungjoon Koo**, *IEEE Access, vol. 11, pp. 12667 - 12682, doi: 10.1109/ACCESS.2024.3355098*, 2024 [*]
- Demystifying the Regional Phishing Landscape in South Korea, Hyunjun Park, Kyungchan Lim, Doowon Kim, Donghyun Yu, and **Hyungjoon Koo**, *IEEE Access, vol. 11, pp. 130131 - 130143, doi: 10.1109/ACCESS.2023.3333883*, 2023 [*]
- Binary Code Representation with Well-balanced Instruction Normalization, **Hyungjoon Koo**, Soyeon Park, Daejin Choi, and Taesoo Kim, *IEEE Access, vol. 11, pp. 29183 - 29198, doi: 10.1109/ACCESS.2023.3259481*, 2023 [*]

WORKSHOPS, POSTERS

- Evaluating Password Composition Policy and Password Meters of Popular Websites, Kyungchan Lim, Joshua Hankyul Kang, Matthew Dixson, **Hyungjoon Koo**, and Doowon Kim, Workshop on Designing Security for the Web (SecWeb '23; Co-located with S&P '23), 2023
- Inference of Compiler Provenance from Malware, Hohyun Jang and **Hyungjoon Koo**, Poster in the the 22nd World Conference on Information Security Applications (WISA '21), 2021 [*]
- Semantic-aware Binary Code Representation with BERT, **Hyungjoon Koo**, Soyeon Park, Daejin Choi and Taesoo Kim (ArXiv), 2021 [*]
- Configuration-Driven Software Debloating, **Hyungjoon Koo**, Seyedhamed Ghavamnia, and Michalis Polychronakis. *In the 12th European Workshop on Systems Security (EuroSec '19; Co-located with EuroSys '19)*, 2019 [*]
- 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 '16)*, 2016

WORK EXPERIENCES

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

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 (Undergraduate level; Robert Johnson), Spring 2014

- [CSE508] Network Security (Graduate level; Michalis Polychronakis), Fall 2017

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

Lecturer Mar 2013 – Jul 2013

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

Security Researcher at Security Compliance Team, *Shinhan Bank* Jul 2011 – Sep 2012

Assistant Manager at Information Security Team, *Samsung SDS* Jan 2006 – Jul 2011

PROFESSIONAL ACTIVITIES

Committee Services

- Co-chair for the Security & Privacy Domain in International Conference on Parallel and Distributed Systems (ICPADS 2024)
- Program Committee in IEEE Symposium on Security and Privacy (S&P, 2024)
- Organizing Committee in IEEE Secure Development Conference (SecDev, 2023-24)
- Program Committee in Annual Computer Security Applications Conference (ACSAC, 2023-24)
- Program Committee in International Symposium on Foundations & Practice of Security (FPS, 2022-23)
- Program Committee in NYU's CSAW (2019-2023)

Journal Services as a Reviewer or an Editor

- Editor, Journal of Information Processing Systems (JIPS, 2024)
- Neurocomputing (2024)
- Information and Software Technology (IST, 2024)
- IEEE Transactions on Dependable and Secure Computing (TDSC, 2022)
- Computers and Security (COSE, 2023, 2021)
- IEEE Internet Computing (IC, 2022)
- International Journal of Information Security (IJIS, 2020-21)
- IEEE Security & Privacy Magazine (S&P, 2019-21, 2024)
- Frontiers of Information Technology & Electronic Engineering (FITEE, 2020, 2024)
- International Journal of Information Security (IJIS, 2020)
- IEEE Access (2019)
- IEEE/ACM Transactions on Networking (TON, 2019)

Patents

- Relative readability index for Decompiled Codes, **Hyungjoon Koo**, Sungjae Hwang, Haeun Eom, Dohee Kim, Sori Lim, (KR) App No. 10-2024-0105125
- Methods and apparatus for inferring function symbols from assembly code in transformer-based executable binary, and recording medium, **Hyungjoon Koo**, Hyunjin Kim, and Jinyeong Bak, (KR) App No. 10-2023-0067351; (US) App No. 18-674-646
- Watermarking method for smart contract, Hyoungshick Kim, Taeyoung Kim, Yunhee Jang, Chanjong Lee, and **Hyungjoon Koo**, (KR) App No. 10-2022-0116335, (US) App No. 18-368-734
- Apparatus and method for detecting similarity of binary code, Sunwoo Ahn, Seonggwan Ahn, **Hyungjoon Koo**, and Yunheung Paek, (KR) App No. 10-2023-0035069; (US) App No. 18-596-194
- Method and device of embedding watermark in software, **Hyungjoon Koo**, Sangjin Lee, and Honggu Kang, (KR) App No. 10-2021-0170916; (US) App No. 18-073-876
- Method of detecting intrusion for infotainment systems and apparatus thereof, **Hyungjoon Koo**, (KR) Patent No. 10-2022-0005421
- System and method for responding DDoS offensive, Changryul Huh, Bonjae Koo, Bonghui Park, **Hyungjoon Koo**, Kyutae Jeong, (KR) Patent No. 10-2010-0065260

Awards/Grants

- Distinguished Paper Award (Title; BENZENE: A Practical Root Cause Analysis System with an Under-Constrained State Mutation) at IEEE Symposium on Security and Privacy 2024 (May 2024)
- Best Paper Award (Title; RoBERTa-based Obfuscated Binary Code Similarity Detection) at Conference on Information Security and Cryptography-Summer 2024 (Jun. 2024)
- Best Paper Award (Title; A Study of Executable Binaries with Emerging Compilation Tools) at Conference on Information Security and Cryptography-Winter 2024 (Jun. 2022)
- Student Grant for the 26th USENIX Security Symposium in Vancouver (Aug. 2017)

Invited Talks

- Executable Binary Analysis with AI, Workshop on Information Security and Cryptography (WISC '23) (Sep. 2023)
- A Transformer based Function Symbol Name Inference Model from an Assembly Language for Binary Reversing, Kyunghee University Seminar (Aug. 2023)
- Understanding of Advanced Code Reuse Attacks and Defenses, UNIST Seminar (Dec. 2022)
- A Practical Binary Similarity Detection Approach, Sejong Cybersecurity Workshop 0x01 (Oct. 2022)
- Binary Code Representation for Deep Learning and its Applications, Software Convergence Symposium (SWCS '22) (Apr. 2022)
- Semantic-aware Binary Code Representation with Deep Learning, Fall KAIST Security Colloquium (Nov. 2021)
- Executable Binary Code Representation with Deep Learning, In the 21ST KOCSEA Technical Symposium Program (Nov. 2021)
- Crash Course on Deep Learning for Security, Soongsil University (Jul. 2021)
- Toward (Better) Binary Code Representation with Deep Learning, Seoul National University (Jun. 2021)
- 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)

Invited Lectures

- Binary Reversing with AI, Lecture Series on AI Applications by KIISC, Korea Institute of Information Security and Cryptography (Aug. 2024)
- Software Security, Seoul Science High School (Jan. 2022-2024)
- Security with AI, Kepco KDN (Nov. 2021)

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)

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)