

Suyoung Lee

✉ suyoung.lee@kaist.ac.kr |  [leeswimming](#)

📍 KAIST E3-1 #4431, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea

🏠 <https://leeswimming.com>

1 Summary

Suyoung Lee is a Ph.D. student at KAIST WSP Lab whose primary research is at the intersection of diverse fields, encompassing computer security, software engineering, and machine learning. In particular, his research focuses on developing and assessing systems designed to identify software vulnerabilities. For instance, he has actively contributed to discovering vulnerabilities in web browsers, web applications, and machine learning-enabled systems. His research has led to several publications in esteemed conferences such as USENIX Security, NDSS, WWW, ICML, and NeurIPS. Furthermore, he has served as a reviewer for ACM Transactions on Software Engineering and Methodology (TOSEM).

2 Education

- | | |
|------------------------|--|
| Sept. 2019 – Current | Ph.D. Student, Graduate School of Information Security
<i>Korea Advanced Institute of Science and Technology (KAIST)</i>
Advisor: Soeul Son |
| Sept. 2017 – Aug. 2019 | M.S., Graduate School of Information Security
<i>Korea Advanced Institute of Science and Technology (KAIST)</i>
Advisor: Soeul Son |
| Mar. 2013 – Aug. 2017 | B.S., Computer Engineering
<i>Sungkyunkwan University</i> |

3 Research Interests

Security, software engineering, program analysis, and machine learning.

4 Honors and Awards

- | | |
|------|--|
| 2022 | Best Paper Award (<i>KCC 2022</i>) |
| 2019 | Cybersecurity Research Competition by KIISC, 3rd & 4th place |
| 2019 | MSRC's 2018-2019 Most Valuable Security Researchers |

2015—2016	Kwanjeong Educational Foundation Scholarship
2014	Distinguished Freshman Award

5 Publications

(*: equal contribution)

5.1 Conference Papers

- [1] Byungjoo Kim, **Suyoung Lee**, Seanie Lee, Sooel Son, and Sung Ju Hwang. Margin-based Neural Network Watermarking. In *Proceedings of the International Conference on Machine Learning (ICML)*, pages 16696—16711, 2023
- [2] Dongwon Shin*, **Suyoung Lee***, and Sooel Son. RICC: Robust Collective Classification of Sybil Accounts. In *Proceedings of the ACM Web Conference (WWW)*, pages 2329—2339, 2023
- [3] Hoyong Jeong, **Suyoung Lee**, Sung Ju Hwang, and Sooel Son. Learning to Generate Inversion-Resistant Model Explanations. In *Proceedings of the Advances in Neural Information Processing Systems (NeurIPS)*, pages 17717—17729, 2022
- [4] Gyumin Lim, Gihyuk Ko, **Suyoung Lee**, and Sooel Son. Adversarial Activation based Neural Network Pruning Revision. In *Proceedings of the Korea Computer Congress (KCC)*, 2022
- [5] **Suyoung Lee**, HyungSeok Han, Sang Kil Cha, and Sooel Son. Montage: A Neural Network Language Model-Guided JavaScript Fuzzer. In *Proceedings of the USENIX Security Symposium (USENIX Security)*, pages 2613—2630, 2020
- [6] Taekjin Lee, Seongil Wi, **Suyoung Lee**, and Sooel Son. FUSE: Finding File Upload Bugs via Penetration Testing. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2020

5.2 Journal Papers

- [1] **Suyoung Lee**, Wonho Song, Suman Jana, Meeyoung Cha, and Sooel Son. Evaluating the Robustness of Trigger Set-Based Watermarks Embedded in Deep Neural Networks. *IEEE Transactions on Dependable and Secure (TDSC)*, 20(4):3434—3448, 2023
- [2] Gyumin Lim, Gihyuk Ko, **Suyoung Lee**, and Sooel Son. Pruning Deep Neural Networks Neurons for Improved Robustness against Adversarial Examples. *Journal of KIISE*, 50(7):588—597, 2023.

6 Patents

- [1] Sooel Son, Dongwon Shin, and **Suyoung Lee**. Random Sampling-based Collective Classification Method and System for Sybil Account Detection. US Patent 18491570, 2023
- [2] Sooel Son, Dongwon Shin, and **Suyoung Lee**. Random Sampling-based Collective Classification Method and System for Sybil Account Detection. Korea Patent 10-2023-0070788, 2023

- [3] Sooel Son, Gyumin Lim, Gihyuk Ko, and **Suyoung Lee**. Method and Apparatus of Revising a deep Neural Network for Adversarial Examples. Korea Patent 10-2022-0187679, 2022
- [4] Sooel Son and **Suyoung Lee**. Evaluating Method of Evaluating Robustness of Artificial Neural Network Watermarking against Model Stealing Attacks. US Patent 17361994, 2021
- [5] Sooel Son and **Suyoung Lee**. Evaluating Method for the Robustness of Watermarks Embedded in Neural Networks against Model Stealing Attacks. Korea Patent 10-2301295-0000, 2021
- [6] Sooel Son, Sang Kil Cha, **Suyoung Lee**, Insung Kim, and Taekyu Kim. Method and Apparatus for Testing JavaScript Interpretation Engine using Machine Learning. Korea Patent 10-2132450-0000, 2020

7 Software Artifacts

- [1] RICC, A Collective Classification Framework for Finding Sybil Accounts, 2023
<https://github.com/WSP-LAB/RICC>
- [2] GNIME, A Defense Framework against Model Inversion Attacks, 2022
<https://github.com/WSP-LAB/GNIME>
- [3] Montage, A Neural Network Language Model-based JavaScript Engine Fuzzer, 2020
<https://github.com/WSP-LAB/Montage>
- [4] FUSE, A Penetration Testing Tool for Finding File Upload Bugs, 2020
<https://github.com/WSP-LAB/FUSE>

8 Reported Security Vulnerabilities

CVE-2019-8594	Arbitrary code execution in JavaScriptCore of Safari
CVE-2019-0923	Memory corruption in ChakraCore of Edge
CVE-2019-0860	Arbitrary code execution in ChakraCore of Edge (\$5,000 reward)
ID #474359	Stored XSS in WordPress (\$600 reward)
XEVE-2019-001	Unrestricted file upload in XE
CVE-2018-19419	Unrestricted file upload in CMSMadeSimple
CVE-2018-19422	Unrestricted file upload in Subrion
CVE-2018-19421	Unrestricted file upload in GetSimpleCMS
CVE-2018-19420	Unrestricted file upload in GetSimpleCMS
CVE-2018-19172	Unrestricted file upload in Elgg

CVE-2018-19146	Unrestricted file upload in Concrete5
CVE-2018-19062	Unrestricted file upload in CMSSimple
CVE-2018-18966	Unrestricted file upload in OsCommerce2
CVE-2018-18965	Unrestricted file upload in OsCommerce2
CVE-2018-18964	Unrestricted file upload in OsCommerce2
CVE-2018-18694	Unrestricted file upload in Monstra
CVE-2018-18637	Unrestricted file upload in ECCube3
CVE-2018-18574	Unrestricted file upload in CMSMadeSimple
CVE-2018-18572	Unrestricted file upload in OsCommerce2
CVE-2018-6383	Unrestricted file upload in Monstra

9 Professional Services

9.1 External Conference Reviewer

2023	IEEE S&P
2022—2023	The Web Conference (WWW)
2021—2023	USENIX Security
2021—2022	ACM CCS
2021—2022	NDSS
2018, 2020—2021	ACSAC

9.2 Journal Reviewer

2023	ACM TOSEM
------	-----------

10 Teaching

10.1 Teaching Assistant

Spring 2021	IS542 – Web Service Security and Privacy	KAIST
Fall 2019	CS492 – Machine Learning Application Trends in Information Security	KAIST
Spring 2019	IS542 – Web Service Security and Privacy	KAIST

Fall 2018

IS593 – Machine Learning Application Trends in Information Security

KAIST

11 Applicable Coursework

Spring 2020

Embedded Systems Security

Fall 2019

Advanced Cyber Security Practice

Fall 2018

Machine Learning Application Trends in Information Security

Spring 2018

Information Security

Information Security Laboratory

Deep Learning

Fall 2017

Web & Mobile Service Security

Binary Code Analysis and Secure Software Systems