Insup Lee

AI & Security Researcher at Abu Dhabi, UAE

insuplee94@gmail.com | LinkedIn | Google Scholar

Summary

I am a cyber officer of ROK Army, currently working in **Abu Dhabi**, UAE. Previously, I spent five years as a researcher at Agency for Defense Development (ADD), where I collaborated on research with Dr. Changhee Choi. My primary research interest lies at the **intersection of AI and cybersecurity**, especially addressing diverse issues with generative models. I am scheduled to be discharged from military service in May 2025.

Research Interests

- **AI + Security**: NLP for threat intelligence, adversarial ML, AI for cybersecurity, LLM for vulnerability detection
- **Generative Models**: diffusion models with transformers & GANs
- **Network and Wireless Security**: drones, robust communications, anomaly detection, network IDS, etc.

Education

Ph.D. Candidate in Cybersecurity, Korea University – Seoul, Republic of Korea — Sep 2019 – Present

- Completed all required coursework for the doctoral program (overall GPA: 4.33/4.50)

B.E. in Cyber Defense, Korea University – Seoul, Republic of Korea — Mar 2014 – Feb 2018

- Studied computer science, cybersecurity, cryptography, and AI

Work Experience

Cyber Officer, Ministry of National Defense – Republic of Korea — Aug 2023 – present

- Collaborated with international team members while working in the UAE
- Developed programs for network defense operations at the Cyber Operations Command

Researcher, Agency for Defense Development – Seoul, Republic of Korea — Jul 2018 – Jul 2023

- Actively contributed to three research projects centered on AI-driven cybersecurity
- Published five international papers [C1, C2, J2, J3, J4], four patents, and 12 domestic papers

Research Projects

Diffusion Models for UAVs — Mar 2024 - Present

- Keywords: diffusion models, vision transformers, drone communications, adversarial robustness
- Frameworks/Tools: PyTorch, GNU Radio

Detection of Nation-Sponsored Cyber Attacks Using NLP Technologies — Apr 2021 - Sep 2024

- Keywords: cyber threat intelligence, NLP, data augmentation, embedding, SOAR, MITRE ATT&CK
- Frameworks/Tools: PyTorch, scikit-learn, FastAPI, Git, PostgreSQL
- Publications: [J2], [J3], [J4]

Generative Adversarial Networks for Robust Modulation Classification — May 2020 - Dec 2022

- Keywords: wireless communications, GANs, adversarial attacks, I/Q data augmentation, adversarial robustness
- Frameworks/Tools: PyTorch, IBM ART
- Publications: [J1], [J5]

Generative Models for Cybersecurity Data Augmentation — Jun 2019 - Oct 2020

- Keywords: host IDS, sequence data, CycleGAN, SeqGAN, Seq2Seq, ADFA-LD
- Frameworks/Tools: TensorFlow, Node.js, Git
- Publications: [C1], [C2]

Network Intrusion Detection Systems Using Incremental Learning Sep 2019 - Apr 2020

- Keywords: network IDS, machine learning, encrypted traffic classification, incremental learning
- Frameworks/Tools: scikit-learn
- Publications: [C3]

IPADS: Integrated Proactive and Adaptive Defense Systems Aug 2018 - May 2019

- Keywords: anomaly detection, network IDS, in-vehicle network, MilCAN, CIC-IDS2017
- Frameworks/Tools: scikit-learn

Awards and Honors

- The 3rd Prize, Military Cybersecurity Experts Hackathon, Ministry of Science and ICT, Republic of Korea Dec 2023
- Full Tuition Scholarship, Ministry of National Defense, Republic of Korea Mar 2014 – Feb 2018

Other Experience

AI Cyber Challenge (AIxCC), DARPA and ARPA-H, USA Apr 2024 – Aug 2024

- Submitted our cyber reasoning system (CRS) to achieve automated program repair (APR), leveraging LLMs for automatic detection and patching of software vulnerabilities
- Participated in the AIxCC semifinal round as a member of Team KORIA

SW Outsourcing Development, KCMVP-Certified Cryptographic Module Jun 2017 – Mar 2018

- ARIA block cipher (mode: ECB/CBC/CTR), Hash (SHA256/SHA512) and HMAC-based DRBG for Windows (.dll) and Linux (.so), implemented by 25,000 LoC with C
- Tested by national security research institute (NSR) and certified by national intelligence service (NIS)

Technical Skills

- Frameworks/Tools: PyTorch, Keras, TensorFlow, scikit-learn, pandas, Git, Docker, Kubernetes, Metasploit
- Programming Languages: Python, C/C++, JavaScript, SQL, HTML, CSS, PHP
- Languages: English, Korean

Publications

Under Review

- Insup Lee and Changhee Choi, "MuCamp: Generating Cyber Campaign Variants via TTP Synonym Replacement for Group Attribution," revised to *IEEE Transactions on Information Forensics and Security* (**IEEE TIFS**).

Journal Articles

J5 Insup Lee and Wonjun Lee, "UniQGAN: Towards Improved Modulation Classification With Adversarial Robustness Using Scalable Generator Design," *IEEE Transactions on Dependable and Secure Computing* (**IEEE TDSC**), Vol. 21, No. 2, pp. 732-745, March-April 2024.

J4 Insup Lee and Changhee Choi, "Camp2Vec: Embedding Cyber Campaign With ATT&CK Framework for Attack Group Analysis," *ICT Express*, Vol. 9, pp. 1065-1070, December 2023.

J3 Chanho Shin, Insup Lee, and Changhee Choi, "Exploiting TTP Co-occurence via GloVe-Based Embedding With ATT&CK Framework," *IEEE Access*, Vol. 11, pp. 100823-100831, September 2023.

J2 Youngjun Kim, Insup Lee, Hyuk Kwon, Gyeongsik Lee, and Jiwon Yoon, "BAN: Predicting APT Attack Based on Bayesian Network With MITRE ATT&CK Framework," *IEEE Access*, Vol. 11, pp. 91949-91968, August 2023.

J1 Insup Lee and Wonjun Lee, "UniQGAN: Unified Generative Adversarial Networks for Augmented Modulation Classification," *IEEE Communications Letters* (**IEEE CL**), Vol. 26, No. 2, pp. 355-358, February 2022.

Conference Proceedings

C3 Insup Lee, Heejun Roh, and Wonjun Lee, "Encrypted Malware Traffic Detection Using Incremental Learning," in *Proc. of the IEEE International Conference on Computer Communications (IEEE INFOCOM 2020) - Poster Session*, Virtual, July 2020.

C2 Sunguk Shin, Insup Lee, and Changhee Choi, "Anomaly Dataset Augmentation Using Sequence Generative Models," in *Proc. of the IEEE International Conference on Machine Learning and Applications (IEEE ICMLA 2019)*, Florida, USA, December 2019.

C1 Changhee Choi, Sunguk Shin, and Insup Lee, "Opcode Sequence Amplifier Using Sequence Generative Adversarial Networks," in *Proc. of the International Conference on ICT Convergence (ICTC 2019)*, Jeju Island, South Korea, October 2019.

Patents

- Changhee Choi and Insup Lee, "Method for Augmentating Cyber Attack Campaign Data to Identify Attack Group, and Security," Korea Patent Application Number. 10-2024-0176082, December 2, 2024.
- Changhee Choi, Insup Lee, Chanho Shin, and Sungho Lee, "Information Identification Method and Electronic Apparatus Thereof," Korea Patent Application Number. 10-2024-0006106, January 15, 2024.
- Changhee Choi, Chanho Shin, Sunguk Shin, Seongyeon Seo, and Insup Lee, "Method for Training Attack Prediction Model and Device Therefor," U.S. Patent Application Number. 18/126,005; U.S. Patent Number. US20230308462A1, September 28, 2023.
- Changhee Choi, Sunguk Shin, and Insup Lee, "Appratus, Method, Computer-readable Storage Medium and Computer Program for Generating Operation Code," Korea Patent Application Number. 10-2019-0141865, November 07, 2019; Korea Patent Number. 10-2246797, April 30, 2021.

Domestic Journals (Korean)

- Kangmun Kim and Insup Lee, "User Behavior Embedding via TF-IDF-BVC for Web Shell Detection," *Journal of The Korea Institute of Information Security & Cryptology (JKIISC)*, Vol. 34, No. 6, pp. 1231-1238, Dec. 2024.
- Yongbin Park, Sunguk Shin, and Insup Lee, "A Study on Evaluation Method of NIDS Datasets in Closed Military Network," *Journal of Internet Computing and Services (JICS)*, Vol. 21, No. 2, pp. 121-130, Apr. 2020.

Domestic Conferences (Korean)

- Insup Lee, Chanho Shin, and Changhee Choi, "Mutating Cyber Camapaign With TTP Word Replacement," in *Proc. of the KIMST Annual Conference*, Jun. 2023.
- Chanho Shin, Insup Lee, and Changhee Choi, "Towards GloVe-Based TTP Embedding With ATT&CK Framework," in *Proc. of the KIMST Annual Conference*, Jun. 2023.
- Changhee Choi, Insup Lee, Chanho Shin, and Sungho Lee, "Cyber Threat Campaign Analysis Based on PEGASUS and RoBERTa Model," in *Proc. of the KIMST Annual Conference*, Jun. 2023.
- Insup Lee, Chanho Shin, Sunguk Shin, Seongyeon Seo, and Changhee Choi, "Analyzing Cyberattack Campaign Similarity via TTP Sequence Embedding," in *Proc. of the KIMST Annual Conference*, Jun. 2022.
- Sunguk Shin, Insup Lee, Chanho Shin, Seongyeon Seo, and Changhee Choi, "Cyber Campaign Analysis With TTP Embedding Using TF-IDF," in *Proc. of the KIMST Annual Conference*, Jun. 2022.
- Chanho Shin, Sunguk Shin, Insup Lee, Seongyeon Seo, and Changhee Choi, "Classifying TTP Based on CIA Labeling," in *Proc. of the KIMST Annual Conference*, Jun. 2022.
- Changhee Choi, Chanho Shin, Sunguk Shin, Seongyeon Seo, and Insup Lee, "Cyber Attack Group Classification Using Siamese LSTM," in *Proc. of the KIMST Annual Conference*, Jun. 2022.
- Chanho Shin, Sunguk Shin, Seongyeon Seo, Insup Lee, and Changhee Choi, "Embedding and Training RNN to Estimating the Goal of Cyber Attack," in *Proc. of the KIMST Fall Conference*, Nov. 2021.
- Sunguk Shin, Chanho Shin, Seongyeon Seo, Insup Lee, and Changhee Choi, "The Proposed Approach for Country Prediction With TTP-based Cyber Data Using GCN," in *Proc. of the KIMST Fall Conference*, Nov. 2021.
- Changhee Choi, Chanho Shin, Sunguk Shin, Seongyeon Seo, and Insup Lee, "Deep Learning for Estimating Next Action of Cyber Attack," in *Proc. of the KIMST Fall Conference*, Nov. 2021.
- Insup Lee, Jingook Kim, and Jeongchan Park, "Analysis of Weight Setting in Incremental Learning to Improve Real-Time Intrusion Detection," in *Proc. of the KIMST Annual Conference*, Jun. 2019.