February 2025

Insup Lee

AI & Security Researcher at Abu Dhabi, UAE

insuplee94@gmail.com | LinkedIn | Google Scholar | ORCiD

Summary

I am a cyber officer in the Republic of Korea Army, currently serving in **Abu Dhabi**, UAE. Previously, I worked as a researcher for five years at the Agency for Defense Development (ADD), where I collaborated on AI-driven security research with Dr. Changhee Choi. I am also a Ph.D. candidate in Cybersecurity at Korea University, where I earned my B.E. in Cyber Defense. My primary research interests lie at the **intersection of AI and cybersecurity**, with a particular focus on addressing diverse challenges through the application of generative models. I am scheduled to complete my military service in May 2025.

Research Interests

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

Employment History

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

- Collaborated with Emirati colleagues and led projects while stationed 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

- Carried out three AI-driven cybersecurity projects, conducting research and in-house software development
  (1) "Detection of Nation-Sponsored Cyber Attacks Using NLP Technologies" (Apr 2021 – Jul 2023)
  (2) "Generative Models for Cybersecurity Data Augmentation" (Jun 2019 – Oct 2020)
  (3) "IPADS: Integrated Proactive and Adaptive Defense Systems" (Aug 2018 – May 2019)
- Published five international papers [C1, C2, J2, J3, J4], four patents, and 12 domestic papers

Education

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

- Completed all required coursework and passed Ph.D. qualifying examination
- Researched generative models to enhance robustness in communication systems

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

- Studied computer science, cybersecurity, cryptography, and secure coding

Technical Skills

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

Research Projects

Diffusion Models for Drones Dec 2023 - Present

- Keywords: diffusion models, vision transformers, drone communications, adversarial robustness
- Frameworks/Tools: PyTorch, GNU Radio
- Publications: two papers are under review

Detection of Nation-Sponsored Cyber Attacks Using NLP Technologies Apr 2021 - Dec 2023

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

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

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 – May 2018

- Implemented a cryptographic module with 25,000 LoC in C while following secure coding conventions
- Covered the ARIA block cipher (modes: ECB, CBC, CTR), hash functions (SHA-256, SHA-512), and HMAC-based DRBG for Windows (.dll) and Linux (.so), respectively

Awards and Honors

- The 3rd Prize, Military Cybersecurity Experts Hackathon, Ministry of Science and ICT, Republic of Korea Dec 2023
- Colonel's Commendation for excellence in web penetration testing, Cyber Operations Command, Republic of Korea Apr 2019
- Full Tuition Scholarship, Ministry of National Defense, Republic of Korea Mar 2014 – Feb 2018

Publications

Under Review

- Enhancing Drone Video Signal Processing with Diffusion Transformers
  Insup Lee, Khalifa Alteneiji, and Mohammed Alghfeli
  submitted to *IEEE Transactions on Vehicular Technology* **(TVT)**
- (Blind review)
  Insup Lee
  submitted to *ACM Conference on Computer and Communications Security* (**CCS**), 2025
- MuCamp: Generating Cyber Campaign Variants via TTP Synonym Replacement for Group Attribution
  Insup Lee and Changhee Choi
  resubmitted after revision to *IEEE Transactions on Information Forensics and Security* (**TIFS**)

Journal Articles

J5 UniQGAN: Towards Improved Modulation Classification With Adversarial Robustness Using Scalable Generator Design
Insup Lee and Wonjun Lee
IEEE Transactions on Dependable and Secure Computing (**TDSC**), 2024
(SCI 2023 I/F Top 5.30% in CS, Software Engineering Category)

J4 Camp2Vec: Embedding Cyber Campaign With ATT&CK Framework for Attack Group Analysis
Insup Lee and Changhee Choi
ICT Express, 2023

J3 Exploiting TTP Co-occurence via GloVe-Based Embedding With ATT&CK Framework
Chanho Shin, Insup Lee, and Changhee Choi
IEEE Access, 2023

J2 BAN: Predicting APT Attack Based on Bayesian Network With MITRE ATT&CK Framework
Youngjun Kim, Insup Lee, Hyuk Kwon, Gyeongsik Lee, and Jiwon Yoon
IEEE Access, 2023

J1 UniQGAN: Unified Generative Adversarial Networks for Augmented Modulation Classification
Insup Lee and Wonjun Lee
IEEE Communications Letters, 2022

Conference Proceedings

C3 Encrypted Malware Traffic Detection Using Incremental Learning
Insup Lee, Heejun Roh, and Wonjun Lee
IEEE International Conference on Computer Communications (INFOCOM) - Poster Session, 2020

C2 Anomaly Dataset Augmentation Using Sequence Generative Models
Sunguk Shin, Insup Lee, and Changhee Choi
IEEE International Conference on Machine Learning and Applications (ICMLA), 2019

C1 Opcode Sequence Amplifier Using Sequence Generative Adversarial Networks
Changhee Choi, Sunguk Shin, and Insup Lee
International Conference on ICT Convergence (ICTC), 2019

Mentoring Experience

- **Hyunjun Park** (Navy Lieutenant at Ministry of National Defense) Nov 2024 – Feb 2025
  DDoS detection via transfer learning (paper submitted to JKIISC)
- **Kangmun Kim** (First Lieutenant at Cyber Operations Command) Jan 2024 – Sep 2024
  Web shell detection via user behavior embedding (paper published at JKIISC)