

Insup Lee

AI & Security Researcher at Abu Dhabi, UAE

insuplee94@gmail.com | website | LinkedIn | GitHub

About Me

I am a captain of ROK Army, currently working in **Abu Dhabi, UAE**. Prior to this, I completed five years of AI-based cybersecurity research at the Agency for Defense Development (ADD). I am in my last year of mandatory military service of seven years, which will conclude in May 2025. I am also a Ph.D. candidate in information security at Korea University, advised by Prof. Wonjun Lee (Network and Security Research Lab). Prior to that, I received my B.Eng. in Cyber Defense (CYDF) from Korea University.

My primary research interest lies at the **intersection of AI and cybersecurity**, especially addressing diverse issues with **generative models**.

Research Interests

- Generative models: diffusion models with transformers and domain-specific scalability in GAN
- Communications security: drones and robust communications via generative models
- Security intelligence: NLP for cyber threat intelligence
- AI security: robustness against adversarial attacks through data augmentation

Education

Korea University, Ph.D. in Information Security Sep 2019 – present

- Dissertation: Unified Generative Models for Robust Modulation Classification
- Advisor: Prof. Wonjun Lee

Korea University, B.Eng. in Cyber Defense Mar 2014 – Feb 2018

Positions Held

Instructor, Ministry of National Defense – Abu Dhabi, UAE Apr 2024 – present

- Delivered lectures for cybersecurity in English: penetration testing (Jul 2024, Sep 2024)
- Received an award for distinguished lecture (Jul 2024)

Security Engineer, Cyber Operations Command – Republic of Korea Aug 2023 – Apr 2024

- Analyzed Access logs for web shell detection using Python
- Developed programs to support network defense operations using JavaScript and Python

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

- Actively contributed to three research projects focused on AI (generative models and NLP) for cybersecurity
- Published 5 international papers, 12 domestic papers and two patents

Research Projects

Unified Generative Models for Robust Modulation Classification May 2020 - present

- Keywords: diffusion models, GAN, wireless communications, vision transformer, adversarial robustness
- Frameworks/Tools: PyTorch, IBM ART
- Publications: [J1], [J5]

AI-Based Cyber Campaign Detection With MITRE ATT&CK Framework Apr 2021 - Dec 2023

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

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

Publications

Under Review

- Insup Lee and Wonjun Lee, "-", submitted to *IEEE International Conference on Computer Communications (INFOCOM)*.
- 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 (TIFS)*.

International Journals

- 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 (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 Chanhoo Shin, Insup Lee, and Changhee Choi, "Exploiting TTP Co-occurrence 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 (CL)*, vol. 26, no. 2, pp. 355-358, February 2022.

International Conferences

- 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 (INFOCOM) - 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 (ICMLA)*, 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)*, Jeju Island, South Korea, October 2019.

US Patents

- P1 Changhee Choi, Chanhoo 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.

Domestic Journals

- 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. xx, no. x, pp. xxx-xxx, 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

- Insup Lee, Chanho Shin, and Changhee Choi, "Mutating Cyber Camapaigh 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, Jinguok 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.

Domestic Patents

- 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.

Software Registrations

- Changhee Choi, Sunguk Shin, and Insup Lee, "Log Extractor For Windows 10 Internet, Event, Process, and Network," Software Registration No. C-2020-035358, October 14, 2020.

Other Experience

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

-
- Programming Languages: Proficient - Python, C, JavaScript & Occasional - SQL, HTML, CSS, PHP
 - Frameworks/Tools: PyTorch, Keras, TensorFlow, scikit-learn, pandas, Git, Burp Suite, Metasploit, GNU Radio