Buse G.(Gül) A.(Atli)

Karakaari 7B, 02610, Espoo, Finland
(+358) 40 665 2020
busega@acm.org
https://busegulatli.github.io/
https://github.com/bussfromspace
buse-gul-atli-18821298

EDUCATION

Doctor of Science (Technology) January 2019 - August 2022
(GPA - 4.00/5.00)
Aalto University, Espoo, Finland

- Doctoral thesis: Securing Machine Learning: Streamlining Attacks and Defenses Under Realistic Adversary Models

Master Of Science (Technology) September 2015 - October 2017
(GPA - 4.46/5.00)
Aalto University, Espoo, Finland

- Master's thesis: Anomaly-Based Intrusion Detection by Modeling Probability Distributions of Flow Characteristics

Bachelor of Science September 2006 - June 2011
Middle East Technical University (METU), Ankara, Turkey

EXPERIENCE

Security Researcher November 2022 -
Nokia Bell Labs, Espoo, Finland

- Part of Network Security Team under Network Systems and Security Research (NSSR) Department.
- Trustworthy AI/ML: Security, privacy, and trust of machine learning (ML) models in decentralized environments that include different stakeholders. Ownership verification for deep-reinforcement learning models to protect intellectual property in case of theft. Feasibility study of security & privacy in ML-based RAN applications. Securing data at rest through the combination of ML-based methods and encryption strategies and improving regulatory compliance through machine learning methods.

Graduate intern June 2022 - October 2022
Intel Corporation, Espoo, Finland

- Part of Secure Intelligence Team led by Jason Martin.
- Private AI/ML: Comprehensive taxonomy of ML model extraction at-

tacks and cost analysis of different defense strategies against such attacks.

Doctoral Researcher September 2018 - August 2022
Aalto University, Espoo, Finland

- Part of Secure Systems Group (SSG) led by Prof. N. Asokan and part of Private AI Collaboration Research Institute (Private AI) that focuses on developing private and trustworthy technologies in decentralized AI/ML.
- Robust AI/ML: Model evasion attacks, adversarial examples & detection of adversarial inputs in computer vision and deep reinforcement learning applications.
- Private AI/ML: Model extraction attacks that replicate model functionality and unauthorized distribution of stolen models. Ownership resolution and ML model watermarking in federated learning. Ownership verification for datasets in the event of misuse or violation of other conditions stipulated in the license under which the data is shared.

Research Assistant October 2017 - September 2018
Aalto University, Espoo, Finland

- Robust AI/ML: Adversarial machine learning and adversarial attacks in computer vision applications.
- ML for cyber security: ML-based anomaly detection using deep neural networks and clustering algorithms.

Trainee in IoT Security Research May 2017 - October 2017
Nokia Bell Labs, Espoo, Finland

- ML for cyber security: Dynamic feature ranking algorithms that can be integrated into machine learning-based intrusion detection systems.

Thesis Worker March 2016 - March 2017
Nokia Bell Labs, Espoo, Finland

- ML for cyber security: Evaluation of network traffic data sets, data preprocessing and sanitization by converting packet-level information to flow-level information, feature extraction, and hierarchical clustering. Modeling the statistical characteristics of sequential network flow data via Extreme Learning Machines (ELM) and detection of malicious network traffic based on approximated statistical information within clustered data.

Software Engineer June 2011 - August 2015
ASELSAN, Ankara, Turkey

- Signal Processing: Image and video enhancement algorithms in thermal camera products: Contrast-limited adaptive histogram equalization (CLAHE), multi-camera image stitching, bad pixel detection and mitigation, automatic focus algorithms for lenses.
- Front-End & Back-End Development: Design and implementation of communication infrastructure between submodules of thermal cameras.

Candidate Engineer December 2010 - July 2011
ASELSAN, Ankara, Turkey

- Front-end & Back-end Development: Evaluation of adaptive image enhancement techniques, design of graphical user interfaces, and unit testing.

TEACHING

CS-E4001 Research Seminar on Security and Privacy of Machine Learning
Course Assistant, Aalto University (*Spring 2021, Fall 2019*)

CS-E4000 Seminar in Computer Science: Internet, Data and Things
Student Tutor, Aalto University (*Fall 2021, Spring 2021, Spring 2019*)

CS-E4310 Mobile Systems Security
Course Assistant, Aalto University (*Spring 2020*)

CS-E4800 Artificial Intelligence
Course Assistant, Aalto University (*Spring 2018*)

CS-E4800 Deep Learning
Course Assistant, Aalto University (*Spring 2017*)

RESEARCH EFFORTS

Publications

- **A. Tekgul, Buse G.**, and N. Asokan. *FLARE: Fingerprinting Deep Reinforcement Learning Agents using Universal Adversarial Masks.* In Proceedings of the 39th Annual Computer Security Applications Conference. 2023.
- **Atlı Tekgül, Buse Gül**. *Securing Machine Learning: Streamlining Attacks and Defenses Under Realistic Adversary Models.*. Doctoral Thesis, Aalto University. (2022).
- **Tekgul, Buse G. A.**, Shelly Wang, Samuel Marchal, and N. Asokan. *Real-time Adversarial Perturbations against Deep Reinforcement Learning Policies: Attacks and Defenses* In European Symposium on Research in Computer Security. Cham: Springer Nature Switzerland, 2022.
- **Tekgul, Buse G. A.**, and N. Asokan. *On the Effectiveness of Dataset Watermarking*. In Proceedings of the 2022 ACM on International Workshop on Security and Privacy Analytics. 2022.
- Szyller, Sebastian, **Buse Gul Atli**, Samuel Marchal, and N. Asokan. *DAWN: Dynamic Adversarial Watermarking of Neural Networks.* In Proceedings of the 29th ACM International Conference on Multimedia (pp. 4417-4425). 2021
- **Tekgul, Buse G. A.**, Yuxi Xia, Samuel Marchal, and N. Asokan. *WAFFLE: Watermarking in Federated Learning.* In 40th International Symposium on Reliable Distributed Systems (SRDS), pp. 310-320. IEEE, 2021.

- **Atli, Buse Gul**, Sebastian Szyller, Mika Juuti, Samuel Marchal, and N. Asokan. *Extraction of Complex DNN Models: Real Threat or Boogeyman?* In International Workshop on Engineering Dependable and Secure Machine Learning Systems, pp. 42-57. Springer, Cham, 2020.
- Juuti, Mika, **Buse Gul Atli**, and N. Asokan. *Making Targeted Black-box Evasion Attacks Effective and Efficient.* In Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security, pp. 83-94. 2019.
- Monshizadeh, Mehrnoosh, Vikramajeet Khatri, **Buse Gul Atli**, Raimo Kantola, and Zheng Yan. *Performance Evaluation of a Combined Anomaly Detection Platform.* IEEE Access 7 (2019): 100964-100978.
- **Atli, Buse Gul**, Yoan Miche, Aapo Kalliola, Ian Oliver, Silke Holtmanns, and Amaury Lendasse. *Anomaly-based Intrusion Detection Using Extreme Learning Machine and Aggregation of Network Traffic Statistics in Probability Space.* Cognitive Computation 10, no. 5 (2018): 848-863.
- Monshizadeh, Mehrnoosh, Vikramajeet Khatri, **Buse Atli**, and Raimo Kantola. *An Intelligent Defense and Filtration Platform for Network Traffic.* In International Conference on Wired/Wireless Internet Communication, pp. 107-118. Springer, Cham, 2018.
- **Atli, Buse Gul**, Yoan Miche, and Alexander Jung. *Network Intrusion Detection Using Flow Statistics.* In 2018 IEEE Statistical Signal Processing Workshop (SSP), pp. 70-74. IEEE, 2018.
- Kalliola, Aapo, Yoan Miche, Ian Oliver, Silke Holtmanns, **Buse Atli**, Amaury Lendasse, Kaj-Mikael Bjork, Anton Akusok, and Tuomas Aura. *Learning Flow Characteristics Distributions with ELM for Distributed Denial of Service Detection and Mitigation.* In Proceedings of ELM-2016, pp. 129-143. Springer, Cham, 2018.

Patents

- *Sparse Sampling Video Contrast Enhancement Apparatus and Method*
  July 2015
  Video contrast enhancement algorithm for low power processors by sparse sampling the original histogram with the help of a massively parallel co-processor. Patent filed in July 2015 as part of the POCS Based Depth Super-Resolution (POCS-DSR) project funded by the European Commission.

Vision Papers/White papers/Technology Transfers

- *Private AI Collaborative Research Institute, Vision, Challenges & Opportunities*
  2021 : Coauthor of the vision document owned by the Private AI Collaborative Institute. Contributed to section titled as: *Protecting the Intellectual Property and Forensics.*

- The techniques developed in the 6th research paper above (*WAFFLE: Watermarking in Federated Learning.*) were adopted by industry partner Intel

and integrated into OpenFL, an open-source federated learning framework.

Volunteering

- Acted as a reviewer in various top-tier and second-tier conferences, journals and external applications: Nokia Bell Labs Price 2023, Knowledge Discovery and Data Mining Conference (KDD) 2023-2024-2025, IEEE/CVF Winter Conference on Applications of Computer Vision (WACV) 2023, IEEE Communications Magazine 2023-2024, Springer International Journal of Computer Vision 2022, IEEE Signal Processing Letters 2023, Experts reviewers in Nokia patent applications (2023-2024).

Supervisions

- Collaboration in the XcARet project and providing technical guidance to Yasintha Rumesh (University of Oulu & VTT), 2023 -
- Master's thesis advisor to MSc. Shelly Wang (University of Waterloo), 2022
  Title: Security and Ownership Verification in Deep Reinforcement Learning
  Supervisor: Prof. N. Asokan (Aalto University, Espoo, Finland & University of Waterloo, Canada)
- Master's thesis advisor to MSc. Minh Hoang, 2021
  Title: Dataset Watermarking
  Supervisor: Prof. N. Asokan (Aalto University, Espoo, Finland & University of Waterloo, Canada)
- Master's thesis advisor to Yuxi Xia, 2020
  Title: Watermarking Federated Deep Neural Network Models
  Supervisor: Prof. N. Asokan (Aalto University, Espoo, Finland & University of Waterloo, Canada)
- Advisor for summer internship, MSc. Yujia Guo, 2022
  Topic: Integrating watermarking feature into Intel OpenFL, watermarking in adversarial settings in federated learning

---

TECHNOLOGY SKILLS

Programming Languages: Python (2.X & 3.X), PyTorch, Tensorflow, Keras, Theano, C++
Computing and Software: Jupyter Notebook, Google Collab, PySyft, MuJoCo, OpenArgus, Rational Rhapsody, Eclipse IDE, Visual Studio, Ray AI framework.
Language: English (Full professional proficiency), Turkish (Native), Finnish (Intermediate proficiency)

EXTRA-CURRICULAR ACTIVITIES

Esbo Arbis Theater Group,
Actress 2023 (Stage manager)-2024

TEDx Otaniemi 2016-2017,
Stage Manager August 2016 - August 2017

Bilkent University Musical Club,
Actress and vocal coach August 2014 - January 2015

METU Musical Club,
Actress, vocal and assistant director August 2011 - September 2014

METU Science Fiction and Fantasy Club (SFFS),
Active member, vice president September 2006 - June 2011