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
- Key courses: Reinforcement Learning, Mobile Systems Security, Network Security, Object Oriented Programming with C++, Programming Parallel Computers, Research Seminar on Security and Privacy of Machine Learning

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
- Key courses: Artificial Intelligence, Convex Optimization for Engineers, Basic Principals of Machine Learning, Kernel Methods in Machine Learning, Machine Learning and Neural Networks, Machine Learning : Advanced Probabilistic Methods, Principals of Pattern Recognition, Algorithmic Methods of Data Mining, Statistical Signal Processing, Statistical Natural Language Processing, Information Security

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

TECHNOLOGY SKILLS

Programming Languages: Python (2.X & 3.X), PyTorch, Tensorflow, Keras, Theano, C++
Software Engineering Practices: Version control (Git), Trello, Scrum, Cpplint, Doxygen.
Computing and Software: Jupyter Notebook, Google Collab, PySyft, MuJoCo, OpenArgus, Rational Rhapsody, Eclipse IDE, Visual Studio.

Language: English (Full professional proficiency), Turkish (Native), Finnish (Intermediate proficiency)

EXPERIENCE

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

- Part of Network Security Team led by Yoan Miche

Graduate Intern July 2022 - October 2022
Intel Corporation, Espoo, Finland

- Part of Secure Intelligence Team led by Jason Martin
- Cost analysis of machine learning (ML) model extraction attacks and defenses

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

- Part of Secure Systems Group led by Prof. N. Asokan.
- Adversarial modelling of attacks against ML applications.
- Model evasion attacks via adversarial examples & defense mechanisms in image classification and deep reinforcement learning.
- ML model theft, model extraction attacks, and IP protection in realistic adversary models.
- Ownership resolution and ML model watermarking in federated learning applications
- Dataset watermarking and IP protection for public & private databases.

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

- Efficient and effective adversarial example generation methods for evading image classifiers
- Implementation of various neural network-based anomaly detection mechanisms in network traffic data.

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

- Online feature ranking module via Support Vector Machines (SVM) in machine learning based intrusion detection systems.
- Application of neural networks for intrusion detection on rare application protocols that run on TCP.

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

- Evaluation of network traffic datasets, 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).
- Detection of malicious network traffic based on the approximated statistical information within clustered data.

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

- Design and implementation of image and video enhancement algorithms in thermal camera products: Contrast Limited Adaptive Histogram Equalization (CLAHE), multiple-camera image stitching, bad pixel detection and mitigation)
- Implementation of automatic focusing in thermal cameras.
- Design and implementation of communication infrastructure between submodules of hand-held cameras.

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

- Adaptive contrast enhancement techniques in thermal images
- Graphical user interface, software testing, client-server setup for various defense products.

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 (*Spring and Fall 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*)

PATENTS

Sparse Sampling Video Contrast Enhancement Apparatus and Method
March 2015
Video contrast enhancement algorithm for low power processors by sparse

sampling the original histogram with the help of a massively parallel coprocessor. Patent filed on March 2015 as a part of POCS Based Depth Super-Resolution (POCS-DSR) project funded by European Commission.

VISION PAPER

Private AI Collaborative Research Institute, Vision, Challenges & Opportunities 2021
Co-author of the vision paper owned by Private AI Collaborative Institute. Contributed to section 3.5: *Protecting the Intellectual Property and Forensic.*

RESEARCH EFFORTS

Publications

- **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* arXiv preprint arXiv:2106.08746, will appear in the proceedings of ESORICS 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.

Supervisions

- Master's thesis advisor to MSc. Shelly Wang, 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

---

EXTRA-CURRICULAR ACTIVITIES

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

Company Musicals,
Actress, vocal and assistant director August 2011 - September 2014

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