Buse Gul Atli Tekgul

Malmiportti 4C 31, Espoo, Finland 02200
(+358) 449174172
buse.atlitekgul@aalto.fi
https://bgatli.github.io/
https://github.com/bussfromspace
buse-gul-atli-18821298

EDUCATION

Doctor of Science (Technology) January 2019 - Present
Aalto University, Espoo, Finland

Master Of Science, September 2015 - October 2017
Aalto University, Espoo, Finland

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: Agile, Continuous Integration, Scrum, Version control (Git), 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

Doctoral Researcher October 2018 - Present
Aalto University, Espoo, Finland

- Part of the Secure Systems Group led by Prof. N. Asokan.
- Analysis of Deep Neural Networks (DNNs) in adversarial settings.
- Improving model evasion attacks via adversarial examples & defense mechanisms in image classification, and deep reinforcement learning.
- Investigation of DNN model stealing attacks and IP protection in realistic threat models.
- Ownership resolution and DNN model watermarking in federated learning applications
- Dataset watermarking and IP protection in open databases.

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

- Efficient and effective adversarial example generation algorithms 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 Networks, 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 Networks, Espoo, Finland

- Evaluation of different 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 and approximating it via Extreme Learning Machines (ELM).
- Detection and mitigation 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 & mitigation)
- Automatic focusing for thermal camera lenses using frequency information.
- System management and messaging between submodules of hand-held cameras.

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

- Adaptive contrast enhancement techniques in thermal images
- User control interface, software testing, building server/client applications between subsystems in complex models.

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.
Seamless Image Registration in Panoramic Data
June 2014
Photometric analysis of 8bit gray-scale images in MATLAB environment. This analysis was combined with different compression, optimization and blending techniques to get seamless image mosaics with different background in extreme outdoor temperatures. Project and the related paper were part of ASELSAN defense product (confidential).

RESEARCH EFFORTS

Publications

- Tekgul, Buse G.A., and N. Asokan. *On the Effectiveness of Dataset Watermarking in Adversarial Settings.* Will appear in the proceedings of CODAPSY-IWSPA 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 (2021).
- 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 Minh Hoang, 2021
  Title: Dataset Watermarking
  Supervisor: Prof. N. Asokan (Aalto University, Espoo, Finland)
- Master's thesis advisor to Yuxi Xia, 2020
  Title: Watermarking Federated Deep Neural Network Models Prof. N. Asokan (Aalto University, Espoo, Finland)
- Advisor for summer internship, Yujia Guo, 2022
  *Topic:*Watermarking integration of OpenFL, watermarking in adversarial settings

---

Master's Thesis

Anomaly-Based Intrusion Detection by Modeling Probability Distributions of Flow Characteristics
Supervisor: Prof. N. Asokan (Aalto University, Espoo, Finland)
Advisor: D.Sc. Yoan Miche (Nokia Bell Labs, Espoo, Finland) *Description:* The thesis proposes an intrusion detection system based on modeling distributions of network statistics and Extreme Learning Machine (ELM) to achieve a high true positive rate. The proposed model aggregates the network traffic at the IP subnetwork level and the distribution of statistics are collected for the most frequent IPv4 addresses encountered as destination. The obtained probability distributions are learned by ELM. This model is evaluated on the ISCX-IDS 2012 dataset, which is collected using a real-time testbed. The model is compared against leading approaches using the same dataset. Experimental results show that the presented method achieves an average detection rate of 91% and a misclassification rate of 9%. (Grade: 5 out of 5)

Related Courses

- Artificial Intelligence

- Reinforcement Learning
- 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
- Object Oriented Programming with C++
- Programming Parallel Computers
- Information Security
- Mobile Systems Security
- Network Security
- Statistical Signal Processing
- Statistical Natural Language Processing

EXTRA-CURRICULAR ACTIVITIES

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