Alesia Chernikova

chernikova.a@northeastern.edu https://www.linkedin.com/in/alesia-chernikova/ (781) 350-0139

Research Interests

Adversarial machine learning, deep learning, network robustness, epidemiological modeling, spectral graph theory, Bayesian machine learning.

Education

Doctor of Philosophy Fall 2017 - Present
Computer Science
Northeastern University, Boston, MA
GPA: 3.9
Advisor: Dr. Alina Oprea

Bachelor of Science Fall 2009 - Spring 2014
Applied Mathematics
Belarusian State University, Minsk, Belarus
GPA: 3.8
Advisor: Dr. Vladimir Malugin
Thesis: "Development of risk management algorithms based on derivatives contracts"

Professional Experience

Research Assistant Fall 2017 - Present
NDS2 Lab, Northeastern University, Boston, MA
Conducting research on:

- Evasion attacks against Deep Neural Networks in cybersecurity and self-driving cars domains;
- Detecting malicious behavior through network data analysis.
- Modeling the behavior of self-propagating malware in the networks with the help of compartmental models of epidemiology.
- Improving network robustness in the face of self-propagating malware by leveraging spectral graph theory.

Applied Scientist Intern May 2021 - September 2021, May 2020 - August 2020
Amazon Web Services, Boston, MA

- Conducting research on cloud security as a part of the ESS-Detective team.

Software Engineer November 2013 - July 2017
IBA IT Park, Minsk, Belarus

- Participated as lead developer in the development and improvement of IBM GSAR web portal.

Research Assistant January 2012 - December 2013
Belarusian State University, Minsk, Belarus

- Participated in the research project for estimation and evaluation of credit rankings of national enterprises using mathematical, statistical, econometric methods and models based on the data from National Bank of the Republic of Belarus enterprise monitoring systems.

Research Projects

Feasible Evasion Attacks on Neural Networks in Constrained Environments
Advisor: Dr. Alina Oprea

- Trained machine learning models for classification of aggregated network traffic into malicious and benign.
- Proposed new type of evasion attack against Feed-Forward Neural Nerwork for network traffic classification.

Evasion Attacks against Deep Neural Networks for Self-Driving Cars
Advisors: Dr. Alina Oprea and Dr. Cristina Nita-Rotaru

- Trained Convolutional Neural Networks for autonomous vechicle direction and steering angle prediction.
- Created adversarial examples for Deep Neural Network that predicts self-driving car direction, proposed new type of evasion attack against steering angle prediction.

Cyber Network Resilience against Self-Propagating Malware Attacks
Advisors: Dr. Alina Oprea

- Proposed and analyzed a new compartmental model that captures the behavior of self-propagating malware (SPM).
- Used real malware traffic logs from WannaCry to fit the proposed model.
- Performed an in-depth evaluation of 10 defense techniques while introducing two novel defenses to increase the robustness of the networks in the face of SPM. The evaluation was performed using large real-world communication graphs from enterprise.
- Provided recommendations on the effectiveness and cost of defenses to inform network operators on various proactive preventive options against SPM attacks.

Publications

Alesia Chernikova, Nicolò Gozzi, Simona Boboila, Nicola Perra, Tina Eliassi-Rad, and Alina Oprea. **Modeling Self-Propagating Malware with Epidemiological Models.** [arxiv]

Alesia Chernikova, Nicolò Gozzi, Simona Boboila, Priyanka Angadi, John Loughner, Matthew Wilden, Nicola Perra, Tina Eliassi-Rad, and Alina Oprea. **Cyber Network Resilience against Self-Propagating Malware Attacks.** [European Symposium on Research in Computer Security (ESORICS) 2022]

Alesia Chernikova and Alina Oprea. **Fence: Feasible evasion attacks on neural networks in constrained environments.** [ACM Transactions on Security and Privacy 2022]

Alesia Chernikova, Alina Oprea, Cristina Nita-Rotaru and Baekgyu Kim. **Are Self-Driving Cars Secure? Evasion Attacks against Deep Neural Networks for Steering Angle Prediction.** [IEEE Workshop on the Internet of Safe Things 2019]

Alesia Chernikova and Vladimir Malugin. **Algorithms for interest-rate swaps hedging**. In the 70th undergraduate, graduate and postgraduate students scientific conference of Belarusian State University (vol. 1, pp. 242 – 245).

Honors & Awards

National Bank of the Republic of Belarus Merit Scholarship (2014-2015)
BSU Excellence Merit Scholarship (2009-2014)

Relevant Skills

Programming Languages: Java, Python, Javascript, C/C++
Frameworks and Libraries: Tensorflow, Keras, scikit-learn, PyTorch

Relevant Courses

Advanced Machine Learning (Bayesian methods for probabilistic modeling and inference), Data Visualization, Machine Learning, Advanced Algorithms, Data Mining (Unsupervised Learning), Distributed Systems, Theory of Probabilities and Mathematical Statistics, Methods of Optimization, Multivariate Statistical Analysis, Mathematical Theory of Forecasting.