Alina Mihaela Oprea

Curriculum Vitae

Contact Information

Address: Northeastern University
Khoury College of Computer Sciences
177 Huntington Ave., Office 516
Boston, MA, 02115
Phone: 617-373-4587
E-mail: a.oprea@northeastern.edu
Website: http://www.ccs.neu.edu/home/alina/

Education

Carnegie Mellon University, Pittsburgh, PA, USA 2001 - 2007

- Ph.D. in Computer Science, Advisor Michael K. Reiter 2007

  Thesis: ”Efficient Cryptographic Techniques for Securing Storage Systems”
- M.S. in Computer Science 2003

University of Bucharest, Bucharest, Romania 1996 - 2000

- B.S. in Computer Science and Mathematics, graduated Magna Cum Laude 2000

Employment (after PhD)

Northeastern University, Khoury College of Computer Science August 2016 - Present

- Professor of Computer Science since July 2024
- Associate Professor of Computer Science 2016 - 2024
- Tenure granted in June 2020

Google Research September 2022 - December 2023

- Visiting Faculty Researcher

National Institute of Standards and Technology (NIST) September 2021 - present

- Visiting Faculty Researcher

RSA Laboratories September 2007 - June 2016

- Principal and Consultant Research Scientist performing research in cloud and storage security, foundations of cybersecurity, applied cryptography, and security analytics for detecting advanced cyber attacks.

Honors And Awards

- CMU Cylab Distinguished Alumni Award 2024
- Caspar Bowden Award for Outstanding Research in Privacy Enhancing Technologies (Runner Up) 2023
- Ruth and Joel Spira Award for Excellence in Teaching 2020
- Google Security and Privacy Award 2019
- Outstanding Student Paper Award at the Conference on Decision and Game Theory for Security (GameSec) 2019

  Paper: "QFlip: An Adaptive Reinforcement Learning Strategy for the FlipIt Security Game"
- Best Paper Award at the 10th ACM Workshop on Artificial Intelligence and Security (AISEC) 2017

  Paper: "Robust Linear Regression Against Training Data Poisoning"
- Cyber Security Challenge Problem Award at the Computational Cybersecurity in Compromised Environments (C3E) workshop 2014
- NYU-Poly AT&T Best Applied Security Paper Award, 3rd place 2012

  Paper: "Iris: A Scalable Cloud File System with Efficient Integrity Checks"
- MIT Technology Review's TR35 Award 2011

  Award given for contributions to cloud security research
- Best Paper Award at the 12th Network and Distributed System Security Symposium (NDSS) 2005

  Paper: "Space-Efficient Block Storage Integrity"

Publications

Notation

* Graduate student mentee at Northeastern at the time work was performed
† Undergraduate student mentee at the time work was performed
‡ Graduate student mentee while at RSA Laboratories

Peer-reviewed conference, workshop, and journal publications:

[1] Ali Naseh, Yuefeng Peng, Anshuman Suri, Harsh Chaudhari*, Alina Oprea, and Amir Houmansadr. Riddle Me This! Stealthy Membership Inference for Retrieval-Augmented Generation. ACM CCS 2025

[2] Aditya Vikram Singh*, Ethan Rathbun*, Emma Graham, Lisa Oakley*, Simona Boboila, Peter Chin, and Alina Oprea. Hierarchical Multi-agent Reinforcement Learning for Cyber Network Defense Reinforcement Learning Conference (RLC), 2025.

[3] Xavier Cadet, Simona Boboila, Edward Koh, Peter Chin, and Alina Oprea. Quantitative Resilience Modeling for Autonomous Cyber Defense. In Reinforcement Learning Conference (RLC), 2025.

[4] Ethan Rathbun*, Alina Oprea, and Christopher Amato. Adversarial Inception for Bounded Backdoor Poisoning in Deep Reinforcement Learning. ICML 2025

[5] Ethan Rathbun*, Christopher Amato, and Alina Oprea. SleeperNets: Universal Backdoor Poisoning Attacks Against Reinforcement Learning Agents. In Proceedings of the 38th Conference on Neural Information Processing Systems (NeurIPS), 2024.

[6] Nikhil Kandpal, Krishna Pillutla, Alina Oprea, Peter Kairouz, Christopher A. Choquette-Choo, and Zheng Xu. User Inference Attacks on Large Language Models. In Conference on Empirical Methods in Natural Language Processing (EMNLP), Oral, 2024

[7] Georgios Syros*, Gokberk Yar*, Simona Boboila, Cristina Nita-Rotaru, and Alina Oprea. Backdoor Attacks in Peer-to-Peer Federated Learning. In *ACM Transactions of Privacy and Security Journal* (TOPS), 2024

[8] Lisa Oakley*, Steven Holtzen, and Alina Oprea. Synthesizing Tight Privacy and Accuracy Bounds via Weighted Model Counting. In *Proceedings of the 37th IEEE Computer Security Foundations Symposium* (CSF), 2024.

[9] John Abascal*, Stanley Wu†, Alina Oprea, and Jonathan Ullman. TMI! Finetuned Models Leak Private Information from their Pretraining Data. In Privacy Enhancing Technologies Symposium (PETS), 2024.

[10] Galen Andrew, Peter Kairouz, Sewoong Oh, Alina Oprea, H. Brendan McMahan, and Vinith Suriyakumar. One-shot Empirical Privacy Estimation for Federated Learning. In International Conference on Learning Representations (ICLR), Oral, 2024.

[11] Harsh Chaudhari*, Giorgio Severi*, Alina Oprea, and Jonathan Ullman. Chameleon: Increasing Label-Only Membership Leakage with Adaptive Poisoning. In International Conference on Learning Representations (ICLR), 2024.

[12] Andrew Yuan†, Alina Oprea, and Cheng Tan. Dropout Attacks. In *Proceedings of the IEEE Security and Privacy Symposium* (S&P), 2024.

[13] Krishna Pillutla, Galen Andrew, Peter Kairouz, H. Brendan McMahan, Alina Oprea, and Sewoong Oh. Unleashing the Power of Randomization in Auditing Differentially Private ML. In *Proceedings of the 37th Conference on Neural Information Processing Systems* (NeurIPS), 2023.

[14] Giorgio Severi*, Simona Boboila, Alina Oprea, John Holodnak, Kendra Kratkiewicz, and Jason Matterer. Poisoning Network Flow Classifiers. In *Proceedings of the Annual Computer Security Applications Conference* (ACSAC), 2023.

[15] Gokberk Yar*, Simona Boboila, Cristina Nita-Rotaru, and Alina Oprea. Backdoor Attacks in Peer-to-Peer Federated Learning. In *IEEE Conference on Communications and Network Security* (CNS), 2023.

[16] Alesia Chernikova*, Nicolo Gozzi, Nicola Perra, Simona Boboila, Tina Eliassi-Rad, and Alina Oprea. Modeling Self-Propagating Malware with Epidemiological Models. In *Journal of Applied Network Science*, 2023.

[17] Joshua Bundt, Michael Davinroy, Ioannis Agadakos, Alina Oprea, and William Robertson. Attacking Neural Binary Function Detection. In *Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses* (RAID), 2023.

[18] Han Wang, David Eklund, Alina Oprea, and Shahid Raza. FL4IoT: IoT Device Fingerprinting and Identification Using Federated Learning. In *ACM Transactions on Internet of Things*, Volume 4, Issue 3, pages 1-24, 2023.

[19] Matthew Jagielski*, Stanley Wu†, Alina Oprea, Jonathan Ullman, and Roxana Geambasu. How to Combine Membership-Inference Attacks on Multiple Updated Models. In *Proceedings of the 23rd Privacy Enhancing Technologies Symposium* (PETS), 2023

[20] Harsh Chaudhari*, John Abascal*, Alina Oprea, Matthew Jagielski, Florian Tramèr, and Jonathan Ullman. SNAP: Efficient Extraction of Private Properties with Poisoning. In *Proceedings of the IEEE Security and Privacy Symposium* (S&P), 2023.

[21] Antonio Emanuele Cinà, Kathrin Grosse, Ambra Demontis, Sebastiano Vascon, Werner Zellinger, Bernhard A Moser, Alina Oprea, Battista Biggio, Marcello Pelillo, and Fabio Roli. Wild Patterns Reloaded: A Survey of Machine Learning Security against Training Data Poisoning. In *ACM Compting Surveys Journal*, Volume 55, Issue 13s, pages 1-39, July 2023.

[22] Harsh Chaudhari*, Matthew Jagielski*, and Alina Oprea. SafeNet: The Unreasonable Effectiveness of Ensembles in Private Collaborative Learning. In *Proceedings of the IEEE Conference on Secure and Trustworthy Machine Learning* (SaTML), 2023.

[23] Afsah Anwar, Yi Hui Chen, Engin Kirda, Alina Oprea, Roy Hodgman, and Tom Sellers. A Recent Year On the Internet: Measuring and Understanding the Threats to Everyday Internet Devices. In *Proceedings of the Annual Computer Security Applications Conference* (ACSAC), 2022.

[24] Samson Ho, Achyut Reddy, Sridhar Venkatesan, Rauf Izmailov, Ritu Chadha, and Alina Oprea. Data Sanitization Approach to Mitigate Clean-Label Attacks Against Malware Detection Systems. In *Proceedings of the Military Communications Conference* (MILCOM), 2022.

[25] Giorgio Severi*, Matthew Jagielski*, Gokberk Yar*, Yuxuan Wang†, Alina Oprea, Cristina Nita-Rotaru. Network-Level Adversaries in Federated Learning. In *Proceedings of the IEEE Conference on Communications and Network Security* (CNS), 2022.

[26] 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. In *Proceedings of the 27th European Symposium on Research in Computer Security* (ESORICS), 2022.

[27] Alesia Chernikova* and Alina Oprea. FENCE: Feasible Evasion Attacks on Neural Networks in Constrained Environments. In *ACM Transactions of Privacy and Security Journal* (TOPS), Volume 25, Issue 4, pages 1-34, July 2022

[28] Lisa Oakley*, Alina Oprea, and Stavros Tripakis. Adversarial Robustness Verification and Attack Synthesis in Stochastic Systems. In *Proceedings of the 35th IEEE Computer Security Foundations Symposium* (CSF), 2022.

[29] Matthew Jagielski*, Giorgio Severi*, Niklas Pousette-Harger†, and Alina Oprea. Subpopulation Data Poisoning Attacks. In *Proceedings of the ACM Conference on Computer and Communications Security* (CCS), 2021.

[30] Xianrui Meng, Dimitrios Papadopoulos, Alina Oprea, and Nikos Triandopoulos. Private Hierarchical Clustering and Efficient Approximation. In *Proceedings of the Cloud Computing Security Workshop* (CCSW), 2021.

[31] Sridhar Venkatesan, Harshvardhan Sikka, Rauf Izmailov, Ritu Chadha, Alina Oprea, and Michael J. De Lucia. Poisoning Attacks and Data Sanitization Mitigations for Machine Learning Models in Network Intrusion Detection Systems. In *Proceedings of the Military Communications Conference* (MILCOM), 2021.

[32] Talha Ongun*, Oliver Spohngellert*, Benjamin Miller, Simona Boboila, Alina Oprea, Tina Eliassi-Rad, Jason Hiser, Alastair Nottingham, Jack Davidson, and Malathi Veeraraghavan. PORTFILER: Port-Level Network Profiling for Self-Propagating Malware Detection. In *Proceedings of the IEEE Conference on Communications and Network Security* (CNS), 2021.

[33] Talha Ongun*, Jay Stokes, Jonathan Bar Or, Ke Tian, Farid Tajaddodianfar, Joshua Neil, Christian Seifert, Alina Oprea, John Platt. Living-Off-The-Land Command Detection Using Active Learning. In *Proceedings of the 24th International Symposium on Research in Attacks, Intrusions and Defenses* (RAID), 2021.

[34] Giorgio Severi*, Jim Meyer, Scott Coull, and Alina Oprea. Explanation-Guided Backdoor Poisoning Attacks Against Malware Classifiers. In *Proceedings of the USENIX Security Symposium*, 2021.

[35] Nicholas Carlini, Florian Tramèr, Eric Wallace, Matthew Jagielski*, Ariel Herbert-Voss, Katherine Lee, Adam Roberts, Tom Brown, Dawn Song, Úlfar Erlingsson, Alina Oprea, and Colin Raffel. Extracting Training Data from Large Language Models. In *Proceedings of the USENIX Security Symposium*, 2021.

[36] Jialin Wen, Benjamin Zi Hao Zhao, Minhui Xue, Alina Oprea, and Haifeng Qian. With Great Dispersion Comes Greater Resilience: Efficient Poisoning Attacks and Defenses for Linear Regression Models. In *ACM Transactions on Information Forensics and Security Journal* (TIFS), Volume 16, pages 3709 - 3723, 2021.

[37] Matthew Jagielski* and Alina Oprea. Does Differential Privacy Defeat Data Poisoning? In *Distributed and Private Machine Learning (DPML) Workshop at International Conference on Learning Representations (ICLR)*, 2021.

[38] Talha Ongun*, Simona Boboila, Alina Oprea, Tina Eliassi-Rad, Alastair Nottingham, Jason Hiser, and Jack Davidson. Collaborative Information Sharing for ML-Based Threat Detection. In *AI/ML for Cybersecurity Workshop at SIAM International Conference on Data Mining (SDM)*, 2021.

[39] Molly Buchanan, Jeffrey W. Collyer, Jack W. Davidson, Saikat Dey, Mark Gardner, Jason D. Hiser, Jeffry Lang, Alastair Nottingham, and Alina Oprea. On Generating and Labeling Network Traffic with Realistic, Self-Propagating Malware. In *AI/ML for Cybersecurity Workshop at SIAM International Conference on Data Mining (SDM)*, 2021.

[40] Matthew Jagielski*, Jonathan Ullman, and Alina Oprea. Auditing Differentially Private Machine Learning: How Private is Private SGD? In *Proceedings of the 34th Conference on Neural Information Processing Systems* (NeurIPS), 2020

[41] Lisa Oakley*, Alina Oprea, and Stavros Tripakis. Adversarial Robustness of AI Agents Acting in Probabilistic Environments. In *Workshop on Foundations of Computer Security* (FCS), 2020

[42] Ahmet Buyukkayhan, Can Gemicioglu, Tobias Lauinger, Alina Oprea, William Robertson, and Engin Kirda. What's in an Exploit? An Empirical Analysis of Reflected XSS Exploitation Techniques. In *Proceedings of the Recent Advances in Intrusion Detection Conference* (RAID), 2020.

[43] Indranil Jana* and Alina Oprea. AppMine: Behavioral Analytics for Web Application Vulnerability Detection. In *Proceedings of the Cloud Computing Security Workshop* (CCSW), 2019.

[44] Lisa Oakley† and Alina Oprea. QFlip: An adaptive reinforcement learning strategy for the FlipIt security game. In *Proceedings of the Conference on Decision and Game Theory for Security* (GameSec), 2019.

[45] Ambra Demontis, Marco Melis, Maura Pintor, Matthew Jagielski*, Battista Biggio, Alina Oprea, Cristina Nita-Rotaru, and Fabio Roli. Why Do Adversarial Attacks Transfer? Explaining Transferability of Evasion and Poisoning Attacks. In *Proceedings of the USENIX Security Symposium*, 2019.

[46] Matthew Jagielski*, Michael Kearns, Jieming Mao, Alina Oprea, Aaron Roth, Saeed Sharifi-Malvajerdi, and Jonathan Ullman. Differentially Private Fair Learning. In *Proceedings of the International Conference on Machine Learning* (ICML), 2019.

[47] Alesia Chernikova*, Matthew Jagielski*, Alina Oprea, Cristina Nita-Rotaru, and BaekGyu Kim. Are Self-Driving Cars Secure? Evasion Attacks against Deep Neural Networks for Self-Driving Cars. In *Proceedings of the IEEE Workshop on the Internet of Safe Things*, 2019.

[48] Jiayi Duan, Ziheng Zeng, Alina Oprea, and Shobha Vasudevan. Automated Generation and Selection of Interpretable Features for Enterprise Security. In *Proceedings of the IEEE International Conference on Big Data*, 2018.

[49] Alina Oprea, Zhou Li, Kevin Bowers, and Robin Norris. MADE: Security Analytics for Enterprise Threat Detection. In *Proceedings of the Annual Computer Security Applications Conference* (ACSAC), 2018.

[50] Matthew Jagielski*, Alina Oprea, Battista Biggio, Chang Liu, Cristina Nita-Rotaru, and Bo Li. Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning. In *Proceedings of the IEEE Symposium on Security and Privacy* (S&P), 2018.

[51] Trishita Tiwari, Ata Turk, Alina Oprea, Katzalin Olcoz, and Ayse K. Coskun. User-Profile-Based Analytics for Detecting Cloud Security Breaches. In *Proceedings of the 4th International Workshop on Privacy and Security of Big Data* (PSBD), 2017.

[52] Chang Liu, Bo Li, Yevgeniy Vorobeychik, and Alina Oprea. Robust Linear Regression Against Training Data Poisoning. In *Proceedings of the ACM Workshop on Artificial Intelligence and Security* (AISEC), 2017.

[53] Ahmet Buyukkayhan‡, Alina Oprea, Zhou Li, and William Robertson. Lens on the Endpoint: Hunting for Malicious Software through Endpoint Data Analysis. In *Proceedings of the Recent Advances in Intrusion Detection Conference* (RAID), 2017.

[54] Alina Oprea, Ata Turk, Cristina Nita-Rotaru, and Orran Krieger. MOSAIC: A Platform for Monitoring and Security Analytics in Public Clouds. In *First IEEE Cybersecurity Development Conference* (SecDev), 2016. Short paper.

[55] Zhou Li and Alina Oprea. Operational Security Log Analytics for Enterprise Breach Detection. In *Proceedings of the First IEEE Cybersecurity Development Conference* (SecDev), 2016.

[56] Sumayah Alrwais‡, Kan Yuan, Eihal Alowaisheq, Xiaojing Liao, Alina Oprea, Xiaofeng Wang, and Zhou Li. Catching Predators at Watering Holes: Finding and Understanding Strategically Compromised Websites. In *Proceedings of the Annual Computer Security Applications Conference* (ACSAC), 2016.

[57] Alina Oprea, Zhou Li, Ting-Fang Yen, Sang H. Chin, and Sumayah Alrwais‡. Detection of Early-Stage Enterprise Infection by Mining Large-Scale Log Data. In *Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks* (DSN), 2015.

[58] Ting-Fang Yen, Victor Heorhiadi‡, Alina Oprea, Michael K. Reiter, and Ari Juels. An Epidemiological Study of Malware Encounters in a Large Enterprise. In *Proceedings of the 21st ACM Conference on Computer and Communications Security* (CCS), 2014.

[59] Marten van Dijk, Ari Juels, Alina Oprea, and Ronald L. Rivest. FlipIt: The Game of Stealthy Takeover. In *Journal of Cryptology*, Volume 26, Issue 4, pages 655-713, 2013.

[60] Ari Juels and Alina Oprea. New Approaches to Security and Availability for Cloud Data. In *Communications of the ACM*, Volume 56, Issue 2, pages 64-73, 2013.

[61] Ting-Fang Yen, Alina Oprea, Kaan Onarlioglu‡, Todd Leetham, William Robertson, Ari Juels, and Engin Kirda. Beehive: Large-Scale Log Analysis for Detecting Suspicious Activity in Enterprise Networks. In *Proceedings of the Annual Computer Security Applications Conference* (ACSAC), 2013.

[62] Jianqiang Luo, Kevin D. Bowers, Alina Oprea, and Lihao Xu. Efficient Implementation of Large Finite Fields GF(2^n) for Secure Storage Applications. In *ACM Transactions on Storage*, Volume 8, Issue 1, 2012.

[63] Marten van Dijk, Ari Juels, Alina Oprea, Ronald L. Rivest, Emil Stefanov‡, and Nikos Triandopoulos. Hourglass Schemes: How to Prove that Cloud Files are Encrypted. In *Proceedings of the 19th ACM Conference on Computer and Communications Security* (CCS), 2012.

[64] Emil Stefanov‡, Marten van Dijk, Alina Oprea, and Ari Juels. Iris: A Scalable Cloud File System with Efficient Integrity Checks. In *Proceedings of the Annual Computer Security Applications Conference* (ACSAC), 2012.

[65] Kevin D. Bowers, Marten van Dijk, Robert Griffin, Ari Juels, Alina Oprea, Ronald L. Rivest, and Nikos Triandopoulos. Defending Against the Unknown Enemy: Applying FlipIt to System Security. In *Proceedings of the Conference on Decision and Game Theory for Security* (GameSec), 2012.

[66] George Amvrosiadis, Bianca Schroeder, and Alina Oprea. Practical Scrubbing: Getting to the Bad Sector at the Right Time. In *Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks* (DSN), 2012.

[67] Kevin D. Bowers, Marten van Dijk, Ari Juels, Alina Oprea, and Ronald L. Rivest. How to Tell if Your Cloud Files Are Vulnerable to Drive Crashes. In *Proceedings of the 16th ACM Conference on Computer and Communications Security* (CCS), 2011.

[68] Yinqian Zhang[‡], Ari Juels, Alina Oprea, and Michael K. Reiter. HomeAlone: Co-Residency Detection in the Cloud via Side-Channel Analysis. In *Proceedings of the 32nd IEEE Symposium on Security and Privacy* (S&P), 2011.

[69] Alina Oprea and Ari Juels. A Clean-Slate Look at Disk Scrubbing. In *Proceedings of the 8th USENIX Conference on File and Storage Technologies* (FAST), 2010.

[70] Kevin Bowers, Ari Juels, and Alina Oprea. HAIL: A High-Availability and Integrity Layer for Cloud Storage. In *Proceedings of the 16th ACM Conference on Computer and Communications Security* (CCS), 2009.

[71] Kevin Bowers, Ari Juels, and Alina Oprea. Proofs of Retrievability: Theory and Implementation. In *Proceedings of the ACM Cloud Computing Security Workshop* (CCSW), 2009.

[72] Alina Oprea and Kevin Bowers. Authentic Time-Stamps for Archival Storage. In *Proceedings of the 14th European Symposium on Research in Computer Security* (ESORICS), 2009.

[73] Alina Oprea and Michael K. Reiter. Integrity Checking in Cryptographic File Systems with Constant Trusted Storage. In *Proceedings of the 16th USENIX Security Symposium*, 2007.

[74] Alina Oprea and Michael K. Reiter. On Consistency of Encrypting Files. In *Proceedings of the 20th International Symposium on Distributed Computing* (DISC), 2006.

[75] Michael Backes, Christian Cachin, and Alina Oprea. Secure Key-Updating for Lazy Revocation. In *Proceedings of the 11th European Symposium On Research In Computer Security* (ESORICS), 2006.

[76] Michael Backes, Christian Cachin, and Alina Oprea. Lazy Revocation in Cryptographic File Systems. In *Proceedings 3rd IEEE Security in Storage Workhsop*, 2005.

[77] Alina Oprea, Michael K. Reiter, and Ke Yang. Space-Efficient Block Storage Integrity. In *Proceedings of the 12th Annual Network and Distributed System Security Symposium* (NDSS), 2005.

[78] Alina Oprea, Dirk Balfanz, Glenn Durfee, and Diana K. Smetters. Securing a Remote Terminal Application with a Mobile Trusted Device. In *Proceedings of the Annual Computer Security Applications Conference* (ACSAC), 2004.

[79] Lea Kissner, Alina Oprea, Michael K. Reiter, Dawn Song, and Ke Yang. Private Keyword-Based Push and Pull with Applications to Anonymous Communication. In *Proceedings of the 2nd Conference of Applied Cryptography and Network Security* (ACNS), 2004.

[80] Philip MacKenzie, Alina Oprea, and Michael K. Reiter. Automatic Generation of Two-Party Computations. In *Proceedings of the 10th ACM Conference on Computer and Communications Security* (CCS), 2003.

Theses:

[81] Alina Oprea. Efficient Cryptographic Techniques for Securing Storage Systems. *Ph.D. Thesis*, Computer Science Department, Carnegie Mellon University, Pittsburgh, PA, USA May 2007.

Other Publications:

[82] Apostol Vassilev, Alina Oprea, Alie Fordyce, and Hyrum Anderson. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. White Paper NIST AI 100-2 E2023, January 2024.

[83] Alina Oprea and Apostol Vassilev. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. White Paper NIST AI 100-2 E2023 draft, March 2023.

[84] Alina Oprea, Anoop Singhal, Apostol Vassilev. Poisoning Attacks Against Machine Learning: Can Machine Learning Be Trustworthy? In *IEEE Computer*, 2022.

[85] Timothy A Sakharov, Benjamin Miller, Talha Ongun,* Alina Oprea, Tina Eliassi-Rad. Detecting Self-Propagating Attacks in Cyber Networks. In *The International Conference on Network Science (NetSci'19), oral presentation*, 2019.

[86] Talha Ongun*, Alina Oprea, Cristina Nita-Rotaru, Mihai Christodorescu, and Negin Salajegheh. The House That Knows You: User Authentication Based on IoT Data. Poster in *ACM Conference on Computer and Communications Security* (CCS), 2018.

[87] Sam Curry, Bret Hartman, David P. Hunter, David Martin, Dennis R. Moreau, Alina Oprea, Uri Rivner, and Dana E. Wolf. Mobilizing Intelligent Security Operations for Advanced Persistent Threats. *RSA Security Brief*, February 2011.

Issued Patents

[1] Nikolaos Triandopoulos, Kevin Bowers, James Kelley‡, Alina Oprea, and Ronald Rivest. Methods and apparatus for private set membership using aggregation for reduced communications. US 10,635,824, 2020.

[2] Alina Oprea, Zhou Li, and Ahmet Buyukkayhan‡. Classifying software modules based on comparisons using a neighborhood distance metric. US 10,122,742, 2018.

[3] Andres Molina-Markham, Alina Oprea, and Kevin Bowers. Flexible Access Management Framework based on Measuring Application Usage Behavior. US 10,063,562, 2018.

[4] Ahmet Buyukkayhan‡, Zhou Li, Alina Oprea, and Martin Rosa. Classifying Potentially Malicious and Benign Software Modules through Similarity Analysis. US 9,998.484, 2018.

[5] Alina Oprea, Zhou Li, Robin Norris, and Kevin Bowers. Detection of Malicious Web Activity in Enterprise Computer Networks. US 9,838,407, 2017.

[6] Alina Oprea, Ting-Fang Yen, Viktor Heorhiadi‡, Michael K. Reiter, and Ari Juels. Determining Risk of Malware Infection in Enterprise Hosts. US 9,674,210, 2017.

[7] Alina Oprea, Zhou Li, Sang H. Chin, and Ting-Fang Yen. Detection of Suspicious Domains through Graph Inference Algorithm Processing of Host-Domain Contacts. US 9,635,049, 2017.

[8] Alina Oprea, Sumayah Alrwais‡, Kevin D. Bowers, Todd Leetham, Zhou Li, and Ronald L. Rivest. Detecting Malicious Websites. US 9,621,576, 2017.

[9] Ting-Fang Yen, Alina Oprea, Kaan Onarlioglu‡, Todd Leetham, William Robertson, Ari Juels, and Engin Kirda. Behavioral Detection of Suspicious Host Activities in an Enterprise. US 9,516,039, 2017.

[10] Ting-Fang Yen, Alina Oprea, and Kaan Onarlioglu‡. Detecting Suspicious Web Traffic from an Enterprise Network. US 9,503,468, 2017

[11] Ari Juels, Marten van Dijk, Alina Oprea, and Ronald L. Rivest. Scheduling of Defensive Security Actions in Information Processing Systems. US 9,471,777, 2017.

[12] Ting-Fang Yen, Ari Juels, Kaan Onarlioglu‡, and Alina Oprea. Time Sanitization of Network Logs from a Geographically Distributed Computer System. US 9,430,501, 2016.

[13] Ting-Fang Yen, Ari Juels, Aditya Kuppa, Kaan Onarlioglu‡, and Alina Oprea. Anomaly Sensor Framework for Detecting Advanced Persistent Threat Attacks. US 9,378,361, 2016.

[14] Alina Oprea and Ting-Fang Yen. Modeling User Working Time using Authentication Events within an Enterprise Network. US 9,338,187, 2016.

[15] Alina Oprea, Kevin D. Bowers, Nikos Triandopoulos, Ting-Fang Yen, and Ari Juels. Credential Recovery with the Assistance of Trusted Entities. US 9,256,725, 2016.

[16] Ting-Fang Yen and Alina Oprea. Identifying Suspicious User Logins in Enterprise Networks. US 9,231,962, 2016.

[17] Ari Juels, Kevin D. Bowers, and Alina Oprea. Distributed Storage System With Efficient Handling Of File Updates. US 8,984,384, 2015.

[18] Ting-Fang Yen, Alina Oprea, and Kaan Onarlioglu‡. Detecting Suspicious Web Traffic From An Enterprise Network. US 9,049,221, 2015.

[19] Marten Van Dijk, Samuel J. Curry, Robert D. Hopley, John G. Linn, Alina Oprea, and Kenneth Ray. Methods And Apparatus For Mediating Access To Derivatives Of Sensitive Data. US 8,978,159, 2015.

[20] Ari Juels, Alina Oprea, Michael K. Reiter, and Yinqian Zhang‡. Co-Residency Detection In A Cloud-Based System. US 9,009,385, 2015.

[21] Kevin Bowers, Marten van Dijk, Ari Juels, Alina Oprea, Ronald L. Rivest, and Nikos Triandopoulos. Graph-based Approach to Deterring Persistent Security Threats. US 8,813,234, 2014.

[22] Emil Stefanov‡, Marten van Dijk, Alina Oprea, and Ari Juels. Remote Verification of File Protections for Cloud Data Storage. US 8,799,334, 2014.

[23] Magnus Nystrom, Alina Oprea, and Adam Back. Controlling Access to Data within Encrypted Copies of Files using Salt Parameters. US 8,751,804, 2014.

[24] Emil Stefanov‡, Marten van Dijk, Alina Oprea, and Ari Juels. Scalable Cloud File System with Efficient Integrity Checks. US 8,706,701, 2014 and 9,323,765, 2016.

[25] Alina Oprea, Yinqian Zhang‡, Vijay Ganti, John P. Field, Ari Juels, and Michael K. Reiter. Security Policy Enforcement Framework for Cloud-based Information Processing Systems. US 8,689,282, 2014.

[26] Ari Juels and Alina Oprea. Counter-based Encryption of Stored Data Blocks. US 8,635,465, 2014.

[27] Alina Oprea. Authentic Time-Stamping for Archival Storage. US 8,510,566, 2013.

[28] Ari Juels, Burton S. Kaliski Jr., Kevin Bowers, and Alina Oprea. Proof of Retrievability for Archived Files. US 8,381,062, 2013.

[29] Ari Juels, Marten van Dijk, Alina Oprea, Ronald Rivest, and Emil Stefanov‡. Remote Verification of File Protections for Cloud Data Storage. US 8,346,742, 2013.

[30] Kevin Bowers, Ari Juels, and Alina Oprea. Distributed Storage System with Enhanced Security. US 8,132,073, 2012.

Teaching Experience

- *CS 4973 / CS 6983: Trustworthy Generative AI* Fall 2024
- *CS 7775: Seminar in Computer Security* Fall 2023

  Graduate-level seminar course on trustworthy AI.
- *CY 7790: Machine Learning Security and Privacy* Fall 2021

  Graduate-level special topics class on the security and privacy of machine learning.
- *CY 2550: Foundations of Cybersecurity* Spring 2020

  Introductory cyber security course for undergraduates in the Computer Science and Cyber Security programs.
- *DS 5220: Supervised Machine Learning and Learning Theory* Fall 2019

  Core MS-level class for Data Science program.
- *DS 4400: Machine Learning and Data Mining I* Fall 2018, Spring 2019, Fall 2020, Spring 2021, Spring 2022

  Designed undergraduate class on machine learning and data mining.
- *CS 4770/CS 6750: Cryptography* Spring 2017, 2018

  Designed cross-listed undergraduate and graduate class on applied cryptography.
- *CS 7775: Seminar in Computer Security* Fall 2016

  Introduced new graduate-level class on the topic of *security analytics*, the application of machine learning in cybersecurity.

Grants

- *Multi-Agent Reinforcement Learning Cyber Defense for Securing Cloud Computing Platforms*

  Sponsor: Amazon

  Investigators: Alina Oprea and Chris Amato

  Funding: $80,000

- *SaTC: TTP: Small: Poisoning-Resilient Machine Learning Models for Threat Detection* 2024-2027

  Sponsor: NSF

  Investigators: Alina Oprea, Simona Boboila (Northeastern), Rauf Izmailov, Sridhar Venkatesan (Peraton Labs)

  Funding: $524,981

- *Adaptive Hierarchical Game-Theoretic RL Training for Cyber Network Defense* 2023-2027

  Sponsor: DARPA

  Investigators: Alina Oprea (PI at Northeastern) and Peter Chin (PI at Darmouth)

  Funding: $1,416,063

- *NeTS: Medium: Resilient-by-Design Data-Driven NextG Open Radio Access Networks* 2023-2026

  Sponsor: NSF

  Investigators: Francesco Restuccia, Tommaso Melodia, and Alina Oprea

  Funding: $900,000

- *SaTC: CORE: Small: Auditing Private Statistical and Machine Learning Algorithms: Theory and Practice* 2023-2026

  Sponsor: NSF

  Investigators: Alina Oprea (PI) and Jonathan Ullman

  Funding: $600,000

- *Backdoor Poisoning Attacks for Network Traffic Classifiers* 2022-2023

  Sponsor: MIT Lincoln Laboratory

  Investigators: Alina Oprea

  Funding: $167,147

- *AutoCoMBOT: Autonomy in Cyberspace through Robot Learning and Man-Bot Teaming* 2021-2024

  Sponsor: ARO

  Investigators: Tina Eliassi-Rad, Cristina Nita-Rotaru, and Alina Oprea.

  Funding: $1,454,369

- *SaTC: CORE: Small Foundations for the Next Generation of Private Learning Systems* 2021-2022
  Sponsor: NSF
  Investigators: Jonathan Ullman and Alina Oprea
  Funding: $200,000

- *Supplement to MACRO: Models for Enabling Continuous Reconfigurability of Secure Missions: Robustness to Adversarial Manipulation in Cyber Networks* 2020-2022
  Sponsor: ARL
  Investigators: Tina Eliassi-Rad and Alina Oprea
  Funding: $762,992

- *MACRO: Models for Enabling Continuous Reconfigurability of Secure Missions: Robustness to Adversarial Manipulation in Cyber Networks* 2018-2023
  Sponsor: ARL
  Investigators: Tina Eliassi-Rad and Alina Oprea
  Funding: $1,725,884

- *P-CORE: Privacy-Enhanced Coordinated Enterprise Defense via Temporal and Topological Representation Learning* 2018-2022
  Sponsor: DARPA
  Investigators: Alina Oprea (PI for Northeastern) and Tina Eliassi-Rad
  Funding: $1,249,850

- *Security Analytics* 2018-2022
  Sponsor: PricewaterhouseCoopers (PwC), $244,152
  Investigators: Tina Eliassi-Rad and Alina Oprea

- *SaTC: CORE: Small: Collaborative: An Integrated Approach for Enterprise Intrusion Resilience* 2017-2021
  Sponsor: NSF
  Investigators: Alina Oprea (PI for Northeastern) and Nikos Triandopoulos (Stevens Institute of Technology)
  Funding: $257,832 (Northeastern part)

- *Privacy-Preserving Assessment of Trust (PPAT)* 2017

Sponsor: DARPA

Investigator: Alina Oprea

Funding: $75,000

- *Microsoft Red Team AI Residency Program* 2021

Sponsor: Microsoft

Investigator: Alina Oprea

Funding: $75,000

- *Auditing Differentially Private Machine Learning* 2020

Sponsor: Apple

Investigators: Jonathan Ullman and Alina Oprea

Funding: $98,899

- *Security of Malware Classifiers* 2020

Sponsor: FireEye

Investigator: Alina Oprea

Funding: $37,697

- *Automated Cyber Defense* 2019

Sponsor: Google

Investigators: Cristina Nita-Rotaru, Alina Oprea, and William Robertson

Funding: $100,000

- *AppMine: Deep Learning Behavioral Analytics for Application Threat Detection* 2018

Sponsor: Cisco

Investigator: Alina Oprea

Funding: $84,741

- *Evasion and Poisoning Attacks for Neural Networks* 2018

Sponsor: Toyota ITC

Investigators: Cristina Nita-Rotaru and Alina Oprea

Funding: $70,000

- *Behavioral Authentication for IoT Clients with Applications to Payment Systems* 2017

Sponsor: Visa Research

Investigators: Cristina Nita-Rotaru and Alina Oprea

Funding: $75,000

Invited Talks

Security and Privacy Risks in AI Systems

– Invited talk at the Cloud Security Alliance (CSA) AI Virtual Summit, January 2025

Training Secure Agents: Is Reinforcement Learning Vulnerable to Poisoning Attacks?

– Keynote at the Adversarial ML Frontiers Workshop at NeurIPS, 2024

On the Security and Privacy Risks of Generative AI Systems

– Keynote at the 9th IEEE European Symposium on Security and Privacy, July 2024

– Keynote at the 17th ACM Workshop on Artificial Intelligence and Security (AISec), October 2024

Privacy Risks and Mitigations in Generative AI Systems

– Invited talk at the J.P. Morgan Chase Data Privacy Week, January 2024

Privacy Attacks in Machine Learning

– Invited talk at the EPFL Summer Research Institute (SuRI), July 2023

On the Connection between Integrity and Privacy Attacks in Adversarial Machine Learning

– Invited talk at the MPI-SWS Research Symposium, March 2023

Resilient Collaborative AI for Cyber Defense

– Keynote at the 5th Deep Learning and Security (DLS) Workshop co-located with the IEEE Security and Privacy Symposium, May 2022

Auditing Differentially Private Machine Learning

– Invited talk at the Microsoft Research Summit, October 2021

– Invited talk at the Apple Privacy workshop, April 2022

Machine Learning Integrity and Privacy in Adversarial Environments

– Invited talk at the Alan Turing Institute, March 2021

– Keynote at the ACM Symposium on Access Control Models and Technologies (SACMAT), 2021

Machine Learning Integrity in Adversarial Environments

– Invited talk at the Security and Safety in Machine Learning Systems Workshop co-located with the International Conference on Learning Representations (ICLR) conference, 2021

– Invited talk at the Microsoft Research, Cryptography and Privacy Colloquium, July 2021

Towards Resilient Machine Learning in Adversarial Environments

– Keynote at the DYnamic and Novel Advances in Machine Learning and Intelligent Cyber Security (DYNAMICS) Workshop at the Annual Computer Security Applications Conference (ACSAC), 2020

– Invited talk at the Recent Advances in Artificial Intelligence for National Security (RAINNS) Workshop at MIT Lincoln Lab, 2020

– Invited talk at the Pacific Northwest National Laboratory MARS Seminar Series, August 2020

– Distinguished Lecture at the University of Virginia, Computer Science Department, November 2019

Resilient Machine Learning in Adversarial Environments

– Invited talk at the Workshop on Aviation Security, Northeastern University, Boston, November 2019

– Invited talk at Adversarial Machine Learning Technical Exchange Meeting organized by NIST and MITRE, September 2019

AI and Cybersecurity: Applications, Challenges, and Future Directions

– Invited talk at Amazon AWS Cambridge, MA, July 2019

AI in Cybersecurity: Current Applications and Future Directions

– Invited talk at the Cyber Security and Information Assurance Interagency Working Group (CSIA IWG), May 2019

AI in Cybersecurity: Applications, Open Problems, and Future Directions

– Keynote talk at RISE-Ericsson Security Day, Stockholm, October 2019

– Keynote at the Annual Computer Security Applications Conference (ACSAC), 2018

Adversarial Poisoning Attacks and Defenses in Machine Learning Systems

– Third ARO Adversarial Machine Learning Workshop, UT Dallas, November 2018

Resilient Machine Learning in Cyber Security

– Second International Conference on Recent Advances in Artificial Intelligence (RAAI), Bucharest, Romania, June 2018

Resilient Machine Learning in the Real World

– MIT Lincoln Lab, CORE Seminar Series, November 2017

MOSAIC: A Platform for Monitoring and Security Analytics in Public Clouds

– Massachusetts Open Cloud Annual Workshop, Boston University, December 2016

Proactive Breach Detection with Security Analytics

– CyberSEED conference, University of Connecticut, October 2016

– Tufts University CS Colloquium, November 2016

– BBN, December 2016

Applications of Machine Learning in Security

– Workshop on Cybersecurity Applications of Big Data, Boston University, January 2016

Analytics-Based Security Service for the MOC

– Massachusetts Open Cloud (MOC) Annual Workshop, Boston University, November 2015

Protecting Cloud Infrastructures against Modern Attacks

– Secure Cloud Computing and Storage Workshop, Boston University, May 2015

– GREPSEC workshop for women in computer security research, May 2015

Detecting Advanced Threats by Mining Large-Scale Log Data

– New England Networking and Systems Day, Boston University, October 2014

Early-Stage APT Detection by Mining Large-Scale Log Data

– MIT Lincoln Laboratory, June 2014

Beehive: Large-Scale Log Analysis for Anomaly Detection in Enterprise Networks

– WPI security seminar, November 2013

– Guest lecture at UMass Boston course on computer forensics, December 2013

Lessons from the FlipIt game

– Workshop On Multi-Spectrum Metrics For Cyber Defense (WMMCD), MIT, October 2013

New Approaches for Securing Cloud Data

– Zurich Information Security Center (ZISC) Workshop, ETH Zurich, June 2012

– CDSP research workshop at Northeastern University, April 2012

– MIT security seminar, April 2012

HomeAlone: Co-residency Detection in the Cloud via Side-Channel Analysis

– MIT security seminar, March 2011

HAIL: A High Availability and Integrity Layer for Cloud Storage

– Guest lecture at cloud computing course at MIT, March 2011

– Microsoft Research Redmond Cryptography Colloquium, December 2009

– Crypto in the Clouds Workshop, MIT, August 2009

Authentic Time-Stamping for Archival Storage

– SNIA Technical Council and Board of Directors, EMC, USA August 2009

– Innovation Network Lecture Series sponsored by EMC Corporation, May 2009

Efficient Integrity Algorithms for Storage Systems

– SNIA Storage Security Summit, CMU, 2007

Student Supervision

PhD Students:

• Evan Rose	Since Fall 2023
• Ethan Rathbun	Since Fall 2023
• Georgios Syros, co-advised with Cristina Nita-Rotaru	Since Fall 2023
• John Abascal, co-advised with Jonathan Ullman	Since Fall 2021
• Harsh Chaudhari	Since Fall 2021
• Lisa Oakley	Since Fall 2020
• Giorgio Severi	Graduated Summer 2024
• Alesia Chernikova	Graduated May 2024
• Talha Ongun	Graduated May 2023
• Matthew Jagielski, co-advised with Cristina Nita-Rotaru	Graduated August 2021

MS Students:

• Aditya Vikram Singh	2024-2025
• Gokberk Yar, co-advised with Cristina Nita-Rotaru	2021-2023
• Alexander Gomez	2019-2020
• Indranil Jana	2017-2019
• Muazzam Asani	2017-2018
• Caleb Wastler, co-advised with Cristina Nita-Rotaru	2017-2018

Undergraduate Students:

- Nico Berrios, co-advised with Jonathan Ullman, Catholic University of Chile Summer 2024
- Andrew Yuan, co-advised with Cheng Tan, Northeastern Khoury January - June 2022
- Stanley Wu, co-advised with Jonathan Ullman, Northeastern Khoury Fall 2020, Spring 2021, Fall 2022
- Hava Kantrowitz, NSF REU Program Fall 2020
- Yuxuan Wang, Northeastern Khoury, Independent Research Study Fall 2019, 2020
- Niklas Pousette Harger, Northeastern Khoury, Independent Research Study Fall 2019
- Marina Moskowitz, Northeastern Khoury, Independent Research Study Fall 2019
- Oliver Spohngellert, Northeastern Khoury, Independent Research Study Spring 2019
- Lisa Oakley, Northeastern Khoury, Independent Research Study Fall 2018
- Diego Delgado, Northeastern ECE January - June 2017
- Gen Ohta, Northeastern ECE, Independent Research Study Fall 2016

PhD Thesis Committee:

- Hai Nguyen, Northeastern University Graduated: Summer 2023
- Bogdan Kulynych, EPFL Graduated: Summer 2023
- Seb Szyller, Aalto University Graduated: Summer 2023
- Avijit Ghosh, Northeastern University Graduated: Summer 2023
- Benjamin Miller, Northeastern University Graduated: Summer 2023
- Bahruz Jabiyev, Northeastern University Graduated: Spring 2023
- Ahmet Buyukkayhan, Northeastern University Graduated: Spring 2019
- Amirali Sanatinia, Northeastern University Graduated: Spring 2018
- Sevtap Duman, Northeastern University Graduated: Summer 2017
- Xianrui Meng, Boston University Graduated: Summer 2016

Professional Service

Editorial Boards

- Associate Editor for IEEE Security and Security Magazine 2021 - 2024
- Associate Editor for ACM Transactions on Privacy and Security (TOPS) 2014 - 2023
- Guest Editor for Special Issue on Machine Learning Security and Privacy November 2022
IEEE Security and Security Magazine

Conference Chairing

- IEEE Symposium on Security and Privacy, General Chair 2026
- IEEE Symposium on Security and Privacy, Vice Chair 2025
- IEEE Symposium on Security and Privacy, PC Co-Chair 2020, 2021
- NeurIPS 2019 Workshop on Robust AI in Financial Services, PC Co-Chair 2019
- Network and Distributed System Security Symposium (NDSS), PC Co-Chair 2018,2019
- ACM Cloud Computing Security Workshop (CCSW), PC Co-Chair 2014

Conference Steering Committees

- Network and Distributed System Security Symposium (NDSS) 2017 - 2022
- IEEE Symposium on Security and Privacy 2021 - present

Conference Program Committee Member

- ACM CCS 2025
- IEEE Conference on Secure and Trustworthy Machine Learning (SaTML) 2023, 2024
- Network and Distributed System Security Symposium (NDSS) 2013,2015,2016,2017
- USENIX Security Symposium 2017, 2018
- IEEE Symposium on Security and Privacy 2014,2015,2017,2019,2024
- Deep Learning and Security Workshop 2018
- Recent Advances in Intrusion Detection 2018
- IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 2016

• Annual Computer Security Applications Conference (ACSAC)	2015, 2016
• ACM SIGMETRICS	2014
• ACM Cloud Computing Security Workshop (CCSW)	2010 - 2013
• ACM Conference on Computer and Communications Security (CCS)	2012,2013,2017
• Conference on Decision and Game Theory for Security (GameSec)	2013
• International Conference on Distributed Computing Systems (ICDCS)	2009,2010,2013
• USENIX Workshop on Hot Topics in Storage and File Systems (HotStorage)	2011
• Applied Cryptography and Network Security Conference (ACNS)	2008,2010
• European Symposium on Research in Computer Security (ESORICS)	2009
• USENIX Conference on File and Storage Technologies (FAST)	2009
• International Workshop on Storage Security and Survivability (StorageSS)	2008

Academic Committees Member at Northeastern University

• Area Chair for Security and Systems	2024-2025
• Hiring Committee Co-Chair	2023-2024
• Hiring Committee	2020-2021
• PhD Admission Committee Co-Chair	2021-2022
• PhD Admission Committee	2016-2017, 2017-2018, 2018-2019
• PhD Curriculum Committee	2017-2018, 2018-2019, 2019-2020, 2020-2021
• Distinguished Lecture Committee	2018-2019, 2019-2020 (chair)