Teodora Baluta

teobaluta@gmail.com • https://teobaluta.github.io/

Updated on December 27, 2024

Latest CV here

ACADEMIC PROFILE

Georgia Institute of Technology, Atlanta, GA, USA — Sep 2024 – present
- Assistant Professor
  - School of Cybersecurity and Privacy, College of Computing

National University of Singapore, Singapore — 2017 – 2024
- Ph.D. in Computer Science
  - Advisers: Prateek Saxena and Kuldeep S. Meel.

Politehnica University of Bucharest, Romania
- M.Sc. in Computer Science — 2014 – 2016
  - Topic: Security of Complex Networks.
- B.Sc. in Computer Science — 2010 – 2014
  - Specialization: Compilers and Operating Systems.

HONORS & AWARDS

- **EECS Rising Stars**, Georgia Tech — 2023
- **Dean's Graduate Research Excellence Award**, National University of Singapore — 2023
- **Google PhD Fellowship**, Google — 2021 – 2023
- **Finalist for Microsoft Research Asia Fellowship**, Microsoft — 2021
- **President's Graduate Fellowship**, National University of Singapore — 2017 – 2021
- **Best Poster Award**, Research Week, National University of Singapore — 2019
- **Research Forum Award**, Deep Learning Security (DLS) Workshop — 2017
- **Merit Scholarship**, Politehnica University of Bucharest — 2011, 2013
  For attaining amongst top GPAs per semester.

PUBLICATIONS

[**PhD Thesis**] "Rigorous Security Analysis of Machine Learning Systems"
Teodora Baluta (2024).

[**NeurIPS24**] "Unlearning in-vs. out-of-distribution data in LLMs under gradient-based methods"
Teodora Baluta, Pascal Lamblin, Daniel Tarlow, Fabian Pedregosa, and Gintare Karolina Dziugaite. *NeurIPS Safe Generative AI Workshop*. 2024.

[**CCS23**] "Unforgeability in Stochastic Gradient Descent"
Teodora Baluta, Ivica Nikolic, Racchit Jain, Divesh Aggarwal, and Prateek Saxena. *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (**CCS**)*. 2023.

[**OOPSLA23**] "User-customizable Transpilation of Scripting Languages"
Bo Wang†, Aashish Kolluri, Ivica Nikolic, **Teodora Baluta**, and Prateek Saxena. *ACM SIGPLAN International Conference on Object-oriented programming systems, languages, and applications (**OOPSLA**)*. 2023.

[**SAT23**] "Explaining SAT Solving Using Causal Reasoning"
Jiong Yang†, Arijit Shaw, **Teodora Baluta**, Mate Soos, and Kuldeep S. Meel. *Proceedings of International Conference on Theory and Applications of Satisfiability Testing (**SAT**)*. 2023.

[**CCS22a**] "Membership Inference Attacks and Generalization: A Causal Perspective"
Teodora Baluta, Shiqi Shen, S Hitarth, Shruti Tople, and Prateek Saxena. *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (**CCS**)*. 2022.

[**CCS22b**] "LPGNet: Link Private Graph Networks for Node Classification"
Aashish Kolluri, **Teodora Baluta**, Bryan Hooi, and Prateek Saxena. *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (**CCS**)*. 2022.

[**ICSE21**] "Scalable Quantitative Verification For Deep Neural Networks"
Teodora Baluta, Zheng Leong Chua, Kuldeep S Meel, and Prateek Saxena. *Proceedings of the 43rd International Conference on Software Engineering (**ICSE**)*. 2021.

[**CCS21**] "Private hierarchical clustering in federated networks"
Aashish Kolluri, **Teodora Baluta**, and Prateek Saxena. *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (**CCS**)*. 2021.

[**ESEC/FSE21**] "SynGuar: guaranteeing generalization in programming by example"
Bo Wang†, **Teodora Baluta**, Aashish Kolluri, and Prateek Saxena. *Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering (**ESEC/FSE**)*. 2021.

[**CCS19**] "Quantitative verification of neural networks and its security applications"
Teodora Baluta, Shiqi Shen, Shweta Shinde, Kuldeep S Meel, and Prateek Saxena. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (**CCS**)*. 2019.

[**NDSS19**] "One Engine To Serve'em All: Inferring Taint Rules Without Architectural Semantics"
Zheng Leong Chua, Yanhao Wang, **Teodora Baluta**, Prateek Saxena, Zhenkai Liang, and Purui Su. *Proceedings of the Symposium on Network and Distributed System Security (**NDSS**)*. 2019.

[**WSC17**] "Modeling the effects of insider threats on cybersecurity of complex systems"
Teodora Baluta, Lavanya Ramapantulu, Yong Meng Teo, and Ee-Chien Chang. *Simulation Conference (**WSC**), 2017 Winter*. IEEE. 2017.

WORK EXPERIENCE

Research Intern, Google Brain, Montreal — 2022
- Hosts: Daniel Tarlow and Fabian Pedregosa.

Research Intern, National University of Singapore — 2016
- Advised by Yong Meng Teo.

Software Engineer, Intel — 2014 – 2016
Developed Linux device drivers for sensors, systems-level interface with Android, RFC for biometric sensors.

TEACHING

Assistant Professor, Georgia Institute of Technology
- Machine Learning Security (CS 4803/8803) — Spring 2025

Teaching Assistant, National University of Singapore
- Introduction to Computer Security (CS3231) — Spring 2018
- Systems Security (CS5231) — Fall 2018, Fall 2019

Teaching Assistant, Politehnica University of Bucharest, Local Area Networks — 2015

SERVICE

Reviewer
- IEEE Symposium on Security & Privacy (Oakland) 2025
- Neural Information Processing Systems (NeurIPS) 2021, 2022, 2024
- Deep Learning Security (DLS) Workshop 2022, 2023
- Privacy-Preserving Machine Learning (PPML) Workshop 2021

Sub-reviewer
- IEEE Symposium on Security & Privacy (Oakland) 2018, 2019
- USENIX Security Symposium (USENIX) 2019

Co-chair, Research Week, National University of Singapore — 2019

OTHER WORK EXPERIENCE

Mozilla Winter of Security Student Project, Mozilla — Oct 2015 – Feb 2016

Linux Kernel Developer Intern, Linux Foundation, Outreachy Program — Dec 2013 – Mar 2013