

# Teodora Baluta

teobaluta@gatech.edu • <https://teobaluta.github.io/>

Updated on November 29, 2025

[Latest CV here](#)

## ACADEMIC PROFILE

<b>Georgia Institute of Technology</b> , Atlanta, GA, USA	Sep 2024 – present
▪ Assistant Professor <ul style="list-style-type: none"><li>School of Cybersecurity and Privacy, College of Computing</li></ul>	
<b>National University of Singapore</b> , Singapore	2017 – 2024
▪ Ph.D. in Computer Science <ul style="list-style-type: none"><li>Advisers: Prateek Saxena and Kuldeep S. Meel.</li></ul>	
<b>Politehnica University of Bucharest</b> , Romania	
▪ M.Sc. in Computer Science <ul style="list-style-type: none"><li>Topic: Security of Complex Networks.</li></ul>	2014 – 2016
▪ B.Sc. in Computer Science <ul style="list-style-type: none"><li>Specialization: Compilers and Operating Systems.</li></ul>	2010 – 2014

## HONORS & AWARDS

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

## PUBLICATIONS

[ <a href="#">NeurIPS25</a> ]	“ <a href="#">Model Provenance Testing for Large Language Models</a> ” Ivica Nikolic, <b>Teodora Baluta</b> , and Prateek Saxena. <i>Advances in Neural Information Processing Systems (NeurIPS)</i> . 2025.
[ <a href="#">PhD Thesis</a> ]	“ <a href="#">Rigorous Security Analysis of Machine Learning Systems</a> ” <b>Teodora Baluta</b> (2024).
[ <a href="#">SafeGenAI24</a> ]	“ <a href="#">Unlearning in-vs. out-of-distribution data in LLMs under gradient-based methods</a> ” <b>Teodora Baluta</b> , Pascal Lamblin, Daniel Tarlow, Fabian Pedregosa, and Gintare Karolina Dziugaite. <i>NeurIPS Safe Generative AI Workshop</i> . 2024.
[ <a href="#">CCS23</a> ]	“ <a href="#">Unforgeability in Stochastic Gradient Descent</a> ” <b>Teodora Baluta</b> , Ivica Nikolic, Racchit Jain, Divesh Aggarwal, and Prateek Saxena. <i>Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS)</i> . 2023.
[ <a href="#">OOPSLA23</a> ]	“ <a href="#">User-customizable Transpilation of Scripting Languages</a> ” Bo Wang <sup>†</sup> , Aashish Kolluri, Ivica Nikolic, <b>Teodora Baluta</b> , and Prateek Saxena. <i>ACM SIGPLAN International Conference on Object-oriented programming systems, languages, and applications (OOPSLA)</i> . 2023.
[ <a href="#">SAT23</a> ]	“ <a href="#">Explaining SAT Solving Using Causal Reasoning</a> ” Jiong Yang <sup>†</sup> , Arijit Shaw, <b>Teodora Baluta</b> , Mate Soos, and Kuldeep S. Meel. <i>Proceedings of International Conference on Theory and Applications of Satisfiability Testing (SAT)</i> . 2023.
[ <a href="#">CCS22a</a> ]	“ <a href="#">Membership Inference Attacks and Generalization: A Causal Perspective</a> ” <b>Teodora Baluta</b> , Shiqi Shen, S Hitarth, Shruti Tople, and Prateek Saxena. <i>Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS)</i> . 2022.
[ <a href="#">CCS22b</a> ]	“ <a href="#">LPGNet: Link Private Graph Networks for Node Classification</a> ” Aashish Kolluri, <b>Teodora Baluta</b> , Bryan Hooi, and Prateek Saxena. <i>Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS)</i> . 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<sup>†</sup>, **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 and Fall 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

- Program Committee**  
  - IEEE Symposium on Security and Privacy (S&P) 2025, 2026
  - Annual Computer Security Applications Conference (ACSAC) 2025
  - IEEE European Symposium on Security and Privacy (Euro S&P) 2026
  - International Conference on Learning Representations (ICLR) 2026
  - International Parallel and Distributed Processing Symposium (IPDPS) 2026, ML/AI Track**Georgia Tech Committee Service**  
  - School of Cybersecurity and Privacy Graduate Committee (2025, 2026)**Reviewer & sub-reviewer**  
  - 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 (S&P) 2018, 2019
  - (Sub-reviewer) USENIX Security Symposium (USENIX) 2019