TEACHING STATEMENT

Teodora Baluta
Ph.D. Candidate at National University of Singapore, Singapore
https://teobaluta.github.io

I believe that my foremost role as an educator is to inspire students to engage with the material beyond the surface level. Can we teach students to think critically and creatively about the world? Can we teach students how to synthesize information and learn in an ever-evolving technological landscape? My core approach is to combine fundamental concepts with the students' personal goals and passions such that students become life-long learners, critical thinkers and creative tinkerers.

Teaching Experience

Undegraduate Introductory Security Courses. My most significant teaching experience comes from being a teaching assistant (TA) during my Ph.D. for an undergraduate-level (approximately 180-student) course. The course introduced several computer security topics such as cryptography, systems security and network security. My TA responsibilities included preparing a set of materials on introductory cryptography topics, co-developing assignments on binary analysis, creating exam questions and grading. The tutorials I gave were a mix between recitation, white-board teaching, and hands-on exercises. The materials I created served as a basis for future iterations of the module. My slides and notes on introductory topics in cryptography had examples and exercises which explained topics such as the one-time pad, hash functions, digital signatures, and key exchange. The hands-on assignments I co-developed were structured similar to capture-the-flag contests, where students were expected to exploit certain vulnerabilities such as buffer overflows, or format string attacks in binaries to obtain the secret flags.

Graduate-level Security Courses. I also TAed for two semesters for a graduate-level course that focused on systems security topics. This included security analysis techniques such as fuzzing, taint analysis, and static/dynamic program analysis at the binary and source-code level. I helped develop and grade the final projects. Thus, I am also comfortable in teaching program analysis and formal methods courses. On the security for ML systems, I have contributed to creating course materials. I worked with an undergraduate student who was doing a final year project on adversarial robustness. The goal of the assignment was to create adversarial examples for a sequence of frames, e.g., closer to the threat model of an ML vision component in a self-driving car. This assignment has been used in graduate courses for ML security.

Diversity in Teaching. My teaching experience is diverse, and my interest in sharing knowledge started prior to my Ph.D. I was a TA for a Networking module at the undergraduate level in Politehnica University of Bucharest, where I conducted tutorials. I also taught children aged 8–14 programming skills for a 7-week course using Scratch and JavaScript, where I created weekly tutorials and assignments. During my undergraduate, I was also involved in a summer school for high-school teachers on how to use technologies effectively in their teaching.

My teaching aims to combine hands-on experience in order to ground theoretical concepts. Students benefit from a good balance between attack-oriented knowledge to break a particular system and formal models for reasoning about security. Another aspect that makes security exciting to teach is that it touches upon many topics in computer science. I noticed that students appreciate when we connect the dots between many aspects of security that go into building real-world applications.

Developing a Graduate-level Course: Rigorous Security for ML Systems

I am most interested in teaching courses in computer security and formal methods both at the undergraduate and graduate levels. I am particularly excited to develop a graduate course on machine learning security. I seek to develop a course on machine learning security that tackles the challenges in the field from *foundational aspects*. My aim is to equip students with the necessary tools to apply security analysis in this new field. I would like to make this module a mix of systems and theory/formal analysis, and critically analyze the "what", not just the "how". The learning objectives of this module is to: (1) establish what formal properties of ML systems are relevent to security and privacy; (2) how tractable are they to check, either exploit or verify, and (3) what are the applications where these properties are important.

The course would introduce security definitions and threat models for machine learning systems, in order to cover the first learning objective (1). For instance, I would start with the decade-old problem of adversarial robustness for which we have a number of verification and testing techniques, so (2) as well. This gives an opportunity to go into techniques such as branch-and-bound algorithms, abstract interpretation

and quantitative verification. Here, more hands-on assignments can be designed around these techniques. The next lecture would consider more setups where other types of robustness are important, i.e., byzantine gradient robustness. The next big set of properties are around privacy leakages in both federated and centralized setup, e.g., around topics of inverting gradients, and forgeability of stochastic gradient descent. Students have the option here as well for practical assignments for evaluating the leakage using some of the existing work, or develop new techniques for these applications. Finally, I would discuss causality as a tool to disentangle generalization from memorization, teaching both causality at the feature learning, i.e., causal learning, as well as at the level of the distribution. These are some of the key topics I shall conver.

Advising and Mentoring: a Two-way Street

As a PhD student, I have worked with a variety of students, including junior Ph.D. students, master's students, and even undergraduate students on research projects. Several publications have resulted from these collaborations, and several students I have worked with have pursued further graduate studies. I feel that mentoring is a two-way street: I feel grateful, fulfilled, and proud to see them succeed. I learn a lot from these experiences, and enjoy collaborating with diverse people. This is also partly why I find academia is such a meaningful career for me. I include below a list of people that have enriched my Ph.D. studies:

- I collaborated with Bo Wang (Ph.D. student) on algorithms that guarantee generalizable program synthesis, and customizable cross-language code translation. These two projects resulted in two publications at ESEC/FSE and OOPSLA.
- I collaborated with Racchit Jain (Undergraduate, intern) while he was still an undergraduate in his last year, and joined our lab as an intern. Together we shaped up his final year project, which was an analysis for a special case of unforgeability in stochastic gradient descent.
- I worked with Jiong Yang (Ph.D. student) and Arijit Shaw (Ph.D. student) on developing causal analysis to understand SAT solvers.
- I worked with S. Hitarth (Master's, intern) who did a remote research internship during his master's studies, during the pandemic. After his internship, he joined a Ph.D. program at Hong Kong University of Science and Technology (HKUST).
- I worked with Jonathan Chen (Undergraduate, NUS) on his Final Year Project. Jonathan developed several assignments that are currently being used for a graduate level course in machine learning security. Together with another Ph.D. candidate, we were developing a private federated social media platform. His final year project in 2021 was on designing social media functionality with end-to-end encryption, and privacy. Jonathan went on to work on computer security within DSO National Laboratories in Singapore.
- Alexandros Dimos (Undergraduate, intern) - Alex was passionate about binary analysis, and we collaborated on a rule-based binary analysis tool, combining logic and learning. Our project won the best poster award at the Deep Learning Security (DLS) Workshop in 2017. Alex went on to pursue a master's at Vrije University, Amsterdam, which he completed in 2020. He is currently working as a software engineer at Meta.

Fostering Communities

I believe that one of the most important avenues for learning is within diverse and inclusive communities. Not only do students begin to have a sense of belonging, but they also learn essential collaborative skills, to think creatively about the world, and to have the autonomy to explore meaningful passion projects.

As an undegraduate student, I benefited from being in such a community. I was a member of the Romanian Open-source Education organization (ROSEdu) where I helped organize several outreach and educational events. I co-organized a summer school about contributing to open-source for first and second-year undegraduate students. Due to my involvement, I got interested in contributing to the Linux kernel, and became passionate about systems. I seek to encourage and establish such communities that connect the classroom materials with real systems.