Ying Meng

ymeng@email.sc.edu • meng2010.github.io/

Education

University of South Carolina

Ph.D. in Science in Computer Science, *Under the supervision of Dr. Pooyan Jamshidi* *01/2018 - 12/2022 (Expected)*

M.S. in Computer Software Science, *Under the supervision of Dr. Gregory Gay* *01/2015 - 12/2017*

Research Projects

Synthena: Synthesizing Dynamic Ensemble-Based Adversarial Defenses

Role: *lead researcher, developer* ***Supervisor:*** *Pooyan Jamshidi* *07/2020 - present*

- **Duty:** Lead the research work. Designed and developed Synthena — a framework for building and updating dynamic ensemble defense against various adversarial attacks. Designed and performed experimental study.

Athena: A Framework of Building Ensemble Defense against Adversarial Attacks

Role: *lead researcher, developer* ***Supervisor:*** *Pooyan Jamshidi* *06/2019 - present*

- **Duty:** Lead the research work. Designed and developed Athena — an infrastructure for building adversarial ensemble defense. Designed and performed experimental study. Implemented and trained weak defenses. Implemented various adversarial attacks on the top of Google Cleverhans and IBM ART, and then crafted adversarial examples. Implemented ensemble varieties and evaluated the realized ensembles against various adversarial attacks in the context of 3 different threat models: zero-knowledge, gray-box, and white-box threat models. Investigated and analyzed why Athena works. Open-sourced Athena: github.com/softsys4ai/athena

Comparison the Difference between the Human-Written Tests and the Automated Generation

Role: *researcher* ***Supervisor:*** *Gregory Gay* *06/2018 - present*

- **Duty:** Generated test data based on branch- and conditional-coverage criteria for each project under test (PUT). Generated (class-level and traditional) mutants as the malfunctioned varieties of each PUT. Set up experimental environments and performed experiments. Performed experiments and collected test results. Analyzed the collected data (over 200 GBs plain text). I was the only student researcher in this project.

Investigating on the impact of solver choice in model-based test generation

Role: *researcher* ***Supervisor:*** *Gregory Gay* *05/2018 - 11/2019*

- **Duty:** Generated mutants as malfunctioned varieties of the models (in Lustre) under test. Generated test obligations based various structural coverage criteria and then crafted test suites using a variety of solvers (CVC4, MathSat5, Yices2, and Z3), by solving the test obligations by the solvers respectively. Performed the experiment and analyzed the test results (over 5 GBs plain texts).

Investigating Faults Missed by Test Suites Achieving High Code Coverage

Role: *researcher* ***Supervisor:*** *Gregory Gay* *03/2018 - 08/2018*

- **Duty:** Generated (class-level and traditional) mutants as the malfunctioned varieties of the projects under test. Set up experimental environments and performed experiments. Performed experiments and collected test results. Analyzed the collected data (over 50 GBs plain text), examining how likely each type of auto-generated mutations are detected by human-written test cases. I was the only student researcher in this project.

Obligation Generator for Observed Structural Coverage Criteria

Role: *researcher, developer* ***Supervisor:*** *Gregory Gay* *03/2016 - 12/2017*

- **Duty:** Designed and developed a tool to extract observability from source code, then generated observability-based test obligations by applying the observability on structural criteria. Performed experiments: generated test obligations based on various structural coverage criteria, generated test obligations based on the combination of observability and structural coverage criteria, crafted test data by solving the obligations by a SMT solver Z3, simulated the models under test with the generated test data, and estimated the models in efficiency and effectiveness of tests generation. Open-sourced the tool: github.com/MENG2010/lustre

Professional Experiences

University of South Carolina

Graduate Research Assistant *09/2017 - present*

- [Fall 2019] Research on topics related to adversarial machine learning. Project: Athena.

- [Summer 2018] Research on software testing and test generation related topics. Project: Investigating Faults Missed by Test Suites Achieving High Code Coverage
- [Fall 2017] Research on software testing and test generation related topics. Project: Obligation Generator for Observed Structural Coverage Criteria.

Graduate Teaching Assistant *01/2015 - present*

- [Fall 2020] CSCE 585 (Machine Learning Systems): Design, develop, and grade course project: github.com/csce585-mlsystems/project-athena. CSCE 145 (Algorithmic Design I): Lab instructor and grader.
- [Fall 2018] CSCE101 (Introduction to Computer Concepts): Gave lectures to a class of 180 students. Held 3 lab sessions. Designed and prepared homework assignments, quizzes, and exams for the class. Graded all assignments and exams.
- [Spring 2015 - Spring 2018, Spring 2019] CSCE 101 (Introduction to Computer Concepts), CSCE 102 (General Application Programming), and CSCE145/146 (Algorithmic Design I/II): Lab instructor and grader.

China Development Lab, IBM China

Project: *Concord,* ***Title:*** *Software Test Specialist* ***Supervisor:*** *Jianping Zhou, Xuefei Duan* *07/2013 - 06/2015*

- Be responsible for Concord's essential features: the mechanism regarding the document loading and rendering, the mechanism of co-editing between multiple users; the infrastructure and mechanism of computations in the spreadsheet editor; the accessibility verification testing (AVT) of the spreadsheet. Worked closely with the designer and developer leads for the requirements and project plans, planed the test, designed and developed the test cases, wrote scripts to generate test data, assigned test tasks, performed the tests, and reported results. The features I owned were delivered on time with high quality.

Project: *Symphony, Concord,* ***Title:*** *Software Tester* ***Supervisor:*** *Jianping Zhou* *07/2011 - 07/2013*

- IBM Lotus Symphony (07/2011-01/2012) was a suite of office applications. Test owner of the pivot table — one of the most complex and powerful tools in the spreadsheet editor. Owned the test of formulas in spreadsheet editor. Owned the test of the side panels in all editors. Worked closely with the designer and developer team to ensure feature's functionality, by making testing plans, designing test cases and test data, writing automatic scripts to generate them, and then performing tests and reporting the results. All the features I owned were the new features contributed to the Apache OpenOffice.
- IBM Concord (01/2012 - 07/2013) was a suite of online office applications for sharing, creating, and co-editing texts, spreadsheets, and presentations. I owned the test of task workflow, spelling check, and auto-correction.

Publication

- Understanding the Impact of Solver Choice in Model-Based Test Generation. *Ying Meng*, Gregory Gay. International Symposium on Empirical Software Engineering and Measurement 2020.
- Investigating Faults Missed by Test Suites Achieving High Code Coverage. Amanda Schwartz, Daniel Puckett, *Ying Meng*, Gregory Gay. Journal of Systems and Software 2018.
- Ensuring the Observability of Structural Test Obligations. *Ying Meng*, Gregory Gay, Michael Whalen. IEEE Transactions on Software Engineering 2018.

Preprint

- ATHENA: A Framework based on Diverse Weak Defenses for Building Adversarial Defense. *Ying Meng*, Jianhai Su, Jason M. O'Kane, Pooyan Jamshidi. arXiv: 2001.00308.

Misc.

Awarded an Operational Machine Learning (OpML)'19 Diversity Grant *04/2019*