YULONG CAO

2371 Leslie Circle ⋄ Ann Arbor, MI 48105
(734) · 680 · 4632 ⋄ yulongc@umich.edu

EDUCATION

University of Michigan, Ann Arbor *Sep 2017 - Present*
Ph.D. candidate in Computer Science & Engineering
University of Michigan, Ann Arbor *May 2017*
B.S. in Computer Science & Engineering
Shanghai Jiao Tong University *August 2017*
B.S. in Electrical and Computer Engineering

PUBLICATION

1. **Yulong Cao**, Chaowei Xiao, Benjamin Cyr, Yimeng Zhou, Park Won, Sara Rampazzi, Qi Alfred Chen, Kevin Fu, and Z. Morley Mao, Adversarial Sensor Attack on LIDAR-based Perception inAutonomous Driving, Proceedings of the 26th ACM Conference on Computer and Communications Security (CCS'19), London, UK, November 2019.
2. Qi Alfred Chen, Eric Osterweil, Matthew Thomas, **Yulong Cao**, Jie Jimmy You, and Z. Morley Mao, Client-side Name Collision Vulnerability in the New gTLD Era: A Systematic Study, Proceedings of the 24th ACM Conference on Computer and Communications Security(CCS'17), Dallas, United States, October 2017.

POSTERS AND TALKS

1. **Yulong Cao**, Qi Alfred Chen, and Z. Morley Mao, Adversarial Machine Learning on LIDAR-based Object Detection in Autonomous Driving: A First Study, Poster and Talks at the 27th USENIX Security Symposium ($USENIX\ Security'$18), Baltimore, United States, August 2018.

INTERESTS

System Security, Machine Learning Security

RESEARCH EXPERIENCE

Adversarial Machine Learning on LIDAR-based Object Detection in Autonomous Driving
Nov 2017 - Nov 2018
Advised by Professor Morley Mao (University of Michigan) *Ann Arbor, MI*

- Performed the first exploitability study of machine learning usage in LIDAR-based perception for AV systems.
- Enabled the model analysis by modeling LIDAR spoofing attack capability
- Improved the model analysis by designing a new sampling based optimization algorithm.
- Constructed two end-to-end attack scenarios: emergency brake attack and AV freezing attack to demonstrate the severity of the attack consequences.

Name Collision Attacks in the New gTLD Era July 2016 - Jan 2017
Advised by Professor Morley Mao (University of Michigan) *Ann Arbor, MI*

- Identified new attack vectors exposed by name collision in new gTLD era;
- Used the threat model to study the vulnerability status in the wild;
- Proposed a set of remediation strategies at root, AS and end user level based on our results.

Server-Aided Dependency Resolution for a Faster Mobile Web July 2016 - Jan 2017
Advised by Professor Harsha V. Madhyastha (University of Michigan) *Ann Arbor, MI*

- Found that solutions to improve web page loading time (PLT) are hard to deploy and we need a light weight solution to improve PLT in real world;
- Built a server proxy that provides dependency hints to client in order to make the best use of client CPU and network resource;
- Evaluated the solution with a replay framework called *Mahimahi* and top 100 sites.

Crowd Source System Supported Active Learning April - July 2016
Advised by Professor Barzan Mozafari (University of Michigan) *Ann Arbor, MI*

- Identified the problem that Amazon MTurk's website is tedious for users to use;
- Built a web interface for Amazon MTurk users to manage their projects, workers and received answers;
- Used active learning system to automatically process workers and clients to attain best training model.

PROJECT EXPERIENCE

Off Track Jan 2017 - April 2017
EECS494 Game Design (Capstone Project) *Ann Arbor, MI*

- Designed and built a 2D side scrolling roller coaster action game: *Off Track* with **Unity**;
- Tested and tuned the players and enemies parameters to gain better playing experiences.

Magic Chess Board Jan 2017 - April 2017
EECS373 Introduction to Embedded System (Course Project) *Ann Arbor, MI*

- Designed and built a chess board where chess pieces are moved by magnetos underneath the board;
- Designed and implemented a scanning system that detects the chess pieces current status;
- Designed and implemented a display program that shows current status of the game on a touch screen (HX8357D).

Context Based Access Control on Emerging Appified IoT Platforms Sept 2016 - April 2017
EECS583 Advanced Compiler (Course Project) *Ann Arbor, MI*

- Identified the control flow patterns of IoT apps to automatically track down sinks;
- Used both program and app context to verify the matching and so forth control the access;
- Proposed a standard for patching program and enhancing access control.

HONORS

- University of Michigan Dean's List (2015, 2016).
- 2014 Mathematical Contest in Modeling (MCM), Honorable mention (top 25% worldwide).
- 2014 Shanghai Jiaotong University Scholarship (top 10%) Award (2013,2014).
- UM-SJTU Joint Institute Dean's List (2013, 2014).

TEACHING

Teaching Assistant Sep - Dec 2014
VV286 HONORS MATHEMATICS III (Shanghai Jiao Tong University) *Shanghai*

- Led weekly discussion, prepared exercises and slides, graded homework and exams.

Teaching Assistant Sep - Dec 2014
VC210 Introduction to Chemistry (Shanghai Jiao Tong University) *Shanghai*

· Led weekly discussion, prepared exercises and slides, graded homework and exams.

ACADEMIC SERVICES

- PC member: AdvMLCV (co-located with CVPR) 2019, SPML (co-located with ICML) 2019