Mulong Luo

Email : ml2558@cornell.edu
Mobile : +858-263-6752

Education

- **Cornell University** — Ithaca, NY
  Ph.D. student in Computer Engineering — *July 2017 - now*
  - **Thesis Topic**: Hardware Security and Safety for Cyber-Physical Systems
  - **Thesis Committee**: G. Edward Suh (chair), Andrew C. Myers, and Zhiru Zhang
- **University of California San Diego** — La Jolla, CA
  M.S. in Computer Science and Engineering — *Sept 2014 - June 2017*
- **Peking University** — Beijing, China
  B.S. in Microelectronics — *Sept 2010 - July 2014*

Research Experience

- **Uncertainty-Aware Path Planning Hardware Accelerator** — Ithaca, NY
  A hardware accelerator that performs path planning algorithm with uncertainty — *August. 2020 - now*
  - Working on incorporating obstacle prediction and uncertainty functions into a new hardware path planning accelerator to reduce overall end-to-end latency.
- **Attacking Sensor Timestamp Integrity of Autonomous Driving** — Ithaca, NY
  An attack on autonomous driving software protected by trusted execution environment — *Sept. 2019 - now*
  - Measured how interrupt by an adversarial OS can affect the sensor timestamp.
  - Demonstrated and evaluated the impact of adversarial interrupt on vehicles ego and obstacle localization.
- **Autonomous Vehicle localization via Cache Side Channel** — Ithaca, NY
  An adversarial cache side channel attack to track autonomous vehicles — *Sept. 2018 - August. 2019*
  - Used cache side channel to collect the memory access patterns of autonomous driving software.
  - Used machine learning to learn the locations of the vehicles via the collected memory access patterns.
- **Secure Autonomous Vehicles via Information Flow Control** — Ithaca, NY
  An autonomous vehicle platform with software and hardware information flow control — *July 2017 - July. 2018*
  - Used an experimental programming language (Java Information Flow) to automatically track and prevent untrusted sensor inputs and enforce vehicle safety under adversarial scenarios.
  - Integrated the software into an in-house secure hardware platform (Hyperflow) that is capable of enforcing information flow control at instruction level.

Professional Skills

- Programming Languages: C/C++, Java, Python, Shell
- System programming: Linux, ROS

Selected Publications

- **M.Luo**, G. E. Suh, "Implications of Microarchitectural Interrupt on Autonomous Driving Safety", manuscript in preparation.
- **M. Luo**, A. C. Myers, G. E. Suh, "Stealthy Tracking of Autonomous Vehicles with Cache Side Channels", in *29th USENIX Security Symposium*, 2020, pp.859-876.
- J. Liu, J. C. Davies, A. Ferraiuolo, A. Ivanov, **M. Luo**, et al., "Secure Autonomous Cyber-Physical Systems Through Verifiable Information Flow Control", in *Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC)*, 2018, pages 48-59 (**Best Paper Award**).
- Z. Fang, **M.Luo**, et al., "Go-realtime: a lightweight framework for multiprocessor real-time system in user space ", in *ACM SIGBED Review*, Volume 14 Issue 4, November 2017 Pages 46-52.