# Milind Srivastava

Homepage milind@cse.iitm.ac.in +91-9940142082 LinkedIn

## Education

**Indian Institute of Technology Madras** — **Chennai, India**
*Dual Degree (B.Tech. Hons. + M.Tech.) Computer Science & Engineering* — *Aug 2015 - Jul 2020**
CGPA: **9.64** (end of 8th semester) — *expected

**Amity International School, Noida** — **Noida, India**
*Physics, Chemistry, Mathematics and Computer Science* — *Apr 2000 - Mar 2015*
CBSE Class XII Board: **97.4%**

## Publications and Posters

**Solomon: An Automated Framework for Detecting Fault Attack Vulnerabilities in Hardware**
*DATE 2020*
**Milind Srivastava**, Patanjali SLPSK, Indrani Roy, Chester Rebeiro, Aritra Hazra, Swarup Bhunia

**Sauron: An Automated Framework for Detecting Fault Attack Vulnerabilities in Hardware**
*ACM SRC (Student Research Competition) ICCAD 2019 - 1st position in undergraduate category*
**Milind Srivastava**, Patanjali SLPSK, Chester Rebeiro

**Do events change opinions on social media? A case study of the 2016 US Presidential Debates**
*SocInfo 2019*
Sopan Khosla, Niyati Chhaya, **Milind Srivastava***, Shivam Jindal*, Oindrila Saha* — * equal contribution

## Achievements

- **1st Position - Embedded Security Challenge, CSAW (India region)** (2019) — *NYU Center for Cybersecurity*
- **1st Position (undergraduate category) - Student Research Competition** (2019) — *ACM SRC @ ICCAD 2019*
- **S.N. Bose Scholarship** (2019) — *Indo US Science and Technology Forum*
- **Best Presentation Award** (2018) — *Adobe Research*
- **Institute Notional Prize** (2016) - Certificate of Merit — *Indian Institute of Technology Madras*
- **AIR 256 in JEE Advanced** (2015) - 99.8 percentile out of 150,000 applicants — *Indian Institute of Technology Bombay*
- **AIR 42 in JEE Mains** (2015) - 99.99 percentile out of 1.3 million applicants — *Central Board of Secondary Education*
- **KVPY Fellow** (2015) — *Department of Science and Technology, Government of India*
- **NTSE Scholar** (2011) — *National Council of Educational Research and Training*

## Professional Experience

**Carnegie Mellon University - Dr. Swarun Kumar** — **Pittsburgh, USA**
*Research Intern* — *May 2019 - Jul 2019*
- Worked towards developing a full duplex system at millimeter wave frequencies
- Designed an optimized PHY base layer with different encoding schemes to enable error detection and correction
- Employed OFDM to combat frequency selective channel
- Extended system performance to 256 QAM at 20 MHz and 64 QAM at 100 MHz
- **Submitted work to MobiCom 2020**

**Adobe Research - Big Data Experience Lab** — **Bangalore, India**
*Research Intern* — *May 2018 - July 2018*
- Studied opinion change regarding 2016 US Presidential Elections on Twitter
- Presented opinion variation analysis coupled with micro and macro level user analysis
- Studied user segments based on their patterns of tweeting and stance towards presidential candidates
- Received Best Presentation Award from Dr. Shriram Revankar, VP, Adobe Research
- **Published work in SocInfo 2019**

**Microsoft Research** — **Bangalore, India**
*Research Intern* — *Dec 2017 - Dec 2017*
- Worked on integrating ML libaries with custom C++ BLAS implementation

**Maximl Labs** **Chennai, India**
*Software Engineering Intern* *May 2017 - July 2017*
- Developed task library to handle large industrial projects with complicated dependencies
- Implemented CPM algorithm to generate optimized project schedules
- Developed heuristic to evaluate and plot parallelism in a project plan
- Involved in re-architecture of core product to enable plugin based system
- Contributed to trial deployments in **Tata Steel**

**Indian Institute of Technology Madras - Dr. Rupesh Nasre** **Chennai, India**
*Software Engineering Intern* *Dec 2016 - Dec 2016*
- Implemented 3 image segmentation algorithms - Connected Component Labelling, Min Cut, Minimum Spanning Tree and compared time complexities

**Zamono Tech LLC** **Remote**
*Software Engineering Intern* *Jun 2016 - Jul 2016*
- Developed end-to-end web app which integrated with Google Calendar API

## Projects

**Detecting hardware trojans using formal techniques** *Sept 2019 - Present*
Mentor: Dr. Chester Rebeiro, IIT Madras (as part of Dual Degree Project)

Hardware trojans are a serious threat to the security of a system. These trojans can be inserted at various steps in the EDA (Electronic Design Automation) flow and are extremely difficult to detect reliably. In this project, we aim to use formal verification techniques to detect hardware trojans reliably.

**An Automated Framework for Detecting Fault Attack Vulnerabilities in Hardware** *Feb 2019 - Present*
Mentor: Dr. Chester Rebeiro, IIT Madras (as part of Dual Degree Project)

Fault attacks pose a severe threat to edge devices. However, out of the large number of faults that can occur, very few are actually exploitable. Current work cannot identify exploitable faults precisely in hardware design. We propose a formal framework that can precisely identify fault vulnerabilities in hardware.
- First work to precisely identify fault vulnerable locations in hardware design
- Works across different levels of abstraction namely RTL, gate-level netlist and placed netlist
- Enables implementation of targeted countermeasures that will reduce power, area and timing overheads
- Developed framework and evaluated on AES, CLEFIA and Simon
- Developed in collaboration with Dr. Aritra Hazra, IIT Kharagpur and Dr. Swarup Bhunia, University of Florida
- **Accepted at DATE 2020**
- **Recognized with first position in undergraduate category at ACM SRC (Student Research Competition) ICCAD 2019**

**Cybersecurity for Automobile Controllers** *Jan 2019 – Apr 2019*
Mentors: Dr. Chester Rebeiro, IIT Madras and Dr. Pratyush Kumar, IIT Madras

Modern automobiles feature numerous electronic units that control different features of the car such as engine, airbags, transmission and braking. These "real-time" units guarantee response within a specified time. With the advent of "smart cars" that can be connected to the internet and can communicate with other systems online, the attack surface increases and security risks become more pronounced. In this project, we explore methods to increase security of automobile controllers while meeting real-time guarantees.
- Surveyed different Real Time Operating Systems (RTOS) for embedded devices
- Ported Linux and Real Time Linux (RTLinux) onto Renesas R-Car M3 board
- Explored use of Security Enhanced Linux (SELinux) to achieve stronger access control and process isolation
- Provided recommendations to Continental AG on hardening automobile controllers against cyber-attacks

**Instruction Cache and Branch Predictor Attacks** *Jul 2018 – Nov 2018*
Mentor: Dr. Chester Rebeiro, IIT Madras (as part of Undergraduate Research Course)

Cache attacks have traditionally used the data cache as an attack vector. There has been little prior work on exploring the Instruction Cache (I-Cache) and Branch Target Buffer (BTB) as potential attack vectors. Moreover, the BTB is proprietary information and details about its structure and configuration and not released by vendors. This significantly increases the complexity of mounting an attack using the BTB.
- Demonstrated cache attack using I-Cache memories

- Designed experiments to test efficacy of BTB as a side channel
- Analyzed necessary conditions for a successful fully black box attack and concluded that it would be infeasible
- Concluded that full/partial knowledge of microarchitectural components would decrease the attack complexity significantly

**Cache Attacks on Intel SGX** *Jan 2018 – May 2018*

Mentor: Dr. Chester Rebeiro, IIT Madras (as part of Undergraduate Research Course)

Caches attempt to reduce memory access times. This optimization improves performance but reduces security by introducing a timing channel. Fine grained counters can be used to determine whether a memory access is a cache hit or miss. This observation can be used to recover secret information from a process.

- Demonstrated cache attack on Intel SGX using L1 and Last Level Cache (LLC) memories
- Applied attacks to reduce the entropy of guessing the key in an AES encryption
- Compared effectiveness of L1 vs LLC cache attack across systems with different number of cores
- Discussed possible ways of optimizing the LLC cache attack

## Competitions

**Intelligent Ground Vehicle Competition (IGVC) 2018** *Oakland University, Jun 2018*

- Led software team of 10 students to develop vehicle control, computer vision and localization algorithms
- Qualified and secured 5th position in Design Challenge amongst 30+ international teams

**Intelligent Ground Vehicle Competition (IGVC) 2017** *Oakland University, May 2017*

- Worked in software team and surveyed path finding algorithms
- Implemented algorithms and performed live testing on ground vehicle
- Qualified in our maiden attempt at IGVC

## Coursework

- **Systems** - Undergraduate Research Courses, Secure Systems Engineering, Network Security, CAD for VLSI Systems, Program Analysis, Computer Architecture, GPU Programming, Operating Systems, Computer Networks, Compiler Design, Introduction to Database Systems, Computer Organization and Architecture
- **Theory** - Theory and Applications of Ontologies, Foundations of Blockchain Technology, Paradigms of Programming, Data Structure and Algorithms, Language, Machines and Computations
- **Data Science** - Principles of Machine Learning, Deep Learning
- **Mathematics** - Probability Statistics and Stochastic Processes, Linear Algebra, Basic Graph Theory

## Skills

- **Languages** - C/C++, Assembly, Python, Verilog, Bluespec SystemVerilog, MATLAB
- **Tools and Frameworks** - CUDA, Zeek Network Security Monitor, Wireshark, Ghidra, Ollydbg, Pin, LLVM, Robot Operating System (ROS)