PRANAV JAIN **Portfolio:** https://www.linkedin.com/in/pranav-jain-a70b7791/
San Diego, CA 92126 | **Github:** https://github.com/pranav7291 | (716)431-8867 | pranavjain7291@gmail.com

WORK EXPERIENCE

Senior Software Engineer **Qualcomm Technologies Inc., San Diego, USA** **April-2017 to present**

- Secure Systems Group's **Windows OS Security team**, involving design and development of software in various areas like –
  - **TrustZone** (TZ) – Trusted Applications (TAs), TZ services and drivers, **Interface Definition Language** (IDL) based communication in TZ
  - **Unified Extensible Firmware Interface** (UEFI) – UEFI drivers and applications
  - **Windows HLOS** – **Trusted Execution Environment** (TrEE) and **Secure Channel Manager** (SCM) **drivers**, applications to display the system security state and testing out various HLOS and TZ security features
- Qualcomm **Windows on Snapdragon** (WoS) chipsets - **Snapdragon 850**, (led bring-ups of) **Snapdragon 8cx Gen 1, Gen 2 and Gen 3**
- Worked on the **Qualcomm TrEE miniport driver** interfaces/services to talk with Qualcomm's secure services hosted in the secure world (TrustZone, Secure Processor Unit) via Secure Monitor Calls (SMCs) and TZ OS syscalls –
  - **High-bandwidth Digital Content Protection** (HDCP) Service for Display driver's communication with HDCP TA
  - Trusted Platform Module (TPM), shared memory, listeners, Secure File System (SFS), Relay Protected Memory Block (RPMB)
- **Trusted Platform Module** (TPM) –
  - Added features to and maintained the Qualcomm **Firmware TPM** code hosted in a TA – code for the non-volatile memory used by it, using Qualcomm's TZ crypto APIs, PCR measurements, etc; **|** Code to communicate with **Discrete TPM**s on Qualcomm chips
  - Wrote the transport layer in the hyperV trusted app and the UEFI TPM driver for communicating with **Integrated TPM**
- **UEFI security** features like **UEFI Secure Boot** for WoS chipsets for allowing only signed entities to load during bootup; **| UEFI Security drivers** like TrEEDxe, TpmDxe, SecurityDxe, ShmBridgeDxe, TzDxe, ScmDxe, MeasureBootDxe, MorPpiDxe, RngDxe and associated test applications; **| Advanced Configuration and Power Interface** (ACPI)**; | Memory Overwrite Request** (MOR) feature; **| Physical Presence Interface** (PPI) feature
- Trusted Applications (TAs) – worked on various TAs hosting/communicating with features like HDCP, Firmware/Discrete/Integrated TPM, **Output Protection Manager** (OPM) key provisioning and encryption-decryption for **Digital Rights Management** (DRM) use cases, **UEFI variables** verification using X.509 certificate and PKCS7 format, displaying security state of the device, watermark service, etc
- Collaborated and carried out **live debugs** with **Microsoft** and various other customers like **Samsung**, **Lenovo**, **HP** on areas like TPM, UEFI Secure Boot, Bitlocker, hyperV, HDCP, DRM, Measured Boot, PPI, etc
- Enabled Windows features like **Bitlocker** (using HW - Inline Crypto Engine and SW crypto), HLOS TPM access, **UEFI Secure Boot** for WoS chips
- Other areas worked on include various debugging efforts spanning TZ, UEFI and HLOS; boot measurements; **HDCP** - **SST**, **MST** and **multi-stream** support; integrating Microsoft Driver Module Framework (DMF) and other Windows Driver Framework updates; encryption, decryption, hashing, random number generators; public & private key cryptography; various signature schemes

Teaching Assistant **State University of New York at Buffalo, New York** **Sep-2016 to December-2016**

- Evaluating homeworks, quizzes, midterms and programming assignments for the undergraduate course CSE 410 – Intro to Computer Security.

Application Developer **BNY MELLON (INAUTIX TECHNOLOGIES), Pune, India** **Sep-2013 to June-2015**

- Projects involving programming in COBOL, JCL, CICS, VSAM & DB2 for the Entitlement Management team for Pershing LLC's NetX360 platform. Duties included batch jobs development & deployment; formulation & optimization of complex DB2 queries.

EDUCATION

Masters in Computer Science, State University of New York at Buffalo, New York **(GPA 3.593)** **December-2016**

Analysis of Algorithms, Information Retrieval, Distributed Systems, Computer Security, Operating Systems, Machine Learning, Applied Cryptography and Computer Security, Database Systems, Algorithms for Modern Computer Systems, Advanced Topics in Computer Security (Seminar).

Bachelors in Computer Engineering, Pune University, India **May-2013**

Object Oriented Programming in C++ and Java, Data Structures, Analysis of Algorithms, Database Systems, Theory of Computation, Computer Networks, Computer Security, Computer Graphics, Computer Organization, Digital Signal Processing, Computer Networks, Software Engineering, Data Communication, Principles of Programming Languages, Artificial Intelligence, Principles of Compiler Design.

TECHNOLOGY SUMMARY

- C, C++, Java, SCons, Python, SQL, DB2, Git, Perforce, Trace32, JTAG debugging, Windbg
- TZ, UEFI and Windows HLOS driver & application development, Cryptography, Information Security

MASTERS, BACHELORS & INDIVIDUAL PROJECTS

- **OS161:** Operating Systems assignments: Implementing Synchronization Primitives, System Calls, and Virtual Memory support for OS161. On the leaderboard in all the assignments. Course page: https://ops-class.org/asst/overview/. (Language: C)
- **Cappr:** An augmented reality and intelligent suggestion tool to facilitate the New Era customers' shopping experience leveraging the Microsoft Face, Computer Vision and Emotion APIs and using our own algorithms. (Python, Django, HTML, CSS, JS)
- **SQL parser & DBMS:** Created an SQL parser and DB management system from scratch for the Database Systems course. (Java, JSON)
- **Machine Learning:** Handwritten digits' recognition using Neural Network, Classification and Regression Comparison, and Comparison between Logistic Regression and SVM as part of the Machine Learning course. (Language: Python)
- **Information Retrieval:** Developed a multilingual Information Retrieval System on Apache Solr that enabled searching data across 5 different languages and included components like content tagging, faceted search, sentiment analysis and summarization.
- **Distributed Systems:** Model checking Dijkstra's token ring and Hybrid Vector clock algorithms on TLA+ tool using PlusCal code.
- **Computer Security:** Web Security and Symmetric Key Crypto Implementation; E-mail forensics with DKIM; Evaluation of Privacy in DNS Private Exchange as part of Computer Security courses.
- **Android security app:** App having random and unique, session-based auth password scheme using text and colors. Stronger than traditional auth schemes and resistant to various attacks including brute force, guessing, shoulder surfing and dictionary attacks. (Java, ADT, Android)

PERSONAL:

2nd Runner Up at the New Era Hackathon 2016; **|** Volunteered to raise funds for children's NGO at BNY Mellon's Community Partnership Campaign; **|**
GRE: 323/340, TOEFL: 107/120