AMIT CHOUDHARI

+33 753436504 | amit.choudhari@polytechnique.edu | https://linkedin.com/in/amit-choudhari-3b560a76

SUMMARY

Seven years of work experience in Embedded engineering and Electronic product design. Worked on building Secure systems by involving TEE, Hypervisor, Secure boot, and Tamper detection.

Experience in working with peripherals devices like NFC, Displays, Camera, Audio, and with I2C, SPI and UART devices.

Expertise in Linux kernel customizations, Device drivers and functionality testing, debugging tools and developing firmware. Experience on technologies like Wireless access points, routers and switches.

EDUCATION

Master of Science in Cyberphysical systems Sep 2020 - Aug 2022(expected)
École Polytechnique (IP Paris)
Awarded IP Paris scholarship (full tuition fee waiver)
Courses: Advanced Cryptography, Information system security, Network security, Reverse engineering, side-channel analysis

Bachelor of Engineering (B.E.) in Electronics Engineering Aug 2009 - May 2013
Ramrao Adik Institute of Technology (Mumbai University)

WORK EXPERIENCE:

ETH Zurich April 2022 - Present
Academic guest (Supervisor: Prof. Shweta Shinde)

- Working on a security enhancement of RISC V to protect userspace applications from higher privileged software such as monitor.

Secure-IC May 2021 - March 2022
Master I and II research project (Supervisor: Sylvain Guilley, CTO)

- Devised a generic rule based dynamic analysis tool to identify misusage of cryptographic libraries.
- Tested the tool on different libraries such as OpenSSL and SoftHSM to identify known vulnerabilities in applications from GitHub repositories and StackOverflow.
- Developed a tool 'Specdefender' to dynamically detect Spectre v1 and v2 attacks using HPC counters, and run an instrumented program while the attack is active.

Qualcomm India Pvt Ltd Mar 2017 - Nov 2020
Sr. Software Engineer
Development of ARM TrustZone based security solutions like Secure UI and Secure Camera, that is majorly focused on securing the data path and ensuring content protection for any payment or authentication use case.

- Implemented a hypervisor-based face authentication solution along with securing camera hardware data path for a payment app Alipay. Compared to the primitive design of frame processing in TrustZone secure OS, this approach of separate VM allowed sandboxing and performance boost.
- Worked on different camera architectures to design and implement a solution to protect the capture data path, from the sensor to consumer (frame processing algorithm).
- Worked on end to end secure payment solution with display and input (touch/keypad) data path secured, i.e. the display buffers and touch coordinates are only accessible from the TEE.

embedUR Systems, Chennai, India Apr 2015 – Feb 2017
Embedded Software Engineer
Development of features on operating systems for embedded devices such as Wireless Controllers and Access Points.

- Designed the validation framework for Dynamic channel and Dynamic Band-width assignment configurations.

- Worked on Qualcomm Atheros network driver and developed enhancements for its stability.

IIT Madras, Chennai, India Aug 2013 – Mar 2015
Research Associate
Involved in developing secure systems for use in the security-critical domain. Worked on developing Secure Tablet for DRDO, with secure boot, TEE and tamper protection capabilities to protected from malicious software and physical tampering.

- Worked on Secure boot (U-boot 2009 and 2014) and Tamper detection systems on i.MX6 processors for protection against rootkits and tampering.
- Developed an Android NFC authentication app for IITM Secure Tablet.
- Ported device drivers for MAX98089 Audio codec, for i.MX6 and hardware modules.
- Involved in hardware debugging, schematic verifications and functionality testing of customized boards based on Freescale i.MX series of processors.
- Worked on sensor modules like Wi-Fi, GPRS, NFC, Digital Mic etc. on the target boards.

ThinkLABS, SINE, IIT Bombay, Mumbai, India Summer 2013
Internship
Developed a Scientific calculator and ported LCD, keypad drivers on AVR ATmega64 Microcontroller.

OTHER PROJECTS

- Developed Baremetal firmware for BeagleBone black.
- Developed USB Host and Gadget drivers for BeagleBone black.
- Final year project on RTX Keil RTOS based gaming console using STM32f4 ARM Cortex-M3.

AWARDS AND ACCOMPLISHMENT

- Received an Orion and 5 Qualstar Awards for outstanding performance at Qualcomm.
- Patent applied for Enhancing user privacy by hiding visual presentation of sensitive data on display.
- Among top 4 in Astronomy Olympiad 2006.

CERTIFICATIONS

- Machine learning by Andrew NG (Coursera)
- Neural networks and deep learning by deeplearning.ai (Coursera)
- Internet of things by USCD (Coursera)
- The Hardware/Software Interface by University of Washington (Coursera)

SKILLS

Processors	Freescale i.MX6, QorIQ processors T4240, AVR ATmega series, STM32f4, Qualcomm Snapdragon series (SDM845, SDM855)
Hardware Exposure	NFC systems, On-board buses and peripherals like I2C, SPI, UART, LCD, Timers, Interrupts, JTAG, PCI Network card, USB host and Gadget devices
Development tools	Eclipse, Arduino IDE, Win AVR, GDB debugging, JTAG, git
Software Exposure	Linux Kernel Customization, U-boot bootloader, RTX Keil RTOS, SoftHSM, OpenSSL
Operating System	GNU/Linux (Ubuntu/Mageia), Android, Cisco IOS
Languages	C, Embedded C, C++, Bash Shell scripting, Python