Sareena K P

Indian Institute of Technology Madras

☎ +91-9445329960 • ✉ sareena[at]cse[dot]iitm[dot]ac[dot]in,sareena.kp[at]gmail[dot]com
⌂ https://sareenakp.github.io/ • https://in.linkedin.com/in/sareenakp

Research Interests

Network Security, Distributed Denial-of-Service (DDoS) Attack Detection and Mitigation, Malware Analysis and Detection, Test beds for Network Experiments

Education and employment

2015-Present	**Doctor of Philosophy (PhD) and Project Associate** *Indian Institute of Technology Madras* Advisors: Prof. Kamakoti V (Dept of CSE) *Grade: 9.22/10*
2004-2015	**Industry Experience** *Identiv Private Limited ((Formerly known as SCM Microsystems Pvt. Ltd)* *Project Lead - Software* Hewlett Packard System Technology Software Division, Bangalore *Senior Software Developer*
2000-2004	**Bachelor of Engineering (B.E)** *Visvesvaraya College of Engineering, Bangalore University, Bangalore* Discipline: Computer Science and Engineering *Grade: 84.56 (3rd Rank)*
1998-2000	**Senior High School (Class XII CBSE AISSCE)** *National Public School Bangalore* *Grade: 87.8*
1987-1998	**High School (Class X CBSE AISSE)** *Kendriya Vidyalaya N.A.L, Bangalore* *Grade: 92.8* 6th at the national level; 2nd at the regional level; School topper

Publications (Peer Reviewed)

- Net-Police: A Network Patrolling Service for Effective Mitigation of Volumetric DDoS Attacks, Sareena Karapoola, Prasanna Karthik Vairam, Shankar Raman, Kamakoti Veezhinathan, *Elsevier Computer Communications*, 2020.
- Towards Identifying Early Indicators of a Malware Compromise, Sareena K.P, Unnati Parekh, Chester Rebeiro and Kamakoti V., Accepted for publication at 14th *ACM Asia Conference on Computer and Communications Security (ASIACCS)* 2019.

Posters

- Early Malware Detection using Network Traffic Analysis, Sareena K.P, Unnati Parekh, Chester Rebeiro and Kamakoti V., at 8Th *International Conference on Security Privacy, and Applied Cryptography Engineering (SPACE) 2018*
- A Secure Framework for Quick and Effective DDoS Mitigation, Sareena K.P. and Kamakoti V., at PhD Conclave, *Asia Security and Privacy Conference 2017*, held at NIT Surat, 29 Jan-1 Feb, 2017.
- Eradicator: An Integrated Approach for Defense against Cyber Attacks in PLC based Industrial Control Systems, at Embedded Security Challenge, *Cyber Security Awareness Week 2017*, held at IIT Kanpur. Won the First place in the Embedded Security Challenge.
- Cracking Open the Safe: Subverting Authentication in RFID Systems, at Embedded Security Challenge, *Cyber Security Awareness Week 2019*, held at IIT Kanpur. Won the First place in the Embedded Security Challenge.

Technical Skills

- **Languages** - {Python, C, C++, Java, Linux Shell Scripting} - Proficient
- **Operating Systems** - Linux, RTOS (FreeRTOS), Windows XP, 7, 10
- **Compilers** - Rowley CrossWorks (ARM Cortex M3), Keil, and Atmel AVR compiler
- **MicroControllers** - ARM Cortex M3 (STM32F family), ARM9 (Atmel), and 8051 (STC2 and STC3)
- **Firmware Developments** -Router and switch development on QorIQ multi-core communication processors, Contactless reader firmware (for ASICs - PN533, PN512, CLRC663,CLRC632, and MFRC531)
- **Driver Development** - Windows drivers for smartcard readers, access control terminals and storage controllers; Linux driver development
- **Technologies** - Network router/switch development, contactless smartcard technology, physical access control terminals, Interfaces: USB, USART, and SPI.
- **Tools/IDE** - Yocto, Zeek, Mininet, Latex, Eclipse, WinDbg, Windows Driver Kit (WDK)
- **Hardware Description Languages** - Verilog
- **High Level Chip Synthesis Tool** - BlusSpec

Research Projects

Sundew

▪ **A Cross-dimensional analysis of malware behaviour and framework for malware detection (Ongoing)**
In this work, we explore the differences of malware behaviour across differing abstractions of the system: network, operating system and hardware.

Malware

▪ **Early detection of malware infection (Ongoing)**
Malware life cycle is known to be long ranging from weeks to months. In this work, we attempt a temporal analysis of how early a malware can be detected.

Net-Police

▪ **A Network Patrolling Service for Effective Mitigation of Volumetric DDoS Attacks.**
Net-Police is a traffic patrolling system for DDoS mitigation, which identifies the sources of attack to facilitate quick filtering at the sources. Unlike prior works, the immediate response effectively prevents the flow of malicious traffic across the ISP networks, thereby benefiting both ISPs and the victim simultaneously.

Jugaad

▪ **A low-cost real-world tested for network experiments**
Jugaad is a lightweight heterogeneous testbed for security-oriented research, with high fidelity to real-world networks. Jugaad testbed uses available low-cost single board computers and desktop systems to quickly build a private testbed with features to facilitate malware analyses and Cyber Physical System research.

CSAW 2019

▪ **Cracking Open the Safe: Subverting Authentication in RFID Systems**
In this work, we explore the potential and applicability of well-known reverse engineering and binary exploitation techniques to subvert RFID access control readers.

Eradicator

▪ **Eradicator: An Integrated Approach for Defense against Cyber Attacks in PLC based Industrial Control Systems**
Eradicator is a comprehensive defense framework for distributed ICS (Industrial Control System) environments, that leverages a holistic view of the ICS and process-specific parameters to detect cyber-attacks, isolate the root cause of the attack and mitigate it.

SDN Security

▪ **Secure SDN Topology Discovery (Course Project)**
We explore spoofing attacks that exploits the vulnerabilities of the SDN operation, and consequently poison the network topology view maintained by the controller.

Industry Projects

Network Switches

- **Indigenous Network Switch Development**
Design and implementation of switch functionalities on the Freescale QorIQ box to build an indigenous low-cost switch (as a part of Make in India program).

Realtime Smartcard reader

- **Firmware with real time OS (FreeRTOS)**
For future scalability and performance improvement of the Identiv products, initiated and worked independently on a research project on the feasibility and porting of USB smart card reader functional firmware onto FreeRTOS. Hardware(STM32F103RET6TR (ARM Cortex M3 core), contact module, contactless (CLRC663) module, USB and serial interfaces.

Smartcard Contact & Contactless Readers

- **Firmware and Drivers for USB smart card contact and contactless readers**
Design and Development of firmware and drivers for smartcard contact and contactless readers. Mirocontrollers: SCM STC2 and STC3, ARM Cortex M3 core (STM32F103RET6TR), contactless ASIC (CLRC632), Atmel with PN512 and CLRC632.

Access Control Terminals

- **Physical access control terminals**
Worked as project lead for the development of different types of contactless physical access control terminals for the American market. The cards supported are high frequency (13.56 MHz), Low Frequency (125 KHz), iClass cards.

eHealth

- **German eHealth application firmware**
Development of eHealth application firmware for a mobile hand-held, battery operated device (with two smart card slots) for the German e-health card program, which is one of the largest electronic healthcare projects in the world. Functionalities include secure access and storage of the patients' data.

Storage Drivers

- **Windows drivers for HP Smart Array controllers**
Development, maintenance, and enhancement of drivers for HP Smart Array Controllers and Fiber Channel (FC) Array Controllers on HP Proliant Servers.

eGovernance

- **Karnataka e-Governance project on Proliant Essentials**
This was a field engagement activity for the Karnataka e-Governance Customer. The requirement was to develop a scripting tool kit to support the following features on remote Proliant Servers (having the Integrated Lights Out remote management card) from a central server, using the Proliant Essentials.

Awards and Recognitions

2020

- **IBM Maitrayee 2020**, selected as one of the top 5 contestants of the blog writing competition at Maitryee 2020, IBM Research-India's annual women outreach event.
- **Star TA Award**, from the Department of CSE, IIT Madras for contributions as a Teaching Assistant.

2019

- **Embedded Security Challenge Winner, First prize** at Embedded Security Challenge, Cyber Security Awareness Week 2019, organized by IIT Kanpur, for presenting '*Cracking Open the Safe:Subverting Authentication in RFID Systems*'.

2017

- **Embedded Security Challenge Winner, First prize** at Embedded Security Challenge, Cyber Security Awareness Week 2017, organized by IIT Kanpur, for presenting '*Eradicator: An Integrated Approach for Defense against Cyber Attacks in PLC based Industrial Control Systems*'.

2010

- **Employee of the Quarter Award**. For developing the eHealth application firmware for the German health care market and receiving certification from the Govt. of Germany [Identiv Private Limited]

2005

- **Filed an invention disclosure** on efficient power saving mechanism in Proliant servers using remote management [Hewlett Packard]

Courses

- CAD for VLSI systems, Digital System Testing and Testable Design, Software Defined Networking, Computer Architecture, Digital Design Verification, Discrete Mathematics, Program Analysis, Cryptography Network Security

Positions of Responsibility during PhD

2021	▪ TA for CAD for VLSI Course
2020	▪ TA for Computer Organization and Architecture ▪ TA for Foundations of Computer Design
2019	▪ TA for Digital System Testing and Testable Design ▪ Shadow PC Member of IEEE Symposium of Security and Privacy 2019.
2018	▪ Shadow PC Member of ACM Internet Measurement Conference 2018.
2015	▪ Project Associate for the Indigenous Router and Switch Development.

References

Prof. V Kamakoti
Professor
Department of Computer Science & Engineering
IIT Madras, Chennai – 600036
Email: kama@cse.iitm.ac.in
Phone: +91-44-22574368

Prof. Krishna Sivalingam
Professor
Dept. of Computer Science and Engineering
IIT Madras, Chennai - 600036
Email: krishna.sivalingam@cse.iitm.ac.in
Phone: +91-44-22574378

Prof. Chester Rebeiro
Associate Professor
Department of Computer Science & Engineering
IIT Madras, Chennai – 600036
Email: chester@cse.iitm.ac.in
Phone: +91-44-22574350

Sudheendran T L
VP Sofwtare Engineering
Mastercard
Email: sudheendran@hotmail.com