Mansi Sheth

Email: mansi.sheth@gmail.com **Mobile**: +1 603 265 0494
LinkedIn: https://www.linkedin.com/in/shethmansi **GitHub**: https://1MansiS.github.io

CAREER SUMMARY

Accomplished security professional with over 15 years of industry experience. Public speaker at premier, peer-reviewed, industry conferences on the subject of applied cryptography. SME with granted patents in static security research. Highly motivated, detail oriented, self-starter with deep passion for Cryptography, Application Security and Open Sourcing. Excellent communicator who can convey technical concepts in clear and concise manner. Exceptional flexibility to work independently and cross-functional teams across the globe. Proven record of leadership and mentoring skills.

PUBLIC SPEAKING & BLOG SERIES

- "JavaCrypto: Don't Just Get it Working, Use it Securely" - SecTor, 2022, JavaZone 2022
- "Cryptography Do's and Don'ts in 2021" – NorthSec 2021
- "Do's, Don'ts and How-To of crypto building blocks" - DefCon, 2020
- "How to store sensitive information in 2020?" SecTor-2020, DefCon, 2020
- "Are we using Java Cryptography API Securely?" JavaOne-2017, JavaZone-2017, AppSecUSA-2018
- Java Crypto Blog Series: Java Cryptography Blog Series
- "Building Security Analytics solution" XML Prague 2015

GRANTED PATENTS

- US 10,229,273 Identifying components for static analysis of software applications
- US 9,645,800 System and Method for facilitating static analysis of software applications.
- U.S. 9,405,906 System and Method for enhancing static analysis of software applications.

PROFESSIONAL EXPERIENCE

Lead Cryptography Software Engineer
SandboxAQ Oct 2023 – Sep 2024

- Technical Lead for Sandwich: Post Quantum Cryptography (**PQC**) enabled **crypto-agile** library
- Designed and developed cutting-edge PKI system focused on cryptographic key protection, along with observability, policy control and post-quantum readiness.

Sr. Principal Security Researcher
Veracode Inc Feb 2013 – Sep 2023

Static Security Research:
- Conduct research in leading languages, frameworks and technologies; statically detecting security anti-patterns, devising strategies and recommending flaw mitigations.
- Domain expert for cryptography, writing blueprint specifications for all cryptographic flaws.
- Work closely with other internal and external teams to give expert strategic product directions.
- Provide mentorship to newer research team members across various product lines.

Research & Development:
- Patented compiler tools to facilitate static analysis for non-grammar based templating languages.
- Architected security analytics platform to extract prevalent programming patterns.
- Developed well-designed programming language analysis tools; indispensable for research activities such as automating False Negative detection, taint analysis, etc. Non-IP part of this work is open-sourced for Java and Python.

Mansi Sheth

Email: mansi.sheth@gmail.com **Mobile**: +1 603 265 0494
LinkedIn: https://www.linkedin.com/in/shethmansi **GitHub**: https://1MansiS.github.io

Speculative Research Projects:

- Employing **Machine Learning & Natural Language Processing**, created models for locating security responsible functionality in any project.
- Finding security vulnerabilities in Ethereum smart contracts written in solidity.
- Visualizing taint flows from entry points to core security functionalities.

Sr. Technology Analyst, Enterprise Application Security Group
Fidelity Investments Feb 2007 – Jan 2013

Penetration Testing:

- Conduct Security assessments and Penetration Testing on Fidelity's critical flagship web applications and infrastructures.

Static Analysis:

- Lead developer of a static analysis product "**Assembly Line**"; factory of static analysis tools, which bridges gap of current static analysis tools.
- Industry expert in devising **Fortify Rules** to automate finding of security vulnerabilities in custom frameworks and reduce false positives and false negatives.

Security Research:

- Contributor of "**OWASP iGoat**" project. Author of iGoat Keychain exercises.
- Architectural influencer in custom security frameworks.

Lead Software Developer Aug 2002 – Jan 2007

- **Intralinks Inc , Boston, USA**
- **Accenture - Mumbai, India**
- **IRIS Ltd - Mumbai, India**

HONORS & AWARDS

- **Thought Leadership, Veracode Inc** for the maximum number of approved patents.
- **You earned it, Fidelity Investments** for outstanding security professional.
- **Super Trooper Performer Accenture, Mumbai** for an exemplary developer.

SKILLS

Languages	Java, Python, Golang, Rust
Technologies	Cryptography, PQC, Static Analysis, Web Security

EDUCATION

Master of Computer Science	University of Massachusetts, Lowell	Dec 2011
Bachelor of Engineering (Computers)	University of Mumbai, India	July 2002
Diploma in Computer Science	Maharashtra State University, India	July 1999