Venkkatesh Sekar

vsekar.me | venkkatesh.sekar@gmail.com | +44 7935168549

EDUCATION

UNIVERSITY COLLEGE LONDON (UCL)

MSc Information Security
Distinction
Grad. Sep 2021 | London, UK

NIT, TRICHY (NITT)

B. Tech in Computer Science and Engineering
Cum. GPA: 8.5 / 10
Grad. May 2018 | Trichy, India

SHRISHTI VIDYASHRAM

Grad. May 2014 | Vellore, India
Graduating Percentage: 95%

LINKS

GitHub:// **Spockuto**
G Scholar:// **Venkkatesh Sekar**
LinkedIn:// **venkkateshsekar**

INTERESTS

Post Quantum Cryptography
Secure Multiparty Computation
Fuzzing & Static Analysis

COURSEWORK

POSTGRADUATE

Introduction to Cryptography
Cryptocurrencies
Distributed Systems and Security
Computer Security I & II
Malware

UNDERGRADUATE

Principles of Cryptography
Automata & Formal Languages
Principles of Compiler Design
Principles of Probability Theory
Data Structures & Algorithms
Discrete Structures
Network Security

SKILLS

PROGRAMMING

Over 10000 lines
• C/C++ • Python • PHP

Over 5000 lines
• Java • JavaScript

Familiar
• Rust • Go • Node
• SQL • Kubernetes • Docker

EXPERIENCE

DFINITY | Product Security Engineer

Sep 2021 - Present | London, United Kingdom

- Performed **security code reviews** on critical components of the **Internet Computer** .
- Implemented security controls to identify and prevent vulnerable dependencies from being onboarded into the codebase. Currently working on improving the dynamic analysis suite by implementing continuous fuzz tests using **ClusterFuzz** .

UNIVERSITY OF SURREY | Security Researcher

Oct 2019 – Sep 2020 (FT) | Oct 2020 - Jun 2021 (PT) | Guildford, United Kingdom

- Developed a real-time vulnerability detection framework for **ASTRID** , an EU funded platform for the secure orchestration of micro-services in virtualized infrastructure.
- In-depth analysis of virtualized functions through inter-working of **fuzzing, concolic execution and remote attestation** algorithms, integrated by eBPF hooks.
- Published two papers in IJIS on concurrent works in cryptography and cybersecurity as part of **Surrey Centre for Cyber Security (SCCS)**

MOZILLA | Software Developer

September 2016 – April 2017 | github.com/Sachin-A/Blake2

- Implemented **BLAKE2 & ARGON2** from scratch, a set of **fast hashing** libraries in **C** for **Network Security Services (NSS)** as part of **Mozilla's Winter of Security**

PROJECTS

TIMELOCK ENC | May 2021 - Aug 2021 | github.com/Spockuto/timelock | Node

- Designed a **timelock encryption** protocol using **Boneh Franklin's IBE** and a beacon producing **Threshold BLS Signatures** , as part of my **MSc Thesis** .
- The protocol can **prevent frontrunning attacks** by creating timelocked transactions and decrypting them (on/off chain) after block finalization, thus **eliminating MEV**
- PoC was developed using Protocol lab's modified **drand** as the randomness beacon.

PASE | June 2017 - July 2017 | github.com/Spockuto/surrey-paks | Node

- **Encrypted file storage web application** to store, search and retrieve encrypted files based on encrypted keywords or tags.
- Authentication of users occur using high entropy keys derived from passwords using a custom two-server based secret-sharing cryptographic protocol.
- **SJCL** and **WebCrypto API** was used to implement the underlying cryptographic infrastructure and achieve native encryption speeds in browsers respectively.

BLOCKHASH Dec 2015 | pypi.python.org/pypi/blockhash | Python

- **Parallelized SHA2** for large files using multi-threading and Merkle trees.
- Achieved **50%** performance boost and **3000** package downloads.
- Support for **SHA3** was added later at **github.com/Spockuto/sha3-parallel** .

AWARDS

2016	2nd	**InOut** , India's largest student based Hackathon, NIT Surat.
2016	Finalist	Capture the Flag, **Microsoft Build the Shield**
2016	Top 200	**Google Capture the Flag** worldwide
2014	1st	Mathematical Quiz, State Level, **VIT**
2006	1st	Japanese Soroban Mental Maths National Competition

PUBLICATIONS

- MSc Thesis - Preventing front-running attacks using timelock encryption. **PDF**
- Manulis, M., Bridges, C. P., Harrison, R., Sekar, V., Davis, A. (2020). Cyber security in New Space. International Journal of Information Security. **DOI**
- Chen, L., Huang, K., Manulis, M., Sekar, V. (2020). Password-authenticated Searchable Encryption. International Journal of Information Security. **DOI**