Sayooj Samuel

Kerala, India
sayoojsamuelgreat@gmail.com
sayoojsamuel.github.io
github.com/sayoojsamuel

Education

2017 – present **Bachelor of Technology** ***Current CGPA: 9.4/10***
Semester 8, Computer Science and Engineering, Amrita School of Engineering, Amritapuri.
Graduation by June 2021.

2015 – 2017 **AISSCE** ***CGPA: 9.6/10***
Completed AISSCE with Computer Science Main from Kendriya Vidyalaya Kanjikode

Experience

2017 - present **Team bi0s** **Academic CTF Team, Amrita School of Engineering, Amritapuri**
Team bi0s primarily participates in Capture the Flag (CTF) competitions, is ranked No. 21 internationally and No. 1 in India in the year 2019 as per ctftime.org

Team Lead 2020 - present
Leading the team of passionate security researchers along with two team mates. Team lead for the cryptography working group, providing mentoring, guidance and training for team members.

Team Member 2017 - present
Active CTF player with focus on Offensive Cryptography and Cryptanalysis of standard cryptosystems. Also minor in Web Security and related research.

2018 - present **InCTF Events** **Team bi0s**
Core Organizing team and Challenge Author

InCTF Junior
Led Cryptography challenge creation team for InCTFj, a CTF conducted by team bi0s for School Students in India.

InCTF Nationals
Challenge Author and Cryptography team lead for the National edition of InCTF, a CTF conducted for University Students in India.

InCTF International
Challenge Author and Cryptography team lead for the international edition of InCTF, a 54 rated CTF on ctftime.org

Projects

June 2020 **Dragonload** *(Github)* **Developer / Maintainer**
A Distributed Download Manager which scales downloads on multiple machines to utilize high speed intranet connected to low speed internet.

- **DragonVault:** An User Portal built with Django to generate the download configuration file.
- **Dragonload:** Self titled Python module which handles distribution, download and sharing of file partitions between active download participants. This servicer relies on urllib, requests and httpServer modules.

Python / **Linux** / **Windows**

May 2020 **breakingByzantine** *(Github)* **Developer**
An optimization to Byzantine Generals problem in distributed computing. Our solution proposes a fault tolerant 3 party consensus in synchronous and asynchronous setup.

Results are achieved with MAC and Time authenticated messages, wherein forging faulty messages are restricted with high cost of generating valid MAC. Proposal is supported with a model of grpc enabled python nodes exchanging authenticated decision to reach a common consensus.
Python / **Linux**

December 2019 — **crypot** *(Github)* — **Developer / Maintainer**
A Cryptography Toolkit and library developed by teambi0s, compiling exploits and attacks. Contributed to public key crypto exploit collection and CLI utility. The collection extends to cover DLP and weak Elliptic Curve vulnerabilities.
SageMath / **Python** / **Linux**

April 2018 — **Soul Keybase** *(Github)* — **Developer / Maintainer**
A Public Keybase REST API Client based on Spring Boot and Java Security. The service creates, stores and authenticate users based on strong RSA keypairs, while serving as a directory listing for User's public keys. This project was initially inspired from keybase.io.
Java

Achievements

December 2020 — **Bronze Medal** *(Certificate) (Scoreboard)* — **International Olympiad in Cryptography**
Won the bronze medal in the category of University Students in the International Olympiad of Cryptography - NSUCRYPTO'20.

December 2019 — **Certificate of Diploma** *(Certificate) (Scoreboard)* — **International Olympiad in Cryptography**
Awarded the Certificate of Diploma for conquering the leaderboards of the International Olympiad of Cryptography - NSUCRYPTO'19.

April 2020 — **Champions, International** — **IJCTF**
Finished the online CTF emerging as the winner, as a part of Team bi0s.

June 2019 — **Champions, International** — **ISITDTU CTF, Duy Tan University, Vietnam**
Champions in the online qualifiers round, as a part of Team bi0s.

Feb 2019 — **Runners Up, International** — **NullCon Security Conference**
Finished the race as runners up in the International CTF, along with Team bi0s.

October 2018 — **Champions, International** — **Hack.lu CTF, Ruhr-Universität, Bochum, Germany**
Crowned the winner in the online CTF organised at the Hack.lu Conference at Luxembourg.

December 2018 — **Certificate of Excellence** — **Amrita Vishwa Vidhyapeetham**
Awardee of Certificate of Excellence exemplary efforts and achievements on the international level.

Skills

Practical Cryptanalysis, Protocol Auditing,
Web Exploitation, Automation, Data Analytics

Research Interest

Public Key Cryptography, Owasp Top 10,
Authentication Models, Fault Injection Attacks,
Linear and Differential Cryptanalysis

Languages

Python, C, C++, Java, Bash

Tools and Frameworks

Cryptool, SageMath, Burp Suite,
Zap Proxy, IDA, Wireshark

Platforms

GNU/Linux, Windows

Workshops Attended

December 2020 — **VeriCrypt: An Introduction to Tools for Verified Cryptography** *(Workshop)* — **Indorypt 2020**
Selected for the workshop on Formal methods and verification tools hosted as part of the Indocrypt Annual Conference on Cryptology, 2020. The workshop included sessions introducing Tamarin Prover, Cryptoverif among other tools with lab exercises. The sessions also detailed how these tools are leveraged for verification of cryptographic primitives and protocols.

January 2020 — **Secure Multi-Party Computation: Theory and Practice** *(Workshop)* — **IISc, Bengaluru**
Selected to attend the workshop on Multi Party Computation (MPC) research as a part of Golden Jubilee Celebrations at IISc. Secure MPC allows n-party computation of joint function over private inputs ensuring privacy and correctness.