Joshua **Limbrey**

Information Security · Cryptography · Software Dev

joshua@supinie.com | supinie

~/

A technically adept, complex problem solver with a proven capability for the highest performance, combining a mathematical background in cryptography and group theory with passion and competency in cryptography and information security.

Awarded Distinction for my MSc thesis on the cryptanalysis of lattice-based PQC, with a focus on Kyber. Developing a no_std Rust library for Crystals (Kyber and Dilithium), with integration to Rust Crypto compatible traits. Aiming to drive the adoption of quantum-resistant cryptography by providing secure and efficient implementations of Kyber and Dilithium in a low-level, memory safe language.

~/education/

Imperial College London

London, UK

PhD *Sep. 2024 - Present*

- Studying the hardness of lattice based cryptography, with a focus on structured lattice reduction algorithms, and evaluation of post-quantum schemes.

Royal Holloway, University of London

Egham, UK

Information Security MSc. Distinction *Sep. 2021 - Sep. 2022*

- Achieved distinction for my dissertation on cryptanalysis of post-quantum LWE based encryption schemes.

Royal Holloway, University of London

Egham, UK

Mathematics BSc. Hons 1st *Sep. 2018 - Jun. 2021*

- Awarded the University of London Wynne-Roberts Prize in recognition of outstanding academic effort and achievement as the highest performing Mathematics student.

~/skills/

Programming	Rust, Go, Python, Ruby, Node.JS, LaTeX
Mathematical	Cryptography, Group/Field Theory, Number Theory, Information Theory, Probability/Combinatorics, Algorithm Design
Systems	AWS, GNU/Linux, Metasploit, Docker, Kubernetes, Nmap, Bash, Burp

~/open_source/

ML-KEM/Kyber

Rust Crypto

- Identified and patched the KyberSlash timing sidechannel attack in the Rust Crypto implementation.
- Contributed to update key formatting and handling to reduce private key sizes by up to 90%.

Nixpkgs

Summer of Nix/Contributor

- Contributor and maintainer for a number of open source privacy related packages within the Nixpkgs ecosystem.
- Began contribution through the Summer of Nix scheme, through which I learnt how the Nix ecosystem works, began contributing under a mentorship scheme, and was able to attend NixCon.

~/experience/

Supinie Solutions LTD

London, UK

PRINCIPAL SOFTWARE DEVELOPMENT ENGINEER *Jun. 2023 - Present*

Core responsibilities:

- Engaging key stakeholders to gather requirements to ensure the solution meets business needs
- Designing and architecting a full-stack solution built in AWS
- Utilising agile workflow methods and CI/CD principles to improve overall productivity and release cycles
- Implemented back end databases, as well as dependable integration with external APIs

Value added:

- Implemented a secure user accounts and authentication system, including organisation management and access control
- Strong logical separation between components alongside rigorous access management controls leading to increased security and robustness
- IdP SSO integration alongside custom authorisation flow to create a smooth and natural UX

Amazon Web Services

Reading, UK

SYSTEM DEVELOPMENT ENGINEER *Sep. 2022 - Jun. 2023*

Core responsibilities:

- A key member of a small team that built AWS Service Catalog into 6 new regions
- Worked to update the region build process to implement robust automation
- Hands on experience maintaining global services
- Owned the full software lifecycle from development, through deployment, to supporting production via CI/CD

Value added:

- Personally owned the build and deployment of 4 internal component services
- Found and created a fix for a fatal bug in an AWS-wide tool
- Refactored internal component service and documentation to remove manual touch points during region build, and reduce technical debt; improving stability and reducing build time by ~1 month
- Insisted on the highest standards, set the standard/best practices for many implementations of automation
- Automation for region build cut down the engineering hours required for new regions by a factor of 10
- Upskilled fellow team members through the creation of new training materials, delivery of in-person engineering development days, and weekly experience exchanges amongst ~50 engineers as a subject matter expert
- Created and developed a new collection of developer tools and scripts to aid engineering workflows within AWS and Service Catalog

Cyber Software Development

London, UK

SOFTWARE DEV *Jun. 2021 - Sep. 2021*

- Developed a unique covert communication capability utilising decentralised peer-to-peer communications
- Full stack web-dev
- Worked with Node.JS back-end and Svelte front-end

~/extracurricular_activity/

Royal Hackaway

Royal Holloway, University of London

BEST WEB-APP WINNER *Jan. 2022*

- Won 'Best Web-App' and finished top 5 overall.
- Participated in a 26 hour national hackathon in a team of two.
- Developed a Svelte web-app with a Python machine learning back-end to predict the weight of an unborn child based on antinatal datapoints.

Guba Doce Pares **(Eskrima-Kali-Arnis; a Filipino stick and dagger martial art)**

London, UK

BLACK BELT/REGISTERED INSTRUCTOR *2014 - Present*

- National men's open close quarters champion, single and double stick national champion, and single stick international champion.
- As a senior member, I spent many years teaching younger members of the club.
- As a registered instructor, I am looking to set up my own club in the near future.

RHUL Esports

Royal Holloway

TEAM CAPTAIN *2019 - 2022*

- Led the Overwatch esports teams, overseeing both GameSoc events and national tournament entries due to my active contributions to the team as a top 100 player in Europe.
- Our team had multiple top 5 finishes in national leagues.

Old Elthamians

Bromley, UK

YOUNG LEADER *2014 - 2018*

- Coached young members of the club, and scoring and umpiring all ages games.
- Awarded a Jack Petchey award for my contributions to the cricket club through the young leaders' programme.