Jack Lloyd
jack@randombit.net
https://randombit.net

Professional Experience

Apr 2021-Present: Senior Developer at DFINITY

- As a member of the cryptography team I wrote Rust code providing cryptographic services required by the higher levels of the Internet Computer.
- Implemented a new threshold ECDSA signature scheme, allowing the IC to transact in BTC.
- Optimized and side channel secured the NIDKG implementation used in the consensus mechanism, removing timing channels while also speeding up most operations by a factor of 2 to 4.

Jun 2020-Mar 2021: Developer at Signal Messenger

- Wrote a new implementation of the Signal client protocol in Rust, along with Java and Swift bindings. Integrated this new library into the existing Signal mobile and desktop applications, replacing the 3 previously used, independently created and occasionally divergent protocol implementations. (`https://github.com/signalapp/libsignal-client`)

Nov 2018-Jun 2020: Senior Engineer at Fortanix

- Maintaining and improving the cryptographic core of Fortanix's FIPS L3 validated HSM product. The product is written almost entirely in Rust, with small amounts of C for low level cryptographic operations. My work included adding post-quantum algorithm support, side channel hardening and performance improvements for critical algorithms, and adding new APIs to the Lua environment allowing customers to run their custom business logic within the HSM.

Mar 2017-Nov 2018: Independent Security Consultant

- Development projects including integrating new cryptographic algorithms into OpenSSL, adding features to a C language OpenPGP library, and implementing cryptographic functionality for an IoT system running on i.MX 6 platform.
- Reviewed security of customer software, including a blockchain application written in Python, an OAuth library written in PHP, custom TLS authentication code in C++, and a DNS server written in C.

Dec 2009-Mar 2017: Senior Developer at Broadway Technology

- Wrote services in C++ handling tasks such as exchange connectivity, rule-based trade execution, systems statistics aggregation, and cluster-wide process mangement.
- Was Broadway's subject matter expert on Linux internals and behavior.

Feb 2007-Jul 2008: Developer at Volant Trading

- Wrote Linux server processes in C++ that handled exchange connectivity, profitability analysis, and trade reconciliation.

May 2006-Feb 2007: Senior Consultant at Stratum Security

- Analyzed customer software for security flaws, reported findings and assisted customers with remediation.

Sep 2005-May 2006: Security Engineer at Atlan Laboratories

- Validated hardware and software cryptographic systems against NIST FIPS-140 standard.
- Maintained and extended Atlan's set of internal tools used for testing and automated analysis.

Feb 2004-Aug 2005: Security Engineer at Cybertrust

- Performed security review of customer software and network systems. Wrote reports identifying issues and assisted developers with remediation.

Open Source

- Botan - a C++ cryptographic toolkit and TLS protocol implementation. Used in numerous commercial and open source projects including automotive and industrial systems. Approved for government/NATO use by the German Federal Office for Information Security. `https://github.com/randombit/botan`
- An implementation of the BN elliptic curve pairing in Python `https://github.com/randombit/pairings.py`

Security Research

In my spare time I enjoy reading through open source code looking for security flaws. Bugs I have found include side channel vulnerabilities in mbedtls (CVE-2019-16910) and Microsoft's SymCrypt (CVE-2019-1171), a denial of service in PolarSSL (CVE-2013-4623), a BLS signature forgery bug in the DEDIS Kyber crypto library, and weak RNG usage leading to key compromise in GNU Classpath's JCE implementation (CVE-2008-5659),

Education

2003, B.Sc. Computer Science, The Johns Hopkins University, Baltimore, MD