

KYLE ISOM

Email: coder@kyleisom.net

Phone: +1.303.335.9072

LINKS

- Homepage - <http://www.kyleisom.net/>
- Github - <https://github.com/kisom/>
- Go Projects - <http://www.gokyle.org>

EXPERIENCE

Security Engineer

Echostar Technologies
Englewood, CO

Summer 2010-Present

Conduct code audits, primarily in C; implement security systems in Linux kernel; write Python scripts to support encrypted software updates for Linux-based set top boxes.

SKILLS

Development: C, Go, Python, Unix / POSIX programming, network programming, security engineering, cryptographic engineering.

Software Engineering: GNU autotools suite, \LaTeX , Texinfo, Unix man pages.

Development Tools: valgrind, lint, rats, vim, emacs.

Development Cycle: Build system setup, documentation, unit testing.

Security: secure programming, reverse engineering, penetration testing.

Deployment: basic familiarity with Puppet and writing Upstart scripts.

SELECTED PROJECTS

Practical Cryptography with Go (Go)

- Book is being published on Leanpub as it's written.
- Homepage: <http://gokyle.org/book/>
- Introduces cryptography to developers who may not have a solid understanding of not only cryptography, but also when to use it and how to safely use it to improve the security of systems.

DHKAM (C and Go)

- C and Go implementations of blinded Diffie-Hellman key agreement using the RFC 3526 group 14 modulus.
- There is also an example implementation of the elliptic curve Diffie-Hellman key agreement method.
- The homepage contains links to all three versions: <http://tyrfingr.is/projects/dhkam>

RSASSA-PSS in Go

- Patch to the Go programming language's standard library to implement the RSASSA-PSS signature scheme from PKCS #1 v2.1.
- After submitting, found out another implementation had gone in two weeks prior.
- Code is on Github as an example: <https://github.com/gokyle/rsa>

srvwd (C)

- Homepage: <http://www.tyrfingr.is/projects/srvwd/>
- Simple file server that serves files in the current working directory.
- Designed to facilitate rapid testing of statically-generated sites.

libbase64 (C)

- OpenBSD base64 functions extracted to an external static library.
- Homepage: <http://tyrfingr.is/projects/base64/>

pypcapfile (Python)

- Homepage: <https://github.com/kisom/pypcapfile>
- Pure Python library for handling libpcap savefiles.

filecache.go

- Homepage: <http://gokyle.github.com/filecache/>
- A simple filecache implementation in Go.