Robbie Harwood <rharwood@pm.me >
GitHub: https://github.com/frozencemetery phone: (508)-397-3117
website/blog: https://mivehind.net location: Boston, MA

I am a systems programmer, focusing on security engineering and cryptographic trust. I write well, both for documentation and in engineering standards bodies. I value mentorship of junior employees.

Employment

Red Hat, Inc. (Intern: Summer 2013, **Senior Software Engineer**: 2014 - present)
- **Bootloader** enablement engineer (2021 - present)
  * Upstream developer of grub2, shim, efibootmgr/efivar, and related technology
  * Work focused on **Secure Boot** development on behalf of RHEL + Fedora
- **Kerberos** Development Lead (until 2021)
  * Upstream developer of MIT Kerberos (krb5) and related technology
  * Created world's first FIPS 140-2 compliant Kerberos implementation
  * Interoperability work with Active Directory as part of FreeIPA team
  * OpenSSL contributor (KDFs, krb5 integration, and test suite)
  * Co-author of python-gssapi (Python bindings to GSSAPI and Kerberos)
  * Wrote HTTPS transport for krb5, reverse engineered from Microsoft's KKDCP protocol
  * Responsible for deprecation / removal of DES, 3DES, and RC4 in krb5
- Package maintainer in RHEL, Fedora, CentOS, EPEL, and Debian
- Formal mentor of several interns and junior employees

Carnegie Mellon University (Fall 2013)
- Teaching assistant: Compiler Design (15-410)
  * co-author of the (obfuscating) reference compiler

Education

Carnegie Mellon University (2011 - 2014)
- B.S. in Computer Science, minor in Ethics/Philosophy
- Featured courses: Operating Systems (15-411), Compiler Design (15-410, later TA)
  * co-wrote UNIX-like kernel with a bootloader and SMP support

Standards bodies

- Member and contributor to UEFI Specification and Security Working Groups (USWG + USST)
- **Chair, IETF kitten** (Common Authentication Technologies, N.G.) working group (2018 - 2022)
- Author on Standards Track Document: Deprecate 1024-bit Diffie-Hellman Moduli in Kerberos PKINIT
- Co-author on Standards Track document: SPAKE Pre-Authentication
- Co-author on Standards Track document: Channel Binding Signaling for GSSAPI
- Contributor to US NIST 800-63-3 ("Digital Identity Guidelines")

Talks and conferences

- Devconf.cz (2021): Proposal reviewing committee, Security / Identity Management track
- Devconf.us (2020): Proposal reviewing committee, Systems Engineering and Hardware track
- MIT SIPB Cluedump (2019): *Kerberos 30 Years Later (A Modern Cryptographic Overview)*
- Devconf.cz (2018): *Unleashing the Underworld: Kerberos for Developers*
- MIT SIPB Cluedump (2017): *Kerberos: An Introduction from the Underworld Up*
- Flock to Fedora (2015): *Conquering the World with Kerberos*

(continues)

Tooling

- Programming languages in regular use (~10 years): **C**, Python, shell, x86/amd64 assembly
- Other programming languages: Rust, Haskell, Standard ML, Lisp (various)
- Development: Linux with: git, gcc + clang, gdb, valgrind, wireshark, autotools / make, meson
- Spoken languages: English (native/professional), Spanish (intermediate), Norwegian Bokmål (beginner)

Interests

- work-related: systems, security / cryptography, reverse engineering, protocols
- other: guitar, audio production, fermentation, hiking / camping, bicycling, obsolete hardware