Kenneth G. Raeburn

Cambridge, MA 02140
raeburn@mit.edu

Skills:

Interests	Network protocols and security; cryptography; compilers; operating systems; distributed systems.
Programming Languages	Working daily in C, GNU Emacs Lisp, Bourne shell, C shell. Some experience with C++, Tcl, Perl, TeX/LaTeX, Python, Scheme, some assembly languages.
Operating Systems	Primarily UNIX (including Mac OS X, Linux, Solaris, NetBSD, AIX, Tru64, HP-UX) with some Windows and Multics experience.

Experience:

Massachusetts Institute of Technology Cambridge, MA 1999—2009
Senior Programmer Analyst, Information Services & Technology

- Enhanced and maintained Kerberos 5 software.
  - Implemented new features and bug fixes, major and minor, including improved error reporting and testing. Implemented shim layers for cross-platform thread safety, IPv6 and basic plugin support, including stubs for configurations missing the basic OS support, resulting in simpler internal application and library code able to use these services when available.
  - Analyzed code for security vulnerabilities. Distributed security advisories. Initiated a survey of static analysis tools for code quality improvement, and fixed some of the problems found.
  - Surveyed MIT Kerberos Consortium sponsors and outside developers for desired functional and documentation improvements, and created detailed proposals for discussion to determine future work.
  - Supported external developers and users via mailing lists, and MIT developers in person. Reviewed and integrated bug fixes and code donations from outside contributors. Supervised a student programmer.
- Work with IETF on Kerberos and GSSAPI protocol revisions and enhancements, including writing, editing, and otherwise contributing to RFCs.
- Assisted with unofficial campus network 6bone experiment and IPv6 support.

Cygnus Solutions Cambridge, MA 1991—1999
Member of technical staff

- Maintained and enhanced Kerberos software, versions 4 and 5; including simplification of installation procedures, and coordinating changes with MIT.
- Added enhancements and bug fixes to GNU C and C++ compilers and assembler, for native and embedded-system target platforms, including parser changes, code generation and optimization changes, processor description enhancements, workarounds for processor defects, and testing in emulators or embedded systems. Maintained assembler and "binutils" packages for Free Software Foundation, including making several releases. Aided in testing compiler tools during release cycles.
- Certified compiler tools and embedded system support and emulation code for Y2K compliance; provided patches for customers for the problems found.
- Performed on-site trouble-shooting in both Kerberos and embedded-system compiler tools for customers.

Watchmaker Computing Cambridge, MA 1990—1991
General partner
Co-founded a consulting partnership, for porting and packaging Project Athena software and other contract programming work.

- Worked on DEC/Athena support.
- Ported AT&T's C++ translator to new platforms.
- Wrote an initial implementation of C++ templates for Cygnus Solutions.

Massachusetts Institute of Technology Cambridge, MA 1985—1991
Student Systems Programmer / Systems Programmer II, Project Athena
Enhanced and maintained external and locally-developed UNIX and Multics system software in C (and occasionally C++, PL/1, and assembler), including some performance improvements and release engineering work.

Other:

Education **Massachusetts Institute of Technology** Cambridge, MA
S.B. degree in Electrical Engineering and Computer Science, 1988.
Graduate course in cryptography, spring 2005.

Publications "The Kerberos Network Authentication Service (V5)," with Sam Hartman, Tom Yu, and Clifford Neuman, RFC 4120, Internet Engineering Task Force, July 2005.

"AES Encryption for Kerberos 5," RFC 3962, Internet Engineering Task Force, February 2005.

"Encryption and Checksum Specifications for Kerberos 5," RFC 3961, Internet Engineering Task Force, February 2005.

"The Perils of Unauthenticated Encryption: Kerberos Version 4," with Tom Yu and Sam Hartman, published in *Proceedings of the Network and Distributed Systems Security Symposium*, The Internet Society, 2004.

"*Discuss:* An Electronic Conferencing System for a Distributed Computing Environment," with Jon Rochlis, William Sommerfeld, and Stan Zanarotti, published in *Conference Proceedings, 1989 Winter USENIX Technical Conference.*

Memberships/ Associations Internet Engineering Task Force; currently appointed "designated expert" for review of new Kerberos encryption systems to be added to IETF registry.
Association for Computing Machinery.

Other Activities Occasional contributions to GNU software projects, primarily Emacs but sometimes Guile or GCC.
MIT Gilbert and Sullivan Players (house manager and webmaster).