Sam Roberts
Vancouver, BC, Canada

Email: vieuxtech@gmail.com
URL: http://sam-github.github.com

Career

Software developer with more than 18 years of experience in a variety of industries, languages, and platforms. Consistently develops innovative tools and technologies that are adopted as core elements of my companies' software development and business practices. Particular interest in operating system services, network protocols, and programming languages.

Skills

Multi-language and platform development: C, Lua, Ruby, Python, C++, Objective-C, Clojure, Linux, QNX, iOS, OS X, VxWorks, Win32, BeOS, WinCE, Symbian, RIM.

Systems programming: event-driven and non-blocking I/O, embedded and real-time systems, device drivers and kernel modules, pseudo filesystems and resource oriented systems, sockets and low-level network programming.

Network protocols and data formats: TCP/UDP/IP, multicast/broadcast, HTTP, POP3, SMTP, IMAP, MIME, mDNS/DNS-SD ("Rendezvous" or "Bonjour"), ASN.1/BER/DER, vCard, iCalendar, BEEP, Zigbee, XML.

Cryptography: CMS, S/MIME, SSL/TLS/WTLS, X.509/PKIX, PKCS #1, #5, #7, #8, #9, #11, and #12, smart cards and hardware accelerators, cryptographic APIs (OpenSSL, Cryptoki, BSAFE, Cswift, CAC), RSA, Diffie-Hellman, and Elliptic Curve crypto-systems.

Development tools: Debian packaging, GNU tool chain (gcc, make, bash, texinfo), qt, cocoa, regular expressions, perl, shell, sqlite/SQL, git/subversion/perforce/CVS/RCS, Wireshark.

Languages: English, French (conversation), Japanese (pretty rusty).

Education

B.A.Sc. in Engineering-Physics, Computer Science Option, 1996
University of British Columbia

History

Senior Architect
Wurldtech (wurldtech.com)
April 2012–present

Architect for an extensible and embeddable intrusion prevention system, still in development.
Achievements:
- TCP reassembly and rule-controlled data windowing allows resistance to common evasions of IPS.
- Protocol dissectors and rules portably specified in Lua, leading to run-time extensibility of protocol support.
- Same rules can be used with both Linux nfqueue and VxWork's firewall for packet processing.

Development Lead
Wurldtech (wurldtech.com)
May 2007–Nov 2012

Lead a team of eight developers on a Linux-based appliance for automating network security testing of industrial equipment.
Achievements:
- Shipped product within first year of development using an agile development process based on Scrum, using development practices such as continuous builds, unit/system/integration tests, automated deployment, etc.
- A network protocol implementation and test framework in Lua, including bindings to Linux networking APIs.
- Structured test platform as thin java/swing client, communicating over XML/BEEP to a python/twisted server on Linux platform.
- Learned, implemented, and developed tests for many IPv4 and industrial protocols (modbus, OSI over TCP, ENIP/CIP, ZigBee, etc.)
- Interfaces to digital and analog I/O, using comedi and USB SDKs.
- Wireshark dissectors for ZigBee and WirelessHART in Lua.
- Managed outsourcing of test appliance hardware platform.

Senior Software Architect
Bycast (bycast.com)
Nov 2005–June 2007

Maintain and enhance a distributed fixed-content storage system composed of a redundant, fault-tolerant, and load-balancing grid of Linux servers.
Achievements:

- Implemented Grid communication protocols in C and Ruby, allowing programmatic interaction from Ruby to a running Grid.
- Exposed Grid capabilities through an RPC-like API, based on HTTP/1.1 and XML, allowing custom 3rd party application integration.
- Integrated Lua into Grid nodes for scripting, component development, interactive debugging, and testing.

Senior Software Developer
Certicom Corp. (certicom.com)
Oct 2000–Oct 2005

Developed C language cryptographic toolkits optimized for high performance and low memory usage.
Achievements:

- Proposed architecture for integrating 3rd party cryptographic support into Certicom's Crypto and protocol toolkits. Proposal was adopted as the Crypto-C API and integrated into all products (IPSEC, TLS, PKI).
- Implemented Crypto-C support for Security Builder, CryptoSwift, BSafe, and PKCS#11.
- Designed Certicom's PKI-C toolkit.
- Implemented cryptographic key store architecture, and plugins using LDAP, file-based PKCS#12, CAC smartcards, Cryptoki (PKCS#11) smartcards, and WinCE servers. Integrated key stores into PKI-C.
- Developed tools to process product headers into API documentation using Ruby, doxygen, XML, MIF, and Framemaker. Tools adopted by the documentation group for use with all C products.
- Developed Ruby extension support for the Cryptoki (PKCS#11) SmartCard API.
- Implemented automated tests designed to expose protocol and memory usage errors, and fixed them.

Software Developer
Cogent Real-Time Systems (cogent.ca)
1998–Oct 2000

Custom QNX development for clients in C and gamma, Cogent's LISP-based rapid application development language.
Achievements:

- Implemented QNX's Send/Receive/Reply Message Passing API for Linux as a loadable kernel module. Cogent's QNX-based tool chain runs unmodified under Linux using it, and real-time Linux development is now part of Cogent's business strategy (cogent.ca/Software/SRR.html).
- Maintained the file, DNS, and news servers and the Linux firewall.

Development Lead
International Submarine Engineering (ise.bc.ca)
1995–Oct 1998

Managed the maintenance and development of ACE, a component-based, runtime configurable, asynchronous event-based kernel implemented in C++.
Achievements:

- Ported ACE kernel to QNX and advocated its use for new projects. Implemented drivers, communication libraries, and ACE components for a remotely operated underwater vehicle.
- Designed and implemented a system for controlling two 7-arm manipulators for the Canadian Space Agency. System is an extensible team of processes sharing data between QNX nodes over a shared-memory network to provide torque and position control at 1 kHz. The core processes and ScramNet network driver were implemented in C++.

Interests

libnet Adopted this widely used packet crafting and injection library, fixed the known bugs, and re-released. It has been accepted downstream by Debian and Fedora, and I continue to maintain it. (github.com/sam-github/libnet)

vPim. Ruby support for vCard and iCalendar formats, and various tools that use them, such as publishing OS X/iCal todo items as an RSS feed. (github.com/sam-github/vpim)

open source Protocol toolkits (BEEP support for lua, ZeroConf for ruby), lua bindings to C/C++ libraries, contributor to luasocket and GNU mailutils, ancient QNX virtual filesystems. (sam-github.github.com)

Judo. Black belt (1st degree), and instructor of both children and adults.

Rock Climbing. Climbed across North America, from Canada to Mexico.