Michael Richardson (v:20220805)

Personal Information

Languages

English Fluent, French Conversational

Contact Information

Address: 470 Dawson Avenue, Ottawa, Ontario, K1Z 5V7
Phone (mobile): +1 613 276-6809
Email: mcr@sandelman.ca
Web: http://www.sandelman.ca/mcr/
Resume:http://www.sandelman.ca/mcr/resume/ (PDF)
Googletalk: mcharlesr@gmail.com

IETF Details

https://datatracker.ietf.org/person/Michael%20Richardson

Linkedin:

http://www.linkedin.com/in/mcr314

Github:

https://github.com/mcr/

Stackoverflow:

http://stackoverflow.com/users/74074/mcr

Work Experience

Sandelman Software Works Corporation

IETF ANIMA implementation, IoT onboarding

2016 to 2022

With support from several major router vendors, co-led IETF ANIMA WG secure bootstrap design team, resulting in RFC8366 (vouchers), RFC8995 (BRSKI), as well as open source reference implementation at: Minerva ANIMA reference implementation. This is the BRSKI effort. Worked through record setting 9 month long IESG review, resulting in the base document finally being approved in April, 2020, with publication in May 2021. Lead weekly multistakeholder BRSKI Design Team to work on multiple extensions to BRSKI, constrained-BRSKI, updates to multiple other dependant RFCs. Lead regular Remote ATtestation proceedureS (RATS) Architecture design team. Helped create IOTOPS IETF Working group focused on IoT operations and security.

CIRA Secure Home Gateway project

2018 to 2021

In order to prepare for the defense of critical Internet infrastructure against the next "Murai"-style Distributed Denial of Service attack, the Canadian Internet Registration Authority (cira.ca) started the Secure Home gateway project The project is to defend IoT devices from Internet attacks, and defend the Internet from IoT devices. The use of RFC8520 standard Manufacturer Usage Description files was a critical part of the October 2018 proof of concept. After some struggles in direction, the project will go into an Alpha test in 2020 as soon as lockdown ends. Led the security stance for the project, introducing and mentoring a number of junior programmers into their first OpenWRT work, using lua, python, shell, Android Java and C. Wrote IETF Internet Drafts to document the parts that the project felt should be industry best practices, leading to the RIPE IoT WG starting a Best-Current Operating Practice (BCoP), which is underway. Throughout this project, have been the OpenWRT (and Turris OS) wrangler, producing the "MEDKIT" to flash new devices. Designed a customized version of IETF BRSKI protocol ("smartkaklink") to accomodote onboarding of the home router without Internet.

IETF Roll implemenator

2009 to 2020

Wrote an open source implementation of the IETF ROLL RPL protocol for the Linux platform, called unstrung. Release 1.0 is yet to come, but have collaboration from one UK company.
Worked with RPL implementation in Contiki-OS.

IETF Roll co-chair

2012 to 2016

Was asked in 2011 to become the IETF ROLL working group co-chair. Was given a mandate to finish off the security aspects of the ROLL protocol, and many of the related security problems. Trained a new co-chair in late 2013. As part of this work, liased with the Zigbee IP specification writers, became involved with 802.15.4e mode of 802.15.4, leading the security design team of the IETF 6tisch working group, and co-lead for the IETF ANIMA secure bootstrap design team.

President

1996 to present

Formed Sandelman Software Works as a contract programming and internet security consulting firm. Projects include: device driver development, embedded Linux (PowerPC405, x86, ARM), VPN/IPsec internals /kernel architecture (FreeS/WAN project), BGP setup (both IPv4 and IPv6) and configuration, gForge/Savannah deployment, corporate security policy creation, network design and architecture, firewall evaluation, securing web servers, secure database replication, Virtual Private Network design, project management, Unix systems management, and cryptographic programming (IPsec).

CREDIL: Founder and Managing Editor

YARN project

July 2013 to 2016

Michael updated a Linux-based PPPoE appliance to include IPv6 functionality: DHCPv6 (RFC3315), Prefix-Delegation (RFC3633), packaging, security updates, specification and evaluation of target hardware, customer support, performance testing using SPIRENT system.
Michael worked with the DHCP WG RFC3315bis design team to publish RFC8415.

Orlando/datatracker.ietf.org

October 2012 to January 2014

Michael lead a team of two to work on an automated and computer-assisted scheduling system for IETF conferences. This involved in django (1.2), javascript (jQuery, JQUnit) and MySQL.

Sombrero/Heart-of-Gold project

August 2011 to May 2012

Michael worked on the embedded Contiki operating system on two projects. Both used the MSP430F54F38 processor; one used the GNU gcc tool-chain, the other used the IAR MSP tool-chain. Network protocols were involved in both cases: TCP/HTTP/HTML in one, and I2C in the other.

Hydra project

March 2010 to March 2014

Michael worked on a virtual desktop solution for translation students and professional. Managed by a Rails system (see wiki (php5, tikiwiki) and portal), with agents written in perl, visual basic, and powershell, a series of XEN servers provides computing services to 150 students simultaneously.

GAP project

December 2009 to October 2013

Michael brought IPv6 expertise to a number of CREDIL sponsor members, including managing a project to bring fiber-optic Internet (IPv4 and IPv6) to an industrial park in Montreal. This included deploying and debugging routing equipment from multiple vendors to run: STP, BGP4, OSPF, SIP. Michael continues to act as Network Architect, having successfully hired and trained operational staff.

SG1 project

Fall 2011 to October 2013, March 2015 to October 2017

Create customer facing front end (django) and support focused back-end (rails) system to process and present Call Detail Records (CDRs) for VoIP telco. The system has to process 100K records/day, and guaranteeing that one client will not

see the other client's records. Extensive postgresql database tuning while managing a team of 3 programmers.

Thomas Watson project

December 2009 to Summer 2010

worked on a new Android phone. Bring up of phone (embedded Linux), debugging, project management. The CREDIL team worked on an H.264 video calling application requiring real time embedded Linux programming, and working with hardware encoders.

Internet Software Consortium

Operations Developer: Solid Name Service (SNS)

January 2014 to October 2014

Took over development and maintenance of anycast based DNS service called SNS. Care and feeding of FreeBSD and Linux based infrastructure, with sh, perl, awk, javascript, Catalyst, PostgresQL and MongoDB components. Took system from all-in-one physical server to easily replicatable and testable VMware vSphere based virtual machines in a more typical front/middle/backend stack.
Updated the DNSSEC Lookaside Validator (dlv.isc.org), from a ruby 1.8/rails 2/postgresql 8 system, running on FreeBSD 7 hardware, to a ruby 1.9/rails 3/bundler/capistrano/postgresql 9 platform, based upon Linux and FreeBSD 10 virtual platforms.
Participated in some day-to-day activities around f-root server operation and planning.

SIMtone Corporation

Director, Consumer Desktop Development

April 2007 to August 2009

Consumer Desktop Unit (CDU), In charge of overall technical direction for the business unit. Manage people, projects, schedules, and write code. The CDU unit provides virtualized desktops to end-customers using XEN and VMware machine virtualization. Backend management was done by IPv6. Custom software provides provisioning, monitoring, and sign up. Software is written in C, Ruby (on Rails), PHP5/Drupal5, Perl, Java and Visual Basic, using XEN, VMware-server and ESXi APIs.

Xelerance Corporation

VP Research and Development

August 2003 to 2007

Formed Xelerance Corporation. Xelerance Corporation is the Open Source security specialists. Xelerance was the home of Openswan: IPsec for Linux (and continuation of Linux FreeS/WAN). Xelerance also dealt with DNSSEC, producing a product, dnsX. Xelerance practiced Test Driven Development, and geographically dispersed agile methods. As a hands-on VP of R&D, I was in charge of all software development, costing and scheduling for projects. Worked with a number of partners to bring hardware accelerated cryptographic operations to IPsec.

Solidum Systems Corporation

Chief Software Designer

February 1998 to October 2000

Responsible for for multiplatform development environment. Consulting with hardware designers and product managers on appropriate design of multi-gigabit packet classification ASSP. PCI device driver work for Linux, NetBSD and VxWorks for multiple products, including network adapters. Technical liason with partners, including most major NPU vendors, lookup engine vendors, and operating system vendors. Worked on all major layer 2, layer 3+ protocols: **MPLS, Ethernet, Packet-over-SONET, IPv4, IPv6, TCP, L2TP, PPPoE, ATM/LANE, SSL, HTTP.**

Field Application Engineer

October 2000 to August 2001

Given superior communications skills, was asked to join salesforce. Responsible for technical presentation to prospective customers, customization of solution to customer need, specification of product requirements, and delivery of technical solutions to customers.

Solidum was acquired by IDT in the fall of 2001.

Milkyway Networks Corporation

Technical manager, System Software

October 1994 to October 1996

Responsible for multiplatform development environment, project schedule, functional specification and assignment of work. Majority of Unix kernel work. C/CVS/Perl under Unix (BSDI/386 and SunOS). Maintenance of ongoing product. Porting to SVR4. Liason to IETF, advanced product research: IPsec, Kerberos, customization. Some VxWorks and ObjecTime. Milkyway Networks (now defunct) made the world's first transparent application layer firewall, originally called the BlackHole.

Bell Northern Research (BNR)

April to October 1994

Work group administrator in FiberWorld Products division. Internal telephone support for computing environment including day-to-day system management, and problem resolution. 1000+ user population on heterogeneous Unix networks (NCD,Sun,HP,Apollo,Mac).

(BNR + Northern Telecom merged to become Nortel and then Nortel Networks)

Achilles Networking

parttime 1992 to 1996

System administrator in startup internet services company. Set up and support for email (DNS, SMTP, UUCP, etc..) and news (INN: NNTP and UUCP). Security auditing.

Carleton University, Ottawa

August 1993 to 1994

Publisher and technical support for a new electronic journal: Conservation Ecology: a peer reviewed journal. Experience with World-Wide-Web (NCSA Mosaic), gopher, anonymous ftp and email servers.

Carp Systems International/Enterprise Planning Systems

1992

Full time Unix network administrator responsable for smooth operation of a dozen Unix hosts (RS/6000 running AIX, HP running HP-UX, SVR4, SCO and Windows on 386, X terminals, Macintosh, others) in an R&D environment of 30+ people. Numerous upgrades and enhancements performed including portions of a platform independant environment for source and binaries.

Fountain Technical Services

1989 to 1991

This job entailed many day to day elements of system administration and system configuration combined with evaluation of various hardware and software products prior to installation at customer sites. Configuration and change management tools were created and prototyped in a variety of languages and environments including: Foxbase, Prolog, Smalltalk.

Cadence Design Automation (formally SDA systems)

summer 1986, summer 1987, and summer 1992

Use of Sun 4 based VLSI design tools including Tangate's Cell-3C, Cadence Framework (Edge) versions 2 - 4.0. Experience writting high level user interfaces in the LISP/C-like language Skill, and writing of analytical geometry programs in C within a large CAD database environment.

Academic Experience

- Combined Honours program in Physics and Computer Science at Carleton University (1996)
- Honours project in physics: *Classical simulation of a flux tube model* dealt with a molecular dynamics simulation of a system of quarks.
- Computer skills are almost completely self taught.
- Courses include: elementary and introductory quantum mechanics, introductory particle physics, large project management, object oriented design (2 years), microprocessor interfacing, algorithms, computability, and numerical analysis.

Publications

- RFC3586 IP Security Policy (IPSP) Requirements.
- RFC4025 A Method for Storing IPsec Keying Material in DNS
- RFC4322 Opportunistic Encryption using the Internet Key Exchange (IKE)
- RFC5386 Better-Than-Nothing Security: An Unauthenticated Mode of IPsec
- RFC7416 A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)
- RFC8366 A Voucher Artifact for Bootstrapping Protocols
- RFC8415 Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [Nov. 2018]
- RFC8925 IPv6-Only-Preferred Option for DHCPv4
- RFC8951 Clarification of Enrollment over Secure Transport (EST): Transfer Encodings and ASN.1
- RFC8974 Extended Tokens and Stateless Clients in the Constrained Application Protocol (CoAP)
- RFC9008 Using RPI Option Type, Routing Header for Source Routes, and IPv6-in-IPv6 Encapsulation in the RPL Data Plane
- RFC9010 Routing for RPL (Routing Protocol for Low-Power and Lossy Networks) Leaves
- Internet of Things Business Show, episode 07, Network Protocols like Lego
- Architectural Considerations for IoT Device Security in the Home (ripe-759)
- RFC8995 Bootstrapping Secure Key Infrastructure (BRSKI)
- RFC9031 Constrained Join Protocol (CoJP) for 6TiSCH
- RFC9032 Encapsulation of 6TiSCH Join and Enrollment Information Elements
- RFC9148: EST over secure CoAP (EST-coaps)
- RFC9164: CBOR tags for IPv4 and IPv6 addresses and prefixes
- RFC9238: Loading Manufacturer Usage Description (MUD) URLs from QR Codes
- RFC9254: Encoding of Data Modeled with YANG in the Concise Binary Object Representation (CBOR)
- RFC9277: On Stable Storage for Items in Concise Binary Object Representation (CBOR)

Interpersonal Skills

- Extensive participation in IETF consensus process, from 1995 onwards. More than 50 meetings attended.
  - In 2012, working group co-chair for ROLL WG. (Documents published: RFC6719, RFC6997, RFC6998, RFC7731, RFC7732 RFC7733, RFC7774 RFC8036)
  - As ROLL WG secretary, rfc8138
  - As CELLAR WG co-chair, rfc8794: Extensible Binary Markup Language
  - IETF NOMCOM member: 2002/2003, 2012/2013, 2013/2014, NOMCOM Chair for 2014-2015, NOMCOM Past-Chair: 2015/2016
- Good communication skills, able to put complex ideas into simpler terms.
- Draws really good diagrams.
- Teaching assistent for first year physics courses (1991-1992), lab consultant for carleton Computing services (1992-1993), TA microprocessor interfacing (1994), BNR helpline (1994)
- Shodan (Black Belt) Shotukan Karate 2007, Nidan 2012. Some years spent teaching kids classes. Still active.
- Independent thinker - ability to initiate own projects.
- Many years experience as project leader, including delegation and critical scheduling.

Entrepreneurial Experience

- Founding director of Center for Research and Experimental Development in Informatic Libre (CREDIL)
- Founder of Xelerance Corporation
- Founder and owner of Sandelman Software Works
- Third person at Solidum Systems Corporation.
- Fourth person at Milkyway Networks.
- Founding member of SympCon -- technical conference registration and electronic paper distribution company
- Financially literate, including extensive budgeting experience at for-profit and non-profit organizations. Organizational finance structures.
- attended Junior Achievement of Ottawa Carleton - 1986-1988
- attended JA conference: EPJAC '88, CANJAC '88

Personal Interests

- past provincial council secretary, and chair of IT cmte for Green Party of Ontario.
- year-round cyclist, past-president and treasurer for Citizens for Safe Cycling
- debating, amateur student journalism, Charlatan Board of directors (Carleton 91-93).
- lives sustainably
- x-country skiing/running, sailing,triathlons
- flute, amateur drama, Karate (second degree black belt)
- community networking
