Seth Robertson

http://www.baka.org/resume • resume@baka.org • +1 732 548 5342

AREAS OF EXPERTISE

System/Network Design and Architecture

Computer Network Operations

Intellectual Property Development

Software Defined Networks SDN

Systems/Network Programming

Systems/Network Administration

Kernel Programming

Infrastructure Development

Scalable Programming

Security

Android Systems Development

Database Design

Remote Development

Appliance Development

Embedded Development

Systems Debugging

Virtual Machines DOCKER/LXC/EC2/KVM/QEMU

Source Code Management GIT

CURRENT LANGUAGES

C, Python, Perl, Unix shells, Lua, P/SQL

CURRENT OS

Linux, Android, OpenBSD, FreeBSD, IOS

SENIOR ARCHITECT FOR SECURITY, SYSTEMS, NETWORKS

Expert in both defensive and offensive Computer Network Operations, with particular emphasis on network-oriented operations. Won and led a large DARPA program on eXtreme DDoS Defense (XD3), won and led an AFRL program on cyber deception using SDN (CINDAM), worked on the DARPA Plan X program for automated cyber war planning and operations, and led technical tasks on the CERDEC programs on smartphone security (SMC) and intrusion detection frameworks and systems (CRUSHPROOF and DEFIANT). Previously, created and led development for a Network Intrusion Detection System company acquired by Raytheon Trusted Computer Solutions, created the first Internet web/LAN load balancer on the market, along with a DNS/WAN load balancer and an anycast load balancer.

EXPERIENCE

VENCORE LABS (A.K.A. APPLIED COMUNICATION SCIENCES) — Basking Ridge, NJ

Senior Scientist — May 2012 – Present

Proposed and am Principal Investigator (PI) for the DARPA Extreme DDoS Defense program (XD3) using deceptive network maneuvers implemented on distributed ephemeral cloud-based VMs to cheaply defend against and deceive both sophisticated high and low volume attacks against any network protocol. Designed and acquired a terabit per second network testbed to allow realistic testing of large scale network attacks; and designed and implemented test software that could work on laptops, the terabit cluster, and live internet cloud providers. Designed, integrated, and tested the DARPA Plan X attribution-hiding cloud provisioning system for Computer Network Operation listening posts, redirectors, and vantage nodes; design and development of test, wargaming, and operational range automated instantiation, initial system capability development and deployment; prototyped Cyber Domain Specific Language and reasoning system. Proposed and was PI for an AFRL program for deception network defense using individualized and adaptive network views. Technically designed, steered, implemented, and tested: (1) a system for prevention cyber attacks against US weapon systems; (2) a high-security Android cell phone (SMC) and Linux security systems (DEFIANT) and frameworks (CRUSHPROOF) for government projects, including development of anomaly detectors plus user and kernel IDS modules for both Android and Linux, synchronizing development on both platforms, plus creating build and deployment infrastructure. Mentor junior staff and create technical documentation and automation tools for team members.

RAYTHEON TRUSTED COMPUTER SOLUTIONS — Herndon, VA

Principal Secure Sys Eng — August 2008 – May 2012

Lead Technologist for and driving the technical design, implementation, core code design, security, and integrity of CounterStorm, a network intrusion and attack detection and response appliance, including SELinux, STIG, and IPv6 implementation. Performed tactical management of a distributed team of developers. Further responsible for RShield-ICAP integration, Nagios monitoring of RShield installations, RShield log analysis and mail load synthesis.

COUNTERSTORM — New York City

Chief Architect — August 2001 – August 2008

Lead Technologist for CounterStorm as described above. Responsible for patents, senior technical liaisons, technical management of DARPA Information Assurance and Army FCS projects, on-site deployment at governmental facilities, and Homeland Security contracts for bot-net and worm detection.

Product users include: New York Police Department, Warner Music Group, The Brookings Institute, McGraw-Hill, Columbia-Presbyterian Hospital, BAE Systems.

Seth Robertson

http://www.baka.org/resume • resume@baka.org • +1 732 548 5342

PROFESSIONAL LINKS

http://linkedin.com/in/sethrobertson

http://sethrobertson.github.com

PROTOCOLS

IP, IPv6, TCP, UDP, 1553, NTP, SSL, HTTP, FTP, SMTP, SMB, NNTP, RIP, OPSF, BGP, IPSP, ICAP, SIP/VoIP

LARGE PROJECTS

CounterStorm, NEMESIS, Crushproof, CINDAM, PlanX, HydraGPS, HydraWEB, RICAP, Proconsul, Brimstone, gitslave, HUDB, Xkernel, chkpt, nfsspy, netdig, pcrack

PROFESSIONAL ORGANIZATIONS AND AWARDS

ACM Member

Bronfman Scholar Columbia University

Dean's List Columbia University

HYDRAWEB TECHNOLOGIES — New York City

Chief Technical Officer — September 1994 – May 2001

Lead Technologist for HydraWEB. Responsible for all technical evaluations, plans, designs, and technical customer proposals. Senior inventor, designer, and developer of HydraGPS (WAN client/server reliability and optimization system), HydraWEB (LAN client/server reliability and optimization device), Brimstone (firewall), and Proconsul (serial console middle ware). Responsible for patents, senior technical liaisons, plus core code design, review, and integrity. Systems/network administrator and guidance for both the company LAN, the Internet connection, plus several large corporate clients with large Unix Internet-connected network installations dealing with Interactive TV and WWW hosting.

Product users include: Allen Bradley, Ascend, Associated Press, ATKK, AT&T, Bear Stearns, Citicorp, Corel, DLJ, Deutsche Post, Dow Jones, JC Penney, Juno, MCI, Monster, Reuters.

COLUMBIA UNIVERSITY — New York City

Systems Manager/Programmer — January 1988 (FT&PT) — FT: March 1992 – August 1994

Solely responsible for all CTR systems, maintenance, and network operations for a network of 300+ users, 90+ Unix machines, and 100+ PCs, Macs, and X-terminals. Including requirement analysis, purchase, installation, and maintenance of all technical equipment and software. Compiled, installed, and maintained all normal Internet services such as DNS, sendmail, USENET, WWW, anonymous FTP, and IRC. Extraordinary duties included the total redesign, purchase and implementation of the network due to a move to a different building.

PUBLICATIONS

S. Robertson, E. Siegel, M. Miller, and S. Stolfo. Surveillance detection in high bandwidth environments. In *DARPA Information Survivability Conference and Exposition (DISCEX)*, 2003.

S. Beitzel, T. Bowen, R. Chadha, J. Chiang, B. Falchuk, Y. Gottlieb, G. Levin, J. Micallef, C. Orji, R. Porter, A. Poylisher, S. Robertson, G. Walther, C. Paprcka, and J. Santos. Cydef: A unified and adaptive cyber defense framework. In *Classified US Military Communications (CUMC) Conference*, 2013.

S. Robertson, S. Alexander, J. Micallef, J. Pucci, J. Tanis, and A. Macera. Cindam: Customized information networks for deception and attack mitigation. In *Self-Adaptive and Self-Organizing Systems Workshops (SASOW), 2015 IEEE Ninth International Conference on*, 2015.

PATENTS

Raytheon Trusted Computer Solutions (CounterStorm): "Detecting Probes and Scans Over High-Bandwidth, Long-Term, Incomplete Network Traffic Information Using Limited Memory." US 7,752,665 granted July 6, 2010.

PATENT APPLICATIONS

HydraWEB Technologies: "Network Provisioning, Addressing Denial of Service Attacks, Reducing Network Bandwidth Arbitrage Fees, and Reducing Government Tariffs on Electronic Transactions."

HydraWEB Technologies: "Method and Apparatus for Reducing and Optimizing Network Traffic."

HydraWEB Technologies: "Method and apparatus of modifying performance of a load-balacing system using an extensible agent."

HydraWEB Technologies: "Wide Area Network Server Load Balancing Using a Network Provisioning System."

EDUCATION

Columbia University, School of Engineering and Applied Sciences. B.S. in Computer Science, 1992

CLEARANCE

TS/SCI