Last Updated on 6th February 2023

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

Network and System Simulation

Software Defined Networks SDN

Systems/Network Programming

Systems/Network Administration

Kernel Programming

Infrastructure Development

Scalable Programming

Security

Database Design

Classified Development

Remote Development

Appliance Development

Embedded Development

Android Systems Development

Systems Debugging

Virtual Machines DOCKER/LXC/EC2/KVM/QEMU

Source Code Management GIT

CURRENT LANGUAGES

C, Python, Perl, Unix shells

CURRENT OS

Linux

CHIEF SCIENTIST FOR SECURITY, SYSTEMS, AND NETWORKS

Creativity, analysis, and leadership across a diverse range of classified and open technological problem areas, such as high speed networking, cloud-based DDoS Defense, realtime U.S. Weapon System defense, dynamic & deceptive networks, Intrusion Detection, Firewalls, Cyberwarfare Planning & Operations, and the first web server load balancer on the market.

EXPERIENCE

PERATON LABS (AKA APPLIED COMMUNICATION SCIENCES, PERSPECTA LABS) — BASKING RIDGE, NJ

Chief Scientist — May 2012 – Present

Ideated, proposed, planned, conducted, and technically directed **$77.8M** over 27 research efforts. For the **defense of U.S. Weapons systems**: invented, architected, and am leading **1553 Bus Defender**, a TRL-7 real-time system to add critically-needed security to both legacy and modern platforms—with 18 programs under Army, Navy, and Air Force; currently being transitioned to multiple platforms. Bus Defender has been tested by five red teams and on the Abrams & Bradley platforms; UH-60V, P-8A, E-2C, F-15, F-16 SILs; and five other surrogate space, UAV, next-generation fixed-wing, and rotary-wing platforms. Additionally, I am leading the extension of Bus Defender to other critical weapon platform communication databuses. For **DARPA FastNICS**, am leading the creation of a 10 Tbps server & cluster with PCIe networking and a High Performance Computing simulator. For the **DARPA Extreme Distributed Denial of Service (DDoS) Defense program (XD3)** program, used deceptive network maneuvers implemented on distributed, ephemeral, cloud-based VMs to inexpensively 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 (now used by 25 contracts); and designed and implemented test software that could work on laptops, the terabit cluster, and live internet cloud providers. For **AFRL Cyber Deception**, created a patented dynamic & ephemeral network environment using Software Defined Networks to deceive and confuse cyber attackers while preserving a seemingly normal user experience.

Developed new business by analyzing and applying advanced methods, theories, and research techniques to create substantiated proposals to solve complex and advanced technical problems posed by customers. Proposal lead for the programs listed above, and helped with the **DARPA EdgeCT** and six classified programs. Won or helped win **$122.1M** in total new business over 33 efforts in last eight years.

Provided leadership, design, development, and testing expertise. For the **DARPA Plan X** program, created an attribution-hiding cloud provisioning system for Computer Network Operation listening posts, redirectors, and vantage nodes; designed and developed test, wargaming, and operational range automated instantiation, performed initial system capability development and deployment; prototyped Cyber Domain Specific Language and reasoning system. For other programs, created a high-security Android cell phone (**SMC**), framework (**CRUSHPROOF**), and Linux security systems (**DEFIANT**) for the **U.S. Army**; 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.

Additionally, authored eight patent applications, published research papers, developed classified lab security audit systems, mentored junior staff, and created technical documentation and automation tools for team members.

RAYTHEON TRUSTED COMPUTER SOLUTIONS — HERNDON, VA

Principal Secure System Engineer — 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.

PROFESSIONAL LINKS

http://linkedin.com/in/sethrobertson

http://sethrobertson.github.io

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

President's Award Perspecta Labs

Bronfman Scholar Columbia University

Dean's List Columbia University

ACM Member

COUNTERSTORM — NEW YORK CITY

Chief Architect — **August 2001 – August 2008**

Chief Architect for CounterStorm as described above until company acquired by Raytheon. 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.

HYDRAWEB TECHNOLOGIES — NEW YORK CITY

Chief Technical Officer — **September 1994 – May 2001**

Lead Technologist for HydraWEB & created first web load balancer on market. 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.

PUBLICATIONS

F. Douglis, S. Robertson, E. van den Berg, J. Micallef, M. Pucci, A. Aiken, K. Bergman, M. Hattink, and M. Seok. Fleet-fast lanes for expedited execution at 10 terabits: Program overview. In *IEEE Internet Computing*, 2021.

E. van den Berg and S. Robertson. Game-theoretic planning to counter ddos in nemesis. In *IEEE Military Communications Conference (MILCOM)*, 2019.

G. Frazier, B. Floyd, J. Mcgil, P. McNeely, R Zarookian, and S. Robertson. The nnbc anti-ddos firewall. In *IEEE Military Communications Conference (MILCOM)*, 2019.

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.

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

PATENTS

Perspecta Labs: "Low Delay Network Intrusion Prevention." US 10,673,816 granted June 2, 2020.

Perspecta Labs: "Customized information networks for deception and attack mitigation." US 10,440,054 granted October 8, 2019.

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

EDUCATION

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

CLEARANCE

TS/SCI