Samuel C Jero

Contact Information

Email: sjero@sjero.net Dedham, MA

Research Interests

Transport protocols, congestion control, Software Defined Networking (SDN), distributed systems, fault tolerance, network security, and automated testing

Education

Purdue University, West Lafayette, Indiana

PhD in Computer Science **August 2013 – present**

- GPA: 4.0
- Expected Graduation: May 2018
- Thesis: *Analysis and Automated Discovery of Attacks in Transport Protocols*
- Advisors: Dr. Cristina Nita-Rotaru and Dr. Sonia Fahmy

Ohio University, Athens, Ohio

Combined Masters and Bachelors in Computer Science **September 2008 – August 2013**

- GPA: 4.0
- Graduated: August 2013
- Thesis: *Performance Analysis of the Datagram Congestion Control Protocol DCCP for Real-Time Streaming Media Applications*
- Advisor: Dr. Shawn Ostermann

Honors and Awards

Purdue University 2017 Bisland Dissertation Fellowship Recipient

IETF/IRTF Applied Networking Research Prize 2016

Best Paper Award at IEEE Conference on Dependable Systems and Networks 2015

Student Travel Grant from IEEE Conference on Dependable Systems and Networks 2015

Student Travel Grant from IEEE Symposium on Security and Privacy 2015

Purdue University 2013 Andrews Fellowship Recipient

Ohio University Dean's List Fall 2008 to Spring 2013 (all terms)

Student Poster Presenter at the 2010 Internet2 Fall Member Meeting

2009 ACM Collegiate Programming Contest Honorable Mention

National Merit Scholar 2008

Publications

Benjamin E. Ujcich, Samuel Jero, Anne Edmundson, Richard Skowyra, James Landry, Adam Bates, William H. Sanders, Cristina Nita-Rotaru, and Hamed Okhravi. "**Securing Software-Defined Networks with App Provenance**", Under Submission, 2017.
Joint First Author

Samuel Jero, Endadul Hoque, David Choffnes, Alan Mislove, and Cristina Nita-Rotaru. "**Automated Attack Discovery in TCP Congestion Control Using a Model-guided Approach**", Network and Distributed Systems Security Symposium (NDSS), 2018. [To Appear]

Arash Molavi Kakhki, Samuel Jero, David Choffnes, Alan Mislove, and Cristina Nita-Rotaru. "**Taking a Long Look at QUIC: An Approach for Rigorous Evaluation of Rapidly Evolving Transport Protocols**", ACM Internet Measurement Conference (IMC), 2017. [*Acceptance Rate: 23%*] [To Appear]

Samuel Jero, Xiangyu Bu, Cristina Nita-Rotaru, Hamed Okhravi, Richard Skowyra, and Sonia Fahmy. "**BEADS: A Framework for Attack Discovery in OpenFlow-based SDN Systems**", 20th International Symposium on Research in Attacks, Intrusions, and Defenses (RAID), 2017. [*Acceptance Rate: 20%*]

Samuel Jero, William Koch, Richard Skowyra, Hamed Okhravi, Cristina Nita-Rotaru, and David Bigelow. "**Identifier Binding Attacks and Defenses in Software-Defined Networks**", 26th USENIX Security Symposium, 2017. [*Acceptance Rate: 16%*]

Samuel Jero, Vijay K. Gurbani, Ray Miller, Bruce Cilli, Charles Payette, and Sameer Sharma. "**Dynamic control of real-time communications (RTC) using SDN: A case study of a 5G end-to-end service**", 2016 IEEE/IFIP Network Operations and Management Symposium (NOMS), April 2016.

Samuel Jero, Hyojeong Lee, and Cristina Nita-Rotaru. "**Leveraging State Information for Automated Attack Discovery in Transport Protocol Implementations**", 45th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), June 2015.
[*Acceptance Rate: 22%*] [*Best Paper*]

Robert Lychev, Samuel Jero, Alexandra Boldyreva, and Cristina Nita-Rotaru. "**How Secure and Quick is QUIC? Provable Security and Performance Analyses**", 36th IEEE Symposium on Security and Privacy (Oakland), May 2015. [*Acceptance Rate: 14%*]
Awarded the 2016 IETF/IRTF Applied Networking Research Prize

Hans Kruse, Samuel Jero, and Shawn Ostermann. "**Datagram Convergence Layers for the Delay- and Disruption-Tolerant Networking (DTN) Bundle Protocol and Licklider Transmission Protocol (LTP)**", *RFC 7122 (Experimental)*, 2014.

Professional Experience

Network And Distributed Systems Security Lab **August 2013 – present**
Purdue University, West Lafayette, Indiana

- *Software Defined Networking Attack Discovery:* Developed techniques and a prototype implementation for practical automatic attack discovery in real, unmodified SDN systems where switches or hosts may be malicious.
- *Software Defined Networking Fault Tolerance:* Examined protocols and techniques used for state distribution and fault tolerance in distributed SDN controllers for the purpose of improving fault tolerance and security. Preliminary work involved adding byzantine fault tolerance to a centralized SDN controller to provide high availability and security for switch to controller communication and analyzing the performance impact.
- *Automatic Vulnerability Detection:* Leveraged the protocol state machine for search space reduction to enable practical automatic vulnerability detection in unmodified network transport protocol implementations using virtualization and network emulation.
- *Congestion Control Attacks:* Developed a model-based technique to systematically generate attacks against TCP congestion control and a state inference algorithm to track the congestion control state of a TCP sender enabling the development of an automated system for identifying attacks against the congestion control of real TCP implementations.
- *QUIC Protocol Attacks:* Identified and implemented five new attacks on the QUIC protocol, which was developed by Google for encrypted connections with 0-RTT connection setup.
- *NLP for Protocol Specifications:* Developed Natural Language Processing techniques to extract network protocol packet formats from natural language specifications. Combined with our automatic vulnerability detection system to enable fully-automatic vulnerability discovery.
- *Undergraduate Advising:* Advised undergraduate student Xiangyu Bu, who developed an OpenFlow malicious proxy capable of intercepting, modifying, and manipulating OpenFlow messages between switches and controllers.

MIT Lincoln Laboratory, Lexington, Massachusetts **May 2017 – August 2017**

- *SDN Controller Provenance:* Developed an SDN system that collects provenance information about app interactions with the controller and can enforce policy over the resulting provenance graph in realtime. Then created a policy to isolate apps from each other that prevents cross app poisoning attacks.
- *SDN Defense Evaluation:* Designed, implemented, and carried out the performance and security evaluation for an SDN-based network defense.

MIT Lincoln Laboratory, Lexington, Massachusetts **May 2016 – August 2016**

- *SDN Attack Discovery:* Completed development of a system for automatic attack discovery in unmodified SDN systems and demonstrated how the small attacks found could compose into powerful attacks that impact core network guarantees.

- *Network Identitifier Attack Prevention:* Developed a system to systematically and completely prevent network identifier spoofing and hijacking attacks (ARP spoofing, DNS spoofing, etc) at multiple levels of the network stack by leveraging SDN's separate control plane and global view of the network in combination with a root of trust provided by IEEE 802.1x.

Alcatel-Lucent Bell Labs, Murray Hill, New Jersey **June 2015 – August 2015**

- *SDN and Real-Time Video for Cellular:* Developed an prototype SDN-based system to dynamically enable or disable network and base station quality of service controls for video calls in a cellular network based on network conditions, thereby optimizing the usage of limited network resources
- *5G, SDN, and NFV:* Identified a number of important considerations for SDN controllers and NFV-graphs for dynamic network services in 5G systems based on a demo involving an example end-to-end dynamic network service
- *5G End-To-End Architecture:* Contributed to discussions on the design of the next-generation 5G end-to-end network architecture, particularly about how to coordinate multiple SDN controllers across the network

Cray, Inc, Saint Paul, Minnesota **May 2014 – August 2014**

- *Filesystem Burst Buffer:* Worked with a team designing an SSD burst buffer system for Cray supercomputers to increase the speed of checkpointing scientific applications across clusters of tens of thousands of machines attached to petabyte-sized filesystems
- *SSD Health Monitoring:* Design and implementation of a system to monitor the health of many SSDs distributed throughout a cluster and protect them from premature wearout due to improperly written checkpointing code in applications distributed across very large clusters with as little overhead as possible

Ohio University Internetworking Research Group, Athens, Ohio **June 2010 – July 2013**

- *Deep Space Networking:* Testing and performance analysis of network protocol implementations designed for deep space environments with high delay and high error-rates, and embedded, real-time operating systems
- *DCCP Performance:* Performance analysis of DCCP, an unreliable congestion controlled protocol designed for VoIP and IPTV, in network testbeds, on the internet, and in long delay environments for real time video streaming applications
- 12 patches accepted into the Linux kernel fixing bugs in the DCCP implementation

US Department of Defense **June 2012 – August 2012**

- Contact me for details

US Department of Defense **June 2011 – September 2011**

- Contact me for details

Relevant Skills

Programming Languages: C/C++, Java, Python, Perl, PHP, SQL

Version Control: Git, Mercurial, Subversion

Networking and OS: Wireshark, Tcptrace, IP/IPv6/TCP development, NS-3, UNIX/Linux, qemu, KVM, Linux kernel development, Cray supercomputer development

SDN: NOX, POX, ONOS, Open vSwitch, Mininet

Other: OpenCV, Android development

Relevant Courses

Data Structures, Algorithms (4 courses), Networking (5 courses), Operating Systems (4 courses), Parallel Computing (2 courses), Security (3 courses), Distributed Systems, Linux Kernel Programming, Advanced Microprocessors, Compilers, Databases, Data Mining

Activities	Coordinated a reading group on Software Defined Networking involving students from programming languages, networking, distributed systems, and security in Fall Semester 2014
	External reviewer for CoNEXT 2017
	Graduate Intervarsity Christian Fellowship
	Campus Crusade for Christ
	Live audio production
	Reading works on fantasy, historical fiction, or theology
Professional Affiliations	ACM (Association for Computing Machinery)
	IEEE Computer Society
References	*Available on request*