Dr. Samuel C Jero

Contact Information

Email: sjero@sjero.net Waltham, MA

Research Interests

Software Defined Networking (SDN), transport protocols, congestion control, embedded systems, network security, and automated testing

Education

Purdue University, West Lafayette, Indiana

PhD in Computer Science **August 2013 – May 2018**

- GPA: 4.0
- Graduated: 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

CERIAS Diamond Award 2018

Cisco Network Security Distinguished Paper Award at NDSS 2018

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)

National Merit Scholar 2008

Publications

Samuel Mergendahl, Samuel Jero, Bryan C. Ward, Juliana Furgala, Gabriel Parmer, Richard Skowyra. "**The Thundering Herd: Amplifying Kernel Interference to Attack Response Times**", Under Submission 2021.

Samuel Jero, Nathan Burow, Bryan Ward, Richard Skowyra, Alexandra Clifford, Roger Khazan, Howard Shrobe, and Hamed Okhravi. "**TAG: Tagged Architecture Guide**", Under Submission, 2020.

Samuel Jero, Juliana Furgala, Phani Kishore Gadepalli, Runyu Pan, Alexandra Clifford, Bite Ye, Roger Khazan, Bryan C. Ward, Gabriel Parmer, and Richard Skowyra. "**Practical Principle of Least Privilege for Secure Embedded Systems**", 27th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), 2021.

Benjamin E. Ujcich, Samuel Jero, Richard Skowyra, Adam Bates, William H. Sanders, and Hamed Okhravi. "**Causal Analysis for Software-Defined Networking Attacks**", USENIX Security Symposium, 2021.

Leila Rashidi, Daniel Kostecki, Alexander James, Anthony Perterson, Samuel Jero, Majid Ghaderi, Cristina Nita-Rotaru, Reihaneh Savafi-Naini, and Hamed Okhravi. "**More than a Fair Share: Network Data Remanence Attacks against Secret Sharing-based Schemes**", Network and Distributed Systems Security Symposium (NDSS), 2021. [*Acceptance Rate: 15%*]

Anthony Peterson, Samuel Jero, Endadul Hoque, Cristina Nita-Rotaru, and David Choffnes. "**aBBRate: Automating BBR Attack Exploration Using a Model-Based Approach**", The 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2020.

Benjamin E. Ujcich, Samuel Jero, Richard Skowyra, Steven R. Gomez, Adam Bates, William H. Sanders, and Hamed Okhravi. "**Automated Discovery of Cross-Plane Event-Based Vulnerabilities in Software-Defined Networking**", Network and Distributed Systems Security Symposium (NDSS), 2020. [*Acceptance Rate: 17%*]

Hamed Okhravi, Nathan Burow, Richard Skowyra, Bryan Ward, Samuel Jero, Roger Kazan, and Howard Schrobe. "**One Giant Leap for Computer Security**", IEEE Security and Privacy Magazine, 2019.

Shan Chen, Samuel Jero, Matthew Jagielski, Alexandra Boldyreva, and Cristina Nita-Rotaru. "**Secure Communication Channel Establishment: TLS 1.3 (over TCP Fast Open) vs. QUIC**", The European Symposium on Research In Computer Security (ESORICS), 2019. [*Acceptance Rate: 20%*]

Steven R. Gomez, Samuel Jero, Richard Skowyra, Jason Martin, Patrick Sullivan, David Bigelow, Zackary Ellenbogen, Bryan C. Ward, Hamed Okhravi, and James W. Landry. "**Controller-Oblivious Dynamic Access Control in Software-Defined Networks**", 49th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2019. [*Acceptance Rate: 21%*]

Bryan C. Ward, Richard Skowyra, Samuel Jero, Nathan Burow, Hamed Okhravi, Howard Shrobe, Roger Khazan. "**Security Considerations for Next-Generation Operating Systems**", 1st International Workshop on Next-Generation Operating Systems for Cyber-Physical Systems (NGOSCPS), 2019.

Samuel Jero, Maria L. Pacheco, Dan Goldwasser, and Cristina Nita-Rotaru. "**Leveraging Textual Specifications for Grammar-based Fuzzing of Network Protocols**", Conference on Innovative Applications of Artificial Intelligence (IAAI), 2019.

Benjamin E. Ujcich, Samuel Jero, Anne Edmundson, Qi Wang, Richard Skowyra, James Landry, Adam Bates, William H. Sanders, Cristina Nita-Rotaru, and Hamed Okhravi. "**Cross-App Poisoning in Software-Defined Networking**", ACM Conference on Computer and Communication Security (CCS), 2018. [*Acceptance Rate: 16%*]

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. [*Acceptance Rate: 21%*]
Cisco Network Security Distinguished Paper

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%*]
Awarded the 2018 IETF/IRTF Applied Networking Research Prize

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 Award*

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

MIT Lincoln Laboratory, Lexington, Massachusetts **May 2018 – Current**
Technical Staff

- *SeL4-based OS in Rust:* As Technical Lead designed, architected, and lead a team to implement an operating system built around the seL4 formally verified microkernel, including elf loading, memory management, threading, shared memory, a variety of coordination mechanisms, timers, a networking stack, a POSIX-like API, and a minimal libc.
- *Isolation for Crypto:* Designed and implemented a system to perform high assurance crypto, including strong isolation, with information flow restriction, from the rest of the system and approaches to ensure correct operation of the crypto itself.
- *Network Analysis for Power Systems:* Developed tools to analyze the networks used in electrical power systems looking for unexpected connectivity or configuration issues. Wrote configuration parsers for Cisco, Juniper, and other networking gear and implemented network analysis tooling very similar to Header Space Analysis, but extended to more complex networks.
- *Tagged Architecture Operating System:* Designed and led a team of graduate students to implement an operating system that leverages tagged architectures to provide fine-grained isolation and truely disjoint privilege, enabling componentization without the overhead of traditional microkernels.
- *Secret Sharing Network Protocols:* Explored the practical implementation of secret sharing protocols for network security and discovered a novel attack, network data remanence, allowing more opportunities for recovering data than previous work indicated.
- *Dynamic Network Reachability:* Implemented and carried out performance and security evaluation for an SDN-based system to dynamically limit network reachability by end systems to only required resources preventing the spread of malware across the network.
- *Multi-SDN Coordination:* Developed techniques for coordinating multiple independent but connected SDN systems in a scalable and efficient manner that only shares required information while allowing the SDNs to act mostly independently. Developed a prototype that establishes and periodically rotates completely disjoint paths through the set of connected SDNs.
- Implemented and submitted a patch providing secure LLDP-based topology discovery for the ONOS SDN controller. Patch was accepted and merged into the official code-base.

Network And Distributed Systems Security Lab **August 2013 – May 2018**
Purdue University, West Lafayette, Indiana
Research Assistant

- *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 grammars 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**
Intern

- *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**
Intern

- *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**
Intern

- *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**
Intern

- *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**
Research Assistant

- *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

Relevant Skills

Programming Languages: C/C++, Rust, Java, Python

Version Control: Git, Subversion

Networking and OS: Wireshark, Tcptrace, IP/IPv6/TCP development, NS-3, UNIX/Linux, qemu, KVM, Linux kernel development, SeL4

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

Activities

Reviewer for NDSS 2021 and NDSS 2022

Reviewer for ACM SDN-NFV 2019

External reviewer for NDSS 2020, CoNEXT 2017

References

Available on request