Samuel C. Hollifield

Oak Ridge National Laboratory

Cyber Security Hardware Engineer
Cyber Security Research Group
Cyber & Applied Data Analytics Division
National Security Sciences Directorate
https://www.0xSam.com
hollifieldsc@ornl.gov

1 Bethel Valley Road
P.O. Box 2008
Mailstop 6418
Oak Ridge, TN 37831
Cell: 865-945-0009

Research Interests

My undergraduate studies are largely in embedded computing systems and computer engineering for security. I contribute to research projects which include transportation security, cyber operations support, signal visualisation, data analytics, and grid security. My on-going efforts focus largely on cyber security implementations for passenger vehicles and heavy-duty trucks, centered mostly around intrusion detection systems for intra-vehicle network communications. I have a passion for communicating the science behind my research through publications, workshops, and presentations.

Education

- B.S. Computer Engineering, Tennessee Technological University, GPA 3.26/4.00 — May 2022

Citizenship

United States Citizen

Professional Experience (Selected Projects)

- **From Can't to CAN:** (Cyber Security Research Engineer, DOE ORNL LDRD, FYs 2019, 2020) Controller Area Networks (CANs) used in vehicles, planes, operating rooms, and industrial facilities provides a lightweight protocol for subsystem communication, but are bereft of security measures; these vulnerabilities leave vehicles and other infrastructure insecure, that is, exposed to cyber attacks with potentially disastrous/fatal consequences. This project seeks intrusion detection of advanced attacks. Individual contributions to this research include:
  - Transferring algorithms and machine learning models to embedded edge devices for in-situ detection of advanced attacks
  - Pioneering hardware solutions which can safely interact with an automotive network
  - Visualizing signals embedded within proprietary, obfuscated data
  - Delivering conference and workshop presentations centered around CAN-based analytics and security solutions
- **ORNL-CORR:** (Cyber Security Research Engineer, DOE ORNL, FY 2020) ORNL's Cyber Operations Research Range (CORR) is a 1300 node, 11TB RAM, 1PB HDD cyber research testbed for evaluating cybersecurity research technologies. CORR provides the computational platform for implementing novel, large-scale experiments with real malicious computer programs and attacks to research and develop cutting-edge security systems. Individual contributions to this project include:
  - Initial configuration & ongoing support for CORR infrastructure and users
  - Tools evaluation including state-of-the-art attack generation and defensive capabilities
  - Creating routes of access and ensuring overall security of CORR as it pertains to the ORNL internal network

- **CyberForce Challenge:** (Industrial Control Systems (ICS) Team Leader, DOE, FYs 2018-2020) By utilizing critical infrastructure focused scenarios, the Department of Energy (DOE) introduces students to the concept of national grid cybersecurity. The energy-focused contest occurs annually, with a cyber-physical construction which must be defended against a plethora of attackers and vulnerabilities. Individual contributions to this research include:
  - Collaborate with representatives from Argonne National Laboratory to prototype and test the individual ICS constructions for each competition
  - Lead a small team (2-5) of researchers which build, program, and manage the ICS constructions prior-to and during the competition.
  - Troubleshoot technology including the embedded microcontrollers used for the competition and how they communicate with cloud (particularly Microsoft Azure) and web-services
- **ORCA-AVD:** (CyberSecurity Research Engineer, DOE ORNL, FYs 2018-2019) The Oak Ridge Cyber Analytics (ORCA) Attack Variant Detector (AVD) is a sensor that uses machine learning technology to analyze behaviors in channels of communication between individual computers. Part of this effort requires the ability to generate, locate, and incorporate malicious data for preliminary data processing stages. Individual contributions to this project include:
  - Creating tools which map known malicious data to their individual packets given a network trace file
  - Researching and uncovering recent threats and the data which they communicate via computer networks
  - Process and prepare malware & attack samples for ingestion into the ORCA-AVD appliance to detect anomalous network traffic

Publications

- M. E. Verma, M. D. Iannacone, R. A. Bridges, S. C. Hollifield, B. Kay, and F. L. Combs, "The ORNL Automotive CAN Real Intrusion Dataset," *In preparation for submission to IEEE Access*, 2020
- M. E. Verma, R. A. Bridges, J. J. Sosnowski, S. C. Hollifield, and M. D. Iannacone, "CAN-D: A Modular Four-Step Pipeline for Comprehensively Decoding Controller Area Network Data," *Submitted to IEEE VTC, preprint available arXiv:2006.05993 [cs, eess]*, Jun 2020. arXiv: 2006.05993
- M. Verma, R. A. Bridges, and S. Hollifield, "ACTT: Automotive CAN Tokenization & Translation," in *IEEE Proceedings of 5th Annual CSCI, Symposium on Computational Intelligence*, IEEE, Dec 2018

Intellectual Property Protection

- M. Verma, R.A. Bridges, M. Iannacone, S.C. Hollifield, J. Sosnowski, June 29, 2020. DOE-S Number: S-162,054, "Universally Applicable Signal-Based Controller Area Network (CAN) Intrusion Detection System" - provisional patent filed
- R.A. Bridges, J.M. Carter, M.E. Verma, S.C. Hollifield, October 08, 2019. DOE-S Number: S-161,919, "Continuous Authentication of Drivers Using Inimitable Characteristics of CAN Data"
- S.C. Hollifield, M. Iannacone, November 2, 2018, DOE-S Number: S-138,942, "Comprehensive Integrated Controller Area Network Test Environment"

Awards

- National Motor Freight Traffic Association HVCS Scholarship ($10K) — July 2020
- 3rd Annual CyberTruck Challenge Most Unique Intrusion Award — July 2019
- Tennessee Tech Research & Creative Inquiry Day ECE Winner — April 2019

- ORAU SULI/CCI Best Abstract Award — November 2018
- ORAU CCI Featured Student Profile — August 2018
- ORAU SULI/CCI IGNITE-Off National Finalist — July 2018
- ORAU SULI/CCI IGNITE-Off Winner — March 2018
- East TN Foundation, James K. Goldston INFOSEC Scholarship ($2K) — February 2018
- Roane State Community College CITC Student Spotlight — November 2017
- Roane State Community College Math Dept. Oustanding Tech Student of the Year — September 2017

Professional Organization Memberships

- SAE

References

- Dr. Robert A. Bridges, Cyber Security Researcher, ORNL, National Security Sciences Directorate, `bridgesra@ornl.gov`
- Dr. Stacy Prowell, Senior Cyber Security Research Scientist, ORNL, National Security Sciences Directorate, `prowellsj@ornl.gov`
- Dr. Jeff Nichols, Cyber Security Research Group Leader, ORNL, National Security Sciences Directorate, `nicholsja2@ornl.gov`

Previous Employment

- Tennessee Technological University — Undergraduate Research Associate, 03/2019-09/2020
- Oak Ridge Associated Universities — Undergraduate Research Intern, 01/2018-12/2019

Conference Presentations, Posters, Attendance

- Presentation "Analysis and Defense of Automotive Networks" at BSides Knoxville, April 2020
- Poster presentation "Securing Automotive Networks with Vehicle-Agnostic Technologies" at 4th Tennessee Technological University, Research and Creative Inquiry Day, April 2020
- Workshop "Analysis and Defense of Automotive Networks" at CodeMash, January 2020
- Attendance, 3rd NMFTA CyberTruck Challenge, July 2019
- Poster presentation, "Cybersecurity Implications of Modern Automobiles" at 3rd Tennessee Technological University, Research and Creative Inquiry Day, April 2019 (Best poster award)
- Presentation "Talking Cars: From Can't to CAN"at BSides Knoxville, April 2019
- Workshop "Talking Cars: From Can't to CAN" at CodeMash, January 2019
- Attendance, 2nd NMFTA CyberTruck Challenge, July 2018