OAK RIDGE National Laboratory

Transportation Cybersecurity

Samuel C. Hollifield (hollifieldsc@ornl.gov)

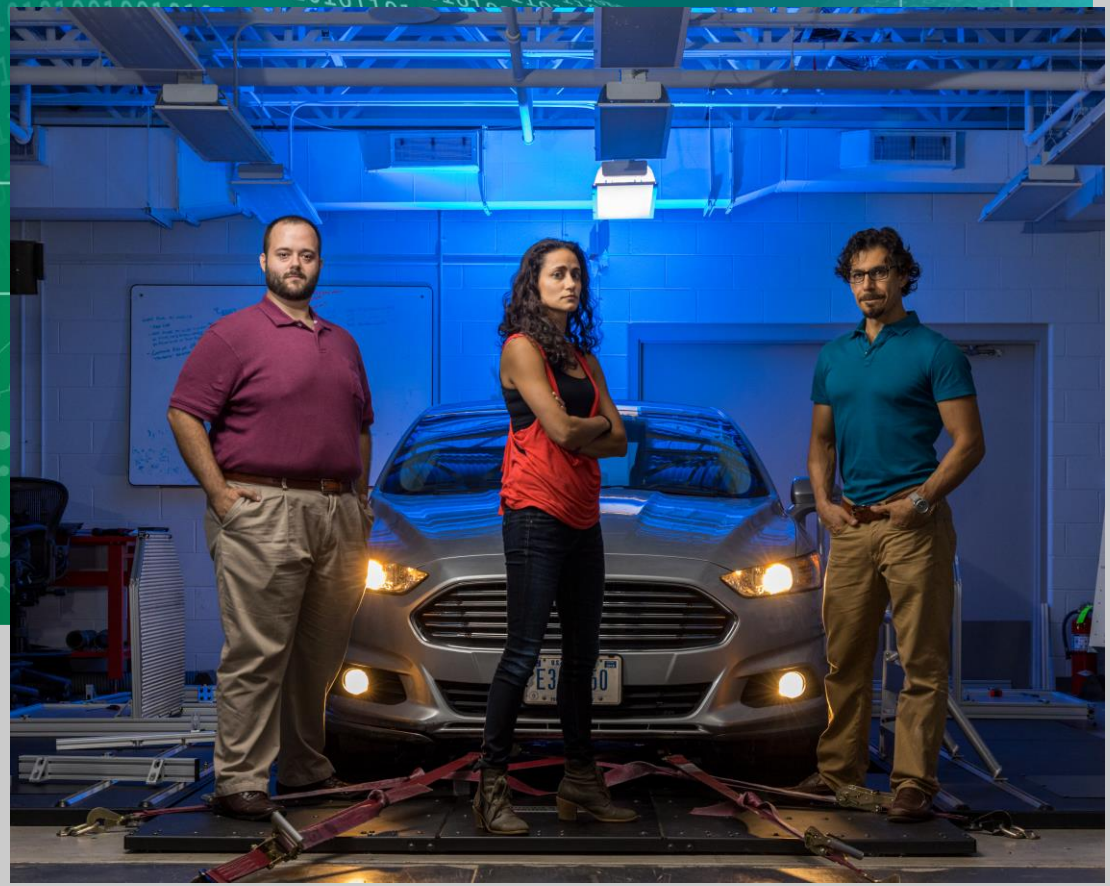
Kevin Spakes (spakesd@ornl.gov)

U.S. DEPARTMENT OF ENERGY

TSUSG Annual Meeting 2023

Transportation Cybersecurity Research Team

- Sam Hollifield
- Joel Asiamah
- Luke Lambert
- Isaac Sikkema
- Kevin Spakes
- Nell Barber
- Adian Cook
- Lilian Swann
- Mingyan Li, PhD
- Isaac Sikkema
- Lilian Swann
- Mahim Mathur
- Max Hankins



National Nuclear Security Administration

Cyber Attacks on Vehicles

Jeep Hack (2015)

Hackers Miller & Valasek remotely kill Chrysler vehicle on highway.

www.cnbc.com/video/2015/07/22/hackers-hijack-moving-jeep-shocking-video.html

Keyfob Replay Attacks (2022)

Although more known—keyfob attacks continue to thwart implemented security (2022)

https://www.blackhat.com/us-22/briefings/schedule/#rollback---a-new-time-agnostic-replay-attack-against-the-automotive-remote-keyless-entry-systems-27185

Gone in 60 Seconds (2022)

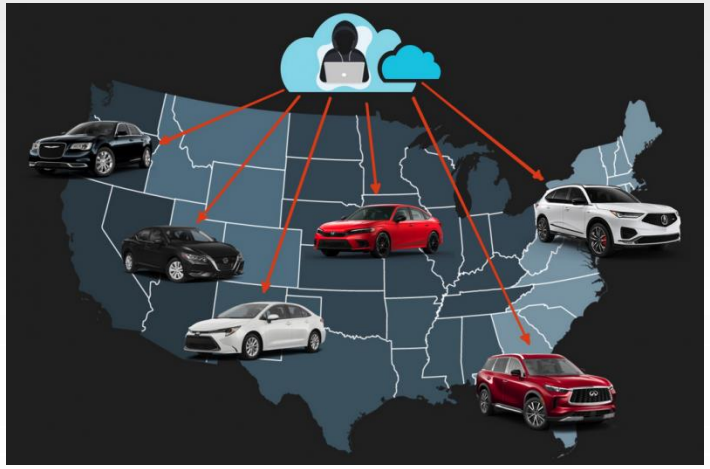
New thieving tool uses headlight plugs to reprogram car keys. Thefts are fast and easy (120s)

https://kentindell.github.io/2023/04/03/can-injection/

Cyber Attacks on Vehicles

Sirius-XM API Leak (2022)

Sirius-XM leak allows hackers to remotely unlock and start vehicles



https://www.securityweek.com/several-car-brands-exposed-hacking-flaw-sirius-xm-connected-vehicle-service/

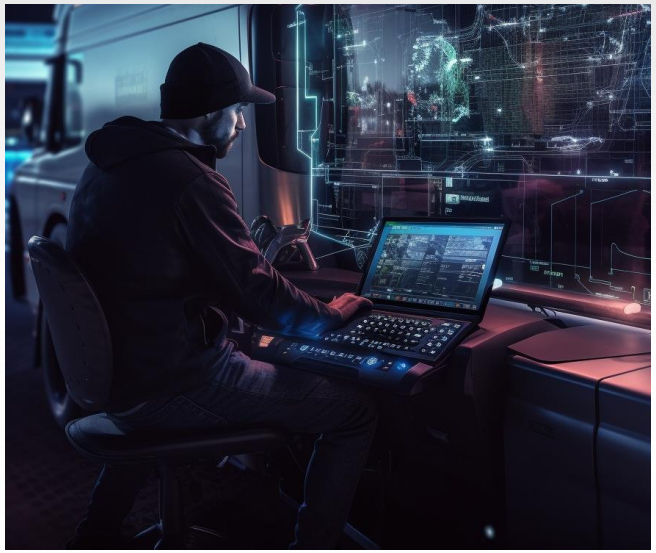
Toyota Location Leak (2023)

Vulnerability in Toyota Cloud Services allows hackers to eavesdrop on vehicle location.

https://www.bleepingcomputer.com/news/security/toyota-car-location-data-of-2-million-customers-exposed-for-ten-years/

Continued API Leaks (2023)

Sam Curry continues research into leaked APIs. Finds vulnerabilities in **16!!!** OEMs



https://samcurry.net/web-hackers-vs-the-auto-industry/

A Simple Attack

Example of what you can do with

- $75 hardware
- Nearly no knowledge
- A modern vehicle

We simply send randomized messages at a high rate

Denial of Service Random Injection Attack Video
Video credit: Frank Combs at ORNL

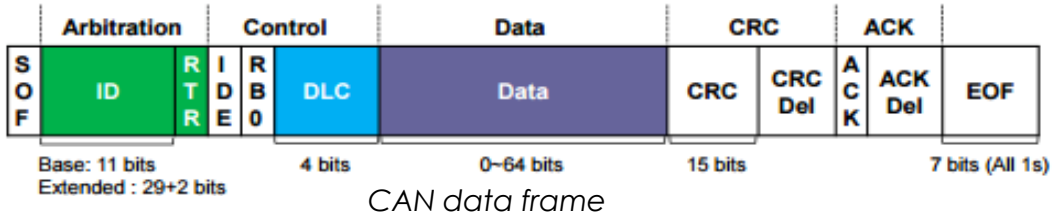
CAN basics

Shared serial communication bus designed to be robust and inexpensive

Implemented as a two-wire differential signal (CAN High and CAN Low)

CAN is a message-based protocol

Messages contain an ID field, a data field, and a few others



CAN data frame
Photo credit: Cho & Shin, *CCS 2016*

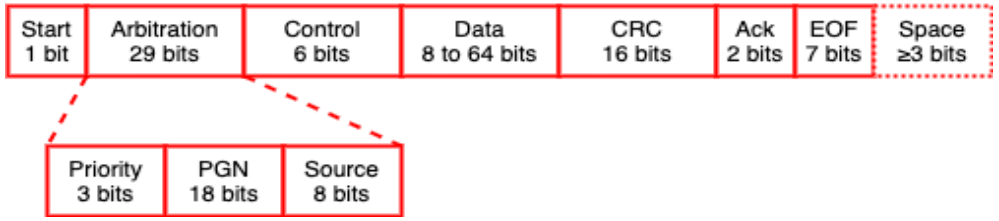


Diagram of CAN frames
Image credit: Mike Iannacone at ORNL

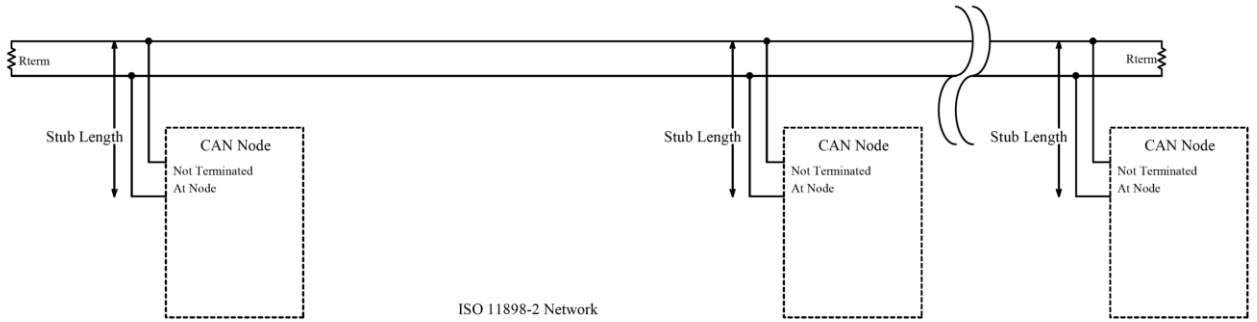


Diagram of CAN network topology
Image credit: EE JRW at Wikimedia Commons

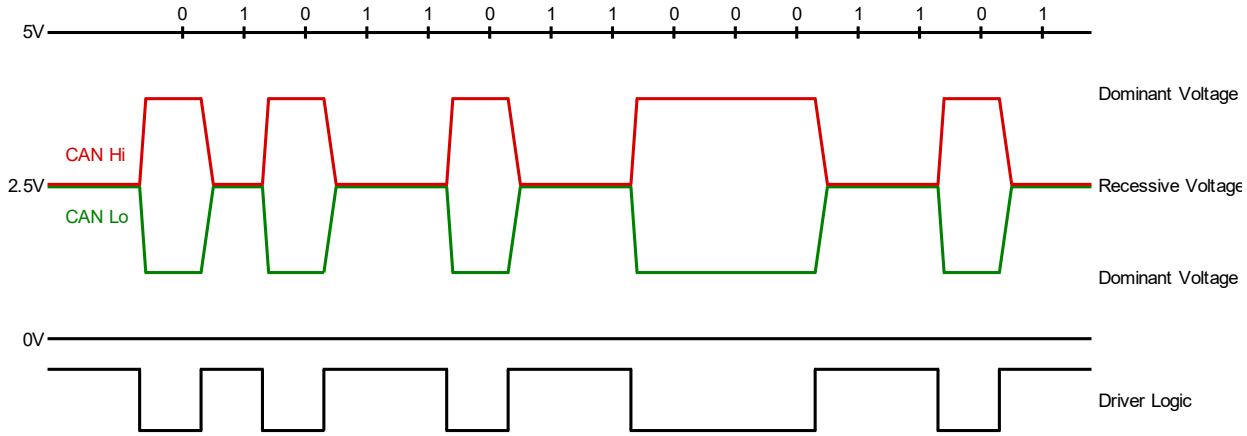


Diagram of CAN network signaling
Image credit: EE JRW at Wikimedia Commons

OAK RIDGE National Laboratory

Defending against Cyber Attacks

Problem: Cybersecurity Resilience Varies Wildly by Manufacturer

Best Practice	OEM A	OEM B	OEM C	OEM D
CAN Gateway	✓		✓	
CAN Message Authentication			✓	
Segmented Networks	✓	✓	✓	
Transparent Vulnerability Handing	✓			
Frequent Security Patching			✓	
Whole-Vehicle Security Assessments				

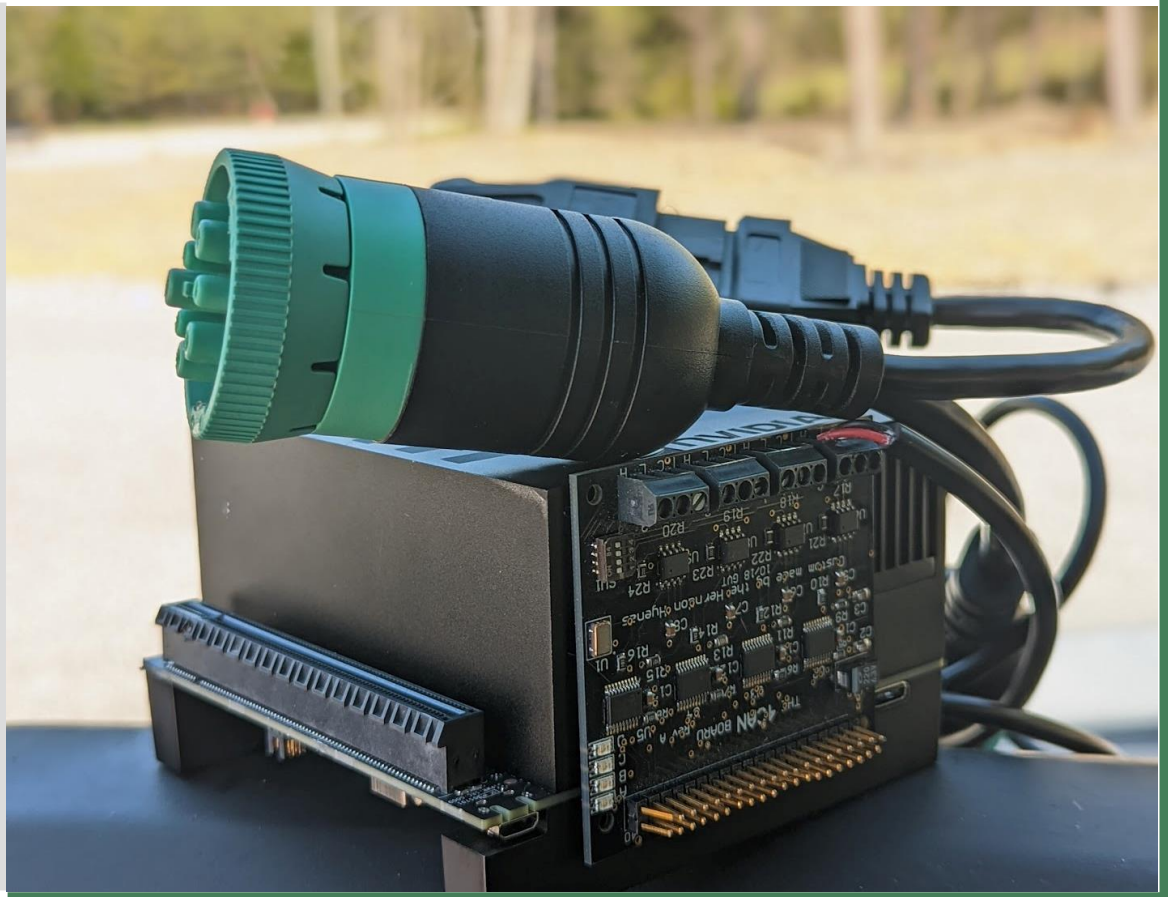
Intrusion Detection & Prevention

- Fabrication Attacks: Simple injected malicious messages
- Suspension Attacks: Preventing ECUs from speaking (e.g., targeted bus-off)
- Masquerade Attack: Very sophisticated. Suspends transmission of real messages, replaces expected data with malicious payload

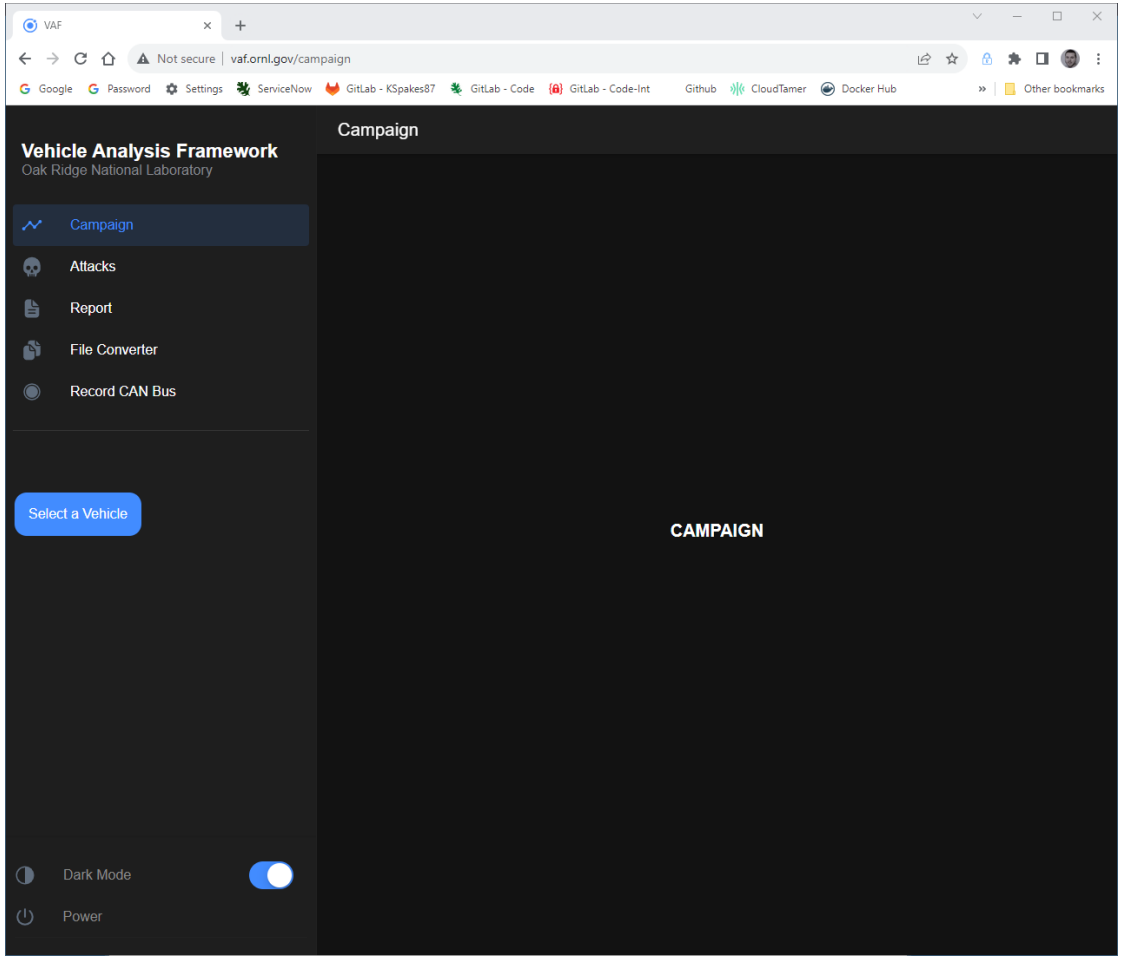
OAK RIDGE National Laboratory

SHIELD: Secure Hijack, Intrusion, and Exploit Layered Detector

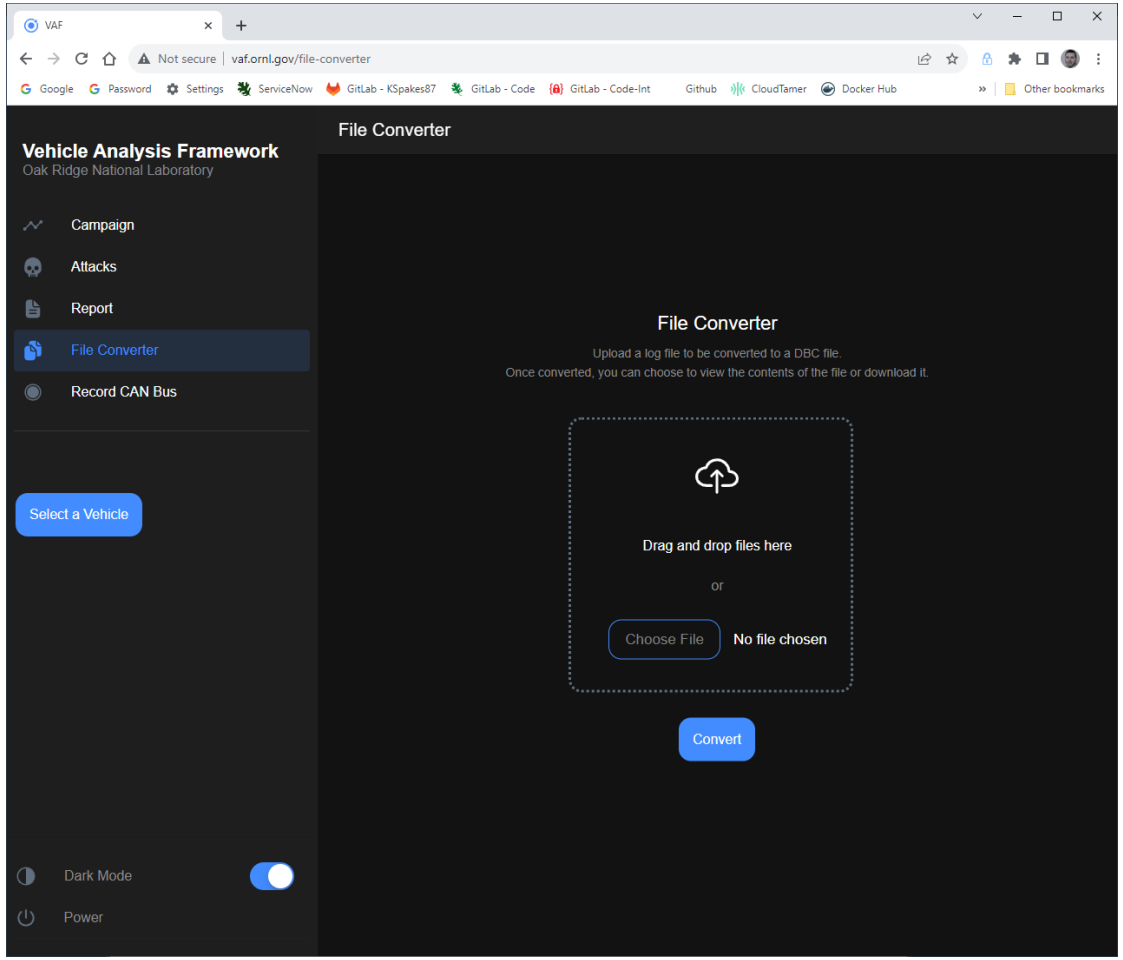
- Ensemble intrusion detection system for in-vehicle Controller Area Networks



ORNL Entire Vehicle Analysis of Cybersecurity (EVAC) Framework



Goal: Automate the analysis of a vehicle's cyber resilience



OAK RIDGE National Laboratory

Bridges, CAN-D

Acknowledgements

CANalytics Team: Robert Bridges, Miki Verma, Sam Hollifield, Mike Iannacone, Stacy Prowell, Bill Kay, Jordan Sosnowski, Deborah Wilkerson, Zach Tyree, Krystof Palewec, Frank Combs, Michael Moore, Michael Starr, Joel Asiamah, Katherine Caudill, Max Boozer, Isaac Sikkema, Mike Huettel, Luke Lambert, Lilian Swann, Mahim Mathur, Nell Barber

Programmatic Help: Mason Rice, Shaun Gleason, Ken Martin, Shannon Morgan, Matt Garrett, Jeff Nichols, Andreana Leskovjan, Liz Neunsinger,

Questions?

Sam Hollifield, hollifieldsc@ornl.gov, https://0xSam.com