INL/CON-22-67638-Revision-0

Presentation slides for OmniTap at TechConnect Expo

June 2022

Keith D Mecham

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-22-67638-Revision-0

Presentation slides for OmniTap at TechConnect Expo

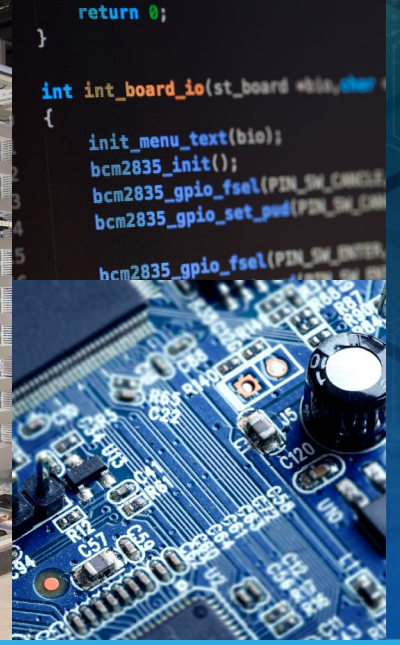
Keith D Mecham

June 2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517



June 14, 2022

Keith Mecham
Critical Infrastructure Cybersecurity Engineer

OmniTap

Universal Capture and Translation of ICS Communication

LRS: INL/CON-22-67638

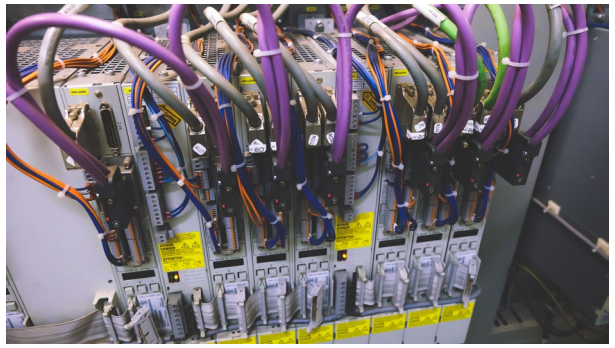
INL is managed by Battelle Energy Alliance for the US Department of Energy

Idaho National Laboratory

ICS Networks are *Still* Vulnerable to Cyber Attack

Current OT cybersecurity tools cannot monitor or protect most ICS networks

- Electrically incompatible or unable to interpret many ICS protocols
- Partially compatible but unable to capture real-time control packets



R&D efforts focus on IT networks:

- More standardized
- Offer better ROI
- Large, stable market

ICS networks are a harder sell:

- Fragmented market,
- Little standardization
- Poor ROI

Unique ICS cybersecurity challenges further discourage investment:

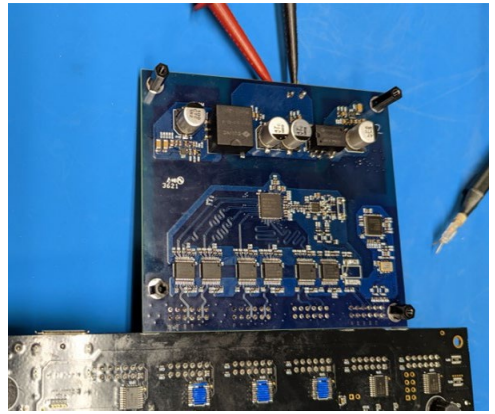
- Mix of serial & industrial Ethernet communication
- Proprietary operating systems and 'closed' ecosystems restrict accessibility
- Performance degradation/disruption are unacceptable

We need to prioritize cyber defense of ICS because the consequences of an attack are extremely severe:

- Loss of life
- Infrastructure damage
- Long-term disruption of energy supply
- Mass starvation
- Environmental contamination

OmniTap Bridges the *Communication* Gap

Today's cybersecurity tools can be leveraged to protect ICS networks… if provided access to network traffic



OmniTap is capable of interfacing with any ICS network:

- Connects to copper network media and captures signals
- Decodes and interprets signals *(up to 1Gbps)*
- Translates data and forwards it to cybersecurity tool/platform in TCP/IP packets

Extend the coverage of existing tools and platforms:

- Universal device simplifies procurement and deployment
- Forward data into your current SIEM, No proprietary platform or 'back-end' required
- OmniTap technology could be 'baked-in' to future cybersecurity tools and sensors

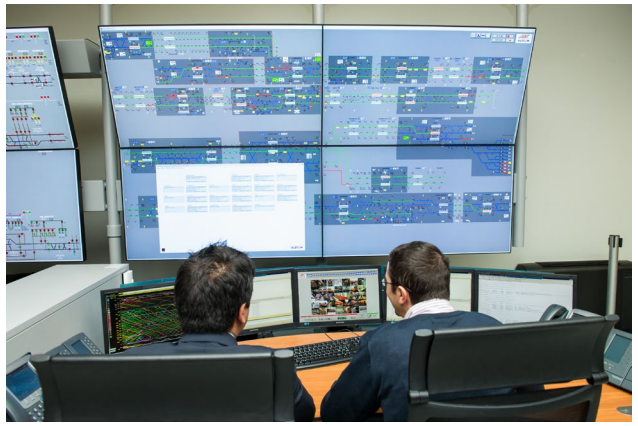
ICS cybersecurity paradigm shift:

- Enable existing cybersecurity tools to monitor and protect ICS networks
- Go beyond 'Defense in Depth' toward comprehensive ICS cyber-defense
- Align IT, OT, and ICS best security practices
- Mitigate ICS market fragmentation, encourage development of next-generation ICS cybersecurity tools

Get OmniTap to Market

The OmniTap technology is nearly ready for commercialization

- Currently at TRL 4, patent pending
- Will achieve TRL 5 upon completion of prototype testing fall 2022
- R&D effort concludes in October 2022



INL seeks partnerships and collaborative opportunities to enhance and accelerate the commercialization of this technology

- Federal and commercial partners involved in Critical Infrastructure cybersecurity
- ICS device, cybersecurity platform, and SIEM developers/vendors
- Incident response & cybersecurity providers/consultants
- CI asset owner/operators

Licensing & commercialization partnership

- INL and GoldenWolf LLC are working to formulate a collaborative commercialization plan to bring OmniTap to market.
- GoldenWolf recognizes the importance of monitoring control system networks in order to defend ICS, building automation, and other control systems against cyber threats.

GOLDENWOLF

GoldenWolf is an 8(a) Certified, Service-Disabled Veteran-Owned, Woman-Owned Small Business that solves facility management obstacles for federal clients.

Jacob Utley
Chief Technology Officer
GoldenWolf LLC
jutley@goldenwolf.com
www.goldenwolf.com

INL
Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.

Keith Mecham
CI Cybersecurity Engineer
Idaho National Laboratory
keith.mecham@inl.gov