Breakout Discussions – Session A (2:00 PM)

Challenges to EDS cyber resiliency from an expanding attack surface – Chancellor Ballroom

Session Chairs: Rakesh Bobba, Oregon State University and Stuart Madnick, MIT

Adoption of commodity operating system and networking technologies, deployment of ubiquitous measurement and control, intelligence of field devices, integration of DER, increased use of Internet-connected devices (aka IoT), wireless (WiFi) connectivity, and connections to third party systems are just some of the ways in which the cyber attack surface in EDS is expanding. The growing complexity may also increase the chances of an inadvertent failure from inadequate understanding on the part of the operator. ***(NOTE: the malicious insider will be discussed in the Evolving Adversary breakout session).***

- What are the pros and cons of adopting commodity OS and networking technologies, with respect to security?
- How do you address information sharing when connecting to third party systems?
- What are best practices for networking IT and OT? Are there pressures that hinder adoption of these best practices? Do IT / OT interfaces increase risks?
- How do you view challenges to securing field devices outside of a physical perimeter (including customer premise devices)?
- Should ICS vendors rethink development so as to permit minimal OS/firmware commands to execute the specific functions of the device?
- Discuss feasibility of disabling OS features, ports, USB interfaces, etc. as a strategy for reducing attack surface.

Compliance – Humanities Room

Session Chairs: David Norton, Federal Energy Regulatory Commission and Alfonso Valdes, University of Illinois at Urbana-Champaign

This session addresses issues of regulatory compliance and best practices as these impact cyber security in EDS.

- Some have expressed the view that compliance becomes an end in itself and a “paper exercise” that does not advance security.
- Do compliance objectives incentivize security objectives?
- It may be the case that compliance works at cross purposes to measures and technologies that potentially advance security (for example, SDN).
- What tools would help achieve and demonstrate compliance?
- Is it possible to develop a time-sequenced planning template for infrastructure improvements that simultaneously improve functionality, infuse security, and achieve and demonstrate compliance of the eventual system?

NOTE: EDS refers to Energy Delivery Systems. IT is Information Technology, and refers to conventional enterprise computer systems, whereas OT refers to operations technology systems, such as data historians, Human Machine Interface (HMI), engineering workstation, Remote Terminal Unit (RTU), Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controller (PLC), and field devices. Note that some OT systems use operating systems and networking technology that are also found in IT.

Breakout Discussions – Session A (2:00 PM)

Human Factors, Usability – Knowledge Room

Session Chairs: Sean W. Smith, Dartmouth College and Michael Siegel, MIT

A frequent complaint about cyber security solutions is that they are difficult to use and can get in the way of actual operational requirements. Well-intentioned users may circumvent security controls simply to get their jobs done. Also, many OT operators justifiably view availability as the most critical security property, and may consider practices such as shared passwords acceptable so that any operator can run the system.

- How can the security R&D community better understand the usability challenges and operational requirements of the real-world staff in the trenches?
- How do we gain buy-in as to the importance of security among management, system operators, and technical staff?
- How do we avoid alarm overload from security systems, when OT already provide alarms under dangerous process states?
- How do we mitigate the impact of security measures on OT systems, such as the difficulty of entering complex passwords for a field device in a physically harsh environment, or the motivation to share credentials because of the need that all operators in a control room must be able to bring a process to a safe state in an emergency?
- How can “best practices” from Safety be brought to Cyberattack Prevention?

Supply Chain Security – Innovation Room

Session Chairs: Paul Skare, Pacific Northwest National Laboratory and Abel Sanchez, MIT

Manufacturing is now a global undertaking, and most modern OT equipment has components, subassemblies, and firmware built or developed in multiple countries. While acceptance testing can verify that a component or system performs its designed function, it is difficult in practice to establish that it does not contain additional rogue functionality. This session identifies concerns arising from this reality, and explores ways to achieve trust in OT systems.

- What are your concerns about supply chain issues in your fielded OT technology?
- (For OT equipment providers) what measures are or should be taken to enhance trust in the supply chain?
- What is the role of vetting suppliers on the one hand, and verification technology on the other (for example, static analysis of firmware)?
- What are effective controls on how are 3rd party equipment maintained and updated? (e.g., employees are not allowed to bring USB into plant, but vendor maintenance personnel can/must.)

NOTE: EDS refers to Energy Delivery Systems. IT is Information Technology, and refers to conventional enterprise computer systems, whereas OT refers to operations technology systems, such as data historians, Human Machine Interface (HMI), engineering workstation, Remote Terminal Unit (RTU), Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controller (PLC), and field devices. Note that some OT systems use operating systems and networking technology that are also found in IT.

Breakout Discussion Notes

Breakout Discussion Notes

Breakout Discussions – Session B (3:15 PM)

Cross-sector Issues – Knowledge Room

Session Chairs: Saman Zonouz, Rutgers University and Tim Yardley, University of Illinois at Urbana-Champaign

Many EDS stakeholders are active in multiple EDS sectors. Many providers of OT and industrial control systems have customers in multiple EDS sectors. There are also sector inter-dependencies that should be explored.

- What are important similarities and differences in threats to electric power, pipeline, and O&G refining?
- What is the concern of common-mode vulnerabilities that may be discovered in OT that is found in multiple sectors?
- What can stakeholders in the various sectors learn from each other?
- Consider co-located heterogeneous infrastructures, such as a co-gen plant at a refinery. What are the reporting relationships (utility, asset owner, multiple)?

Data Analytics – Humanities Room

Session Chairs: Anna Scaglione, Arizona State University and Adam Hahn, Washington State University

EDS asset owners are collecting an unprecedented and increasing amount of data for a variety of operational and business functions. This session will explore how modern "big data analytics" can advance EDS cyber security.

- What data and analytical techniques are specific to EDS OT security (on the assumption that IT security is deployed where appropriate)?
- What are some differences in IT and OT security, and how can we leverage properties of OT for improved security?
- What models of information sharing are appropriate? At what time scale? Among EDS peer entities, or between these entities and managed security services?
- What are some ways to leverage EDS physical measurements with more conventional security tools to advance OT security?

NOTE: EDS refers to Energy Delivery Systems. IT is Information Technology, and refers to conventional enterprise computer systems, whereas OT refers to operations technology systems, such as data historians, Human Machine Interface (HMI), engineering workstation, Remote Terminal Unit (RTU), Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controller (PLC), and field devices. Note that some OT systems use operating systems and networking technology that are also found in IT.

Breakout Discussions – Session B (3:15 PM)

Evolving Adversary – Chancellor Ballroom

Session Chairs: Art Conklin, University of Houston and Michael Bailey, University of Illinois at Urbana-Champaign

Stuxnet and more recently the Ukraine incident demonstrate that attacks against OT are not hypothetical, and can have significant destructive impact. The most advanced attacks are increasing in sophistication, but today's sophisticated attack is tomorrow's ordinary hacker toolkit.

- Discuss adversary hierarchy, from nation state to major syndicate to ordinary hacker. Address persistence, financing, motivation, and countermeasures.
- What are the implications of sophisticated attack tools finding their way to hacker commodity markets? What does the hacker commodity market look like and how can we learn more about it?
- What are your concerns about the malicious insider? What are some ways this can be addressed?
- How do we as defenders stay ahead?

Workforce Development, Training, Education – Innovation Room

Session Chairs: Jana Sebestik, University of Illinois at Urbana-Champaign and Lori Ross O'Neil, Pacific Northwest National Laboratory

The required skills of an EDS system operator are very different from what they were a generation ago, and are continually evolving. On the other hand, the workforce that knows how to operate the system without the advanced controls is rapidly aging out. The modern EDS workforce must be aware of cyber security in addition to having the sophisticated knowledge required for system operation. As EDS also interface with the public (for example, demand response in electric utility settings), some degree of awareness of the OT issues in EDS among the public is desirable in order to bring about informed policy decisions.

- How do EDS stakeholders maintain workforce skills in the OT domain?
- How do EDS stakeholders grow cybersecurity workforce skills in the OT domain?
- Which knowledge, skills and abilities do EDS cybersecurity professionals need to be effective?
- What can educational institutions do to prepare and produce future cybersecurity EDS professionals?
- How can EDS stakeholders engage the public to achieve cybersecurity energy/economic/environment "win-win"?

NOTE: EDS refers to Energy Delivery Systems. IT is Information Technology, and refers to conventional enterprise computer systems, whereas OT refers to operations technology systems, such as data historians, Human Machine Interface (HMI), engineering workstation, Remote Terminal Unit (RTU), Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controller (PLC), and field devices. Note that some OT systems use operating systems and networking technology that are also found in IT.

Breakout Discussion Notes

Breakout Discussion Notes