CITES RESEARCH NEEDS ASSESSMENT – Fall 2022

Zero-trust networking

The fundamental idea behind zero-trust networking is to push provenance, authentication, integrity, and policy checking to edge devices in the network. In a zero-trust network compromised network devices might impede legitimate traffic, but edge devices are not fooled by corrupted traffic. Design and installation of zero-trust technology introduces significant added complexity to security management on edge devices. A real challenge is understanding if and how zero-trust networking can be effectively deployed in energy system OT networks.

Example (but not exclusive) problems

- OT systems cannot depend on cloud-based solutions for managing security credentials, policies, and associated data. Where should internal servers that manage them be placed with a company's system in such a way that the system is resilient to attempts to interfere with them?
- Zero-trust networks push security questions to the edge, but still rely on the network delivering the traffic to these devices. What kinds of network architectures and traffic management are best suited for making traffic delivery resilient to interference?

Intra-layer security management

The classic Purdue model for OT systems defines system layers Enterprise, DMZ, Operational and Control, Process, and, Physical, conceptualized as a "North-South." A layer is often treated as a single security zone, with security policies (like Biba) imposed between them. The problem is that better trust management is required within a layer, e.g., between RTUs within the Process layer. A challenge problem is to understand how to introduce so-called 'East-West' management of security.

Example (but not exclusive) problems

- What sort of model might replace the Purdue model?
- How can one best create and manage network zones to implement East-West trust, and what are the risks to resiliency associated with these approaches?
- How can one enhance security of current and emerging energy system OT pub-sub protocols, such as IEC 61850 GOOSE and Open Field Message Bus (OpenFMB)?

Secure System/Software Development and Lifecycle

A significant factor that leads to compromised computer systems is design and implementation flaws in the software components, and the ways they are connected to create a system. Security must be "baked" in, and part of that involves the methodologies and testing that are used in the development of that system or software. The needs extend throughout the entire lifecycle (requirements, planning, design, development, testing, deployment, maintenance).

Example (but not exclusive) problems

- Define the background/scope, including needs of utilities, needs of vendors, and needs of system integrators/distributers/wholesalers and subcontractors with respect to the lifecycle of security in software and systems. This would include a product lifecycle definition from identifying the product/needs for a product all the way through end of life and disposal.
- A gap analysis of the software and system lifecycle, comparing tools that are available for managing the lifecycle available, with needs.

Interacting Systems

New devices, applications, and systems designed to improve security are often envisioned without considering the dependence that the security they provide has on the security of the new entity itself. For example, introduction of PKI within an OT network necessitates introduction of a certificate server, which, if compromised or inaccessible, inhibits the security apparatus that depends on the PKI. The challenge is to identify techniques, methodologies, and/or analyses that help one to identify, consider, or forestall the risks attendant with introduction of that technology.

Example (but not exclusive) problems

- A critical component of any security system is effective and high-integrity device authentication. Security that relies on this impedes threats to that would otherwise exist to authentication systems. A problem is to identify such device identification techniques and quantify the reduction of risk to an OT's authentication system.
- OT software technology is created using a variety of commercial and open-source software modules. A software bill-of-goods may (and soon will) be associated with deployed code, so that when a vulnerability is reported in some module the dependency of other modules on that flaw can be identified. The problem is to proactively determine which software modules have the most significant impact on the system if they were to fail.
- Industrial internet of things devices may become involved in control systems. These rely on cellular communication, probably 5G, and may interact with cloud-based systems for things like state-estimation. How might these technologies be used together, and what are the benefits and (importantly) risks of that integration.

Energy System Protection

Advancing software and hardware technologies for protecting energy systems from cyber malfeasance. This needs area is broad.

Example (but not exclusive) problems

- Intrusion detection tailored to energy systems
- Technologies for describing and analyzing cyber-attacks and defenses in energy systems
- Hardware support for device identification
- Decision aids for application of security controls in energy systems
- Security for energy system micro-electronics
- Evaluation of access-control devices against formalized security policies typical in energy systems
- Protection against insider risk
- Models for determining/providing the "right" level of cryptographic strength of techniques that provide confidentiality, and integrity.
- Automate techniques to assess security posture, provide options to improve security management, add detection mechanisms, mitigate possible vulnerabilities
- Many others that are focused on protection in energy systems.

Secure Digital Infrastructure for Energy

Society is on the cusp of a new energy ecosystem, driven by requirements for efficiency and decarbonization as well as advances in energy sources, electric transportation, and market models. Realizing this vision will require a secure digital infrastructure for secure interoperability, trust relations among multiple stakeholder communities, secure and verifiable transactions, integration of non-conventional generation at multiple grid scales, and secure cloud operations.

Example (but not exclusive) Problems

- Secure integration of alternative energy resources, in distribution and transmission systems. Stability under high penetration of some alternative energy resources such as wind and solar present a challenge to system stability due to their intermittent nature. This can be potentially addressed by storage at all grid scales. IEEE 1547-2018 (in revision) for distributed energy resource (DER) integration mandates “ride through” for certain classes of DER to avoid the stability impact from a high penetration of DER all tripping at once in response to a disturbance. This integration requires complex control and communication, possibly between a utility and a third-party virtual power plant. How can we secure this communication and develop trust that the control commands are safe?
- Electric transportation. EV charging presents a significant grid impact, particularly as fast charging technology emerges. Fast charging requires more power for shorter duration than the currently typical charging operation that takes hours to complete. An error or malicious operation in fast charging can impact the vehicle, the charger, and possibly the distribution grid. The vehicle battery must authenticate to the charging provider to ensure correct billing and road use taxes. This should preserve vehicle operator privacy as to routes driven. Scheduling in an environment with many vehicles, or for a fleet of electric buses, must be done carefully so as to maintain system safety and fair (possibly time-sensitive) billing.
- What is the potential of edge-to-cloud frameworks for cyber-physical models running in faster than real time to verify correct AEPS-DER interoperability?