Reliability and Cyber-Physical Threat Model Generation from a Standards Influenced Ontology

Website: http://cred-c.org/researchactivity/edsthreatontology

Researchers (Illinois): Ken Keefe, Alfonso Valdes

Industry Collaboration:

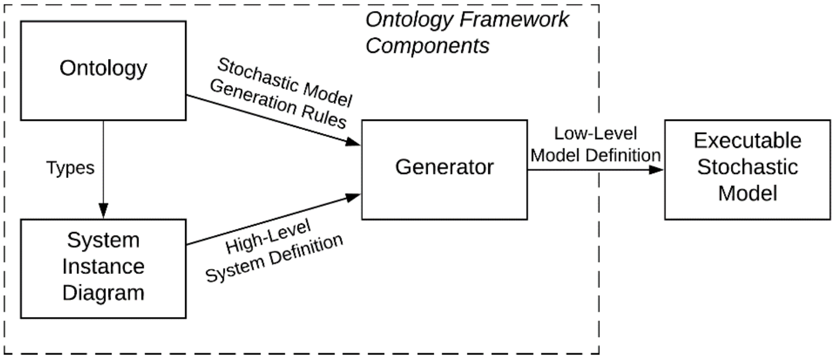
- ABB
- Duke Energy
- Also seeking additional industry collaborators in the electric power and O&G pipeline sectors.

Although we build on work done in electric power, specifically microgrid systems, we believe the concepts will generalize to different energy structures, and we will approach current industry contacts in the O&G pipeline sector.

Description of research activity: We propose to develop a theoretically sound methodology and associated tools to enable EDS stakeholders to model cyber adversaries, identify likely attack paths through an EDS, and identify candidate countermeasures to thwart attacker objectives. This will be based on an existing and proven adversary modeling framework, extended to comprehend an underlying physical EDS, and loosely coupled with a physical system simulation to estimate system impact of evolving attacker capability and identify the most damaging attacker pathways. By “loosely coupled,” we mean that model results when an attacker reaches an intermediate objective, as well as the system state, will form inputs to a physical system simulation to determine how the physical system would evolve from that point, with intermediate results fed back to the evolving adversary model.

ADversary VIew Security Evaluation (ADVISE) [1] [2] [3] has been developed and implemented in the Möbius modeling tool [4] to construct formal models of adversaries attempting to compromise a cyber-physical system. The Möbius tool evaluates ADVISE models using discrete-event simulation to gather observations and calculate estimated values of custom system metric functions. Several case studies [2] [5] [6] have examined the effectiveness of the Möbius ADVISE approach. While ADVISE models have proven useful in understanding threats against a system, the complexity of real world models prove to be too challenging for human modelers to effectively construct ADVISE models directly.

The ADVISE Meta approach resolves this problem by abstracting and formalizing the ADVISE model construction process by using the Möbius ontology framework. With ADVISE Meta, the modeler develops an ontology of component types, semantic relationship types among components, and ADVISE model fragments that are used to automatically generate an ADVISE model from a high-level system definition (System Instance Diagram) using the types defined in the ontology. Case studies [7] [8] have shown that this ontology-based model generation approach is practical and useful.


Ontology Framework Components
Ontology
Stochastic Model Generation Rules
Types
Generator
Low-Level Model Definition
Executable Stochastic Model
System Instance Diagram
High-Level System Definition

Dynamic Reliability Block Diagrams (DRBD) [9] [10] provide a rich, flexible way for modeling the reliability of systems and their constituent components. DRBD models are based on traditional, combinatorial reliability block diagram analysis methods, but incorporates a dynamic state over time to allow for evaluation of models using discrete-event simulation, which enables the evaluation of more complex systems. While the DRBD formalism has been implemented in the Möbius tool, the model generation extensions using the Möbius ontology framework have not.

The Möbius tool has a mature modeling framework that allows multiple models to be connected together to create a composed model. This composition is done by formally specifying how model state variables are unified or actions are synchronized. While Möbius has several composed model formalisms, the Rep/Join formalism is very well suited for connecting ADVISE and DRBD models to result in a comprehensive model for understanding intentional and unintentional faults. As ADVISE and DRBD models scale, this model composition can become difficult and would also benefit from the model generation approach offered by the Möbius ontology framework.

Möbius also allows the connection of outside code libraries and information sources in the execution and evaluation of its models. An important enhancement resulting from this activity will be a loose coupling of the ADVISE/ Möbius framework with high-fidelity simulations of the underlying physical system. For example, as an attack scenario evolves, the attacker may disable components such as relays (electric) or valves (O&G), which results in physical changes to the system. In the case of electric power, we will study and enable options for connecting external simulations implemented on platforms such as MatPower, Opal-RT, and RTDS. MatPower is software-only and runs in simulated time. Opal and RTDS support hardware-in-the-loop and real-time simulation.

This project seeks to enable the generation of comprehensive, detailed, stochastic models for exploring the reliability and security of energy delivery systems from high-level block-diagram system specifications. To accomplish this, the previous ADVISE Meta work will be expanded to generate dynamic reliability block diagram (DRBD) models using the Möbius ontology framework. ADVISE security models and DRBD reliability models will be generated from the same high-level system diagram. Additionally, Rep/Join models that connect the reliability and security models together will also be generated from the single system diagram.

In conjunction with expanding the model generation capabilities of the Möbius ontology framework, we will develop a new Möbius ontology that connects with previous ontology work and enables the generation of models that accurately represent an EDS. This ontology can be used for generating comprehensive, useful, stochastic models for exploring the reliability and security of energy delivery systems.

To develop and validate the information in the EDS ontology, as well as the models and metric values Möbius produces, we will engage an industry partner to develop an EDS case study. At regular meetings, we will continually discuss system definitions, intentional and unintentional fault risks, operations behavior, and metrics of interest.

The tool and the ontology (including model fragments) can be used by EDS stakeholders to assess relative security of alternative system configurations and identify security-critical system components that are candidates for increased investment in security and redundancy.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?

In order to effectively maintain and improve an existing EDS or design a new EDS, an analysis of cyber-physical threats must be undertaken. This project will provide the necessary tools to conduct such a rigorous analysis. With it, stakeholders will be able to assess their system designs for weak points. Users will be able to consider various design options and understand how different changes or improvements will impact overall system reliability and security.

The activity directly supports Roadmap objectives to “Assess and Monitor Risk” with a sound methodology that models risk dynamically as a threat to a system evolves [11].

More specifically, this work will develop methodology and tools to assess aspects of the NESCOR failure scenarios[12], for example, by providing a formal way to model criteria for effects on (attack) likelihood and opportunity (NESCOR section 4.2) as well as the stepwise evolution of the attack scenarios themselves (NESCOR chapter 5).

Summary of EDS gap analysis: Modern energy delivery systems (EDS) are an especially attractive target for attackers due to the high potential for damage to life and property. EDS owners, managers, designers, and other stakeholders lack risk assessment and adversary modeling methodologies and tools that (1) are theoretically sound, but usable, (2) consider both cyber and physical aspects of system operation, and (3) consider both intentional and unintentional faults, as well as how faults in one class can cascade into faults of the other.

Such a suite of tools and methodologies will allow an EDS stakeholder to formally model the threat to an infrastructure as that threat evolves. The benefit is a comparative analysis from a security standpoint of system design alternatives, as well as an identification of security-critical components in which to invest extra hardening measures.

Full EDS gap analysis: Attacks against the Ukraine Grid in 2015 and 2016 [13] and evidence of nation-state adversary activity against US energy systems [14] prove that energy systems are vulnerable to cyberattack, and that cyber adversaries are developing increasingly sophisticated techniques to attack these systems.

Understanding risk to an EDS is essential in order for EDS stakeholders to identify critical attack paths through an EDS, compare EDS design alternatives from the standpoint of risk, and identify critical components common to many attack paths to enable hardening of these components. Chapter 5 of the NESCOR failure scenarios [12] describes attack steps that an attacker might follow to achieve some adversary objective, but in fact these are typically one or a few paths of many that are possible to achieve the same objective. The NESCOR scenarios are therefore informative but not exhaustive in the sense of a formal analysis. There is currently no methodology or tool suite for formal risk modeling in EDS that is theoretically sound and considers cyber and physical aspects of EDS.

Additionally, there is no such methodology and tool suite that models and adversary’s path and alternative paths as these evolve through an attack, considering the value an adversary places on such objectives as stealth on the one hand and maximal system impact (outage or component damage) on the other.

The availability of such a methodology and tool suite would provide stakeholders with the ability to evaluate design alternatives with respect to security, identify critical attack paths through an EDS in pursuit of particular adversary objectives, and identify components on which defenses should be focused.

Bibliography:

[1] E. LeMay, Adversary-Driven State-Based System Security Evaluation, Urbana, Illinois: University of Illinois, 2011.

[2] E. LeMay, M. D. Ford, K. Keefe, W. H. Sanders and C. Muehrcke, "Model-Based Security Metrics using ADversary VIew Security Evaluation (ADVISE)," in *8th International Conference on Quantitative Evaluation of SysTems (QEST 2011)*, Aachen, Germany, Sept. 5-8, 2011.

[3] M. D. Ford, K. Keefe, E. LeMay, W. H. Sanders and C. Muehrcke, "Implementing the ADVISE Security Modeling Formalism in Möbius," in *43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2013)*, Budapest, Hungary, June, 2013.

[4] G. Clark, T. Courtney, D. Daly, D. D. Deavours, S. Derisavi, J. M. Doyle, W. H. Sanders and P. G. Webster, "The Möbius Modeling Tool," in *Ninth International Workshop on Petri Nets and Performance Models (PNPM 2001)*, Aachen, Germany, Sept., 2001.

[5] R. Wright, K. Keefe, B. Feddersen and W. H. Sanders, "A Case Study Assessing the Effects of Cyber Attacks on a River Zonal Dispatcher," in *11th International Conference on Critical Information Infrastructions Security (CRITIS)*, Paris, France, Oct. 10-12, 2016.

[6] M. Rausch, B. Feddersen, K. Keefe and W. H. Sanders, "A Comparison of Different Intrusion Detection Approaches in an Advanced Metering Infrastructure Network Using ADVISE," in *13th International Conference on Quantitative Evaluation of SysTems (QEST 2016)*, Quebec City, Canada, Aug. 23-26, 2016.

[7] M. Rausch, K. Keefe, B. Feddersen and W. H. Sanders, "Automatically Generating Security Models From System Models to Aid in the Evaluation of AMI Deployment Options," in *12th International Conference on Critical Information Infrastructures Security (CRITIS 2017)*, Lucca, Italy, Oct. 9-13, 2017.

[8] C. Cheh, K. Keefe, B. Feddersen, B. Chen, W. G. Temple and W. H. Sanders, "Developing Models for Physical Attacks in Cyber-Physical Systems," in *2017 Workshop on Cyber-Physical System Security and PrivaCy (CPS-SPC 2017)*, Dallas, Texas, USA, Nov. 3, 2017.

[9] K. Keefe and W. H. Sanders, "Reliability Analysis with Dynamic Reliability Block Diagrams in the Möbius Modeling Tool," in *9th EAI International Conference on Performance Evaluation Methodologies and Tools (VALUETOOLS 2015)*, Berlin, Germany, Dec. 14-16, 2015.

[10] T. Courtney, S. Gaonkar, K. Keefe, E. W. D. Rozier and W. H. Sanders, "Möbius 2.3: An Extensible Tool for Dependability, Security, and Performance Evaluation of Large and Complex System Models," in *39th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2009)*, Lisbon, Portugal, June, 2009.

[11] Energy Sector Control Systems Working Group. “Roadmap to Achieve Energy Delivery Systems Cybersecurity,” September 2011.

[12] National Energy Sector Cybersecurity Organization Resource (NESCOR). “Electric Sector Failure Scenarios and Impact Analyses, Version 3.0,” December 2015

[13] Robert M. Lee. “CrashOverride: Analysis of the Threat to Electric Grid Operations.” Available at https://dragos.com/blog/crashoverride/

[14] https://www.us-cert.gov/ncas/alerts/TA18-074A, last accessed March 20, 2018.