Customer: Bruce McMillin, ff@mst.edu, Professor of Computer Science

Project Description

Modern cyber-physical systems (CPS) contain multiple access points, particularly through edge devices such as smart meters, house monitors, cameras, and health devices. Attacks against infrastructure cyber-physical systems are growing in scale and sophistication. In September 2017 USA Today and other media outlets reported on a nine-month-long coordinated attack, discovered by Symantec, that successfully compromised U.S. power companies at an operational level [1]. ICS-CERT indicates manufacturing, energy, and water are all under attack [2, 3]. Traditional hierarchical firewall architectures are inadequate to secure against attacks within CPS; the key issue in the hierarchical approach is the need to rely on trust among the levels and trust among components within a level [4]. **The proposed approach secures systems by treating every aspect of the CPS as its own security domain and builds resilience to attack through securing the cyber and physical information flow present in the system.** While most security solutions focus on authentication, physically unclonable functions, and security domains [5], the proposed approach assumes components themselves cannot be trusted and, therefore, focuses on averting damage from Stuxnet-like [6] attacks that occur inside a security domain. Stuxnet, or man-in-the-middle, attacks are the most insidious as they can modify information streams without a system's knowledge, and, as in the case of Stuxnet, result in physical damage.

Efforts to secure the cyber-physical systems protecting the nation's infrastructure must contend with a wide range of complexities, including:

- Combining cyber and physical information flows affords the use of a single model to represent both. However, the semantics of combined cyber-physical information flow among security domains is not well understood from the point of view of effects of cyber operations on physical activity and physical activity on cyber operations, but must become understood if automation of securing information flows is to be achieved.
- Information flow is fundamentally bidirectional between two security domains [7]. Information flow either simultaneously preserves integrity and not confidentiality or simultaneously preserves confidentiality but not integrity, and this needs to be made clear to system designers.
- Mining a system's behavior through observing the system's operation may not uncover all of its operational modes, or may result in an overly complex model with a surplus of generated rules.
- Observations of the physical system may not be timely, accurate, or complete due to malicious information, bad data, communication delays, or noisy data.
- Proliferation of individual security domains causes a high model complexity, but merging too many of them results in a trivial, all-encompassing security domain.

The solution to the current vulnerability of infrastructure cyber-physical systems is to enhance the security of a CPS beyond what can be achieved through firewalls and trusted components, instead **building trust from observed behavior.** Physical systems must satisfy physical principles, such as conservation of energy and flows. Therefore, information flows through the physical network (e.g., power flow through transmission and distribution lines, water through pipes, vehicles through roadways, etc.), the cyber network (e.g., SCADA or smart meter infrastructure), and control actions (e.g., switched device settings or chemical dosing). These behaviors are **encoded into the system as invariants**. Redundant, yet inconsistent, information flows that do not satisfy

the invariants will be used to identify and isolate a malfunctioning device or a cyber intrusion. These invariants are **derived from scientific/engineering principles and/or learned**. State estimation affords a consistent view from which to evaluate the invariants. Figure 1 depicts the proposed architecture as applied to a water treatment system as an example of a **constructed cyber-physical system** that will be used to validate and assess the proposed work.

If a system is designed with an assumption of trusted devices, important information may be hidden, or to be precise, may be multiple security domain non-deducibility (MSDND) secure. The proposed project develops a system design (see Figure 1) in which each device, or even a subsystem within a device, forms a security domain that exchanges information with other security domains. Without suitable redundancy, the information such as the state of variable x within security domain SD^B is only known to security domain SD^A if SD^A trusts SD^B. Thus, if SD^B is breached, the intrusion cannot be detected. If instead, there are sufficient redundant information flows among many security domains, information within SD^B may be deduced by SD^A through its valuation V. Thus if SD^B is compromised, SD^A can identify the intrusion and isolate SD^B. These flows are physical, cyber, and cyber-physical in nature. By interpreting flows in this manner, a trusted system may be built up through the interactions of components.

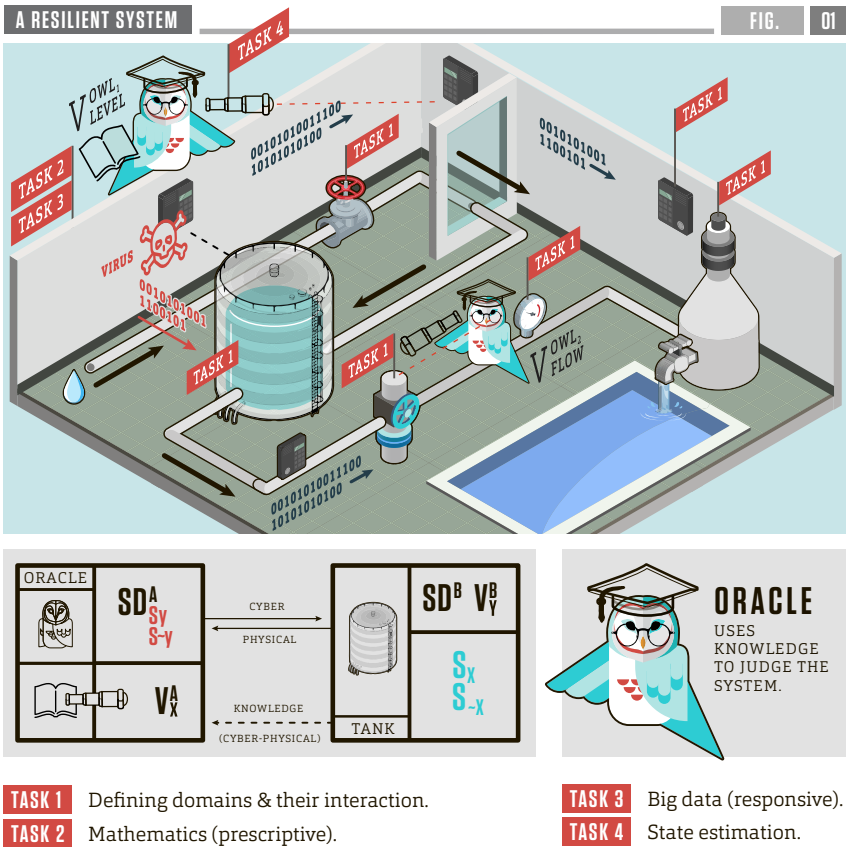

Figure 1: A water treatment system in which each component is in its own security domain. Each portion of the process is monitored (each with an owl who is an oracle of knowledge) through a valuation V (its spyglass) from that domain to other domains that contain information from the physical flows, cyber flows, and knowledge in the form of invariants (the books to ensure system operation. The Task labels show how the first 4 proposal tasks interrelate.

1 Research Description

The proposed work encapsulates the operational semantics of the system as a defense against attack, transforming the systems engineering to include knowledge of its operation. In previous work small-scale automobile systems [8], Stuxnet [9], chemical plant [10], and airspace management [11] were

analyzed, obfuscated information was identified, and additional information flows were added by a group of researchers with domain expertise. In the proposed work, the process will be automated to enable analysis of larger, more complex systems. The key innovation is a semantic encoding of the security domains and information flows. With appropriate semantics, machine learning techniques may be applied to ensure that the system is always deducible to defenders. The work proposed here deduces conditions that must hold during the operation of a physical process, and when violated, are indicative of cyber attack or component fault. The proposed solution will ensure the security of a wide range of CPSs.

1.1 Vision and Objectives

By changing the hierarchical approach to secured systems as prescribed by NERC CIP [12], NIST [13, 14], and National Academies [15] models, as well as most CPS security approaches [5], the proposed work fundamentally unseats the Bell La Padula/Biba (also Lipner) [16] models of security and integrity. The key issue in the hierarchical approach is the need to rely on trust among the levels and trust among components within a level (see [17] for a detailed discussion of this within the electric utility industry). Instead of relying on encryption, physically unclonable functions, and other authentication techniques to ensure the identity of each component, the proposed work ensures that these components are operating properly through attestation based on system operational rules.

Cyber-physical security embraces the concept that attacks may come to the cyber system, the physical system, or a combination of the two. However, most defenses are based in purely information systems. Extensive surveys [5, 18] enumerate many attacks in Industrial Control Systems (ICS), smart grid, vehicle, and medical domains. It is the view of the research team that all of these attacks are a disruption of the flow of signals, readings, or commodities. As such, securing the information flow (or, as we posit, disrupting the security of information flow) provides a unified way to describe attacks and defenses in cyber-physical security. The objectives undertaken to enable this vision include

1.2 Class Project

CPS are increasingly pervasive in society, but the risks to them and how to defend against risks is not well appreciated by the public. Technological fears can creep in (such as fear of self-driving cars). To better educate the population on risks so that they can make informed decisions, the research proposed to create accessible content. One way to excite young people about building trusted systems is with a tabletop game. In [19]], deep engagement occurs when the game incorporates direct interaction to facilitate abilities that map to learning outcomes. A water system-themed tabletop game is proposed to show students how water production can be disrupted by an attacker. Building and attacking teams will construct water systems out of component pieces of the water system that are be chained together. The attacker works to disrupt the flow. The defender comes up with rules that are applied to the system to locate and defeat the attacker. This game will be designed to encourage logical thought and an understanding of a cyber-physical security world 2.

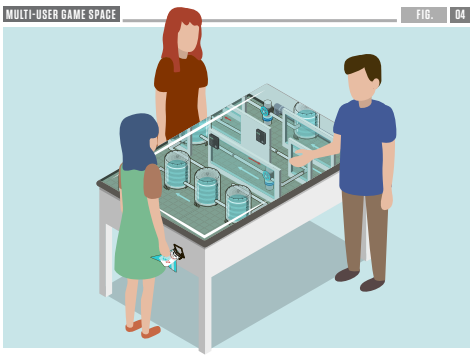

Figure 2: A Multi-User Multi-Touch Water Treatment Game in which at attacker can disrupt the system and the defender and add to the system (with the owl) as a concurrent competition

Students in the CS 4096 class will create the game and

deploy it on Multi-User Multi Touch (MUMT) monitors [20]. The students will work with the local community's hands-on STEM learning center, Kaleidoscope, to develop and deploy games for K-8 students.

Phases:

1. Semester 1 - develop prototype and simple mouse-enabled placement of the owl using prescribed information flows on a water system.
2. Semester 2 - Develop Game semantics using the prototype as a development tool
3. Semester 3 - Implement game on MUMT equipment
4. Semester 4 - test game among college students and link to actual CPS
5. Semester 5 - Deploy game at Kaleidoscope

References

[1] "Intrusion - but no attack - on U.S. energy grid is a warning, says former NSA official." [Online]. Available: https://www.usatoday.com/story/tech/news/2017/09/06/dozens-power-companies-breached-hackers-cybersecurity-researcher-says/638503001/

[2] "Year in Review 2015 | ICS-CERT." [Online]. Available: https://ics-cert.us-cert.gov/Year-Review-2015

[3] "Year in Review 2016 | ICS-CERT." [Online]. Available: https://ics-cert.us-cert.gov/Year-Review-2016

[4] C. E. Landwehr, "Formal models for computer security," *ACM Comput. Surv.*, vol. 13, no. 3, pp. 247–278, Sep. 1981. [Online]. Available: http://doi.acm.org/10.1145/356850.356852

[5] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security - a survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, Dec 2017.

[6] G. Howser and B. McMillin, "A modal model of stuxnet attacks on cyber-physical systems: A matter of trust," in *2014 Eighth International Conference on Software Security and Reliability (SERE)*, June 2014, pp. 225–234.

[7] D. Sutherland, "A model of information," in *Proc. 9th National Computer Security Conference*. DTIC Document, 1986, pp. 175–183.

[8] G. Howser and B. McMillin, "A multiple security domain model of a drive-by-wire system," in *2013 IEEE 37th Annual Computer Software and Applications Conference*, July 2013, pp. 369–374.

[9] G. Howser and B. M. McMillin, "A modal model of Stuxnet attacks on cyber-physical systems: A matter of trust," in *Software Security and Reliability (SERE), 2014 Eighth International Conference on*, June 2014, pp. 225–234.

[10] P. R. Dunaka and B. McMillin, "Cyber-physical security of a chemical plant," in *2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)*, Jan 2017, pp. 33–40.

[11] A. Thudimilla and B. McMillin, "Multiple security domain nondeducibility air traffic surveillance systems," in *2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)*, Jan 2017, pp. 136–139.

[12] North American Electric Reliability Corporation (NERC), http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx, accessed December 30, 2015, Tech. Rep., 2015.

[13] National Institute of Standards and Technology, http://sgip.org/NISTIR-7628-User-s-Guide—Smart-Grid-Cyber-Security-Implementation-Guidelines, accessed December 30, 2015, Tech. Rep., 2010.

[14] National Institute of Standards and Technology, http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pd accessed December 30, 2015, Tech. Rep., 2014.

[15] *Terrorism and the Electric Power Delivery System*. National Academies Press, 2012.

[16] M. Bishop, *Computer Security: Art and Science*. Boston, MA: Addison-Wesley Longman Publishing Co., Inc., 2002.

[17] B. McMillin, T. Roth, E. Bertino, and R. Sandhu, *Cyber-Physical Security and Privacy in the Electric Smart Grid*. Morgan & Claypool, 2017. [Online]. Available: https://ieeexplore-ieee-org.libproxy.mst.edu/xpl/articleDetails.jsp?arnumber=8025534

[18] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, "Security and privacy in cyber-physical systems: A survey of surveys," *IEEE Design Test*, vol. 34, no. 4, pp. 7–17, Aug 2017.

[19] S. Nicholson, "Making gameplay matter: Designing modern educational tabletop games," *Knowledge Quest*, vol. 40, no. 1, pp. 60–65, Sep-Oct 2011.

[20] S. Niu, D. S. McCrickard, and S. M. Nguyen, "Learning with interactive tabletop displays," in *2016 IEEE Frontiers in Education Conference (FIE)*, Oct 2016, pp. 1–9.