Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 61 (2015) 221 – 226

Procedia Computer Science

Complex Adaptive Systems, Publication 5
Cihan H. Dagli, Editor in Chief
Conference Organized by Missouri University of Science and Technology
2015-San Jose, CA

Using Discrete Event Simulation to Model Attacker Interactions with Cyber and Physical Security Systems

Casey Perkins[a], George Muller[a]

[a]*Pacific Northwest National Laboratory, Richland, WA, USA*

Abstract

The number of connections between physical and cyber security systems is rapidly increasing due to centralized control from automated and remotely connected means. As the number of interfaces between systems continues to grow, the interactions and interdependencies between them cannot be ignored. Historically, physical and cyber vulnerability assessments have been performed independently. This independent evaluation omits important aspects of the integrated system, where the impacts resulting from malicious or opportunistic attacks are not easily known or understood. We describe a discrete event simulation model that uses information about integrated physical and cyber security systems, attacker characteristics and simple response rules to identify key safeguards that limit an attacker's likelihood of success. Key features of the proposed model include comprehensive data generation to support a variety of sophisticated analyses, and full parameterization of safeguard performance characteristics and attacker behaviours to evaluate a range of scenarios. We also describe the core data requirements and the network of networks that serves as the underlying simulation structure.

Peer-review under responsibility of scientific committee of Missouri University of Science and Technology

Keywords: Cyber-physical systems; vulnerability assessment; discrete event simulation; risk analysis

1. Introduction

In the realm of system security, the ability to quantify risk and vulnerability has been rigorously pursued. Often, the threat and consequence elements are determined to be outside of a system's control; subsequently, the stand-alone vulnerability assessment (VA) has been widely adopted. One such methodology relies upon the concept of timeliness of detection, attempting to identify the point in the system at which the response to a security breach has sufficient time to act to neutralize the threat, avoiding the realization of any consequence. Security analysts use Vas to build and evaluate representations of their systems against a host of threats, attempting to arrive at some metric to

Peer-review under responsibility of scientific committee of Missouri University of Science and Technology
doi:10.1016/j.procs.2015.09.199

measure the attacker's ability to "win". The definitions of consequence and what it means to "win" depend on the system under study, but the aim of reducing risk by reducing vulnerability is largely universal. While security analysts working in the physical security domain have been performing standardized vulnerability assessments for decades, cyber security vulnerability analyses are still, in most respects, in early stages. While these assessments have matured, cyber VAs and physical VAs are still not executed in an integrated fashion. Because cyber-physical systems combine the physical nature of cyber networks and the cyber aspect of the evolving physical security system, it is unclear whether separate vulnerability assessments for the cyber and physical systems analyses are sufficient for comprehensive analysis. The framework in this paper details an approach that can be used to perform an integrated cyber-physical vulnerability assessment.

2. Literature Review

The emergence and growth of cyber-physical systems (CPS) has complicated traditional vulnerability analyses (VA) by exposing novel access mechanisms and unanticipated interdependencies between cyber and physical infrastructure. Typically, VAs are performed for either cyber or physical infrastructure. These analyses overlook complex interactions that exist as a result of system interfaces. Physical protection methodologies, such as the timeliness of detection methodology, are currently employed in the analysis of physical systems. Methodologies for cyber VA are continually being researched and developed in response to cyber tools that are continuously being developed to exploit new network vulnerabilities.

Haimes (1) provides a concise set of requirements to assess risk from infrastructure vulnerabilities. These include the determination of the likelihood of the threat or attack scenario, models for response of the interdependent state variables that comprise the system, and the assessment of the consequences from a successful attack. Ezell (2) provides an infrastructure vulnerability assessment model (I-VAM) that quantifies vulnerability in terms of the scenario being studied. I-VAM assesses security effectiveness using a value model that incorporates deterrence, delay, detection, and response factors. The I-VAM model uses Monte Carlo simulation to develop a probability distribution for system vulnerability based on a specified scenario.

Jordan et al (3) describe a discrete-event simulation for physical protection systems. This approach allows greater fidelity in protection system assessments than was previously available. The result is greater insight into the interactions for physical infrastructure systems.

Byres et al (4) apply attack trees to assess supervisory control and data acquisition (SCADA) systems. Attack trees, originally proposed by Schneier (5), allow qualitative assessment by enumerating the ways that a system can be exploited and the steps required to perform an attack. Leaves of the attack tree correspond to attacker outcomes at various levels within the tree.

Ingols et al (6) extend the attack tree methodology to explicitly account for specific attacks, detection mechanisms and prevention systems on a network. This method uses the set of vulnerabilities and a reachability metric for the network to generate the set of attack graphs. The authors tested this method on an operational network with 85 hosts, and a simulated network with 40,000 hosts. The results provide insights into the best uses of countermeasures and safeguards to prevent disruptive cyber attacks on these networks.

Shi et al (7) present distinguishing features for cyber-physical systems. The authors describe CPS exemplars, including healthcare and medicine technology systems, electric power grid and intelligent transportation systems. Each of these systems is an example of the Internet-of-Things and yields real-world consequences that could result from malicious information-domain exploits.

Hadjsaid et al (8) describe methods to explore the interdependencies and cascading failures in information-connected power systems. These include simulation, an application of network theory, and Bayesian networks. The authors suggest a set of precedence graphs and modified failure modes, effects, and criticality analysis be used to explore the interdependencies in these networks. Cardenas et al (9) describe three challenges in cyber-physical system security. These include understanding the threats and potential consequences, identifying the unique characteristics of cyber-physical systems that differentiate them from traditional information technology systems, and developing security methods for cyber-physical systems that address these unique characteristics. The authors apply this discussion to a SCADA system and discuss an approach to constructing a cyber-physical system testbed to explore these challenges.

Chen et al (10) use low- and high-level Petri nets to simulate combined cyber-physical attacks against a CPS. The authors apply the method to a smart meter attack, primarily using binary state variables for the system's protection mechanisms. Sridhar et al (11) present risk analysis methods and open challenges for cyber-physical security of the electric power grid. The authors build on existing methods such as Byzantine fault tolerance and N-1 contingency analysis, and present open challenges in CPS for the power grid.

The complex interdependencies that exist in the integrated security infrastructure make it difficult to evaluate the security posture of integrated cyber-physical systems. This paper provides a method that offers insight into the security posture of these complex cyber-physical systems to inform decision makers in the effective application of safeguards for infrastructure protection against cyber-physical threats. Because of interdependent system components, unplanned cyber-physical interactions weaken overall infrastructure security effectiveness. Our work implements the methodology described by MacDonald et al (12) and focuses on the types of CPS described by Shi et al (7). The implementation extends a similar discrete-event approach by Jordan et al (3) to include cyber infrastructure, which also enables a greater level of fidelity for analysis of the safeguards and countermeasures protecting the system.

3. Method

Traditional physical infrastructure vulnerability assessments use a system effectiveness score as the overall system security performance measure. The system effectiveness score often represents probability of attacker failure. Security system designers and decision makers perform trade studies to identify security improvements that result in improved overall system effectiveness. Cyber security research is often modeled for specific threats or vulnerabilities, typically addressing a small subset of overall system vulnerabilities. These analyses overlook important implications for an integrated system. The integration of these systems results in cascading effects that can render safeguards in one domain useless. Modeling the integrated network at an appropriate level allows deeper analysis of specific pathways to identify patterns of vulnerability and identify specific pathways or safeguards that should be targeted for improvement.

The method described below applies to the following attack scenario: a blended cyber-physical attack initially exploits vulnerabilities in the enterprise network to access a connected security system. The security system software is exploited to reduce the effectiveness of safeguards through simple changes to safeguard settings. The attack then progresses in the physical domain, where the attackers take advantage of degraded safeguards to reach the objective unimpeded.

The integrated cyber-physical security system simulation models the interactions of an attacker with the security elements of the system where the attacker's goal is to reach a specified target within the system before being neutralized. The goal for security system designers is to design a system such that the likelihood of an attacker successfully reaching a target, or set of targets, is minimized. System security is comprised of different types of safeguards that contribute to the delay and detection of an attacker. Safeguards are the primary point of interaction between the attacker and the security system for both cyber and physical domains. The primary goal of the model is to support vulnerability analysis of an integrated system and analyze how interactions between cyber and physical elements contribute to overall vulnerability.

Like traditional discrete event simulation, the integrated security system simulation framework is comprised of a set of entities with attributes and an event graph that controls the entity flow logic. The basis for the movement of the attacker is defined by a super-graph with one sub-graph representing the cyber nodes and arcs and a second sub-graph representing the physical nodes and arcs. The system graph provides the landscape in which the attacker will attempt to execute an attack to reach a specified target. Two key interactions between the sub-graphs illustrate the impact of integrated systems: 1) cyber elements are physically located within the system, providing direct access if physically manipulated, and 2) safeguard performance in either domain can be altered via access gained in the other domain.

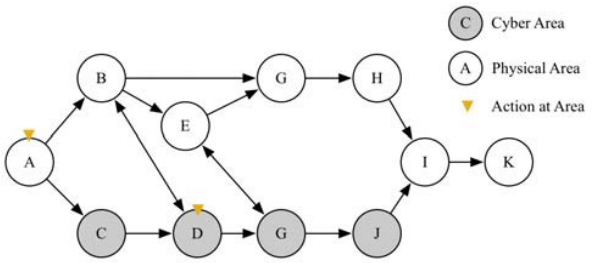

Figure 1. Graph representation of integrated cyber-physical system.

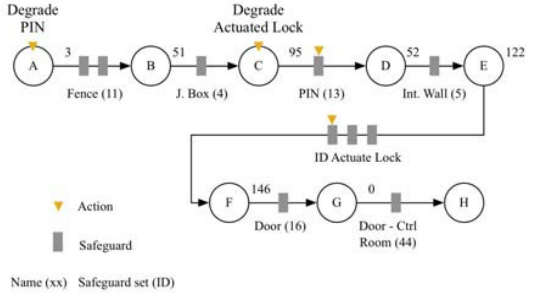

Figure 2. A pathway generated by the simulation. These pathways result from the integrated cyber-physical system, which allow effects to propagate.

3.1. System Representation

The construction of the object space for the system is represented by a graph or, more specifically, two sub-graphs with with directed arcs: the first sub-graph represents the physical system and the second sub-graph the cyber system. In each graph, the areas of the system are modeled as nodes and the arcs of the graph represent connections between areas. Arcs on the physical sub-graph represent avenues of access, such as doorways, hallways or open areas. For the cyber sub-graph, the arcs represent connections between zones or domains on a network. Safeguards are located on arcs, separating access from one area to another. During a simulated attack, the attacker traverses the graph from one node to an adjacent node, seeking to ultimately reach a single target or a set of targets.

Additional arcs exist that connect the two sub-graphs to form the higher-level system graph (Figure 1). These connections are strictly directed, meaning that arcs between cyber and physical areas can only exist in one direction: from the physical area to the cyber area. One example of a connection between a physical area and a cyber area is the location of network assets within a physical area, such as a terminal located in a server room, or work stations in offices. These connections represent the first type of cyber-physical interactions in integrated systems. The second type of interaction occurs when physical elements (e.g. safeguards) depend on cyber elements. These dependencies are not represented in the graph structure, but rather as events that dynamically alter states of safeguards within the simulation.

A strict graph representation for this problem requires several assumptions since an attack can introduce cycles in the super graph. To overcome these limitations, we developed a discrete event simulation (DES) with logic to control attacker behavior for the directed arcs of the graph.

3.2. Entities

The entity types for this model include an attacker type and a response type. The attacker entity is defined by several key attributes including target location information as well as competency in negotiating both physical and cyber safeguards. Real world attacks typically follow two different modes: speed and stealth. Each attacker is initially assigned either a speed or stealth attack mode. The goal of a swift attack is to reach the target before a response is able to disrupt the attack. These attacks occur quickly with little or no regard by the attacker to the overall likelihood of detection. Examples include brute-force and denial-of-service cyber-attacks or smash-and-grab physical attacks. Stealth attacks occur when the attacker is intent on reaching an objective unnoticed and when the overall likelihood of success is limited by a capable security response.

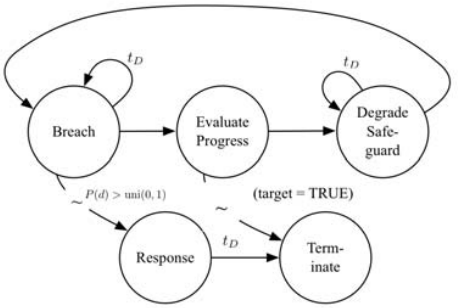

Figure 3. The event graph of the discrete event simulation includes time delays and detection likelihoods for both cyber and physical security measures.

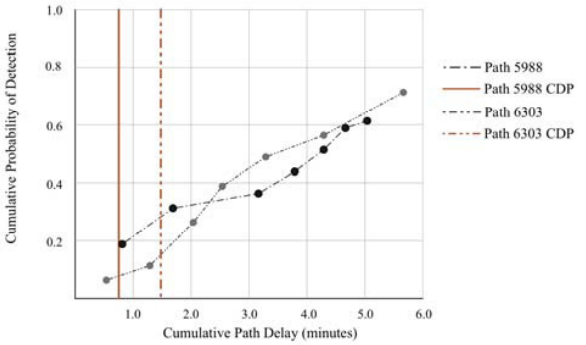

Figure 4. Each generated pathway is a path through the cyber-physical attack tree. These pathways differ in their performance and enable exploration to identify weaknesses in the integrated system security.

The response entity is more simply characterized by assigning a response time: the time it takes to respond after detection of the attack. With the introduction of the response type entity rather than a simpler response timer, the framework may be extended to allow for not only interdiction and neutralization attributes, but also for multiple response entities with more specific capabilities. Implementation of the original DES prototype used only a single attacker and a single response; however, the framework is intended to allow for multiple attackers and multiple response types, though that would require additional entity event logic to handle coordination between entities.

3.3. Events and Safeguards

The event graph (Figure 3) associated with the model illustrates the logic that dictates the attacker and response entity flow. The attacker entity executes three primary events: selecting an area to gain access, breaching safeguards along the way, and degrading safeguard performance in the system. Additional events occur that handle detection and evaluate attack progress. The detection event initiates the response entity into action and the evaluation of progress provides a means to simulation termination. Once a detection event occurs in the attacker event graph, the response entity proceeds to neutralize the attacker after a prescribed amount of time. There are two terminating conditions to end a single attack: the attacker either reaches all targets or the response entity successfully neutralizes the attacker.

Area nodes are separated by one or more sets of one or more safeguards. Safeguards are the security measures deployed in the system to defend against attackers, and provide two key functions. The first is to delay the attacker as they navigate the system and the second is to detect the attack. For each safeguard, the detection and delay performance values are attacker dependent: the amount of delay and probability of detection are dependent on the attacker's skill levels in cyber or physical attacks. The degradation of safeguards behavior is at the core of representing the integrated cyber-physical network. As an attacker progresses through the integrated system, changes to safeguard delay and detection are propagated based on the adversary's exploitation of connections between the cyber and physical sub-graphs. The key events are:

- Breach safeguard: The attacker experiences a time delay and an opportunity to be detected for each safeguard encountered. The delay time for speed attacks is usually shorter than for stealth attacks, but usually comes with a higher detection probability.
- Response: If the attacker is detected, a response is initiated. For detection on a physical safeguard, a physical response force is launched. For detection on a network (cyber) safeguard, the response is to close the affected network connections. If the response is completed before the attacker reaches the target, the attack is neutralized and the system is successfully defended.
- Evaluate progress: Upon reaching the next area, the attacker evaluates if there are any remaining targets left to attain. If not, then the simulation terminates.

- Degrade safeguard: If breached or exploited, a safeguard will remain in a degraded state for the remainder of the attack. The percent performance reduction is a safeguard dependent variable. In addition, certain areas within the integrated cyber-physical system allow degradation of safeguard performance.

4. Discussion

The simulation results are used to explore the range of outcomes from the model. Decision makers require an understanding of the system behavior to improve the security effectiveness of the system. The critical detection point (CDP) is widely used in physical VAs to identify the point at which the attacker must be detected in order to successfully neutralize the attack. The decision maker then has three opportunities to improve system effectiveness: add detection *before* the CDP; add delay *after* the CDP; or reduce the response time. Figure 4 depicts the cumulative probability of detection versus cumulative time in the system for two unique pathways through the system. A perfect system would achieve 100% cumulative probability of detection before the CDP. A range of CDP probability of detection intersections can be visualized by including all of the pathways generated by the simulation. The decision maker can then add or update safeguards to improve detection likelihood to the left of the CDP, increase delay to the right of the CDP, or move the CDP to the right by reducing the response time.

The use of cost-benefit analysis improves the decision support utility of the simulation. Improving safeguards can be costly. Understanding the implications of these improvements allows the decision maker to selectively target the safeguards that best benefit the overall system. This cost-benefit analysis allows decision makers to quickly identify the individual safeguard improvements that result in the best overall increase in system effectiveness.

5. Conclusions

This paper demonstrated an analysis method for complex cyber-physical infrastructure attacks. The connections between these domains will continue to grow with new technologies that emerge as part of the Internet-of-Things. However, as these technologies grow, so do the vulnerabilities between connected cyber and physical systems. This analysis method extends existing vulnerability assessment approaches to obtain deeper insights into the how integrated security systems can be improved. We have described a novel performance measure that succinctly describes the effectiveness of the integrated system and how this measure can be used to inform decision making. Additional work is needed to rapidly model the integrated cyber-physical system, develop better cyber response models, and to explore additional analysis methods that are suited to the detailed discrete event simulation results.

References

1. Haimes YY. On the definition of vulnerabilities in measuring risks to infrastructures. Risk Anal. 2006;26(2):293–6.
2. Ezell BC. Infrastructure vulnerability assessment model (I-VAM). Risk Anal. 2007;27(3):571–83.
3. Jordan SE, Snell MK, Madsen MM, Smith JS, Peters BA. Discrete-event simulation for the design and evaluation of physical protection systems. Proceedings of the 1998 Winter Simulation Conference. 1998. p. 899–905.
4. Byres EJ, Franz M, Miller D. The use of attack trees in assessing vulnerabilities in SCADA systems. Int Infrastruct Surviv Work [Internet]. 2004;1–9. Available from: http://www.ida.liu.se/~rtslab/iisw04/camready/SCADA-Attack-Trees-Final.pdf
5. Schneier B. Attack Trees. Dr Dobbs J [Internet]. 1999;24(December):21–9. Available from: http://www.schneier.com/paper-attacktrees-ddj-ft.html
6. Ingols K, Chu M, Lippmann R, Webster S, Boyer S. Modeling modern network attacks and countermeasures using attack graphs. Proc - Annu Comput Secur Appl Conf ACSAC. 2009;117–26.
7. Shi J, Wan J, Yan H, Suo H. A survey of Cyber-Physical Systems. 2011 Int Conf Wirel Commun Signal Process WCSP 2011. 2011;
8. Hadjsaid N, Tranchita C, Rozel B, Viziteu MG, Caire R. Modeling cyber and physical interdependencies - Application in ICT and power grids. 2009 IEEE/PES Power Syst Conf Expo PSCE 2009. 2009;1–6.
9. Cardenas AA, Amin S, Sinopoli B, Giani A, Perrig A, Sastry S. Challenges for Securing Cyber Physical Systems. Work Futur Dir cyber-physical Syst Secur [Internet]. 2009; Available from: http://chess.eecs.berkeley.edu/pubs/416.html
10. Chen TM, Sanchez-Aarnoutse JC, Buford J. Petri net modeling of cyber-physical attacks on smart grid. IEEE Trans Smart Grid. 2011;2(4):741–9.
11. Sridhar S, Hahn A, Govindarasu M. Cyber-physical system security for the electric power grid. Proc IEEE. 2012;100(1):210–24.
12. MacDonald D, Clements SL, Patrick SW, Perkins C, Muller G, Lancaster MJ, et al. Cyber/physical security vulnerability assessment integration. 2013 IEEE PES Innov Smart Grid Technol Conf ISGT, 2013.