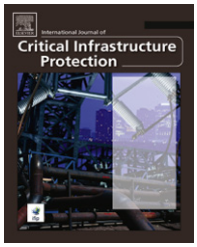
available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/ijcip



Coupled Petri nets for computer network risk analysis

*Matthew H. Henry**, *Ryan M. Layer*, *David R. Zaret*

Johns Hopkins University Applied Physics Laboratory, Laurel, Maryland 20723, USA

ARTICLE INFO

Article history:
Received 15 January 2010
Accepted 8 April 2010

Keywords:
Petri nets
Computer network attack modeling
Risk analysis

ABSTRACT

This paper presents a framework for quantifying the risk induced by the potential for cyber attacks levied against network-supported operations. It also permits a formal assessment of candidate risk management policies that address network host vulnerabilities and host-process coupling. The framework incorporates a novel application of Petri net state coverability analysis coupled with process failure mode analysis. It extends previous work on Petri nets for attack analysis in three ways: (i) new metrics that quantify risk as a function of Petri net state and techniques for evaluating the metrics based on the minimal coverability set of a Petri net; (ii) a new method for coupling a Petri net representation of a computer network attack to a process failure modes model; and (iii) a new method for identifying high-value risk management opportunities. The paper concludes by presenting an application of the analysis techniques to evaluate risk in process control networks.

1. Introduction

In an earlier paper [1], we presented a Petri-net-based model and analysis technique for evaluating the risk induced by computer network attacks levied against industrial process control systems. More specifically, we described an application of the Petri net formalism to computer network attack modeling, along with a technique based on coverability analysis [2,3] for computing a practical abstraction of attack state reachability. In addition, we informally described an approach for evaluating risk based on mapping Petri net coverability to measures of operational consequence.

This paper describes a more formal approach to coupling the state dynamics of a computer network attack to the system operations for which the network nominally conveys command and control authority. It also presents a method for identifying high-value risk mitigation opportunities and communicating them to decision-makers in terms of efficient cost-benefit tradeoffs.

2. Motivation

A variety of research efforts have investigated techniques for evaluating the risk of computer network attacks. The recent interest in critical infrastructure protection has spawned several research threads related to the risk of computer network attacks directed against industrial process control systems (PCS). Several of these threads (see, e.g., [4–6]) describe techniques for evaluating risk in terms of the likelihood and consequences of outcomes in accordance with the classic definition of risk codified by Lowrance [7]. In many cases, the parameters needed to support probabilistic measures may be difficult to estimate due to the lack of credible data, although we recognize the value of devising data collection regimes to facilitate such parametric techniques.

In contrast with these data-intensive approaches to risk analysis, we seek a robust technique that does not rely on measures of likelihood. In particular, we seek metrics that account for a reachable attack state given initial conditions

* *Corresponding author.*
E-mail addresses: matthew.henry@jhaupl.edu (M.H. Henry), ryan.layer@jhaupl.edu (R.M. Layer), david.zaret@jhaupl.edu (D.R. Zaret).

1874-5482/$ - see front matter
doi:10.1016/j.ijcip.2010.05.002

on attacker access to network resources, specified host configurations in the network and a set of known host vulnerabilities. Using these measures, we support a more flexible notion of risk that can be resolved as one of several computable measures on the discrete attack space.

In this paper, we discuss a technique for modeling a computer network attack, the system whose operations are impeded or manipulated by the attacker's control of network resources, and the logical coupling relationships that permit the attacker, given control of network resources, to impede or manipulate system operations. In particular, we construct separate Petri nets for each of these model elements and couple them using appropriately designed interfaces. The advantage of this approach over the informal approach in [1] is that the system failure state's reachability is computed directly as part of the coverability set, which reduces the analysis time. This approach also supports a traceback technique to identify high-value (in terms of operational consequences) risk mitigation opportunities.

3. Related work

Petri nets have been discussed in the recent literature as a useful formalism for network security evaluation [8–10]. Several papers consider the use of colored Petri nets for attack modeling. Zhou, et al. [10] discuss the advantages of this formalism and describe a process for mapping an attack tree to a colored Petri net. Dahl [8] provides a more detailed discussion of colored Petri nets. In particular, Dahl emphasizes, as we do, that Petri nets can be used to model concurrency and attack progress. Also, Dahl presents several examples of attack modeling using colored Petri nets.

Our paper differs from those by Zhou, et al. [10] and Dahl [8] by focusing on the simpler "place-transition" Petri net formalism. We develop several ideas that are initially sketched in [9], although our work stands out from others (e.g., [8–10]) in that it uses Petri nets to capture a resource-based conception of risk, develop techniques for risk analysis based on the construction of a Petri net coverability graph, and create a coupling between the Petri net that models the attack space and the corresponding Petri net that models the correctly operating network or application.

Other methodologies such as NetSPA [11] approach risk assessment from a similar vantage point. NetSPA employs strong assumptions regarding the homogeneity of hosts and the monotonicity of attacks to deal with very large systems. Our Petri net approach scales comparably under similar assumptions of monotonicity and network host homogeneity; however, it differs in how the model is constructed and in the distribution of atomic action pre-conditions over the set of network resources. In our view, our Petri net approach offers a more flexible modeling paradigm than the attack graph technique adopted by NetSPA.

4. Problem definition

This paper focuses on the problems of risk assessment and risk management. The risk assessment problem can be stated as: determine the degree to which a specified network-dependent system is at risk due to the potential for computer network attack. In addressing this problem, we model the network-dependent system as a Petri net in which the attack state dynamics discussed in [1] are coupled to failure modes and effects using an appropriately designed interface. Our coupling scheme represents the functionality of network hosts (over which an attacker can gain control via intrusion and privilege escalation) in terms of process interface and control applications. By doing this, we increase the dimensionality of the attack state space described in [1] to include the process state space. The result is a compound state space over which coverability (an abstraction of state reachability) can be computed directly to assess risk, as each process state has a set of operational consequences associated with it expressed in terms that are meaningful for cost-benefit analysis of risk mitigation alternatives.

The risk management problem can be stated as: given a computed coverability set for the network-dependent system of interest, determine the relative costs and benefits of implementing identified candidate risk mitigation policies in terms of resources expended and operational consequences avoided, respectively. In addressing this problem, we conduct informed searches over the coverability set to identify network host vulnerabilities, access control policy failures and architectural weaknesses that, if corrected, yield high returns in terms of avoided operational consequences. These returns are compared against the cost of implementing the candidate corrections in the cost-benefit space to identify the efficient courses of action. While we have not yet automated this process, the principles are well-understood and yield useful insights.

5. Petri nets for risk assessment

This section describes our extended risk assessment methodology based on the approach introduced in [1]. We are concerned with computer network attacks on systems with corresponding process failure modes of operational consequence. That is, we are concerned with failure modes that result in the disruption of some broadly defined system mission such as process control, which results in substantial material loss. We do not consider the compromise of any particular host or network account to be of operational consequence *per se*. Rather, operational consequences are derived from the actions taken after the attacker has compromised the host or account. These post-compromise actions are assumed to either increase attacker access to network resources (which also have no direct corresponding operational consequences) or manipulate process elements such that the process supported by the network-dependent system fails.

To this end, we model the dynamics of the computer network attack, the process that is executed by the system of interest, and the coupling of dynamics in the information and material domains in order to permit direct risk assessment via coverability analysis. This section reviews the basic principles of Petri net structure and mechanics. Interested readers are referred to [1] for a more thorough discussion