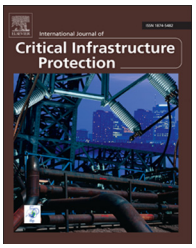
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



A computational asset vulnerability model for the strategic protection of the critical infrastructure

*Richard White**, Terrance Boult, Edward Chow*

Department of Computer Science, University of Colorado at Colorado Springs, 1420 Austin Bluffs Parkway, P.O. Box 7150, Colorado Springs, Colorado 80933-7150, USA

ARTICLE INFO

Article history:
Received 8 January 2014
Accepted 20 June 2014
Available online 10 July 2014

Keywords:
Critical infrastructure
Strategic protection
Attack modeling and simulation
Evaluation measures
Decision support

ABSTRACT

A 2010 study by the National Research Council determined that the U.S. Department of Homeland Security (DHS) lacks adequate risk measures to guide strategic investment decisions for protecting the critical infrastructure. Current threat-driven approaches are hampered by a dearth of historical data that could support robust statistical analysis. This paper presents an asset vulnerability model (AVM) that is designed to address the problem and to provide a strategic risk measure. The AVM risk formulation is predicated on Θ, the probability of failure of an attacker, based on earlier work in game theory. Working within the DHS Risk Management Framework, AVM supports baseline analysis, cost–benefit analysis and the development of decision support tools that convey current risk levels, evaluate alternative protection measures, demonstrate risk reduction across multiple assets, and measure and track improvements over time. Moreover, AVM supports a computational approach for evaluating alternative risk reduction strategies. Seven strategies are examined using AVM: least cost, least protected, region protection, sector protection, highest protective gain, highest consequence and random protection. Experimental results indicate that the highest consequence investment strategy achieves the best protection over time. This paper also summarizes AVM research and demonstrates how it can help guide the strategic protection of the critical infrastructure.

© 2014 Elsevier B.V. All rights reserved.

1. Introduction

The attacks of September 11, 2001, exposed the vulnerability of the critical infrastructure to asymmetric domestic attacks. The 2002 Homeland Security Act made critical infrastructure protection a core mission of the Department of Homeland Security (DHS). Today, this mission is guided by the 2013 National Infrastructure Protection Plan [3] under which DHS works with states and industry within its five-step Risk Management Framework to systematically identify, prioritize and buy-down risk through the purchase of protective improvements using the Homeland Security Grant Program. The DHS Risk Management Framework is predicated on a risk formulation that assesses risk as a function of threat, vulnerability and consequence [3]. A 2010 review of this formulation by the National Research Council of the National Academies [14] found it "seriously deficient and in need of a major revision." Without a viable risk measure, it is not possible to assess the current protective status, evaluate proposed protective improvements and account for protective investments.

The National Research Council report [14] cites 10 challenges to developing a viable measure for guiding strategic investment decisions. First among them is the difficulty in predicting attacks. The DHS risk formulation applies a threat-driven approach

*Corresponding author.
E-mail address: rwhite3572@gmail.com (R. White).

http://dx.doi.org/10.1016/j.ijcip.2014.06.002
1874-5482/© 2014 Elsevier B.V. All rights reserved.

supported by decades of experience in safety and reliability engineering that uses logic trees, influence diagrams, causal loop diagrams and other such methods to model human-initiated events [4]. According to McGill [11], "threat-driven approaches are appropriate for studying initiating events that are well understood and whose rate of occurrence can be reliably predicted from historical data; however, they ultimately fail to consider emerging or unrecognized threats devised by an innovative adversary." In the insurance community and the financial sector, risk assessments benefit from rich, voluminous data sets that can be mined for historical behavior patterns. While several governmental and non-governmental databases maintain terrorism data, the databases are not particularly robust [10]; moreover, access to some of the databases is restricted. Not surprisingly, the National Research Council report [14] concludes that "it will rarely be possible to develop statistically valid estimates of attack frequencies (threat) or success probabilities (vulnerability) based on historical data."

2. Related work

By one estimate there are more than 250 proposed risk assessment methodologies for the critical infrastructure [8]. Drawing on two separate surveys [6,15], we were able to identify 41 risk models. Of these 41 risk models, the 22 models listed in Table 1 offer sufficient information to draw some inferences. Of the 22 models listed, 54% (twelve models) employ a threat-driven risk approach, 32% (seven models) use an asset-driven approach and 14% (three models) are unspecified. Note that T&R in Table 1 stands for transparent and repeatable, ADA stands for asset-driven approach, CS stands for comprehensive scope and NI stands for national impact. Moreover, Y, N and U stand for yes, no and unknown, respectively.

Unlike threat-driven risk methodologies, an asset-driven approach estimates the consequences and probability of adversary success for an exhaustive set of plausible initiating events without regard to their probability of occurrence [11]. The main criticism of the asset-driven approach is that it is an "impact analysis," not a "risk analysis" [6]. Since it does not take into account the probability of occurrence, the asset-driven approach is deemed to be less efficient at directing resources where they are most needed (e.g., to assets that are the most likely to be attacked).

However, this argument appears to overlook the practical application of statistical analysis. Even with a robust data set, as in the case of natural phenomena, forecasters still cannot predict with certitude where or when a natural disaster will strike. The primary benefit of statistical analysis, at least with regard to natural hazards, is in localizing their effects. Thus, for example, while earthquakes are a national phenomenon, California justifiably bears the cost of more stringent seismic standards compared with Connecticut. Localization can be similarly applied to the critical infrastructure, albeit with a reduced level of statistical analysis. Homeland Security Presidential Directive #7 [17] specifies the protection of assets "whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to the use of a weapon of mass destruction… [or] have a debilitating effect on security and economic well-being." Of the 16 infrastructure sectors currently categorized by the federal government [18], only the nine sectors listed in Table 2 may be targeted to precipitate mass or debilitating effects. Excluded from the list are commercial facilities, communications, critical manufacturing, defense industrial base, emergency services, government facilities, and healthcare and public health; by themselves, these sectors cannot be subverted to create mass effects. On the other hand, it was the subversion of the transportation sector that precipitated the devastation caused by the 9/11 terrorist attacks.

In addition to the difficulty of making reliable threat predictions, the National Research Council [14] cautioned against risk formulations that are either too simple or too complex. The problem with developing high fidelity risk models is the same lack of historical data that troubles threat estimation. In the absence of hard data, assumptions must be made; but the more complex the model, the more the assumptions that must be made, which compounds the potential errors. The middle ground, recommended by the National Research Council, is to develop risk models that are "documented, transparent and repeatable."

For the purpose of guiding strategic decisions, risk formulation must also be comprehensive in scope. Indeed,

Table 1 – Critical infrastructure risk assessment models.

Method	ADA	T&R	CS	NI
BIRR [6]	N	Y	N	Y
BMI [6]	N	U	U	U
CAPRA [11]	N	N	N	N
CARVER2 [6,15]	Y	Y	N	Y
CIMS [6,15]	U	Y	N	U
CIPDSS [6,15]	N	U	N	Y
CIPMA [6,15]	Y	U	N	U
CommAspen [6,15]	Y	N	N	U
COUNTERACT [6]	N	U	U	U
DECRIS [6]	N	Y	N	U
EURACOM [6]	U	U	N	U
FAIT [6,15]	Y	U	N	U
MDM [6]	U	N	U	U
MIN [6,15]	Y	N	N	U
N-ABLE [6,15]	Y	N	U	U
NEMO [6,15]	Y	U	U	U
NSRAM [6,15]	N	U	U	U
RAMCAP-Plus [6]	N	Y	U	U
RMCIS [6]	N	N/U	N	U
DHS RMF [3]	N	N	N	N
RVA [6]	N	U	N	U
SRAM [6]	N	N	U	U

Table 2 – Nine critical infrastructure sectors.

ID	Infrastructure sector
1	Chemical Plants
2	Dams
3	Energy
4	Financial Services
5	Food and Agriculture
6	Information Networks
7	Nuclear Reactors, Materials and Waste
8	Transportation Systems
9	Water and Wastewater Systems

Download English Version:

https://daneshyari.com/en/article/275194

Download Persian Version:

https://daneshyari.com/article/275194

Daneshyari.com