Proposal for the Development of Models of Cyber Security with Application to the Electric Grid

Project Description

Dr. Norman Schneidewind
IEEE Congressional Fellow, US Senate, 2005
Fellow of the IEEE, Naval Postgraduate School

Introduction

We are interested in developing concepts about models of cyber security to serve as an inspiration for researchers to advance the technology of models for counteracting cyber threats; for practitioners to use as a guide for responding to cyber terror; for university students to use in preparing for careers in cyber security; and as a contribution to society as a whole by reducing the threat of cyber terror. We are motivated to develop model concepts, and the models that flow from the concepts, because of the severity of the cyber security problem, and the havoc that cyber attacks are wrecking on the world's information infrastructure. In addition, since a major problem in cyber security is the inability to predict risk associated with a given type of attack, our proposed models include an approximation of risk prediction as a function of probability of attack, vulnerabilities, and the consequences of the specified type of attack.

We expect this research to have cross discipline application in the fields of computer science, systems engineering, electrical engineering, and operations research. For example, the models we have developed, as applied to the electric grid, involve knowledge of electrical engineering and operations research for model building. Also, we anticipate that by doing a detailed analysis of the cyber threat to the electric grid, and by sharing the research results with other researchers and grid operators, a better *understanding* of the cyber threat problem will be achieved.

We propose to tackle this problem by developing fundamental concepts in the realm of cyber threat predictive modeling. Furthermore we propose to map our cyber security models to the electric grid environment. We have already done considerable work in developing the concepts and models, as the detailed examples will attest. In addition, we plan to identify and collect cyber security data from electric grid operators, such as the data shown in Table 1 that would be used in the process.

Table 1. Electric Grid Cyber Security Data Types

Vulnerability	**Risk**	**Type of Attack**	**Severity**	**Duration of Attack**	**Consequence**	**Counter-measure**
unprotected voltage regulation	loss of customers	disrupt voltage	High	1 hour	loss of power to customers	recovery circuits

Research Plan

The research to date is comprised of the conceptualization and experimentation with several models, with application to the electric grid. The key facets of our plan are the following:

- Model Elements
  - Objects
  - Events
  - States
  - Probabilities

- Model Properties
  - Cyber Attacks
  - Vulnerabilities
  - Risks
  - Uncertainty in Model Predictions to Avoid Attacks
  - Power transmission Routing to Avoid Attack

A major effort in future research would be to integrate the above facets of model building into a suite of models that could aid cyber security officials in preventing, mitigating, and recovering from attacks.

Need for the Proposed Research

The need for this research is exemplified by the following [MIL05]:

The number, speed, and sophistication of network attacks continue to grow; naturally, this dynamic, yet escalating, threat environment requires a comprehensive approach to security that also includes vulnerability and risk analyses. Many vulnerability assessments are just results of a checklist's completion; they offer no assurance that the list is comprehensive.

Supervisory, control, and data acquisition (SCADA) systems, with various communication links for redundancy and control-center management software, perform the system monitoring between field electric grid operations and control centers. Communication links can traverse the public Internet; thus, the threat space is literally the world. Safety considerations have encouraged the use of remote control and management, and a growing number of companies now control their SCADA systems from offsite.

One of a critical infrastructure's most vulnerable aspects is network access to its SCADA systems. To understand a dynamic network architecture, we need tools, such as the model proposed in this research, that facilitate *knowledge* of and *understanding* of the cyber threat.

[MIL05] ANN MILLER, University of Missouri, "Trends in Process Control Systems Security", IEEE SECURITY & PRIVACY, SEPTEMBER/OCTOBER 2005. pp. 57-60.