Automated Decision Support System (DSS) to Supplement the Quality of Service and Cyber Security of an Information System

1.0 Innovative Claims

NBS Enterprise (NBS) has developed a decision support system (DSS) that prioritizes detection types, reflects all aspects of operations, assists with graceful degradation and control, and provides a global view of threat impacts and information system performance in near real-time. Current processes and technology hinder manager and staff ability to manage large-scale information technology (IT) systems and to develop and execute courses of action in response to cyber security conditions. Extensive data and variables must be factored into a decision process. Time lines, mission characteristics and command, control, and communications (C3) performance might not be well defined. Labor intensive processes, in many cases, require several person hours to develop a course of action (COA). A nonlinear, asynchronous solution space, under current conditions, produces inaccurate stovepipe results. In addition, a response to ongoing events not only relies on organic detections within an IT system purview, but also actionable intelligence from external sources. However, a flood of collected data has seriously degraded the timely assessments of cyber information and the identification of high-value quanta of information. An obvious, but difficult solution is to automate as much of an evaluation process as possible while still retaining the expertise of human judgment. Steady improvements in data access rates and formatting have been realized with data warehouse technology. Data mining has similarly enhanced decision support systems. Still lacking is the capability to effectively fuse diverse sources of information, to incorporate the essence of asynchronous events, and to propagate the belief of evidence in the context of time-dependent scenarios. The primary challenges of developing computational models for DSS are 1) identification and prioritization of intrusion types, 2) the structuring of detections for input to a system context model and an integration with other modeling variables, and 3) the representation of context models that will accept all relevant data inputs and provide quantitative mission information.

2.0 Benefits

Measurement tools for cyber security are readily available for the continual monitoring of system performance. But in addition, decision makers and their staff require an encompassing decision support environment to effectively manage large-scale information systems and to develop and execute courses of action in response to deleterious events.

The proposed prototype produces a response to the results of measurements and the prioritization of those measurements. Measures of intruder performance (MOP) are defined and if they portray danger to systems operations, countermeasures are instigated immediately. Thus, a means is

12 ½ South King Street, Leesburg, VA 20175
Phone: 703-258-1616

available to compute MOP and to prioritize detections of system intrusion. The foundation of countermeasures implementation is a continual source of measurements and the processing of their importance within a systems context..

3.0 Approach

3.1 Process Model and Superior Performance

The overall thrust of a decision making tool, which assesses the combined effects of operational components and measurements, is to transition data to performance models. Thereafter, the models are exercised to produce an analysis and a quantification of probabilistic outcomes. Fundamentally, descriptions of system components, risk assessment results and asynchronous measurements are emplaced in a structured database. The database objects are mapped to sets of metadata that produces associations of measured events, their inputs and outputs (I/O), and times to respond to the events. Associations are further mapped to a context model that is exercised to provide courses of action.

3.2 Mapping of Measurements and Risk Assessment Results

Metadata provides rules for the association of timed or probabilistic events and their I/O, an automated mapping is visualized where first unstructured data are directed to an extraction tool suite. The extractor produces structured databases, which are transitioned by metadata to a definition of associations. The associations are further transitioned and positioned within a system context model that feeds analytical equations or a simulation of an IT system domain. By exercising the model, performance statistics are derived that encapsulate actions initiated by an asynchronous situation, as well as the context model, which represents an entire system of interest.

3.3 General Purpose Problem Solver

The backbone of the decision support system (DSS) and a system representation is a general purpose problem solver (GPPS) that employs one network representation to permit performance computations and optimization. The primary representation of the existing tool suite is a rule-based encapsulation of a network or any complex system. Rules are further appended with values for mean processing times of individual nodes, as well as distribution functions. Time related statistics are generated the same as any simulation of a network. But, in addition to performance statistics, optimization is accomplished using the same rule-based representation. Optimization is always accomplished in the context of a systems model. Only one measure of system effectiveness can be optimized while all system variables are balanced to best achieve an objective. The variables represent competing measures of performance such as minimum risk of intrusion by a hacker versus system response time. Further, impact, sensitivity and what if analyses are achievable for any queries submitted by managers and their staff. In addition to a

12 ½ South King Street, Leesburg, VA 20175
Phone: 703-258-1616

network model, a myriad of algorithms orchestrates the optimization and performance analysis procedures.

3.4 Concept of Operations

A concept of operations for an automated decision support system is outlined in Table 1. A context model is prepared for a domain. Many facets might be included in the context model such as IT assets and data flow within a network. Given that a new set of measurements is obtained, which describe detections of possible network intrusions, the ontology assists with a mapping to the context model. The context model is expanded to include the additional information and is exercised to display the impact of the change.
:

Table 1
Concept of Operations

1) A risk assessment is established for an IT enterprise.
2) Descriptions of risk are prepared for system components (locations of vulnerability, priorities, down times given a successful penetration, countermeasures).
3) Metrics are defined and measurements are applied to vulnerable areas.,
4) An analytical context model is defined to represent all IT system components and risk assessment factors,
5) Impact, sensitivity and what-if analysis are conducted with the context model to provide analytical forecasting,
6) Measurements of non catastrophic events, failures and penetrations are recorded,
7) Relevant asynchronous data are transitioned to a structured database.
8) Metadata assist with the derivation of new associations which are mapped to the context model,
9) The expanded context model is exercised to provide performance statistics (response times, impediments, uncertainties),
10) Based upon performance statistics, countermeasures are recommended/ course of action,
11) Measurements are processed continually to derive new courses of action.

Operations for the above scenario are accomplished within minutes as opposed to several hours of think time. Optimization functions are available for all possible violation types: physical, personnel, software, hardware, network, and data. The products of the automated decision support system contribute to reporting, the definition of tests, revisions to risk assessment, and a view of total system operations. Vulnerabilities, in and by themselves, in many cases are misconstrued, whereas a global representation of vulnerability interactions clearly identifies the most critical regions of system compromises. Further, countermeasures to potential or actual threats are displayed automatically for view by IT managers.

12 ½ South King Street, Leesburg, VA 20175
Phone: 703-258-1616

3.5 Metrics
3.5.1 Selection of Metrics

The selection of metrics for performance measures is an ongoing and volatile pursuit. First, metrics differ for various levels of personnel. Management might be interested in measures of costs and downtime, while technicians are more concerned with measures such as failures per unit time. Regardless, measurements and recordings of results are hierarchical. The metrics must correlate with the hierarchy. Initially, measurements are made for a high-level phenomenon such as mean number of penetrations per unit time. Thereafter, granularity ensues: penetrations of type A, penetrations of type B, etc. Special categories of a penetration type might also be necessary.

3.5.2 Data Recordings

Measurements are recorded electronically as they are obtained in the format specified by an enterprise. The time, place and type of measurement are stored in a relational database so that reports are generated on a periodic basis. Further, dashboard displays are available for personnel observations. SQL queries are made so that the nature of measurement results is readily available. Measurements of effectiveness are derived from measurements and metrics so that system and component performance is defined for any point in time.

3.6 Analytical Forecasting and Enhancements of Operational Procedures

A measures and metrics leader continually reviews all measurements, decision support results and feedback from system operators to provide analytical forecasting and recommendations for new measurement applications.

3.7 Prioritization of Measurements

From the aspect of intruder operations, the NBS algorithms are able to accept descriptions of viral behavior and the potential to cause damage to specific nodes within a network. Qualitative descriptions are transitioned to quantitative representations which are exercised by the algorithmic tool suite. The results probabilistically bound potential outcomes of intrusions. A contributor to countermeasures is the development of intruder measures of performance so that a prioritization of detection types is possible. Time critical courses of action are formulated in response to serious cases, while less significant detections are addressed at a more leisurely pace.

3.8 Graceful Degradation

The quantification of network nodal interactions begins with the development of a model from descriptions of processing, connectivity of nodes and communications. Examples of selected parameters include definitions of all devices, locations of nodes, protocols, concepts of operation and physical phenomena of a threat. Dynamic changes are imposed in an asynchronous manner

12 ½ South King Street, Leesburg, VA 20175
Phone: 703-258-1616

upon network components. Changes in a model follow directly from changes in an IT system. If a node is compromised, it is deleted from a network representation. A new performance is computed using the reduced model. Thus, a network's response to intrusions is quantified and optimization components of the tool suite provide revised operations.

3.9 Modeling Results and Prioritization

Once a model is represented, it is exercised to provide network performance results. Thereafter, an asynchronous event is injected into the model. Table 1 relates modeling results to the information required for detection prioritization.

Table 1

Modeling Statistic	Significance of the Statistic
1) Throughput at a node generated by an insert	Probability that the impact of an insert reaches a particular node
2) Timing	Time required for an insert to reach a node
3) Secondary throughput	Throughput generated by a compromised node and sent to other network nodes
4) Mean time to repair	Time to repair a compromised node

The value of a function within a network is established in two ways: 1) value established by a heuristic judgment, and 2) by modeling results. Given functional failure, the reduced performance of a network is quantified. Nodal downtime for a function is indicated by the mean time to repair. To further instantiate the prioritization, information through risk analysis is made available. The information comprises estimates of which functions might be compromised given an intrusion of type X. A measure of performance (MOP) for prioritization can require combinations of more than one statistic. Interest might exist for multiple MOP such as mean time to repair, propagation time of a virus through a network or reduced system performance. An NBS paradigm exists which combines two or more MOP into a single measure of effectiveness (MOE).

12 ½ South King Street, Leesburg, VA 20175
Phone: 703-258-1616

4.0 Section D: Measures of Success

Measures of project success are 1) capability to prioritize intrusion/ detection types, 2) capability of a context model for an information system that assists with graceful degradation and the control of all assets, and 3) development measures of effectiveness that relate to system requirements and needs.

5.0 Section E: Project Phases

A two-Phase project is proposed:
Phase I: Six months for engineering development.
Phase II: Prototyping.Six months for fabrication, six months for tests and evaluation.

12 ½ South King Street, Leesburg, VA 20175
Phone: 703-258-1616