A major purpose of the Technical Information Center is to provide the broadest dissemination possible of information contained in DOE's Research and Development Reports to business, industry, the academic community, and federal, state and local governments.

Although a small portion of this report is not reproducible, it is being made available to expedite the availability of information on the research discussed herein.
TITLE  MODELING RISK ASSESSMENT APPLICATIONS WITH LAVA

AUTHOR(S) Suzanne T. Smith

SUBMITTED TO Fifth Annual Symposium and Technical Displays on Physical and Electronic Security, Philadelphia, August 15-17, 1989

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED
Modeling risk assessment applications with LAVA

Suzanne T. Smith

Los Alamos National Laboratory, Safeguards Systems Group
P. O. Box 1663, MS-E541, Los Alamos, New Mexico 87544

ABSTRACT

LAVA (the Los Alamos Vulnerability/Risk Assessment system) is a three-part systematic approach to vulnerability and risk assessment that can be used to model a variety of application systems such as physical or operational security systems, communications security systems, information security systems, and others. Using LAVA, we build knowledge-based expert systems to assess risks in application systems comprising a subject system and a safeguards system. The methodology provides a framework for creating a variety of applications systems upon which the general software engine operates. All application-specific information is supplied as data and requires no code changes in the general software engine. This paper discusses the ingredients for creating a LAVA application system.

INTRODUCTION

LAVA (the Los Alamos Vulnerability/Risk Assessment system) is a three-part systematic approach to vulnerability and risk assessment that can be used to model a variety of application systems. The details of the methodology have been published extensively.

The first part of LAVA is the mathematical methodology based on such disciplines as hierarchical system theory, fuzzy systems theory, decision theory, utility theory, and knowledge-based expert system theory. The second part is the general software engine, written for a large class of personal computers that implements the mathematical risk model. The third part is the application data sets written for a specific application system. The methodology provides a framework for creating applications for the software engine to operate upon; all application-specific information is data. Using LAVA, we build knowledge-based expert systems to assess risks in application systems comprising a subject system and a safeguards system. The subject system model is sets of threats, assets, and undesirable outcomes. The safeguards system model is sets of safeguards functions for protecting the assets from the threats by preventing or ameliorating the undesirable outcomes; sets of safeguards subfunctions whose performance determine whether the function is adequate and complete; and sets of issues, appearing as interactive questionnaires, whose measures (in both monetary and linguistic terms) define both the weaknesses in the safeguards system and the potential costs of undesirable outcomes. The user need have no knowledge of formal risk assessment techniques—all the technical expertise and specialized knowledge are built into the software engine and the application system itself.

LAVA applications include our popular computer and information security application (LAVA/CIS) and applications for embedded systems, survivability systems, transborder data flow systems, property control systems, and others. Currently under development are LAVA application systems for operations security, weapons system security, and nuclear safeguards systems. LAVA application systems have been in use by Federal government agencies since 1984.

PRELIMINARY MODEL DEVELOPMENT TASKS

The first step in modeling an application system for LAVA is to define the scope of the problem. This means limiting the problem to a manageable size by restricting its universe to something considerably less than the entire Universe. Included in this preliminary step is deciding what the goals of the assessment process are, who will perform the assessments with the LAVA software, and what form the automatically generated reports will take and for whom they will be written.

DEFINING THE THREAT, ASSET, AND OUTCOME SPACES

The next step is to define categories of assets (those things of value to the organization that should be protected), threats (the active malevolent forces acting on the system), and potential bad outcomes (those events that should be prevented or ameliorated).
For example, the computer and information security application of LAVA, LAVADIS, models four asset categories: 1) an organization, its physical plant, personnel, and support equipment; 2) its information in machine-interpretable forms; 3) its information in human-interpretable forms; and 4) its computers and related hardware. Most applications will use three threat categories: 1) threats of nature, such as fire, flood, and so on; 2) humans on site, including the authorized insider; and 3) humans off site. Categories of undesirable outcomes might include such things as 1) unauthorized access or use; 2) unauthorized disclosure; 3) modification or tampering; 4) damage or destruction; 5) denial of use; 6) theft or abuse; and so forth.

An outcome possibility matrix is created by considering the various ways that the threats can interact with the assets to produce a specific outcome. Here, depending on the degree of granularity required by the application, each possible [threat, asset, outcome] triplet can be assigned a membership function value commensurate with the required level of detail. For most cases, an ordinary set membership function definition will suffice: this has two allowable values, zero for no membership (the outcome is impossible for the specific [threat, asset] pair) and unity for complete membership. If a greater level of detail is required, values lying between zero and unity can be calculated.

**The Safeguards System Model**

The next step is to relate the threat set and the asset set hierarchically to decompose the problem for systematic analysis. We consider each threat-asset hierarchy (or interaction) separately in postulating how each threat could harm each asset and how each of the outcomes could happen. We model an ideal safeguards system in terms of the operative functions that could prevent the outcomes from happening. Then, for each safeguards function on each threat-asset hierarchy, we determine the safeguards subfunctions that assure the completeness of that safeguards function.

The specific safeguards (or countermeasures or protective mechanisms) are modeled as a weighted interactive questionnaire. This is where the facts, knowledge, intuition, and general expertise come into play. We consider all the ways that a threat can attack an asset, and we put forth an optimal set of individual countermeasures; these are called safeguards elements. We then consider what is required for each element and the safeguards elements, the elements assure the effectiveness of the safeguards subfunctions, and the subfunctions determine the completeness of the safeguards functions. Each safeguards element is related to one or more of the safeguards subfunctions; these relationships are associated with the overall weighting scheme.

**The Dynamic Threat Model**

The next step is to develop a set of questions to assess the strength of the dynamic, or current, threat. The threat strength is calculated in terms of the attractiveness of the asset to the threat agent and the threat agent's motivation, capability, and opportunity factors with respect to each [threat, asset, safeguards function] triplet. **Asset attractiveness** is the attractiveness of the asset to the threat agent and the threat agent's motivation, capability, and opportunity factors with respect to each [threat, asset, safeguards function] triplet. **Motivation** is a measure both of how much effort or what part of his resources the threat agent is willing to expend on an attack and of how dedicated he is to carrying out the attack. **Capability** is a measure of how much knowledge, information, funds, resources, expertise, equipment, skills, armament, and/or force the threat agent has at his disposal. **Opportunity** is a measure of the threat agent's ability to achieve an enabling proximity—how easy it is for him physically to reach the object of the attack, how easy it is for him to travel undetected, how easy it is for him to dial into a network, and so forth; opportunity is separate and different from potential system vulnerabilities.

This step produces another questionnaire to elicit the necessary information. The questionnaire can be of a general nature, or, if necessary, it can relate to specific intelligence issues for those who have both access and need.

**Outcome Severity**

Outcomes may occur in varying degrees of severity. It is valid to assume the worst, which gives a conservative estimate of overall risk. It is equally valid to assume the presence of a variety of mitigating factors and estimate how much these factors might contribute to reducing outcome
severities. If the latter course is chosen, this step produces another questionnaire that examines the mitigating factors for each threat, asset, safeguards function, outcome, and nonmonetary triplet.

THE IMPACT MODEL

The object of this model is to identify the kinds of costs, both monetary and nonmonetary, that are important to the organization in terms of how they arise. The monetary costs include such things as direct losses from fraud, theft, or embezzlement; costs of investigation and follow-up; costs associated with repair and replacement; litigation costs; costs of personnel actions; costs associated with training replacement personnel; costs associated with training personnel on new equipment or procedures; loss of potential funding; costs of interim operation; costs of business termination; and so forth. Nonmonetary costs include such things as embarrassment to the organization, reputation damage, loss of employee morale, loss of public trust, loss of strategic posture, and other similar things.

Once again, the product of this step is another questionnaire that elicits information about these costs for each threat, asset, outcome triplet.

LOSS EXPOSURE

LAVA models risk, or the exposure to loss faced by an organization, as a function of weaknesses in the safeguards system, the value of the assets to the organization, the strength of the threats to these assets (which includes the attractiveness of the assets to the threat agents), the severity of the outcome, and the monetary and nonmonetary impacts. LAVA expresses loss exposure as a pair of values (monetary and nonmonetary) for each threat, asset, outcome, safeguards function, and nonmonetary triplet. Loss exposure can be aggregated to whatever level is desired, but we think that the less aggregation, averaging, and annualizing that is done, the more decision-making information the organization will have at its fingertips.

REPORT GENERATOR DESIGN

The final task in setting up a LAVA application model is a two-part one: deciding what specific information the organization wants to see and designing the format in which to display that information. LAVA comes with built-in report generators, but it is not necessary to use them; the report generators can be built to the specifications of the users by the users (with a little help from us).

CONCLUSIONS

LAVA is an original approach to risk management developed at Los Alamos National Laboratory. LAVA provides a systematic framework for evaluating vulnerabilities and risks in complex safeguards and security systems. Modular in structure, it is designed for implementation on a personal computer and for execution in a team environment.

The subject systems to which LAVA can be applied are usually massive, complicated systems characterized by large bodies of imprecise data (very little "hard" information and enormous quantities of "soft" and subjective information). Indeterminate events (events that may or may not have happened or, if they happened, may not have been detected), and a large human component. The outcomes resulting from threats exploiting system vulnerabilities are often of a catastrophic nature, defying quantification by ordinary means.

For a subject system, LAVA evaluates safeguards system vulnerabilities, analyzes the consequences of vulnerability exploitation, and calculates the set of loss exposures resulting from the consequence set. The methodology gives both qualitative and quantitative insights into the vulnerabilities in the system of safeguards, yields an accurate picture of the effectiveness of the subject organization's safeguards system, and produces both qualitative and quantitative expressions for loss exposure (risk).

Because of the team environment in which LAVA is executed, there are two additional benefits that accrue above and beyond the accomplishment of vulnerability and risk assessment. First of all, going through the LAVA questionnaires in the team environment raises the overall security consciousness level of the organization and the result of the depth and breadth of the questions. Second, the team discussions of the issues that arise during a LAVA assessment seem to increase overall communications within the organization, on a lasting basis, making the working environment more pleasant, more cordial, and more effective because of the improved interpersonal relationships that were forged during the LAVA assessment process.
REFERENCES


