LA-UR -86-2282

CONF-860654--21

MASTER

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36.

LA-UR--86-2282

RECEIVED b DE86 012420

TITLE: LAVA - A CONCEPTUAL FRAMEWORK FOR AUTOMATED RISK ASSESSMENT

AUTHOR(S): S. T. Smith, D. C. Brown, T. H. Erkkila, P. L. FitzGerald, J. J. Lim, L. Massagli, J. R. Phillips, and R. M. Tisinger

SUBMITTED TO: Proceedings of the 27th Annual Meeting of the Institute of Nuclear Materials Management

DISCLAIMER

Los Alamos Los Alamos National Laboratory
Los Alamos, New Mexico 87545

FORM NO 836 R4
ST NO 2629 5/81

LAVA - A CONCEPTUAL FRAMEWORK FOR AUTOMATED RISK ASSESSMENT*

S. T. Smith, D. C. Brown,** T. H. Erkkila, P. D. FitzGerald,**
J. J. Lim, L. Massagli, J. R. Phillips, and R. M. Tisinger

Los Alamos National Laboratory

Los Alamos, NM 87545

ABSTRACT

At the Los Alamos National Laboratory we are developing the framework for generating knowledge-based systems that perform automated risk analyses on an organization's assets. An organization's assets can be subdivided into tangible and intangible assets. Tangible assets include facilities, materiel, personnel, and time, while intangible assets include such factors as reputation, employee morale, and technical knowledge. The potential loss exposure of an asset is dependent upon the threats (both static and dynamic), the vulnerabilities in the mechanisms protecting the assets from the threats, and the consequences of the threats successfully exploiting the protective systems vulnerabilities. The methodology is based upon decision analysis, fuzzy set theory, natural-language processing, and event-tree structures. The Los Alamos Vulnerability and Risk Assessment (LAVA) methodology has been applied to computer security. LAVA is modeled using an interactive questionnaire in natural language and is fully automated on a personal computer. The program generates both summary reports for use by both management personnel and detailed reports for use by operations staff. LAVA has been in use by the Nuclear Regulatory Commission and the National Bureau of Standards for nearly two years and is presently under evaluation by other governmental agencies.

INTRODUCTION

The goals and objectives of a risk management program are defined by both external and internal requirements. External requirements arise from guidelines or rules issued by governmental agencies and legal responsibilities of the organization, as well as constraints placed upon the organization by society. Internal requirements arise from consideration of such factors as organizational vitality, profitability, and moral responsibility. Both sets of requirements must be considered during the formulation of an organization's risk management program.

There are three basic components to an effective risk management program: (1) identification of the assets, (2) identification of the potential threats, and (3) reduction of potential loss exposure by defining the set of safeguards functions (mechanisms, policies, and procedures) that safeguard the asset from the threat. By using this approach, we eliminate the necessity for defining elaborate scenarios (where we are not assured that the scenario set is complete), eliminate the requirement of estimating event probabilities from a set of inadequate or incomplete data, and measure the consequences more accurately by using both monetary and nonmonetary (or linguistic) descriptors.[1-5]

Identification of Assets

The assets must be defined precisely before any risk management program can be established. Oftentimes an organization's assets are vaguely defined as "those things that make up" the organization. This type of definition is not satisfactory for risk management. Generally, the assets can be subdivided into two categories: tangible assets and intangible assets. Tangible assets include facilities, materiel, personnel, and time. Intangible assets are more difficult to define precisely but can be as or more important than the tangible assets. Intangible assets include organizational reputation, employee motivation and morale, and the technological basis of an organization. An asset may be, at the same time, both tangible and intangible. An employee is a tangible asset, while his technical knowledge and motivation are intangible assets.

Identification of Potential Threats

To define the potential for loss exposure to an organization and its assets, a threat analysis must first determine the existence of potential threats taking into account possible threat agents and their potential targets. The threat component consists of two parts: the static (or relatively constant background) threat, and the dynamic (or changing) threat. The threat component measures the relative strengths of identifiable threat agents in terms of motivation, opportunity, and capability against the safeguards functions (the functional objectives of the controls and mechanisms that protect the assets from the threats).

*This work was supported by the Department of Energy, Office of Safeguards and Security.

**Employed by the U.S. Government.

Motivation is a measure of how many of his resources a threat agent is willing to expend in an attack, or how dedicated he is to carrying out the attack. Opportunity is a measure of ease with which a threat agent can physically reach the asset (opportunity is separate and different from potential site vulnerabilities). Capability is a measure of how much knowledge, information, expertise, and/or resources the threat agent has at his disposal.

The threat component that acts to exploit the vulnerabilities of a safeguards function is the sum of both the static (or constant threat) and the dynamic threat. If we assume the static threat is always present (in the background), we can assign the value of unity to the static threat's membership function in the fuzzy set of "all threats operating on the system." A value of unity implies complete or total membership in the fuzzy set. The dynamic threat changes with time, so its membership in the same fuzzy set will vary between zero (no membership) and unity (complete membership), depending upon the circumstances at the time of analysis.

Reduction of Loss Exposure

There are three components involved with the reduction of loss exposure: vulnerability assessment, consequence analysis, and cost/benefit analysis. According to DOE Order 1000.3 (April 28, 1986), a vulnerability assessment is defined as a review of the susceptibility of an organization "to loss or unauthorized use of resources, errors in reports and information, illegal or unethical acts."[6]

The previous two sections discussed the factors necessary to define the assets and to quantify the threat components. Once these two processes are complete, the threat and assets must be combined into threat/asset pairs. For each threat/asset pair there are certain safeguards functions that can be employed to protect the asset. These safeguards functions are based upon an idealized system that assumes if all the safeguards functions are in place, the asset has zero vulnerability. Each of the safeguards functions may be composed of several subfunctions, which are composed of elements that are composed of attributes. The adequacy and completeness of the safeguards function or subfunction must be determined to evaluate the effectiveness of the function and, subsequently, the vulnerability of the asset to the specific threat. The adequacy of a function is measured by determining the presence of required elements. The completeness is measured by assessing the presence of required attributes.

To illustrate this process, consider the case where an asset is contained in a facility and the safeguards function is perimeter control. The adequacy of the perimeter control function can be measured by determining if there are fences surrounding the facility or if there are intrusion alarms. The completeness of the fences is determined by evaluating if there are multiple entrances, if the fence is of minimum height, and if the fence is constructed of concrete or chain-link fencing. The completeness of the intrusion alarms is determined by evaluating if intrusion alarms are on all entrances, if the alarms transmit to a central station, and if the alarms are recorded for future reference.

By combining the adequacy and completeness factors, one obtains a value for the vulnerability of specific safeguards functions. These relative values can be combined to determine the vulnerability of an asset (or a set of similar assets) to a specific threat agent. Once the set of vulnerabilities has been established, then the consequence analysis is performed to determine the set of possible outcomes and their severities or impacts upon the organization.

The consequence component measures the potential monetary and nonmonetary impact of a successfully exploited vulnerability with respect to the severity of the outcome. The outcome severity metric includes a measure of both the sensitivity and criticality of the object of attack and the effectiveness of controls that might mitigate the outcome severity. Mitigation includes after-the-fact detection mechanisms and both long-term and short-term contingency plans. Consequence impacts are represented in both monetary and nonmonetary terms: the monetary descriptor is used when the consequences can be given in terms of monetary costs (replacement of buildings or equipment), and the nonmonetary descriptor is used when the consequences can be given only in terms of intangible costs (loss of reputation or morale).

Potential for loss exposure of an asset by a threat that exploits the vulnerability of a particular safeguards function is a function of the threat, vulnerability, and consequence:

$$\text{Risk} = f(T, V, C)$$

There must be a threat agent for a vulnerability to exist; therefore, the vulnerability assessment is driven by the threat assessment. Similarly, the consequence analysis is driven by the vulnerability assessment. In evaluating the risk measure when a vulnerability exists in a safeguards function, the measure or degree of risk can be increased by the real threat measure (combining the static and dynamic components) or reduced by the real consequence measure. The risk measure can be reduced to insignificance if the consequences of an attack are themselves insignificant.

Cost/benefit analysis is the last step in the reduction of loss potential. All organizations have limited resources to apply to risk management. Therefore, management must be able to perform "what if" scenarios. What if we built a new perimeter fence? Would that decrease significantly the vulnerability of the facility? Each organization has certain constraints upon the type and amount of resources available; therefore, the optimal solution for each organization is unique.

LOS ALAMOS VULNERABILITY AND RISK ASSESSMENT METHODOLOGY – LAVA

The Los Alamos Vulnerability and Risk Assessment Methodology (LAVA) is a systematic method for assessing vulnerabilities in safeguards systems. We have applied the LAVA methodology to model supply and property systems, control systems for awarding and administrating contracts, international communications and information flow systems,[7] and computer security systems. We have implemented the vulnerability assessment portion for computer security and are presently implementing the consequence analysis portion. The LAVA implementation yields qualitative insights into the vulnerabilities of computer systems to natural hazards and on-site human threat agents. The assessment process is based upon a team approach for the evaluation of the vulnerabilities of established safeguards functions at a facility.

A. Definition of Threat/Asset Pairs

For computer security we have defined four general categories of tangible assets: facility, hardware, software, and documentation. The facility includes the physical structure of the computer facility, adjacent supporting facilities (air-conditioning units, power distribution stations), and personnel. Hardware is restricted to the physical parts of the computer system, like central processing unit, disk drives, printers, and terminals. Software (or machine-readable information) includes both commercially produced software as well as internally produced software and information. Documents (or human-readable information) consist of manuals, printer/plotter output information, and display screens.

We have identified three threat agents for these four categories of assets: natural hazards, on-site human (the agent must be physically present), and off-site human (the agent is not physically present; for example, the agent can access the computer system through dial-up lines). For the unclassified version of LAVA we address only the static component of the natural hazards and the on-site human threat agents. The interaction of these threat agents with the previously defined assets is represented in Fig. 1. The natural hazard threat agent does not distinguish between the assets—it "attacks" all the assets without discrimination. Therefore, the threat/asset pair for natural hazards is the same for all combinations. However, given the case of the on-site human threat agent, there are unique threat/asset pairs that must be considered when the vulnerabilities of the computer facility are evaluated. There is a unique set of safeguards functions that should be in place to protect each of the categories of assets. A few safeguards functions are common to all four categories of assets.

B. Definition of the Safeguards Functions

A unique set of safeguards functions is associated with each threat/asset pair. As discussed in the previous sections, each safeguards function may be composed of several subfunctions. There is an optimal set of safeguards functions to protect a specific asset from a specific threat. The adequacy and completeness of these functions and subfunctions are determined by evaluating the presence or absence of elements and attributes by answering a set of specially designed questions. The responses to these questions measure the degree to which the elements and attributes are complete.

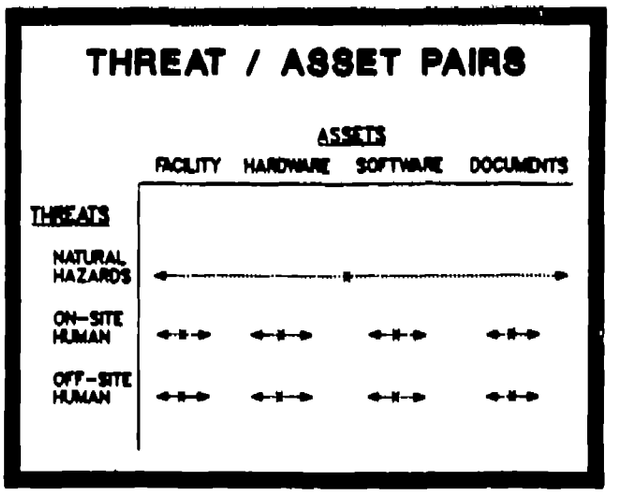

Fig. 1.
Threats from natural hazards are indiscriminate, affecting all assets equally. On-site and off-site human threats can target specific assets or groups of assets.

C. Evaluation of the Vulnerabilities of Safeguards Functions

The evaluation process is based upon a team approach. This approach is vital for arriving at results that are real and interpretable. The quality of the assessment depends upon the quality of the team members. The broader the spectrum of the backgrounds and expertise of the team members, the better (and more accurate) the assessment will be. There are two parts to the team: a core team whose members are present throughout the entire assessment period, and a transient team whose members attend only during those times their expertise is required. The team members should have specialized knowledge about different aspects of the facility and its assets. Desirable backgrounds or expertise for the team members include physical security, technical security, building engineering, software development, communication systems, computer operations, and other areas of expertise.

There are four parts to the assessment process. The first part consists of a review of the computer installation to be assessed. A visit to the facility is completed by the entire assessment team. The components (or assets) are identified, procedures and policies are discussed, and individuals that the assessment team can contact for

further information are identified. Answering the questionnaire is the second part of the assessment. Each question is answered only after a consensus has been reached by the team members. This is the real strength of the team approach. The questionnaire is subdivided into separate modules that can be answered in any order, depending upon the availability of the members of the assessment team. The third part involves the execution of the scoring and report-generating programs. The scoring process relates the vulnerability of each safeguards function to the corresponding threat/ asset pair. The final step of the assessment process is a discussion of the results with the managerial and operational staff. LAVA automatically prepares reports at two levels of detail; one is a summary report that is useful to upper management in identifying areas in which vulnerabilities exist. The second report is sufficiently detailed for use by the operational staff to address specific problems. The total time involved in a typical assessment of a computer facility ranges from 3-5 days. This type of vulnerability assessment has minimal impact upon the operations of a computer facility when compared to other methods of vulnerability assessment that can require weeks or months to complete.

Because the vulnerability assessment process is completely automated on a personal computer, the assessment can be rerun at any time to determine the effectiveness of any corrective actions that may have been implemented. The program offers an objective measurement of the vulnerability of the safeguards functions.

CONCLUSIONS

An automated vulnerability assessment process has been developed and demonstrated for computer security. This methodology can be applied to evaluate the effectiveness of any set of safeguards functions that protect a set of assets from threat agents. The methodology does not require the assignment of probabilities to any event occurring. Therefore, it is applicable to many of the problems of risk management that can not be quantified using previously developed methodologies. This methodology can be applied to assessing the vulnerability of nuclear material accountancy systems to diversion or loss of material.

The specific application of this methodology to computer security has been very favorably received throughout the federal and local governments. Besides being used by the Department of Energy, the Nuclear Regulatory Commission, and the National Bureau of Standards, it is being evaluated by the Department of Defense, federal and state law-enforcement agencies, and the Postal Department as a method for identifying vulnerabilities and for providing guidance on possible improvements.

ACKNOWLEDGMENTS

The development of this methodology would not have been possible without the support and suggestions of our colleagues.

REFERENCES

1. S. T. Smith and J. J. Lim, "LAVA: An Automated Computer Security Vulnerability Assessment Software System (Version 0.9)," Los Alamos National Laboratory document LA-UR-85-4014 (December 1985).

2. S. T. Smith and J. J. Lim, "A Framework for Generating Expert Systems to Perform Computer Security Risk Analysis," Proc. 1st Armed Forces Communications and Electronics Association Symposium, Philadelphia, PA, August 1985.

3. S. T. Smith and J. J. Lim, "Risk Analysis in Computer Systems - An Automated Procedure," Information Age 7(1) (January 1985).

4. S. T. Smith and J. J. Lim, "Assessment of Computer Security Effectiveness for Safe Plant Operation," Proc. ANS 1984 Annual Meeting, New Orleans, LA (June 1984).

5. S. T. Smith, J. R. Phillips, D. C. Brown, and P. D. FitzGerald, "Assessing the Threat Component for LAVA Risk Management Methodology," Proc. of the Ninth DOE Computer Security Conference, Las Vegas, NV, May 6-8, 1986.

6. Department of Energy Order DOE 1000.3 "Internal Control Systems", April 23, 1982; revised as DOE 1000.3a May 3, 1986.

7. S. T. Smith, J. J. Lim, and J. Lobel, "Application of Risk Assessment Methodology to Transborder Data Flow," Proc. TDR Conference on the International Information Economy, Williamsburg, VA (November 1985).