A SECURITY METHODOLOGY FOR COMPUTER NETWORKS

Lyndon G. Pierson and Edward L. Witzke

Lyndon G. Pierson *is a member of technical staff in the Network Systems Department at Sandia National Laboratories in Albuquerque, New Mexico.* ***Edward L. Witzke*** *is a consultant at Sandia National Laboratories and is a staff member of The BDM Corporation in Albuquerque, New Mexico. Mr. Pierson's current areas of interest are the communications services and security of intersite (wide-area) computer networks. He joined the company in 1975 and holds a B.S.E.E. from New Mexico State University and an M.S.E.E. from Stanford University. Mr. Witzke's current areas of interest and research include computer communications and networking and computer security. He has a Bachelor of University Studies (with a concentration in computer science) from the University of New Mexico.*

The world's businesses, industries, and governments are beginning to rely on computer networks for timely transmission of sensitive data between geographically distributed sites. To ensure the security integrity of the entire complex, the networks that bind these distributed facilities must be integral to all security considerations. The methodology described here provides a framework for developing the planning documentation and procedures for network security. It also bounds five security documentation and analysis problems that were previously unbounded. This methodology separates a computer network's "security life" into two phases. The first phase—design, review, and accreditation—deals with system-security planning, implementation, certification, and accreditation for operation. The second—or operational—phase involves processing unusual events that may be of security interest during the operation of a computer network. The various elements, relationships, and decisions for each phase are examined.

Background

In computer security literature, one can find many rule books and theoretical models about computer security, guides for analyzing risk, etc. In this paper, we describe how these components or elements relate and thus form a security methodology (documents and procedures) for computer networks. This general methodology separates the "security life" of a computer network into two phases:

- *Design, review, and accreditation* phase—system security planning, implementation, certification, and accreditation for operation.
- *Operational* phase—the processing of unusual events that may be of security interest during a computer network's operation. A series of

"filters" processes each unusual event to determine if it is associated with a loss or unauthorized activity. Detection and processing of certain kinds of unusual events may cause the update and review of elements in the first phase (design, review, and accreditation).

Design, Review, and Accreditation Phase

In this section, we describe the following major components and their relationships (Figure 1) for the network's design, review, and accreditation phase:

- Definition of protected resources.
- Security policy.
- Statement of threat. A *threat* is an event or method that can potentially cause the theft, destruction, corruption, or denial of either service, information, resources, or materials.
- Protection measures.
- Risk analysis.
- Incident detection mechanisms.
- Security plan.
- Certification, accreditation, recertification, and reaccreditation.

While guidance abounds on certain aspects of computer security[1-5]—such as risk analysis, password protection, basic operating-system security features, certification, and accreditation—their relationships are not always clear.

Before this methodology was developed, the security planner typically addressed the protection measures, incident detection procedures, risk analysis, and system security testing independently. Frequently, this was done without considering the content of the statement of threat. (The statement of threat might not even be formalized!) When a planner develops these important security items independently, he or she faces the difficult task of deciding when each element is adequately addressed. This leads to inconsistent depth of planning, which may manifest itself as holes in the planned network's security.

The central element of the methodology we describe is the statement of threat. An *incident* is an occurrence of a threat that is itemized in the statement of threat. Protection measures are applied to prevent each itemized threat from occurring. System security tests are done to ensure that security measures are effectively implemented to counter each threat itemized. *Risk* is also quantified and analyzed for each threat itemized.

Because these elements map to the statement of threat, the mapping (Figure 2) provides the framework for developing the protection measures, incident detection mechanisms, system security tests, and risk analysis. This mapping to the statement of threat bounds the scope of the other elements, clarifying the effort required to address each element.

When any element in Figure 1 is altered, changes will ripple through the system of security elements until it comes back into equilibrium, similar to changing a cell in a spreadsheet. Elements that have a major effect include:

- Change in definition, configuration, or application of the protected resource
- New threats
- Obsolete threats
- Changes in budget for protection measures
- Mandatory reanalysis of risk
- Mandatory recertification and reaccreditation.

Protected Resources. The first step of this methodology is to identify the resources to be protected and to develop a policy that states the level of protection or effort to be applied to each resource. Protected resources may include:

- Computing and communications equipment
- Buildings, utilities, or other facilities required for computer operation
- Computer programs and data
- Computer processing or communication capability
- Running computer processes—currently operating or suspended sequences of computer instructions
- Computer artifacts that a running computer process may require: available memory, data structures, allocatable devices, CPU (central processing unit) cycles, etc.

Each resource or related set of resources to be protected must be well-defined before one can compile the statement of threat. Once these resources have been identified and their desired protection levels established, one can examine threats to them and develop protection measures.

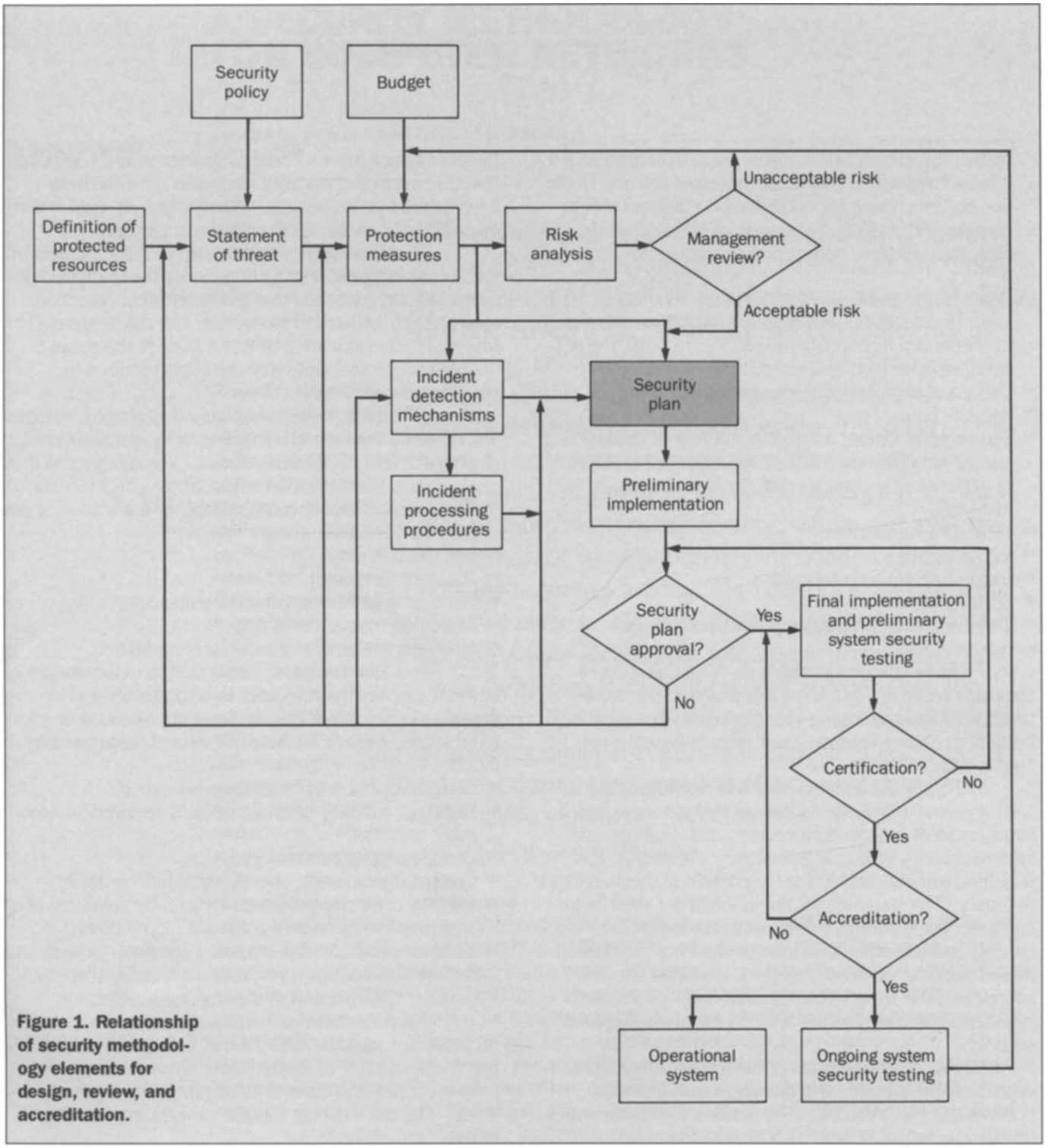

Figure 1. Relationship of security methodology elements for design, review, and accreditation.

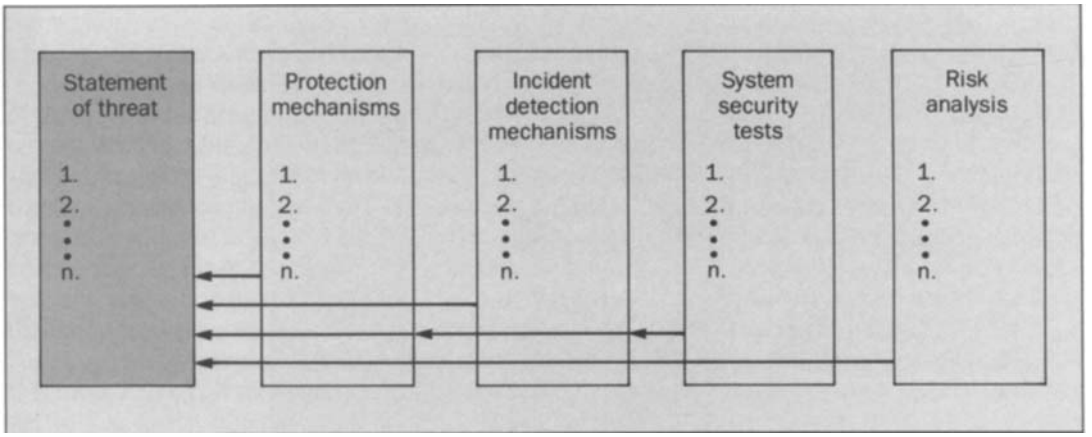

Figure 2. Mapping of security elements onto the statement of threat. The statement of threat limits the scope and granularity of all elements.

The *definition of protected resources* is a statement that includes a list of the location and nature of each resource, replacement cost of associated equipment, cost of displaced service or utility, and cost associated with compromise of data. Any costs that are intangible or cannot be estimated should be described in narrative form.

Security Policy. The security policy is a simple statement of management intent about protecting computing or communication resources. This statement identifies to what extent important classes of resources are to be protected from broad classes of perpetrators. A security policy should briefly describe the appropriate use of computing or communication resources. It should also describe the intent of protections against compromise of need-to-know, privacy, corporate security, national security, or other applicable losses perpetrated by insiders or outsiders or caused by natural hazards. *Insiders* are personnel authorized to enter physical security boundaries, while *outsiders* are those who are not.

A security policy need not be formalized with a mathematical model of computer security, although formal computer security models may aid in the development of protection measures for certain resources. Computer or communications resources and threats vary widely. So, it is unlikely that a single formal model and associated formal security policy can be used to plan adequately for all aspects of computer and communications security or for all computer networks.

A paper by Carl Landwehr states:[6]

A system security model defines the security rules that every implementation must enforce. It may reflect the demands of a general security policy on a particular application environment. A security model can act as a basis both for users to understand system operation and for system design. If stated formally and used as a basis for formal specification proofs, the security model rigorously defines system security.

Based on this description, several elements in Figure 1 would be included in a security model. The security model encompasses the security policy and the definition of protected resources. They supply the *demands of a general security policy* and *a particular application environment.* In addition, the model may include the statement of threat and the protection measures. They help establish *the security rules that every implementation must enforce.*

Statement of Threat. Implementors of secure computer networks have little concern with identifying the resources available to specific classes of perpetrators. Instead, they presume that a perpetrator will apply resources in proportion to the value of the protected resource to be subverted.

As stated before, a threat can cause theft, destruction, corruption, or denial of service, information, resources, or materials. To charactize a threat, we use the attributes, resources, and actions required to cause the event or carry out the method.

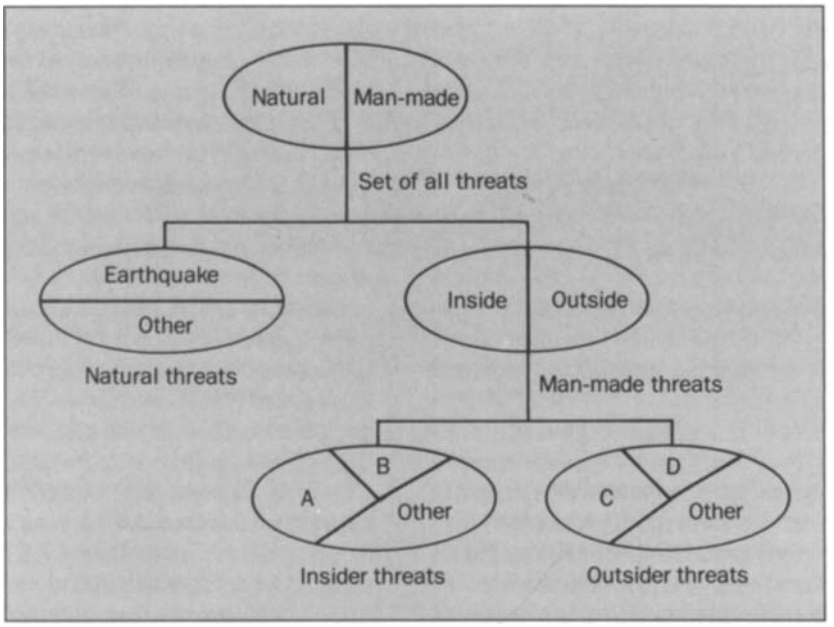

Figure 3. An example of binary decomposition of the statement of threat. "Insiders" are people who have authorized access to protected facilities; "outsiders" do not.

We must emphasize that a threat is a *what* or *how*, not a *who*. Perpetrators are the *who* elements and may be characterized by various motivations, levels of funding, and weapons or equipment.

Different kinds of perpetrators may use the same method, and one perpetrator may use many different methods. They may employ these methods from inside or outside a facility. One goal of incident detection and reporting procedures is to identify perpetrators so that they can be apprehended while a security incident is in progress and prosecuted later. For computer security planning, the projected category of perpetrator who may be likely to try to subvert protected resources is of little value. But categorizing threat events or methods is of great importance, because protection mechanisms are based on the methods that may be used independently by various perpetrators.

The statement of threat should define the types of threat events or methods that pertain to the network being examined. Any item that is not included in the statement of threat will not be analyzed in the risk analysis. In addition, protection measures will not be identified for it, nor will incident detection mechanisms be associated with it. Countermeasures are developed specifically for those threats defined in the statement of threat.

What drives the statement of threat is the security policy and the definition of the protected resources. If the security plan is not approved, the approving authority's reasons may also be sent to the plan's developers to revise the statement of threat.

To develop the statement of threat, we use binary decomposition (Figure 3). We begin with the universal *set of all hazards*, and typically divide it into natural and nonnatural (man-made) events or methods. Eventually, each subtree's decomposition ends with a general category such as *other events or methods*. The threat list that results should not overlap, but has a granularity (level of detail) determined early in the methodology. The granularity of this statement of threat also governs the granularity of the documented protection mechanisms, incident detection mechanisms, risk analysis, and system security tests.

All threats then map into a specific item identified in the statement of threat or into a nonspecific item identified as *other*.

After more experience is gained with the comput-

ing network to be secured, planners can add more detail to items in the statement of threat.

Protection Measures. For each item in the statement of threat, one or more measures should be developed to protect each identified resource. Protection measures are countermeasures that defeat or help to defeat one or more threats. A given countermeasure may partially negate several threats; but to negate a threat fully, more than one countermeasure may be needed. Also, attempts to circumvent the protection measures should trigger the incident detection mechanisms.

The budget available is an important constraint for this methodology. If more money becomes available for network security, other protection measures can be implemented, possibly reducing the residual risk. If budgets are cut, protection measures not yet installed or those with ongoing costs may have to be eliminated, possibly increasing residual risk.

If the security plan is not approved, the approving authority's reasons may also be sent to the plan's developers to change the protection measures.

Risk Analysis. Risk analysis is an analysis of the network's resources, controls, and vulnerabilities to determine the level of risk to which the resources are exposed. *Residual risk* is the portion of risk that remains after security measures have been applied. *Acceptable risk* is the level of residual risk that will be tolerated.

For each item, management must review the residual risk that the risk analysis identified to determine if the level of risk is acceptable. If it is not acceptable, more or improved protection measures should be added, subject to budget constraints. The risk analysis must address each item in the statement of threat.

Incident Detection. An incident is an event that is judged unusual enough to warrant further investigation to determine if a threat event occurred or a threat method was attempted, and if a loss occurred or might yet occur.

Incident detection mechanisms should include logging and reporting an event, and should be triggered by any attempt to circumvent the various protection measures. Incident processing procedures should be defined so they may be fully described in the security plan and should include incident reporting requirements.

Security Plan. The security plan document includes—by incorporation or reference—a description of all the security methodology elements for design, review, record of approval, certification of implementation, and accreditation (Figure 1). The security plan should specifically:

- Define resources to be protected
- Describe the protection measures that have been developed
- Describe the incident detection mechanisms that have been developed
- Describe the incident processing procedures.

In addition, the security plan should specify the acceptable risk; that is, the amount of residual risk that management agrees is acceptable when reviewing the results of the risk analysis. If the security plan is not approved, the approving authority should identify unacceptable aspects of the plan so that these elements may be properly revised.

The preliminary implementation (described in serial fashion for clarity in Figure 1) is frequently an ongoing process that may proceed in parallel with much of the security design. This parallel process provides valuable feedback to developers of protection measures and incident detection measures about feasibility of implementation and alternatives.

Certificiation and Accreditation. When the security designers decide that the security plan is complete, the plan is submitted to local computer-system security officials for approval. For intersite computing networks (wide-area networks), local computer-system security officials at each interconnected site must concur on the security plan's contents.

After local approval of the plan, final implementation of the security measures, and system security testing, the appropriate local computer-system security officials certify that the security measures called for in the approved plan are properly implemented and tested.

Accreditation is the approval and permission granted for a computer system or network to process classified or sensitive unclassified data. The designated approving authority grants this accreditation after reviewing the certifications done by the local computer-system security officers. A joint approval process must be defined

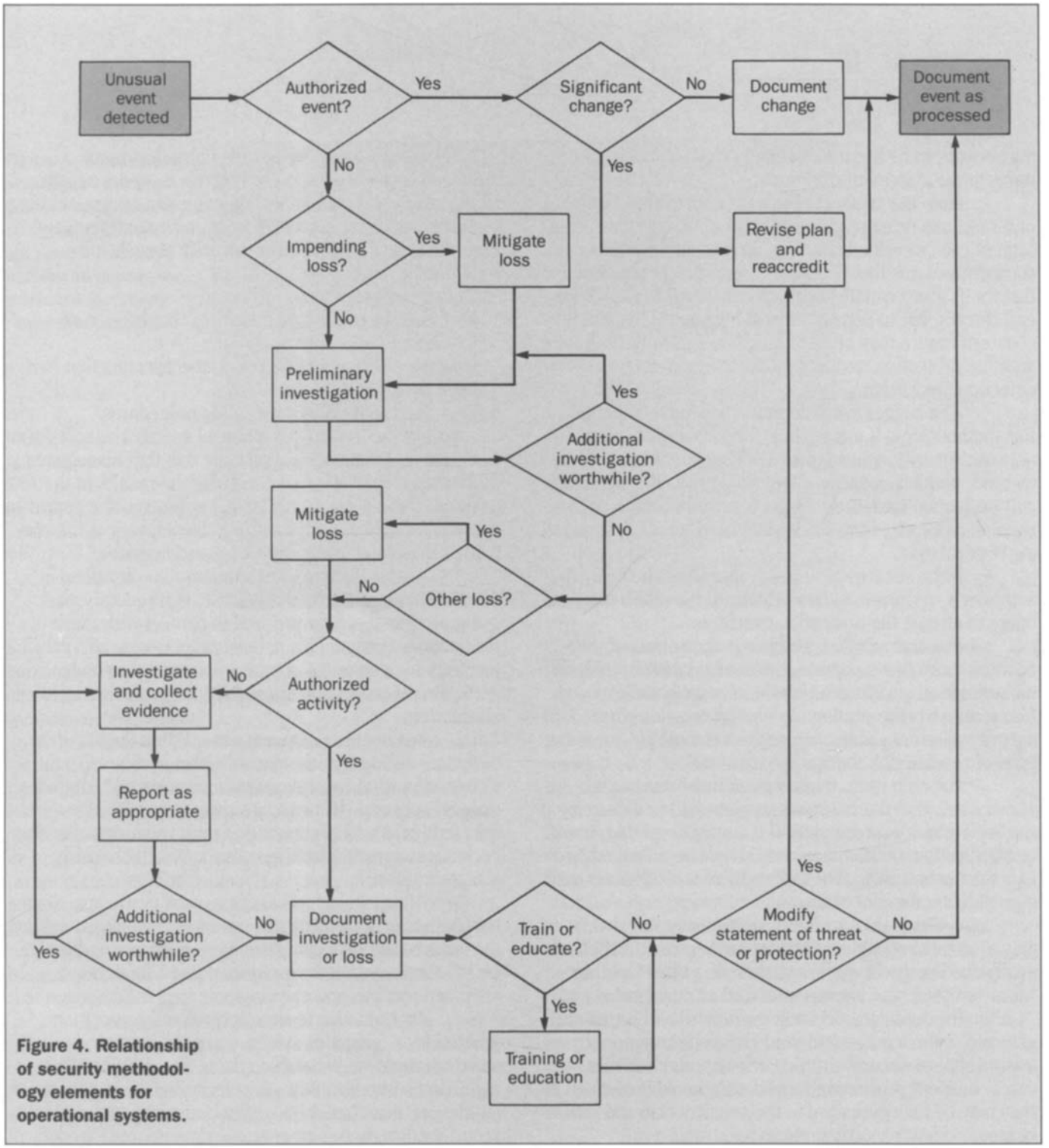

Figure 4. Relationship of security methodology elements for operational systems.

for networks of resources that are under multiple accreditation authorities.

System security testing is an ongoing, periodic process to verify that security measures identified in the security plan are still in place and are still effective in the changing technical environment. The security plan should also describe the type and frequency of ongoing system security testing.

Operational Phase

Because the security methodology for operational networks involves many decisions, its elements and relationships are not as easily described as those for design, review, and accreditation. Figure 4 shows the relationships for the various elements and the decisions.

The focus of the operational phase is the processing of unusual events to mitigate losses and improve protection. This processing may also result in the detection, apprehension, and prosecution of perpetrators who managed to subvert protected resources in spite of protections implemented in the design, review, and accreditation phase. The operational phase also provides ways for documenting unusual events. These records are fed to other possible investigations, and are used to change the statement of threat and protection mechanisms as a result of investigations of unusual events.

When some detection mechanism detects an unusual event, check the event to determine if it is authorized. System security tests (authorized "Black Hat" activity) should trigger events that will be detected.

If the event is authorized, decide if this event represents a significant change. A significant change is one that the local computer-system security official determines has changed the effectiveness of the security measures described in the security plan. This implies that the security official is well-versed in computer, network, and communications technology. If the event is not a significant change (e.g., a system manager changed a page-fault parameter), document the detected change for future reference.

A significant change should enter the security methodology for the design, review, and accreditation phase and feed through the methodology elements until they return to equilibrium. It may generate a one-page addendum to the security plan, or even a whole new security plan. This change may result in implementation changes, culminating with the network being reaccredited as described previously in Figure 1. If significant changes are scheduled (not just detected in operation), the network should be reaccredited before the change is placed in production.

If the event is not authorized, check to see if there is an impending loss and, if so, mitigate that loss. Next, do a preliminary investigation that may involve coordinating with personnel at other nodes or sites. If other losses are discovered, mitigate them too. If the activity turns out to be unauthorized, then investigate, collect evidence, report as appropriate, and document the investigation or loss. (Disciplinary action, even if the investigation suggests it, is beyond the scope of the computer security methodology.)

If further training or education is necessary, provide it. If the statement of threat or protection mechanisms need to be modified, the network's security plan reenters the design, review, and accreditation phase and the necessary changes are made. These changes will feed through the methodology elements until they come back into equilibrium. Again, the changes may yield a one-page addendum to the security plan or even a new security plan. As before, they must be recertified and reaccredited.

For either an authorized or unauthorized event, the detected event is finally documented as *processed.*

Proper execution of the incident processing procedure requires close interaction and cooperation between the system manager and the computer-system security official. But intersite computer networks (wide-area networks) pose a larger problem, because processing and communications equipment at the sites usually are under different management, possibly even different corporate management. A mechanism must be defined to ensure that all network nodes or sites cooperate to maintain proper protection of resources.

Experience

We have started to apply this methodology to computer systems and networks. Gains have been made in

the time required to analyze, secure, certify, and accredit systems because of the specific framework and clear bounds imposed on the security elements. The most important aspect appears to be the mapping of protection mechanisms, incident detection mechanisms, risk analysis, and system security tests to individual elements of a well-developed statement of threat.

But a major problem remains. How do you gain responsive security management of a network whose components fall under the authority of organizations widely separated in an interorganizational hierarchy? The multiple network managements or multiple accreditation authorities that exist create this problem.

Conclusion

We have described the elements of a security methodology for computer networks. This methodology applies equally to single computers or distributed systems. Its major elements that should have greater prominence in current security practice include:

- Definition of the protected resources
- A competent and well-structured statement of threat
- Protection measures
- Incident detection mechanisms
- A concise risk analysis.

Through the granularity of the statement of threat, this methodology bounds the scope of protection measures, incident detection mechanisms, system security testing, and the risk analysis activities.

The elements of this general methodology are not new. However, these elements and their relationships change over time, depending on whether the computer system or network is in design, review, and accreditation or in operation. If all these elements are incorporated, with proper feedback among them, a more robust security posture will result than from any subset of them used independently.

Acknowledgment

The work to develop this methodology was funded under Sandia National Laboratories Contract DE-AC04-76DP00789 for the U.S. Department of Energy.

References

1. *Computer Security Guidelines for Implementing the Privacy Act of 1974*, Federal Information Processing Standards Publication No. 41, National Bureau of Standards, May 30, 1975.
2. *Department of Defense Trusted Computer Security Evaluation Criteria*, DOD 5200.28-STD, National Computer Security Center, December 1985.
3. *Guidelines for Automatic Data Processing Risk Analyses*, Federal Information Processing Standards Publication No. 65, National Bureau of Standards, August 1, 1979.
4. *Guideline for Computer Security Certification and Accreditation*, Federal Information Processing Standards Publication No. 102, National Bureau of Standards, September 27, 1983.
5. *Password Usage*, Federal Information Processing Standards Publication No. 112, National Bureau of Standards, May 30, 1985.
6. C. E. Landwehr, "The Best Available Technologies for Computer Security," *Computer*, Vol. 16, No. 7, July 1983, pp. 88-100.
7. H. G. Pringle et al., "Computer System Security (CSS) Literature Review, Current Research Review, and Data Base Assemblage," Technical Report No. BDM/A-84-108-TR, The BDM Corporation, Albuquerque, New Mexico, October 31, 1984.
8. *Trusted Network Interpretation*, Version 1, Report No. NCSC-TC-005, National Computer Security Center, July 31, 1987.

(Manuscript received February 3, 1988)