Local Area Network Security

Editor's Note
This report provides practical information for managers having direct or indirect responsibility for the security of information processing resources and assets that reside on LANs. Topics addressed include LAN security vulnerabilities, potential risks, and potential countermeasures. The report also describes an approach to implementing a viable network security program and gaining upper management support for that program.

Report Highlights
Local area networks (LANs) present unique security issues and concerns. Security should be considered very early in a LAN's life-cycle. LAN security is often viewed as a knee-jerk reaction to a catastrophic event. Retrofitting a LAN with security, once it is operational, will almost certainly be more expensive and less effective.

An organization incurs costs for LAN security features not only for added equipment, but in terms of performance as well. Security adds performance overhead for encryption, user authentication, etc. The costs for LAN security are incurred immediately, but the benefits may be intangible. How can an organization quantify the cost savings for events that might have occurred were a security mechanism not in place?

The Fundamental Paradox between Networking and Security

A fundamental paradox exists in networking today—the need to share information and resources across distributed systems while at the same time controlling access to that information. LANs and LAN internetworks are implemented to provide global access, resource sharing, information sharing, application sharing, and other shared services, but security features attempt to restrict, condense, isolate, and mediate users' actions and the information and services they access. The problem is

This report was developed exclusively for Datapro by Steven L. Shaffer and L. Michael Sabo. Mr. Shaffer is manager of security engineering for SSDS, Inc. and is responsible for security design, security policy development, risk analysis, and countermeasure application for both the Department of Defense and commercial clients. He holds a BS degree in Computer Science and an MA degree in Computer Resource Management. Mr. Sabo is a communications network consultant with SSDS, Inc. and is currently developing a high performance networking architecture for interactive distributed real-time processing. He holds a BS degree in Computer Science and an MS degree in Data Processing Management. Mr. Sabo is a member of the Advisory Board for Datapro Network Management.

complex, and in many cases underlines the prevalent belief that "networks should always be considered insecure." This notion must be overcome through sound security engineering and management practices.

Primary goals for LAN implementations are to foster cooperation among computing entities and make access to information processing resources easy and flexible. Networking usually involves increased access and the removal of barriers, restrictions, and limitations. Security, on the other hand, normally involves limited cooperation; confinement of users, processes, and data; reductions in communications; limitation of access to resources; and the establishment of barriers and obstacles.

Why LANs Are Vulnerable

Virtually every activity in a modern society involves computers and automation. Computer systems have evolved though multiple cycles of change, and now are experiencing a networking revolution. Most computer systems today are found on desktops and other individual worker areas. Many of these desktop computer systems are linked by LANs.

A "perpetrator" (security violator) can do significantly more damage faster on a LAN than on a standalone computer system. For example, a terminal connected to a host via an RS-232-C cable can achieve a data transfer rate of up to 19.2K bps; a file transfer over an Ethernet LAN could easily occur at 300K bps.

Increased reliance on LANs for interoffice communications also increases the vulnerability of the data on the LAN. There are a number of reasons for this.

Larger Security Perimeter

LAN security managers must worry not only about controlling access to a central computer system and to desktop workstations; they must address computer systems security in a much broader sense. From the standpoint of security, a LAN can be considered as one contiguous system that must be protected in its entirety.

Increased Span of Control

In addition to the larger physical perimeter of a LAN network, the span of management and control also increases. Security managers must be concerned with security enforcement and control across multiple boundaries, and possibly across boundaries that are out of their control. A common security problem is the difficulty in implementing a common security management approach across multiple departments, organizations, and even companies. What one manager considers secure in one organization or department may not be so treated in another. Nevertheless, since all share a common communications highway, an organization's many entities must find an acceptable method for ensuring that they share common security goals.

Greater Physical Access

Many more physical points of penetration are available on a LAN than on a centralized system. Instead of requiring access to a specific computer system for a successful penetration, a perpetrator need only access the physical cable plant, which is usually easily accessible. Once again, networking creates an environment that is more difficult to protect and secure.

Attack from a Position of Safety

One of the most common ways to access networks is through dial-up services into a modem pool. This method provides a very comfortable means of penetration. The perpetrator can dial-in via a modem using the common services provided by the telephone company, and the perpetrator risks no personal physical harm.

Attack with Limited Exposure

When the perpetrator attempts to penetrate a computer network, he/she leaves no physical evidence of the attempt. Thus, the perpetrator has very limited risk of exposure.

Increased Connection Complexity and Vicarious Access

The complexity associated with attacks against networks today creates several problems for security managers. Perpetrators enjoy many options and they present technical challenges for even the most astute managers. For example, a perpetrator can access a LAN without approaching it physically.

Vicarious access occurs when a perpetrator gains access to multiple systems through a process acting on his/her behalf. By gaining access to a single system on a network, the perpetrator is then able to propagate his/her access rights to multiple systems on the network. In many LAN environments, a user need only to log on to the network once; all subsequent access is assumed to be authorized throughout the entire LAN. It then becomes virtually impossible for a manager to track the events of a perpetrator, and more importantly, map the attacking process to a specific individual.

A perpetrator is able to hide in time as well as space, making it difficult to locate the physical point of attack. Since the perpetrator utilizes a process to act on his/her behalf, it is possible to plant a software routine and tie it to a system clock for activation at any time the perpetrator desires. When the routine activates, the perpetrator may be miles away from the system being attacked.

Less Expensive and More Sophisticated Means of Attack

The ease in which a LAN can be attacked, and the commercial availability of the penetration "tools," exacerbates security problems. A LAN analyzer, for instance, can capture passwords as well as any other information traversing the network.

Changes in the Data Processing Climate

Networks have changed the very climate of information processing. For example, Management Information System (MIS) administrators, who once had centralized and unyielding control over corporations' information processing assets, are now yielding control to users.

Significant changes also occurred in the attitudes of computer professionals. Technical computer professionals used to work in an organization for 10 or 15 years, perhaps even until retirement. Few, if any, of them ever considered attacking a computer system for the purpose of information compromise, unauthorized disclosure, or denial of service. A primary reason for the lack of malicious incidences was the size of the community and the possibility of being "blackballed" from the industry if caught.

Today, however, there appears to be less dedication and loyalty in the computer industry. For example, demand for computer professionals is so great that one could perform a malicious act against a network, be caught and fired, and receive a job offer from another company the next day. Companies often will not prosecute due to the bad publicity or loss of public trust that may result. Much of this change in attitude has been caused by the intense demand for information processing skills, including experience with LANs.

Larger and Smarter User Population

The increase in network penetrations, malicious use of networking resources, and the introduction of malicious logic (such as Trojan Horses, viruses, and worms) results from the larger and smarter user population that exists today. Workstations have replaced dumb terminals for most network users. This permits users to develop and introduce software into the network, and access network resources, both local and remote, via communications software.

Difficult Implementation of Cohesive and Consistent Security Policy

One of the most frustrating issues for a network manager who is earnestly interested in designing a secure LAN, and ultimately managing the security of that LAN, is the difficulty implementing a LAN security policy. Because of the diversity, rapidly changing environments, and dynamic interface requirements characteristic of LANs, it is nearly impossible to implement a consistent and cohesive security policy.

A manager must also be concerned with the technical and political ramifications associated with distributed security control and distributed security management. If, for example, a single contiguous logical LAN serves multiple divisions or organizations within a company, those different operating entities may not operate under the same security provisions. One division may provide a specific level of security and degree of assurance; however, its efforts may be worthless if another division on the same LAN does not implement and support the same security features. Many security problems are caused by heterogeneous security policies, rules, countermeasures, and even the dissimilar implementation of identical countermeasures.

The options available for the use of malicious logic to act on behalf of a user, are many. Malicious logic can take many forms, but the three most common forms are:

1. Trojan Horses

2. Viruses
3. Worms

In most cases, malicious logic is imbedded within legitimate applications and software programs. This method of covert association allows the malicious logic to be "invited in" by an unsuspecting user.

A common method used to introduce malicious logic into a LAN is through shared resources on the network. In almost all instances, the users are comfortable with the resources that they access and the use of those resources. The perpetrator understands this, and as a result places the malicious logic in an enticing or new application, game, or other shared software. Common examples include:

- Shared Software Libraries/Applications/ Utilities/Games
- Bulletin Boards
- Public Domain Software
- Electronic Mail
- File Servers/Computer Systems with Public Directories

Information Requiring Protection

Typically, information security is associated with the protection of military secrets and classified information. In the commercial environment, information which could have harmed an organization if accessed improperly includes personnel data, strategic information, and various other types of proprietary information. Disclosure of protected information, whether military or commercial, could cause a loss in competitive edge and thus represents a real dollar loss.

Risk Analysis

Each LAN implementation is different; thus, security risks differ. To satisfactorily judge the security of a LAN, a qualified engineering staff should perform a risk analysis.

The ultimate goal of risk analysis is to determine, through practical examples, how an adversary, criminal, perpetrator, or malicious insider could cause any of the following events to occur:

- unauthorized disclosure of information;
- unauthorized modification of information;
- denial of service; or
- disruption in the continuity of operations.

Using practical examples, it should be clear where and what vulnerabilities exist within the LAN environment. The principle objective of risk analysis is to determine the LAN's vulnerabilities, and how they can be exploited. Unfortunately, a flawless, complete, and totally accurate risk analysis is theoretically impossible. For example, additional vulnerabilities may appear at a later date. Risk analysis should, however, provide insight into the LAN's more serious vulnerabilities.

Current Environment

In addition to evaluating a new or proposed LAN, the risk analysis should assess the existing security environment into which a LAN will be placed. This includes all relevant security disciplines that directly or indirectly affect the operations and security of the LAN. Specific security disciplines evaluated include physical security, personnel security, information security, and communications security. Each security discipline should be evaluated, taking into account how specific threats could be used to exploit existing vulnerabilities.

Objectives

Risk analysis is based on the fundamental premise that a risk-free LAN environment is impossible. Risks, therefore, must be managed. Any risk can be defined as the resultant value derived from the mapping of perceived and known threats against perceived and known system vulnerabilities. The qualification of risks is one of the necessary activities in determining which threats should be controlled. Risk analysis identifies those network risks, derived from various activities, which could impact the secrecy, integrity, and/or operational continuity of the network. The risk analysis process provides the information necessary to support risk management and the cost effective application of security countermeasures. Risk analysis is essential to the successful management of a LAN security program.

Independent Validation and Verifications

It is best to have an independent agency assess the threats, vulnerabilities, and derived risk associated with the LAN. An autonomous organization will

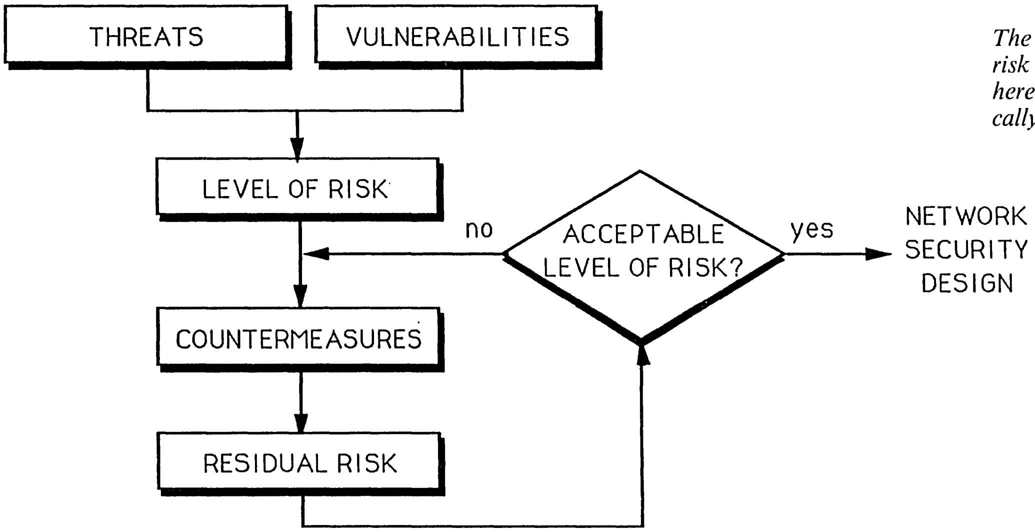


Figure 1.
The Risk Analysis Process

The methodology used for risk analysis is illustrated here in sequential and logically ordered steps.

prevent personal biases and influences from corrupting the accuracy of the findings. Independence provides the catalyst for information discovery, technical enlightenment, and the ability to shed new light on the security environment of the LAN.

Technical Focus and Direction

Risk analysis must have a focused technical direction with specific objectives. Without bounded direction and technical areas of focus, risks analysis can become a repetitive, nonproductive process. Therefore, a critical first step in the process is to provide technical direction and define the system to be evaluated. This sets the tone for future security engineering activities. Identification of specific areas of risk allows a manager to focus attention on those areas.

Justification

It is important to assess threats to a LAN, determine the LAN's vulnerabilities, and apply countermeasures sufficient to reduce risk. However, blind application of security countermeasures, without first understanding the inherent risks in the network, is likely to be unproductive, costly, and insufficient. A frequently overlooked benefit of risk analysis is its ability to provide additional technical justification for the acquisition and implementation of security countermeasures for specific threats. These countermeasures can be provided through hardware, software, procedures, personnel, or other means.

Performing Risk Analysis

Modeling a risk analysis process to derive useful abstractions from the model ensures an organized and technically consistent information presentation, through credible and useful numeric representations. To achieve this, the methodology used for risk analysis (shown in Figure 1) is described below in sequential and logically ordered steps.

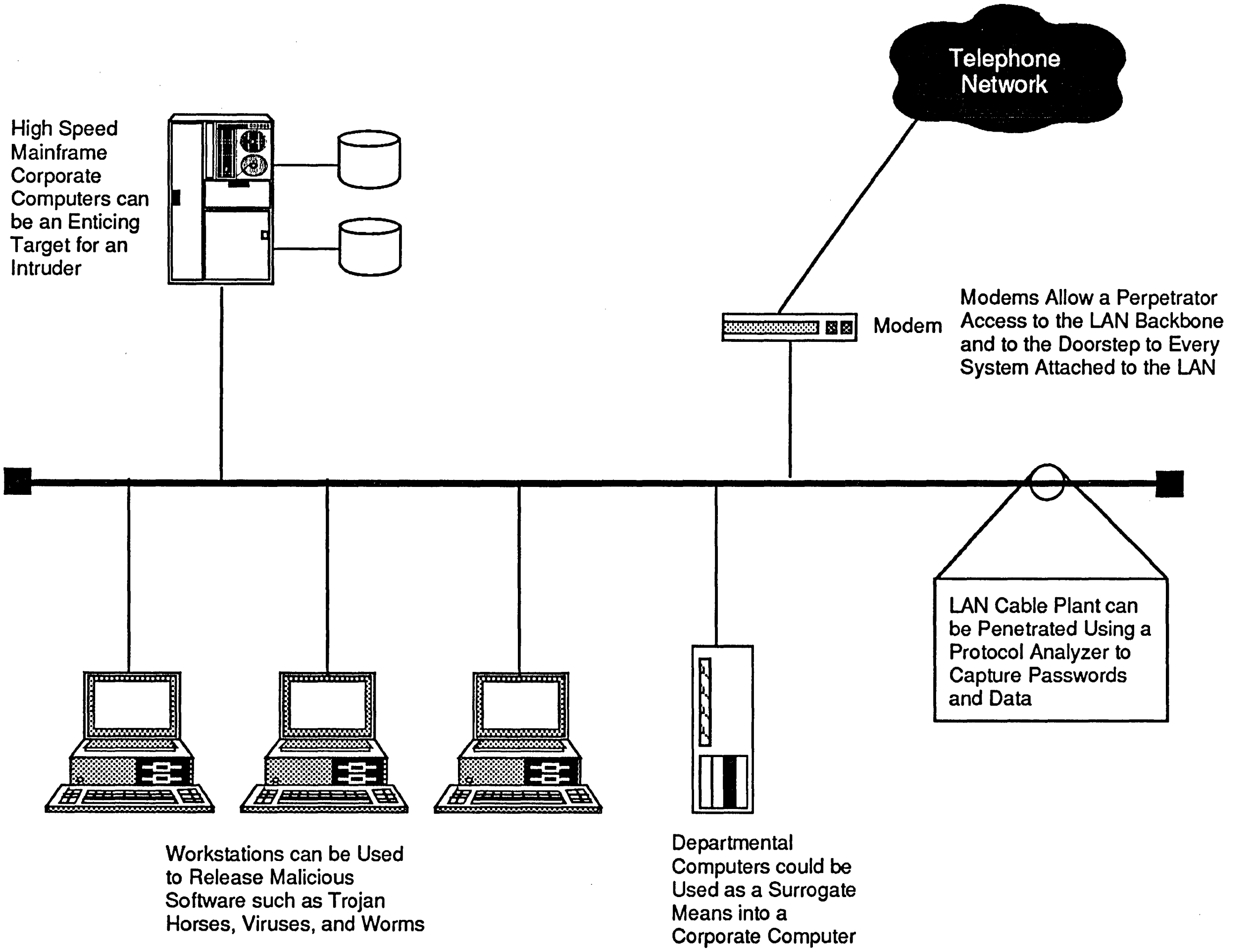
System Decomposition

The first step in the risk analysis process defines and logically separates the network into elements. Network elements include hardware, software, communications, and supporting systems and components.

Identification of Threats

Next, define potential threats against each network element identified in the preceding step. This can be a long and laborious task, with no assurance that the list will be complete. It is important, however, that the threat definition process have specific focus and direction. For example, threats identified should be those that specifically target

Figure 2.
Areas of LAN Vulnerability


Telephone Network
High Speed Mainframe Corporate Computers can be an Enticing Target for an Intruder
Modem
Modems Allow a Perpetrator Access to the LAN Backbone and to the Doorstep to Every System Attached to the LAN
LAN Cable Plant can be Penetrated Using a Protocol Analyzer to Capture Passwords and Data
Workstations can be Used to Release Malicious Software such as Trojan Horses, Viruses, and Worms
Departmental Computers could be Used as a Surrogate Means into a Corporate Computer

elements, systems, or information that might compromise the integrity of the network.

Many specific threats may exist; however, their likelihood of occurrence may be negligible. This can be determined from logical data and systematic analysis of the element being investigated. Therefore, *threat rejection logic* is an important way to limit the number of threats to be considered during the risk analysis process. For the purpose of performing trade-off analyses, the number of initial threat models is usually large; however, many are subsequently discarded because they have ceased to be relevant for one of three possible reasons:

1. the threat objective is no longer a practical goal;
2. plausible means to satisfy the threat objective no longer exist;
3. the threat is no longer considered viable.

The first two reasons relate to the network design or operational concept. The third is related to the official estimate of the threat. Only those threats that are deemed relevant should be investigated further.

Once the threats to a network are identified, they can be illustrated in *threat logic tree* format. The use of a threat logic tree enables a specific threat to be traced from a general description (i.e., denial of service) to a specific cause (i.e., resource exhaustion). Each threat is explained in detail (e.g., what does wire tapping mean and why is it a relevant threat to the network?).

Determine Vulnerability to Threats

A given element's vulnerability to a specific threat is determined by combining the probability of threat occurrence and the element's susceptibility to the threat. Table 1 provides the information

Table 1. Vulnerability Determination

Elements' Weakness to Threat	Probability of Threat Occurrence High	Moderate	Low
High	3	3	2
Moderate	3	2	2
Low	2	2	1

Key:
3—High probability of occurence.
2—Moderate probability of occurence.
1—Low probability of occurence.

necessary to make this determination. It is important to note that the ability to select the appropriate category or level (3—High, 2—Moderate, and 1—Low) is a function of historical/empirical data, existing documentation, practical experience, and a comprehensive analysis. For instance, if the element's weakness to a particular threat is high and the probability of the threat occurring is moderate, then Table 1 shows that the element's vulnerability rating is 3 (high probability of occurrence). Figure 2 presents specific areas where LANs are vulnerable. Typically, these ratings assume worst-case in an attempt to reveal security problems and concerns.

Determine Degree of Risk

To determine any given risk level, the severity of the threat and the element's level of vulnerability to that threat are combined. Table 2 provides the information necessary to make this determination.

Countermeasure Application

The countermeasure application process reduces or eliminates an identified risk. During this step, the value or benefit of applying the countermeasure must be quantified. In other words, countermeasures should be selected and applied against specific risks. This provides systematic traceability for countermeasure application and justifies their cost.

Situations exist where the application of a single countermeasure supports risk reduction or elimination in several areas. For example, encryption of data communications provides risk reduction against both information compromise and information modification. These multipurpose countermeasures can therefore be shown in several risk reduction scenarios.

Security countermeasures fall into three general categories: Access Control, Accountability, and Continuity of Service.

Access Control: includes doors, locks, physical barriers, passwords, user IDs, user accounts, encryption, personnel badges, biometric devices, and keyboard locks. Access control mechanisms are the most common form of security measures used in LANs today.

Accountability: these are typically audit trails or audit records. These contermeasures monitor, record, and sometimes detect security-relevant actions (e.g., incorrect passwords being entered a number of times). Accountability provides the security manager with the evidence necessary to take action once security violations are detected. Security countermeasures that provide cost-effective and useful functions in the security management of LANs are the most complex mechanisms in existence today.

Continuity of Service: includes those mechanisms that prevent loss of power (i.e., back-up power supplies or UPS) damage from flood, fire, or other natural disaster; and loss of service caused by user error, malicious acts, or other acts. Common countermeasures include alternate routing, full-mesh architectures, redundant communications paths/services, and fault-tolerant architectures. Robust protocols also provide an additional layer of assurance with regard to data communications integrity.

Table 2. Determining the Degree of Risk

Severity of Threat	Level of Vulnerability High	Moderate	Low
High	3	3	2
Moderate	3	2	2
Low	2	2	1

Key:
3—High level of vulnerability.
2—Moderate level of vulnerability.
1—Low level of vulnerability.

Table 3. Determining the Level of Residual Risk

Counter-measure Effectiveness	Degree of Risk High	Moderate	Low
High	2	1	1
Moderate	3	2	1
Low	3	2	1

Key:
3—High degree of risk.
2—Moderate degree of risk.
1—Low degree of risk.

IEEE Developments

The IEEE (Institute of Electrical and Electronics Engineers) is now developing LAN security countermeasures, to be applied to OSI Layer 2, through the Standard for Interoperable LAN Security (SILS), IEEE 802.10 effort. IEEE 802.10 defines SILS for standard services, protocols, data formats, and interfaces as a foundation to allow secure IEEE 802 LAN products to interoperate. IEEE 802.10 has specified four areas for standardization:

- SILS model (P802.10A);
- Secure Data Exchange (P802.10B);
- Key Management (P802.10C); and
- Security Management (P802.10D).

The IEEE 802.10 standards use encryption mechanisms to support access control, data confidentially, connectionless data integrity, and data origin authentication. Additionally, IEEE 802.10 security services will be transparent to the upper layer protocols traversing the LAN.

Determine Residual Risk

Residual risk is the remaining risk value after countermeasure(s) have been applied. Residual risk is determined by comparing the initial risk level against the utility of the selected countermeasure. Table 3 provides the necessary information to make this determination.

Process Iteration

It may become necessary to iterate the two previous steps until residual risk is less than or equal to "low." A residual risk level no greater than "low," for all intents and purposes, is considered adequate. There are instances where such a rating is mandatory, owing to the sensitive and/or critical nature of a particular application, or the damage that could be caused by information compromise, modification, or destruction. In these instances, residual risk can be lowered through the application of additional countermeasures.

It is important to note that a point of diminishing returns occurs in which the use of additional countermeasures may not increase the security of a system (by reducing residual risk), but can actually degrade performance and operations and significantly increase system acquisition and maintenance costs. Risk reduction is a function of many interwoven functions, facets, and parameters, all of which must be examined. The ultimate decision to apply additional countermeasures must be determined by the network manager in conjunction with the organization and users.

The identification of vulnerabilities alerts decision makers and creates additional security awareness; nevertheless, the risk analysis process is not an end unto itself, but rather a catalyst for increased attention and vulnerability resolution. The methodology provided above reduces risk through the application of countermeasures and the iterative determination of residual risk levels.

Summary

The process of securing a LAN is not trivial. The time, effort, and money spent should reflect the value of the information assets residing on the systems attached to the LAN. Consider LAN security very early in the system development process. After-the-fact retrofitting of security on a LAN will never provide as good a solution as a designed-in approach. ■