J. Webster (ed.), *Wiley Encyclopedia of Electrical and Electronics Engineering*

NETWORK SECURITY FRAMEWORK

The article "Network Security Fundamentals" outlines security threats, concerns, and components, all of which are elements of the overall security posture of a network. In an increasingly dynamic environment, where diverse user groups are being interconnected, there arises naturally the need for a universal definition and framework for network security. The framework must provide a comprehensive picture of network security and enable all parties to define and describe their security posture and concerns.

This article first reviews the current literature in network security and then describes a fundamental framework for network security that consists of eight perspectives and nine attributes of a secure network. The framework approach has been adopted by the National Security Agency (*NSA*) to underlie its Network Rating Methodology (*NRM*). The perspectives, termed *pillars*, individually provide orthogonal views of network security and collectively constitute a comprehensive stable structure that supports the total network security. The attributes refer to the inherent characteristics of a secure network.

The general concept of security in message communications may be traced back to the advent of human civilization. In contrast, however, security in automation and control is a recent phenomenon, originating with the computer age, and is rapidly gaining importance with the proliferation of networks. With computer networks integrating the dual functions of (1) communications and (2) automation and control, computer network security must address the security issues inherent in both communications and automation. Until recently, research and development in computer security was strongly linked with cryptography, including encryption and decryption of electronic messages. However, as computer networks have started to proliferate into large, complex, real-world systems such as electronic banking, the power grid, and the proposed intelligent vehicle highway system, the authors believe that computer network security has transcended the traditional definition and has migrated to a higher, logical level. In current and future networks, the information riding on the network may control parts of the network while the control, in turn, may ensure the correct propagation of information from the source to the intended destination. Thus, networks constitute complex, multidimensional entities that require security at different levels of both network hardware and network software.

The computer-driven integration of the fields of (1) communications and (2) automation and control has been primarily responsible for the proliferation of today's networks. Computer networks have grown from a simple time-sharing systems—a number of terminals connected to a central computer—to large, complex environments that provide the infrastructure to many critical and economically valuable components of the economy. Many of the large-scale real-world systems in the government, military, and industrial sectors consist of a number of geographically dispersed hardware and software entities that are interconnected through a network that facilitates the exchange of both data and control traffic. Examples include the Federal Reserve banking network, the power grid, the proposed intelligent vehicle highway system network, the US Treasury network (1), the FBI network (1), and the proposed community health care network.

There is an increased reliance on computer networks today that may not be widely known to the general public. In fact, most of us, do not realize that we rely on hundreds of computer networks during the normal course of the day and the proper functioning of these networks is critical to their well-being and survival. As a result, the risk to the economy, infrastructure, and well-being of the population has not been widely reported.

Such complex systems, however, are often vulnerable to failures, intrusion, and other catastrophes. Backhouse and Dhillon (2) estimate the yearly damage to the vulnerable finance and banking sectors in the United States at $2,000 million. With the growing use and ubiquitous reliance on such computer networks, an increasing emphasis is being placed on security. Both industry and government are engaged in developing new ways to ensure that the networks are more reliable, survivable, and secure.

The military started out with the idea of securing each individual computer and later expanded the concept to securing a network of computers and devices. However, it is not the only organization that requires and has implemented some form of security. Network security has evolved over the years, and other departments of government and government networks—including the US Treasury (1), the FBI (1), and the Federal Reserve banking network—as well as commercial institutions and commercial networks such as the banks, financial institutions, and credit card transaction networks (3), have embraced the idea of developing a secure network. Recently, the commercial banking industry has become very much interested in security of networks, since now a favorable cost benefit can be associated with security. The Internet's growing popularity and potential for commerce (4) has increased the amount of money and effort devoted to producing and enforcing security with respect to privacy and nonrepudiation (3). Corporations, such as General Electric, that have lost money as a result of intrusion can justify increased attention and spending on network security. The vulnerability of the power grid has raised deep concerns about the stability and reliability of networks.

Fundamentally, the reason underlying network security is the value of the information riding on the network. Admiral Grace Hopper (5) pointed out, as early as in the 1970s, that the industry is engrossed in the processing aspect of the information processors, and lacks a basic understanding of the *value of the information*. Even though computers and networks have been around for decades, there appears to be a lack of a community-wide agreement on adopting a common framework to define, describe, and evaluate network security. In the literature, definitions of network security terms are influenced heavily by the respective researcher's affiliation and background—industry, government, or military. Each of the three sectors continues to maintain its individual vocabulary, which is built around the perceived threat and cost benefit. However, the distinction is increasingly being blurred by overlapping networks, as is highlighted by a recent fact—90% of the electronic of the Department of Defense (*DoD*) traffic runs over the public networks (6). The lack of a common language to describe network security and the consequent inability to discuss network security hampers progress in the field and threatens the livelihood of millions of people and hundreds of corporations and government agencies. It is therefore imperative for all parties involved to agree on a common framework and revitalize the efforts towards evaluating network security. Recognizing this problem, the National Security Agency, the nation's chief proponent for computer and network security, organized the first Network Rating Model conference in Williamsburg, VA, on March 20–22, 1996 (7, 8). The goal was to develop a comprehensive model to rate the security of networks that would be acceptable to government, industry, defense, university, and other relevant organizations.

The development of security in automation and control over the years has been ad hoc, led primarily by the available technology and the goals of the funding agency. During World War II, the focus was on cryptography, which aimed to protect written traffic between encoding and decoding machines. This was defined as communications security. With the proliferation of computers and the birth of networks, the role of cryptography also expanded. However, cryptography is only one attribute of a secure network, and it alone cannot guarantee comprehensive security, particularly with today's and tomorrow's sophisticated computer-literate population.

The US military has methodically categorized the security attributes in the Orange Book (9). While the concepts of *communications security* (*COMSEC*) and *information security* (*INFOSEC*) are well understood within the Department of Defense, they mean little to most of industry and many civilian government agencies. In writing this article, first a comprehensive literature search was carried out, culminating in a detailed listing of the attributes of network security, as used by the military, and the specific terms used to describe them in industry and government. Then, the common terms were grouped together, and the best fit term was

selected to describe each issue. As an example, consider the term "classification," which the military uses to describe whether a network is restricted to a particular person, group, or class. This is further subdivided into the categories of unclassified, for official use only, confidential, secret, and top secret. In contrast, the term, "private" or "proprietary" in industry restricts the use of a network to a specific person, group or class and therefore corresponds to the military's "classified." Motorola's POPI classification is based on whether failure to protect data may disrupt business, provide undue economic advantage to the receivers, cause embarrassment, permit access to other classified data, provide undue advantage to a competitor in the marketplace or in its negotiations with a mutual customer or in its market strategy or access to technology, or lead to legal problems including liability.

A key difference between the industry, government, and defense perspectives has traditionally concerned threats and their sources. This difference is also becoming blurred. To the military, the traditional threat has been the enemy, typically a hostile government or terrorist, whose efforts were aimed at stealing valuable information from the network. Today, however, a new kind of threat, termed *information warfare* (10), has gained notoriety. It consists in disabling or rendering useless the enemy's key networks, including the command and control (10), power grid (6), financial, and telecommunications networks. In addition, the threat of economic espionage—that is, stealing secrets from industry and government networks—is on the increase. There is increasing evidence that insiders (disgruntled and recently fired employees) constitute the most significant threat (1). Malfeasants are another threat capable of causing mischief or serious harm to networks.

The remainder of the article is organized as follows. The next section reviews the current literature on network security. The section after presents the network security framework, and the last section presents a summary.

Review of Current Research in Network Security

The *DoD's* perspective on trusted computer systems is presented in the Orange Book (9). 5 presents a generalization of the *INFOSEC* and *COMSEC* concepts [9] to network security and provides the following general definitions. Information security (*INFOSEC*) is defined to consist of procedures and actions designed to prevent, at a given level of certainty, the unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional, of information in a network. Information includes data, control, voice, video, images, FAX, and so on. In contrast, communications security (*COMSEC*) refers to the protection resulting from the application of cryptosecurity, transmission security, and emissions security measures to telecommunications and from the application of physical security measures to communications security information.

Abrams and Joyce (11) review the trusted system concepts and reference validation mechanism and explore a new computer architecture to generalize the concepts for distributed systems. (Nessett (12) reviews the difficulties in authentication and notes the security advantages of centralized authentication during logon in distributed systems. Lin and Lin 13 note that in enterprise networks, the principle security "areas" include confidentiality, integrity, data-origin authentication, nonrepudiation, user authentication, and access control. They review public-key and secret-key cryptographic techniques for confidentiality, and kerberos for third-party authentication. They also suggest the use of centralized security management over distributed schemes to reduce overhead and security risks. Cryptography has continued to play a major role in security. To (Janson and Molva (14), network security involves controlling access to objects, enumerating the access rights of subjects, the threats that must be considered during access control design, and mechanisms to enforce access control. They describe the role of cryptography as central to both authentication and access control. In addition, they propose tracking resource usage by authorized users, at least for accountability, and for subscribers to identify themselves to each other to fend off masquerading intruders.

Power (10) introduces the notion of information warfare and notes that its scope includes (1) the electronic battlefield (disruption of enemy command and control), (2) infrastructure attacks, (on key telecommunications,

financial systems, and transportation), (3) industrial espionage, (covert operations aimed at stealing proprietary secrets or sabotage of company information network), and (4) personal privacy (theft of private information such as credit card or driver's license or social security numbers). The security services required in electronic commerce (*EC*) networks (3) include authentication, authorization, accountability, integrity, confidentiality, and nonrepudiation. 3 also identifies two kinds of possible attacks on *EC* networks—(1) passive, or pure listening, and (2) active, or insertion of modified packets. To defeat such attacks, the goals of security must be aimed at preventing traffic analysis attacks, preventing release of contents attacks, detection of message-stream modification attacks, detection of denial-of-service attacks, and detection of spurious association initiation attacks.

Hosmer (15) remarks that the desired goal in the current computer security paradigm is absolute security. This requires both logical and mathematical precision, and it is unfortunate that precision and complexity are inversely related. A related complication is that the future may witness other types of threats to network security.

According to Hill and Smith [16], the risks in the corporate world include personnel, property, information, and liability. Today's corporations are concerned with (1) protecting financial resources, personnel, facilities, and information, (2) access control for facilities and management information systems, and (3) recovery from disaster and continuity of operations.

Chambers [17] underscores the difficulty in detecting intrusion and notes that although the FDA network was successfully penetrated in 1991, the logging and monitoring tools, left running for weeks, revealed no signs of unauthorized access. Wolfe (18) underscores the value of the information contained in the hardware by pointing out that for many likely events that arise from the lack of security, such as virus attacks, there is no widely accepted measure of risk and the risk is not insurable.

Oliver [19] traces the concept of privacy of computer users and individual-related data to the US Constitution and notes that it is provided by a third party as far as distribution, publication, and linkage of the information to the individual are concerned. Oliver also addresses the debate as to whether computer users making anonymous statements may be held accountable. Hitchings [20] stresses the need to examine the human issues—cultures of people involved, attitudes, morale, and differences between personnel and organization objectives—relative to network security.

The literature on the use of audit trails to realize accountability, detect anomalous behavior of users, and possibly flag intrusion is rich. Vaccaro and Liepins [21] describe their experiences with recording and analyzing anomalous behavior in computer systems at Los Alamos National Laboratory immediately following an intrusion. Helman and Liepins [22] present a stochastic foundation for audit trail analysis. They also suggest several criteria for selecting attributes. Janson and Molva (14) propose the tracking of system resource usage by authorized users for accounting as well as intruder detection. They point out the need to (1) identify objects access to which must be controlled, (2) identify subjects whose access must be controlled, (3) identify the possible threats that must be defeated, and (4) catalog enforcement mechanisms. Lunt and Jagannathan (23) enumerate several discrete and continuous intrusion detection criteria and state that their system maintained system usage profiles of users, which in turn were periodically updated based on the *a priori* known user behavior. Kumar and Spafford 24 encode the knowledge of known attack procedures through specialized graphs in their system and use a pattern-matching scheme to detect network penetration. Soh and Dillon 25 present a Markov model of intrusion detection and devise a "secure computation index" measure to quantify the intrusion resistance of a system. Their results, however, are limited to a single computer system. In her survey of intrusion detection techniques, Lunt 26 notes that they are primarily based on maintaining audit trails and observes a few key controversial issues. They include the appropriate level of auditing, the voluminous amount of audit information, the comprehensibility of detailed audit information, the possible performance degradation as a result of audit, and the invasion of privacy of computer users. A variation of the audit trail concept has been proposed for the electric power industry. Weerasooriya and colleagues (27) present a neural network solution to the problem of security assessment in large-scale power systems. They use neural nets for

fast pattern matching of the state of the power system immediately following a "contingency" with historical trends. Their results are, however, limited to static security.

Recent research in intrusion detection continue to focus on the use of audit trails (28, 29), attempt to detect patterns in the traces of data and privilege flows (30, 31) and employ statistical and neural network models (32,33,34). 35 proposes the use of autonomous agents to collect break-in information. Following testing of the current intrusion detection products by vendors, Newman et al. observe that no product is capable of successfully detecting all attacks under heavy network loading, a conclusion corroborated by Lunt (37).

An analysis of the current literature reveals the following. First, the nature of the security concerns differs for each of the sectors—military, government, and industry. This has led to problems, since many of these sectors are forced, for efficiency and economy reasons, to use each other's networks. Third, there is the lack of a common framework to describe security and intrusn resistance of networks, an important issue that had dominated the Network Rating Model workshop.

The network Security Framework

Recently, many computer network experts (4, 6) have joined the electric power system researchers in sharing the latter's long-held belief in system availability (38 39,40) and transient stability (41) as primary security concerns. Fitzpatrick and Hargaden 42 argue that the design of complex networks must take into account scenarios where the network may be rendered unavailable by enemy action. They point out that in military command and control networks, units may need to continue fighting while out of contact with the higher headquarters and adjacent units, acting on their own initiative within the framework of the commander's intent.

Given the wide scope of today's networks and their enormous future potential, the goal of achieving comprehensive network security is challenging. The National Security Agency realized the need for a comprehensive definition of network security and organized an *NRM* workshop to address the issue. The overall goal of the workshop was to determine the degree of protection that should or could be provided, synthesize a measure of protection and a methodology for evaluation, and determine the cost and performance tradeoffs. The workshop was organized to first arrive at a definition of network security, acceptable to the government, military, industry, and university. Next, the potential threats were enumerated and the key attributes of a secure network identified. Logically, one must bound what one is protecting before one can analyze how well one is protecting it. Thus, the attributes serve as potential weak points in a network. It has become increasingly evident that the vulnerability or security of a network may be viewed from different conceptual points of view, termed *perspectives* in this article. Although this idea has been referred to as "disciplines" in the literature, the term "perspectives" appears to capture the underlying meaning more accurately. The total security of a network requires its detailed evaluation relative to every perspective. While one organization, building on its assumption of a specific set of threats, may find one subset of the perspectives important, another organization may find a different subset of the perspectives critical based on its own perceived threats.

The consensus definition of a *network rating model* is: "A consistent, cost-effective methodology based upon a defined set of characteristics for assessing the total security of any network or combinations of networks, either in operation or development; to define what exists, determine what is needed, identify what could affect security, and provide a universally acceptable assessment report."

In the definition, the term "consistency" stresses the need for the security rating of a network to apply uniformly across different sectors. Furthermore, a rating must be valid for a reasonable length of time into the future despite rapid advances in the networking technology. The cost-effectiveness criterion underscores the need to balance the cost of the threat against the cost of implementing security. The defined set of characteristics is currently under consideration. The total security refers to the different dimensions of a secure network, while the phrase "network or combinations of networks" reflects the increasing bluring of network boundaries. Since

the report must be universally acceptable and useful, it must record the security measures currently in place in the network, which in turn will facilitate identifying what more is required to ensure total security.

In order to define the characteristics or attributes of a given secure network, it was decided at the workshop that one must focus on the relevant set of network security perspectives to yield security services that satisfy stated concerns. The comprehensive list of perspectives include (1) systemic, (2) communication, (3) physical, (4) personnel, (5) operational, (6) application, and (7) performance, and (8) design correctness. The services were enumerated as (a) access control, (b) confidentiality, (c) integrity, (d) authentication, (e) traffic flow security, (f) assured service, (g) nonrepudiation, (h) anonymity, and (i) intrusion detection. The concerns included (i) accountability, (ii) availability, (iii) liability, (iv) reliability, (v) auditability, (vi) interoperability, (vii) confidentiality, (viii) integrity, and (ix) uncertainty. These perspectives, services, and concerns were corroborated in Ref. 1

At the first *NRM* workshop, given the limited time available for a thorough discussion, security services and concerns were separated into two distinct lists. This split was driven by the divergent views of the representatives of industry, government, and military, which, in turn, stemmed from differing perceptions of the threat sources.

Defining the Framework for Network Security. Upon careful analysis, it became increasingly evident to the authors that a unified approach to total network security, across the military, government, industry, and university sectors, requires the recognition of two fundamental components of network security. First, any secure network must possess a few inherent characteristics, regardless of the sector to which it belongs and independent of any specific threat. These characteristics are referred to as *attributes* of a secure network and are the result of unifying security services and concerns. Second, a network's security may be viewed at different conceptual layers, each view reflecting a threat, being relatively orthogonal of others, and thereby permitting independent development and evaluation. The conceptual aspects are referred to as *perspectives* or *pillars*. The list of attributes includes (1) privacy, (2) integrity, (3) accountability, (4) availability, (5) reliability, (6) connectivity, (7) recovery from disaster, (8) liability, and (9) uncertainty, and they constitute a superset of the attributes proposed in the literature. The list of pillars includes (a) systemic, (b) communication, (c) physical, (d) personnel, (e) operational, (f) application, (g) performance, and (h) design correctness. This orthogonal framework approach was also adopted at the second *NRM* author's group workshop in July 1996.

Figure 1 shows the network security framework wherein the attributes permeate each of the pillars that, in turn, collectively hold up network security. The relative strengths of the pillars may vary, depending on the perceived threats in a given scenario. Thus, network security is only as strong as the weakest pillar. Figure 1 presents a representation of the framework through a matrix. It provides an organized framework for the network security evaluation information, which may be utilized to improve security or to evaluate the security resulting from interconnecting two or more networks. Ideally, a fully secure network would require every attribute to be strongly protected in all pillars, subject to some standard threat, relative or absolute. However, this may be neither cost-effective nor practical, due to limited time and resources. Network-security-related decisions are based on the perceived threat to a particular pillar and/or attribute and the level of risk that the security management is willing to assume.

Pillars of Network Security. The choice of the term pillars reflects the eight foundation blocks, each of which may be under attack, either independently or together, that cumulatively support a network's security. Thus, each pillar, corresponding to one the eight perspectives, describes an orthogonal conceptual view of network security and may be developed and evaluated independently, based on the degree of importance assigned to the appropriate threats. Consequently, the pillars may exhibit different relative strengths. Should new types of threats emerge in the future, requiring additional views of network vulnerability, additional pillars may need to be incorporated into the framework. The scope of the eight pillars is elaborated as follows.

- *Systemic* encompasses the software that operates the network and constitutes the basic infrastructure of the high-level application software.

	Privacy	Integrity	Accountability	Availability	Reliability	Connectivity	Recovery	Liability	Uncertainty
Systemic									
Communication									
Physical									
Personnel									
Operational									
Application									
Performance									
Design correctness									

Fig. 1. Components of network security.

- *Communications* encompasses the links and devices that interconnect the computers to constitute the network.
- *Physical* encompasses the equipment, material, and documents associated with the network.
- *Personnel* encompasses the people associated with the operation or use of the network.
- *Operational* encompasses the procedures, policies, and guidelines that constitute the security posture of networks.
- *Application* encompasses the high-level software that executes on the network.
- *Performance* encompasses the normal range of operating parameters and throughput of the network.
- *Design correctness* encompasses the correctness of the total system. The complex interactions between the different components of the system will, in general, result in a very large number of states and state transitions. Without ensuring that every state and state transition is correct, the threat of the system entering an unstable state, which then triggers catastrophic failure, is very real.

Attributes of a Secure Network. Each of the attributes will bear a specific degree of relationship to each of the seven perspectives defined by the network and the current understanding of security attacks. While most of the relationships are readily understood, a few are unclear at the present time, while all are subject to evolution as our understanding of network security matures. For instance, the privacy attribute bears a strong relationship to the personnel pillar. In contrast, consider the relationship between the performance pillar and the liability attribute. At the present time, the relationship is weak, since it is difficult to prosecute a hacker for degrading a network's performance and even more difficult to quantify the degradation and, therefore, determine a commensurate punishment. However, as society acquires a better grip on the responsibilities and consequences, the relationship will be greatly refined. The relationships may be evaluated, objectively or subjectively, through mechanisms, some of which are well known while others are yet undefined. As an example, the use of background checks may help strengthen the privacy attribute and the personnel pillar. Similarly, the strength of the relationship between the systemic pillar and privacy attribute for a given network may be evaluated through the access controls implemented. While the dependencies (1) between the "design

correctness" pillar and all of the attributes and (2) between the "uncertainty" and "liability" attributes and all of the pillars are clear, the exact relationships and the corresponding mechanisms to evaluate them are yet to be defined. The attributes are elaborated as follows:

- *Privacy* (10, 19) is defined as intention for or restriction to the use of a particular person, group, or class. It applies to data, control signals, and traffic flow. Synonymous and associated words in the literature include confidentiality (3, 14), anonymity (19), classification (9), proprietary, TRANSEC, cryptosecurity, EMSEC, and encryption (5).
- *Integrity* (3, 40) is defined as ensuring that information held in a system is a proper representation of the information intended and that it has not been modified, created, destroyed, or inserted by an unauthorized entity. Integrity also refers to the processes, process sequences, and other system assets. Synonyms and associated words include soundness, incorruptibility, completeness, and honesty.
- *Accountability* (19) is defined as a statement or exposition of reasons, causes, or motives to furnish a justifying analysis or explanation that can be documented or traced and ownership established. Synonyms and associated words include nonrepudiation (40), auditability (32), audit trail (26), answerable, authentication (3), signature, and responsibility.
- *Availability* (24, 40) is defined as being qualified and present or ready for immediate use by authorized users and worthy of acceptance or belief as conforming to fact or reality. Synonyms and associated words include access control (14), authentication (3), and confirmation.
- *Reliability* is defined as generating consistent results during successive trials. Synonyms and associated words include assured service, assuredness, certainty, and dependability.
- *Connectivity* (43) is defined to consist of the devices that constitute the network including the computers and links between them, and the intelligence that supports the seamless and transparent integration of a wide variety of different protocol-driven terminals and host computers. Synonyms and associated words include interoperability, traffic flow, logical flow, associations, relationships, emissions control, and TEMPEST.
- *Recovery* (15) is defined as returning from a disaster and continuity of operations. Synonyms and associated words include self-healing and contingency planning.
- *Liability* (16) is defined as having to do with legal obligation and responsibility that may affect property and information. Synonyms and associated words include responsibility, due process, ethical responsibility, open, and exposure (i.e., lack of protection or powers of resistance against something actually present or threatening).
- *Uncertainty* reflects the lack of complete knowledge of the system security as a result of previous penetrations, with known and unknown consequences, that may degrade future network security. This attribute may be viewed as a generalization of the concept of anomaly detection (23, 26) in a user's behavior through audit trail analysis.

Uses of the Network Security Framework. The framework provides a basis to address, fundamentally, every weakness in a given network. Furthermore, it applies to every level of the network, from the highest network-of-networks level down to the single computing node that maintains connections with other nodes. Thus, the framework enables the comprehensive understanding of the security posture of an individual network, the comparative evaluation of the security of two or more networks, and the determination of the resulting security of a composite network that is formed from connecting two or more networks with known security. These uses of the framework can be extrapolated to establish a user-level security-on-demand system in an *ATM* network.

The value of the proposed framework is that it stimulates the network designers to examine the vulnerabilities of all eight pillars even when they may appear inconsequential. For instance, while a credit card network, operating on the Internet, may successfully address the privacy attribute and feel secure, malicious agents may penetrate the network and reduce the availability so that customers are prevented from making

purchases. An examination of the performance pillar may be advisable under these circumstances. In a different scenario, while the military assigns resources to ensure the privacy and connectivity attributes, a disgruntled employee may send out an unauthorized message, under an assumed ID, to the finance and accounting military pay program, take advantage of a weakness in the accountability attribute, and deny hundreds of thousands of soldiers their pay on time.

The first use of the framework is to provide an overall view of a network's security posture. The procedure for determining a rating of a network consists of the following. For a given standard threat level, relative or absolute, and a given environment, the strengths of the intersection points in the matrix are obtained through evaluating the corresponding mechanisms. The evaluations may assume the form of numerical values, narratives, or graphs, subjective or objective. To improve the security posture of the network, either (1) the individual values along a row that constitute an evaluation of the corresponding pillar may be examined against a perceived threat level, or (2) the values along a column that reflect an evaluation of the strength of the corresponding attribute may be compared against a desired measure for the attribute. Clearly, the desired measure will reflect a cost–benefit analysis, with respect to the level of risk that the security management is willing to assume. As indicated earlier, the matrix provides a meaningfully organized framework for the evaluation of network security information, in terms of its fundamental characteristics. Thus, to compare the security postures of two or more networks, either (1) the individual values along a row of the corresponding matrices may be examined against each other, or (2) the values along a column of the corresponding matrices may be contrasted. It should also be noted that network security is a continuous process and must be exercised periodically. With time and as the roles of networks evolve, security breaches may appear in previously unsuspected areas.

To understand the operation of the framework, consider that the military perceives the primary threat to its networks and data from hostile governments. Clearly, to the military, the communications and physical pillars are vulnerable. This, in turn, points to the connectivity attribute. Furthermore, the desire to protect data riding on the network requires focus on the privacy attribute. In contrast, consider a financial network's concern that a malicious agent may disrupt its financial services. Clearly, the systemic pillar is vulnerable, which in turn points to the connectivity attribute. In addition, the privacy attribute may also be flagged due to the confidential nature of the financial transactions.

Assume that a defense agency plans to send top secret traffic through an *ATM* network. Initially, it will insert the highest value, say 0, in the entire privacy column and communication row of the matrix associated with the corresponding call request. To successfully propagate the traffic through the network, the call setup process must first determine a route, if possible, where each and every *ATM* node along the route offers a privacy value of 0 in every pillar and 0 in every attribute of the communications pillar. The values assigned to the elements of the security framework matrix of the node reflect the strengths of the security in the respective domain. The values of the individual elements may differ over a wide range, with some elements possibly being 9, implying the absence of security in that element area. Examples of three matrices, corresponding to three military traffic types—top secret, secret, and confidential—are presented in Fig. 2 along with the relevant element values.

The framework's second use is in computing the resulting security of the composite network, AB, formed from connecting two networks A and B, with known security, as shown in Fig. 3.

By design, the framework applies to every level of the network, from the highest network-of-networks level down to the single computing node that maintains connections with other nodes. A key goal of the framework is to provide a template for organizing the different aspects of network security to permit the military, government, and industry to start their connectivity discussions from a common baseline. Whether they choose to use or ignore some or all of the elements of the framework is their decision and is based on the amount of risk they wish to assume. In any case, they will all be aware of the total framework and all of its elements.

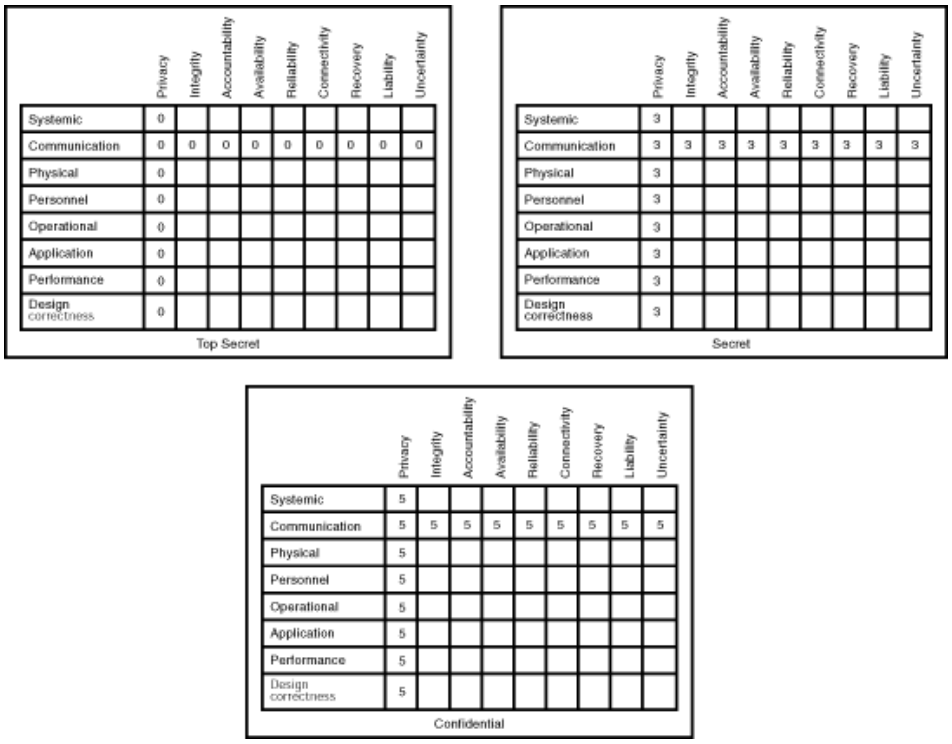

Fig. 2. User-specified security matrices for military traffic.

The framework's third use is in a user-level security-on-demand system where the framework is used by both the user and the network operating software and hardware to determine a path between source and destination that satisfies the user security requirements or rejects the traffic. Such a system has been modeled and simulated for a large-scale asynchronous transfer mode (*ATM*) network (44, 45). The advantages of an *ATM* network include its high speed, small packet size, point-to-point connection, and virtual path-oriented transmission of messages. The comprehensive framework provides the ability for all user groups to define their security requirements within the context of the framework. The framework, when integrated into an *ATM* network, provides a template for matching network security resources to user requirements. The user-level aspect of the security-on-demand system is possible in an *ATM* network due to *ATM*'s unique call setup process. *ATM* networks are ideal for implementation of the proposed user-level, security-on-demand system because the route the user's data will follow is known *a priori* and can be manipulated during the call setup, ensuring that the user-required security is provided or the call is not established. The security-on-demand approach in *ATM* networks is yet to be deployed by the industry.

Summary

This chapter has reviewed the current literature in network security and presented the definition of the Network Rating Model, arrived at by consensus at the National Security Agency's *NRM* conference in March 1996 and a subsequent *NRM* author's group workshop in July 1996. It has defined a fundamental framework for network security, which consists of eight perspectives of network security and nine attributes of a secure

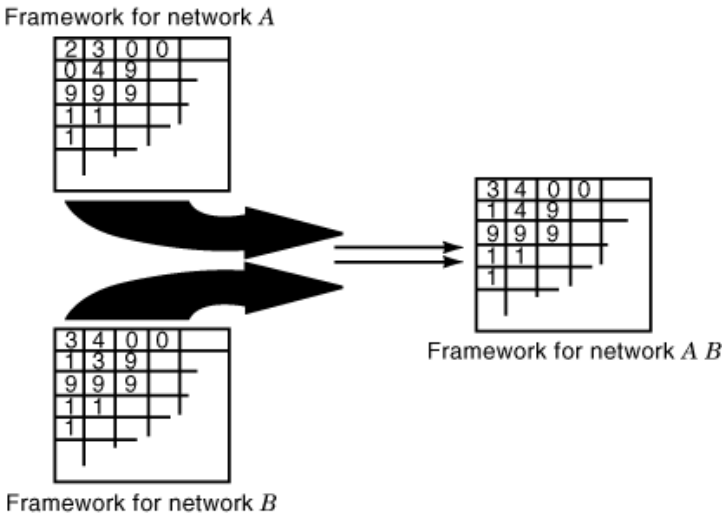

Fig. 3. Comparing two networks' security.

network. The perspectives, termed "pillars" in this article, individually provide orthogonal views of network security and collectively constitute a comprehensive stable structure that supports the total network security. The attributes reflect the inherent characteristics of a secure network. The framework addresses a previously unfulfilled need within the community. The uses of the framework are threefold. The framework enables the understanding of the security posture of an individual network in a comprehensive manner, the comparative evaluation of the security of two or more networks, and the determination of the resulting security of a composite network that is formed from connecting two or more networks with known security. The framework can also be used as a basis for a user-level security-on-demand system in an *ATM* network.

BIBLIOGRAPHY

1. P. Edfors presented at Network Rating Model Conference, Department of Justice, Williamsburg, VA, 1996.
2. J. Backhouse G. Dhillon Managing computer crime: A research outlook, *Comput. and Security*, **14** (7): 645–651, 1995.
3. D. E. Geer Electronic commerce, banking and you, *Comput. Security J.*, **XI** (2): 55–62, 1995.
4. J. M. Tenenbaum *et al.* "CommerceNet: Spontaneous electronic commerce on the Internet, *Proc. IEEE Comput. Soc. Int. Conf. '95 (COMPCON 95)*, 1995, pp. 38–43.
5. T. W. Madron *Network Security in the '90s—Issues and Solutions for Managers*, New York: Wiley, 1992.
6. C. Baggett Keynote address, Network Rating Model, First Public Workshop, National Security Agency, Williamsburg, VA, 1996.
7. *NSA*, Network Rating Model: Operational Capability Maturity Model (OCMM), National Security Agency, March 6, 1996.
8. *NSA*, Network Rating Model (*NRM*): Strawman, National Security Agency, March 20–22, 1996.
9. Department of Defense, Department of Defense trusted computer system evaluation criteria, 5200.28-STD, Washington, DC, 1985.
10. R. Power CSI special report on information warfare, *Comput. Security J.*, **XI**, (2): 63–73, 1995.
11. M. D. Abrams M. V. Joyce Trusted system concepts, *Comput. and Security*, **14** (1): 45–56, 1995.
12. D. M. Nessett Layering central authentication on existing distributed system terminal services, Proc. *IEEE 1989 Comput. Soc. Symp. Security and Privacy*, Oakland, CA, 1989, pp. 290–299.

13. P. Lin L. Lin Security in enterprise networking: A quick tour, *IEEE Commun. Mag.*, Jan. 1996, pp. 56–61.
14. P. Janson R. Molva Security in open networks and distributed systems, *Comput. Netw. ISDN Syst.*, **22**: 323–346, 1991.
15. H. H. Hosmer Security is fuzzy! Applying fuzzy logic to the multipolicy paradigm, *Comput. Security J.*, **XI** (2): 35–45, 1995.
16. S. Hill M. Smith Risk management and corporate security, *Comput. and Security*, **14** (3): 199–204, 1995.
17. T. Chambers Case study: A managerial perspective on an Internet security incident, *Comput. Security J.*, **XI** (1): 17–23, 1995.
18. H. B. Wolfe Computer security: For fun and profit, *Comput. and Security*, **14** (2): 113–115, 1995.
19. C. Oliver Privacy, anonymity, and accountability, *Comput. and Security*, **14**: 489–490, 1995.
20. J. Hitchings Deficiencies of the traditional approach to information security and the requirements for a new methodology, *Comput. and Security*, **14** (5): 377–383, 1995.
21. R. S. Vaccaro G. E. Liepins Detection of anomalous computer session activity, *Proc. 1989 IEEE Comput. Soc. Symp. Security and Privacy*, Oakland, CA, 1989, pp. 280–289.
22. P. Helman G. Liepins Statistical foundations of audit trail analysis for the detection of computer misuse, *IEEE Trans. Softw. Eng.*, **19**: 886–901, 1993.
23. T. F. Lunt R. Jagannathan A prototype real-time intrusion-detection expert system, *Proc. 1988 IEEE Comput. Soc. Symp. Security and Privacy*, Oakland, CA, 1988, pp. 59–66.
24. S. Kumar E. H. Spafford An application of pattern matching model in intrusion detection, Technical Report 94-013, Dept. of Computer Sciences, Purdue Univ., 1994.
25. B. C. Soh T. S. Dillon Setting optimal intrusion-detection thresholds, *Comput. and Security*, **14** (7): 621–631, 1995.
26. T. F. Lunt A survey of intrusion detection techniques, *Comput. and Security*, **12** (4): 405–418, 1993.
27. S. Weerasooriya *et al.* Towards static-security assessment of a large-scale power system using neural networks, *IEE Proc. C Generation Transmission Distribution*, **139** (1): 64–70, 1992.
28. M. Esmaili R. Safavi-Naini, M. B. Balachandran AUTOGUARD: A continuous case-based intrusion detection system, *Austral. Comput. Sci. Commun.*, **19** (1): 392–401, 1997.
29. A. P. Kosoresow S. A. Hofmeyr Intrusion detection via system call traces, *IEEE Softw.*, **14** (5): 35–42, 1997.
30. S. P. Shieh V. D. Gligor On a pattern-oriented model for intrusion detection, *IEEE Trans. Knowl. Data Eng.*, **9**: 661–667, 1997.
31. N. Puketza *et al.* Software platform for testing intrusion detection system, *IEEE Softw.*, **14** (5): 43–51, 1997.
32. D. Qu *et al.* Statistical anomaly detection for link-state routing protocols, *Proc. 1998 Int. Conf. Netw. Protocols, ICNP*, Austin, TX, 1998, pp. 62–70.
33. G. P. Kumar P. Venkataram Security management architecture for access control to network resources, *IEE Proc. Comput. Digital Tech.*, **144** (6): 362–370, 1997.
34. J. Mauricio Bonifacio Jr. *et al.* Neural networks applied in intrusion detection systems, *IEEE Int. Conf. Neural Netw.—Conf. Proc. IEEE World Cong. Comput. Intell. Proc. 1998 IEEE Int. Joint Conf. Neural Netw.*, Part 1, Anchorage, AK, 1998, Vol. 1, pp. 205–210.
35. M. Asaka Information gathering with mobile agents for an intrusion detection system, *Sys. Comput. Japan*, **30** (2): 31–37, 1999.
36. D. Newman, T. Giorgis, F. Yavari-Issalou Intrusion detection systems: Suspicious finds, *Data Commun.*, **27** (11): 8, 1998.
37. Teresa Lunt, Panelist, National Information Systems Security Conference, Oct 8, Baltimore, MD, 1997.
38. R. Billington E. Khan A security based approach to composite power system reliability evaluation, *IEEE Trans. Power Syst.*, **7**: 65–71, 1992.
39. Computer Sciences Corp., UCA and DIAS information security analysis, EPRI Technical Report TR-103773, 1994, Electric Power Research Institute, Palo Alto, CA.
40. S. A. Klein J. N. Menendez Information security considerations in open systems architecture, *IEEE Trans. Power Sys.*, **8**: 224–229, 1993.
41. J. A. Pecas Lopes *et al.* A new approach for transient security assessment and enhancement by pattern recognition, *Proc. Second Eur. Workshop on Fault Diagnostics, Reliability, and Related Knowledge Based Approaches*, Pergamon Press, 1987, pp. 189–215.
42. S. K. Fitzpatrick P. J. Hargaden Multimedia communications in a tactical environment, *Proc. IEEE MILCOM*, 1994, Vol. 1, pp. 242–246.

43. L. Guidoux Intelligent solutions for data communications networks, *Telecommunications, Int. Ed.*, **29** (6): 25–29, 1995.
44. H. J. Schumacher S. Ghosh An integrated approach to security on demand in *ATM* networks, *Inf. Syst. Security*, **6** (4): 10–21, 1998.
45. H. J. Schumacher S. Ghosh A fundamental framework for network security towards enabling security on demand in an *ATM* network, *Comput. and Security*, **17** (6): 527–542, 1998.

H. J. SCHUMACHER
Arizona State University
SUMIT GHOSH
Arizona State University