Journal of Network and Computer Applications (1997) **20,** 305–322

A fundamental framework for network security

H. J. Schumacher and Sumit Ghosh

Networking and Distributed Algorithms Lab, Department of Computer Science & Engineering, Arizona State University, Tempe, AZ 85287, USA

The general concept of security in message communications may be traced 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 (i) communications and (ii) 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, multi-dimensional entities that require security at di erent levels of both network hardware and network software.

This paper first reviews the current literature in network security, in detail. Second, it presents the definition of the network rating model, arrived at by consensus, at the National Security Agency's Network Rating Model (NRM) conference in March 1996 and a subsequent NRM author's group workshop in July 1996. Third, it proposes a fundamental framework for network security that consists of eight perspectives of network security and nine attributes of a secure network. The framework approach was adopted at the NRM author's group workshop. The perspectives, termed 'pillars' in this paper, 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 paper then presents a list of the research e orts in high-level security and intrusion resistance and logically argues for their need towards comprehensive network security. A few of the key research areas stressed in this position paper include, (i) the stability of networks under perturbation, (ii) formal proofs of correctness of the algorithms designed to ensure network security, (iii) the use of fuzzy logic and fuzzy thresholds for modeling networks and security criteria, (iv) dynamicity of the parameters constituting the security criteria, over time, to foil intrusion attempts, and (v) the design of innovative schemes aimed at reducing performance impact of security overhead by exploiting key environment or protocol characteristics of the network under consideration.

© 1997 Academic Press Limited

1. Introduction

The computer-driven integration of the fields of (i) communications and (ii) automation and control, has been primarily responsible for the proliferation of today's networks.

email: jerry.s@computer.org; sumit.ghosh@asu.edu

1084–8045/97/030305 + 18 $25.00/0 ma970058 © 1997 Academic Press Limited

Computer networks have grown from a simple time-sharing system—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 civilian 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 tra c. 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. While the successful demonstration of remote surgery by the US Army attests to the capability of today's networks, it also underscores the critical need for network security.

There is an increased reliance on computer networks today that is not necessarily widely known to the general public. In fact, most of us, US residents, 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 our wellbeing and survival. As a result, the risk to the economy, infrastructure and wellbeing of the population, has not necessarily been widely reported. Such complex systems, however, are often vulnerable to failures, intrusion, and other catastrophes. Backhouse and Dhillon [2] estimate the yearly damages to the vulnerable finance and banking sectors in the US 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], 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 industry has become very 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 e ort devoted to produce and enforce security for the privacy and non-repudiation attributes [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 possibly leading to catastrophic loss of electric power in the country, has raised deep concerns about the reliability of networks.

Fundamentally, the reason underlying network security is the value of the information riding on the network. Admiral Grace Hopper [5] had pointed out, as early as in the 1970s, that the industry is engrossed only 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 the 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 a liation and

background—industry, government, or military. Each of the three sectors continue to maintain their individual vocabulary which is built around the perceived threat and cost benefit. However, the distinction is being increasingly blurred by overlapping networks as is highlighted by a recent fact; 90% of the Department of Defence's electronic tra c 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 involved parties to agree on a common framework and revitalize the e orts towards evaluating network security. Recognizing this problem, the National Security Agency, the nation's proponent for computer and network security, organized the First Network Rating Model (NRM) conference in Williamsburg, VA, on March 20–22, 1996 [7]. 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 tra c 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 [8]. While the concepts of 'COMmunications SECurity' (COMSEC) and 'INFOrmation SECurity' (INFOSEC) are well understood within the DoD, they mean little to most of industry and many civilian government agencies. In this paper, 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 the respective 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 o cial 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 'classification'. 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 di erence between the industry, government, and defense perspectives has traditionally hovered around threats and their sources. This di erence is also becoming blurred. To the military, the traditional threat has been the enemy, typically a hostile government or terrorist, whose e orts were aimed at stealing valuable information from the network. Today, however, a new kind of threat, termed 'information warfare' [4], has gained notoriety. It consists of disabling or rendering useless the enemy's key

networks including the command and control [9], power grid [6], financial, and telecommunications networks. In addition, the threat of economic espionage, i.e. 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 paper is organized as follows. Section 2 reviews the current literature on network security. Section 3 presents the key issues in network security while Section 4 enumerates a partial list of key research problems that need to be addressed towards developing a comprehensive network security model. Finally, Section 5 presents some conclusions.

2. Review of current research in network security

The DoD's perspective on trusted computer systems is presented in the Orange Book [8]. Madron [5] presents a generalization of the INFOSEC and COMSEC concepts [8] to network security and provides the following general definitions. Information security (INFOSEC) is defined to consist of procedures and actions designed to prevent, for 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, etc. 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 [10] review the trusted system concepts and reference validation mechanism and explores a new computer architecture to generalize the concepts for distributed systems. Nessett [11] reviews the di culties in authentication and notes the security advantages of centralized authentication during logon in distributed systems. Ping and Lin [12] note that in enterprise networks, the principle security 'areas' include confidentiality, integrity, data-origin authentication, non-repudiation, 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 [13], network security involves the tasks of 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 o masquerading intruders.

Power [9] introduces the notion of information warfare and notes that its scope includes (i) the electronic battlefield, i.e. disruption of enemy command and control, (ii) infrastructure attacks, i.e. failing key telecommunications, financial systems, and transportation, (iii) industrial espionage, i.e. covert operations aimed at stealing proprietary secrets or sabotage of company information network, and (iv) personal privacy, i.e. stolen 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 non-repudiation. Geer [3] also identifies two kinds of possible attacks on EC networks; (i) passive or pure listening and (ii) active or insertion of modified packets. To defeat such attacks, the goals of security must be aimed at preventing tra c 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 [14] remarks that the desired goal in the current computer security paradigm is absolute security. This requires logical and mathematical precision while, unfortunately, 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 [15], the risks in the corporate world include personnel, property, information, and liability. Today's corporations are concerned with (i) protecting financial resources, personnel, facilities, and information, (ii) access control for facilities and management information systems, and (iii) recovery from disaster and continuity of operations. Chambers [16] underscore the di culty in detecting intrusionand 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 [17] 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, thereis neither a widely accepted measure of risk nor is it likely to obtain insurance. Oliver [18] 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 linkageof the information to the individual is concerned. Oliver also addresses the debate as to whether computer users making anonymous statements may be held accountable. Hitchings [19] stresses the need to examine the human issues—cultures of people involved, attitudes, morale, and di erences 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 [20] describe their experiences with recording and analyzing anomalous behavior in computer systems at Los Alamos National Laboratory immediately following an intrusion. Helman and Liepins [21] present a stochastic foundation for and analysis of audit trail analysis. They also suggest several criteria for selecting attributes. Janson and Molva [13] proposes the tracking of system resource usage by authorized users for accounting as well as intruder detection. They enumerate the need to (i) identify objects to which access must be controlled, (ii) identify subjects whose access must be controlled, (iii) identification of the possible threats that must be defeated, and (iv) cataloging of enforcement mechanisms. Lunt and Jagannathan [22] 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 Spa ord [23] 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 [24] 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 [25] 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 [26] 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.

Recently, many computer network experts [1,6] have joined the electric power system researchers in sharing the latter's long-held belief of system availability [27–29] and transient stability [30] as primary security concerns. Fitzpatrick and Hargaden [31] 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 out of their own initiative within the framework of the commander's intent.

An analysis of the current literature reveals the following. First, the nature of the security concerns di ers for each of the sectors—military, government, and industry. Second, this has lead to problems since many of these sectors are forced, for e ciency and economy reasons, to use each others networks. Third, there is the lack of a common framework to describe security and intrusion resistance of networks, an important issue that had dominated the Network Rating Model workshop. Fourth, the traditional security criteria have already been transcended and it has become critically important to address the issues of stability of networks, formal correctness of security algorithms, intrusion resistance, privacy, and other high-level security issues that will be elaborated subsequently in this paper.

3. Issues in network security

Given the wide scope of today's networks and their enormous future potential, the goal to achieve comprehensive network security is challenging. The overall goals of the NRM 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 tradeo s. The workshop was organized to 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 di erent conceptual points of view, termed perspectives in this paper. Although this idea has been referred to as 'disciplines' in the literature, the term 'perspectives' appears to capture the underlying meaning more accurately. Therefore, 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 di erent subset of the perspectives critical based on its own perceived threats.

3.1 *Defining the framework for network security*

The consensus definition of a Network Rating Model is: 'a consistent, cost-e ective 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 a ect 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 di erent 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 e ectiveness criteria 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 di erent dimensions of a secure network while the phrase 'network or combinations of networks' reflects the increasing blur between 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 agreed 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 are systemic, communication, physical, personnel, operational, application, and performance. The services were enumerated as access control, confidentiality, integrity, authentication, tra c flow security, assured service, non-repudiation, anonymity, and intrusion detection. The concerns included accountability, availability, liability, reliability, audit-ability, interoperability, confidentiality, and integrity. These perspectives, services, and concerns were corroborated by Edfors [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 di ering perceptions of the threat sources. Upon careful analysis, it became increasingly evident to the authors that a unified approach to total network security, i.e. 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. The characteristics are referred to as attributes of a secure network and is the result of unifying security services and concerns. Second, a network's security may be viewed at di erent conceptual layers, each view reflecting a threat, being relatively orthogonal of others, and thereby permitting independent development and evaluation. The conceptual layers are referred to as perspectives or 'pillars'. The list of attributes includes privacy, integrity, accountability, availability, reliability, connectivity, recovery from disaster, liability, and uncertainty, and they constitute a superset of the attributes proposed in the literature.

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

Figure 1. Components of Network Security.

A new perspective—'design correctness'—is added to the list of pillars and its characteristics are elaborated in section 3.3. Thus, the list of pillars includes systemic, communication, physical, personnel, operational, application, performance, and design correctness. This orthogonal framework approach was adopted at the second NRM author's group workshop in July 1996.

Conceptually, network security may be viewed as one where 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 resulting security 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 e ective 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.

3.2 *Threats to network security*

In contrast to the classic threats, e.g. the military espionage of the former Soviet Union, hostile governments, and terrorist organizations, the new threats include information warfare [9] and, more recently, the threat of liability law suits, stemming from failure to protect information. While they list threat sources, Edfors [1], Madron [5], and Simonds [32], reveal that the greatest threat has always and continues to be 'insiders'.

Madron estimates that as high as 75% of possible attacks on a network emanate from one or more sources inside the network establishment. In response, both government and industry are emphasizing internal threats. Threats may be leveled at a network corresponding to each of the eight pillars. That is, while a hacker may infiltrate the 'application' pillar and divert financial transactions to a fictitious account, another intruder may attack the 'performance' pillar and render the network virtually unusable. The following is a list of the key threat sources:

- Outside threats including terrorism, hackers, malfeasants, ex-employees, foreign espionage, economic espionage by foreign governments or foreign or domestic corporations, and liability law suits.
- Inside threats including employees, hackers, mischief, legal, and uneducated users.

3.3 *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, and they cumulatively support a network's security. Thus, each pillar corresponding to the eight perspectives, reflect the eight foundation blocks that individually describe 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 di erent 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 are elaborated as follows.

- Systemic encompasses the software that operates the network and constitutes the basic infrastructure of the high-level application software.
- 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 di erent 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. This is possibly the most complex pillar and is further elaborated in Section 4 of this paper.

3.4 *Attributes of a secure network*

Each of the attributes will bear a specific degree of relationship to each of the eight 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 di cult to prosecute a hacker for degrading a network's performance and even more di cult to quantify the degradation and, therefore, determine a commensurate punishment. However, as society acquires a better grip of 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 between the (i) 'Design correctness' pillar and the attributes and the (ii) 'Uncertainty' and 'Liability' attributes and 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 [9,18] is defined as intended for or restricted to the use of a particular person, group or class, on a need-to-know basis. It applies to data, control signals, and tra c flow. Synonymous and associated words in the literature include confidentiality [3,13], disclosure, anonymity [18], classification [8], proprietary, TRANSEC, cryptosecurity, EMSEC, and encryption [5].
- Integrity [3,29] 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 [18] is defined as a statement or exposition of reasons, causes, or motives to furnish a justifying analysis or explanation which can be documented or traced and ownership established. Synonyms and associated words include non-repudiation [29], audit-ability [25], audit trail [25], answerable, authentication [3], signature, and responsibility.
- Availability [13,29] is defined as 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 [13], authentication [3], continuity of service, and confirmation.
- Reliability is defined as generating consistent results during successive trials. Synonyms and associated words include assured service, assuredness, certainty, and dependability.
- Connectivity [33] 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 di erent protocol

driven terminals and host computers. Synonyms and associated words include interoperability, tra c 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 [15] is defined as having to do with legal obligation and responsibility that may a ect 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 [22,25] in a user's behavior through audit trail analysis.

3.5 *Evaluating and rating network security*

To understand the operation of the framework, consider that the military perceives hostile governments as the sources of the primary threats to its networks and data. 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.

The value of the proposed framework is in 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 such that customers are denied from making purchases. An examination of the Performance pillar may be advisable under these circumstances. In a di erent 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 procedure for determining an NRM rating of a network consists of the following: first, 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 (i) the individual values along a row that constitute an evaluation of the corresponding pillar may be examined against a perceived threat level, or (ii) 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. Thus, one may imagine a second hypothetical matrix where the elements reflect the desired security

posture for the network. Clearly, the desired measure will reflect a cost-benefit analysis, i.e. the level of risk that the security management is willing to assume. As indicated earlier, the matrix provides a meaningfully organized framework for the network security evaluation information, in terms of its fundamental characteristics. Thus, to compare the security postures of two or more networks, either (i) the individual values along a row of the corresponding matrices may be examined against each other, or (ii) the values along a column of the corresponding matrices may be contrasted.

It must also be pointed out 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.

4. Research efforts required in high-level security and intrusion resistance

The literature records the use of audit trails, cryptography, and authentication techniques to ensure network security. However, these techniques are essentially confined at the lower level and are ad hoc. Hitchings [19] strongly believes that a new approach to information security is needed. This paper theorizes the need for a logical, high-level approach towards comprehensive network security and argues that the networks and algorithms, underlying the high level applications, must integrate the security concerns into their design. In addition, this paper provides motivations for the subsequent research e orts. The overall approach must continuously monitor the exchange of data between sites and within a site to detect or defeat intrusions and unauthorized activities as well as a fail-safe method for detecting system faults before they become catastrophic. The approach must anticipate the presence of malicious and ignorant users everywhere and not take the validity of any data for granted.

4.1 Stability

Increasingly, experts in computer systems are recognizing the vital role of system availability or stability, a concept that has long been recognized in the electric power community. If an enemy succeeds in degrading the command and control network su ciently, none of the sophisticated cryptographic schemes are useful since no messages will get across the networks. The nation's well being is at risk if an enemy is capable ofrendering the telecommunications network unavailable, without engaging the traditional defense forces or firing a single shot. Stability is linked to the performance and design correctness pillars.

The phenomenal growth of distributed networked systems coupled with their enormous future potential marks a new era in the information age. On the other hand, their ubiquity and our near total dependence for our day to day activities, coupled with their complexity and vulnerability to stability raises a deep concern. The algorithms that underlie the distributed systems are complex and are susceptible to external and environmental disturbances. The well known incidents of unexplained system failures in IBM mainframes despite smooth running for decades, the discovery of previously unknown errors in AT&T network software, and the numerous unreported telephone system failures across the country, all attest to the complexity of the underlying algorithms. A researcher from a major manufacturer of ATM machines acknowledges

that the nation's Automated Teller Network is a collection of patchwork and it is a miracle that it works. The perturbations, even if transient, may degrade the system performance, either lightly or severely, or cause catastrophic failure. It is therefore imperative that the research community undertake serious e orts to understand the issue of stability in depth and synthesize performance metrics.

Recently, Lee [34] has addressed the fundamental property of stability in asynchronous distributed decision-making (ADDM) systems that are the most complex of all distributed algorithms. These algorithms hold enormous promise to solve many real world problems and have been successfully demonstrated for distributed banking [38], intelligent vehicle highway system [36], and railway networks [37]. Lee [34] conducts a thorough survey of research e orts in stability in all relevant scientific disciplines including control systems engineering and carefully reviews Lyapunov's [38] work on stability of motion.

The authors theorize that insider attacks, attempts by foreign intruders, and internal system failures may cause disturbances in the stability of the network which may be detected through continuous monitoring of the stability parameters.

4.2 *Formal proof of correctness*

The NRM workshop witnessed justifiable concern among the participants, relative to assurances of the correctness of the security schemes. Hosmer [14] remarks that the desired goal in the current computer security paradigm is absolute security. Since this requires logical and mathematical precision and as precision and complexity are unfortunately inversely related, the issue of guaranteeing correctness is di cult and elusive. This paper argues that the issue of correctness of a security scheme, implemented in a network, is tied to that the underlying algorithm. While proofs of correctness of distributed algorithms are known to be di cult, there are precedences in the literature [35,39]. Yan [40] presents a quantitative performance modeling e ort for network utilizing fuzzy logic. The authors believe, based on prior experience, that even the more complex, asynchronous, distributed algorithms lend themselves to constructing proofs of correctness, that such proofs must be developed to guarantee the accuracy of the algorithms and ultimately the correctness of the system, and that without such proofs there is the strong likelihood of the algorithms executing erroneously. The issue of formal proof of correctness is linked to the last pillar—design correctness.

The design of the underlying distributed algorithms should also reflect scalability. That is, the algorithms continue to apply and there is no need for a total redesign in the event that the network experiences expansion.

The proof of correctness must take into consideration each of the threats represented by the pillars, account for all possible scenarios to which the network may be subject, examine each of the states to which the network may migrate, and consider all possible internal system failures and input and environmental perturbations. This paper theorizes that upon successfully developing the proof of correctness, the threat to the 'design correctness' pillar will be e ectively addressed.

4.3 *Use of fuzzy logic and thresholds for modeling networks and security criteria*

Given the complexity of the networks and the application programs, classic analytical

modeling may be di cult or impractical. This paper proposes the study and implementation of fuzzy set theory and approximate reasoning to model networks and the security criteria. Corresponding to each security and network criteria, the most important and likely values are identified and expressed through fuzzy sets. Fundamentally, Zadeh's fuzzy set theory [41] provides a robust mathematical framework for dealing with 'real-world' imprecision and non-statistical uncertainty. Given that the present day complex networks are dynamic, that there is great uncertainty associated with the occurrence of attacks and internal system errors, and that they defy accurate analytical modeling, fuzzy logic appears to be a promising approach to address many aspects of security in networks. The advantages of using fuzzy sets are many. First, the use of fuzzy thresholds [42] promises a robust and highly adaptive system. Second, the likelihood of false alarms [25] relative to attacks and penetration is likely to decrease. Third, the modeling in the continuum mathematics of fuzzy sets rather than with traditional, discrete values, coupled with extensive simulation, o ers a reasonable compromise between rigorous analytical modeling and purely qualitative simulation. This study is expected to benefit the last pillar, design correctness, and the last attribute, uncertainty.

This paper also proposes to monitor the stability of networks through the use of fuzzy sets. When subject to perturbations, the system is likely to fluctuate. The variation of the fuzzy set values determine the degree of the system fluctuation, which is then compared against a fuzzy threshold [42] to evaluate the stability of the system.

4.4 *Dynamicity of the parameters constituting the security criteria*

As with cryptosecurity, a key weakness of logical security is time, i.e. an intruder may detect and defeat the security measures in finite time. A number of studies in the literature report on the time intervals required to break the keys to encryption algorithms. Given a key of size 56 bits and a processor performing 1 encryption per microsecond, it would require 1,142 years to break the key. When the processor power increases to 10^6 encryptions per microsecond, the required time drops to 10.01 h [43]. Given enough time, a smart intruder is very likely to determine the logic used in the security checks for the fuzzy thresholds. To defeat such intruders, this paper proposes to develop a basis for dynamically changing the fuzzy set values and the fuzzy threshold function, at appropriate time intervals. As a result of the updates, a potential intruder's e orts to learn the fuzzy thresholds and fuzzy set values may be preempted, forcing him/her to start from scratch and thereby leaving the system unharmed. The frequency of the intervals will be defined by the threat, desired level of security, and other factors. Study in this area is expected to impact the uncertainty attribute.

4.5 *Design of innovative schemes to reduce performance impact of security*

The authors hypothesize that key attributes of specific networks may be exploited to reduce the potential performance impacts that may arise from implementing security measures. To achieve security in ISDN networks, Fernandez and Subbarao [44] claim to implement Rivest-Shamir-Adleman (RSA) encryption algorithm for authentication and Data Encryption Standard (DES) algorithm for encryption, transparent to the user and without any software upgrades to the switch, through embedding the schemes

in the ISDN Customer Premises Equipment (CPE). Given the growing popularity of ATM networks, their future potential, and the lack of comprehensive high-level security characteristics, this paper proposes a study of the hardware and software details against the security requirements of ATM networks. Clearly, this issue is linked to the performance pillar of the framework.

The advantages of an an ATM network include its high speed, small packet size, point to point connection, and virtual path-oriented transmission of messages. Other issues important towards developing security mechanisms include whether the ATM nodes are physically secure, whether the network will be statically configured or permit dynamic reconfiguration, whether routing will be primarily limited to domestic nodes or exploit the less heavily used international nodes, whether commercial carrier links will be utilized, whether the dropped cells, if any, are destroyed thoroughly, and whether the commercial networks will be capable of implementing levels of security. Where the network is dynamic, the procedure for adding and deleting nodes including the authenticity of the control message to add or delete a specific node will impact on security. Where routing occurs through foreign countries, perhaps with di erent communications eavesdropping laws, countermeasures must be designed to protect the information riding on the network. Otherwise, specific bits in the message header may be added at call setup time to (i) ensure that sensitive tra c utilize only domestic carriers while other tra c may propagate unrestricted and (ii) specify encryption requirements or other security services.

5. Conclusions

This paper 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 Network Rating Model (NRM) conference in March 1996 and a subsequent NRM author's group workshop in July 1996. It has proposed a fundamental framework for network security which consists of eight perspectives of network security and nine attributes of a secure network. The framework approach was adopted at the NRM author's group workshop. The perspectives, termed 'pillars' in this paper, 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 paper also presented a list of key research e orts in high-level security and intrusion resistance and logically argued for their need towards comprehensive network security. The authors are currently engaged in applying the security framework to an ATM network to idntify the key security issues and to integrate security measures into the di erent elements of the ATM network. The authors also plan to develop metrics for measuring network stability and to construct proofs of correctness.

6. Acknowledgements

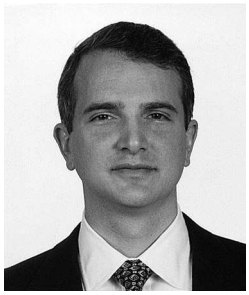
The authors gratefully acknowledge the National Security Agency and to Patricia Edfors of the Justice Department for their help and feedback relative to this paper. The authors also express sincere thanks to the participants of the first and second

NRM workshops. The support by the US BMDO and Army Research O ces under the grant DAAH04-95-1-0101 is gratefully acknowledged.

References

1. Patricia Edfors, Department of Justice, Speaker on 21 March 1996, Network Rating Model Conference, Williamsburg, VA.
2. J. Backhouse and G. Dhillon 1995. Managing computer crime: a research outlook, *Computers and Security*, **14**, 645–651.
3. D. E. Geer 1995. Electronic commerce, banking and you. *Computer Security Journal*, **XI**, 55–62.
4. J. M. Tenenbaum, C. Medich, A. M. Schi man and W. T. Wong 1995. CommerceNet: Spontaneous Electronic Commerce on the Internet. *Proceedings of the IEEE Computer Society International Conference '95 (COMPCON '95)*, 38–43.
5. T. W. Madron 1992. *Network Security in the 90s—Issues and Solutions for Managers*, John Wiley and Sons, Inc., New York.
6. C. C. Baggett 1996. Keynote address *Network Rating Model, First Public Workshop*, March 20–22, National Security Agency, Williamsburg, VA.
7. Network Rating Model (NRM): Strawman, National Security Agency, 20–22 March 1996.
8. Department of Defense 1985. *Department of Defense Trusted Computer System Evaluation Criteria*, 5200.28-STD, Washington, DC.
9. R. Power 1995. CSI special report on information warfare. *Computer Security Journal*, **XI**, 63–73.
10. M. D. Abrams and M. V. Joyce 1995. Trusted System Concepts, *Computers and Security* **14**, 45–56.
11. D. M. Nessett 1989. Layering central authentication on existing distributed system terminal services. *Proceedings of the IEEE 1989 Computer Society Symposium on Security and Privacy*, May 1–3, Oakland, CA., pp. 290–299.
12. P. Lin and L. Lin 1996. Security in enterprise networking: a quick tour, *IEEE Communications Magazine*, 56–61.
13. P. Janson and R. Molva 1991. Security in open networks and distributed systems. *Computer Networks and ISDN Systems*, **22**, 323–346.
14. H. H. Hosmer 1995. Security is Fuzzy! Applying Fuzzy Logic to the Multipolicy Paradigm. *Computer Security Journal*, **XI**, 35–45.
15. S. Hill and M. Smith 1995. Risk management and corporate security, *Computers and Security*, **14**, 199–204.
16. T. Chambers 1995. Case study: a managerial perspective on an Internet security incident, *Computer Security Journal*, **XI**, 17–23.
17. H. B. Wolfe 1995. Computer security: for fun and profit, *Computers and Security*, **14**, 113–115.
18. C. Oliver 1995. Privacy, anonymity, and accountability, *Computers and Security*, **14**, 489–490.
19. J. Hitchings 1995. Deficiencies of the traditional approach to information security and the requirements for a new methodology, *Computers and Security*, **14**, 377–383.
20. R. S. Vaccaro and G. E. Liepins 1989. Detection of ANOMALOUS Computer Session Activity. *Proceedings of the 1989 IEEE Computer Society Symposium on Security and Privacy*, May 1–3, Oakland, CA, pp. 280–289.
21. P. Helman and G. Liepins 1993. Statistical foundations of audir trail analysis for the detection of computer misuse, *IEEE Transactions on Software Engineering*, **19**, 886–901.
22. T. F. Lunt and R. Jagannathan 1988. A prototype real-time intrusion-detection expert system. *Proceedings of the 1988 IEEE Computer Society Symposium on Security and Privacy*, Apr 18–21, Oakland, CA, pp. 59–66.
23. S. Kumar and E. H. Spa ord 1994. *An application of pattern matching model in intrusion detection*, Technical report 94-013, Department of Computer Sciences, Purdue University.
24. B. C. Soh and T. S. Dillon 1995. Setting optimal intrusion-detection thresholds, *Computers and Security*, **14**, 621–631.

25. T. F. Lunt 1993. A survey of intrusion detection techniques. *Computers and Security*, **12**, 405–418.
26. S. Weerasooriya, M. A. El-Sharkawi, M. Damborg, and R. J. Marks II 1992. Towards static-security assessment of a large-scale power system using neural networks. *IEE Proceedings, Part C, Generation, Transmission, and Distribution*, **139**, 64–70.
27. R. Billington and E. Khan 1992. A Security Based Approach to Composite Power System Reliability Evaluation, *IEEE Transactions on Power Systems*, **7**, 65–71.
28. Computer Sciences Corporation 1994. *UCA and DIAS information security analysis, EPRI technical report TR-103773*, Aug, Electric Power Research Institute, Palo Alto, CA.
29. S. A. Klein and J. N. Menendez 1993. Information security considerations in open systems architecture, *IEEE Transactions on Power Systems*, **8**, 224–229.
30. J. A. Pecas Lopes, F. P. Maciel Barbosa, J. P. Marques de Sa and J. M. G. Sa da Costa 1987. A new approach for transient security assessment and enhancement by pattern recognition. *Proceedings of the Second European Workshop on Fault Diagnostics, Reliability, and Related Knowledge Based Approaches*, April 6–8, Pergamon Press, pp. 189–215.
31. S. K. Fitzpatrick and P. J. Hargaden 1994. Multimedia communications in a tactical environment. *Proceedings of the IEEE MILCOM*, **1**, 242–246.
32. Fred Simonds 1996. *Network Security*, New York: McGraw-Hill.
33. L. Guidoux 1995. Intelligent Solutions for Data Communications Networks, *Telecommunications, International Edition*, **29**, 25–29.
34. Tony Lee 1996. On the Concept of 'Stability' in Asynchronous, Distributed, Decision-Making Systems, Ph.D. Thesis, Brown University, Providence, RI 02912.
35. Sumit Ghosh 1993. NOVADIB: a novel architecture for asynchronous distributed real-time banking modeled on loosely-coupled parallel processors, *IEEE Transactions on Systems, Man, and Cybernetics*, **23**, 917–927.
36. Noppanunt Utamaphethai and Sumit Ghosh 1996. DICAF, a high performance, distributed, scalable architecture for IVHS utilizing a continuous function—Congestion Measure, *IEEE Computer*.
37. Raj V. Iyer and Sumit Ghosh 1995. DARYN, a distributed decision-making algorithm for railway networks: modeling and simulation, *IEEE Transactions on Vehicular Technology*, **44**, 180–191.
38. A. M. Lyapunov 1992. *The General Problem of the Stability of Motion*, Taylor & Francis.
39. Sumit Ghosh 1996. On the proof of correctness of yet another asynchronous distributed discrete event simulation algorithm (YADDES). *IEEE Transactions on Systems, Man, and Cybernetics*, **26**, 68–74.
40. B-P Yan 1994. An HGF integrated evaluation method for computer network. In: *Proceedings of the IEEE Singapore ICCS '94 Conference*, Nov 14–18, Singapore, Vol. 1, pp. 86–89.
41. L. A. Zadeh 1965. Fuzzy Sets. *Information and Control*, **8**, 338–353.
42. A. R. Bonde and Sumit Ghosh 1994. A comparative study of fuzzy versus fixed thresholds for robust queue management in cell-switching networks, *IEEE/ACM Transactions on Networking*, **2**, 337–344.
43. William Stallings 1996. *Practical Cryptography for Data Internetworks*, IEEE Computer Society Press.
44. I. B. Fernandez and W. V. Subbarao 1994. Encryption based security for ISDN Communication: Technique and Application, IEEE SOUTHEASTCON '94, pp. 70–73.



H. J. (Jerry) Schumacher is a Major in the US Army and is currently working on his PhD in computer science at Arizona State University. He received his Bachelor's Degree from West Point in 1983 and his Master's Degree in Computer Science from Georgia Tech in 1987. He has held several positions in the automation/communications arena in the US Department of Defense: Computer Engineer, Army Computer Engineering Center 1988–90, Executive O cer, Defense Information Systems Agency 1991–93 and Operations O cer, Network Operations Center, White House Communications Agency 1993–95. His interests are in security, ATM networks, and distributed algorithms.

Sumit Ghosh is currently an associate professor and the associate chair for research and graduate programs in the Computer Science and Engineering Department at Arizona State University. He had received his BTech degree from IIT Kanpur, India, and his MS and PhD degrees from Stanford University, California. Prior to his current assignment, Sumit had been on the faculty at Brown University, Rhode Island, and before that he had worked at Bell Labs Research in Holmdel, New Jersey. Sumit's research interests are in fundamental problems from the disciplines of asynchronous distributed algorithms, modeling and distributed simulation of complex system, networking, network security, computer-aided design of digital systems, continuity of care in medicine, and metrics to evaluate advanced graduate courses. Presently, he serves on the editorial board of the IEEE Press Book Series on Microelectronic Systems Principles and Practice. Sumit is a US citizen.