SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks (2012)
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.623

RESEARCH ARTICLE

A taxonomy framework based on ITU-TX-805 security architecture for quantitative determination of computer network vulnerabilities

Shahriyar Mohammadi[1], Mohammad Hussein Sherkat[2]* and Mona Jamporazmey[2]

[1] Department of Industrial engineering, Khajeh Nasir Toosi University of Technology (KNTU), Tehran, Iran
[2] Management School, University of Tehran, Tehran, Iran

ABSTRACT

Network vulnerability taxonomy has become increasingly important in the area of information and data exchange for its potential use not only in identification of vulnerabilities but also in their assessment and prioritization. Computer networks play an important role in information and communication infrastructure. However, they are constantly exposed to a variety of vulnerability risks. In their attempts to create secure information exchange systems, scientists have concentrated on understanding the nature and typology of these vulnerabilities. Their efforts aimed at establishing secure networks have led to the development of a variety of methods and techniques for quantifying vulnerability. The objectives of the present paper are twofold: (1) to develop a taxonomy framework for the classification of network vulnerabilities on the basis of the ITU-TX-805 security architecture and (2) to develop a method on the basis of the second edition of Common Vulnerability Scoring System for the quantification of vulnerabilities within the proposed taxonomy framework. It is expected that the framework proposed in this paper will provide a comprehensive taxonomic structure that can be extended to all the different aspects of network vulnerability. Furthermore, it will help in the identification and effective management of vulnerabilities by their quantification. Copyright © 2012 John Wiley & Sons, Ltd.

KEYWORDS
vulnerability; computer network vulnerability; taxonomy of vulnerabilities; ITU-TX-805 security architecture; quantifying vulnerabilities; Common Vulnerability Scoring System

***Correspondence**
Mohammad Hussein Sherkat, Management School, University of Tehran, Tehran, Iran.
E-mail: mh_sherkat@yahoo.com

1. INTRODUCTION

In our modern world, private companies, government agencies, and non-government organizations are increasingly storing their vital information in the form of databases on local and global computer networks that make data available any time anywhere. Like any other computer system, however, these computer networks are not entirely safe and may suffer from a variety of weaknesses and inadequacies that make them vulnerable to hacking, data theft, or ultimate collapse. The aggregate of these problems have been termed “computer network vulnerabilities” [1].

Vulnerability provides a potential backdoor for penetration by attackers. Once abused, it will lead to an undesired and incorrect behavior [2]. According to Ramakrishnan and Sekar, vulnerability is an inadequacy or weakness in the system that can be exploited to jeopardize system security [3]. Bishop considers vulnerability as a system characteristic that potentially causes its abuse while it can be itself the result of one or more attacks or abuses [4]. Ammann *et al.* define vulnerability as any feature of a computer system that makes it possible to violate system security policies [5]. In a different definition, Bishop views vulnerability as existing weaknesses in a system security that allows for its abuse and threaten its information integrity by attackers [6].

In order to secure immune networks, it is essential to determine the causes and types of vulnerabilities and to calculate them quantitatively. These requirements, in turn, warrant an effective taxonomy of vulnerabilities that will facilitate the vulnerability identification process and that provide effective management resources to confront vulnerabilities.

In this paper, efforts will be made to provide a framework for the classification of network vulnerabilities based on the ITU-TX-805 security architecture. Compared to similar frameworks and security architectures, the ITU-TX-805 security architecture is not only more comprehensive but also applicable to most network types while it provides a top–down view of network security for components, services, and network applications to identify, prevent, and remedy vulnerabilities [7]. In this paper, a method named Network Common Vulnerability Scoring System (NCVSS) will also be developed on the basis of the second edition of the Common Vulnerability Scoring System (CVSS) that will be used to calculate vulnerability based on the proposed taxonomy.

The remainder of this paper is organized as follows. In Section 1, the literature on vulnerability taxonomy will be reviewed. In Section 2, the proposed taxonomy framework and vulnerability quantification method will be introduced. In Section 3, the research methodology employed will be presented followed by a description of the research framework, research population and sample, and the reliability and validity of the proposed taxonomy framework. In Section 4, the data gathered from a survey will be analyzed. Section 5 discusses a sample of quantitative calculations using the proposed method along with a case study. Finally, results and conclusions will be presented in Section 6.

2. LITERATURE REVIEW

Developing an effective classification system and a common language are important and necessary prerequisites to the systematic study of a new field [8]. Stressing the importance of vulnerability classification, Krsul maintains that proper classification categories should have four features: objectivity, determinism, repeatability, and specificity [9]. Lough adds the features of being structured, integrity, clarity, and efficiency in any type of classification and believes that by providing common concepts, a classification system provides a structured way of viewing, analyzing, and assessing vulnerabilities [10].

Bishop maintains that the first step in understanding vulnerabilities is to classify them on the basis of their characteristics because taxonomy classifies a large number of vulnerabilities according to an understandable grouping [6]. According to Bisbey and Hollingworth, one of the goals for vulnerability taxonomy is to develop auto-tools for assessing security [11]. Mirkovic and Reiher stated that taxonomy of vulnerabilities provides a means for discovering gaps and unknown attacks [12].

However, no single taxonomy is proposed in the literature. The first classification in the area of vulnerability dates back to 1967 in the US where the Federal Government forced computational centers to investigate software vulnerabilities, especially those related to operating systems [13].

Abbott and his research group conducted the RISOS research project in order to understand security problems of existing operating systems and proposed appropriate solutions to enhance their security [14]. In their project, the classification criteria were based on the problems and vulnerabilities created during the programming and code generation process. Another classification is production analysis (PA) conducted in 1978 in order to produce safe operating systems. PA research focused on protection errors in four operating systems and their identification techniques. In this project, four main categories of security gaps were identified in operating systems that included domain, validation, naming, and serialization [11].

Ristenbatt developed an identification method named network communication vulnerability assessment (NCVA) for assessing network vulnerabilities [15]. NCVA methodology uses two taxonomies. The first involves classification of different types of networks on the basis of their design, whereas the second introduces capabilities or features that are subject to susceptibility. Ristenbatt distinguished between susceptibility and vulnerability and concentrated on the classification of system features that might be the target of attackers. This taxonomy comprises five layers (topology, physical layer, data transfer layer, network layer, and control and management layer). Potential features determined in every layer can be targeted by attackers.

Landwher *et al.* provided a classification for security gaps in computer programs. Their objective was to help designers and producers of software systems to produce safe products. They conducted a comprehensive investigation of the history of software errors as well as software life cycle [16]. In their study, Landwher *et al.* used 50 case studies in a variety of computational environments and classified software gaps from the three viewpoints of gap emergence, location, and time of occurrence.

Aslam developed a classification system for software errors of the UNIX operating system. These categories had no overlaps and provided a database for identifying vulnerabilities. In his classification, security gaps were explained in the three categories of configuration, synchronization, and condition validation [17].

Du and Mathur classified vulnerabilities of computer networks into seven categories that included validation, authentication, verification, serialization, boundary checking, domain, weak and incorrect designing, and other extractable logical discrepancies. The purpose of their classification was to persuade vendors of attack discovering systems and firewalls to produce products that are capable of discovering all possible attacks that abuse these vulnerabilities [18]. They maintained that vulnerability did not depend on mutual exclusivity. They also believed that grouping vulnerabilities in a single class would lead to loss of data as a result of abstraction.

Bishop described vulnerability in a way that is useful for intrusion detection mechanisms. In his study, vulnerabilities are classified on the basis of their nature, time of occurrence, resulting abuse, effects resulting from vulnerability, minimum number of vulnerable components, and source of vulnerability identified [19].

Kamara *et al.* also attempted to provide a taxonomy framework for vulnerability analysis in firewalls, based on the classification presented by Du and Mathur. This framework may be considered as an example of using a taxonomy system for the security analysis of other systems [20].

Pothamsetty and Akyol provided a taxonomy structure in the domain of protocol vulnerabilities. The purpose of their study is to identify vulnerabilities based on the characteristics or operations of software protocols that probably have gaps in them in order to identify and prevent vulnerabilities.

To the extent that their focus is on software protocols, their taxonomy is similar to those of PA and RISOS [21].

Weber *et al*. (2005) proposed a taxonomy of software gaps. Like the taxonomy proposed by Lanthower *et al*., theirs is based on how gaps emerge [22].

Hamed and Al-shaer developed a taxonomy for network security policy inconsistencies that may potentially lead to vulnerability in a system or between different active systems in different network environments [23].

With the importance attached by network specialists to diagnosing and combating the dangers of distributed denial of service (DDoS), Asosheh and Ramezani proposed a taxonomy of DDoS potential and active attacks based on *K*-mean algorithm. They used *K*-mean clustering algorithm to cluster and label clusters for vulnerability classification [24].

Wiesauer and Sametinger surveyed the literature on software vulnerabilities in order to define software taxonomy vulnerabilities and extracted attack patterns. A main feature of their work is the development of a combined taxonomy based on attack patterns that make it possible to classify and identify combined attacks. Another major feature of their work is its simple taxonomy structure that makes it usable by non-professional users [25].

Stressing the lack of taxonomic systems in the field of wireless network vulnerability and the inefficiency of the existing taxonomies for use in these networks, Ryoo *et al*. attempted to develop an appropriate taxonomy for such networks. One of the features of their proposed taxonomy is its hierarchical and multi-dimensional structure that not only allows for the classification of known vulnerabilities in the field of wireless networks but has the additional capability of accommodating future vulnerabilities as well [26]. Radmand *et al*. added other dimensions to the taxonomy developed by Ryoo *et al*. [27].

Zeidanloo *et al*. presented a taxonomy technique for Botnet attacks. Botnets are networks of infected computers that are controlled by a set of instructions through a software system that is installed intentionally and is controlled by a malicious computer. Botnets may have legal operations, but in most cases, they involve criminal activities for publishing spam, malware, or identification theft attacks. When a computer is infected by botnet software, it is not able to execute owner commands or may refuse to implement them. In the taxonomy technique presented, the two approaches of honey nets and intrusion detection system are used [28].

Table I provides a summary of the main vulnerability classification types and their key features. The studies reported in this literature review and the results summarized in Table I reveal that the following criteria have been used in the vulnerability taxonomies presented so far:

- Vulnerability classification according to the approach employed in vulnerability abuse.
- Classification of vulnerabilities based on software and hardware components and the relationships that cause vulnerability.
- Classification of vulnerabilities based on their nature and causes.
- Classification of vulnerabilities based on time of occurrence.
- Classification of vulnerabilities based on scope.

Given the fact that the objectives of vulnerability analysis in network security is to identify and discover attacks before the event, it follows that vulnerabilities should be studied and classified in a manner that their role in attacks is duly identified and determined. Moreover, while taxonomies should be comprehensive, generalizable to a variety of situations, and capable of determining the role and effect of network vulnerabilities in attack events, they should be able to specify the effects causing the violation of network security features following a vulnerability abuse event [1]. Accordingly, one of the shortcomings of previous studies may be claimed to be the lack of a multi-dimensional and hierarchical structure in the vulnerability taxonomies developed. It was seen earlier that only one study had included this feature in its proposed taxonomy (i.e., that of Ryoo *et al*.), whereas all other taxonomies had only one single layer or a singly dimensional nature.

3. PROPOSED FRAMEWORK

On the basis of what was mentioned in the previous section, this section attempts to provide a professional taxonomy framework for network vulnerabilities. In addition to being comprehensive and generalizable, the proposed framework is capable of providing a scalar or quantitative vulnerability computation base in the taxonomy structures while it is also able to determine the effects resulting from security feature violations.

For the purposes of this study, which is aimed at developing a taxonomic system for the classification of network vulnerabilities, the requirements for an efficient network vulnerability classification have been investigated from three different perspectives: first, the potential threats and the protection measures required to confront them; second, the components and features in the network structure that may be prone to vulnerability and that need to be protected; and third, the vulnerable activities in the network that may need protection. In this study, these three perspectives are considered severally under the rubrics of threats, components, and network activities, respectively, within the proposed taxonomy framework.

The ITU-TX-805 security architecture has been used in this study in order to handle these three components simultaneously. Figure 1 displays a schematic view of the ITU-TX-805 security architecture. The reasons for using this architecture in the proposed framework may be summarized as follows:

(1) The architecture in question is designed in such a way that it is applicable to all networks and applications and is properly responsive to security concerns

Table I. Summary of the main taxonomies in the vulnerability domain.

#	Researcher/s	Taxonomy criterion	Thematic focus	Feature
1	Abbott [14]	Problems and vulnerabilities of programming time and production of program code	Operating systems	Single layer
2	Bibsy and Hollingworth [11]	Protective errors in the use process	Operating systems	Single layer
3	Ristenbatt [15]	Designing network and vulnerable features	Networks	Single layer
4	Landwehr *et al.* [16]	Existence, place of gap and time of its production	Software	Single layer
5	Aslam [17]	Problems and vulnerabilities of programming time and production of program code	UNIX operating system	Single layer
6	Bishop [4]	Problems and vulnerabilities of programming time and production of program code	Software	Single layer
7	Du and Mathur [18]	Types of attacks and vulnerabilities of fire wall	Networks	Single layer
8	Bishop [19]	Nature, time of occurrence, abuse, effect, minimum numbers of vulnerable components, identification source	Public	Single layer
9	Kamara *et al.* [20]	Types of attacks and vulnerabilities of fire wall	Firewalls	Single layer
10	Pothamsetty and Akyol [21]	Available gaps in the software protocol	Protocols	Single layer
11	Weber *et al.* [22]	Manner of emergence and causes of its emergence	Software	Single layer
12	Hamed and Al-Shaer [23]	Inconsistency of security policy	Networks	Single layer
13	Asosheh and Ramezani [24]	Dangers resulted from distributed denial of service	Networks	Single layer
14	Wiesauer and Sametinger [25]	Attacks pattern	Software	Single layer
15	Ryoo *et al.* [26]	Manner of emergence and causes of its emergence	Wireless networks	Hierarchy and multi-dimensional
16	Zeidanloo *et al.* [28]	Honeynets and intrusion detection systems	Botnets	Single layer

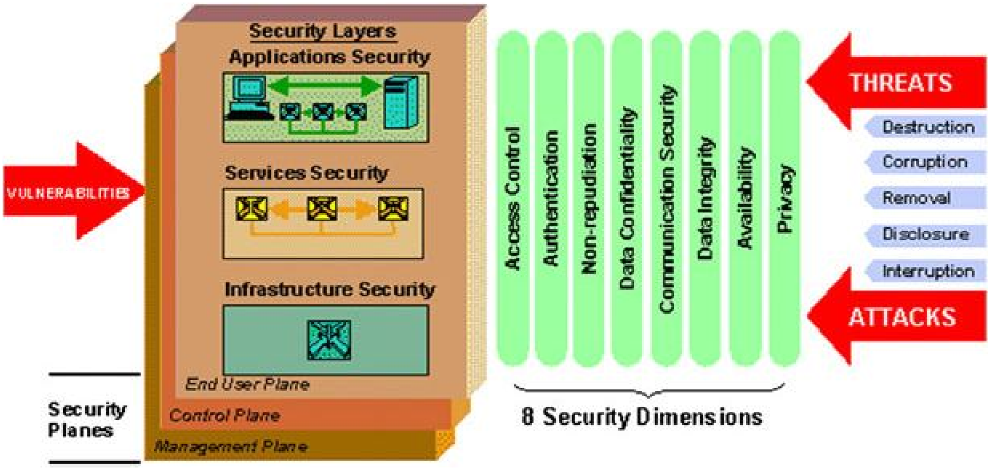


Figure 1. ITU-TX-805 security architecture [29].

related to the management and use of infrastructure, services, and network applications.

(2) It provides a comprehensive and top–down view of network security for items, services, and network applications [29].

With the structure of the ITU-TX-805 security architecture, the three perspectives considered in the proposed framework are handled by three main components of the ITU-TX-805 architecture, namely security dimensions, security layers, and security planes. Security dimensions comprise the set of security measures designed to determine a specific aspect of network security. In this architecture, eight sets specified in the security dimension provide protection against major security threats. To provide an exhaustive security solution, one should be able to use security dimensions designated as security layers for the hierarchical structure of equipments and network components. Accordingly, three security layers of infrastructure, service, and application are defined in this architecture. Each layer is built on another layer to provide a comprehensive solution. In these conditions, the infrastructure layer activates the service layer, which, in turn, activates the application layer.

The security architecture indicates that each layer has its own vulnerabilities. Security planes are the main groups of network activities that are protected by security dimensions. In this architecture, three security planes are defined to provide three groups of activities in the network. These planes are designated as management plane, control plane, and end-user plane. Application of the eight security dimensions to the planes and layers leads to an integrated view and the ultimate formation of 72 individual security views so that different aspects of a security gap or vulnerability can be squarely assessed.

With the aforementioned considerations, a three-dimensional classification structure is proposed that can simultaneously include the three aforementioned components within the ITU-TX-805 security architecture. The number of dimensions may be increased where necessary. The first dimension of the classification identifies the group of network components (equipment or network facilities) to which the vulnerability is related. The second dimension determines the category of network activities to which the vulnerability belongs. Finally, the third dimension determines the group of security dimensions responsible for the vulnerability leading to specific dangers, threats, or attacks. The first level of each of the three dimensions is based on the dimensions of the ITU-TX-805 security architecture. Any number of levels may be devised for each of these dimensions as may be necessary. For illustration, Table II shows the items applicable to the second level of the three proposed dimensions based on those proposed by McGee *et al*. and Hajian *et al*. [7,29].

❖ The first dimension: As can be seen in Table II, the first level of network components comprises network infrastructure, services, and applications. The network infrastructure consists of individual elements and communication facilities in the network. In fact, network infrastructure is the main component that constitutes networks, services, and applications. It can, therefore, be imagined to be subdivided into network components, communication facilities, and platforms. Network components mean all software and hardware elements, such as rotors and switches, that constitute a network [29].

Communication facilities consist of the communication links that connect network components. These links can be of different types, depending on network properties. Platforms include all network components such as the operating systems of rotor, switches, servers, and so on. Network services are further subdivided into the five categories of basic transport services, base protocols, base services, application services, and value-added services. Network application includes the two categories of base applications and advanced applications [7]. As already mentioned, this subclassification may continue endlessly. With the use of the aforementioned procedure, a new group can be set up where there is no

Table II. The first and second layers in the proposed taxonomy.

Dimension	First layer	Second layer
Network components	Network infrastructure	Network components, communication facilities, platforms (operating systems, databases)
	Network services	Basic transport services, basic protocols, basic services, value-added services.
	Network applications	Advanced applications, basic applications
Network activities	Management activities	Operational, maintenance, logistics, configuration, security
	Control activities	Send/receive control information, processing control information, updating control information
	End-user activities	Using a network that is provider of connection, using network services, using network applications
Network security aspects	Access control	Access permission list, detection and prevention of intrusion systems, and role based access control
	Authentication	Usernames and passwords, Kerberos, X.509
	Nonrepudiation	File access to web services, detection and intrusion prevention system, digital signature
	Data confidentiality	Encryption (3DES, AES), lists of access permissions, file permissions
	Communications security	VPN communications, MPLS channels, private lease lines
	Data integrity	Message validation codes such as HMAC and CRCs
	Availability	Redundancy and backup, firewalls, detection and intrusion prevention system
	Privacy	Proxies, NAT services, identity preservation services, making anonymous

3DES, triple data encryption standard; AES, advance encryption standard; VPN, virtual private network; MPLS, multiprotocol label switching; HMAC, hash-based message authentication code; CRC, cyclic redundancy code; NAT, network address translation.

specific group for a product so that special versions can be accommodated in each group.

- The second dimension: This dimension allows all network activities to be categorized and ascribes a specific vulnerability to the relevant activities of network components specified in the first dimension. The first level of the network activities includes managerial activities, control activities, and end-user activities.

  Managerial activities are recognized as one of the main types of network activities that are often periodically conducted by a network manager or network security manager. These activities cover all operational, maintenance, logistics, and configuration activities as well as security issues related to the infrastructure elements, services, and network applications [29].

  Control activities are those that provide effective and efficient delivery of data, services, and applications throughout the network. They often involve information on machines relations (such as rotors and switches) used to determine the best route for data transfer throughout the network [29]. Such information is called control or signaling information. Hence, most control activities involve the transfer, receipt, updating, and processing of control or signaling information for the effective and efficient delivery of information, services, and applications throughout the network [7].

  End-user activities involve user's access and use of network service providers for such purposes as using a connection provider network or net-based services and applications [29]. In these activities, the users' information flow is of great importance. Users' data transfer through network components or communication lines, users voice signals on Voice Over Internet Protocol (VOIP) services, and users' credit card number data used by e-commerce applications are examples of end-user data related to infrastructure, services, and network applications [29].
- The third dimensionThe third dimension identifies the group of security dimensions to which vulnerabilities leading to danger, threat, or attack belong. The first level of this dimension includes eight security dimensions specified in the ITU-TX-805 security architecture. Each security dimension also is further divided into subcategories according to the mechanisms used. It is essential to determine security aspects at risk in a specific vulnerability event for both the assessment of the security weakness in the network and assignment of the security measures required for confronting the specific vulnerability. Each specific vulnerability may threaten just more than one security dimension, may be related to several types of activity, or may even include more than one of the network components. Because most vulnerabilities encountered nowadays are of a combined nature (i.e., a combination of different services or of a service and a network infrastructure component or application), the proposed taxonomy covers these kinds of vulnerabilities.

3.1. Quantification of vulnerabilities in the proposed taxonomy

Quantitative assessment of vulnerability for each vulnerability dimension in computer networks is of great importance. This is because the more vulnerable a network dimension, the greater is its potential for abuse by attackers. Ghorghe and Vamanu proposed a practical general framework for quantitative assessment of system vulnerabilities. In this framework, the amount of vulnerability of a system is measured quantitatively and reported as a figure between 0 and 100 [30]. Alhazmi and Malaiya introduced "vulnerability density" as a criterion for quantitative vulnerability assessment and prediction of the discovery rate of future vulnerabilities [31]. Emami and Jafarian developed a framework to compute vulnerability in open text database management systems. In their study, they used number of vulnerabilities, number of current versions, and system popularity for computing vulnerability rate in open text database management systems and used their proposed framework to compute vulnerability rates in Firebird, Ingres, PostgreSQL, and MySql [32].

The CVSS has been used for the quantitative computation of network vulnerabilities in the security dimension of the

Table III. Corresponding components in the proposed taxonomy and the Common Vulnerability Scoring System (CVSS) base metrics.

Components of the first level of the third dimension in the proposed taxonomy	Base criteria in CVSS
Access control	Access vector (AV)
Authentication	Authentication (AU)
Nonrepudiation	—
Data confidentiality	Confidentiality impact (C)
Communications security	—
Data integrity	Integrity impact (I)
Availability	Access complexity (AC)
Privacy	Availability impact (A)

Table IV. The base metrics components of the Network Common Vulnerability Scoring System (NCVSS) approach and the corresponding ones in the proposed taxonomy.

Components of the first level of the third dimension in the proposed taxonomy	Base criteria of NCVSS
Access control	Access vector (AV)
Authentication	Authentication (AU)
Nonrepudiation	Activity verification (AF)
Data confidentiality	Confidentiality impact (C)
Communications security	Communications security (CS)
Data integrity	Integrity impact (I)
Availability	Access complexity (AC)
Privacy	Availability impact (A)

taxonomy structure proposed in the present study. CVSS was first introduced in 2007 for quantitative determination of vulnerability by the Forum of Incident Response and Security Teams (FIRST).

Common Vulnerability Scoring System is composed of the three standard groups of base metrics, temporal metrics, and environmental metrics, each of which further includes a set of other subcriteria. Base metrics are the main features of a vulnerability that are constant over time and do not depend on the user environment. In contrast, temporal metrics change over time but do not vary from one user environment to another. Environmental metrics are exclusively characteristic of a special environment [33].

One aspect of the CVSS approach is its simplicity, which makes it easy to understand. Once appropriate values are assigned to the base metrics, the base equation in this approach will take a value between 0 and 10 and will form a vector. The vector is a textual string including the values assigned to each criterion. This makes it easy for users to read the value assigned to each criterion so that they can confirm its validity if necessary. Temporal and environmental metrics are optional, but by assigning appropriate values, they can be used to modify the base metrics values. The use of temporal and environmental metrics can reflect more accurately the risk associated with a given vulnerability; however, it may not be necessary to use such metrics, and depending on the objectives, it may suffice to use the base metrics only [33].

Table V. Base Metrics in the Network Common Vulnerability Scoring System method.

Criterion	Characteristic	Description
Access vector	LAN	In cases of vulnerability that are exploitable only with local access. Attackers with physical access to vulnerable systems require a local account.
	W-LAN	Attacker should be in the domain of a wireless network.
	Internet network	In vulnerability cases that are extractable via the internet, the attacker does not need to have access to LAN or placed in the domain.
Access complexity	High (H)	Access conditions are needed. In these cases, the attacker needs high-level skills, needs the information required for the activity not accessible manually, and must use specialized software.
	Medium (M)	Access conditions are somewhat specialized. In these cases, the attacker must have skill and information collected from within the network to act. The network has no default settings or arrangements.
	Low (L)	There are no professional access conditions. In this case, little skill is needed, penetration to the network is possible manually without any special software, and there is no need for additional information to exploit the network.
Authentication	Multiple (M)	The attacker exploiting the vulnerability should confirm authenticity two times or more (even if the same password and username are used).
	Single (S)	An authenticity confirmation is required to access and exploit the vulnerability.
	None (N)	There is no need for authenticity verification to exploit the vulnerability.
Activity verification	Multiple (M)	There are many ways to verify activities in the system.
	Single (S)	There is one way to verify activities in the system..
	None (N)	There is no way to prevent denial.
Confidentiality impact	None (N)	It has no effect on the system privacy.
	Partial (P)	There is considerable information disclosure, and access to some system files is possible, but either the attacker has no control over anything that he obtains or the loss domain is limited; an example is the vulnerability that can disclose special tables of databases.
	Complete (C)	All system files have been disclosed, and the attacker can read all the system data.
Communications security	Multiple (M)	There are many layers to provide communications security.
	Single (S)	There is one layer to provide communications security.
	None (N)	There is no solution to secure communications.
Integrity impact	None (N)	It has no effect on the information integrity (no change can be made in the information or available files on the active system in the network).
	Partial (P)	Changing some files or information is possible, but the attacker has no control over things that can be changed, or the domain that the attacker can affect is limited.
	Complete (C)	Attacker can change any file.
Accessibility	None (N)	It has no impact on system accessibility
	Partial (P)	Causes interruptions for authorized users' access or decrease efficiency.
	Complete (C)	Others' access to the network is disconnected because of the attack.

A number of studies have been so far conducted to customize the CVSS base model for use by organizations, for vulnerability computations for different purposes, and for enhancement of the model's efficiency. Mell and Scarfone (2007, 2009) made efforts to determine the efficiencies and inefficiencies of the CVSS model and to adapt it to certain applications [34,35]. Fruhwirth and Mannisto (2009) focused on customizing the CVSS base model for application by different organizations with enhanced benefits from its capabilities [36]. Gallon (2010) studied the effects of environmental metrics on the efficiency of the CVSS model. He also suggested mechanisms that take full account of environmental metrics in the base equation as the main factor in customizing the CVSS model [37]. Harda *et al.* (2010) studied the significance of environmental metrics for customizing the CVSS base model and the role of target distribution criterion as a customizing factor in accounting for the effects of environmental conditions in each organization in the process of effective vulnerability computations by the model [38].

Hoump and Franqueira used the CVSS model to develop a model for predicting the probability of vulnerability occurrence and the associated risk in organizations [39]. In this model, two indices of abuse repetition and effect of vulnerability abuse are used to predict vulnerabilities on the basis of the Markov process. With the use of this approach, vulnerabilities can be transformed into services needed to deal with vulnerabilities [39]. The vulnerability abuse repetition index is calculated on the basis of base and temporal metrics, whereas the vulnerability abuse effect index is calculated on the basis of base and environmental metrics.

Comparison of the characteristics used in the CVSS base metrics and the items proposed for the first level of the third dimension in our proposed taxonomy indicates that the structure of the CVSS base metrics closely matches that of our proposed taxonomy and that CVSS can be duly modified to compute network vulnerabilities on the basis of the taxonomy structure proposed in the present study. The method proposed here is called NCVSS. Table III compares the components of the first level of the third dimension in our proposed taxonomy and the criteria of the CVSS model.

Clearly, there are certain items in components of the proposed taxonomy that do not have corresponding ones in the base metrics of CVSS. These gaps are in the fields of Nonrepudiation and Communications Security. As shown in Table IV, two new variables in the base metrics have been introduced in the proposed approach (NCVSS) to resolve this problem.

With the aforementioned considerations, base metrics and their characteristics in the CVSS model are proposed within the framework of the NCVSS method as presented in Table V. It is clear from Table V that the two criteria of Activity Verification and Communications Security are added to the base metrics in the proposed NCVSS method. Characteristics and definitions of these criteria are presented in the table. The other base metrics in the two NCVSS CVSS models are the same. Regarding the temporal and environmental metrics,

Table VI. Temporal Metrics in the Network Common Vulnerability Scoring System method.

Criterion	Characteristic	Description
Exploitability	Unproven (U)	No exploit software or tools are available, or an exploit is entirely theoretical.
	Proof ofconcept (POC)	Proof-of-concept exploit code or an attack demonstration that is not practical for most systems is available. The code or technique is not functional in all situations and may require substantial modification by a skilled attacker.
	Functional (F)	Functional exploit tools and software are available. These tools and software work in most situations where the vulnerability exists.
	High (H)	Extensive and comprehensive tools and software along with their details are available for all individuals and its use is simple and widely used.
	Not defined (ND)	Assigning this value to the metric will not affect the score.
Remediation Level	Official fix (OF)	The organization has an official and defined solution.
	Temporary fix (TF)	Organization to act to provide a temporary solution.
	Workaround (W)	The organization requires taking the time to determine a possible solution to resolve the problem but the problem is solvable.
	Unavailable (U)	A solution is not available or its application is impossible.
	Not defined (ND)	Assigning this value to the metric will not affect the score.
Report confidence	Unconfirmed (UN)	There is a single unconfirmed source or possibly multiple conflicting reports. There is little confidence in the validity of the reports.
	Uncorroborated (UR)	There are multiple non-official sources, possibly including independent security companies or research organizations. At this point, there may be conflicting technical details or some other lingering ambiguity.
	Confirmed(C)	Vulnerability is approved by authorities.
	Not defined(ND)	Assigning this value to the metric will not influence the score.

DOI: 10.1002/sec

they have similar criteria and characteristics in both models. Temporal and environmental metrics and their characteristics are provided in Tables VI and VII.

In order to quantify the results and to assign scores to vulnerabilities, the base equations of CVSS model have been revised within the framework of the NCVSS approach. As a result of this, the criteria of Activity Verification and Communications Security have been added to the computational structure of the CVSS model. Also, in the NCVSS approach, temporal and environmental equations similar to those in the CVSS model have been used. Table VIII presents the computational structure of the base, temporal, and environmental equations in the proposed approach (NCVSS).

4. RESEARCH METHODOLOGY

4.1. Research framework

In terms of objectives, the present study is an applied research that aims at knowledge development in the taxonomy and quantitative assessment of network vulnerabilities. Regarding the data gathering method employed, it may be considered as a survey. The literature review on security and network vulnerability is followed by extraction of relevant indices in network vulnerability taxonomy. The theoretical framework of the study is presented in Table IX. With this framework, a questionnaire was designed and distributed among the statistical population. The data thus obtained were subjected to analysis using factor analyses (principal components analysis and varimax rotation), and the results were used to test the theoretical framework adopted.

4.2. Statistical population and sample

The statistical population used consisted of experts in the field of information security and network. Expert views and judgments were collected using the judgment sampling method for evaluating the criteria of the proposed research framework. According to this method, a portion of the statistical population is selected whose membership is decided upon by the researcher's judgment of experts' knowledge

Table VII. Environmental Metrics in the NCVSS method.

Criterion	Characteristic	Description
Collateral damage potential	None (N)	There is no possibility of damaging or productivity and efficiency decrease.
	Low (L)	A successful exploitation of vulnerability has little financial or physical damage or has little impact on the efficiency or performance.
	Low–medium (LM)	A successful exploitation of vulnerability has medium financial or physical damage, or has medium impact on the efficiency or performance.
	Medium–high (MH)	A successful exploitation of vulnerability has considerable financial or physical damage or has considerable impact on the efficiency or performance.
	High (H)	A successful exploitation of vulnerability has significant financial or physical damage, or has significant impact on the efficiency or performance.
	Not defined (ND)	Assigning this value to the metric will not influence the score.
Target distribution	None (N)	No target systems exist, or targets are so highly specialized that they only exist in a laboratory setting. Effectively 0% of the environment is at risk.
	Low (L)	Targets exist inside the environment, but on a small scale. Between 1% and 25% of the total environment is at risk.
	Medium (M)	Targets exist inside the environment, but on a medium scale. Between 26% and 75% of the total environment is at risk.
	High (H)	Targets exist inside the environment on a considerable scale. Between 76% and 100% of the total environment is considered at risk.
	Not defined (ND)	Assigning this value to the metric will not influence the score.
Security requirements	Low (L)	Loss of confidentiality/integrity/availability is likely to have only a limited adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).
	Medium (M)	Loss of confidentiality/integrity/availability is likely to have a serious adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).
	High (H)	Loss of confidentiality/integrity/availability is likely to have a catastrophic adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).
	Not defined (ND)	Assigning this value to the metric will not influence the score.

of the field [40]. The objective is to collect data and views from people with effective experience and knowledge about the subject. The criteria used in sampling for the purposes of this study included work experience in the field of information security and network, teaching relevant subjects at academic centers and universities, and publications (article, dissertations, books) in the field. With the use of these criteria, 75 experts were identified who received the

Table VIII. Base, temporal, and environmental equations in the proposed Network Common Vulnerability Scoring System (NCVSS) method.

Base Metrics in the NCVSS proposed method	BaseScore = round_to_1_decimal (((0.6*Impact) + (0.4*Exploitability)-1.5)*f (Impact)) Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact)) Exploitability = 20*AccessVector*AccessComplexity*Authentication*NonRepudiation*Communication Security f (impact)= 0 if Impact=0, 1.176 otherwise AccessVector = case AccessVector of requires local access: 0.395 adjacent network accessible: 0.646 network accessible: 1.0 AccessComplexity = case AccessComplexity of high: 0.35 medium: 0.61 low: 0.71 Authentication = case Authentication of requires multiple instances of authentication: 0.45 requires single instance of authentication: 0.56 requires no authentication: 0.704 ConfImpact = case ConfidentialityImpact of none: 0.0 partial: 0.275 complete: 0.660 IntegImpact = case IntegrityImpact of none: 0.0 partial: 0.275 complete: 0.660 AvailImpact = case AvailabilityImpact of none: 0.0 partial: 0.275 complete: 0.660 Non Repudiation = case Non Repudiation of requires multiple instances of approve: 0.45 requires single instance of approve: 0.56 requires no approve: 0.704 Communication Security= case communication security of requires multiple instances of Communication Security: 0.45 requires single instance of Communication Security: 0.56 requires no Communication Security: 0.704	Environmental Metrics in the NCVSS proposed method	EnvironmentalScore = round_to_1_decimal ((AdjustedTemporal+ (10-AdjustedTemporal)*CollateralDamagePotential)*TargetDistribution)) AdjustedBase = (((0.6* AdjustedImpact) + (0.4* AdjustedImpact)-1.5)*f (Impact)) AdjustedTemporal == (AdjustedBase * Exploitability * Remediation Level * Report Confidence) AdjustedImpact = min(10,10.41*(1-(1-ConfImpact*ConfReq)*(1-IntegImpact*IntegReq)*(1-AvailImpact*AvailReq))) CollateralDamagePotential = case CollateralDamagePotential of none: 0 low: 0.1 low-medium: 0.3 medium-high: 0.4 high: 0.5 not defined: 0 TargetDistribution = case TargetDistribution of none: 0 low: 0.25 medium: 0.75 high: 1.00 not defined: 1.00 ConfReq = case ConfReq of low: 0.5 medium: 1.0 high: 1.51 not defined: 1.0 IntegReq = case IntegReq of low: 0.5 medium: 1.0 high: 1.51 not defined: 1.0 AvailReq = case AvailReq of low: 0.5 medium: 1.0 high: 1.51 not defined: 1.0
Temporal Metrics in the NCVSS proposed method	TemporalScore = round_to_1_decimal(BaseScore*Exploitability*RemediationLevel*ReportConfidence) Exploitability = case Exploitability of unproven: 0.85 proof-of-concept: 0.9 functional: 0.95 high: 1.00 not defined: 1.00 RemediationLevel = case RemediationLevel of official-fix: 0.87 temporary-fix: 0.90 workaround: 0.95 unavailable: 1.00 not defined: 1.00 ReportConfidence = case ReportConfidence of unconfirmed: 0.90 uncorroborated: 0.95 confirmed: 1.00 not defined: 1.00		

questionnaires directly or by e-mail. Ultimately, 40 questionnaires were collected and used for data analysis (a response rate of 53.3%).

4.3. Validity and reliability

To ensure the validity of the survey, its first edition was reviewed by five prominent scholars and experts in the field of IT, information security and network. Their recommendations were accordingly incorporated into the questionnaire.

Reliability of the questionnaire was assessed by using Cronbach's alpha. With the use of SPSS16, the Cronbach's alpha value for the total number of questionnaires was calculated to be 0.851, which indicates the high reliability of the questions in the questionnaire. Then, also, the amount of Cronbach's alpha was separately calculated for each of construct. Internal scale reliabilities were found to be greater than the acceptable limit (0.7) [41]. The values for each of the constructs are presented in Table X.

5. DATA ANALYSES

The demographic profile of the respondents indicates that 28.4% of respondents were female and 71.6% were male. In terms of educational level, 19% held bachelor's degrees, 61.3% master's degrees, and 19.7% held doctorate degrees in the relevant fields. In terms of age, 26.4% of the respondents aged 25–35 years, 44.36% 35–45, and 29.24% were above 45 years old.

Results obtained from the Kaiser–Meyer–Olkin (KMO) measure of sampling Adequacy (KMO = 0.653, which is greater than the acceptable level of 0.6) [42] and the significant value of the Bartlett's test (which is less than 0.05) indicate that the data collected were adequate for factor analysis and that the sampling size was large enough. The results of factor analysis and the descriptive statistics of the data are presented in Table X.

On the basis of the result of computations, the cumulative variance for all the variables is equal to 61.98%. This means that the proposed construct properly identified 61.98% of the vulnerability and that the validity of the questions was satisfactory. As shown in Table X, all the measures have factor loadings of greater than 0.5. In order to test for discriminant validity, the loadings of an item with its associated perspective to its cross-loadings were compared. Table X demonstrates that all items had loadings above 0.5 with their corresponding perspective compared with their cross-loadings, which were less than 0.5 [43].

On the basis of the values in Table X, the mean values of all the dimensions were greater than 3. This indicates the positive response of experts to the proposed constructs. On the basis of the result obtained from factor analyses in Table X, factor loadings of all the criteria were higher than 0.5 and all the criteria showed an important role in the explaining network vulnerabilities. With the results presented in the table, base metrics (factor loading = 30.143) had the greatest role in explaining network vulnerabilities followed by environmental metrics (factor loading = 16.28) and temporal metrics

Table IX. Theoretical framework.

Criterion		Explanations
Base metrics	Access vector	Identifying attackers' access method used to access the network and their distance
	Access complexity	The skills and talent required for exploiting information, environment and available systems in the network after accessing the network
	Authentication	Number of times that the attacker has to verify authenticity before accessing his target and exploiting it
	Activity verification	Number and diversity of usable approaches for not denying the activities conducted in the network
	Confidentiality Impact	Rate of successful exploitation of a network vulnerability disclosure and use of confidential information in the network domain
	Communications Security	Number of security layers used for providing secure communication
	Integrity impact	Amount of change the attacker can cause in the information, environment, and systems available in the network after access
	Availability	Amount of change the attacker can create in users' access to the network after penetration
Temporal metrics	Exploitability	Amount of public access to software, codes, and techniques that can be used to penetrate and damage the network
	Remediation level	Organizational solutions for managing and confronting damages
	Report confidence	Rate of vulnerability confidence and credibility of the technical details
Environmental metrics	Collateral damage potential	The amount of damage caused by attacks or unauthorized access to the network (including economic compensation, performance, efficiency)
	Target distribution	Rate of systems that can be influenced by network vulnerabilities
	Security requirements	The effect of loss of security in the integrity, accessibility, and privacy aspects

(factor loading = 15.811). These values indicate the significance of each metrics in identifying network vulnerabilities. The criterion of collateral damage potential of environmental metrics sets (factor loading = 0.835) had the highest factor loading, whereas communications security (factor loading = −0.183) had the least value among the network vulnerabilities criteria investigated.

6. A CASE STUDY

A case study is presented in this section in order to illustrate the application of the NCVSS method. A ceramic and tile manufacturing firm is selected for the case study, which has one manufacturing zone and two regional offices. There are 153 active users using the network in the manufacturing zone, 27 in the first regional office designated as A, and 54 in the second regional office designated as B. The link between these three zones is provided through a Multiprotocol Label Switching network and wireless communication. The company recently attempted to set up its web-based enterprise resource planning systems, and 70% of the modules have been already implemented and operated. In order to enhance its organizational information security, the firm has developed a plan called FAVA Security. The

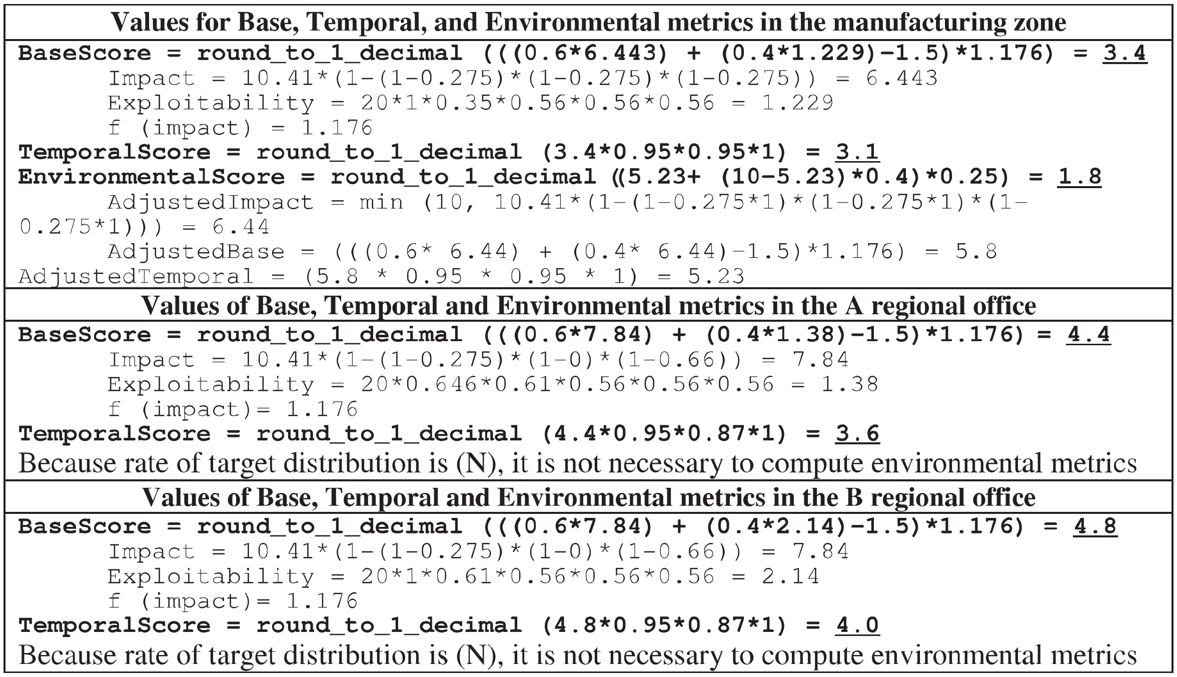
Table X. Results of Data Analysis.

	Criterion	Mean	Standard Deviation	Factor loading			Special value	variance	Cronbach alpha
				1st Factor	2ed Factor	3th Factor			
Base metrics (mean=30.09,SD=0.72)	Access vector	3.1	1.032	0.703	0.134	0.196	4.514	30.143	0.87
	Access complexity	3	1.086	0.682	-0.075	0.016			
	Authentication	2.4	1.128	0.805	0.242	0.372			
	Activity verification	2.55	0.904	0.697	0.174	0.221			
	Confidentiality Impact	2.9	1.081	0.857	-0.132	0.168			
	Communications Security	3.65	0.949	0.559	-0.183	-0.408			
	Integrity Impact	3.98	0.981	0.615	-0.146	-0.228			
	Availability	3.175	0.931	0.794	-0.152	0.218			
Temporal Metrics (mean = 3.062، SD = 0.82)	Exploitability	3.62	1.102	0.123	0.046	0.695	1.873	15.811	0.71
	Remediation Level	3.72	0.877	0.155	-0.047	0.82			
	Report Confidence	3.5	11.086	0.091	-0.083	0.713			
Environmental Metrics (mean = 3.9, SD = 0.94)	Collateral Damage Potential	3.77	1.25	0.013	0.895	-0.138	2.29	16.028	0.79
	Target Distribution	3.7	1.265	-0.148	0.842	0.094			
	Security Requirements	4.225	0.8	0.039	0.718	-0.008			

Table XI. Values for variable in the base, temporal and environmental metrics in the sample.

		Manufacturing zone		Regional office A		Regional office B	
Criterion		Status of the sample with regard to the characteristic	Quantity	Status of the sample with regard to the characteristic	Quantity	Status of the sample with regard to the characteristic	Quantity
Base metrics	Access vector	LAN W-LAN Internet	1	LAN Internet	0.646	LAN W-LAN Internet	1
	Access complexity	High (H)	0.35	Medium (M)	0.61	Medium (M)	0.61
	Authentication	Single (S)	0.56	Single (S)	0.56	Single (S)	0.56
	Activity verification	Single (S)	0.56	Single (S)	0.56	Single (S)	0.56
	Confidentiality impact	Partial (P)	0.275	Partial (P)	0.275	Partial (P)	0.275
	Communications security	Single (S)	0.56	Single (S)	0.56	Single (S)	0.56
	Integrity impact	Partial (P)	0.275	None (N)	0	None (N)	0
	Availability	Partial (P)	0.275	Complete (C)	0.66	Complete (C)	0.66
Temporal metrics	Exploitability	Functional (F)	0.95	Functional (F)	0.95	Functional (F)	0.95
	Remediation level	Workaround (W)	0.95	Official fix (OF)	0.87	Temporary fix (TF)	0.87
	Report confidence	Not defined(ND)	1	Not defined (ND)	1	Not defined (ND)	1
Environmental metrics	Collateral damage potential	Medium–high(MH)	0.4	Low (L)	0.1	Medium–high (MH)	1
	Target distribution	Low (L)	0.25	None (N)	0	None (N)	0
	Security requirements	Medium(M)	1	Low (L)	0.5	Low (L)	0.5

Table XII. Computation of base, temporal, and environmental criteria in the sample.



Values for Base, Temporal, and Environmental metrics in the manufacturing zone

```
BaseScore = round_to_1_decimal (((0.6*6.443) + (0.4*1.229)-1.5)*1.176) = 3.4
      Impact = 10.41*(1-(1-0.275)*(1-0.275)*(1-0.275)) = 6.443
      Exploitability = 20*1*0.35*0.56*0.56*0.56 = 1.229
      f (impact) = 1.176
TemporalScore = round_to_1_decimal (3.4*0.95*0.95*1) = 3.1
EnvironmentalScore = round_to_1_decimal ((5.23+ (10-5.23)*0.4)*0.25) = 1.8
      AdjustedImpact = min (10, 10.41*(1-(1-0.275*1)*(1-0.275*1)*(1-
0.275*1))) = 6.44
      AdjustedBase = (((0.6* 6.44) + (0.4* 6.44)-1.5)*1.176) = 5.8
AdjustedTemporal = (5.8 * 0.95 * 0.95 * 1) = 5.23
```

Values of Base, Temporal and Environmental metrics in the A regional office

```
BaseScore = round_to_1_decimal (((0.6*7.84) + (0.4*1.38)-1.5)*1.176) = 4.4
      Impact = 10.41*(1-(1-0.275)*(1-0)*(1-0.66)) = 7.84
      Exploitability = 20*0.646*0.61*0.56*0.56*0.56 = 1.38
      f (impact)= 1.176
TemporalScore = round_to_1_decimal (4.4*0.95*0.87*1) = 3.6
```

Because rate of target distribution is (N), it is not necessary to compute environmental metrics

Values of Base, Temporal and Environmental metrics in the B regional office

```
BaseScore = round_to_1_decimal (((0.6*7.84) + (0.4*2.14)-1.5)*1.176) = 4.8
      Impact = 10.41*(1-(1-0.275)*(1-0)*(1-0.66)) = 7.84
      Exploitability = 20*1*0.61*0.56*0.56*0.56 = 2.14
      f (impact)= 1.176
TemporalScore = round_to_1_decimal (4.8*0.95*0.87*1) = 4.0
```

Because rate of target distribution is (N), it is not necessary to compute environmental metrics

approach proposed in this paper was introduced to this firm, and the management was encouraged to use NCVSS for prioritizing the FAVASEC plan in the three zones of the firm. For this purpose, a meeting was held with the IT professionals of the firm, and they were briefed on the proposed method. The required data were subsequently collected in cooperation of the IT unit of the firm. A summary of the data gathered is presented in Table XI.

Substituting the values presented in Table XI in the relevant equations of the proposed method (on the basis of the computation method described in Table VIII), the values for the base, environmental, and temporal metrics were calculated for the three zones. These values are reported in Table XII. As indicated by these values, regional office B has the highest values for the base and temporal metrics in the network of this firm followed by its regional office A. With the computations, the network in the manufacturing zone has minimal values for the environmental, temporal, and base metrics.

In the base metrics section, the main causes for the high vulnerability of the network in regional office B as compared with that of the manufacturing zone are the values for access complexity measures and availability. Although these values in both offices A and B are the same, regional office A has a better status as judged by its access vector criterion.

Also, regarding the temporal metrics, the cause for the high vulnerability of the networks in regional offices A and B compared with that of the manufacturing zone may be related to the remediation level. Under the same conditions and with regard to the effect of the base metrics on the temporal metrics, the temporal metrics will be higher in regional office B than that in regional office A because of the higher values of base metrics in the former than that in the latter. On the basis of our computations, it may be concluded that this firm should implement its FAVASEC security enhancement plan in the priority order of regional offices A and B followed by its manufacturing zone.

7. CONCLUSION

This paper pursued two primary objectives: first, to develop and evaluate a classification system for network vulnerabilities on the basis of the ITU-TX-805, and second, to develop a method for quantitative computation of computer network vulnerabilities on the basis of NCVSS.

With the proposed framework, attempts were made to obtain a comprehensive and extendable taxonomy structure for different aspects of network vulnerabilities. The structure thus obtained is capable of identifying vulnerabilities and helping network managers to manage network vulnerabilities in an effective manner while it also quantifies vulnerabilities. The proposed taxonomy provides different applications in the field of vulnerability management such as creating a common classification structure, facilitating assessment process, analyzing vulnerabilities, and facilitating the quantifying process of vulnerabilities aimed at proper handling of likely vulnerabilities. These objectives were realized by developing a multi-dimensional taxonomy on the basis of the ITU-TX-805 security architecture. The major features of the proposed framework include comprehensiveness, generalization, possibility for identification and discovery of attacks before their occurrence, and the ability to classify vulnerabilities on the basis of their roles in the attacks. These facilitate the process of quantification of network vulnerabilities. Features of the proposed taxonomy include the ability for simultaneously accounting for the three components of threat type, vulnerable equipments due to threats, and type of network activities that may be exposed to vulnerabilities. These three components were considered on the basis of the ITU-TX-805 security architecture and designed in such way that they are applicable to all networks and applications while they also provide a comprehensive, top–down structure of network security for components, services and network applications.

REFERENCES

1. Omidian A, Norallahi ravari A, Jalili R. Categorizing recognized vulnerabilities in database management systems (In Persian). *The First Conference of Security Incidents and Vulnerabilities in the Exchange of Information* Tehran, Iran, 2009.
2. Hansman S, Hunt R. A taxonomy of network and computer attacks. *Computers & Security* 2005; **24**:31–43.
3. Ramakrishnan CR, Sekar R. Model-based vulnerability analysis of computer systems. *2nd Int'l Workshop on Verification, Model Checking and Abstract Interpretation*, 1998.
4. Bishop M. A Taxonomy of UNIX System and Network Vulnerabilities. Technical Report CSE-95-8, Dept. of Computer Science, University of California at Davis, Davis, CA 95616-8562 1995.
5. Ammann P, Wijesekera D, Kaushik S. Scalable, graph-based network vulnerability analysis. *The 9th ACM Conference on Computer and Communications Security*, 2002.
6. Bishop M. *Computer Security: Art and Science*. Addison-Wesley: Boston, Mass.; London, 2003.
7. Hajian S, Hendesi F, Berenjkob M, Hashemi SH, Golshani P. A new classification for network vulnerabilities (in Persian). *The First Conference of Security Incidents and Vulnerabilities in the Exchange of Information* Tehran, Iran, 2009.
8. Howard JD, Longstaff TA. A Common Language for Computer Security Incidents. SANDIA REPORT, SAND 98-8667, 1998.
9. Krsul IV. Software Vulnerability Analysis. *Ph.D. Thesis*, Purdue University, West Lafayette, Indiana, 1998.
10. Lough DL. A Taxonomy of Computer Attacks with Applications to Wireless Networks. *Ph.D. thesis*, Department of Electrical and Computer Engineering, VirginiaTech, Virginia, 2001.
11. Bisbey R, Hollingworth D. Protection Analysis: Final Report. (Vol. ISI/SR-78-13, USC/Info. Sci. Inst.): Marina Del Rey, CA, 1978.
12. Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. *Computer Communication Review* 2004; **34**:39–53.
13. Ammala DE. Derivation of Metrics for Effective Evaluation of Vulnerability Assessment Technology. Thesis (M.S.)–Mississippi State University, Department of Computer Science and Engineering. Mississippi State, 2004.
14. Abbott RP, Chin JS, Donnelley JE, *et al.*. *Security Analysis and Enhancements of Computer Operating Systems*. Institute for Computer Science and Technology, National Bureau of Standards: Washington, D.C, 1976; 1–62.
15. Ristenbatt MP. Methodology for network communication vulnerability analysis. *21st Century Military Communications Conference*, 1988.
16. Landwehr CE, Bull AR, McDermott JP, Choi WS. A Taxonomy of Computer Program Security Flaws. *ACM Computing Surveys* 1994; **26**:211–254.
17. Aslam T. *A Taxonomy of Security Faults in the UNIX Operating System*. Purdue University: West Lafayette, 1995.
18. Du W, Mathur A. Categorization of Software Errors that Lead to Security Breaches. *COAST technical report*. West Lafayette, Indiana: Department of Computer Sciences, Purdue University, 1997.
19. Bishop M. Vulnerabilities analysis. *Second International Symposium on Recent Advances in Intrusion Detection* 1999.
20. Kamara S, Fahmy S, Schultz E, Kerschbaum F, Frantzen M. Analysis of vulnerabilities in Internet firewalls. *Computers & Security* 2003; **22**:214–232.
21. Pothamsetty V, Akyol BA. A vulnerability taxonomy for network protocols: corresponding engineering best practice countermeasures. *IASTED International Conference on Communications, Internet and Information Technology*. Thomas, US Virgin Islands, 2004.
22. Weber S, Karger PA, Paradkar A. A software flaw taxonomy: aiming tools at security. *SESS '05 Proceedings of the 2005 Workshop on Software Engineering for Secure Systems—Building Trustworthy Applications*. St. Louis, Missouri, 2005.
23. Hamed H, Al-Shaer E. Taxonomy of conflicts in network security policies. *IEEE Communications Magazine* 2006; **44**:134–141.
24. Asosheh A, Ramezani N. A comprehensive taxonomy of DDoS attacks and defense mechanism applying in a smart classification. *WSEAS Transactions on Computers* 2008; **7**:281–290.
25. Wiesauer A, Sametinger J. A Security Design Pattern Taxonomy Based on Attack Patterns: Findings of a

Systematic Literature Review. Proceedings of the International Conference on Security and Cryptography, Milan, Italy, 2009: 7–10.

26. Ryoo J, Choi YB, Oh TH, Corbin G. A multidimensional classification framework for developing context-specific wireless local area network attack taxonomies. *International Journal of Mobile Communications* 2009; **7**:253–267.
27. Radmand P, Talevski A, Petersen S, Carlsen S. Taxonomy of wireless sensor network cyber security attacks in the oil and gas industries. *24th IEEE International Conference on Advanced Information Networking and Applications (AINA)* 2010.
28. Zeidanloo HR, Zadeh MJ, Shooshtari MJZ, *et al*. A taxonomy of Botnet detection techniques. *3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT)* Chengdu, 2010.
29. McGee AR, Vasireddy SR, Xie C, *et al*. A framework for ensuring network security. *Bell Laboratories Technical Journal* 2004; **8**:7–27.
30. Gheorghe AV, Vamanu DV. Towards QVA—quantitative vulnerability assessment: a generic practical model. *Journal of Risk Research* 2004; **7**:613–628.
31. Alhazmi OH, Malaiya YK. Quantitative vulnerability assessment of systems software. *Annual Reliability and Maintainability Symposium, 2005 Proceedings*, 2005; 615–620.
32. Emami S, Jafarian JH. Calculating systems vulnerability degree (In Persian). *The First Conference of Security Incidents and Vulnerabilities in the Exchange of Information* Tehran, Iran, 2009.
33. Mell P, Scarfone K, Romanosky S. Common Vulnerability Scoring System. *Security & Privacy, IEEE.* 2006; **4**:85–89.
34. Scarfone K, Mell P. An analysis of CVSS version 2 vulnerability scoring. *Empirical Software Engineering and Measurement, 2009. ESEM 2009. 3rd International Symposium on*, 2009.
35. Mell P, Scarfone K. Improving the Common Vulnerability Scoring System. *Information Security, IET.* 2007; **1**:119–127.
36. Fruhwirth C, Mannisto T. Improving CVSS-based vulnerability prioritization and response with context information. *Empirical Software Engineering and Measurement, 2009. ESEM 2009. 3rd International Symposium on*, 2009.
37. Gallon L. On the impact of environmental metrics on CVSS Scores. *Social Computing (SocialCom), 2010 IEEE Second International Conference on*, 2010.
38. Harada T, Kanaoka A, Okamoto E, Kato M. Identifying potentially-impacted area by vulnerabilities in networked systems using CVSS. *Applications and the Internet (SAINT), 2010 10th IEEE/IPSJ International Symposium on*, 2010.
39. Houmb SH, Franqueira VNL. Estimating ToE risk level using CVSS. *Availability, Reliability and Security, 2009. ARES '09. International Conference on*, 2009.
40. Danaei far H, Alvani SM, Azar A. *Quantitative Methodology in Management, Comprehensive Approach (in Persian)*. Safar: Tehran, 2008.
41. Nunnally JC, Bernstein IH *Psychometric Theory* (3rd edn). McGraw-Hill: New York, 1994.
42. Hair JF. *Multivariate Data Analysis*. Prentice Hall: Upper Saddle River, N.J., 1998.
43. Sedghi A, Seyed javadin SR, Motalebi D, Hoseini SJ, Yazdani HR. Comparison customer satisfaction indices and finding a model for measurement taxpayer satisfaction (in Persian). *Iranian Business Management* 2010; **1**:101–118.

Appendix I: Sample Questionnaire

General profile of respondents

Gender: Male○ Female○

Age (year): Under 30○ 30 to 39○ 40 to 50○ Over 50○
Education degree: Associates ○ BS.c ○ MS.c ○ Ph.D ○
Professional experiences in network security (year):
Under 5○ 5 to 10○ 10 to 15○ Over 15○

	Criterion	Explanations	Very low	Low	Med	High	Very high
Base Metrics	Access vector	Identifying attackers' access method used to access the network and their distance					
	Access complexity	The skills and talent required for exploiting information, environment and available systems in the network after accessing the network					
	Authentication	Number of times that the attacker has to verify authenticity before accessing his target and exploiting it					
	Activity verification	Number and diversity of usable approaches for not denying the activities conducted in the network					
	Confidentiality impact	Rate of successful exploitation of a network vulnerability disclosure and use of confidential information in the network domain					
	Communications security	Number of security layers used for providing secure communication					
	Integrity impact	Amount of change the attacker can cause in the information, environment and systems available in the network after access					
	Availability	Amount of change the attacker can create in users' access to the network after penetration					
Temporal Metrics	Exploitability	Amount of public access to software, codes and techniques that can be used to penetrate and damage the network					
	Remediation level	Organizational solutions for managing and confronting damages					
	Report confidence	Rate of vulnerability confidence and credibility of the technical details					
Environmental Metrics	Collateral damage potential	The amount of damage caused by attacks or unauthorized access to the network (including economic compensation, performance, efficiency)					
	Target distribution	Rate of systems that can be influenced by network vulnerabilities					
	Security requirements	The effect of loss of security in the integrity, accessibility and privacy aspects.					