IJICT International Journal of Information & Communication Technology

ITRC

Volume 2- Number 1- May 2010 (pp.29-44)

A Taxonomy for Network Vulnerabilities

Sara Hajian
APA-IUTcert
Department of Electrical and Computer Engineering
Isfahan University of Technology
hajian@nsec.ir

Faramarz Hendessi
APA-IUTcert
Department of Electrical and Computer Engineering
Isfahan University of Technology
hendessi@cc.iut.ac.ir

Mehdi Berenjkoub
APA-IUTcert
Department of Electrical and Computer Engineering
Isfahan University of Technology
brnjkb@cc.iut.ac.ir

Received: January 23, 2010- Accepted: May 4, 2010

Abstract— **The number of reported vulnerabilities is dramatically rising every year. In addition, the combination of different kinds of network devices, services and applications in a complex manner lead to increase the complexity of vulnerabilities. Increasing the number of vulnerabilities and their complications show the importance of vulnerability taxonomies which could provide a common language for defining vulnerabilities and help analyze and assess them. Both the advantages of using vulnerability taxonomies and the features of the taxonomies that have ever been suggested encouraged us to offer the new network vulnerability taxonomy. Our proposed taxonomy is a multi-dimensional and hierarchical taxonomy which classifies network vulnerabilities based on their location, cause and impact. These are three dimensions of our taxonomy. We use ITU-T X-805 security architecture to provide a comprehensive layered classification for the location dimension and also use common weakness enumeration (CWE) project to provide a complete layered classification for the cause dimension of the proposed taxonomy. Finally, we evaluate our taxonomy based on taxonomy requirements. In addition, to demonstrate the usefulness of our taxonomy, a case study applies the taxonomy to a number of network vulnerabilities. We also use this taxonomy to analyze network vulnerabilities. The result of our analysis is a matrix that demonstrates the distribution of network vulnerabilities based on their causes, locations and impacts. In addition to offering a taxonomy that is specific to network vulnerabilities and is beneficial for analyzing network vulnerabilities by covering almost all possible combinations of causes, locations, and impacts, we also introduce and consider network activities in the classification of location dimension for the first time.**

Keywords- Taxonomy; network vulnerabilities; ITU-T X-805 security architecture; common weakness enumeration (CWE); network vulnerability analysis.

I. INTRODUCTION

A vulnerability is a potential and susceptible avenue of attack. In other words, a vulnerability is a defect which, when exercised, can produce undesired and incorrect behavior [1]. Since 1995 there has been a marked increase in the number of vulnerabilities. The statistics reported by CERT/CC over the past thirteen year's show that the number of vulnerabilities rises to 44074 until third quarter of 2008 [3]. This increases the number of vulnerabilities and also their complexities demonstrate the importance of classifying vulnerabilities.

Taxonomy is a classification scheme that partitions a body of knowledge and defines the relationships among the pieces. While beginning the scientific study of a new field, a good taxonomy is considered an "important and necessary prerequisite for systematic study" [4]. A good taxonomy also provides a common language for the study of the field [4].

The first step in understanding vulnerabilities is to classify them into a taxonomy based on their characteristics. A taxonomy classifies the large number of vulnerabilities into a few well defined and easily understood categories [5]. Such classification can serve as a guiding framework for performing a systematic security assessment of a system. Indeed, one of the main goals of developing taxonomies of vulnerabilities has been to develop automated tools for performing security assessment [15]. Although this goal has not been completely realized, the taxonomies nonetheless serve as a very useful framework for security assessment. In addition, information bodies such as CERT can communicate between group's members more efficiently by using common vulnerability taxonomies [2]. Thus, a taxonomy by providing a series of common concepts can deliver a structured way to visit, analyze and assess vulnerabilities.

In this paper, we classify network vulnerabilities according to one overall view. Until now, a number of taxonomies aimed at classifying vulnerabilities have been proposed. With respect to context, vulnerability taxonomies could be general or specific. Most of the proposed vulnerability taxonomies are general or only specific to operating systems or software flaws. Only Ristenbatt in [6] proposed a specific taxonomy for the network vulnerabilities. On the other hand, with respect to classifications scheme, there are different models of vulnerability taxonomies. Vulnerability taxonomies could be flat or multidimensional. In addition, vulnerability taxonomies could be hierarchical (layered) or linear (horizontal). Only a layered taxonomy would provide an objective methodology to identify and assess vulnerabilities [2]. In this paper we propose a multidimensional and hierarchical taxonomy which classify network vulnerabilities by a new approach based on ITU-T X-805 [7] security architecture. ITU-T X-805 security architecture is more comprehensive than other security architectures and models. This architecture could be applied to various kinds of networks and able to provide a comprehensive and top-down perspective of network security for network elements, services, and applications to detect, correct, and prevent security vulnerabilities [7]. We introduced the initial idea and preliminary results of our proposed taxonomy in [35]. In this paper, we extend our proposed taxonomy to fulfill the necessary requirements of a beneficial vulnerability taxonomy. In addition, we use the proposed taxonomy to analyze network vulnerabilities and present our analyzing results for twenty of network vulnerabilities in this paper.

The remainder of this paper is organized as follows. Section II presents the related works. Section III, briefly reviews ITU-T X-805 security architecture. The proposed Taxonomy is introduced in section IV. In Section V, a case study, the results of analyzing the sample of network vulnerabilities based on the proposed taxonomy, is presented. The evaluation of the proposed taxonomy is explained in section VI. Finally, some concluding remarks are mentioned in section VII. More detailed information about the sample of network vulnerabilities and classification results of them are presented in Appendix A.

II. RELATED WORKS

A summary of the vulnerability taxonomies is presented in Table I. This table shows name, goals, basis (dimensions) and comments of each taxonomy. As mentioned before, Ristenbatt in [6] proposed a specific taxonomy for the network vulnerabilities. In [6] Ristenbatt describes a methodology named Network Communications Vulnerability Assessment (NCVA), which was developed to perform network vulnerability assessment. The NCVA methodology used two taxonomies, neither of which actually classified information about known attacks and vulnerabilities. The first taxonomy classified the various types of networks according to their design [2]. The objective of this taxonomy was to provide the analyst with a high-level overview of the network. The top-level categories are:

- The transfer strategy (circuit-switched or packet-switched)
- The network transfer control method
- The transfer link structure
- Link access method or protocol
- System topology architecture

The second taxonomy in [6] outlined the typical network susceptibilities. Ristenbatt distinguishes between susceptibilities and vulnerabilities. He defines susceptibilities as system features that might be targeted by attackers. In other words, they are potential vulnerabilities. The network susceptibilities taxonomy has five categories:

- Topology
- Physical layer
- Data link layer
- Network layer
- Management and control

This suggests that the dimension of classification at the first level is system components. Within each class, Ristenbatt lists possible features that could be targeted by attackers. The taxonomy is not hierarchical (layered), but nevertheless it is a good example of a taxonomy providing a systematic assessment methodology [2].

Du and Mathur in [8] indicate that a taxonomy of vulnerabilities need not have the mutual exclusivity property. They argue that by classifying each flaw under a single category, we may lose a lot of information due to the abstraction. "The more accurately we categorize flaws, the easier it is to avoid a strong bias in selecting security errors." [8]

Table I shows that other vulnerability taxonomies are general or deal with software programs, operating systems, or communication protocol vulnerabilities.

TABLE I. THE SUMMARIZATION OF VULNERABILITY TAXONOMIES, DERIVED FROM [2]

Title	Goals	Basis/dimension of taxonomy	Comments
Integrity Flaws [12]	Identify flaws in operating system	Based on characteristic of Vulnerabilities	Points out that many flaws are due to valid design trade-offs
IBM VM/370 OS (Attanasio1976) [13]	Did not develop a taxonomy; they were conducting a penetration testing experiment on the VM/370.	No classification	Gives a list of OS features that are likely to have flaws
Operating System Flaws (RISOS project 1976) [14]	Characterize operating system flaws	'by operations' or 'by features'	The categories can be included in a layered taxonomy that refines functional blocks
Operating System Flaws (Protection Analysis Project 1978) [15]	To abstract patterns from flaws and hope to automate the search for flaws	Similar to the RISOS taxonomy, but it had only 7 categories	Categories can be included in a layered taxonomy
Operating System Flaws [16]	"Understandable record of flaws"; "understand which parts of the system have more flaws"; "help designers and analysts"	Three taxonomies based on: 1. Genesis 2. Time of introduction 3. Location	The three separate taxonomies presented in the article can be combined under one single framework for security assessment
UNIX security Flaws [17]	"Provide basis for data organization of a vulnerability database"	By cause	This is similar to the RISOS and PA classification
Software Program Flaws [18]	Characterize operating system flaws	Assumption made by the programmer	A unique dimension of classification
Software Vulnerabilities [19]	"Develop a tool that assists…in the assessment of tests of distributed software aimed at detecting security flaws"	1. By cause 2. By impact 3. By fix	Similar categories as Landwehr, but also considers defenses or fixes
Vulnerabilities (Bishop) [20]	"Describe vulnerabilities in a form useful for intrusion detection echanisms"	1. Nature 2. Time 3. Exploitation 4. Effect 5. Minimum number of components 6. Source of ID	Covers most of the major dimensions of vulnerability classification
Network Vulnerabilities [6]	For use in a network vulnerability assessment procedure	By the protocol layers in which the vulnerabilities are present	Covers all components of network systematically
Threat Taxonomy [21]	Use taxonomy to build a security architecture for a wireless network	By security property violated: confidentiality, integrity	The threats are actually attacks
Analysis of Vulnerabilities in Firewalls [22]	"To understand firewall vulnerabilities in the context of firewall operations"	Used Du and Mathur's taxonomy	This is an example of work that used an established taxonomy for analyzing the security of other systems
Vulnerability Taxonomy (Gray) [23]	Develop a taxonomy to help the organization's management	Used a combination of existing taxonomies	Demonstrates the use of security taxonomies to help management
Vulnerability Taxonomy for Auditing [24]	Develop a taxonomy for auditing software	Used Landwehr's taxonomy	Used all dimensions of classification for effective security testing
Protocol Vulnerabilities [25]	."... Highlight these vulnerabilities such that the teams can find and prevent ... vulnerabilities "	According to the features or operations of the protocol software that are likely to have flaws	Similar to RISOS and PA taxonomies, except that it focuses on protocol software
Vulnerabilities (Yongzheng, Xiochun — 2004) [26]	"Designed for security risk assessment" "Warn designers against repeating mistakes"	Based on concepts of privilege sets and privilege escalation	Explores relationship between risk and vulnerability
Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors [27]	seek to simplify the existing software vulnerabilities axonomies. In order to help software developers and security practitioners	According to errors in source code, and one is related to configuration and environment issues.	Cover causes of vulnerabilities
Software Vulnerability Analysis for Web Services Software Systems [28]	provide a framework for analyzing the security of Web software services	they relate all the attacks with the software vulnerabilities each attack exploits	Classification for both attacks and vulnerabilities

In addition, each taxonomy was developed for a specific purpose.

Some open source projects are also recently established to provide software security problem lists. The first is the "OWASP Top Ten Most Critical Web Application Security Vulnerabilities" available on the web [10]. This project provides a high-level list of most critical web application vulnerabilities.

The second is the "Common weakness enumeration (CWE)" available on the web [11]. The CWE provides a common language of discourse for discussing, finding and dealing with the causes of software security vulnerabilities as they are found in code, design, or system architecture. Each individual CWE represents a single vulnerability type. CWE is currently maintained by the MITRE Corporation with support from the National Cyber Security Division.

There are also some works that use vulnerability taxonomies for analyzing vulnerabilities. In [22] Kamara et al. successfully use Du and Mathur's taxonomy for analyzing vulnerabilities in Internet firewalls. They break down a firewall into its constituent components (protocol layers), and its operations and data flow. They analyze some of the well-known firewall vulnerabilities, and map them to both Du and Mathur's taxonomy and the specific operations and parts of the firewalls. Jiwnani et al. [24, 29] used Landwehr taxonomy to build a matrix that helps software developers, testers, and software auditors understand the distribution of security vulnerabilities and prioritize their effort to achieve a higher level of security for subsequent software releases. Jiwnani et al. shows that the beneficial vulnerability taxonomy for assessment process must have three dimensions of cause, location and impact. The assessment process can be more systematic if these dimensions are arranged hierarchically, thereby ensuring that all possible combinations of causes, locations, and impacts are covered. For example, validation errors within the system initialization function of an operating system could lead to unauthorized access.

Most of the existing multidimensional vulnerability taxonomies do not consider all of these three dimensions or not classify each dimension hierarchically. In addition, most of them are used for classifying operating systems vulnerabilities. In this paper we propose a taxonomy with all those three dimensions and then each of them is arranged hierarchically by using some standard architectures and projects to ensure that almost all possible combinations of causes, locations, and impacts are covered in the context of network vulnerabilities.

III. Review of ITU-T X-805 Security Architecture

Security architecture is a detailed description of all aspects of the system that relate to security, along with a set of principles to guide the design. A security architecture describes how the system is put together to satisfy the security requirements [9]. Until now, the number of security frameworks, models, architectures, and sets of recommendations has been published. Most of them are only suit to a particular type of network or applications (e.g., the OSI security model [30], the TMN security model [31], The IEEE LAN/MAN Security Model [32]).

The OSI security model was taken by the International Organization for Standardization (ISO) to define security for the basic Open Systems Interconnection (OSI) reference model. The objective of the OSI security model is to provide a model for securing application communications. Just as with OSI, TMN is applicable to applications and support software, and not the actual network infrastructure. In fact, the TMN standard actually assumes that the OSI layer model is used and provides a discussion of security services and their linkage to the OSI layers. Additionally, just as the OSI model provides additional detail relative to protocol and application security specifics, the TMN security model provides in-depth recommendations for network management security implementations in the management plane. The TMN model does not address the end-user and control planes. The Institute of Electrical and Electronics Engineers (IEEE) security architecture framework for LAN/MAN security deals specifically with recommending security protocols and services that provide secure data exchange between entities connected by a LAN or MAN. As a result, this framework also maps onto a subset of the security space covered by the ITU-T X-805 security architecture.

ITU-T X-805 security architecture is more comprehensive than other security architectures and models [33]. This architecture could be applied to various kinds of networks and addressed security needs associated with network management activities, network control activities, and end-user activities of network infrastructure, services and applications. ITU-T X-805 security architecture provides a comprehensive and top-down perspective of network security for network elements, services, and applications to detect, correct, and prevent security vulnerabilities. The security architecture addresses three essential questions [7]:

1) What kind of protection is needed and against what threats?

2) What are the distinct types of network equipment and facility groupings that need to be protected?

3) What are the distinct types of network activities that need to be protected?

These questions are addressed by three architectural components: 1) security dimensions, 2) security layers, and 3) security planes. Fig. 1 shows ITU-T X-805 security architecture. A security dimension is a set of security measures designed to address a particular aspect of the network security. This architecture identifies eight such sets that protect against all major security threats. In order to provide a complete security solution, the security dimensions must be applied to a hierarchy of network equipment and facility groupings, which are referred to as security layers. This architecture defines three security layers: 1) the Infrastructure Security Layer, 2) the Services Security Layer, and 3) the Applications

Security Layer which build on one another to provide network-based solutions. The security layers are a series of enablers for secure network solutions: the infrastructure layer enables the services layer and the services layer enables the applications layer. The security architecture addresses the fact that each layer has different security vulnerabilities and offers the flexibility of countering the potential threats in a way most suited for a particular security layer. A security plane is a certain type of network activity protected by security dimensions. This architecture defines three security planes to represent the three types of protected activities that take place on a network. The security planes are: 1) the Management Plane, 2) the Control Plane; and 3) the End-User Plane.

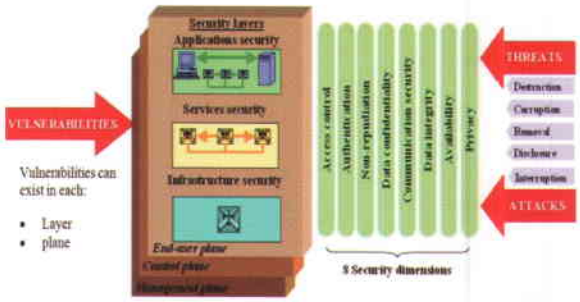

Fig. 1. ITU-T X-805 security architecture [7]

Applying the eight security dimensions to the planes and layers yields an aggregate view that is reproduced in Fig. 1.

IV. THE PROPOSED TAXONOMY

There have been many attempts to improve the process of systematic study to find vulnerabilities. These attempts have largely involved the development of attack and vulnerability taxonomies that provide valuable insights into different systems. Many taxonomies of attacks and vulnerabilities have been published over the years (table I), but there is still no standard or universally accepted taxonomy. The goal of the proposed taxonomy in this paper is providing a common language among different groups to define network vulnerabilities, classifying all vulnerabilities assets in network and using it for vulnerability discovery (Proactive) and vulnerability handling (Reactive). In this section of the paper, a new vulnerability taxonomy that identifies the location of vulnerabilities including network elements and network activities, causes of vulnerabilities and their impacts on different security domains is presented. In other words, it is a comprehensive taxonomy that covers all parts of network and indicates the place (position) of network vulnerabilities from different perspectives.

A. *Type of taxonomy*

There are different models for developing taxonomies. With respect to context, vulnerability taxonomies can be general or specific [2]. General taxonomies consider vulnerabilities without attention to their hosts, yet specific taxonomies consider vulnerabilities which are dedicated to the particular application or system. Taxonomies developed for a particular system are rarely useful for different systems. However, they are more practical than general taxonomies in context of using them for vulnerability analysis of those specific systems. In this paper we proposed a specific taxonomy for the network vulnerabilities.

Also with respect to classifications scheme, there are different models of vulnerability taxonomies. Vulnerability taxonomies could be flat or multidimensional [2]. A flat taxonomy is one that divides the set of security vulnerabilities according to one general criterion, but multidimensional taxonomies classify flaws according to more than one attribute. In addition, vulnerability taxonomies could be hierarchical (layered) or linear (horizontal). Only a layered taxonomy will provide an objective methodology to identify and assess vulnerabilities. In contrast, linear or horizontal taxonomies such as [34] are useful only for understanding the features of a vulnerability. They also do not aid to reduce the subjectivity of the vulnerability assessment process. The taxonomy must begin at a high level of abstraction and progressively go lower. Even the lowest level of some of the existing taxonomies has a fairly high-level representation of the vulnerability. Such abstract classes do not help identify specific vulnerabilities. This shows that an effective taxonomy must be both multidimensional and hierarchical to ensure that all possible combinations of dimensions are covered. In this paper we propose a multidimensional and hierarchical taxonomy. The proposed taxonomy could provide a comprehensive and well-defined taxonomy for different groups of users (general or expert ones).

B. *Dimensions of the proposed taxonomy*

The proposed taxonomy has three main dimensions. The first dimension (named cause) of the taxonomy covers causes of vulnerabilities. We use CWE project for classifying this dimension hierarchically in such a way that the taxonomy could covers possible causes of network vulnerabilities. As mentioned before, The CWE is a project that provides a common language of discourse for discussing, finding and dealing with the causes vulnerabilities. We have used this project because it is one of the most complete and latest projects in this context covering all previous taxonomies. The second dimension (named location) of taxonomy covers the locations of network vulnerabilities. In the proposed taxonomy the locations of network vulnerabilities are specified by both network elements (equipments and facilities) and network activities. The third dimension (named impact) of the taxonomy covers impacts of vulnerabilities. In other words, which groups of security dimensions are damaged due to each exploited vulnerability? Each vulnerability could be specified by the CVE (Common Vulnerability Exposures) identifier or any other standard and unique vulnerability identifier. After determining the dimensions of taxonomy, each dimension hierarchically divides to suitable sub categories in the first, second, third and maybe more layers. The subcategories of different layers of cause dimension are a collection of CWE causes that are more related to network vulnerabilities. The subcategories of first layer of location dimension are defined based on ITU-T X-805 security architecture layers, planes and dimensions. The subcategories of the other layers of

location dimension are defined based on more related references such as [33, 7] and the results of researches and experiments in this center (as one CSIRT). Table II shows the dimensions of the proposed taxonomy.

TABLE II. AN OVERVIEW OF THE PROPOSED TAXONOMY

Cause				Location								Impact	
				Network elements				Network activities					
Layer1	Layer2	Layer3	...	Layer1	Layer2	Layer3	...	Layer1	Layer2	Layer3	...	Layer1	layer2
Subc1	Subc11	Subc111 Subc112	... ...	Subc1	Subc11	Subc111 Subc112		Subc1	Subc11	Subc111 Subc112		Subc1	Subc11
	Subc12	Subc121 Subc122			Subc12	Subc121 Subc122			Subc12 ...	Subc121 Subc122			Subc12 ... ...
Subc2	Subc21	Subc211 Subc212		Subc2	Subc21	Subc211 Subc212		Subc2	Subc21	Subc211 Subc212		Subc2	Subc21
	Subc22	Subc221 Subc222			Subc22	Subc221 Subc222			Subc22 ...	Subc221 Subc222			Subc22 ...
....	....			... ...	... ...			... ...	...				...

1) The first dimension (Cause)

The first dimension of the proposed taxonomy covers causes of vulnerabilities. For classifying this dimension hierarchically in such a way that the taxonomy could covers almost all of the possible causes of network vulnerabilities, the CWE project is used. We have used this project because it is one of the most complete and latest projects in this context covering all previous taxonomies. We study the CWE project and choose the causes which are more associated with network vulnerabilities. In other words, CWE cross section mapped for network vulnerabilities is provided. The first layer of the first dimension (cause) in the proposed taxonomy includes implementation (coding) errors, environment errors and configuration errors. The classification of the first dimension (cause) of the proposed taxonomy demonstrated in tree structure to illustrate the hierarchically structure of this dimension more obviously. Fig. 2 shows the tree structure of the first dimension.

Coding errors are typically introduced during code development, including specification, design, and implementation that lead to the vulnerability. There are different kinds of coding errors that are classified in the next layer of the dimension. Environment errors include everything that is outside of the source code but is still critical to the security of the product that is being created. Because the issues covered by these errors are not directly related to source code, they are separated from the coding errors. Errors related to .NET or J2EE are samples of these kinds of errors.

Configuration errors are typically introduced during the configuration of the networks or part of it. User faults in configuring network elements (e.g. CVE-2009-0399), network elements default configuration (e.g. CVE-2009-0621, CVE-2008-4311), and incorrect and incomplete functions and settings of some parts of the functions or components of the network (e.g. CVE-2009-0641, CVE-2008-5027) all are samples of configuration errors.

2) The second dimension (Location)

In the proposed taxonomy, we consider both of network elements (security layers) and network activities (security planes) in the location dimension because a network vulnerability is occurred on the intersection of a network element and activity. Therefore, the location dimension in the proposed taxonomy included two main parts: network elements and network activities. Then each part is independently divided to suitable sub categories in the first, second, third and maybe more layers.

a) Network elements:

The classification of first part (network elements) of the second dimension of the proposed taxonomy is summarized in table III. The classification of layer2 is done in such a way that could be covered all groups of network infrastructures, services and network-based applications to provide proper solution to classify each subcategory of the first layer.

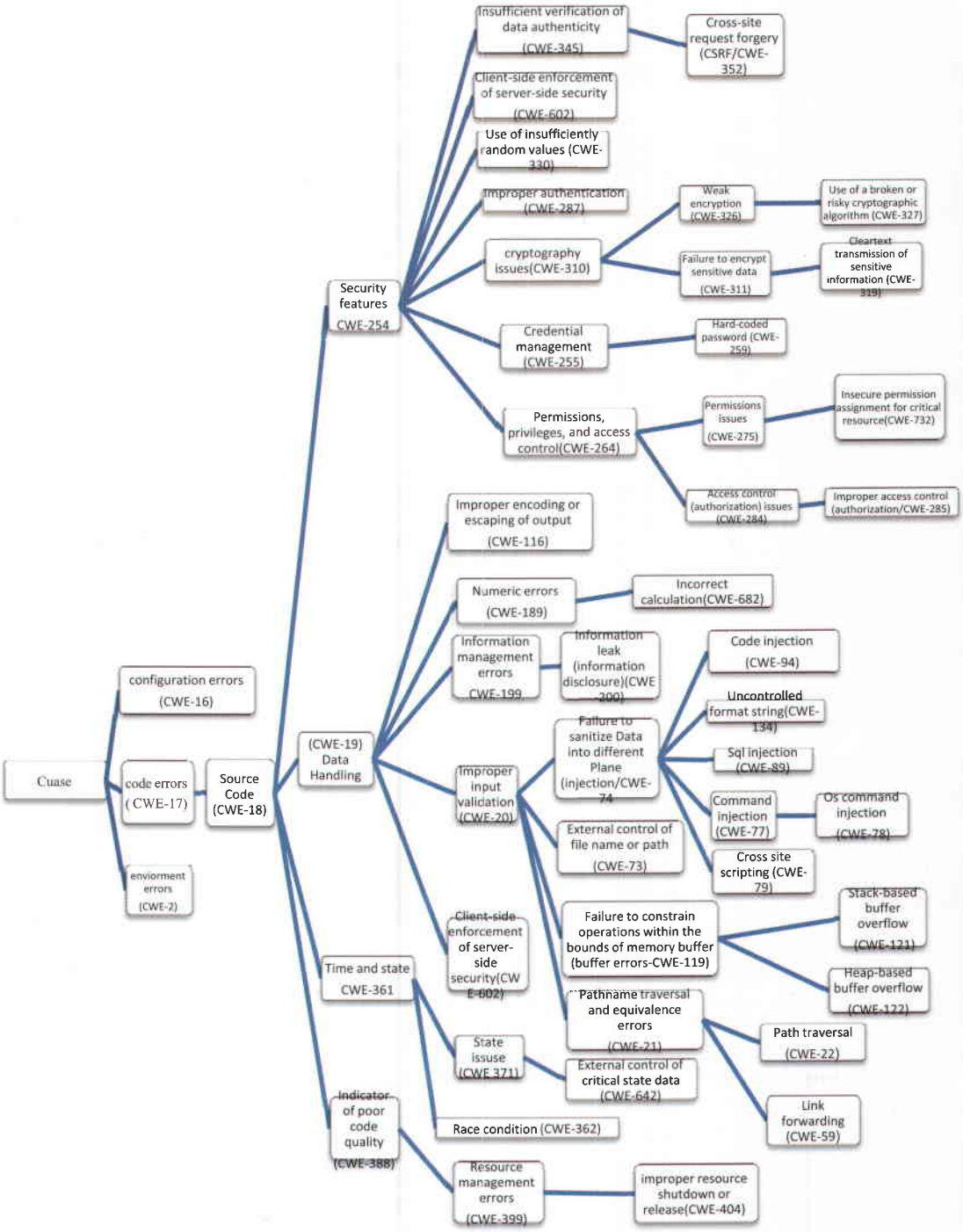

Fig. 2. The classification of the first dimension (cause)

As you can see in table III, the first layer of network elements includes network infrastructure, network services and network-based applications. The network infrastructure consists of the network transmission facilities as well as individual network appliances. In fact, infrastructure represents the fundamental building blocks of networks, their services and applications. Therefore, network infrastructure could be divided into three main parts: network appliances, communication facilities andplatforms. All kinds of hardware or software equipments which create a network are considered as network appliances. Examples of components that belong to the network appliances are individual routers, switches, bridges and firewalls. Communication facilities include different types of communication links that could be existed between network appliances. Communication links are different with respect to type of network. Platforms include platforms of network elements such as operating systems of routers, switches, servers and so on.

TABLE III. THE CLASSIFICATION OF NETWORK ELEMENTS

Layer1	Layer2	Layer3
Network infrastructure	Network appliances	Routers
		Switches
		Bridges
		firewalls
		...
	Communications facilities	Point-to-Point WAN Links
		Ethernet Links
		...
	Platforms	OS
		DB
		...
Network services	basic transport services	Carrier Facilities (DS-1, DS-3)
		Frame Relay
		ATM
		...
	Basic protocols	ARP/RARP
		NDP
		IP(IPv4, IPv6)
		TCP
		...
	Basic services	Name service
		Time
		RPC
		DHCP
		...
	Application services	WEB
		Mail
		Print
		Directory
		AAA
		File sharing
		...
	Value-added services	VOIP
		VPN
		Location services
		800-services
		QoS
		Instant messaging (IM)
		...
Network-based applications	Basic applications	File transport
		File sharing
		Web browsing/ Web browsers
		Directory assistance
		Network-based voice messaging
		e-mail
		VOIP
		Instant messaging
		...
	Advanced applications	CRM
		Human resource systems
		Electronic/mobile commerce
		Network-based training
		Video collaboration
		...

The network services are divided into five groups: basic transport services such as ATM and frame Rely, basic protocols such as ARP and IP, basic services such as RPC and DHCP, application services such as Mail and WEB and value-added services such as VOIP and VPN. The network-based applications are divided into basic applications and advanced applications.

In the proposed taxonomy, the number of layers could be extended to more than 3 layers. For example, for adding Cisco routers series, firstly a "Cisco series" entry should be created under "network infrastructure→ network appliances →routers" category. Finally, the leaf nodes of the structure should be specific versions of a product. If a category for the product does not exist, a new category should be created using the above method, thus allowing for specific versions to reside in that category.

b) Network activities:

This part of taxonomy could provide a complete classification for all network activity types. After determining network elements in the first part of location dimension, the group of network activities that the vulnerability is belonged to is also determined in the second part of the location dimension. The first layer of network activities includes management activities, control activities and end-user activities. The classification of network activities is summarized in table IV.

TABLE IV. THE CLASSIFICATION OF NETWORK ACTIVITIES

Layer1	Layer2
Management activities	Operation
	Administration
	Maintenance
	Provisioning
	Configuration
	Security
Control activities	Send / receive control information
	Processing control information
	Updating control information
End-user activities	For Using a network that only provides connectivity
	For using a network services
	For using network-based applications

Network management activities are considered as one of the most important kinds of network activities and almost done by network administrators, security administrators periodically. These activities support both OAM&P (operation, administration, maintenance and provisioning) and FCAPS (fault, capacity, administration, provisioning, and security) functions related to network infrastructure, services and applications [7]. OAM&P and FCAPS have same purpose. However, OAM&P covered wider area in comparison with FCAPS. Therefore, the options of the second layer of network management activities classification are selected from both OAM&P and FCAPS in such a way that they covered all possible network management activities. It should be noted that the network carrying the traffic for these activities may be in-band or out-of-band. Administration of user mailboxes in an email application, provision of authorized users of an IP service, and configuration of an individual router or switch are samples of network management activities for network applications, services and infrastructure, respectively.

The control activities enable the efficient delivery of information, services and applications across the network [7]. It typically involves machine-to-machine communications of information that allows the machines (e.g., switches or routers) to determine how best to route or switch traffic across the underlying transport network. This type of information is sometimes referred to as control information. So that control activities include sending, receiving, updating and processing control information to provide the efficient delivery of information, services and applications across the network. The network carrying these types of messages may be in-band or out-of-band with respect to the service provider's user traffic. For example, IP networks carry their control information in-band. Example traffic of this type includes routing protocols, DNS, SIP, SS7, Megaco/H.248, etc. There are different kinds of control information such as routing tables, switching tables, etc. Sending routing tables to a router, Sending message to initiate and maintain the VoIP sessions by the SIP protocol, controlling the delivery of email by SMTP and POP protocols are samples of network control activities for network infrastructure, services and applications, respectively.

Different kinds of end-user activities are related to accessing and using the service provider's network by customers for different purposes such as using a network that only provides connectivity, using a network services or using network-based applications [7]. End-user data flows are very important in these groups of activities. Transporting user data or voice through network appliances, as well as while it is being transported across communications links, user's conversation related to VoIP service and user's credit card number in an e-commerce application are samples of end-user data for network infrastructure, services and applications, respectively.

3) The third dimension (Impact)

The type of security dimensions that are damaged by the vulnerability is determined in the third dimension of the taxonomy. The classification of the third dimension of the proposed taxonomy is summarized in table V. The first layer of this dimension includes eight security dimensions of ITU-T X-805 security architecture. Each subcategory of the first layer is also divided into some subcategories in the second layer with respect to their counter mechanisms. Determining the impact kind (the damaged security dimension) of the vulnerability in a network is most important and helpful for security assessment of the network. In addition, it is considerable to determine necessary security actions to deal with vulnerabilities.

It is possible that the exploited vulnerability threatens more than one of the security dimensions and is related to more than one kind of network activities or elements. With respect to nature of vulnerabilities which are maybe combinational (i.e. combination of a specific kind of network elements with a specific kind of network services, two specific services or other), the

proposed taxonomy should cover these groups of vulnerabilities. Therefore, it doesn't have a mutual exclusivity property.

V. CASE STUDY

In this section, we present a result of analyzing twenty random vulnerabilities based on the proposed taxonomy. These vulnerabilities are selected from vulnerability databases and reports such as national vulnerability database (NVD) [36], securityfocus [37], milw0rm [38]. Then, they are divided between our three expert teams. In addition, we design a form based on the proposed taxonomy to gain required information about vulnerabilities. The result of our analysis is one matrix that demonstrates the distribution of network vulnerabilities based on their causes, locations and impacts for the selected sample. More detailed information about the vulnerabilities and also results of classifying them by the proposed taxonomy are presented in Appendix A.

TABLE V. THE CLASSIFICATION OF THE THIRD DIMENSION (IMPACT)

Layer1	Layer2
Access control	Access control lists
	Intrusion detection and Prevention (ID&P) system
	Role-based Access control
	...
Authentication	Logins and passwords
	X.509 certificates
	Kerberos
	Radius ،Diameter
	...
Non-repudiation	Log file from web servers
	Digitally signed emails and other communications
	...
Data confidentiality	Encryption (3DES, AES)
	Access control Lists
	File permissions
	...
Communication security	VPN technologies Like IPsec and L2TP
	MPLS tunnels
	Private (leased) lines
	Separately managed networks
	...
Data integrity	HMAC(MD5, SHA-1, SHA-256)
	CRCs
	...
Availability	Redundancy and backup
	Firewalls
	ID&P techniques
	Business continuity plans
	Service level agreements with vendors of critical infrastructure
	...
Privacy	Application-specific proxies
	Network Address translators
	Identity protection
	Anonymity
	...

We construct one matrix that offers different perspectives of network vulnerabilities. The three dimensional matrix, given in table VI, cross references network vulnerabilities' locations (intersection of network elements and network activities), causes and their impacts. After examining each vulnerability, we specify the place of that in the cell of matrix that corresponds to its classification in our proposed taxonomy. We use this matrix to gain valuable information about network vulnerabilities. First, we will use this matrix to develop an intuition about which network elements and activities are most vulnerable to. For example, we find that most of the examined network vulnerabilities are occurred on the intersection of network services (network element) and control activities (network activities) in the first place, the intersection of network infrastructure and management activities in the second place and the intersection of Network-based applications and user-end activities in the third place. Second, we use the matrix to gain valuable information about impact of network vulnerabilities. For example, we find that the number of availability impact is higher than other network vulnerabilities' impact. Third, we examine network vulnerabilities' impact with respect to their locations. For example, most of the vulnerabilities that occur on the intersection of network services and control activities lead to availability impact. Forth, we infer from this matrix to find the most prevalent causes of network vulnerabilities, their locations and impacts. For example, we find that most of the examined network vulnerabilities are due to coding errors in first place and configuration errors in second place. In addition, all of the coding error vulnerabilities are due

TABLE VI. THE THREE DIMENSIONAL NETWORK VULNERABILITY MATRIX: THIS MATRIX CROSS REFERENCES THREE DIMENSIONS: VULNERABILITY LOCATIONS, VULNERABILITY CAUSES AND VULNERABILITY IMPACTS BASED ON THE PROPOSED TAXONOMY AND DEMONSTRATES THE CLASSIFICATION RESULTS OF 20 VULNERABILITIES.

		cause												
		Configuration errors			Coding errors							Environment errors		
					Data handling			Security features			...			
Location	Network infrastructure – management activities	AC: 2	DC: 2	AV: 2	AC: 1	DC: 1	AV: 1	AC:0	DC: 2	AV:1		AC: 0	DC: 0	AV: 0
		AU:0	CS:0	PR:0	AU: 0	CS:0	PR:0	AU: 1	CS:0	PR:		AU:0	CS:0	PR:0
		NR:0	DI: 2		NR:0	DI: 1		NR:0	DI: 1			NR:0	DI: 0	
	Network infrastructure – control activities	AC:0	DC: 1	AV: 1	AC: 1	DC:0	AV: 2	AC: 0	DC: 0	AV: 0		AC: 0	DC: 0	AV: 0
		AU:0	CS:0	PR: 0	AU:0	CS:0	PR:0	AU:0	CS:0	PR:0		AU:0	CS:0	PR:0
		NR:0	DI:0		NR:0	DI:0		NR:0	DI: 0			NR:0	DI: 0	
	Network infrastructure – User-end activities	AC: 1	DC: 1	AV: 1	AC: 0	DC: 0	AV: 0	AC: 0	DC: 0	AV: 0		AC: 0	DC: 0	AV: 0
		AU:0	CS:0	PR:0	AU:0	CS:0	PR:0	AU:0	CS:0	PR:0		AU:0	CS:0	PR:0
		NR:0	DI: 1		NR:0	DI: 0		NR:0	DI: 0			NR:0	DI: 0	
	Network services– management activities	AC: 0	DC: 0	AV: 0	AC: 0	DC: 0	AV: 0	AC: 0	DC: 0	AV: 0		AC: 0	DC: 0	AV: 0
		AU:0	CS:0	PR:0	AU:0	CS:0	PR:0	AU:0	CS:0	PR:0		AU:0	CS:0	PR:0
		NR:0	DI: 0		NR:0	DI: 0		NR:0	DI: 0			NR:0	DI: 0	
	Network services– control activities	AC:0	DC:1	AV: 1	AC: 3	DC: 4	AV: 6	AC: 0	DC: 0	AV: 0		AC: 0	DC: 0	AV: 0
		AU:0	CS:0	PR: 0	AU:0	CS:0	PR: 0	AU:0	CS:0	PR:0		AU:0	CS:0	PR:0
		NR:0	DI: 1		NR:0	DI: 4		NR:0	DI: 0			NR:0	DI: 0	
	Network services– user-end activities	AC: 0	DC: 0	AV: 0	AC: 0	DC: 0	AV: 0	AC: 0	DC: 0	AV: 0		AC: 0	DC: 0	AV: 0
		AU:0	CS:0	PR:0	AU:0	CS:0	PR:0	AU:0	CS:0	PR:0		AU:0	CS:0	PR:0
		NR:0	DI: 0		NR:0	DI: 0		NR:0	DI: 0			NR:0	DI: 0	
	Network-based applications – management activities	AC: 0	DC: 0	AV: 0	AC: 0	DC: 1	AV: 1	AC: 0	DC: 0	AV: 0		AC: 0	DC: 0	AV: 0
		AU:0	CS:0	PR:0	AU: 0	CS:0	PR:0	AU:0	CS:0	PR:0		AU:0	CS:0	PR:0
		NR:0	DI: 0		NR:0	DI: 1		NR:0	DI: 0			NR:0	DI: 0	
	Network-based applications – control activities	AC: 0	DC: 0	AV: 0	AC: 0	DC: 0	AV: 0	AC: 0	DC: 0	AV: 0		AC: 0	DC: 0	AV: 0
		AU:0	CS:0	PR:0	AU:0	CS:0	PR:0	AU:0	CS:0	PR:0		AU:0	CS:0	PR:0
		NR:0	DI: 0		NR:0	DI: 0		NR:0	DI: 0			NR:0	DI: 0	
	Network-based applications – user-end activities	AC: 0	DC: 0	AV: 0	AC: 2	DC: 2	AV: 1	AC: 0	DC: 0	AV: 0		AC: 0	DC: 0	AV: 0
		AU:0	CS:0	PR:0	AU: 2	CS: 2	PR:0	AU:0	CS:0	PR:0		AU:0	CS:0	PR:0
		NR:0	DI: 0		NR:0	DI: 3		NR:0	DI: 0			NR:0	DI: 0	

to problems in data handling (most of them) and security features. Fifth, this matrix indicates which causes of vulnerabilities in a certain location tend to have and lead to what groups of vulnerability impacts. For example, we find that most of the configuration error vulnerabilities are occur on the intersection of network infrastructure and management activities, most of the data handling vulnerabilities are occur on the intersection of network services and control activities and on the Network-based applications and user-end activities and finally most of the security feature vulnerabilities are on the intersection of network infrastructure and management activities. With respect to vulnerabilities' impact, most of the configuration error vulnerabilities lead to data confidentially and availability impact, most of the data handling vulnerabilities lead to availability impact and most of the security feature vulnerabilities lead to data confidentially impact.

VI. EVALUATION OF THE PROPOSED TAXONOMY

In this section, we evaluate the proposed taxonomy based on the basic requirements of a taxonomy. We consider the proposed taxonomy to see whether the requirements are met or not.

A. Requirements

A good taxonomy must be providing the basic requirements of the taxonomy. In other words, for a taxonomy to be useful it has to meet some basic requirements. Therefore, it is important to define the taxonomy's requirements. They are defined in [39]. In this section, those requirements (except mutual exclusivity that is not necessary for vulnerability

taxonomies) are considered in regards to the proposed taxonomy to evaluate it. Except structured requirement, we refer to our case study and results of classifying samples of vulnerabilities to evaluate other requirements.

1) Being Structured

If the taxonomy be structured, it could be become generally approved and accepted by the security industry. The proposed taxonomy is based on ITU-T X-805 security architecture providing a comprehensive and top-down perspective of network security for network elements, services, and applications and can be applied to various kinds of networks. Therefore, it is structured and acceptable.

2) Completeness

A taxonomy in this context is complete if it could cover all possible vulnerabilities and classify them. Although it is a hard requirement to prove, classifying samples of actual vulnerabilities by the proposed taxonomy to some degree shows the completeness of the proposed taxonomy. In other words, all of these vulnerabilities are properly classified with the taxonomy. On the other hand, the best reason to show the completeness of the proposed taxonomy is ITU-T X-805 security architecture. In addition, it is an extendable taxonomy so it could be adaptable with probable future vulnerabilities.

3) Being Comprehensive/ Deterministic/ unambiguous/ terms well defined

A comprehensible taxonomy will be able to be understood by those who are in the security field, as well as those who only have an interest in it. The determinism means the procedure of classifying must be clearly defined. Unambiguous means each category of the taxonomy must be clearly defined so that there is no ambiguity as to where a vulnerability should be classified. Terms well defined means there should be no confusion as to what a term means. As it is so obvious, these four requirements have same goal and are similar property so we consider them in one group.

As mentioned before, we select twenty random vulnerability and divide them between three expert groups (seven expert person) in our center to classify the vulnerabilities. Similar functionality of all experts in using the taxonomy to some degree shows determinism and unambiguous property of the proposed taxonomy. After studying the procedure of classification in our proposed taxonomy, all of the experts gain same perception about the taxonomy and without any problem use it for classifying vulnerabilities. Meanwhile, the results show that there is enough discriminating criteria in the taxonomy to prevent specifying more than one subcategory in each layer of each dimension (except in required conditions) for each vulnerability.

Besides, we obviously describe the procedure by which classification occurs in the proposed taxonomy. The proposed taxonomy has three dimensions and each of them is separately classifying as different subcategories in one or more layers. The names of each dimension described each dimension obviously. In addition, the terms and terminologies used in the proposed taxonomy are almost prevalent and unambiguous. Therefore, there is no confusion as to what a term means. In the proposed taxonomy uses the Common Vulnerabilities and Exposures (CVE) project to determine vulnerabilities. The CVE project is well established and provides terminology for describing vulnerabilities.

4) Usefulness

A useful taxonomy will be able to be used in the security industry. For example, the taxonomy should be able to be used by incident response teams. For the proposed taxonomy to be useful, the security community must see it as useful and use it in some way. As a result, Usefulness is a requirement that cannot currently be tested. However, as shown in previous section, classifying the number of vulnerabilities, which are selected randomly, with the proposed taxonomy and also using it for analyzing vulnerabilities in our center partly demonstrate the usefulness of the proposed taxonomy. A template form based on the proposed taxonomy is used as a vulnerability analysis form in our center.

VII. Conclusion

The taxonomies of vulnerabilities have many advantages especially for understanding, analyzing, detecting and even assessing them. In this paper, after studying the existing vulnerability taxonomies and their features, we proposed a new multi dimensional and hierarchical taxonomy for classifying network vulnerabilities. For this purpose, we also used ITU-T X-805 security architecture and CWE project to provide a taxonomy that could be able to cover all kinds of network vulnerabilities. The proposed taxonomy is considerable both in providing a general classification and in analyzing network vulnerabilities. The results of evaluation the proposed taxonomy based on the basic requirements for a proper taxonomy and classification of the samples of vulnerabilities and analyzing them by using this taxonomy demonstrate the helpfulness of it.

Appendix A

A number of vulnerabilities were classified by using the proposed taxonomy to show how the taxonomy is applied practically. Table APP.I shows the classification result. Different centers have been established for identification and consideration of vulnerabilities detected in computer systems. They are examining the reported vulnerabilities and publishing them if their correctness is proven. NVD, SecurityFocus and milw0rm are samples of these centers. Each of these centers uses a unique identifier

TABLE APP.I Classification results

Vulnerability	Cause	Location		Impact
		Network elements	Network activities	
CVE-2009-2832	Coding errors→ source code→ data handling→ improper input validation→ buffer errors	Network services→ application services→ FTP service→ Apple FTP server→ before 10.6.2 / Network infrastructure→ platforms→OS→client→ Mac OS X	Control activities→ processing control information	Access control / availability
CVE-2009-1892	Configuration errors → when the dhcp-client-identifier and hardware ethernet configuration settings are both used	Network services →Basic services→DHCP→ Debian→3	Control activities → processing control information → processing of certain DHCP requests	Confidentially/data integrity/availability
CVE-2009-1730	Coding errors→ source code→ data handling→ improper input validation → Pathname traversal and equivalence errors→ path traversal	Network services→ application services→ TFTP service→ NetMechanica NetDecision TFTP Server→4.2	Control activities → sending and receiving control information	Data Confidentially/data integrity/availability
CVE-2007-1301	Coding errors→ Source code → data handling → improper input validation → buffer errors → Stack-based buffer overflow	Network services →application services → mail service → MailEnable Enterprise and Professional Editions → before 2.37	Control activities→ Processing control information → IMAP "APPEND" command	Access control/data confidentially/data integrity/availability
CVE-2008-1358	Coding errors→ Source code → data handling → improper input validation → buffer errors → Stack-based buffer overflow	Network services→ application services → mail service → Alt-N Technologies MDaemon→ 9.6.4	Control activities → sending and receiving control information → IMAP "FETCH" command	Access control/data confidentially/ data integrity/availability
CVE-2009-1602	Coding errors→ Source code → data handling → improper input validation → buffer errors	Network services→ application services → mail service→ Quick 'n Easy Mail Server → 3.3	Control activities → sending and receiving control information → SMTP commands	availability
CVE-2009-3315	Coding errors→ source code→ data handling→ improper input validation → Failure to sanitize Data into different Plane (injection) → Sql injection	Network-based applications → Advanced applications→ CMS → NeLogic Nephp Publisher Enterprise → 3.5.9 and 4.5	End-user activities → For using network-based applications→ admin/index.php → Username field	data confidentially/ data integrity/availability
Bid 33944	Coding errors→ source code→ data handling→ improper input validation → Failure to sanitize Data into different Plane (injection) → Cross site scripting	Network-based applications → Advanced applications→ CMS → Yektaweb Academic	End-user activities → For using network-based applications	Access control/ Authentication/ Data confidentially/ Communication security/ data integrity
milw0rm 2438	Coding errors→ source code→ data handling→ representation errors → improper sanitization of special elements → Failure to sanitize special element→ Failure to sanitize multiple leading special elements	Network-based applications → Advanced applications→ CMS → Kietu Hit	End-user activities → For using network-based applications	Communication security/Access control/Authentication/
CVE-2009-3663	Coding errors→ source code→ data handling→ Failure to sanitize Data into different Plane (injection)→ Uncontrolled format string	Network services → application services → WEB service → WEB server → httpdx Web Server →1.4	Control activities → sending and receiving control information→ h_readrequest function	Data confidentially / data integrity/ availability

CVE-2009-3636	Coding errors→ source code→ data handling→ improper input validation → Failure to sanitize Data into different Plane (injection) → Cross site scripting	Network-based applications → Advanced applications→ CMS → TYPO3 → 4.0.13 and earlier	End-user activities → For using network-based applications→ the Install Tool subcomponent	Data integrity
CVE-2009-3758	Coding errors→ source code→ data handling→ improper input validation → Failure to sanitize Data into different Plane (injection) → Sql injection	Network-based applications→ WEB applications → WEB-based applications → WEB console → Citrix XenCenterWeb	Management activities → administration → XenServer Resource Kit	Data confidentially/data integrity/availability
CVE-2006-3291	Configuration errors → changing Admin Access configuration from "Default Authentication" to "Local User List Only"	Network infrastructure → network appliances → wireless access point / Bridge→ Cisco * 350 Wireless Access Point and Wireless Bridge * 1100 Wireless Access Point * 1130 Wireless Access Point * 1200 Wireless Access Point * 1240 Wireless Access Point * 1310 Wireless Bridge * 1410 Wireless Access Point Network infrastructure → platforms → OS → Cisco IOS → 12.3(8)JA and 12.3(8)JA1	End-user activities → web-browser interface	Access control / data confidentially / data integrity / availability
CVE-2009-1155	Coding errors→ source code→ security features→ improper authentication	Network infrastructure→ network appliances → security devices → firewall → Cisco ASA/ Cisco PIX → 5500 series / 7.1(1) through 7.1(2)82, 7.2 before 7.2(4)27, 8.0 before 8.0(4)25, and 8.1 before 8.1(2)15	Management activities → security → → AAA override-account-disable is entered in a general-attributes field	Authentication/ confidentially
CVE-2009-2049	Configuration errors → enable RFC4893 BGP routing	Network infrastructure → platforms → OS → Cisco IOS → Cisco IOS 12.x Cisco IOS R12.x Cisco IOS XE 2.3.x Cisco IOS XE 2.4.x	Control activities → Processing control information → processing of BGP update messages	Availability
CVE-2008-3807	Configuration errors → configured for linecard redundancy	Network infrastructure→ network appliances → routers → Cisco → uBR10012 Series Network infrastructure → platforms → OS → Cisco IOS → 12.2 and 12.3	Management activities→ Administration → enable Simple Network Management Protocol (SNMP) read/write access to the device	Access control / data confidentially / data integrity / availability
CVE-2009-1473	Coding errors→ source code→ security features→ cryptography issues	Network infrastructure → network appliances → switches → ATEN products → ATEN KH1516i IP KVM switch with firmware 1.0.063 and the KN9116 IP KVM switch with firmware 1.1.104	Management activities → security → do not properly use RSA cryptography for a symmetric session-key negotiation	Confidentially / data integrity / availability
CVE-2008-6497	Coding errors→ source code→ data handling→ improper input validation	Network infrastructure → network appliances → router → Neostrada Livebox ADSL Router	Control activities → Processing control information → processing HTTP requests	Availability
CVE-2008-1156	Coding errors → source code → data handling → information management errors → information leak (information disclosure) / Configuration errors	Network infrastructure → platforms → OS → Cisco IOS → 12.0, 12.2, 12.3, and 12.4	Management activities→ security → implementation of Multicast Virtual Private Networks (MVPN)	Access control/ Confidentially / data integrity / availability

CVE-2008-2060	Configuration errors → inline mode and jumbo Ethernet support are enabled	Network infrastructure → network appliances → security devices → IPS (intrusion Prevention System) → Cisco IPS 5.x before 5.1(8)E2 and 6.x before 6.0(5)E2	Control activities → Processing control information → processing of Jumbo Ethernet frames received on a Gigabit network interface	Confidentially

for each vulnerability. CVE, Bid and milw0rm are vulnerability identifier of NVD, Security Focus and milw0rm, respectively. As mentioned before, we randomly select a number of vulnerabilities from NVD, securityfocus and milw0rm. The results of analyzing these vulnerabilities are previously reported in section V.

ACKNOWLEDGMENT

Authors are grateful to expert members of APA-IUTcert for taking part in classifying vulnerabilities presented in case study section of the paper, including SayedHadi Hashemi, Parisa Delparastaran, Maliheh Eebrahimi, niloofar fathi, Elahe Jafari and Peyman Golshani.

REFERENCES

[1] Hansman, S., Hunt, R., "A Taxonomy of Network and Computer Attacks", Comp. & Sec., Vol. 24, No. 1, pp. 31–43, 2005.

[2] Igue, V. M., Williams, R.D., "Taxonomies of attacks and vulnerabilities in computer systems," IEEE communications Surveys and tutorials, vol. 10, no. 1, 2008, pp. 10-19.

[3] http://www.cert.org/stats/

[4] Howard, J. D., Longstaff, T. A., "A Common Language for Computer Security Incidents", Sandia tech. rep. SAND98-8667, Oct. 1998.

[5] Bishop, Matthew A., Computer Security, Addison-Wesley, 2002.

[6] Ristenbatt, M. P., "Methodology for Network Communication Vulnerability Analysis," MILCOM 1988, Vol. 2, 23–26 Oct., pp.493–99.

[7] International Telecommunication Union, Telecommunication Standardization Sector, "Security architecture for systems providing end-to-end communications", ITU-T Rec. X.805, 2003.

[8] Du, W., Mathur, A. P., "Categorization of Software Errors that Led to Security Breaches," Proc. 21st Nat'l Info. Sys. Sec.Conf, 1998.

[9] http://en.wikipedia.org/wiki/Security_Architecture

[10] OWASP Top Ten Most Critical Web Application Security Vulnerabilities. http://www.owasp.org/documentation/topten.html.

[11] http://cwe.mitre.org/

[12] McPhee, W. S., "Operating System Integrity in OS/VS2", IBM Sys. J., vol. 13, no. 3, 1974, pp. 230–52.

[13] Attanasio, C., Markenstein, P., Phillips, R. J., "Penetrating an Operating System: a Study of VM/370 Integrity", IBM Sys.J., vol. 15, no. 1, 1976, pp. 102–16.

[14] Abbott, R. P., "Security Analysis and Enhancements of Computer Operating Systems", Tech. rep. NBSIR 76-1041, Lawrence Livermore Lab., Inst. For Comp. Sci. and Tech./Nat'l.Bureau of Standards, RISOS Project, Washington, DC, Apr.1976.

[15] Bisbey II, R. and Hollingworth, D., "Protection Analysis: Final Report", ISI/SR-78-13, USC/Info. Sci. Inst., Marina Del Rey, CA, May 1978.

[16] Landwehr, C. E., et al., "A Taxonomy of Computer Program Security Flaws," ACM Comp. Surveys, vol. 26, no. 3, Sept.1994, pp. 211–54.

[17] Aslam, T., "A Taxonomy of Security Faults in the Unix Operating System", M.S. thesis, Dept. of Comp. Sci., Purdue Univ.Coast TR 95–09, 1995.

[18] Krsul, I., "Software Vulnerability Analysis", Ph.D. dissertation, Purdue Univ., Coast TR 98–09, 1998.

[19] Du, W., Mathur, A. P., "Categorization of Software Errors that Led to Security Breaches", Proc. 21st Nat'l Info. Sys. Sec.Conf, 1998.

[20] Bishop, M., "Vulnerabilities Analysis", Proc. 2nd Int'l. Symp.Recent Advances in Intrusion Detection, Sept. 1999, pp.125–36.

[21] Welch, D., Lathrop, S., "Wireless Security Threat Taxonomy", Info. Assurance Wksp., IEEE Sys., Man and Cybernetics Soc., 18–20 June 2003, pp. 76–83.

[22] Kamara, S., et al., "Analysis of Vulnerabilities in Internet Firewalls", Comp. & Sec., vol. 22, no. 3, 2003, pp. 214–32.

[23] Gray, A., "An Historical Perspective of Software Vulnerability Management", Info. Sec. Tech. Rep., vol. 8, no. 4, Apr. 2003, pp. 34–44.

[24] Jiwnani, K., Zelkowitz, M., "Susceptibility Matrix: A New Aid to Software Auditing", IEEE Sec. & Privacy, vol. 2, no. 2, 2004, pp.16–21.

[25] Pothamsetty, V., Akyol, B., "A Vulnerability Taxonomy for Network Protocols: Corresponding Engineering Best Practice Countermeasures", Proc. 3rd IASTED Int'l Conf. Commun., Internet, and Info. Tech., 2004, pp. 168–75.

[26] Yongzheng, Z., Xiaochun, Y., "A New Vulnerability Taxonomy Based on Privilege Escalation", Proc. 6th Int'l Conf. Enterprise Info. Sys, 2004, pp. 596–600.

[27] K. Tsipenyuk, B. Chess, andG. McGraw, "Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors," IEEE Sec.& Privacy, vol. 3, no. 6, Nov.–Dec. 2005, pp. 81–84.

[28] W. D. Yu, D. Aravind, and P. Supthaweesuk, "Software Vulnerability Analysis for Web Services Software Systems," Proc. 11th IEEE Symp. Comp. and Commun, 26–29 June 2006, pp. 740–48.

[29] K. Jiwnani and M. Zelkowitz, "Maintaining Software with a Security Perspective," Proc. Int'l Conf. Software Maintenance, 3–6 Oct. 2002, pp. 194–203.

[30] International Organization for Standardization, "Information Processing Systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture," ISO/IEC Standard 7498-2, 1989, <http://www.iso.org>.

[31] International Telecommunication Union, Telecommunication Standardization Sector, "Principles for a Telecommunications Management Network", ITU-T Rec. M.3010, 2000, <http://www.itu.int>.

[32] The Institute of Electrical and Electronics Engineers, "IEEE Standards for Local and Metropolitan Area Networks: Supplement to Standard for Interoperable LAN/MAN Security (SILS)—Security Architecture Framework", IEEE Standard 802.10a, 1999, <http://www.ieee.org>.

[33] McGee, A. R., Vasireddy, S. R., Xie, C., Picklesimer, D. D., Chandrashekhar, U., Richman, S. H., "A framework for ensuring network security", Bell Labs Technical Journal, Vol. 8, No.4, pp.7-27, 2004.

[34] P. G. Neumann, "Denial-of-Service Attacks," ACM Commun,. vol 43. no. 4, Apr. 2000, pp. 136.

[35] Hajian, S., Hendesi, F., Berenjkoub, M., Hashemi, S.H., Golshani, P., "A new taxonomy for network vulnerabilities," Proc. of the 1th Conf. on Cyberspace Security Incidents and Vulnerabilities, Tehran, Iran, June. 10-11 (2009).

[36] National vulnerability database, http://nvd.nist.gov/

[37] www.securityfocus.com

[38] www.milw0rm.com

[39] Lough, D. L., A Taxonomy of Computer Attacks with Applications to Wireless Networks, Ph.D. dissertation, Virginia Tech, Apr. 2001.

Sara Hajian graduated from Iran University of science and Technology with a M.S. degree in Information technology engineering in 2008. She is a member of APA-IUTcert in Isfahan University of Technology. Her research interests include information security, privacy and privacy preserving data mining.

Faramarz Hendessi received the M.Sc. degrees from Isfahan University of Technology, Isfahan, IRAN and the Ph.D. degree from the Carleton University, Ottawa, in 1994. Since 1994, Dr. Hendessi has been with the faculty of the Electrical and Computer Engineering at the Isfahan University of Technology (http://www.iut.ac.ir) where he currently holds an Associate Professor position. He serves on the editorial board of the International Journal of Information and Communication Technology, IRAN, and on the Technical Program Committees of several conferences. Prof. Hendessi's current research interests are in the areas of wireless communications, networking and security. Prof. Hendessi's email address is hendessi@cc.iut.ac.ir.

Mehdi Berenjkoub received the Ph.D. degree from Department of Electrical and Computer Engineering, Isfahan University of Technology in 2000. The title of his dissertation is two-party key distribution protocols in cryptography. He started his work in the same department as an assistant professor from that time. Graduate courses presented by him include Fundamentals of Cryptography, Cryptographic Protocols, Network Security, and Speech Processing. He has supervised more than a dozen M.Sc. students and Ph.D. candidates in related areas. He also was one of the founder members for Iranian Society of Cryptology in 2001. He has continued his cooperation with the society as an active member. He along with his colleagues recently established a research group on Security in Networks and Systems in IUT. He also is responsible for a newly established academic CSIRT in IUT. His current interested research topics are wireless network security and authentication protocols.