ADMIT- A Five Dimensional Approach towards Standardization of Network and Computer Attack Taxonomies

Chanchala Joshi
Institute of Computer Science
Vikram University, Ujjain, M.P. India

Umesh Kumar Singh
Institute of Computer Science
Vikram University, Ujjain, M.P. India

ABSTRACT

This paper proposed a five dimensional taxonomy ADMIT which captures five major classifiers to characterize the nature of attacks. These are classification by attack vector, classification by defense, classification by method, classification by impact and classification by attack target. The classification structure of proposed taxonomy described the nature of attacks thoroughly. The administrator can use the proposed taxonomy to locate strategies that are appropriate for securing their system against vulnerabilities that can be exploited. Use of ADMIT taxonomy in network defense strategies can improve the overall level of security.

Keywords

Network security; Vulnerability; Attack taxonomy

1. INTRODUCTION

Security threats to computers and networks have been a problem since computers and networks were firstly used. With the rapid growth of the Internet, attacks are no longer limited in computer alone. They have created a global threat, causing great damages in individuals, communities and national security. Network attacks are almost a subset of computer attacks but some network attacks are outside the computer attack domain [1]. For security assessment it is necessary to find and classify these attacks. The first step in understanding attacks is to classify them into a taxonomy based on their characteristics. Taxonomy classifies attack into well-defined and easily understood categories. Such classification can be used for performing a systematic security assessment of a system.

Taxonomy provides a way to know about attacks at a level higher than a simple list of vulnerabilities. It provides a classification system that ideally suggests ways to mitigate attacks by prevention, detection and recovery. It can aid risk management by identifying vulnerabilities and making attacker characteristics explicit. Ideally its insights can predict future attacks by exposing unguarded areas. Every attack is performed by someone and every attacker has an identity and the motive of the attack is to do certain thing. An attack targets some service or layer exploiting vulnerability. Each of these attack elements or say dimensions is necessary to understand which includes the whole process of attack. Therefore useful and standard taxonomy should answer the following questions:

i. Who is the attacker?
ii. How to face the attack?
iii. How is it attacked?
iv. What are the results?
v. What is the target?

The proposed taxonomy ADMIT answers the each question in turn. Taken altogether the attack vector, defense, method, impact and the target, describe the nature of attack. ADMIT provides useful information to the network administrator. This paper provides a mean to classify vulnerabilities with their impact and also with defensive strategies.

2. MOTIVATION

One of the major problems in computer and network system security assessment is lack of standard vulnerability categorization scheme called taxonomy. A standard vulnerability categorization scheme also aids in finding general trends which are responsible for existence of vulnerabilities. Many of the attempts have been made in this direction in the past but still this issue is unresolved. The overall objective of this research work is to analyze different categories of prominent vulnerability taxonomies to identify the level of abstraction and common factors for standardization of network vulnerability taxonomy.

3. RELATED WORK

One of the first taxonomies to be developed was given in RISOS (Research In Secure Operating Systems) project [3]. The RISOS security taxonomy was based on flaws found in three operating systems: IBM’s OS/MVT for the IBM 360, UNIVAC’s 1100 Series operating system and Bolt Beranek and Newman’s TENEX system for the PDP-10. The classification consisted of seven categories. The main contribution of this study was the classification of integrity flaws found in operating systems. It also led to classify the same flaw in multiple categories

Protection Analysis (PA) Taxonomy [4] was one of the earliest to address security concerns. The objective of the PA project was to provide a basis for categorizing protection errors according to their security relevant properties using an automated and pattern-matching approach. This taxonomy was based on 100 flaws found in six different operating systems. It had four global categories: improper protection (initialization and enforcement), improper validation, improper synchronization and improper choice of operand or operation. The categories in this taxonomy were broad and the same flaw was classified into multiple categories. The contribution of this study was the introduction of several types of security flaws like allocation or deallocation of residuals and serialization errors that remained relevant.

Aslam defined a classification of security faults [5, 6] in the Unix Operating System. He focused on UNIX operating system flaws only and presented three main categories: Operational fault, Environmental fault and Coding fault. Coding faults, comprising faults introduced during software development and Operational faults, resulting from improper installation of software, unexpected integration incompatibilities, or when a programmer fails to completely understand the limitations of the run-time modules.

Krsul [7] extends Aslam’s work and developed a detailed taxonomy. Main categories proposed in this taxonomy were: Design, Environmental assumptions, Coding faultsand Configuration errors. In proposed scheme, there is ambiguity in distinguishing between objects and attributes because of interpretation scope permitted by taxonomy. It also fails to elaborate on how assumptions lead to vulnerabilities.

Bishop [8] analyzed the RISOS, PA and Aslam's taxonomies and showed that these classes could be mapped onto each other. Bishop presents taxonomy of UNIX vulnerabilities by classifying them with explicit goal of describing a technique to find vulnerabilities. Bishop's work focused on categorizing security vulnerabilities in software to assist security practitioners in maintaining more secure systems through an understanding of these vulnerabilities. John Howard [9] extended this idea in his work in which he analyzed and classified 4299 security related incidents on the internet. Howard's work was notable because he included attackers, results and objectives as classification categories expanding threat taxonomies beyond the technical details of an attack to include more intangible factors such as an attacker's motivation for conducting an attack.

Kjaerland's [10] study categorized cyber intrusions based on four categories; (1) method of operations, (2) impact of the intrusion, (3) source of the intrusion and (4) target. This study examined the likelihood of attacks against different kinds of targets and the likelihood of various kinds of attacks occurring together on a given target.

Lough [11] proposed an attack-centric taxonomy called VERDICT (Validation, Exposure Randomness, Deallocation, Improper Conditions Taxonomy). Lough focuses on four major causes of security errors: Improper Validation, Improper Exposure, Improper Randomness and Improper Deallocation. Validation refers to improperly validating or unconstrained data which also includes physical security. Exposure involves the improper exposure of information that could be used directly or indirectly for the exploitation of vulnerability. Randomness deals with the fundamentals of cryptography and the improper usage of randomness. Deallocation is the improper destruction of information or residuals of data which also includes dumpster diving. He uses one or more of these characteristics to describe vulnerability within a system. Hansman and Hunt [1] describe Lough's taxonomy as lacking pertinent information that would be beneficial for knowledge bodies such as CERT, to classify day-to-day attacks and issuing advisories. Lough's taxonomy lacks the classification to the type of attack, such as worms, Trojans, viruses, etc.

Chris Simmons [2] created a cyber-attack taxonomy called AVOIDIT which described attacks using five, extensible classifications: Attack Vector, Operational Impact, Defense, Informational Impact and Target. This taxonomy was created as a network taxonomy which unlike previous efforts, allowed the classification of blended attacks. Additionally, it also allowed for the classification of attacks by both operational and informational impacts and was designed to help educate defenders by looking at attacks' various impacts, vectors or target types. While this taxonomy focused exclusively on cyber-attacks, its structure and style were very useful in designing the proposed taxonomy in this paper, especially the ability to view and categorize attacks from Applegate different taxonomic perspectives.

Scott D. [12] proposed cyber conflict taxonomy. Subjects of the taxonomy were entered as either events or entities and then categorized using the categories and subcategories of actions or actors. Each of these categories then further subdivided into increasingly specific subcategories used to describe the defining characteristics of each subject and labeled lateral linkages are used to illustrate the associative relationships between entities and events. The categories were organized in both a hierarchical and associative manner to illustrate the relationships between subjects and categories.

4. PROPOSED TAXONOMY- ADMIT

Development of a successful taxonomy is required to meet some standard properties. E. G. Amoroso [13] lists the well accepted principles of a good classification as: Public acceptance, Comprehensibility, Completeness, Determinism, Mutual exclusion, Repeatability, Unambiguous and Useful. A good taxonomy should adhere to these properties. Applying these requirements for a complete taxonomy a standard taxonomy ADMIT is proposed to classify network and computer vulnerability.

The proposed taxonomy ADMIT uses five major classifiers as five dimensions to characterize the nature of an attack, which are classification by attack vector, classification by defense, classification by method, classification by impact and classification by attack target. The first dimension is used to categorize the attack based on attack vector, a path by which an attacker can access to a host. The second dimension covers the defense, the action taken to protect the system from attack. Method of operation is covered in third dimension, which refers to the methods used by perpetrator to carry out an attack. Fourth dimension covers the impact, the effect of the attack; and the attack target is covered in the fifth dimension.

Fig1 provides an overview of proposed taxonomy.

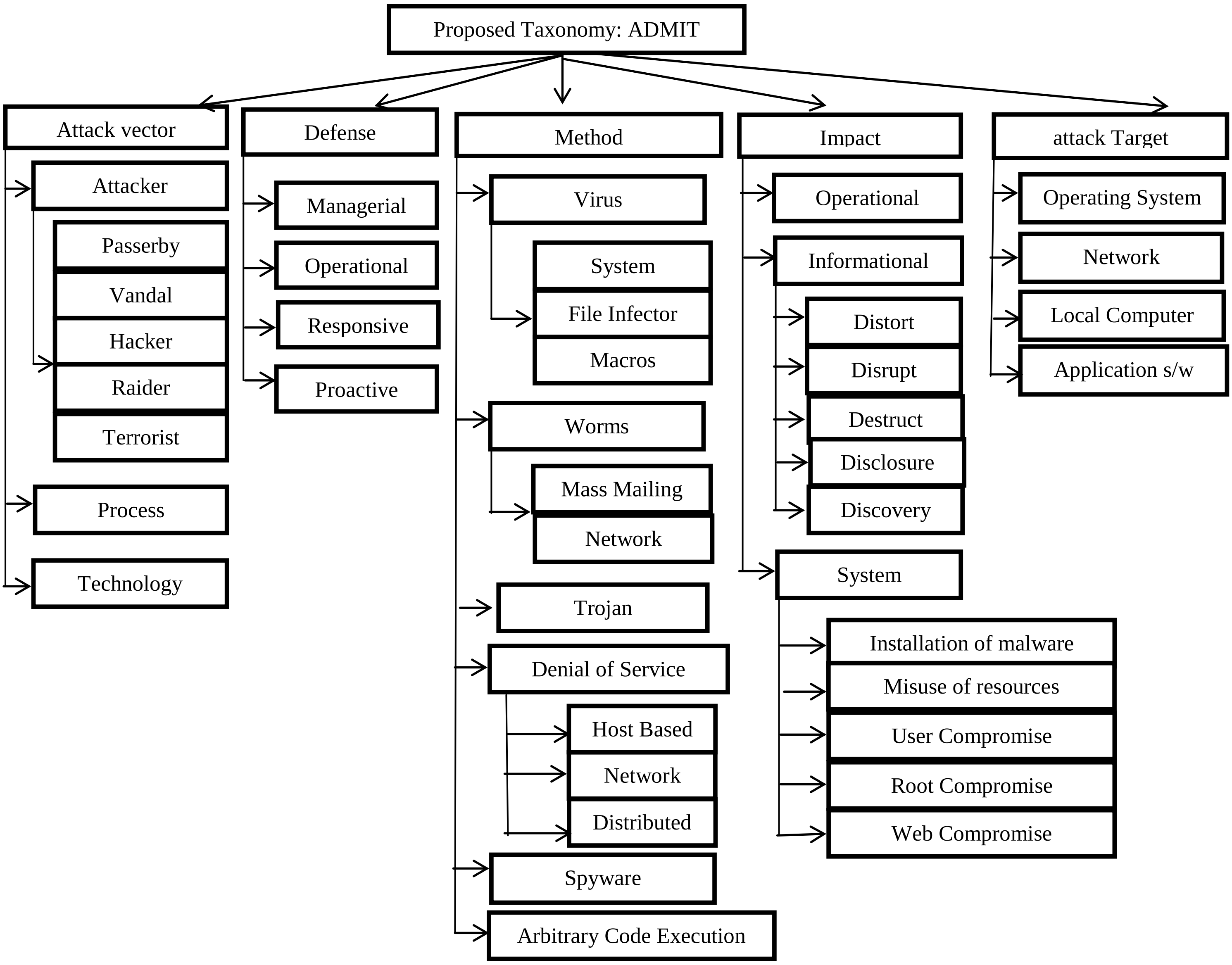

Fig1. ADMIT: An Approach towards Network and Computer attacks

4.1 Classification by Attack Vector

An attack vector describes the path or means by which an attacker attempts to gain access to a network or computer system. This category has been further divided into three sub vectors which are attackers, processes and technology. Each of these subdivisions could be further subdivided into increasingly specific and discrete vector.

4.1.1 Attacker

It is valuable to know who the attacker is in so far. As it will imply what they are likely to do and how well they would be able to do it. The attackers consist of a range of types of people who may launch an attack. These range from hackers to terrorists. Anthony [14] characterizes an attacker according to four dimensions: motive, determination, knowledge and resources:

i. Passerby: Motivated by spontaneity; not determined; very little knowledge; few resources.
ii. Vandal: Desires to make damages, perhaps visibility; moderately determined; little knowledge; few resources necessary.
iii. Hacker: Desires access, motivated by curiosity and interest; highly determined; highly knowledgeable; moderate resources.
iv. Raider: Driven by personal or organizational monetary and/or political gain; highly determined; moderately .highly knowledgeable; moderate resources.
v. Terrorist or Foreign Power: Causes real-world damage by compromise of critical systems, motivated by enmity; very determined; highly knowledgeable; very well resourced with time, money and man-power.

4.1.2 Process

This subcategory describes the vector based on the manipulation of flawed organizational processes. For example suppose an organization allows a visitor to carry their security passes rather than mandating that the credentials be verified directly with the issuing source. Then an attacker might exploit this flawed process to illegitimately gain legitimate credentials to a system.

4.1.3 Technology

This category describes a vector based on the manipulation of technology and technical processes. An example would be exploiting vulnerability in a software program.

4.2 Classification by Defense

This category describes the action taken to protect the system from attack. National Institute of Standard and Technology divided the defense into two dimensions: managerial and operational. Scott [12] expanded the NIST standard by adding responsive defense. A new dimension proactive defense is added in this category.

4.2.1 Managerial

These are defensive techniques and methods adopted by management. It is like an organization's security strategy.

i. Remove from network: Remove infected hosts, preventing further damage.

4.2.2 Operational

These are defensive policies and procedure implemented to improve security of system.

i. White listing: This is a list of permissible connections that are known to the defender.
ii. Reference advertisement: These are the notes provided by the defender to mitigate an attack or a vulnerability database reference number that is used to mitigate the vulnerability or attack.

4.2.3 Responsive

Under this take the appropriate step to correct the situation during exploitation

i. Patch System: [2] Applying patches the vendor has released due to some vulnerability within software in use. When a vulnerability or attack is present, a defender fails to utilize the patches a vendor provides.
ii. Correct Code: [2] An organization may release a code patch to specific application that will close the potential for an attacker to exploit.

4.2.4 Proactive tool

These are defensive techniques or strategies executed by automated system to improve the security of system.

4.3 Classification by Method

This classification refers to the way used by an intruder to carry out an attack. It also tells about the tools used and also about the access point.

4.3.1 Virus

A virus is a piece of code that while running will attach itself with other programs which will run again when those programs are running.

4.3.2 Worms

This is a program that propagates itself by attacking other machines and copying itself with them.

4.3.3 Trojans

It is a program that adds subversive functionality to an existing program.

4.3.4 Denial of Service

Denial of service (DoS) is an attack to deny a victim access to a particular resource or service. It has become one of the major threats and has been rated among the hardest Internet security issues [15]. This subcategory can be further classified into following:

i. Host Based - A Host based DoS aims the attack at specific computer target within the configuration, operating system or software of a host. These types of attacks usually involved resource hogs that aim at consuming all resources on computer crashers which attempts to crash the host system [15].
ii. Network Based - A network based DoS targets the complete network of computers to prevent the network providing normal services. Network based DoS usually occurs in the form of flooding with packets where the network's connectivity and bandwidth are the targets [15].
iii. Distributed - A Distributed Denial of Service (DDoS) is becoming more popular as an attacker's choice of DoS. Distributed denial of service uses multiple attack vectors to obtain its goal [15].

4.3.5 Spyware

It is a type of malware program that is covertly installed and infects its target by collecting information from a computing system without owner's consent.

4.3.6 Arbitrary Code Execution

It involves a malicious entity that gains control through some vulnerability injecting its own code to perform any operation the overall application has permission [15].

4.4 Classification by Impact

4.4.1 Operational Impact

This category describes the impact of an intrusion on victim's operations.

i. Organizational disruption: Impact of an intrusion which causes the disruption of operations within an organization. An example is altering information in a supplier database system to reroute critical supplies to the wrong destinations.
ii. Loss of competitive advantage: It is due to disclosure of plans or confidential data.

4.4.2 Informational Impact

[2] This category describes the impact an intrusion has directly on victim's information.

i. Distort: It's a distortion of information. It usually happens when an attack has caused a modification of life.
ii. Disrupt: It is usually from Denial of Service. When an attack involves disruption, it is an access change or removal of access to victim or information.
iii. Destruct: Destruction is called when an attack has caused a deletion of life or removal of access.
iv. Disclosure [12]: A disclosure of information provides a view of information to the attacker of which they would not have access to.
v. Discovery: It is related to discover information that is not previously known.

4.4.3 Organization's System Impact:

This category describes the impact of an intrusion on the actual system of victim's organization.

i. Installation of malware: The installation of malicious software onto the target host or system.
ii. Misuse of resources: An unauthorized use of system resources.
iii. User Compromise: A perpetrator gaining unauthorized use of user privileges on a host, as a user compromise [10].
iv. Root Compromise: Gaining unauthorized privileges of an administrator on a particular host [10].

v. Web Compromise: A website or web application using vulnerabilities to further an attack [10]. An attack can occur through a web compromise, usually via cross site scripting or sql injection

4.5 Classification by Attack Target

Fifth dimension covers the attack target. Various attacks target a variety of hosts.

4.5.1 Operating System

An attack can be formulated to target vulnerabilities within a particular operating system.

4.5.2 Network

Target a particular network or gain access through a vulnerability within a network or one of the network protocols.

4.5.3 Local Computer

It includes an attack targeting user's local computer.

4.5.4 Application Software

It includes an attack towards specific software. An application can be either client or server. A client application is software that is available to aid a user performing common tasks. A server application is software designed to serve as a host to multiple concurrent users [2].

5. CLASSIFICATION STRUCTURE OF ADMIT

Classification structure describes how the proposed taxonomy can be practically applied. Also the classification structure evaluates and analyzes the proposed taxonomy.

Table 1 shows the classification of ADMIT taxonomy.

Table 1: classification by ADMIT taxonomy

Attack Name	Attack Vector	Defense	Method	Impact	Target
Blaster	Buffer Overflow	White listing Patch System	Network Aware Worm	Distort	Windows NT 4.0, XP, 2000
Chernobyl	Misconfiguration	Reference Advertisement	Virus: File infector	Disrupt	Operating System
Code Red	Buffer Overflow	Patch System	Worm: Network aware	Discovery	Network
Debian Admin	Kernel flaw	Patch System	Virus: System Infector	Root compromise Disrupt	Operating System
Infector	Design flaw	Reference Advertisement	Worm: File infector	Distort	Operating System: DOS
Melissa	Technology: Misconfiguration	Patch System	Worm: Mass mailing	Disrupt	Application: MS Word 97,2000
MS RPC Stack Overflow	Buffer Overflow: Stack	Installed Malware: ACE	Reference Advisement Patch System	Distort	OS: Windows Server
Nimda	Misconfiguration	White listing Reference Advertisement	File Infector, Trojan & DoS	Disrupt	Application: IE
Slammer	Technology: Misconfiguration	Patch system	Worm: Installed malware	Discovery	Network
Yamanner	Technology: Design flaw	Reference Advertisement	Worm: Installed malware	Disrupt	Local computer

6. EVALUEATION OF ADMIT

In this section the proposed taxonomy ADMIT is compared with past taxonomies described in section 1.2. The comparison result represents that how successfully it captures vulnerability attack information and provides a defender countermeasures that can be efficient in preventing attacks.

6.1 Blaster

The Blaster Worm was a computer worm that spread on computers running the Microsoft operating systems Windows XP and Windows 2000, during August 2003 [18].

In Table 2 comparison of Blaster attack with other prominent taxonomies is shown.

Table 2: Blaster attack classification

Lough's taxonomy: VERDICT

Attack Name	Improper Validation	Improper Exposure	Improper Randomness	Improper Deallocation
Blaster	X	X		

Howard's taxonomy

Attack Name	Tools	Vulnerability	Action	Target	Unauthorized Result
Blaster	Program	Buffer Overflow	Modify	Network	Corruption of Information

Hansman and Hunt's taxonomy

Attack Name	1st Dimension	2nd Dimension	3rd Dimension	4th Dimension
Blaster	Network – Aware Worm	Network	CAN-2003-0352	TCP packet flooding DoS

Proposed taxonomy : ADMIT

Attack Name	Attack vector	Defense	Method	Impact	Target
Blaster	Buffer Overflow	White listing Patch System	Computer Worm	Distort	Windows XP, 2000

6.2 *Melissa*

First found on March 26, 1999, Melissa shut down Internet E-mail systems that got clogged with infected e-mails propagating from the virus. Melissa was not originally designed for harm, but it overloaded servers and caused problems [18].

In Table 3, comparison of Melissa attack with other prominent taxonomies is shown.

Table 3: Melissa attack classification

Lough's taxonomy: VERDICT

Attack Name	Improper Validation	Improper Exposure	Improper Randomness	Improper Deallocation
Melissa		X		X

Howard's taxonomy

Attack Name	Tools	Vulnerability	Action	Target	Unauthorized Result
Melissa	Script	Configuration	Authenticate	Data	Corruption of Information

Hansman and Hunt's taxonomy

Attack Name	1st Dimension	2nd Dimension	3rd Dimension	4th Dimension
Melissa	Mass- Mailing Worm	Microsoft Word 97,2000	Configuration	Macro Virus &TCP packet flooding DoS

Proposed taxonomy : ADMIT

Attack Name	Attack vector	Defense	Method	Impact	Target
Melissa	Misconfiguration	Patch System	Worm: Mass mailing	Disrupt	Application: MS Word 97,2000

In Table2, Table3 evaluation of ADMIT taxonomy by comparing it with other prominent taxonomies is shown. These comparisons conclude that Lough's does not provide useful information in describing the attacks. Howard's taxonomy provides general information. Hansman and Hunt's taxonomy provides more useful information about method of operation, target, vulnerability and payload. The proposed ADMIT taxonomy provides information to network administrator about the cause of attack, possible defense mechanism, method of attack, attack result and target to reduce attack's impact.

7. LIMITATIONS OF ADMIT

Attacks have become increasingly present in computer and network system. Provide the ability to prevent all attacks is extremely difficult [17]. Risk factor is an important aspect in achieving security. Although the proposed taxonomy is able to classify the vulnerability thoroughly but there is no such dimension or attack attribute in classification structure associated with attack that directly implies the severity of vulnerability. Further research can be done to include remediation plans to reduce the risks to acceptable level and to address exposures.

8. CONCLUSION

This paper provides a five dimensional taxonomy which captures five major classifiers to characterize the nature of attacks. These are attack vector, defense, method, impact and attack target. The classification structure is able to thoroughly classify vulnerabilities and provides a more apparent approach to educate the defender on possible attacks using vulnerability details. The classification structure of proposed taxonomy provides information to network administrator about the cause of attack, possible defense mechanism, attack method, attack result and target to reduce attack's impact. The administrator can also use the proposed taxonomy to locate strategies that are appropriate for securing their system against vulnerabilities that can be exploited and used for unauthorized access. Use of ADMIT in a network defense strategies can improve the overall level of security. In future research remediation plans will be included to reduce the risks to acceptable level and to address exposures.

9. REFERENCES

[1] Hansman, S., Hunt R., "A taxonomy of network and computer attacks". Computer and Security, vol. 24, issue 1, Feb 2005, PP. 31-43.

[2] Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., & Wu, Q. "AVOIDIT: A Cyber Attack Taxonomy", University of Memphis, Technical Report CS-09-003, 2009. [Online]. Available: http://issrl.cs.memphis.edu/files/papers/CyberAttackTaxonomy IEEE Mag.pdf

[3] R. P. Abbott et al, "Security Analysis and Enhancements of Computer Operating Systems," Report NBSIR 76-1041, Institute for Computer Science and Technology, Natl. Bur. of Stnds, Apr. 1976.

[4] Bisbey, R. and D. Hollingsworth, "Protection Analysis Project Final Report, "Information Sciences Institute, University of Southern California, Marina Del Rey, CA, 1978.

[5] T. Aslam, "A taxonomy of Security Faults in the Unix Operating System," M.S. Thesis, Purdue University, 1995.

[6] T. Aslam, "Use of a taxonomy of Security Faults," Technical Report 96-05, COAST Laboratory, Department of Computer Science, Purdue University, March 1996.

[7] I. Krsul, "Software Vulnerability Analysis," Ph.D. dissertation, Purdue Univ., 1998.

[8] M. Bishop, "A Taxonomy of UNIX System and Network Vulnerabilities," Technical Report CSE-95-10, Purdue University, May 1995.

[9] Howard, John D. and Longstaff, Thomas A. "A Common Language for Computer Security Incidents," Technical report, Sandia National Laboratories, Oct. 1998.

[10] Kjaerland, M., "A taxonomy and comparison of computer security incidents from the commercial and government sectors". Computers and Security, Volume 25, Issue 7, October 2006, PP 522–538.

[11] Lough, Daniel. "A Taxonomy of Computer Attacks with Applications to Wireless Networks," PhD thesis, Virginia Polytechnic Institute and State University, 2001.

[12] Scott D., Angelos S," Towards a Cyber Conflict Taxonomy", 5th International Conference on Cyber Conflict K. Podins, J. Stinissen, M. Maybaum (Eds.), 2013.

[13] E. G. Amoroso, "Fundamentals of Computer Security Technology", Upper Saddle River, NJ: Prentice-HallPTR, 1994.

[14] Anthony D. Wood, John A. Stankovic, "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks," Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, CRC Press, 2004.

[15] C. Douligeris and A. Mitrokotsa, "DDoS Attacks and Defense Mechanisms: Classification and State-of-theart," Comp. Networks, Volume 44, Issue 5, April 2004, PP 643–666

[16] David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford and Nicholas Weaver. "Inside the slammer worm", IEEE Security and Privacy, volume 1, 2003, PP 33-39.

[17] William A. Arbaugh, William L. Fithen, and John McHugh, "Windows of Vulnerability: A Case Study Analysis", IEEE Computer, 33, issue 12, Dec. 2000, PP 52-59.

[18] CERT Coordination Center, "CERT Advisory CA-2003-20 W32/Blaster worm," Aug. 2003; www.cert. org/advisories/CA-2003-20.html.