ISSN 2047-3338

A Survey on Taxonomies of Attacks and Vulnerabilities in Computer Systems

Waqas Ahmad, Zeeshan Hayat, Bilal Zafar, Fawad Ali Khan, Farid ud Din and Iqtidar Shah

Gandahara University Peshawar, Pakistan
Agriculture University Peshawar, Pakistan
Ministry of Information Technology, Peshawar, Pakistan

***Abstract* - Security evaluation of a system is a complicated problem. The majority of the recent efforts in Security evaluation involve for discovering well-known Vulnerabilities. Discovering unidentified Vulnerabilities yet mostly remains a subjective procedure. The procedure knows how to be improved by considering the Characteristics and behavior of well-known Vulnerabilities. The information therefore obtained knows how to be planned into an appropriate Taxonomy, and then can be used as a structure for systematically and investigating new Systems for related however at the same time as yet unidentified Vulnerabilities. There have been several efforts at producing such Taxonomies. This paper offers a detailed review of the significant work done on developing Taxonomies of Attacks and Vulnerabilities in Computer Systems. This review covers work done in security related taxonomies. Apart from giving a state of the art review of Taxonomies, furthermore we examine their efficiency for use in a security evaluation procedure. In conclusion, we sum up the significant characteristics of various taxonomies to provide a structure for organizing information about well-known attacks and vulnerabilities into a taxonomy that would help the security evaluation procedure.**

***Index Terms* - Security, Attacks, Vulnerabilities, Evaluation and Taxonomy**

I. INTRODUCTION

SECURITY evaluation of a System is the procedure of determining the system's capability to resist attacks. This procedure typically involves probing the system to detect the presence of well-known vulnerabilities because most attacks typically exploit well-known vulnerabilities that have not been patched in computer security; vulnerability is a weak point, which permits an attacker to decrease a system's information reassurance.

Vulnerability is the connection of three basics: a system vulnerability or error, attacker access to the flaw, and attacker potential to exploit the error [1]. To exploit susceptibility, an attacker has to at least one appropriate instrument or methods that can join to a system weak point. In this frame, vulnerability is also well known as the attack surface. Vulnerability administration is the cyclical perform of recognizing, organizing, remediation, and mitigating vulnerabilities [2]. This observance in general refers to software Vulnerabilities in computing Systems. A Security hazard might be classified as vulnerability. The practice of vulnerability with the same significance of risk can guide to uncertainty. The threat is tied to the potential of a significant failure. Then there are vulnerabilities with no hazard: e.g., when the affected asset has no value. Vulnerability with one or other well-known occasion of working and fully execute attacks is classify as an exploitable vulnerability. The window of vulnerability is the time from when the security hole was begin or manifest in organize software, to when entrance was removed, a security join was offered, or the attacker was immobilize.

Security bug is a narrower concept; there are vulnerabilities which are not linked to software; hardware, site personal vulnerabilities are examples of vulnerabilities which are not software security bugs [3]. Constructs in programming languages that are difficult to utilize appropriately can be a huge source of vulnerabilities. As we know that vulnerabilities are weak point in the security system, e.g., in procedures, plan, or execution that may be exploited to make failure or damage. This type contains only general details of vulnerabilities. System explicit information is accessible in attacks grouping. Underneath are a few general vulnerabilities:

A. Hardware Vulnerabilities

As we know how to observe which devices are hooked to the system, it is somewhat easy to attack by adding together devices, varying them, eliminating them, interrupting the traffic to them, or flooding them with traffic until they know how to no longer work properly.

Involuntary machine slaughter: unintentional perform not planned to do severe harm to the hardware involved.

Voluntary machine slaughter: typically engages someone who in reality desires to damage the computer hardware or software.

B. Software Vulnerabilities

Deletion: as of software 's elevated price to a marketable computing interior, access to software is typically cautiously restricted throughout a procedure described configuration management as a result that software is not deleted, damaged, or restore by accident.

Modification:

- *Logic bombs:* modification completed as a result that a program be unsuccessful when definite circumstances are met or when a definite date or time is attained.
- *Trojan-Horse:* a program that openly do one thing at the same time as doing one more thing.
- *Virus:* a particular kind of Trojan-Horse which can be exercised to extend its "infection" as of one Computer to another computer.
- *Trapdoor:* a program that has a secret access point.
- *Information leaks:* code that formulates Information reachable to illegal people or programs
- *Theft:* illegal copying of software

Non malicious program error:

- Buffer overflow
- Incomplete Mediation
- time–of-check to time–of-use-error

Viruses and other malevolent code

- Virus
- Trojan Horse
- Logic bombs
- Time bombs
- Worm
- Rabbit
- Backdoor
- Covert channel

C. Data Vulnerabilities

Confidentiality: Numerous be able to collect data way, e.g., tapping wires, planting bugs in o/p devices, sift all the way through trash receptacles, examine electromagnetic radiation, corrupt main workers, gather one data point from extra principles, or basically demand the Data. As data are frequently obtainable in a form people are able to read, the Confidentiality of data is a main apprehension in Computer Security.

Integrity: Data are particularly susceptible to Modification. Undersized and adeptly completed Modification might not be sense in normal ways.

D. Networks Vulnerabilities

Networks are particular sets of hardware, software, and data. Each Network node is itself a computing system; it practices the entire typical Security dilemma.

Precursor to attack

- Port scans
- Social engineering
- Reconnaissance
- OS and application Fingerprinting

Authentication failures

- Impersonation
- Guessing
- Eavesdropping
- Spoofing
- Session hijacking
- Man in middle

Programming flaws

- Buffer overflow
- Addressing errors
- Parameters modification, Time–of-check to Time–of-use error
- Server side includes
- Cookie
- Malevolent active code: java, Active-X
- Malevolent code: Virus, Worm, Trojan Horse
- Malevolent typed code

Confidentiality

- Protocols flaws
- Eavesdropping
- Passive wiretaps
- Miss delivery
- Exposure in network
- Traffic flow analysis
- Cookie

Integrity

- Protocols flaws
- Active wiretaps
- Impersonation
- Falsification of message
- Noise
- Web site defacement
- DNS attacks

Availability

- Protocols flaws
- Communication or module failure
- Denial of service
- DNS attacks
- Traffic redirection
- Distributed Denial of service

E. Access Vulnerabilities

Access to computing apparatus guide to three kinds of vulnerabilities:

Trespasser might steal computer time to do common-principle computing that do not bother the reliability of the system itself.

Malevolent contact to a computing system, whereby an interfering individual or system in reality demolish software or data.

Unlawful contact might reject service to a legal user.

F. People Vulnerabilities

The people can be important weak points in security. In exacting, a discontented employee can make severe harm by means of inside information of the system and the data that are maneuver.

II. TAXONOMIES AND SECURITY EVALUATION

Taxonomy is properly described as “the study of the common principle of scientific classification” [5]. The statement Taxonomy is furthermore used to indicate the actual categorization of objects. This classification is completed according to the associations among the distinctiveness of the objects. At the same time as commencement the scientific study of an original field, a good quality Taxonomy is measured a “considerable and essential requirement for systematic study" [6], [7]. An effortless gathering of a great number of objects is not very constructive for Systematic study. The gathering turns into functional only when it is categorized according to set of laws [7], [8].

A good Taxonomy furthermore suggests a general language for the learning of the field [6]. As recommended in the beginning, Taxonomies of Vulnerabilities may be helpful in the Security evaluation procedure. Apart from that, Taxonomies of Vulnerabilities and Attacks can furthermore be helpful for System designer. The Information be able to assist designers circumvent building features that are expected to have errors. Vulnerability Taxonomy can furthermore offer a method to discover unidentified Attacks [9], [10]. An empty leaf node or a subdivision in a taxonomy characterize a potential utilize. From a Security organization viewpoint, Taxonomy can help to split Vulnerabilities and Attacks that previously contain defense solutions from those that require original defense methods [9], [11].

If the taxonomy has a grade system that can select vulnerabilities according to their seriousness, it knows how to assist prioritize the assets of the defense group. In order to facilitate distributes information of latest vulnerabilities and attacks, several security organizations preserve fundamental databases of vulnerabilities, such as the USCERT database [12] and the common vulnerabilities and exposure (CVE) [13] database. The organizations or separately who locate latest vulnerabilities, report them to this central database where they are classify and accumulated.

Taxonomy furthermore offers a consistent language for exposure events to reply teams for example CERT etc. Numerous taxonomies of attacks and vulnerabilities have been available over the years, but there is up till now no standard or generally established taxonomy. Several diverse taxonomies are there as each one is generally appropriate simply to an exacting field of importance [14]. A thorough evaluation of taxonomies of attacks and errors is presented in [15]. Apart from the effort previous to [15], this paper furthermore deals with the work completed since [15].

Our main concentration is in the growth and exploit of attack and Vulnerability Taxonomies in the security evaluation procedure. This objective need query further than the listing of taxonomies to assume probable general features from these Taxonomies that will assist security evaluation. A proportional study must supply near into the support of and disadvantages of the dissimilar types of taxonomies. In summary, this paper tries to reply the inquiry: What is the most excellent method to categorize information concerning well-known vulnerabilities and attacks to assist a security evaluation procedure systematically and detailed study a new system for determining associated but unidentified vulnerabilities and attacks?

A relative reading is supposed to supply approaching into the support of and disadvantages of the dissimilar kinds of taxonomies. The complexion connected with security evaluation has been well well known for a long time [16]. There have been numerous efforts to develop the procedure of systematic system reading to discover vulnerabilities. These efforts have generally concerned the expansion of attack and vulnerability taxonomies that offer important approaching into probing systems.

III. PROPERTIES OF TAXONOMY FOR SECURITY EVALUATION

In several of the previous mechanism on taxonomies in computer security, the usual objective of the taxonomy was explain in wide terms for example offering and taking into consideration of the a variety of attacks and vulnerabilities.

Our objective in these reviews to recognize a set of characters for a very precise taxonomy: one that know how to be use efficiently in a security evaluation procedure. The Taxonomy have to be modified to the point of view of an evaluation specialized. It should furthermore assist formulate the procedure, as objective as achievable. The taxonomy has to attach attacks with the system vulnerabilities that are the reason of the attacks. From the previous debate on attack taxonomies, we can end that the essential dimensions for attack categorization are impact, target, source and vulnerability. Apart from the vulnerabilities, the number of kinds of impact, target and source are limited for a specified system. The number of vulnerabilities is always unidentified, and the aim of the security evaluation procedure is to discover them. Consequently, a proficient technique of organizing information about attacks would be in a hierarchical way, starting with the impact of the attack and gradually moving lesser to recognize the vulnerabilities.

The essential properties of such Taxonomy would be:

- *Application or system specific Taxonomy:* The amount of Vulnerabilities is therefore high that to perform an efficient Security evaluation, we have to exercise a Taxonomy committed to the function. Taxonomies developed for an exacting System are seldom helpful for dissimilar Systems. This is one of the causes there are numerous Taxonomies in the literature. Every of them concentrate on a precise type of system. E.g., a Taxonomy of Vulnerabilities in operating systems is of small exercise when perform a Security evaluation of a cryptographic protocol.

- *Taxonomy has to be layered or hierarchical:* Only a layered Taxonomy will offer a purpose methodology to recognize vulnerabilities. In comparison, linear or horizontal Taxonomies, such as the Web Attacks Taxonomy in [18], are helpful simply for considering the features of an attack. The use of that Information would then depend on the person performing an evaluation. The linear collection does not help in dropping the subjectivity of the procedure. The Taxonomy has to start at a high intensity of idea and gradually go poorer. Still the lowest level of a number of the presented Taxonomies, for instance has a moderately high-level illustration of the attack or vulnerability. Such abstract programs do not assist to recognize definite vulnerabilities.

- *First level of classification— attack impact:* all attack abuse one of the vital Security properties. Consequently, each attack can be grouped below the exacting Security property it breaches. We start with the Security properties and listing the fundamental types of Attacks that disobey these properties. By study the information of the Attacks, we know how to obtain a considering of the vulnerabilities that allow the attacks. Each attack has numerous penalties. For our reasons, we believe simply the direct impact of an exploit. The instantaneous effect of an attack is a failure of some security property. On the other hand, once the attacker violates a single property, he may furthermore get rights to transmit out numerous Attacks. The secondary Attacks depend simply on the urge of the attacker.

• *Second level of classification —system specific attacks types:* As we have observed from Taxonomies of DoS Attacks [20], DDoS Attacks [9], rerun Attacks, and others, each distinctive System has a small amount of particular types of Attacks. E.g., a DoS Attacks know how to momentarily disturb service or effect stable shutdown need repair. Such programs of attack blow ought to formulate the second level of categorization. As acknowledged beyond, the aim is to constrict the attack to the particular Vulnerability.

•*Third level of classification — system components attacks (attacks target):* all attack furthermore marks an exacting subsystem of the system. In order to perform a comprehensive evaluation, one ought to contain a whole listing of all the system mechanisms. The grouping in this level will be enormously system-specific. E.g., if evaluate the vulnerabilities of a protocol, the grouping in this level would be the variety of protocol levels. An illustration of such categorization is in [19] that observe the variety of DoS attacks in WSNs. At a system level, this furthermore communicates to Landwehr's categorization by position.

• *Fourth level of classification — system features (source of Vulnerability):* This is not the very last stage of arrangement. Every System part has to be promoted sophisticated to recognize the exacting characteristic of the System that effect the attack. The quantity of levels follow this level would depend on the difficulty of the System.

• *Classes need not be equally exclusive:* As argued in earlier, numerous previous mechanisms claim on having equally exclusive classes in the Taxonomy. The Taxonomy with the above properties is certainly not communally exclusive. An exacting Vulnerability might be broken to guide to a failure of confidentiality and loss of availability, and by itself it will be scheduled under equally classes. We suppose that this classification assist generate better Vulnerability exposure in the procedure. Vulnerability not perceived under one class may be noticed under a second class. Consequently, no uniqueness really provides us a functional redundancy, promoting the procedure. The effectiveness of a Security evaluation procedure be supposed to be calculated by its independence and Vulnerability exposure. Objectivity of the procedure involve that it generate the similar outcomes free of the person perform the evaluation. A process with high-quality Vulnerability exposure search all related System features that are possible to have vulnerabilities. Even though as of at the present there are no metrics for calculating objectivity and vulnerability exposure, we suppose that a taxonomy with the above properties very much helps a security evaluation procedure [21].

IV. CONCLUSIONS

Security evaluation is a hard problem, and taxonomies of attacks and vulnerabilities have been conventionally used to help in this procedure. This paper shows a review of all taxonomies related to computer and network security. The review examines presented work on security taxonomies and assesses their effectiveness in terms of security evaluation. The examination assists to recognize particular properties of taxonomies that help security evaluation.

REFERENCES

[1] The Three Tenents of Cyber Security. U.S. Air Force Software Protection Initiative. http://www.spi.dod.mil/tenets.htm. Retrieved 2009-12-15.

[2] Foreman, P: Vulnerability Management, page 1. Taylor & Francis Group, 2010. ISBN 978-1-4398-0150-5

[3] J. D. Howard and T. A. Long staff, “A Common Language for Computer Security Incidents,” Sandia tech. rep. SAND98-8667, Oct. 1998.

[4] U. Lindquist and E. Jonsson, “How to Systematically Classify Computer Security Intrusions,” Proc. IEEE Symp. Sec. and Privacy, 4–7 May 1997, pp.154–63.

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

[6] J. Mirkovic and P. Reiher, “A Taxonomy of DDoS Attack and DDoS Defense Mechanisms,” ACM SIGCOMM Comp. Commun. Rev., vol. 34, no. 2, Apr. 2004, pp. 39–53.

[7] V. Raskin et al., “Ontology in Information Security: A Useful Theoretical Foundation and Methodological Tool,” Proc. NewSec. Paradigms Wksp., Cloudcroft, NM, 2001, pp. 53–59.

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

[9] CERT Coordination Center Vulnerability Database,http://www.kb.cert.org/vuls

[10] Common Vulnerabilities and Exposures List, http://www.cve.mitre.org/

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

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

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

[14] Hussein, J. Heinemann, and C. Papadopoulos, “Denial-of Service: A Framework for Classifying Denial of Service Attacks,”Proc.Conf. Apps. Tech., Architectures, and Protocols for Comp Comm., Aug. 2003, pp. 99–110.

[15] G. Alvarez and S. Petrovic, “A Taxonomy of Web Attacks Suitable for Efficient Encoding,” Comp. & Sec., vol. 22, no. 5, 2003, pp. 435–49.

[16] Wood and J. A. Stankovic, “Denial of Service in Sensor Networks,” IEEE Computer, vol. 35, no. 10, Oct. 2002, pp. 54–62.

[17] T. S. Perry and P. Wallich, “Can Computer Crime Be Stopped?”IEEE Spectrum, vol. 21, no. 5, May 1984, pp. 34–45.

[18] 1st Quarter 2008, Volume 10, No. 1 IEEE Communications Surveys The Electronic Magazine of Original Peer-Reviewed Survey Articles www. Comsoc.org /pubs /surveys