Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on Taxonomies of Attacks and Vulnerability in Computer and Network System

Chanchala Joshi, Umesh Kumar Singh, Kapil Tarey
Institute of Computer Science, Vikram University,
Ujjain, M.P. India

Abstract— In order to gain trusted system detection and remediation of vulnerability is crucial. In computer network to solve the problem of security vulnerability, study of vulnerability is essential to know cause of vulnerability. By considering the characteristics and behavior of known vulnerabilities we can improve the security evaluation procedure. The information about known vulnerability can be used to design an appropriate taxonomy that can be further used in investigating new system and also for identifying unidentified vulnerabilities. Several attempts have been made for producing such taxonomies. This paper offers a detailed review of significant work has been done in development of taxonomies of attacks and vulnerability present in the system. Also this paper examines the efficiency of taxonomies for use in a security evaluation procedure. Further this paper summarizes the characteristics of various prominent taxonomies and provides a structure for organizing information about well-known attacks and vulnerabilities that would help in security evaluation procedure.

Keywords-Network security; Vulnerability; taxonomy

I. INTRODUCTION

Vulnerability is the root cause of network and security attacks. Any system can be termed as secure if it has no flaws and vulnerability. Therefore the detection and remediation of vulnerability is crucial to guarantee the security of the system [22]. For proper security assessment it is essential to determine system's capability to resist attacks. Security evaluation procedure generally involves probing the system to detect the presence of well-known vulnerabilities because most of the attacks typically exploit well known vulnerabilities that have not been patched. Vulnerability is the weak point in system by which hacker can gain access to the network. For security assessment it is necessary to find and classify these vulnerabilities. The first step in understanding vulnerabilities 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 is formally defined by Merriam-Webster Online Dictionary as "the study of the general principles of scientific classification". The word taxonomy is also used to denote the actual classification of objects. This classification is done according to the relationships between the characteristics of the objects. While beginning the scientific study of a new field, a good taxonomy is considered an "important and necessary prerequisite for systematic study" [29]. A simple collection of a large number of objects is not very useful for systematic study. The collection becomes useful only when it is classified according to set of rules. A good taxonomy also provides a common language for the study of the field.

II. APPROACHES TOWARDS TAXONOMOIES

Several attempts were made to model the taxonomy during the development of taxonomies. The initial approach was flat taxonomy. Flat taxonomy or single dimensional taxonomy divides the set of vulnerabilities according to one general criterion. McPhee [1], PA [3] and Aslam's [5] taxonomies fall under the flat taxonomy. These are the simplest taxonomies. Next level of development of taxonomy approaches tree like structure that follows hierarchical classification with more general categories at the top and specific categories at leaves. Weber [15], Bazaz and Arthur [20] taxonomies come into this category. This tree approach could not deal with blended attack as if the attack contain other attack then this would lead to a messy tree. The more efficient and appropriate approach towards standardization of taxonomies is multidimensional approach. In which vulnerabilities are classified on the basis of multiple vectors which are called dimensions. Multidimensional approach is able to thoroughly classify vulnerabilities and provides a more apparent approach to educate the defender on possible attacks using vulnerabilities details. Hansman, Kjaerland, Igure follow this multidimensional approach to classify vulnerabilities.

III. STANDARD PROPERTIES OF TAXONOMIES

The most important work of vulnerabilities classifications is to find attributes of vulnerabilities.
With the attributes quantified by classification, we can effectively analyze vulnerabilities that will help in enhancing security procedure. E. G. Amoroso [27] lists the well accepted principles of a good classification as:

i. Public acceptance: A classification should have good structure to be accepted publicly.

ii. Comprehensibility: A classification should be understood by both security experts and people who are interested in this area.
iii. Completeness: A classification can classify all of the possible vulnerabilities.
iv. Determinism: The process of a classification should have legible definitions.
v. Mutual exclusion: A classification should classify vulnerability into at most one class.
vi. Repeatability: The classification process can be repeatable.
vii. Terminology complying with established security terminology.

IV. STUDY OF PROMINENT TAXONOMIES

RISOS [2] (Research in Secure Operating Systems) project was one of the first taxonomy. It was based on flaws found in three operating systems: IBM's OS/MVT for the IBM 360, UNIVAC's 1100. It categorizes operating system integrity flaws in seven categories. Classification criteria were operations of OS, which can be the reason for attacks, if misused. The seven classes of vulnerabilities were:

- Incomplete parameter validation
- Inconsistent parameter validation
- Implicit sharing of privileged/confidential data
- Asynchronous validation/Inadequate serialization
- Inadequate identification/authentication/authorization
- Violable prohibition/limit
- Exploitable logic error

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 [3] 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] 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 [7] 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 [26] 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 [18] 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 [9] 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 [17] 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 [22] 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. [24] 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.

V. COMPARISION OF TAXONOMIES OF VULNERABILITIES

SN	Taxonomy	Classification Scheme	Classifier Attribute Description	Objective	Comments
1	McPhee 1974 [1]	Single Dimension	Flaws are due to vulnerability in design	Identify operating system flaws	Identify vulnerabilities characteristics
2	RISOS project 1976 [2]	Layered	By operations or features	Characterize operating system flaws	Operating System oriented
3	PA, 1978 [3]	Single Dimension	Operating System Flaws	To abstract patterns from flaws and automate the search for flaws	Operating System oriented
4	Landwehr, 1994 [4]	Single Dimension	Operating System Flaws categorized vulnerability by Genesis, Time of introduction and Location	To consider possible sources of flaws from different perspectives	Provide framework for security assessment
5	Aslam, 1995 [5]	Single Dimension	UNIX Security Flaws	To organize information being stored in a vulnerability database	Helps in organization of vulnerability database
6	Krsul, 1998 [6]	Single Dimension	Software Flaws	Characterize operating system flaw	Represents programmer view
7	Bishop, 1999 [7]	Single Dimension	Nature, Time, Exploitation, Effect, Minimum number of components, Source of ID	UNIX System and Network Vulnerabilities, describe vulnerabilities in a form useful for IDS	Classifies vulnerabilities in a manner useful for security mechanism.
8	Du and Mathur 2000 [8]	Three dimensions	By cause, By impact and By fix	To develop a practical and usable categorization of software errors	characterize Software Vulnerabilities, also include defense mechanism
9	VERDICT, 2001 [9]	Four dimensional	Validation, Exposure Randomness, Deallocation, Improper Conditions Taxonomy	describe vulnerability within a system	focuses on four major causes of security errors
10	Piessens, 2002 [10]	Single Dimension	Software Vulnerabilities	To help developers to focus on most frequently occurring causes of vulnerabilities	Phases of SDLC
11	Andy Gray,	Layered	Vulnerability	To help	Used a

	2003 [11]		Taxonomy	organization's management	combination of existing taxonomies
12	Jiwnani 2004 [12]	Three dimensional	Software development issues, Location of flaws in the system and Impact of flaws on the system	To identify parts of system that have higher concentration of vulnerabilities	Software Flaws
13	Pothemsetty and Akyol, 2004 [13]	Layered	Protocol Vulnerabilities	Categorize network protocol related vulnerabilities	Features or operations of the protocol software
14	Tsipenyuk, 2005 [14]	Multidimensional	Coding Errors	To help software developers in understanding causes and impact of software errors	Errors in source code
15	Weber, 2005 [15]	Layered	Software Flaw	To help in development of code analysis tools to detect software	By Genesis
16	Seacord, 2005 [16]	Multidimensional	Vulnerability Taxonomy	To provide multidimensional view of vulnerabilities to increase automation in analyzing vulnerabilities	By attribute-value pairs
17	Hansman, 2005 [17]	Four Dimensional	method, target, vulnerability, payload	To provide assistance in combating new attacks, improving computer and network security	Attacks centric, Computer system and network based classification
18	Kjaerland, 2006 [18]	Four Dimensional	method of operations, impact of the intrusion, source of the intrusion, target	To focus on the motive of the attacker	quantify why the attacks take place, and where the attacks originated
19	Fortify Taxonomy, 2006 [19]	two hierarchical levels -kingdoms (classes of errors)and phyla(specific errors)	Input validation &representation , API abuse, Security features, Time and State, Errors, Code quality, Encapsulation, Environment	To understand common types of coding errors that lead to vulnerabilities	Follows Tsipenyuk's approach for vulnerability classification
20	Bazaz and Arthur, 2007 [20]	Hierarchical	Vulnerability Taxonomy	To provide view of relationship between computer system resources, process and vulnerabilities	Based on resources of computer system
21	Igure 2008 [21]	MultiDimensional	Attack vulnerability	To provide view of relationship between computer system resources, process and vulnerabilities	Attack characteristic based on vulnerability classification
22	AVOIDIT, 2009 [22]	Five dimensional	Attack Vector, Operational Impact, Defense,	Focused on cyber-attacks	network taxonomy, classifies blended

			Informational Impact, Target		attacks very well
23	Operational cyber security risks, 2010 [23]	Hierarchical	actions of people, systems and technology failures, failed internal processes, and external events	To identify and organize the sources of operational cyber security risk	Cyber attacks
24	Cyber conflict, 2013 [24]	Hierarchical	network taxonomy	Categorized using the categories and subcategories of actions or actors.	Explore the relationship between events and the states, groups or individuals
25	ADMIT, 2014 [25]	Five dimensional	Attack Entity, Defense, Method, Impact, Target	Characterize nature of attacks	Uses five major classifier that causes attacks

VI. CONCLUSION AND FUTURE WORK

This paper reviewed and compared 25 vulnerability classification methods. In the past various flaw and vulnerability taxonomies have been proposed and all these suffer from various drawbacks or have certain limitations. These taxonomies serve different purposes and useful for stated purposes up to some extent. Although a lot of approaches in this topic have been proposed none is generally accepted. The main reason is that no classification satisfies all the principles about classifications, such as comprehensibility, completeness, determinism, and mutual exclusiveness [27]. All previous taxonomies are now outdated and of very limited use. It is necessary to update taxonomies in order to maintain their usability with respect to security issues associated with today's software products and attack mechanisms. Updating process is a difficult task in view of the large number of new vulnerabilities reported every day. To be consistently useful, taxonomy should be able to classify newly discovered vulnerabilities automatically without manual effort. As a result, no existing taxonomy is universally accepted till today. Taxonomy should be able to adapt changes in trends that happen over time to maintain its usability. A standard vulnerability taxonomy or categorization scheme is required for efficient and effective security assessment of software systems, tools and services. Many issues on vulnerability classifications open for further research, such as whether the attributes discovered by the existing classifications are enough to describe any vulnerability, how to quantify each attribute of vulnerability in order to make a reasonable network security evaluation, and how to evaluate the damage attribute of vulnerability. In addition to develop an automatic classification scheme to handle the ever-increasing vulnerability is also main task that requires further work in this field.

REFERENCES

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

[2] 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.

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

[4] C. E. Landwehr, A. R. Bull, J. P. McDermott and W.S. Choi. "A taxonomy of computer program security flaws", ACM Computing Surveys, Vol. 26 (3), pp. 211-254, 1994.

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

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

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

[8] W. Du and A. P. Mathur. "Testing for software vulnerability using environment perturbation", Proceeding of the International Conference on Dependable Systems and Networks (DSN 2000), Workshop on Dependability Versus Malicious Faults,http://www.cerias.purdue.edu/homes/duw/ research/paper/ftcs30 workshop. ps., pp. 603-612, 2000.

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

[10] F. Piessens. "A taxonomy of causes of software vulnerabilities in internet software", Supp lementary Proceedings of the 13th International Sympo sium on Software Reliability Engineering, 2002.

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

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

[13] V. Pothamsetty, B. Akyol, "A Vulnerability Taxonomy for Network Protocols: Corresponding Engineering Best Practice Countermeasures," in IASTED Int. Conf. on Commun., Internet, and Inform. Tech. (CIIT), ACTA Press, US Virgin Islands, 2004.

[14] 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.

[15] S. Weber, P. A. Karger and A. Paradkar. "A Software Flaw Taxonomy. Aiming Tools", At Security Software Engineering for Secure Systems–Building Trustworthy Applications (SESS'05) 2005.

[16] R. C. Seacord, "Secure Coding in C and C++". USA: Addison-Wesley Professional, 2005.

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

[18] 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.

[19] FORTIFY,http://www.fortifysoftware.com/

[20] A, Bazaz, James D. Arthur, "Towards a Taxonomy of Vulnerabilities", HICSS, 2007, Proceedings of the 40th Annual Hawaii International Conference on System Sciences, 2007, pp. 163a, doi:10.1109/HICSS.2007.566

[21] V. M. Igure and R. D. Williams, "Taxonomies of Attacks and vulnerabilities in Computer Systems", IEEE Communications Surveys & Tutorials 1st Quarter 2008.

[22] 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

[23] Cebula, J. J., & Lisa, R. Y. (2010), "A Taxonomy of Operational Cyber Security Risks", (Carnegie Mellon University / Software Engineering Institute No. CMU/SEI-2010- TN-028). Retrieved from http://www.sei.cmu.edu/library/abstracts/reports/10tn028.cfm

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

[25] C. Joshi and U. K. Singh. "ADMIT- A Five Dimensional Approach towards Standardization of Network and Computer Attack Taxonomies". International Journal of Computer Applications 100(5):30-36, August 2014.

[26] Howard, John D. and Longstaff, Thomas A. "A Common Language for Computer Security Incidents," Technical report, Sandia National Laboratories, SAND98-8667, Oct. 1998.

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

[28] 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.

[29] 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.

