Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics
San Antonio, TX, USA - October 2009

A Review of Classification Methods for Network Vulnerability

Shuyuan Jin
Institute of Computing Technology
Chinese Academy of Sciences
jinshuyuan@software.ict.ac.cn

Yong Wang
Institute of Computing Technology
Chinese Academy of Sciences
wangyongjut@gmail.com

Xiang Cui
Institute of Computing Technology
Chinese Academy of Sciences
cuixiang@software.ict.ac.cn

Xiaochun Yun
Institute of Computing Technology
Chinese Academy of Sciences
xiaochunyun@ict.ac.cn

Abstract—**Classification of network vulnerability is critical to detection and risk analysis of network vulnerability. A broad range of classification methods have been proposed in literature. This paper reviews a total of 25 selected approaches and identifies the differences and relations among them. It also points out some open issues for research in this field.**

Keywords—**network vulnerability, vulnerability attribute, vulnerability classification.**

I. Introduction

An increasing number of network vulnerabilities results in great threats to reliability of information systems. The CERT/CC (Computer Emergency Response Team Coordination Center) reported that the economic loss invoked by the intrusion events has reached about 6.66 billion US dollars in 2003. The existing vulnerabilities in the information systems are the main reasons to invoke the intrusion events. Even worse, the number of network vulnerabilities is increasing with time. For example, there were a total of 7236 vulnerabilities in 2007, and this number reached 4110 by the end of the first two quarter of 2008 [1]. Because there is no way to eliminate vulnerabilities during the implementations of operation systems and software applications [2], vulnerability analysis has become important to protect network security.

Classification of network vulnerabilities is the first step in vulnerability analysis. If a vulnerability classification is good enough, it can identify any vulnerability sufficiently. A good vulnerability classification can help in 1) vulnerability publish, storage and acquisition; 2) known and unknown vulnerability identification; 3) vulnerability analysis and evaluation.

The paper is organized as follows. Section 2 presents the basic concepts of vulnerability and vulnerability classification. We compare a total of 25 classification methods in Section 3 and identify the inheritances among them in Section 4. In Section 5, we list some open issues and conclude the paper.

II. Vulnerability Classification

Network vulnerability has been researched for many years. However, one of the recurrent debates is what is *Network vulnerability*? One broadly accepted definition was proposed by Bishop and Bailey [3]: “A vulnerable state is an authorized state from which an unauthorized state can be reached using authorized state transitions; a vulnerability is a characterization of a vulnerable state which distinguishes it from all non-vulnerable states.”

A general way to describe vulnerability is to find attributes of vulnerabilities, which is the main work of vulnerabilities classifications. With the attributes provided and quantified by a classification, we can quantitatively analyze network vulnerabilities in evaluating security risks.

978-1-4244-2794-9/09/$25.00 ©2009 IEEE

We list the well accepted principles of a good classification [4] as follows:

- Public acceptance: A classification should have good structure to be accepted publicly.
- Comprehensibility: A classification should be understood by both security experts and people who are interested in this area.
- Completeness: A classification can classify all of the possible vulnerabilities.
- Determinism: The process of a classification should have legible definitions.
- Mutual exclusion: A classification should classify a vulnerability into at most one class.
- Repeatability: The classification process can be repeatable.
- Terminology complying with established security terminology.

III. Comparison

The research on vulnerability analysis began in 1970s [5-7]. McPhee identified the vulnerability in the design of a computer system for the first time [8] in 1974. At that time, the vulnerability was introduced by the tradeoff between the performance and technique limitations, rather than by the design errors. After that, protecting computer security from vulnerability was publicly accepted as an essential demand in computer system design. Up to now a large number of vulnerability classifications have been proposed in literature. We review a total of 25 different vulnerability classifications. A comparison of these classifications is given as Table 1.

In table 1, we name each classification with its proposed authors and time in Column 2. Column 3 gives a rough description of classification attributes. By the classification dimensions, we distinguish single dimension classifications and multiple dimension classifications, as shown in Column 4. According to the different objectives, we categorize the classifications into 4 groups: OS (Operation System) oriented, attack oriented, wireless network oriented, and general classifications, as shown in Column 5.

IV. Inheritances

The latter proposed classifications often modify or extend the former ones. We list in Table 2 the inheritances among the classifications. For example, *Aslam 1995* and *Krsul 1998* are both Unix operation system oriented, and *Krsul 1998* inherits and further develops the main ideas of *Aslam 1995*.

TABLE I. Inheritances among the classifications.

Classifications being inherited	**Classifications inheriting**
Aslam 1995 [6]	Krsul 1998 [10]
Landwehr 1994 [20]	Kanta Jiwnani 2004 [29]
Landwehr 1994 [20], DeMillo and Mathur 1995 [12]	Du,Mathur 1998 [24]
Landwehr 1994 [20]	Sam Weber 2005 [21]

V. Conclusions

In this paper, we reviewed and compared 25 vulnerability classification methods. 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 (as described in Section 2).

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, how to make an automatic classification to handle the ever-increasing vulnerability is also a real problem worth studying.

Acknowledgment

This work is supported by the National High-Tech Research and Development Plan of China under Grant Nos. 2009AA01Z438, 2009AA01Z431, and the National Natural Science Foundation of China under Grant No. 60703021.

TABLE II. COMPARISON OF DIFFERENT VULNERABILITY CLASSIFICATIONS

Label	Classification Name	Classification Attribute Description	Classification Dimension	Classification Objective
1	Abbott 1976 [7]	Operation based classification	Single	OS oriented
2	Bisbey 1978 [6]	Protection Analysis based classification	Single	OS oriented
3	Aslam 1995 [6]	Causation based classification	Single	OS oriented
4	Bishop 1995 [9]	Causation based classification	Single	General
5	Krsul 1998 [10]	Causation based classification	Single	OS oriented
6	Frank Piessens 2002 [11]	Causation based classification	Single	General
7	DeMillo and Mathur 1995 [12]	Prevention based classification	Single	General
8	Dodson 1996 [13]	Problem based classification	Single	General
9	Power 1996 [14]	Criticality based classification	Single	General
10	Krsul 1997 [15]	Damage based classification	Single	General
11	Cohen 1997 [16]	Attack method based classification	Single	Attack oriented
12	Du and Mathur 2000 [17]	Condition based classification	Single	General
13	Lough 2001 [18]	Wireless network vulnerability classification	Single	General
14	Lv 2005 [19]	C/C++ program vulnerability classification	Single	Wireless network oriented
15	Landwehr 1994 [20]	Vulnerability attributes include origin, introduced time and position.	3-dimension	OS oriented
16	Sam Weber 2005 [21]	Vulnerability attributes include origin, introduced time and position.	3-dimension	OS oriented
17	Longstaff 1997 [22]	Vulnerability attributes include origin, access privilege, operation system type, availability	4-dimension	General
18	Howard 1997 [23]	Attack process based vulnerability classification	5-dimension	Attack oriented
19	Du and Mathur 1998 [24]	Classification attributes include: vulnerability origin, affection and remedy methods.	3-dimension	General
20	Bishop 1999 [25]	6-aixes classification	Multiple	General
21	Knight 2000 [26]	General classification	Multiple	General
22	Wang 2002 [27]	Software based classification	Multiple	General
23	Hansman 2003 [28]	Computer system and network based classification	4-dimension	General
24	Jiwnani 2004 [29]	Classification attributes include: vulnerability origin, position and affection	3-dimension	General
25	Igure 2008 [30]	Attack characteristic based vulnerability classification	Multiple	Attack oriented

REFERENCES

[1]CERT/CC. 2008. CERT/CC Statistics 1995-2008. Information from the web at http://www.cert.org/stats/fullstats.htm#historic.

[2] W. R. Cheswick and S. M. Bellovin. Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley, 1994.

[3] M. Bishop and D. Bailey. A Critical Analysis of Vulnerability Taxonomies. Tech. Rep. CSE-96-11, Department of Computer Science at the University of California at Davis, 1996.

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

[5] A. Endres. An Analysis of Errors and Their Causes in System Programs. IEEE Transactions on Software Engineering SE-1,2 (June), 140-149, 1975.

[6] R. Bisbey and D. Hollingworth. Protection analysis: final report. Technical report, University of Southern California; May 1978.

[7] R. P. Abbott, J. S. Chin, J. E. Donnelley, W. L. Konigsford, S. Tokubo and D. A. Webb. Security analysis and enhancements of computer operating systems. Technical Report NBSIR 76 1041, Institute for Computer Sciences and Technology, National Bureau of Standards; April 1976.

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

[9] T. Aslam. A Taxonomy of Security Faults in the Unix Operating System. M.S.thesis, Purdue University, 1995.

[10] I. Krsul. Software Vulnerability analysis. PhD thesis. Department of Computer Science, Purdue University, West Lafayette, USA, 1998.

[11] F. Piessens. A taxonomy of causes of software vulnerabilities in internet software[C]. Supp lementary P roceedings of the 13th International Sympo sium on Software Reliability Engineering, 2002.

[12] R. A. DeMillo and A. P. Mathur. A Grammar Based Fault Classification Scheme and its Application to the Classification of the Errors of TeX. Tech. Rep. SERC-TR-165-P, Software Engineering Research Center, Purdue University. September, 1995.

[13] J. Dodson. Specification and Classification of Generic Security Flaws for the Tester's Assistant Library. M.S.thesis, University of California at Davis., 1996.

[14] R. Power. Current And Future Danger: A CSI Primer of Computer Crime & Information Warfare. CSI Bulletin, 1996.

[15] I. Krsul. Computer Vulnerability Analysis. Technical Report CSD-TR-97-026, The COAST Laboratory, Department of Computer Science, Purdue University, April 15, 1997.

[16] F.Cohen. Information system attack s: a preliminary classification scheme. Computers & Security, 16 (2). 1997.

[17] 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.

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

[19] W. Lv and J. Liu. The Classification and Analysis on Safety Holes of C/C++ Programs. I*n Chinese*. Computer Engineering and Applications. Vol.41, No.5. pp. 123-125,228, 2005.

[20] 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.

[21] 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.

[22] T. Longstaff. Update: CERT/CC Vulnerability Knowledge base. Technical pre-sentation at a DARPA workshop in Savannah, Georgia,, 1997.

[23] Howard J D. An analysis of security incidents on the internet:198921995[D]. CarnegieMellon U niversity, 1997.

[24] W. Du and A.P. Mathur. Categorization of software errors that led to security breaches. Proceedings of the 21st National Information Systems Security Conference (NISSC' 98), http://www.cerias.purdue.edu/homes/duw/research/paper /nissc98.ps, 1998.

[25] M. Bishop. Vulnerabilities analysis. International symposium on recent advances in intrusion detection, 1999.

[26] E. Knight and B. V. Hartley. Is your network inviting an attack. Internet Security Advisor, (5/6): 2-5, 2000.

[27] L. Wang. A quantitative risk evaluation method for computer system and network security. PhD thesis. Department of Computer Science, Harbin Institute of Technology, China, 2002.

[28] S. Hansman. A Taxonomy of Network and Computer Attack Methodologies. Department of Computer Science and Software Engineering University of Canterbury, Christchurch, New Zealand， November 7, 2003.

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