Journal of Engineering Science and Technology Review 6 (5) (2013) 101-106

JOURNAL OF
Engineering Science
and Technology Review

www.jestr.org

Research Article

DMAT: A New Network and Computer Attack Classification

Wei JIANG[1,2,3,*], Zhi-hong TIAN[4] and Xiang CUI[5]

[1]College of Computer Science, Beijing University of Technology,Beijing 100124,. China
[2]School of Computer, National University of Defense Technology, Changsha 410073, China
[3]Key Laboratory of Information and Network Security, Ministry of Public Security, Shanghai 201204, China
[4]School of Computer Science and Technology, Harbin Institute of Technology, Haerbin 150001, China
[5]The Institute of Computing Technology of the Chinese Academy of Sciences,Beijing 100080, China

Received 2 September 2013 ; Accepted 8 November 2013

Abstract

With the rapid development of computer network and information technology, the Internet has been suffering from a variety of security attacks over the past few years. Attacks have become both numerous and complex, and the defender can not understand. In order to understand and defend against cyber attacks, it is necessary to understand the kind of attack. In this paper, we study computer and network attacks, and introduce a classification of them and propose a cyber attack classification called DMAT (Defense-oriented Multidimensional Attack Taxonomy). We use nine categories to describe the characteristic of the attack, which are attack target, attack impact, attack purpose, attack cost, attack exploiting, attack source, attack automation, attack loss and defense. The ninth category in the DMAT, classification by defense, is used to provide the defender with instructions of how to defense an attack. Compared to the existing taxonomies, our taxonomy efficiently classifies complex attacks and guide the defender to defense the possible attack.

Keywords: Network Security, Attack Survey, Attack Taxonomy, Attack Defense

1. Introduction

Classification of attack is an important aspect of network security research, scientific and reasonable classification classification for network security has important reference value. Against the existing classification methods do not meet the basic requirements of taxonomy, without considering the dependence of the characteristics of attack and defense strategies. Taking into account the size of the computational complexity of the offensive and defensive strategies, we must study the taxonomy of network and computer attack.

Currently, researchers have conducted a lot of research work in the attack classification. But so far, no attacks on computer networks and a widely accepted classification. The main purpose of any such classification is proposed classification features, wherein the classification of the object is fully described.

The rest of the paper is organized as follows. Section 2 discusses resrarch taxonomy for network and computer attack.The new attack taxonomy is presented in Section 3. In Section 4, we discuss our analysis method along with the preliminary results. Section 5 concludes this paper with a brief description of future work.

2. Survey of Network and Computer Attack Classifica - tion [1]

In our previous work[1], we have investigated and discussed the taxonomy related to the computer and network attacks before several. Existing work can be classified into the following categories attack. which are classification by vulnerability,classification by lists of terms, classification by application, classification by multiple dimensions.

2.1 Classification by Vulnerability

Most attacks are exploited weaknesses in software and hardware systems so the attack early classification is based on weakness developed on the basis of the classification. U.S. Naval Research Laboratory Landwehr et al [2] according to the genesis of computer system security vulnerabilities, the introduction of time and location in the computer system of three aspects of the attack classification. A summary of the classification is shown in Fig.1. This classification helps system designers and application developers design and development of secure systems.

Matt Bishop et al. [3] adopted a similar approach to vulnerability classification and clarify the use of the program features may be attacked. Zhang et al. [4] proposed a privilege escalation vulnerabilities based on multi-dimensional quantification taxonomy attributes.

[*] E-mail address: j8w8@sohu.com

ISSN: 1791-2377 © 2013 Kavala Institute of Technology. All rights reserved.

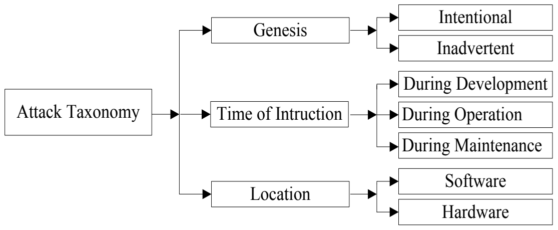

Fig. 1. Attack classification by security vulnerabilities

2.2 Classification by Lists of Terms

Based on experience in terms of attack classification method is the use of technical terms commonly used in the network or social terms to describe the attack, and its classification. This classification is single, a list of definitions of terms, and is a popular and simple classification. Such a simple classification lists only one term without classifying the attacks.

Cohen et al [5] presented some terms for attack classification based on experience term such as, Trojan horse attack, forgery network information, posing, network scanning, spilling email, logic bombs, and other types. The classification method began to be used early attacks and intrusion detection analysis, the connotation of the term due to the lack of understanding of the attack, resulting in the classification logic, science and hierarchy is not clear, is not conducive to the understanding and application. In particular, there is a new attack, the need to increase the term, have poor scalability, and has not been widely used.

2.3 Classification by Application

Attack classification based applications is generally for specific applications. Against certain types of attacks described in detail the characteristics and properties to meet the needs of specific areas, with greater use value. However, this method can not be applied multiple applications.

Alvarez et al. [6] proposed an Web attack taxonomy based on the life cycle of the attack. The classification from 10 classes to classify web attacks, every class of the attack is divided into sub-categories. As shown in Fig. 2, the classification method to study the life cycle of attack, well reflects the process of attack, help to understand the nature of the attack, scalability, and easy procedure attack encoded.

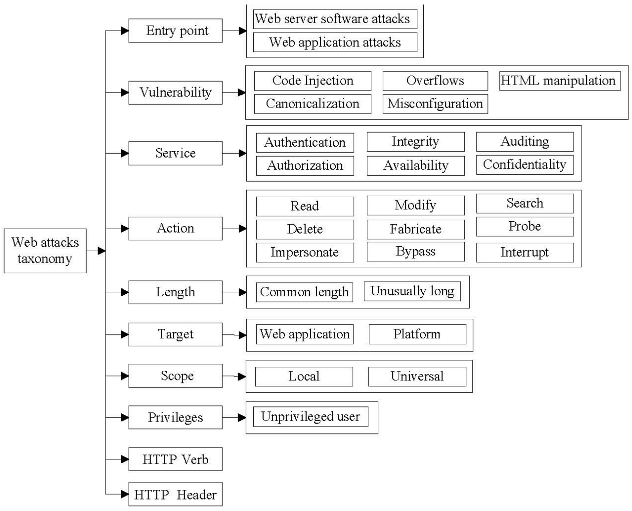

Fig. 2 . Classification of web attck [6]

Weaver et al. [7] proposed a classification of worm attacks. Which classification by target discovery, classification by propagation carrier, classification by the activation mechanism, classification by payloads and classification by attacker motivations. Propagation carrier, activation,and the payloads are independent.

As shown in Fig.3, Anthony et al. [8] proposed a Denial of service attack classification in wireless sensor networks. The classification include 5 classes, which are the attacker, the capabilities, the attack target, vulnerabilities, the result.

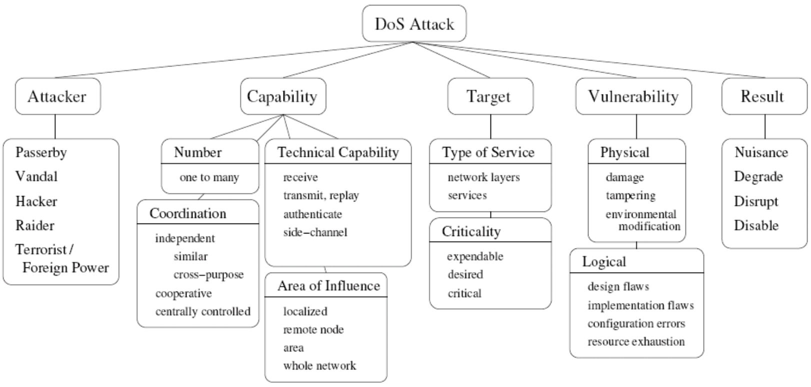

Fig. 3 Classification for Dos attacks in WSN[8]

Mirkovic et al. [9] presented an attacks and defenses classification for classifying denial-of-service attacks. Classification criteria arethe weakness being used, degree of automation, communication mechanisms, the impact on the victim. These standards are an important feature of the attack. Each categories of attack can be divided into several sub-categories, such as victim category can be divided into application, host, resource, network and infrastructure.The description is shown in Fig.4.

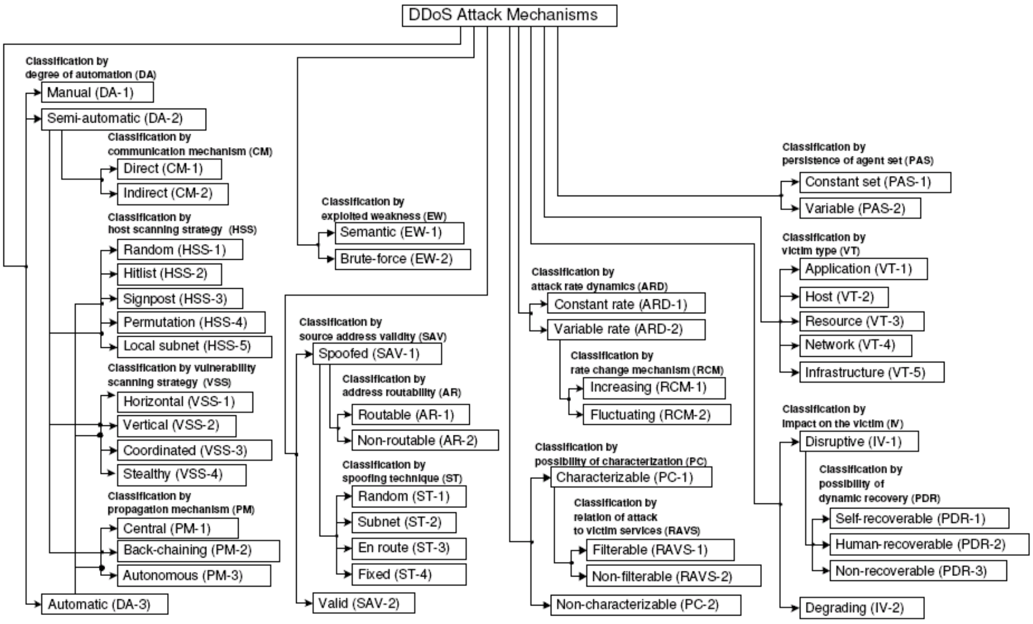
DDoS Attack Mechanisms
Classification by degree of automation (DA)
Manual (DA-1)
Semi-automatic (DA-2)
Classification by communication mechanism (CM)
Direct (CM-1)
Indirect (CM-2)
Classification by host scanning strategy (HSS)
Random (HSS-1)
Hitlist (HSS-2)
Signpost (HSS-3)
Permutation (HSS-4)
Local subnet (HSS-5)
Classification by vulnerability scanning strategy (VSS)
Horizontal (VSS-1)
Vertical (VSS-2)
Coordinated (VSS-3)
Stealthy (VSS-4)
Classification by propagation mechanism (PM)
Central (PM-1)
Back-chaining (PM-2)
Autonomous (PM-3)
Automatic (DA-3)
Classification by exploited weakness (EW)
Semantic (EW-1)
Brute-force (EW-2)
Classification by source address validity (SAV)
Spoofed (SAV-1)
Classification by address routability (AR)
Routable (AR-1)
Non-routable (AR-2)
Classification by spoofing technique (ST)
Random (ST-1)
Subnet (ST-2)
En route (ST-3)
Fixed (ST-4)
Valid (SAV-2)
Classification by attack rate dynamics (ARD)
Constant rate (ARD-1)
Variable rate (ARD-2)
Classification by rate change mechanism (RCM)
Increasing (RCM-1)
Fluctuating (RCM-2)
Classification by possibility of characterization (PC)
Characterizable (PC-1)
Classification by relation of attack to victim services (RAVS)
Filterable (RAVS-1)
Non-filterable (RAVS-2)
Non-characterizable (PC-2)
Classification by persistence of agent set (PAS)
Constant set (PAS-1)
Variable (PAS-2)
Classification by victim type (VT)
Application (VT-1)
Host (VT-2)
Resource (VT-3)
Network (VT-4)
Infrastructure (VT-5)
Classification by impact on the victim (IV)
Disruptive (IV-1)
Classification by possibility of dynamic recovery (PDR)
Self-recoverable (PDR-1)
Human-recoverable (PDR-2)
Non-recoverable (PDR-3)
Degrading (IV-2)

Fig. 4. Classification of DDoS attack [9]

2.4 Classification by Multiple Dimensions

Most of attack have multiple stages with spatial and temporal characteristics. Each stage has different characteristics. Attacks can be described by more than one property, a single property can not describe the characteristics of the entire process in all stages of the attack.

Many existing studies are classified attack from different dimensions. Some brief multidimensional classification methods below.

Lough et al. [10] proposed the VERDICT (Valida-tion Exposure Randomness Deallocation Improper Conditions Taxono-my) based on the characteristics of the attack. Its classification attack into four categories:

(1) Improper validation: the unauthorized access to information or systems inadequate or incorrect authentication.

(2) Improper exposure: the system or information is incorrect leak, the attacker may be directly or indirectly exploit the vulnerability.

(3) Improper randomness: randomness inadequate or random incorrect result in the attacks. For example, cryptography incorrect use of randomness.

(4) Improper deallocation: Information incorrect deleted after use, are vulnerable to attack.

The VERDICT lacks of worms, Trojan horses, viruses and other malicious code classification.

Howard et al. [11] presented a multi-dimensional classification of computer and network attacks. The method takes into account the attacker, tools, attacks motivated attack targets. As Fig.5 shows, attack is divided into five dimensions according to attack process: Attackers, Tools, Access, Results and Objectives. Each dimension is further divided, such as Attackers can be divided Hackers, Spies, Terrorists, Corporate Raiders, Professional Criminals and Vandals. We found that the classification is helpful for understanding the attack process, but not very practical.

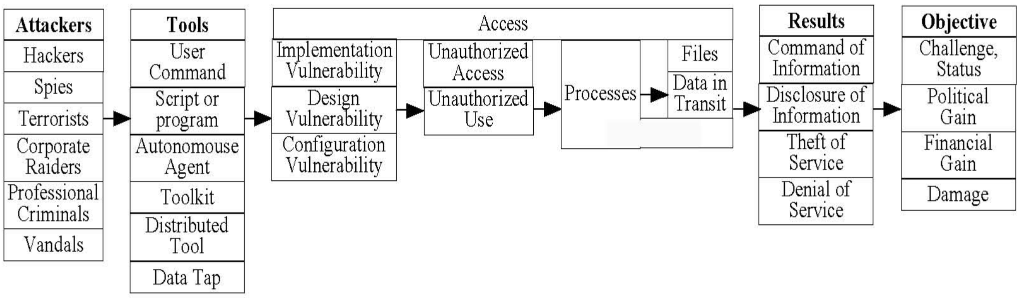

Fig.5 Howard‘s attack classification [11]

Due to the complexity of the attack and mixed, result in difficulties and the actual availability in the attack classification. To this end, Hansman et al. [12] proposed the attack classification method using four dimensions to describe computer and network attacks, shown in Fig.6.

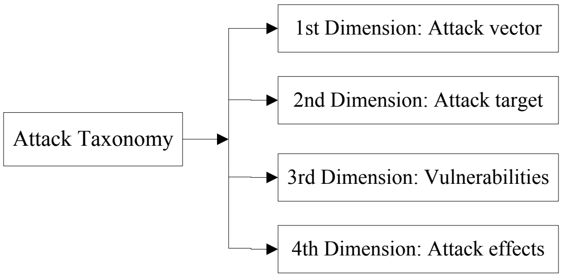
Attack Taxonomy
1st Dimension: Attack vector
2nd Dimension: Attack target
3rd Dimension: Vulnerabilities
4th Dimension: Attack effects

Fig. 6 Hansman's Attck classification

Richard et al. [13] proposed a multi-dimensional attack classification method based on elevation of privilege, which has been recognized by most researchers praise. Privileges from the user elevating to root privileges is an example of the effect of the attack. In the course of the attack, the attacker usually plays the role of a certain user and the user has the appropriate permissions set. From the general visitors to the ordinary user, then the system administrator, the attacker role changes, reflecting the impact of the attack on the target system. As shown in Fig.7, the classification of the attack into four categories:User-to-root (U2R), Remote-to-local (R2L), Denial-of-service (Dos) and Surveilance / probe.

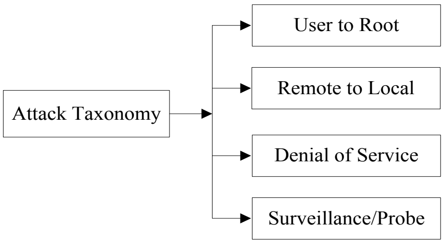

Fig.7 Classification of Lincoln Lab in MIT

3. DMAT. A New Attack Taxonomy

The 1999 DARPA intrusion detection evaluations contained 58 different attack types. Based on the DARPA's attack types and new attacks, and applying attack classification requirements and characteristics for a complete taxonomy, we propose the Defense-oriented Multidimensional Attack Taxonomy, DMAT. The DMAT regard defense as an attack attributes, and take full account of the attack cost and loss. We use nine categories to describe the characteristic of the attack, which are attack target, attack impact, attack purpose, attack cost, attack exploiting, attack source, attack automation, attack loss and defense. The ninth category in the DMAT, classification by defense, is used to provide the defender with instructions of how to defense an attack. Compared to the existing taxonomies, our taxonomy efficiently classifies complex attacks and guide the defender to defense the possible attack. As shown in Figure 8 , our proposed attack classification provides a comprehensive analysis and detailed information of attack to support the understanding of each attack classification, as well as a representative overview of how various attacks in each category. It is included important problem in the evaluating effectiveness and usefulness of the defense.

4. Comparison of The Related Classifica-tion Method

In this section, we will compare our DMAT to previous classification described in Section 2. We will focus on how our network and computer attack classification successfully captured the attack information, and provide a defense and countermeasures to prevent or quell a successful attack is effective. By Red code and Wu-ftpd attack instances, we will compare our classification method and previous classification method, analysis their advantages and disadvantages. Specific as shown in tab.1, tab.2, tab.3.

Howard's classification is too simple to provide value information in characterizing the attack; Hansman's classification provides basic attack information, which is able capture more detail in comparison to Howard. Our classification provides mpre information on what caused the worm infection, and possible defense strategies a network administrator can use to reduce the malware's ability to further propagate and cause damage.

For example，Code Red was a computer worm and attacked computers running Microsoft's IIS web server, described in Microsoft Security Bulletin MS01-033, for which a patch had been available a month earlier. The worm spread itself using a common type of vulnerability known as a buffer overflow. It did this by using a long string of the repeated character 'N' to overflow a buffer, allowing the worm to execute arbitrary code and infect the machine. Kenneth D. Eichman was the first to discover how to block it, and was invited to the White House for his discovery [16]. In our DMAT taxonomy，the source of Code Red is a local network and external network.Code Red attack network by using a long string of the repeated character 'N' to overflow a buffer. Attack object is Windows IIS web server (version 4, 5, 6.0beta), using the configuration vulnerability CVE-2001-0500.Using the Stack buffer overflowor launched network DoS attack. causing the system loss is very high. Attack harmfulness larger, you can install the patch or close the IIS service for defense. Using DMAT, if the first insertion was alleviated, the Code Red worm would not be able to spread.

Table.1. Howard's Attck taxonomy

Attack	Tools	Access	Results	Objectives
Code Red[14]	Script	CVE-2001-0500	Stack Buffer Overflow& TCP packet flooding	Damage
Wu-ftpd[15]	N/A	CVE-1999-0878	Buffer Overflows	Gain root privilege

Table 2. Hansman's Attck taxonomy

Name	1st Dimension	2nd Dimension	3rd Dimension	4th Dimension
Code Red[14]	Network-AwareWorm	IIS 4, 5, & 6.0 beta	CVE-2001-0500	Stack Buffer Overflow& TCP packet flooding DoS
Wu-ftpd[15]	Buffer Overflows	WU-FTPD daemon or its derivatives	CVE-1999-0878	Message File Buffer Overflow & Message File Buffer Overflow

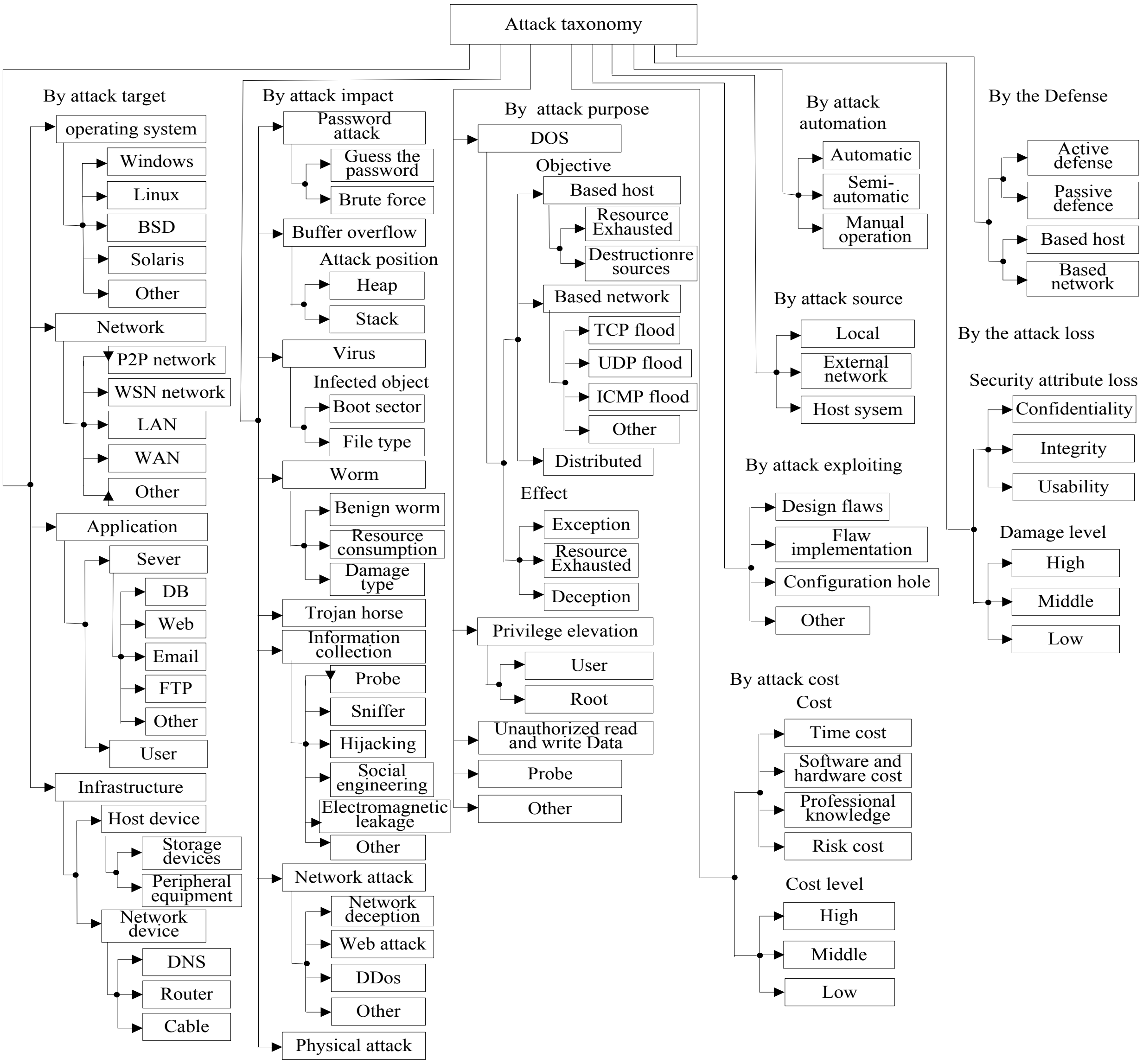

Fig. 8. The DMAT attack taxonomy

Table 3. DMAT attck taxonomy

Attack	Attack source	Attack impact	attack target	Attack Exploiting	Attack automation	Attack purpose	Attack cost	Attack loss	defense
Code Red[14]	Local& external network	Stack Buffer Overflow& TCP packet flooding	Windows IIS web server, 4, 5, 6.0 b	CVE-2001-0500	Semi-automation	Dos	Midlle	High	Install the patch or shut down the IIS service
Wu-ftpd[15]	Local& external network	Stack Buffer Overflow&Mapping_chdir Buffer Overflow	Unix WU-FTPD	CVE - 1999-0878	Semi-automation	Gain root privilege	Low	High	Install the patch or shut down the FTP service

5. Conclusions

Classification of network attack and defense is an important network security research. In this paper we introduced and analyzed previous most popular attack classifications. Although most popular attack classifications provides an content-rich baseline for cyber attack and defense. To solve the problem that the existing attack taxonomy does not consider the characteristics of attack and defensive strategic interdependence. In this paper, we proposed a defense-oriented and multi-dimensional attack taxonomy method, using a variety of relevant attributes of attack and defense as classification. our proposed attack classification provides a comprehensive analysis and detailed information of attack to support the understanding of each attack classification, as well as a representative overview of how various attacks in each category. It is included important problem in the evaluating effectiveness and usefulness of the defense.

Nevertheless, our work in attack classification and analysis is still preliminary. Our approach has provided us with the analysis results necessary to move forward to our next steps which are defence attack. Several important research issues need to be further explored. In particular, in our future work (a) we would refine our attack taxonomy; (b) we would investigate complete discription for every category; (c) we verify and analyses the DMAT ability to network attacks.

Acknowledgements

The paper is supported by the Research Fund for the Doctoral Program (New Teachers), Ministry of Education of China under Grant No. 20121103120032, Humanity and Social Science Youth foundation of Ministry of Education of China under Grant No. 13YJCZH065, Opening Project of Key Lab of Information Network Security of Ministry of Public Security(The Third Research Institute of Ministry of Public Security) under Grant No. C13613, General Program of Science and Technology Development Project of Beijing Municipal Education Commission of China under Grant No. km201410005012, Research on education and teaching of Beijing University of Technology under Grant No. ER2013C24, Beijing Municipal Natural Science Foundation, Sponsored by Hunan Postdoctoral Scientific Program, Open Research Fund of Beijing Key Laboratory of Trusted Computing, Project funded by China Postdoctoral Science Foundation.

References

1. Wei Jiang,“Survey of network and computer attack taxonomy”, in proceedings of 2012 IEEE Symposium on Robotics and Applications(ISRA), 2012, pp.294-297
2. C. E. Landwehr, A. R. Bull, J. P. McDermott, W. S. Choi, “A Taxonomy of Computer Program Security Flaws, with Examples”, ACM Computing Surveys26(3), 1994, pp.211-254
3. Matt Bishop, “A taxonomy of Unix and network security vulnerabilities”,Technical report, Department of Computer Science, University of California at Davis, 1995
4. Zhang Yong-zheng,YunXiaoChun, “A New Vulnerability Taxonomy Based on Privilege Escalation”.[C]In Proceedings of the 6th International Conference on Enterprise Information Systems, Porto, 2004, pp.586-590
5. Frederick B. Cohen, “Information System Attacks: A Preliminary Classification Scheme”, Computers and Security, 16(1), 1997, pp.29-46
6. Álvarez, G. and Petrović, S, “A new taxonomy of. Web attacks suitable for efficient encoding”, Computers &.Security22(5), 2003, pp.435-449
7. Weaver N, Paxson V, Stani'ord S, et al, “A taxonomy of computer worms”, The First Workshop on Rapid Malcode (WORM) , Washington, DC, ACM Press,2003, pp.11-18
8. A.D. Wood, J.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
9. Jelena Mirkovic, Janice Martin, Peter Reiher, “A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms”, UCLA Technical Report #020018, 2002
10. Lough DL, “A taxonomy of computer attacks with applications to wireless networks”, PhD thesis, Virginia Polytechnic Institute and State University, 2001
11. John D. Howard, “An analysis of security incidents on the Internet 1989-1995”, PhD thesis. Carnegie Mellon University, 1997
12. Hansman, S., Hunt R., “A taxonomy of network and computer attacks”, Computer and Security, 2005
13. Richard Lippmann, Joshua W. Haines, David J Fried, Jonathan Korba, and Kumar Das, “Analysis and results of the 1999 DARPA off-line intrusion detection evaluation”, in Proceedings of the Third International Workshop on Recent Advances in Intrusion Detection. 2000, pp.162-182
14. Lemos, Rob, “Virulent worm calls into doubt our ability to protect the Net”,Tracking Code Red. CNET News, Retrieved 14 March 2013
15. CERT Coordination Center. Advisory CA-2001-19 Code Red Worm Exploiting Buffer Overflow In IIS Indexing Service DLL. July 2001(http://www.cert.org/advisories/CA-2001-19.html. Access ed 2 June 2013)
16. CERT Coordination Center, Advisory CA-1999-13 Multiple Vulnerabilities in WU-FTPD (http://www. cert.org/advisories/CA-1999-13.html. Accessed 2 June 2013)
17. Peiqing Zhang, Bjarne E. Helvik,”Modeling Push-based Live P2P Streaming by Stochastic Activity Networks”, Journal of Digital Informati'on Management 10(2),2012,pp. 236-244
18. Sadeghkhani,A.Ketabi,R.Feuillet, “Artifical Neural Network Based Method to Mitigate Temporary Overvoltages”,Journal of Engineering Science and Technology Review,4(2),2011,pp.193-200.
19. R. Kopitov, “Formalization of A Reliable Enterprise Design”, Computer Modelling and New Technologies, 16(1),2012, pp.15-29.