ELECTRONICS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 2006. Nr. 2(66)
ELEKTRONIKA IR ELEKTROTECHNIKA

AUTOMATION, ROBOTICS
T 125
AUTOMATIZAVIMAS, ROBOTOTECHNIKA

Computer System Attack Classification

N. Paulauskas, E. Garsva
Vilnius Gediminas Technical University, Department of Computer Engineering, Naugardukas str. 41, LT–03227 Vilnius, Lithuania, phone: +370 5 2744767, e-mail.: nerijus.paulauskas@el.vtu.lt, eimaslt@computer.org

Introduction

Computer systems are interconnected to achieve more efficiency and better information exchange. The number of potential threats increases because of the computer system integration. Evaluation of the impact on the system is possible when specific features, type and possible influence are known.

A computer system is a heterogeneous, distributed computer network, which faces some attacks. An attack is realization of threat, the harmful action aiming to find and exploit the system vulnerability. A successful attack causes intrusion. Vulnerability is some poor characteristic of the system establishing conditions for the threat to arise. The computer system is affected by the active element – a subject (a user or a process) that initiates the query for the object (resource) access and usage. Access is interaction between the subject and the object during which they exchange information. Incident consists of the attack and the computer system response to it. Attack can fail to achieve the intended objective for some reasons, but even then there exists possibility that the system becomes more vulnerable.

The main purpose of any classification is to suggest such classification features, by which the classification object is fully described. Hypothetical numerical values describing the attack severity are usually used in the computer system security modeling [1]. For more options of modeling and better accuracy the numerical values used in modeling must represent real attack classes and their characteristics. In this article analysis of the known attack classifications is performed, the composed computer system attack classification which is more universal and convenient for future research is presented, and the method of the attack severity numerical evaluation using the computer system attack classification is suggested.

Analysis of known attack classifications

There are lots of known computer system attack classifications, and taxonomies some of them have been analysed in this research [2, 3, 4, 5]. Many investigators have proposed taxonomies that classify attacks based on the intended effect of the attack from the attacker's perspective. An example of the attack effect is the elevation of an attacker's privileges from user to root. These taxonomies often incorporate the technique by which the attacker achieves this effect, such as automated password guessing. Lindqvist and Jonsson [6] presented such taxonomy using these two dimensions of an attack. Howard [7] classified attacks according to *Attackers, Tools, Access, Results* and *Objectives*. The weakness of these classifications is that properties of attacks are not clearly separated.

In his Ph.D. thesis [8] Kumar introduced a classification based on attack signatures used within the IDS IDIOT. This classification is based on the type of observation required to be able to detect a given attack.

Probably one of the best known taxonomies is the Defence Advanced Projects Agency (DARPA) attack taxonomy. This taxonomy was developed in 1998 for classifying attacks in order to simplify the process of evaluating intrusion detection systems [9]. The original purpose of the taxonomy was to reduce the number of attacks needed for the evaluations. Instead of developing a large number of attacks, it should be sufficient to pick a representative subset of each category of attacks. However, it is difficult to define an accurate taxonomy without knowing all possible attack types and considering alternate approaches to grouping attacks. New attacks are constantly being discovered. An improved classification system is being devised to accurately deal with this problem.

The current taxonomy classifies attacks by transitions made between privilege levels and actions performed. Privilege levels (or access levels) are ranked in the taxonomy. The lowest level of access is Remote network access in which minimal network access is possible via an interconnected network of systems. Local network access refers to the ability to read and write from the same network as the victim machine. User access allows someone to run normal user commands on a system. Root/Super-user access describes a set of privileges reserved for system super-users and administrators. The highest level of access is Physical access to a machine, that is, the ability to remove drives, insert disks, and power the machine on and off. This list represents a subset of access

levels relevant to attacks used for the DARPA intrusion detection evaluations.

The 1999 evaluation contained 58 different attack types. This was a substantial increase from the 1998 evaluation, which had only 38 attack types. New attacks were added for Windows NT [10] as well as stealthy versions of old attacks, insider attacks, and six new UNIX attacks [11, 12]. Attacks were grouped into five major categories [13]: Probe or scan, Denial of Service (DoS), Remote to Local (R2L), User to Root (U2R), Data.

Computer Emergency Response Team (CERT) classifies attacks by their degree of success in obtaining access, such as root break-in, account break-in, access attempts and as unauthorised use, e. g. denial-of-service attacks, information corruption and information disclosure [7].

In the well known and widely used open source network intrusion prevention and detection system Snort, the attack classification is based on its impact on the computer system. The attacks whose effect is the most critical have the highest priority. The priority levels are divided into high, medium and low ones. High-level priority attacks are such as the attempted administrator privilege gain, a network "Trojan", web application attack. Denial of service (DoS) attacks are assigned to medium priority attacks, this priority is also given when: a nonstandard protocol or event, potentially bad traffic, attempted log-in using a suspicious user and others are detected. Low-level priority attacks are ICMP event, a network scan, generic protocol command [14].

Suggested Computer System Attack Classification

The computer system attack classification based on the known attack classification analysis and personal knowledge was composed (Fig 1). Every attack possesses all 14 listed features.

Objective achievement is most important for the attacker (1), therefore the attack severity numerical evaluation is based on it.

The effect type (2) most depends on the intruder's objective as well as the subject and object location. ISO/OSI model can characterize all computer system processes. The application layer (3.7) is most suitable because of its potentiality and complexity to perform attacks. There is a variety of operating systems OS in the global network, specific OS families have common vulnerabilities which attract OS specific (4) attacks. Location of the attack subject (5) affects the effect type and the probability of attack object achievements. Attack technology and possible threats are affected by the type of object location (6) and attacked service (7). The attack can be concentrated in one packet, and then the attack is called atomic (8.1) or can be fragmented to several packets (8.2). Feedback (9) is not necessary for all attacks, e.g. sniffing. In order to avoid detection or for better efficiency on the system attackers can choose different initial execution conditions (10), the impact type (11) or automation level. According to the attack objective and the effect type the number of attack sources (13) and connection quantity (14) may differ.

Attack Severity Numerical Evaluation

Modeling is usually used for the computer system security evaluation, incident and security level change forecast. Numerical values are essential for modeling or some automated data processing of the impact on the computer system. Using numbers, which represent the attack, it is possible to group, generate, compare attacks and their distribution in different computer systems and others. The attack is characterized by severity and time characteristics, such as the rate, time between incidents, etc. Time characteristics evaluation is simple, but to evaluate the attack severity is a more complicated task. As it was stated before the possible attack severity can be evaluated by the objective of the attack (1). The attack severity description must be close to those available in Intrusion Detection Systems (IDS) because IDS is used for the attack statistic data collection. The attack description by the objective is used in SNORT IDS and by CERT organization, which has most experience in detecting intrusions and evaluating their effect on computer systems. The 5 level attack severity numerical evaluation was organized using the suggested attack classification and above mentioned IDS classifications. The numerical evaluation using 5 severity levels was chosen because the 3 level severity evaluation is not sufficiently accurate for a vast variety of attacks, and the 10 level evaluation would make the model too large and complicated.

First level attacks are most severe, while fifth level attacks are least severe and having least possible effect on the computer system. The suggested attack severity numerical evaluation is presented in table 1.

A super-user (administrator, root, etc.) has highest rights in the system and is intended to be used for the system administration. The attacker who gains super-user rights (1.1) can have the largest influence on the system.

Table 1. Computer system attack severity numerical evaluation

Attack severity level	Attack class
1	1.1
2	1.2
3	1.3
4	1.4
	1.5
5	1.6
	1.7

A computer system user (1.2) has some specified rights and privileges, which depend on security and network access policy. The intruder having ability to connect to the system as a user can affect the system confidentiality, integrity and cause denial of service. User rights make it easier to acquire super-user rights. The total computer system control is usually the final objective of the intruders.

The system availability is the computer system ability to provide proper service during a defined amount of time. When the system fails to provide some service (1.3), the computer system does not accomplish its mission and the threat to information confidentiality and integrity arises.

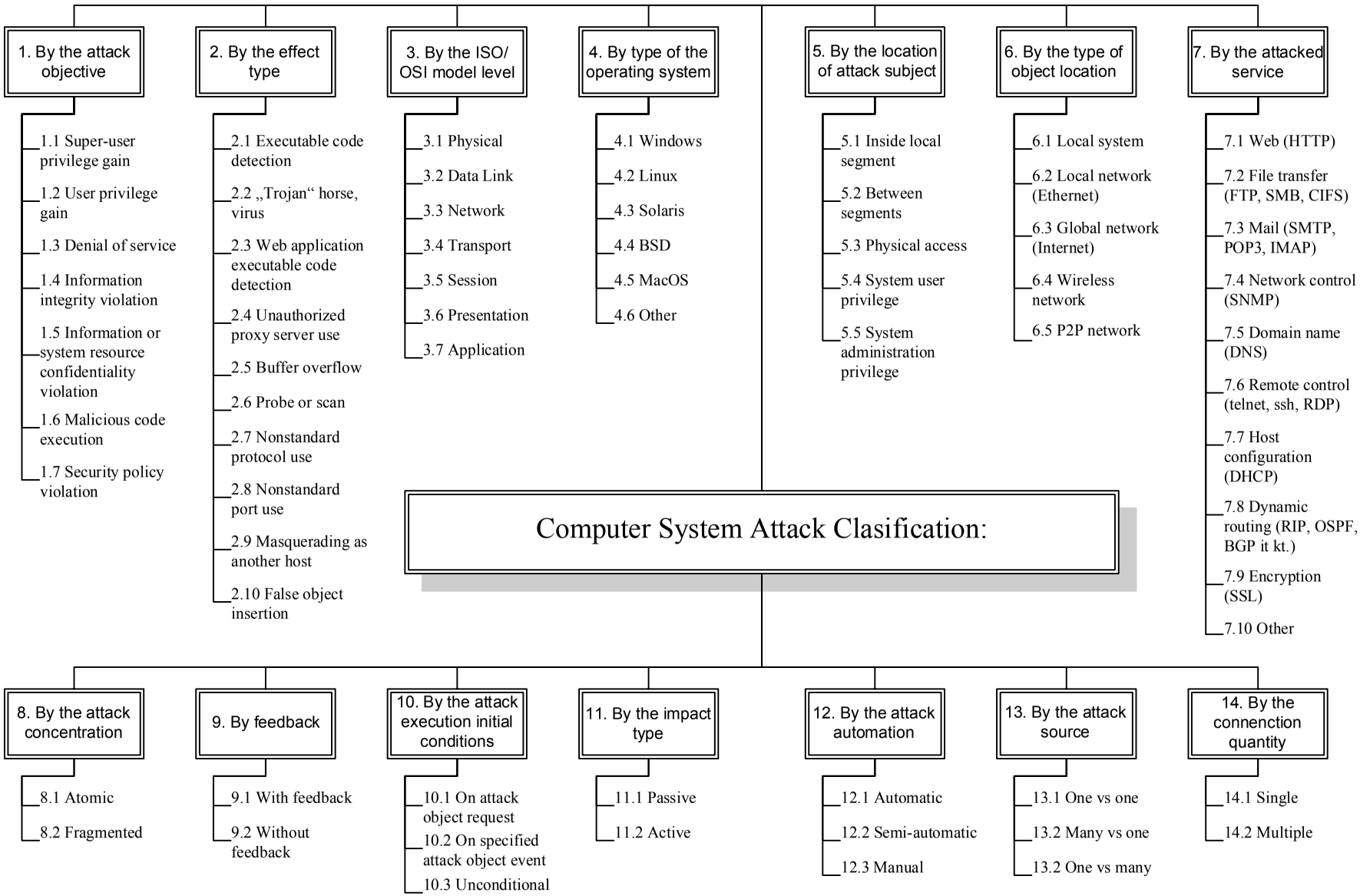

Fig. 1. Suggested computer system attack classification

The information integrity violation (1.4), caused by information corruption, information control between system objects, masquerading as another host, and confidentiality violation (1.5) compromise the system.

The malicious code execution (1.6) and security policy violation (1.7) may compromise the system and reveal valuable information to the attacker and encourage to strive for larger rights in the system.

Conclusions

The computer system modeling and incident forecast need universal classification covering every attack aspect. Most popular attack classifications have been analyzed during the research and the method of the attack severity numerical evaluation using the computer system attack classification is suggested.

1. Existing classification used in intrusion detection systems is considered in the composed computer system attack classification because attack statistical data are gathered using it.
2. Technology evolution will uncover new attacks and new aspects. The suggested classification is open for expansion. New effect types (2), operating systems (4), object locations (6) and services (7) are most possible.
3. The computer system security modeling needs a numerical attack severity evaluation. It is rational to use the 5 level attack severity numerical evaluation based on the attack objective.

References

1. **Garsva E.** Computer system survivability modeling // Electronics and Electrical Engineering. – Kaunas: Technology, 2006. – No. 1 (62). – P. 60–63./in Lithuanian/
2. **Alvarez G., Petrovic S.** A new taxonomy of web attacks suitable for efficient encoding. // Computers and Security, 22(5): p. 435–449, July 2003.
3. **Bishop M.** A taxonomy of Unix and network security vulnerabilities. Technical report, Department of Computer Science, University of California at Davis, May 1995.
4. **Krsul I. V.** Software Vulnerability Analysis. PhD thesis, Comp. Sci. Dept., Purdue University, May 1998.
5. **Landwehr C. E., Bull A. R.** A taxonomy of computer program security flaws, with examples // ACM Computing Surveys, 26(3): p. 211–254, September 1994.
6. **Lindqvist U., Jonsson E.** How to systematically classify computer security intrusions. // IEEE Symposium on Security and Privacy, p. 154–163, Los Alamitos, CA, 1997.
7. **Howard J. D.** An analysis of security incidents on the Internet, 1989-1995. PhD thesis, Carnegie Mellon University, Department of Engineering and Public Policy, April 1997. // www.cert.org/research/JHThesis/table_of_contents.html
8. **Kumar S.** Classification and Detection of Computer Intrusions. PhD thesis, West Lafayette, IN: Purdue University, Computer Sciences, August 1995.
9. **Weber D. J.** A taxonomy of computer intrusions. Master's thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, June 1998.
10. **Korba J.** Windows NT Attacks for the Evaluation of Intrusion Detection Systems, M. Eng. Thesis, MIT Department of Electrical Engineering and Computer Science, June 2000.
11. **Haines J. W., Lippmann R. P.** 1999 DARPA Intrusion Detection System Evaluation: Design and Procedures, A Lincoln Laboratory Technical Report, 2000.
12. **Kendall K.** A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems, M. Eng. Thesis, MIT Department of Electrical Engineering and Computer Science, June 1999.
13. **Lippmann R. P., Haines J. W., Fried D. J., Korba J.** The 1999 DARPA Off-Line Intrusion Detection Evaluation, submitted to Proceedings of 3rd International Workshop on Recent Advances in Intrusion Detection (RAID 2000).
14. **Baker A., Beale J., B. Caswell**, Snort 2.1 Intrusion Detection (Second Edition) 2004, 751 p.

Pateikta spaudai 2005 12 21

N. Paulauskas, E. Garšva. Computer System Attack Classification // Electronics and Electrical Engineering. – Kaunas: Technology, 2006. – No. 2(66). – P. 84–87.

The computer system security modeling needs a numerical attack severity evaluation. Some hypothetical attack severity values are usually used. With the aim to make modeling more accurate and to expand the model abilities it is necessary to relate numerical values used in modeling with real attacks and their classes. In this article most popular attack classifications have been analyzed and the computer system attack classification covering 14 aspects of the attack and suitable for future research is suggested. The method of the attack severity numerical evaluation applying the computer system attack classification using a 5 level attack severity numerical evaluation, based on the attack objective, is suggested. Ill. 1, bibl. 14 (in Lithuanian; summary in Englishб Russian and Lithuanian).

Н. Паулаускас, Э. Гаршва. Классификация атак компьютерных систем // Электроника и электротехника. – Каунас: Технология, 2006. – № 2(66). – С. 84–87.

Моделируя безопасность компьютерных систем, часто задаются предполагаемые численные значения, по которым определяется эффективность атаки. С целью наиболее расширенного и точного моделирования в нем необходимо связать используемые численные значения с реальными атаками и с их классами. В этой статье обсуждается широко используемые классификации атак, предлагается классификация атак полезная в научных исследованиях, которая охватывает 14 признаков атак и представляется численная их оценка. Численная оценка атак делится по пятибальной шкале, которая определяется эффективностью и целью атаки. Ил. 1, библ. 14 (на литовском языке; рефераты на английском, русском и литовском яз.).

N. Paulauskas, E. Garšva. Kompiuterių sistemų atakų klasifikacija // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2006. – Nr. 2(66). – P. 84–87.

Modeliuojant kompiuterių sistemos saugumą dažnai parenkamos hipotetinės atakos sunkumą nusakančios skaitinės vertės. Modeliavimo galimybėms ir tikslumui padidinti modeliavimui naudojamas skaitines vertes būtina susieti su realiomis atakomis ar jų klasėmis. Šiame straipsnyje aptariamos plačiai naudojamos atakų klasifikacijos, siūloma moksliniams tyrimams patogi atakų klasifikacija pagal 14 požymių, pateikiamas skaitinis kompiuterių sistemos atakų įvertinimas penkiais sunkumo lygiais, kurie tiesiogiai priklauso nuo atakos tikslo. Il. 1, bibl. 14 (lietuvių kalba; santraukos anglų, rusų ir lietuvių k.).

DOI: 10.5755/j02.eie.10619