Quantitative Evaluation for Survivability of Autonomic Intrusion Tolerance System

Qingtao Wu, Jie Chen and Ruijuan Zheng

Electronic & Information Engineering College, Henan University of Science and Technology Luoyang, Henan Province 471023, China

Summary
A quantitative method for evaluating survivability of an autonomic intrusion tolerance system is proposed based on the features of the aforementioned system that are different from those of a common network security system. Four survivability evaluation criteria, namely, data confidentiality, data completion, service availability, and system autonomy, are built with quantization methods for their respective features after considering the effects of intrusion on the system as well as automatic intrusion tolerance functions. The survivability of an autonomic intrusion tolerance system is quantitatively calculated using the four criteria.

Keywords:
Autonomic Computing, Intrusion Tolerance, Survivability, Evaluation Criteria.

1. Introduction

Increasing network complexity, system size, and operation speed has resulted in ever-increasing risks and threats against network system security. Traditional information security systems rely on whether user terminals are certified and authorized to access a protected network. However, traditional methods cannot make accurate user-credibility evaluation because of lack of reliable evidence for network systems to determine credible network access. Therefore, effectively protecting network systems from security threats is not always successful. Traditional methods can only defend networks and cannot meet security demands in the presence of complex attacks.

Intrusion tolerance systems belong to third-generation network information security technology [1]. These systems emphasize the fact that when several parts of a system are attacked by intruders, the entire system maintains normal or degraded services and ensures data confidentiality, completeness, and availability [2]. Researchers have adopted autonomic computing in recent years to develop an intrusion tolerance system, with the hope that this system can operate autonomically and adapt to different environments. An autonomic intrusion tolerance system is a new type of network information security system which integrates work mechanism into an autonomic computing intrusion tolerance system to provide automatic intrusion tolerance capability [3–5].

This study is motivated by limitations in evaluation criteria for assessing survivability. System survivability evaluation reflects security condition of the current system during operation, and reminds the system administrator to promptly conduct effective security measures. Compared with common network systems, the most significant features of an autonomic intrusion tolerance system lie in its tolerance and capability for autonomy against intrusion behavior. Therefore, system tolerance and autonomy against intrusion behavior should be emphasized in studying survivability of an autonomic intrusion tolerance system. Existing network system evaluation methods for autonomic intrusion tolerance system survivability cannot meet the aforementioned requirements [6]. Thus, a novel survivability evaluation method is proposed in this study.

The rest of the paper is organized as follows. In Section 2, survivability evaluation is introduced, then the proposed method is presented to establish criteria for survivability quantitative evaluation of autonomic intrusion tolerance system and to determine expected evaluation values. In Section 3, experiments are conducted to validate the proposed method. The conclusion is provided in Section 4.

2. Survivability evaluation

Survivability refers to the capability of a system to complete key tasks in case of a network attack, system errors, and accidents. System survivability applies to the entire system rather than to a single part. It emphasizes the ability to provide effective or degraded services in case of an attack [7]. Current studies on system survivability include two major areas, namely, survivability design and survivability evaluation. The latter explores procedures for evaluating system survivability and offers an evaluation standard for implementing survivability authentication at information security level.

Manuscript received October 5, 2012
Manuscript revised October 20, 2012

2.1 Evaluation analysis

Intrusion goals fall into one of three categories based on intrusion effects on survivability of system data and services. These categories are: 1) obtaining confidential data, 2) destroying important data, and 3) causing system failure in offering normal services. When a system is under intrusion attack, survivability requires the system to ensure data confidentiality, completeness, and service availability. Therefore, three evaluation criteria, namely, data confidentiality level, data completion, and service availability, are proposed in this research.

A fourth evaluation criterion, system autonomy, is given according to unique automatic functions of an autonomic intrusion tolerance system and the conditions required to adjust system capacity against intrusion. Thus, this study evaluates the survivability situation of an autonomic intrusion tolerance system by defining and quantizing the four aforementioned criteria.

2.2 Definition and quantization of evaluation criteria

Definition 1: Data confidentiality

Data confidentiality level *B* measures the extent of system capability to ensure that confidential data will not be cracked by intruders.

In an autonomic intrusion tolerance system, (*t*, *n*) threshold cryptography programs are generally used to process confidential data to allow certain tolerance of confidential data for intrusion. Confidential data are split into *n* subshares stored in different spaces in the system, from which the intruder needs to obtain at least *t* subshares to crack confidential data. Assuming the intruder has obtained t_0 subshares of confidential data during an intrusion attack, then the confidentiality level of these data is presented as the probability sum that the subshare t_0 obtained by the intruder is smaller than *t*; and the probability that subshare t_0 is equal to or greater than *t* but cannot be decrypted, i.e.:

$$B_i = P\{t_0 < t\} + P\{fail / t_0 \geq t\} \quad (1)$$

Assuming a total of n_0 important data, the confidentiality of which must be ensured in the autonomic intrusion tolerance system, then the data confidentiality level of the system is:

$$B = \frac{1}{n_0}\sum_{i=1}^{n_0} B_i \quad (2)$$

Definition 2: Data completion

Data completion *T* is the extent to which the system is capable of protecting data from being destroyed by intruders.

In an autonomic intrusion tolerance system, (*t*, *n*) threshold cryptography program is commonly used to back up important data and to improve data completeness while maintaining data confidentiality. The system only needs to obtain any *t* subshares to restore original data. Therefore, even if the intruder destroys several subshares, data can still be restored as long as the surviving subshares are not less than *t*. Data are still kept confidential as long as the number of subshares obtained by the intruder is smaller than *t*. Calculation method of completion for several data in the autonomic intrusion tolerance system is as follows:

$$T_t = \begin{cases} \dfrac{n-m-t+1}{n-t+1} & n-m \geq t \\ 0 & n-m < t \end{cases} \quad (3)$$

where T_i is the completion of a single data, *n* is the backup number of the threshold cryptography program applied by the data (*t*, *n*), *t* is the threshold value of threshold cryptography, *n* is the unused threshold cryptography program, $t = 1$, and *m* is the number of data subshares already destroyed by the intruder.

Assuming that a total of n_1 important data is found in an autonomic intrusion tolerance system, the completeness of which must be ensured, then data completion of the system is:

$$T_t = \frac{1}{n_1}\sum_{i=1}^{n_1} T_i \quad (4)$$

Definition 3: Service availability

Service availability *U* refers to the capability of a system to offer normal services to legal users when an intruder attempts to cause system failure in delivering several normal services.

Assuming that the types of services the system is capable of offering are $\{X_1, X_2, \ldots, X_L\}$, then service conditions can be classified into five levels {Excellent, Good, Ordinary, Relatively bad, and System collapse}, which are assigned certain values {5, 4, 3, 2, and 1}. *k* services are available in Type *i* service X_i, and the availability of the service $U(X_i)$ is the service under the greatest effect of such type of service, i.e.:

$$U(X_i) = \max\{U(X_{ij})\},\ j \in (1,k) \quad (5)$$

Therefore, the service availability of the system is:

$$U = \frac{1}{L}\sum_{i=1}^{L}\frac{1}{U(X_i)} \quad (6)$$

Definition 4: System autonomy

System autonomy *A* refers to the capability of the system to automatically adjust intrusion tolerance under intruder attack.

Assuming that (*0*, *t*) is a section of time that is sufficiently long, within which h_0 intrusion tolerance incidents happen, and h_1 refers to the incidents in which the system offers effective services that occurred after automatic tolerance for intrusion, then the system autonomy is:

$$A=\frac{h_1}{h_0} \quad (7)$$

Definition 5: System survivability

The survivability *S* in the autonomic intrusion tolerance system is a comprehensive evaluation of the extent to which the system stands against or tolerates intrusion behaviors. It refers to the capability of the system for autonomy.

In summary, the calculation method for the survivability of an autonomic intrusion tolerance system can be expressed as:

$$S=\varepsilon_1 B+\varepsilon_2 T+\varepsilon_3 U+\varepsilon_4 A \quad (8)$$

where ε_1, ε_2, ε_3, and ε_4 are weighting coefficients through which $\varepsilon_1+\varepsilon_2+\varepsilon_3+\varepsilon_4 = 1$ is satisfied. The specific value of the weighting coefficient should be determined by the extent to which the actual system values various criteria. Specific value is determined based on experiences or by evaluation technology.

S evaluation value is the standard for evaluating survivability of an autonomic intrusion tolerance system, which is shown in Table 1. This value describes changes in survivability situation of an autonomic intrusion tolerance system.

Table 1: Survivability grade description.

S evaluation value range	***Survivability level***
0.9 to 1.0	Excellent
0.8 to 0.9	Good
0.6 to 0.8	Ordinary
0.4 to 0.6	Relatively bad
0 to 0.4	System collapse

3. Verification and Analysis

3.1 Experimental environment

The experimental environment, as demonstrated in Figure 1, primarily comprises the following components: one Windows XP system console server with an Intel Pentium IV 2.8 G processor, six application servers with different operational systems, an HP128 port fiber channel (FC) switch, and so on. Among these components, the console server has a specific autonomy and tolerance mechanism that takes charge of receiving service requests from the user, sending such requests to various application servers, and receiving and processing results of various server responses to take specific management measures. Important data, confidentiality, and completeness of data must be ensured to allow (*t, n*) threshold cryptography program to be saved in several application servers.

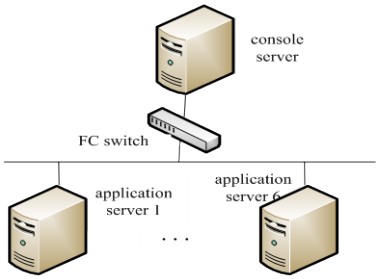

Fig. 1. Structure of experimental system.

Survivability of the console server is disregarded to operate the experimental system, i.e., the evaluation of system survivability only included survivability of various application servers. In the experimental system, six important data sets use (t, n) threshold cryptography program to be saved in various application servers. In addition, the threshold values used are as follows: D1 is (3, 4), D2 is (3, 5), D3 is (2, 3), D4 is (2, 5), D5 is (2, 4), and D6 is (3, 5). The aforementioned threshold values are used because of varying confidentiality and completeness requirements of different data. The experimental system can address three services: file transfer protocol, Web, and e-mail.

3.2 Quantitative evaluation and result analysis

A group of students was organized to imitate hacker intrusion behaviors. The students conducted various intrusion attacks on the experimental system for a time period (6:00 to 24:00). During this period, different forms of attacks, such as probing, remote-to-local attacks, user-to-root attacks, and denial of service, among others, were attempted on various application servers.

Intrusion attack behaviors attempt to obtain or destroy subshares of confidential or important data saved in various application servers. This type of attack also hinders normal services being offered by various application servers. During the test procedure, system survivability was comprehensively analyzed based on the definitions and quantization methods of various criteria discussed earlier. System data confidentiality level, data completion, service availability, and system autonomy were all measured. Figure 2 illustrates the security situation of the four criteria. Figure 3 demonstrates changes in survivability of the entire system over time with weighting coefficients $\varepsilon1=\varepsilon2=\varepsilon3=\varepsilon4=0.25$.

A sampling time point was conducted for each hour between 6:00 and 24:00. Table 2 shows the survivability situation level of the system at various sampling time points.

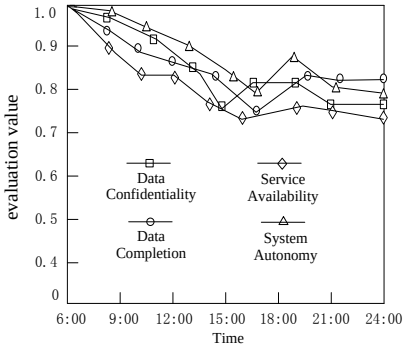

Fig. 2. Structure situation of various criteria of the system.

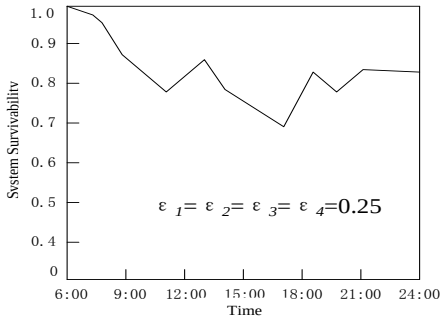

Fig. 3. Changes in system survivability over time.

Table 2. Survivability level at different time points during system sampling.

Time points	*S range*	*level*	*Time points*	*S range*	*level*
7:00	0.9–1.0	Excellent	16:00	0.6–0.7	Worse
800	0.9–1.0	Excellent	17:00	0.8–0.9	Good
9:00	0.8–0.9	Good	18:00	0.8–0.9	Good
10:00	0.8–0.9	Good	19:00	0.8–0.9	Good
11:00	0.7–0.8	Worse	20:00	0.7–0.8	Worse
12:00	0.8–0.9	Good	21:00	0.8–0.9	Good
13:00	0.8–0.9	Good	22:00	0.8–0.9	Good
14:00	0.7–0.8	Worse	23:00	0.8–0.9	Good
15:00	0.7–0.8	Worse	24:00	0.8–0.9	Good

Based on Table 2 , Figure 2, and Figure 3, system survivability level is excellent between 6:00 and 8:00.
Over time, with the number of hackers, attack types, and frequency gradually increasing, system performance slightly decreased at 9:00. However, survivability level was still good. At approximately 11:00, system survivability level worsened. As system survivability situation failed to reach the level beyond good, specific index conditions that were breached by intrusion can be derived from Figure 2. Subsequently, the autonomy mechanism of the autonomic intrusion tolerance system began to play a role in dynamically and automatically adjusting various functional parameters.
At approximately 12:00, system survivability level once again became good. As the students became more familiar with the experimental system and with the increasing attack types and methods, system survivability situation fluctuated across all levels, and then finally became stable.
The experiment shows that the quantitative evaluation method for autonomic intrusion tolerance system survivability can correctly reflect survivability situation. The survivability situation map promptly informs the system administrator of the current security condition of the system. Thus, the system administrator can take effective measures to reinforce weak points and to increase system tolerance against intrusion.

4. Conclusions

An evaluation method for autonomic intrusion tolerance system survivability based on autonomic intrusion tolerance system features is proposed in this paper. Four survivability evaluation criteria, namely, data confidentiality level, data completion, service availability, and system autonomy, are built with quantization methods for their respective features after considering the effects of intrusion on the system and the functions of automatic intrusion tolerance. The effects of existing system deficiencies and attack behaviors on survivability are studied using defined quantitative measures.
System survivability evaluation criteria given in the present work, including vigorousness, adaptability, and steady state, among others, are still incomplete. However, these criteria are all important factors that affect system survivability. Therefore, further studies must construct and subsequently prove the efficiency of comprehensive survivability evaluation indicators.

Acknowledgments

The authors want to thank the anonymous reviewers for their valuable comments and suggestions. This work is sponsored partially by the National Natural Science Foundation of China (No. 61003035 and 61142002) and the Plan For Scientific Innovation Talent of Henan Province (No. 124100510006)

References

[1] ZHANG Yun-ying, NURBOL, WANG Cheng-ming, et al. "Status of Intrusion Tolerance", Journal of JILIN University(Information Science Edition), 2009, vol. 27, No.4, pp. 389-394.
[2] Hai Wang and Peng Liu. "Modelling and Evaluating the Survivability of an Intrusion Tolerant Database System", Lecture Notes in Computer Science, 2006, vol. 4189, pp. 207-224.
[3] GUO Shi-ze, NIU Guan-jie, ZHENG Kang-feng. "An Intrusion Tolerance Model and Quantizing Analysis", Journal of Beijing University of Posts and Telecom. 2007, Vol. 30, pp. 36-39.
[4] LI Bing-yang, WANG Hui-qiang, FENG Guang-sheng. "Model construction and quantitative analysis of autonomic intrusion tolerance system", APPLICATION RESEARCH OF COMPUTERS. 2009, vol. 26, No.5, pp.1883-1887.
[5] Stroud R.,Welch I.,Warne, J., et al. "A qualitative analysis of the intrusion-tolerance capabilities of the MAFTIA architecture", 2004 International Conference on Dependable Systems and Networks. 2004, pp.453-61.
[6] YIN Li-hua, FANG Bin-xing. "Security Attributes Analysis for Intrusion Tolerant Systems", Chinese Journal of Computers, 2006, vol. 29, No.8, pp.1505-1512.
[7] WANG Huiqiang, RONG Ji. "Design and Implementation of an Intrusion-tolerant COTS-based Server on Heterogeneous Platforms", Computer Engineering. 2006, vol. 23, No.3, pp.177-179,182.

Qingtao Wu, born in 1975. PhD and master supervisor. Member of China Computer Federation. His main research interests include computer system security, intelligent information processing, etc.

Jie Chen, born in 1985. Expected Master degree in computer science and technology from Henan University of Science and Technology. His main research interests include computer system security, intelligent information processing, etc.

Ruijuan Zheng, born in 1980. PhD and master supervisor. Member of China Computer Federation. His main research interests include computer system security, network security, etc.