Research on risk assessment technology of China's railway ticket selling and reservation system

Yingming Zhao1a, Dedong Zhang2 & Jubao Li2
1 China academy of railway sciences, Postgraduate Department, Beijing, China
2 China academy of railway sciences, Institute of computing technology, Beijing, China
a295771854@qq.com

Abstract. Application of Internet ticketing in railway ticketing is increasingly critical and the corresponding security risk problem is more prominent with development of science and technology. This paper realized analysis of core risk factors of railway ticket selling and reservation system of China and presented a quantifiable risk assessment model with fuzzy mathematics basing on the characteristics of this system with good usability by experimental results.

1. Introduction
Railway ticket selling and reservation system of China (hereinafter referred to as the ticketing system) was established to improve the management level and service quality of railway passenger transport, realizing reservation and sale of train tickets through the Internet.

The ticketing system has been launched since 1996, with more than 20 years of technical and business accumulation, realizing the transformation from manual ticketing to computer ticketing [1].

Ticketing system has been achieved a variety of external services as Internet ticketing, mobile ticketing and electronic payment at present. What’s more, number of registered users and access scale have grown rapidly since the launch of the system. Up to now, the peak day page views of 12306 platform have exceeded 150 billion, and the highest day tickets sold have exceeded 12 million, which accounts for more than 80% of the total ticket sales.

With the increasing of the total ticket volume, the safety and stability of the railway ticket reservation and selling system are more significant. To ensure the safe and stable operation of the system, the threat of China's railway ticket sales and reservation system finding out in time is very important.

2. Architecture of the ticketing system
The ticketing system is a cloud computing platform of more than 2000 stations comprising with 1 head office center and 18 regional centers. Among them, the head office center is a double-live structure, supporting the operation of 12306 website to ensure safety and stability of the system [2].

Overall structure of ticketing system is shown in figure 1:
3. Security risks of the ticketing system

Risk assessment is to evaluate and estimate potential risks of system with quantitative or qualitative methods.

According to the view of OWASP 2017, assets, threats and vulnerability should be comprehensively considered as the three aspects of the risk assessment of network system.

The formula is:

\[ R = f(Z, S, V) \]

Where, Z represents the asset set of the system; S represents the possibility of risk occurrence of the system; and V represents the impact of risk occurrence to the system.

The main steps of the risk assessment are as follows:

Step 1: identifying the scope of assets to be protected;
Step 2: identifying the risk categories facing the system;
Step 3: assessing possible risk factors;
Step 4: assessing the impact of risk on system security;
Step 5: determining the risk level of the system;

The assets with impact on the security of ticketing system are mainly divided into two parts as physical assets and information assets.

1) Physical assets: the physical assets of the ticketing system are consisted of various host equipment, network equipment, security equipment, storage equipment and machine room environment. The site, power supply and various disaster emergency facilities as earthquake and fire prevention are included in machine room environment.

2) Information assets: the information assets of the ticketing system are constituted with various software, as business application software, general application software, operating system, database, middleware, various management software and security system.

4. Risk analysis of the ticketing system

The ticketing system is a large and complex system with a huge structure and a wide range of security threats from all sides. Moreover, the security risks involved in the ticketing system are roughly divided into several categories, which are elaborated and analyzed respectively in this paper.

4.1 Risk of base environment of system

Basic environment of the ticketing system is consisting of software and hardware. Moreover, application system, operating system, database, middleware, Virtual Server, management system and
security system are included in software system. And host equipment, network equipment, security equipment, storage equipment and computer room environment are involved in hardware [3].

Due to numerous system security problems caused by software and hardware failures, the overall influence of various software and hardware contained in the system are different as well. Therefore, reasonably evaluation of security threat of software and hardware problems on the whole system is significant, for locating the system and maintaining the stability of the system quickly and accurately.

4.2 External threats of system
Network is fragile. What’s more, threats from all aspects of the outside world would be faced with the system running in the network environment. Therefore, information leakage, system crash, business suspension and a series of problems are easily led by attack of external attackers on the system.

Pressure and load of system are huge during the peak period, due to business characteristics of ticketing system.

Conducting precautions are required to against external security threats of ticketing system, relating to national economy and people's livelihood.

4.3 Risks from application layer traffic
Due to the application characteristics of the ticketing system itself, the pressure and load of the system are huge during the peak period. The pressure of server from application layer traffic on the system is almost equal to a large DDoS attack, which is also a great threat to the security of the ticket system.

4.4 Risks from Management Gaps and People
Disordered management, unclear rights and responsibilities, imperfect safety management system, insufficient safety awareness of practitioners, and insufficient technical ability are potential factors of system safety risks.

Hence, fully consideration of the impact of management and personnel risks on the system when conducting risk assessment of the system is significant.

5. Risk assessment model
According to the four major risk factors of the ticketing system described above, different algorithms to calculate its risk index $R_i$ are adopted respectively in this paper. Combining the risk index of four main risk factors, the overall risk index of the system is finally obtained. Moreover, risk assessment method is conducted to more targeted discovery of weaknesses in the design, operation and maintenance of system.

5.1 Risk index of operation of system’s basic environment
Risk index of operation of system’s basic environment is [4];

$$R_i = (a_1 \cdot p_1, a_2 \cdot p_2, \ldots, a_i \cdot p_i) \cdot E^T \cdot N_i$$  (1)

Among them:

$$A = \{a_1, a_2, \ldots, a_i\}$$  (2)

$a_1, a_2, \ldots, a_i$ are referred to importance of hardware and software components of system's basic environment as hardware equipment, database and security equipment [5].

$$p_i = \{p_1, p_2, \ldots, p_i\}$$  (3)

$$p_1 + p_2 + \cdots + p_i = 1$$  (4)

$p_1, p_2, \ldots, p_i$ represents probability of risk events occurring in this part during system operation.

The risk matrix $E_i = \{e_1, e_2, \ldots, e_i\}$, $e_i \in [0, 1]$, represents the hazard degree of possible security events occurring.
For the ticketing system adopting redundancy architecture, which plays a positive role in the security of the system, $N_d$ indicates the robustness of the redundancy architecture of the ticketing system. $N_d \in (0, 10]$, the smaller the value of $N_d$, the higher the robustness of the redundant architecture is.

### 5.2 Risk index of external threats of system

Risk brought to system by threats from outside of the system are relied on technical level of attackers, degree of harm and exposure range of system vulnerabilities [6].

$$K_{ij} = S_k \cdot (B_1, B_2, B_3)$$

Where, $S_k$ represents the technical level of the attacker, $S_k \in [1, 5]$; $B_1$ represents the intention of the attacker, $B_1 \in [1, 5]$; $B_2$ represents the opportunity level created by the current environment for the attacker, $B_2 \in [1, 5]$; and $B_3$ represents the scale of the attacker in the current society, $B_3 \in [0, 4]$.

The risk matrix brought by the security vulnerability of the system is:

$$Q_{i1} = N_{IDS} \cdot C_2 \cdot C_3$$

Where, $N_{IDS}$ represents the robustness of the intrusion detection system of the system, $N_{IDS} \in [0, 10]$; $C_1$ represents the difficulty of finding vulnerabilities, $C_1 \in [1, 5]$; $C_2$ represents the difficulty of exploiting vulnerabilities, $C_2 \in [1, 5]$; $C_3$ represents the propagation of vulnerabilities, $C_3 \in [1, 5]$.

Therefore, the risk index of external threats is:

$$R_k = K_{ij} \cdot Q_{i1}$$

Where, level of attackers and risk index of external threats is directly proportion, while intrusion of detection system and risk index of external threats is inversion [7].

### 5.3 The risk index from application layer traffic

For the ticketing system itself, the huge traffic during the peak period of ticket sales will caused great pressure on the system. This will be a serious test for the system.

Therefore, the index of risks caused by application layer traffic is $R_3$, which is a function dynamically changing with time $t$.

By the analysis of previous business data, $R_3$ is constructed as:

$$R_3 = \begin{cases} 
100 - 3t & t = 6, 12, 15 \\
50 - \ln t & t \in (6, 23), t \neq 6, 12, 15 \\
0 & t \in (0, 6) \cup (23, 24) 
\end{cases}$$

### 5.4 Risk index of management gaps and people

Probability of security incident is $P_M$ affected by management error, personnel safety awareness and insufficient technology.

$$P_{M_i} = P(M_i|D_i) \cdot P(D_i) + P(M_i|\overline{D_i}) \cdot P(\overline{D_i})$$

Where, $M$ represents the existing security risks and $D$ represents the security problems caused by the security risks.

Therefore, risk index $R_M$ described by management errors, personnel skills and insufficient safety awareness is:
\[ R_M = \sum P(M_i) \cdot C_i \]  \hspace{1cm} (10)

Where, \( C_i \) represents the harm degree of the corresponding security event \( D_i \) to the system.

5.5 Risk index of whole system

Risk from system’s basic environment, risk of external threats and risk of management gaps and people are included in risk of system. Hence, risk index of whole system is [8]:

\[ R = R_s + R_t + R_0 + R_M \]  \hspace{1cm} (11)

Based on previous experience and data analysis, risk index obtained under the risk assessment model is classified into the following categories:

| risk index | degree of risk |
|------------|----------------|
| 0~100      | low            |
| 100~200    | mid            |
| 200~300    | high           |

6. Testing of risk assessment models

To effectively verify the effectiveness of the risk assessment model, ticketing system of a railway bureau is taken as an example to test and verified the risk assessment model mentioned in this paper.

Railway authority is composed by two core switches, four chain switches, four FC switches, two storage devices and several physical servers. The architecture is shown in figure 2:

![Architecture diagram of a railway test environment](image)

Figure 2. Architecture diagram of a railway test environment

The flow analysis system is deployed at the key nodes of the system to analyze and monitor the overall operation situation of the system.

After analysis, the threat from the system is divided into four parts as network and hardware security risks, software security risks, system design vulnerabilities and computer room environment security risks.

Therefore:

\[ A = \{a_1, a_2, \ldots, a_4\} \]  \hspace{1cm} (12)
According to expert knowledge and the result of the date analysis, the importance degree and risk value of each part of the system are assigned, and RS value of that environment is obtained eventually [9].

\[ A = \{a_1, a_2, ..., a_4\} = \{7, 8, 5, 6\} \]  \hspace{1cm} (13)

The percentage of risk events occurring in each part is assigned as:

\[ P_i = \{p_1, p_2, p_3, p_4\} = \{0.5, 0.2, 0.1, 0.1\} \]  \hspace{1cm} (14)

The severity of risk events of each part to the system is:

\[ E_i = \{e_1, e_2, ..., e_4\} = \{3, 6, 2, 6\} \]  \hspace{1cm} (15)

The robustness of the redundant architecture of this system is:

\[ N_d = 3 \]  \hspace{1cm} (16)

The risk index of operation of system’s basic environment is:

\[ R_s = (a_1 \cdot p_1, a_2 \cdot p_2, a_3 \cdot p_3, a_4 \cdot p_4) \cdot E \cdot N_d = 22.23 \]  \hspace{1cm} (17)

According to the current social development, it is determined that the general technical level of attackers is 3; the willingness to attack is 4; the opportunity created by the environment for attackers is 3; and the scale of attackers is 4.

Hence, the attack matrix is:

\[ K_B = S_B \cdot (B_1, B_2, B_3) = (12, 9, 12) \]  \hspace{1cm} (18)

Intrusion detection system with a strong robustness of system could be assigned with a small value of 1. What’s more, the difficulty of finding vulnerabilities is 1; the difficulty of exploiting vulnerabilities is 2; and the size of vulnerability propagation is 3.

\[ C_1 \]

\[ Q_3 = N_{IDS} \cdot C_2 = (1, 2, 3) \]  \hspace{1cm} (19)

Therefore, the risk index of external threats is:

\[ R_c = K_B \cdot Q_3 = 66 \]  \hspace{1cm} (20)

The risk index from application layer traffic is obtained by taking 15 o’clock, the peak time of ticket sales, as an example:

\[ R_s = 50 \]  \hspace{1cm} (21)

According to the existing knowledge, probability of occurrence of security events due to management errors, personnel safety awareness and technical deficiencies is assigned, and the probability matrix \( P \) and the influence degree matrix \( C \) of security events are obtained by calculation:

\[ R_M = \sum P(M) \cdot C = 34 \]  \hspace{1cm} (22)

Therefore, the risk index of this bureau is:

\[ R = R_s + R_c + R_M = 172.23 \]  \hspace{1cm} (23)

Risk is large for over 100 of risk index, so the environment of this bureau could be improved by rectification and adjustment of risk prevention.

7. Conclusion

Application of high availability risk assessment model is becoming significant in the railway ticket selling and reservation system with development of information technology.

A targeted risk assessment model is put forward in this paper, solving the existing problems as lacking pertinence to some extent and influencing of system structure adjustment, optimization, future management and decision-making positively.
References

[1] Z. H. Wu, M. Z. Ye, and X. K. Liu, “Research and development of safety technology of railway ticket reservation and sale system,” T.H.Chen. China Railw. Sci. Beijing, vol. 22, pp. 63-66, January 2001.

[2] H. T. Li, Y. Liu, and D. Q. He, “A security risk evaluation model for IT system and its application on railway passenger ticket system,” W.H.Liu. China Railw. Sci. Beijing, vol. 1, pp. 127-130, 2007.

[3] C. J. Wang, Z. X. Jiang, T. Wang, and X. H. Guan, “The model of network security risk assessment system based on fuzzing mathematics,” Y.B.Wang. Net. Security Tech. Appl. Beijing, vol. 10, pp. 22-25, September 2003.

[4] M. Fang, K. Y. Xu, T. Q. Yang, F. W. Meng, and C. Yu, “A distributed network risk assessment method based on attack graph,” Y.L.Zhu. Appl. Mech. Mater. Chongqing, vol. 40, pp. 139-144, 2013.

[5] J. Li., D. D. Qian, K. Luo, and Y. Niu, “Risk assessment of network node resource risk based on monte carlo,” Y. Liu. Comput. Digital Eng. Wuhan, vol. 47, pp. 577-581, May 2019.

[6] Q. Li, D. P. Xu, G. Z. Zhu, X. K. Liu, L. Shen, and J. B. Li, “Research on optimization of railway ticketing emergency plan based on virtualization,” R.Chen. Railw. Comput. Appl. Beijing, vol. 2, pp. 5-8, June 2018.

[7] Y. Chen, “Computer network information security risk assessment standard and method of study,” Qingdao: China Marine University, 2015.

[8] W. Q. Wang, D. D. Zhang, and Q. L. Huang, “Research and design of railway network and information security management system,” X.F.Chun. Railw. Comput. Appl. Beijing, vol. 11, pp. 40-43, 2017.

[9] L. Y. Zhang, “Dynamic risk fuzzy estimation method for information system development,” X.Li. Sys. Eng. Theory Practice. Beijing, vol. 21, pp. 88-92, 2001.