RAMID: A Novel Risk Assessment Model of Information Dissemination on Social Network

Hongzhou Sha[1,3], Xiaoqian Li*[2], Qingyun Liu[3], Zhou Zhou[3], Liang Zhang[2], and Lidong Wang[2]

[1] Beijing University of Posts and Telecommunications, Beijing, China
buptss@bupt.edu.cn
[2] National Computer Network Emergency Response Technical Team, Beijing, China
xiaoqianli@bjtu.edu.cn,wld@cert.org.cn,zl@isc.org.cn
[3] Institute of information engineering Chinese academy of sciences, Beijing, China
{liuqingyun,zhouzhou}@iie.ac.cn

Abstract. In recent years, a large number of social applications created new challenges to inhibit the spread of false information. And how to evaluate the threats of the false information dissemination remains one of the major concerns in the Internet security issues. Existing schemes focused on the operational safety of information systems and ignored the importance of assessment of false information dissemination. In this paper, we propose a novel method to evaluate the threat of false information dissemination. By analyzing social network application's structure and the information transmission mode, it proposed a risk assessment model for the false information dissemination. With this model, it is easy to evaluate and estimate the level of risks in social applications. Experiment verifies the effectiveness and correctness of this model in providing security recommendations and finding the most dangerous risk point.

Keywords: Network security, risk assessment model, analytic hierarchy process, social application

1 Introduction

In recent years, social applications have become one of the most important platforms for people to post and share information [1]. However, they also provide new ways for the transmission of false information [2], which has a widely impact in other fields, such as privacy protection [3], authentication [4], security assessment and data access control [5]. For instance, on April 24, 2013, the hacker stole the Twitter account of Associated Press and released false news which claim that the White House has suffered two bombing attacks and the U.S. President Obama was injured in the blast. Affected by the wide spread of the false information, the U.S., stocks fluctuate significantly while the Dow fell 140 points in two minutes. Therefore, it is an urgent task to quantify or estimate the risks of false information dissemination in social applications.

To address this issue, lots of traditional risk assessment methods [6] have been proposed. They work well for the traditional information systems. However, they cannot

* Corresponding author: xiaoqianli@bjtu.edu.cn

be applied for the social applications [7] because the introduction of social networking elements has a tremendous impact on the dissemination of false information. In fact, it is a new topic for the risk assessment of false information dissemination in social network application where little progress has been made.

In this paper, we propose a novel assessment model named by RAMID (Risk Assessment Model of Information Dissemination) in order to estimate the risks of social applications. More precisely, it first analyzes the security requirements caused by the dissemination of false information and compare it with other traditional threats. Then, it puts forward an assessment model of information dissemination for the social application, and finally gives out the corresponding quantitative calculation. In this way, it is easy for people to quantify the risks of information transmission and compare the risks between different network applications. Experimental results indicate the correctness and effectiveness of this evaluation method.

2 Related Work

The general network security assessment methods can be divided into two categories: artificial assessment and automatic evaluation. Artificial assessment usually carries out questionnaires, and depends on experts' advice. It is simple, effective, and has a wide range of assessment objectives. But, it is easy to introduce subjective factors, which may lead to a different result of the same application's evaluation by different people. Automatic methods evaluate the object by taking a method which automatically identifies vulnerabilities or attack. It is automatic, repeatable and easy to control, and it can be accepted by people much more easily compared to the manual evaluation. Therefore, there are many works based on the automatic evaluation method. For instance, Shen Zhiwei et al [8] analyzes the spread of false information, and gives out safety recommendations for different situations. But it did not make the analysis of actual network applications. Feng Deng et al [9] reviewed the assessment model, evaluation criteria, assessment methods and assessment tools in the area of information security assessment. But their risk evaluation is mainly based on the vulnerability scanning technology.

In summary, the traditional risk assessment methods [10] focused on the assessment of threats in the operating system. Thus, it usually takes the attacks and weaknesses log as its source of data. However, the threat introduced by false information dissemination differs from before [11]. And the traditional network security assessment in this aspect is neither universal nor feasible. In this paper, we propose a social application-oriented information dissemination risk assessment model, give the corresponding quantitative calculation method, and verify the correctness and effectiveness based on the analysis of real instance.

3 Risk Assessment of False Information Dissemination

Social network applications may generate different information from normal web applications. In this section, we start from the analysis of the security requirements for the threats of information dissemination, then discuss the social information dissemination model and finally the structure of the information transmission risk. A hierarchical risk

Table 1. Threats and Security Requirements

Threats	Security Requirement					
	Confidentiality	Integrity	Reliability	Audibility	Repudiation	Controllability
System Threat	√	√	√	√	√	√
Communication Threat	√	√	√	√	×	×
Application Threat	√	√	√	√	√	√
Performance Threat	×	×	√	√	×	×
Correctness of Design	√	×	√	√	×	×
False Information	×	×	×	√	√	√

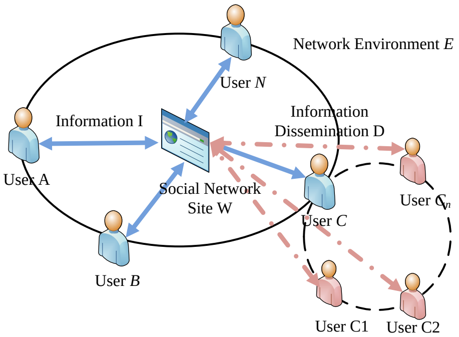

Fig. 1. The transmission mode of information of social network application

assessment model of false information dissemination is carried out by using of system decomposition technique. And people may evaluate the threats of false information dissemination faced by such application based on the risk items involved in the information dissemination process.

3.1 The Analysis of Security Requirements

People in different areas may have different requirements and emphases for the network system. Traditional network security risk assessment focused on the threat to the operation of software system [12]; while the threat introduced by false information dissemination is related to the trust [13]. The correspondence between the security requirements and threats is shown in Table 1. It is obvious that the risk assessment of false information dissemination has some special security needs. For example, its requirement for confidentiality, integrity and availability are not obvious, but it has a higher requirement for the reliability, controllability and non-repudiation.

3.2 Information Dissemination Model of Social Network

Figure 1 shows the information dissemination model of social network applications. In Figure 1, W represents social networking site which is the beginning or ending places for information dissemination; $A-N$ represents different user of social network application who is the provider and consumer of information; the C_1-C_n represents the user's followers are disseminators of and consumer of information; I represents the information which users publish; D represents the dissemination process; E represents the

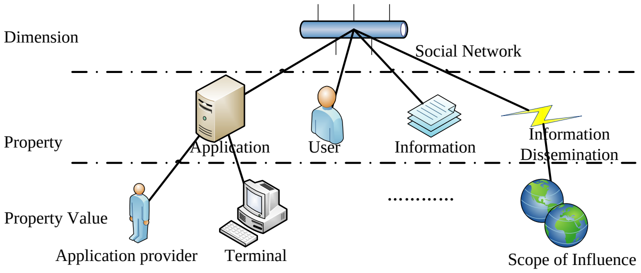

Fig. 2. The transmission mode of information of social network application

network environment which is the place where the dissemination process of information occurs.

Figure 1 indicates that in a network environment E, the elements of social applications include social application site W, users $U = A, B, \ldots, N$, information I and information dissemination D. In social applications, the dissemination process of false information is produced by the above four elements.

3.3 Risk Assessment Model of Information Dissemination

We first give out two related concepts before the introducing of the risk assessment model of information dissemination.

Definition 1 (Information Dissemination Risk). The likelihood of adverse effects on the Internet user due to the content the transmission of the information is called as information dissemination risk.

Definition 2 (Risk Network of False Information Dissemination). We define it as a relation network, which expresses the risks of false information dissemination based on the visit relationship. It is formally defined as $G = \{V, E\}$, where V represents the set of social network nodes, E represents a set of directed edges. $V = \{V_i | F, R\}$ where V_i is the i_{th} network node whose risk is described by F, R. F represents the functional value of V_i, which in other words means the losses suffered by losing node V_i. R represents the total risk of V_i. $R = \{R_i | G, W\}$ where G represents the possibility of spreading false information through vertex V_i. W represents the safety impact of vertex V_i. It is typically used in this way $R = G * W$[12]. Besides, $E = \{E_i | U_s, U_e, \rho\}$, where U_s represents the starting point of the edge, U_e represents the end of a directed edge, and ρ represents the probability of passing information risk.

On the basis of related definitions given above, the social network application is decomposed into three levels: dimension, property and property value. And Figure 2 proposes a hierarchical risk assessment model using system decomposition technique. The threats of false information dissemination for each social application can be evaluated based on the risk items involved in the information dissemination process. As shown in Figure 2, a top-down hierarchical order are dimension, property and property value.

In order to facilitate comparison and quantitative calculations, Table 2 shows the structure of the detailed evaluation model. Among them, the second and third indica-

Table 2. The Weight and Structure of the Risk Assessment Model RAMID

Dimension	Property	Weight	Property Value	Weight
Website	Application Provider	0.5	Types of Application Provider	1
	Access Terminal	0.5	Support Platform of Application	1
User	User Identity	0.7	User Authentication	0.5
			IP Address Hiding Technology Usage	0.5
	User Relationship	0.3	User Contact Tightness	1
Information	Information Relevance	0.3	Information Relevance Degree	1
	Information Audibility	0.7	Information Post Audibility	0.4
			Information Repost Audibility	0.3
			Comment Audibility	0.3
Dissemination Process	Transmission of Information	0.6	Information Access Method	0.4
			Direction of the Information Flow	0.3
			Communication Method	0.3
	Dissemination Effectiveness	0.4	Total Number of Users	0.5
			Number of Daily Active Users	0.5

tors characterize the impact of various elements on the spread of false information. They are from four dimensions that are social networking sites, users, information and information dissemination process. And Section 3.4 will further discuss the weights of each indicator.

3.4 Determining the weights of evaluation indicators

Weight is a magnitude which is used to evaluate the relative importance of various factors in a form of comparison. It reflects the influence degree of various factors to the assessment target. Let a judge object decompose into n judge factors: u_1,u_2,u_3,...,u_n. The relative weight of each assessment criteria for the evaluation object is: w_1,w_2,...,w_n, and they constitute the weight vector $W = \{w_1, w_2, \ldots, w_n\}^T$. The following two steps are adopted to determine the relative weights of several factors under a certain level by using pairwise comparison judgment matrix and consistency test method.

1) Construct pairwise comparison, judgment matrix of all levels. The decision maker compares each two factors, and establishes the judgment matrix: $A = a_{ij\,n*n}$, where a_{ij} denotes the relative importance of factor u_i and u_j.

2) Consistency check. Root method is used to calculate the relative weights. The elements of the matrix A is multiplied by row; calculate the n_{th} root of the result (the order of matrix A: n); and normalize the root vector into vector W; calculate the maximum eigenvalue of matrix $\lambda_{max} = \sum_{i=1}^{n} \frac{(Aw)_i}{nw_i}$, where $(Aw)_i$ represents the i_{th} element of Aw. Calculate the consistency index CI: $CI = \frac{\lambda_{max}-n}{n-1}$, where n is the order of the matrix A. Calculate the consistency ratio: $CR = \frac{CI}{RI}$ For $n = 1, 2, ..., 9$, Satty [14] gives out the value of RI. And the consistency of judgment matrix is acceptable when $CR < 0.10$, otherwise the matrix should be reviewed in order to be accepted. For example, the judgment matrix A of information Auditability is shown in Table 3. $\lambda_{max} = 3.0016, CI = 0.0008, CR = 0.0014 < 0.10$. The weights are rounded to be reserved with a decimal. And the weights of each evaluation index as shown in Table 2.

Table 3. Pairwise Comparison Judgement Matrix of Information Auditability

Information Audibility	Post	Repost	Comment	Weight
Post	1	4:3	4:3	0.4
Repost	3:4	1	9:08	0.312
Comment	3:4	8:09	1	0.288

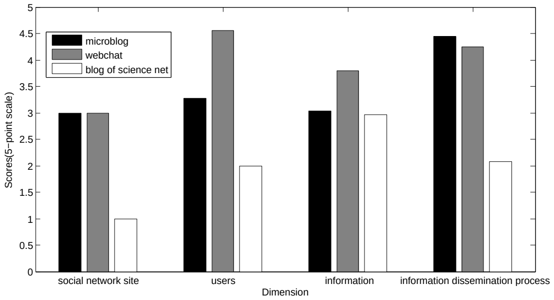

Fig. 3. The histogram of risk profile of typical applications

4 The Experiment of Risk Assessment

In order to verify the correctness of the risk assessment model, this section analyzes some typical social applications with the risk assessment model.

4.1 The evaluation and verification

Two typical social applications are selected in our experiment: 1) Sina Microblog; 2)Tencent Webchat. Both applications own some features such as convenience of message delivery, introduction of a new mode of interaction. And they have become the most widely used social network applications. The analysis of these two applications has great practical significance and certain representation. The risk profile among microbiology, webchat and traditional application (Web of Science blog) of each dimension are listed in Table 4. Among them, the scores of the user authentication are estimated by the calculation of 100 randomly selected users. In order to provide appropriate security suggestions, risks of the three applications are compared together in four dimensions as shown in Figure 3. The data source of Figure 3 includes the data in Table 4 and the weight given above.

As shown in Table 4 and Figure 3, compared to traditional applications, social applications has greater potential risk in the false information dissemination. The major causes of the risk are the rapid development of mobile terminal for social network applications, the significant increase of the number of anonymous users, the forwarding feature allows faster dissemination of information and so on.

Figure 3 presents the comparison of the scores of Microblog and Webchat. As it illustrates, Webchat creates more risks than Microblog in the dimension of users and information content, where the main risk comes from the user authentication and information auditability. And Microblog produce more risks than webchat in the dimension

Table 4. Risk Item Scores of Typical Application

	Risk Item Score		
Dimension	Sina Weibo	Tencent Webchat	Blog of Sciencenet
Type of Application	1	1	1
Support Platform of Application	5	5	1
User Authentication	2.4	3.8	2.1
Use of Hiding Techniques	1	1	1
Tightness Degree of User Contact	3	4	3
Information Relevance Degree	5	1	1
Information Post Audibility	1	5	5
Information Repost Audibility	3	5	1
Comment Audibility	3	5	5
Information Access Method	5	5	1
Direction of the Information Flow	5	5	5
Communication Method	3	3	3
Total Number of Users	5	5	1
Number of Daily Active Users	4	3	1

of information dissemination process, since Microblog is more likely to spread false information further with a large number of daily active users. Moreover, their risk scores are not far-off from the dimension of websites.

4.2 Comparison with Traditional Assessment Method

In this section, it illustrates the comparison with traditional assessment methods from the perspective of the evaluation effectiveness and safety recommendations.

Effectiveness of Assessment. In the evaluation process, the traditional methods usually consider the security threats of the system operation, and simply add the risk of different vulnerability together. Compared with traditional methods, this novel method focuses on the analysis of the threat in social applications introduced by false information dissemination. With full consideration of the impact of risk dissemination, it is more accurate than traditional methods. In addition, the visual representation of the assessment results avoids the loss of information caused by calculating risk by simple superposition method.

Safety Recommendations. In the field of risk assessment, the premise of developing safety recommendations is to figure out which vulnerability with the greatest impact[12]. In the aspect of comparison between different risks, traditional methods over-rely on experts' advice, which makes the risk of specific applications not comparable. In our model, with the introduction of some objective risk items, it is much more convenient for an evaluator to compare different applications, identify the most risky points, and further analyze the most dangerous risk point. It also provides reliable evidence to develop security recommendations. Therefore, it is better than the traditional assessment method.

5 Conclusion

In this paper, we present an evaluation method constitute by the evaluation model and three levels of evaluation indicators. In the future, we will further analyze the false information dissemination in social applications, and introduce more cases to improve this model.

Acknowledgment

This work was supported by The National Science and Technology Support Program (Grant No. 2012BAH46B02); the National Natural Science Foundation (Grant No. 61402464,61402474).

References

1. Yan, M.X.G.: Electric systems analysis (2004)
2. Li, Y., Liu, J.: Mechanism and improvement of direct anonymous attestation scheme [j]. Journal of Henan University (Natural Science) **37**(2) (2007) 195-197
3. Cohen, J.E.: Drm and privacy. Communications of the ACM **46**(4) (2003) 46-49
4. Das, M.L., Saxena, A., Gulati, V.P.: A dynamic id-based remote user authentication scheme. Consumer Electronics, IEEE Transactions on **50**(2) (2004) 629-631
5. Yu, S., Wang, C., Ren, K., Lou, W.: Achieving secure, scalable, and fine-grained data access control in cloud computing. In: INFOCOM, 2010 Proceedings IEEE, IEEE (2010) 1-9
6. Budak, C., Agrawal, D., El Abbadi, A.: Limiting the spread of misinformation in social networks. In: Proceedings of the 20th international conference on World wide web, ACM (2011) 665-674
7. Bass, T.: Intrusion detection systems and multisensor data fusion. Communications of the ACM **43**(4) (2000) 99-105
8. Shen, Z., Zhang, B., Li, F.: Research of internet governance based on harmful information propagation model. (2010)
9. Feng, D.g., Zhang, Y., Zhang, Y.q.: Survey of information security risk assessment. JOURNAL-CHINA INSTITUTE OF COMMUNICATIONS **25**(7) (2004) 10-18
10. Zhang, T., Hu, M.z., Yun, X.c., Zhang, Y.z.: Research on computer network security analysis model. JOURNAL-CHINA INSTITUTE OF COMMUNICATIONS **26**(12) (2005) 100
11. Joshi, J.B., Aref, W.G., Ghafoor, A., Spafford, E.H.: Security models for web-based applications. Communications of the ACM **44**(2) (2001) 38-44
12. Zhang, Y.Z., Fang, B.X., Chi, Y., Yun, X.C.: Risk propagation model for assessing network informationsystems. Journal of Software **18**(1) (2007) 137-145
13. Le, K., Jiwu, J., Yuewu, W.: The trust expansion and control in social network service. J Comput Res Dev **47**(9) (2010) 1611-1621
14. Saaty, T.L.: How to make a decision: the analytic hierarchy process. European journal of operational research **48**(1) (1990) 9-26