Network Security Situation Awareness using Exponential and Logarithmic Analysis

Tan Xiaobin
Department of Automation
USTC
Hefei, P.R.China
xbtan@ustc.edu.cn

Qin Guihong
Department of Automation
USTC
Hefei, P.R.China
qingh@mail.ustc.edu.cn

Zhang Yong
Department of Automation
USTC
Hefei, P.R.China
jzhang@mail.ustc.edu.cn

Liang Ping
Department of Automation
USTC
Hefei, P.R.China
liangp49@mail.ustc.edu.cn

Abstract

Network security situation awareness (NSSA) is a hotspot in the network security research field, based on the security situation values, decision makers can be aware of the actual security situation of their networks and then make rational decision to make their networks safer. In this paper, we build a multi-level quantization model for NSSA firstly: this model is comprised of three levels, namely, special oriented level, essential oriented level and holistic level. We can not only perform a certain kind of situation awareness, but also an overall one using this model. Different from the previous methods which compute network security situation of whole network just by summing up the values of each asset’s network security situation, we propose a novel algorithm based on exponential and logarithmic analysis, this novel method is more appropriate to obtain rational results. Our model and algorithm are proved to be feasible and effective through a series of experiments.

1. Introduction

Due to rapid development of the Internet, network scales and structures have become more and more complex and difficult to control, there come forth many kinds of threats aiming at hosts and network, such as worms, remote intrusions, distributed deny-of-service (DDoS), etc. To defend these threats, and make decisions on controlling the security situation of whole network, security situation awareness for it must be accomplished first.

The concept of situation awareness (SA) is derived from the research of human factors in aviation psychology[1]-[4], and then wildly used in military battlefield[5], nuclear-reactor control[6] and air traffic control (ATC)[7][8], etc.

Network situation awareness (NSA), which is derived from the air traffic control (ATC), is a new concept, and there are not many researchers devoting themselves to this field now. In 1999, Tim Bass proposed the concept of Network situation awareness[9], and then compared the network situation awareness with ATC, aiming at introducing the theory of ATC into network situation awareness (NSA).

In this paper, we focus on the network security situation awareness (NSSA), which gives more attention on security than network situation awareness (NSA). There are a series of models of NSSA, but most of them are framework without practical value and only give qualitative analysis of NSSA without precise mathematic model. Based on these models, we build a multi-level quantitative model of NSSA based on exponential and logarithmic analysis.

The remainder of this paper is organized as follows. Section 2 constructs a multi-level quantization model for NSSA. Section 3 proposes the algorithms for computing security situation of each level. In section 4 we make experiment to prove the rationality of our method. Finally, we give a general conclusion in section 5.

2. Multi-Level Quantization Model
2.1. The quantized description of network security situation

Various business and positions of decision-makers have various intention and understanding on network security situation, so subjectivity is a large part in NSSA. But a quantized description of network security situation awareness is important for all decision-makers, aiming at getting quantized and widely accepted description of it.

The evaluation criterion of information security is described detailedly in Information Assurance (IA) as information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation [10].

In [11], these five properties of information security are described as table 1.

<table>
<thead>
<tr>
<th>properties</th>
<th>explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>availability</td>
<td>The property of being accessible and usable upon demand</td>
</tr>
<tr>
<td>integrity</td>
<td>The property that data has not been altered or destroyed in an unauthorized manner</td>
</tr>
<tr>
<td>authentication</td>
<td>The provision of assurance of the claimed identity of an entity</td>
</tr>
<tr>
<td>non-repudiation</td>
<td>A service intended to protect against an entity's false denial of having participated in all or part of the communication</td>
</tr>
<tr>
<td>confidentiality</td>
<td>The property that information is not made available or disclosed to unauthorized individuals, entities, or processes (note: secrecy is a synonymous term)</td>
</tr>
</tbody>
</table>

In 2001, Applied Computer Security Associates (ANSA) and MITRE Corporation give the definition of information system’s security attribution quantification: value, selected from a partially ordered set by some assessment procedure, which represents as IS-related quality of some object of concern. It provides, or is used to create, a description, prediction, or comparison, with some degree of confidence [12]. Based on this definition, we can give quantized descriptions for our NSSA model. Each level of the model can be described by a vector, which can be limited into a range, the smaller of this value denotes the higher the security and the larger of it denotes the lower the security.

2.2. Establishment of model

Based on the former methods and our new algorithm, we establish a three-level model for NSSA, as be pictured in figure 1.

In our model, we adopt three properties of information security as the metrics of NSSA: availability, integrity, confidentiality, because these three properties are more common, and we can easily obtain related data of them. We call this level the essential oriented level. But these three properties in this level only describe the abstract aspects of NSSA, while for some departments or vocations they need an overall evaluation for a particular kind of threat, such as, malicious code, false configuration, vulnerabilities, network intrusion, etc. So we need to introduce the special oriented level to evaluate the specific threats and we call this level the special oriented level.

We think the essential oriented level and the special oriented level are not enough, because we need a simple result which can denote the security situation of whole network system, so we introduce the holistic level.

2.2.1. Data collection. The threats aiming at compromising the network include worm, Trojan, remote intrusion, distributed deny-of-service (DDoS), etc, so the data collection part of this model should include vulnerability scan system, malware detection system, intrusion detection system (IDS) and firewall, etc. The detection results collected by data collection
part is the basis of our model, they can be used to compute the special oriented level of NSSA.

2.2.2. Special oriented level. Special oriented level, which concerns the related information of all network security events, is founded for manufacturers of all security-related productions and other interested users. In this level we analyze the security situation from three angles, which are threat, asset and vulnerability. For each angle we count the number and distribution, etc. through statistic analysis, and then we get the description vectors.

2.2.3. Essential oriented level. Availability, integrity, and confidentiality compose the essential oriented level. The values of this level can be computed from the special oriented level, because the special oriented level description vector includes the corresponding values. This level is brought forward for various industries and other interested users who concern different aspects of the network security. For example, the confidentiality is most important for the government, but for entertainment industry, the availability is the most crucial thing.

2.2.4. Holistic level. NSSA is an auxiliary tool for decision-makers, who may not know well about security-related technology, so they need a simple and clear result. As we mentioned in previous section, for various business and positions of decision-makers, what they mainly concerned are different, so subjectivity is a large part in NSSA. To get more objective assessment results, in the process of computing the situation values in this level, we should concern about the different weight numbers for different users.

3. Algorithm of security situation for each level

3.1. Special oriented level

In this level, we adopt statistic analysis to compute the security situation value of threat, vulnerability, and asset. The calculation result is described in vector form.

3.2. Essential oriented level

There are a lot of algorithms computing network security situation of whole network by summing up the value of each asset’s network security situation. We believe that these methods are not appropriate to do it, let us think over an example:

There are two networks ready for assessment, denoted by A and B, if A has a asset whose security situation value are 5, and B has two assets whose security situation values are 3 and 4 respectively, if we consult security experts, there will no one who thinks network A is more security than network B, but using the methods we mentioned previous, we will get a positive answer.

To solve the problem, we propose a novel method based on exponential and logarithmic analysis. For example, we can compute the availability value ($S_{total}^A$) of whole network system using the following method.

$$S_{Asset}^A = \log_b \left( \sum_{t \in \text{threat}} \left( b^{t^A} \times b^{v^A} \times b^{a^A} \right) \right)$$ (1)

$$S_{total}^A = \log_b \left( \sum_{i \in \text{asset}} b^{S_i^A} \right)$$ (2)

Where: $S_{Asset}^A$ is the situation value on availability of a single asset: $A_t^T$ is the availability value of threat $t$; $A_v^V$ is the availability value of vulnerability $v$; $A_a^A$ is the availability value of asset $a$; $b$ is the base.

The security situation values of confidentiality and integrity can also be computed using this novel method.

3.3. Holistic level

To obtain more objective results, we firstly establish a weighted table for different points of view, which reflect the focus of different users, based on this weighted table, the value of the holistic level can be computed using the following method:

$$V_i^H = \sum_{i \in \{C,I,A\}} \alpha_i \times i$$ (3)

Where, C, I, A, denotes the values of confidentiality, integrity, and availability respectively; $\alpha_i$ denotes the weight number of C, I, A, which can be looked up from the weight table we create for users.

4. Experiment verification

We complete the experiment in our test bed. Figure 2 denotes the holistic security situation of the enterprise we evaluate.

The bar chart denotes the number of the assets we evaluate. The dotted line denotes the security situation of the most dangerous threat, and this is a feasible assessment method which selects the maximal situation as the holistic situation. The real line denotes the holistic security situation obtained using our
exponential and logarithmic analysis method. As can be seen from the figure, the dotted line and the real line have a little diversity in the former two times, and then coincide in the later three times. We also can see from the figure that, the assessment results using our method are limited between zero and twenty, while adopting the previous methods, the situation values span from zero to infinity, so our method is more readable.

The experiment result indicates our method is more rational and readable to implement assessment.

![Figure 2. Holistic security situation awareness](image)

5. Conclusions

Network security situation awareness (NSSA) is the perception, comprehension and forecast of the security situation for the network systems. To satisfy different users, in this paper we build a multi-level quantization model for NSSA, it employs three levels, namely, special oriented level, essential oriented level, and holistic level. Different from previous algorithms which compute network security situation of whole network by summing up the value of each asset's network security situation, we propose a novel method based on exponential and logarithmic analysis, which can give a rational result. This method is suitable for all kinds of users, and it can help users get quantized and objective results. The experiment results show the rationality and efficiency of our method.

Acknowledgment

This work is supported by the National 863 High-tech Program of China (No. 2006AA01Z449) and the 42nd National Science Foundation for Postdoctoral Scientists of China (No. 20070420738).

References


