Advanced Science and Technology Letters
Vol.31 (MulGraB 2013), pp.163-166
http://dx.doi.org/10.14257/astl.2013.31.36

Network Security Situation Assessment Ecurity Based on the Associated Diffusion Analysis

Xiangdong Cai[1,*],Fushuai Zhang[1],Yuran Wang[1],Yangjing yi[2]

[1] School of Automation, Harbin University of Science and Technology
150080 Harbin, PR China
[2] Harbin Engineering University
150001 Harbin, PR China
82380102@163.com,308595109@qq.com

Abstract. Aiming at the complex security situation, situation assessment through a comprehensive analysis of the conclusions drawn generalization to ease management staff awareness and response pressure. From the potential risks, dynamic threats, using the overlay method and clustering method to speculate attacks intended, identify coordinated attack and guiding automatic defense. This model adaptable well, and it's able to draw more precise conclusions credible assessment.

Keywords: network security; situation evaluation; correlation analysis; spread analysis; attack intention

1 Introduction

As the increasingly large, complex and heterogeneous network, security threats, tend to be diversified, in the face of a large number of different format, form the log and alarm of each different, the traditional safety assessment have been overwhelmed[1-3].

With time series analysis as the main line, accurate prediction is extremely difficult to achieve[4]. But the problem should not be ignored, this paper proposes a framework for evaluating model of intrusion detection and access control.

1.1 System and Concept

Figure 1 in concept describes the relationship between the safety factor. And we can use $A[1]$ method against $V[1]$, also can take $C[1]$ countermeasure to defense against attacks.

ISSN: 2287-1233 ASTL

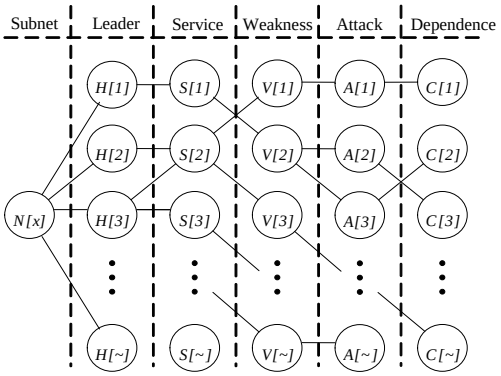

Fig. 1. Using multilevel hierarchy nomenclature expression from refers to specifically limited step by step, symbols are shaped like $X.Y$ refer to $X\,'sY$ members or attributes, in the other words, $X.Y$ attach to X or in the X defined namespace domain, and there is difference with individual Y .

1.2 Authorization and Rely On

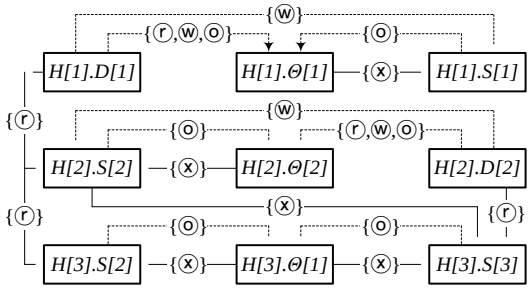

Fig. 2. This picture shows an example of environment, $D[i] \in D$ refer to the data, $S[i] \in S$ refer to general service specifically refer to the operating system. From the resource node refers to the dotted line arc single refers to the authorized user nodes, dot-dash line arc single refers to rely on, arc standard is set operation, the same start-stop, direction and arc mark dotted line and point crossed into solid line arc overlay welding .

$$\begin{aligned}&(\forall h)(h.O_D \times И_D \cup h.O_S \times И_S \subseteq \Gamma_{Sa\ R}\\&(h.\Theta) \wedge h.(S-\{\Theta\}) \subseteq \Psi_O(h.\Theta,ⓧ))\end{aligned} \tag{1}$$

Φ and Ψ only describe the dominant direct dependence , recessive indirect dependence or transfer rely on see later . Strict segmentation of dependencies should be able to form a directed acyclic graph, or illegal infinite recursion relies on, but no this requirement for authorization.

2 Main Propose

2.1 The Attack Position

In view of the s services, according to attack the point of discussion: (1) $s.u$ user attempts to steal passwords endanger $s.u$ set of permissions $\Gamma_{Ua\ R}(s.u)$. (2) $s.v$ weakness of the attempt to overcome endanger $s.v$ set of permissions $\Gamma_{Va\ R}(s.v)$ that can be exposed, and legal codes usually have execute permissions equivalent. Attack $\Theta.u$ or $\Theta.v$ can cause a collapse of the host.

(DoS/DDoS) denial of service attack, also known as the point of weakness, even though it may not be exposed to permissions, but the threat of attacks over the direct infringement of availability.

2.2 Risk Measure

Relying on the discrete-time model, the slot δ is the frequency of the measurement interval of attack, the attacker is defined as the number of contiguous window counting time slots even into $(t_i, t_i + (j-i)\times\delta]$, with the passage δ Change : (1) Adjust the current time. (2) If δ has a new attack occurs, the starting time of t_i unchanged otherwise be adjusted to $t_i \leftarrow t_i + \delta$.

3 Experimental Analysis

Table 1. Attack and response parameters

	Launch time	Fall time	Response time	Attack equivalent	Attack counting sequence
$a1$	0	5	8	0.24	(7,3,0,2,4)
$a2$	0	6	9	1.20	(1,3,0,2,0,1)
$a3$	0	0	11	0.01	—
$a4$	0	6	11	0.35	(5,3,1,0,4,2)

Table 1 lists the simulation parameters related to four attacks, defense and repair response includes two areas, covering more value due to breakdown and are not listed. Front-end system detects an attack, self-starting distributed infringement monitor, repair, infestation can be manually stopped.

4 Conclusion

This paper reviews the research situation, analyzes the flaws exposed. Expounded the security elements, authorization relations and dependencies, discusses the attack position, risk measure, superposition algorithm and the right to harm conversion. Then propose a vector-based evaluation algorithm, from three levels assess posture. The model to eliminate or weaken the defects previously summarized, with good size scalability, can more truly reflect the security posture.

References

1. Wang Juan, Zhang Fengli, Fu Chong, *et al*. Study on index system in network situation awareness [J]. Computer Applications, 2007, 27(8):1907-1909 (in Chinese)
2. Xiao Haidong. Analysis of security situational awareness of cyberspace [D]. Shanghai: School of Electronics and Electric Engineering, Shanghai Jiao Tong University, 2007
3. Wei Yong, Lian Yifeng, Feng Dengguo. A network security situational awareness model based on information fusion [J]. Journal of Computer Research and Development, 2009, 46(3):353-362 (in Chinese)
4. Zhang Yongzheng, Fang Binxing, Chi Yue, *et al*. Risk propagation model for assessing network information systems [J]. Journal of Software, 2007, 18(1):137-145 (in Chinese)

