An Immune-Based Model for Service Survivability

Jinquan Zeng, Xiaojie Liu, Tao Li, Feixian Sun, Lingxi Peng, and Caiming Liu

Department of Computer Science, Sichuan University, Chengdu 610065, China
liuxiaojie@cs.scu.edu.cn, zengjq@371.net

Abstract. In order to enhance service survivability, an immune-based model for service survivability, referred to as ISSM, is presented. In the model, the concepts and formal definitions of self, nonself, immunocyte, diversity system, and etc., are given; the antibody concentration and the dynamic change process of host status are described. Building on the relationship between the antibody concentration and the state of an illness in the human immune system, the systemic service capability and the service risk are calculated quantitatively. Based on the differences of the immune system among individuals, a service survivability algorithm, dynamic service migration algorithm, is put forth. Simulation results show that the model is real-time and adaptive, thus providing an effective solution for service survivability.

Keywords: artificial immune system, service survivability, risk evaluation.

1 Introduction

In the long course of human being fighting against antigens, a unique defense system is formed in our body to safeguard us [1]. In the human immune system, the first defense is the skin, saliva, sweat, and etc., which obstruct antigens from intrusion. The second is phagocytes or macrophages that surveil and kill them once antigens invade. In spite of the two kinds of defenses, some antigens still can break through and invade our body. Then the last defense, Adaptive Immune System, plays a vital role in the human immune system. Through the adaptive immune response, the system can adaptively recognize antigens and protect our body. Meanwhile, each individual has different immune system. The virus or bacteria causing one ill does not necessarily do the same to another. It is just the differences that enable some of us to survive some severe illnesses (e.g. plague) and enhance survivability of the whole human being.

Amazingly similar to the human immune system, the development of the network security technology mainly witnesses the three phases. The first phase studies how to prevent intrusion, such as firewall, encryption, and etc. The second phase studies how to detect intrusion involving intrusion detection, integrality verification, and etc. As not all unknown attacks are predictable and not all security holes are prohibited, some attacks will succeed in intrusion. So it is necessary to study how the system, after attacked, can fulfill its services while ‘being sick’. The study of the third phase

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301, pp. 354–363, 2006.
© Springer-Verlag Berlin Heidelberg 2006

emphasizes the system's capability in fulfilling essential services in the present of attacks, failures, or accidents, which is a new direction of network security technology development.

Currently, the studies of survivability mainly include the definition [2], requirement analysis method [3], the design model [4], and etc. Westmark summarized the studies of network survivability and finds that most studies focus on the definition and significance of survivability, but the realizable method is little studied [5]. Zhang et al. gave a realizable method, emergency algorithm [6], which is only a simply idea without concrete realization. Chen et al. gave a model based mobile agent for service survivability by delivering essential services [15], but which lacks risk evaluation and active response strategies. Real-time risk evaluation and response are vital in the survivability system, where the system can actively adjust its defense strategies to fulfill essential services and decrease damages. However, most current methods of risk evaluation lack real time [9] and adaptability [10], and can not evaluate service risk [11].

The paper proposes a realizable model for service survivability, called ISSM. According to the relationship in the human immune system between the antibody concentration and the state of an illness, the 'health status' and service capability are evaluated real-timely by calculating the antibody concentration, and based on the differences of the immune system among individuals, an active-defense method, dynamic service migration algorithm, is presented. Fast migration and different defense capabilities in the diversity system hope to transfer attacking target in real time to reduce attacking damages and fulfill essential services.

The rest of the paper is organized as follows. In Section 2, we establish an immune-based model for service survivability. In Section 3, simulations and experimental results are provided. Finally, Section 4 contains our summary and conclusions.

2 Model Theories

2.1 Lifecycle Model

Compared to the conventional network security technology, survivability emphasizes the system's capability in fulfilling essential services while 'being sick'. Every one suffers illness at times, and he can keep working when it is not serious. If it is too serious to fulfill his work, then he needs treatment to recover and his job will be transferred to another healthy person to do. This process is a cycle: healthy, ill, treated, recovered.

Similarly, the information system also confronts various attacks. Fig. 1 shows the lifecycle of the system status. If a serving host suffers attacks, when the risk reaches a certain degree, the host will send the alarm signal and transform into the alarm status. If the attacks lessens or the host resumes to the normal status through self-adjustment, then the alarm will be removed, but if the host suffers the continuous attacks at the