SURVIVABILITY ASSESSMENT: MODELING A RECOVERY PROCESS

Irving Vitra Paputungan[1], Azween Abdullah[2]
IT Department
[1]Islamic University of Indonesia, Yogyakarta, Indonesia
[2]Technology University of Petronas, Malaysia
e-mail: [1]ipink@engineer.com, [2]azweenabdullah@petronas.com.my

ABSTRACT

Survivability is the ability of a system to continue operating, in a timely manner, in the presence of attacks, failures, or accidents. Recovery in survivability is a process of a system to heal or recover from damage as early as possible to fulfill its mission as condition permit. In this paper, we show a preliminary recovery model to enhance the system survivability. The model focuses on how we preserve the system and resumes its critical service under attacks as soon as possible.

Keywords: *survivability, recovery, critical service*

1. INTRODUCTION

Our society is becoming more dependent on Information Systems. An important part of our society is dependant on large sets of systems that electronically hold the information needed to provide essential services. Our information is held by databases in insurance companies, in companies we have worked for, in medical systems, financial infrastructure, manufacturing, telecommunications, education, transportation etc. Most of this information is accessible through public communication channels, such as the Internet, the unbounded network [12].

Unbounded networks have no central administrative control and no unified security policy. Furthermore, the number and nature of the nodes connected to such networks cannot be fully known. Despite the best effort of security practitioners, no amount of system hardening can assure that a system that is connected to an unbounded network will be invulnerable to attack [1]. We know that, now, malicious attacks (actions and software or hardware) are becoming more attractive and feasible Corporate and nation-state espionage, electronic terrorism, information warfare, loss of privacy, and identity theft, are examples of the inherent dangers associated with the creation of such system of systems [12].

Traditional security does not generally address these problems (i.e. interdependence, lack of control, untrustworthiness, among others) of highly distributed systems [1]. Traditional security technologies were not designed to protect systems against the evolving threats that result from the interconnection of systems that were not designed to be interconnected in the first place. These systems typically employ a hierarchical design approach, appropriate for systems with centralized administration and coordination. But it cannot provide a survivable solution in the context of unbounded systems [12].

In this paper, we show our preliminary model of a simple survivable system by recovering the destroyed service. It is a first step of our research in specifying system survivability from recovery perspective.

The rest of this paper is organized by follows. In Section 2, we describe the definition of survivability, the properties of survivable system and the focus of this research. Next, in section 3 we explore some related works in survivability by some researchers and conclude the problem among them. How we approach the problem is shown in section 4. Last, section 5, we give some discussions and the future works of this research.

2. SURVIVABILITY

2.1 Definition of Survivability

The definition for survivability was not always consistent or even present in the current literature discussing survivability. We use the standard definition [1] as our basis to explain what survivability is. Survivability is the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.

The term s*ystem* is used typically in a large-scale network system that includes many components (nodes) that are required to deliver services to the end user. The system environment and the essential services that the system provides are defined for this survivable network system. State whether the system is bounded or unbounded. The system is unbounded if all nodes that provide the essential services are not known.

Mission refers to a set of very high-level requirements or goals. It is not limited to military settings; any successful organization or project must have a vision of its objectives, whether they are expressed implicitly or a formal mission statement. Mission can be judged by the expectations of the user [4]. Mission is related to critical services that system provides. For example, check clearing is a critical service of a banking system; it means the mission of a survivable banking system is to continue providing this service despite the presence of faults.

Timeliness is a critical factor that is typically included in the very high-level requirements that define a mission. For example: for a networked distributed system, a required service may be a specified response time to the end user. For a time-critical system, the description of a required service may include the maximum time allowable between user request and system response.

The terms *attack, failure,* and *accident* can be considered as threats. It is something that may prevent the system from providing services to the user in the prescribed amount of time or may prevent the system from providing the services at all. Threat categories include: 1) Accidental threats: software errors, hardware errors, and human errors, 2) Intentional or malicious threats: sabotage, intrusion, or terrorist attacks, and 3) Catastrophic threats typically do not allow delivery of required service to the user, which includes acts of nature (thunderstorms, hurricanes, lightning, flood, earthquake, etc.), acts of war, and power failures.

We can add one template for survivability definition, business case [4]. A business case is required for each survivability definition. The rationale provides the business case for the definition of survivability. There is an extra cost associated with the design, development, and operation of a survivable system. The business case is developed based on the cost/benefit analysis from which the threat is identified and required responses are specified. Note: A separate cost/benefit analysis is required for each level of threat. A non-malicious virus may degrade system performance but not shut the system down. If the degraded performance is within the defined minimum level of service, no action may be required with respect to survivability.

To compare the concept of survivability with the traditional security, we would say that the survivability focus on different properties of a system than security. In security, it is protection oriented, which means, that people trying to protect their information, machine, or physical property trough security. As survivability, it is mission oriented, which means that people are trying to get their job done in time no matter what happens to the system.

2.2 Properties of Survivability

A key characteristic of survivable systems is their capability to deliver essential services in the face of attack, failure or accident. To maintain that capability, survivable systems have ‘3R’ [1], [5], [11]: Resistance, Recognition and Recovery, and Adaptation as its four properties.

Resistance describes strategies how to prevent our system from possible damage. A survivable system should resist attacks, accidents, or failure. System and user authentication, access control mechanism, encryption technologies, firewall, dispersion of data, strong configuration management can be used for this purpose.

Recognition describes how to detect damage (by attacks etc.) and understand the current state of the system, including evaluating the extent of damage. Every layer of computational infrastructure must be monitored, and detection responses will be correlated to obtain a better understanding of the threat environment. Log analyses program, intrusion detection system, virus scan, internal integrity checking, auditing can be used for this purpose.

Recovery means how to maintain or restore the essential or critical service from damage as early as possible to fulfill its mission as condition permit. Recovery depends on the severity of the damage (i.e. how many resources have been affected), recovery strategies and remaining undamaged resources that are in place. There are some strategies such redundancy, data replication, and system backup and restoration.

Adaptation in survivability means improving system based on knowledge gained form intrusions to reduce effectiveness of future attack. It can be an incorporation of new pattern for intrusion recognition or adaptive logging and filtering. Perhaps, this property is the hardest part, because the system needs to resist a never-before-seen attack or intrusions.

We use the terms recovery as our focus on this work. As long as system can detects attacks or faults and configure resources reasonably in structure and reconfigure resources under attack, and ultimately keep the critical services running all along to support the mission, the system will survive. Hence, we must consider how to recover the system after attacks or faults to improve system survivability by creating a technique [6] [3] [7].

3. RELATED WORKS

There has been considerable work done on survivability. Fisher found a new method, emergent algorithm, and a language, EASEL (Emergent Algorithm Simulation Environment Language), for enhancing survivability in an unbounded network [13] and Christie used EASEL to analysis network survivability [8]. Moitra et al. proposed a complete episodes simulation model for managing Survivability of networked Information System, including the responses of the system to attacks [6]. The author said that the return of the system to the normal state when incident occurs should be relaxed in the future. Jha et al. uses a Constrained Markov Decision Process (CMDP) to form the basis of survivability analysis, which is composed of reliability, latency, and cost-benefit [2]. The author described each node in networked system using finite state machine, and utilized model checking, Bayesian analysis, probabilistic system and other mathematics method for qualitative and quantitative analysis. Similar as [2], Koroma et al. proposed a quantitative approach using a generalized model (Markov chain) to achieve how the system will function in the wake of failures, what will be the impact of failures on the user, and how to overcome these failures [9]. Krings et al. proposed a conversion idea of question space, which converts the analysis of system survivability info a framework of solving some typical question of graph [10]. Lin et al. provided a framework for quantifying the '3R' of survivability [11]. Zhao et al. proposes a novel quantitative analysis method based on grey relational analysis to analysis the actual network survivability [7]. Unfortunately, all of those works did not consider about system's recovery as part of survivability, how the system recover from faults.

Park et al. proposed a hybrid survivability model by identifying the static and dynamic survivability model [5]. It compares the benefits and limitations of each in terms of simplicity, resource efficiency, adaptation, service downtime, immunization, and robustness.

Wang et al. developed ERAS (Emergent Response Algorithm for Survivability of Critical services) to recover the system's critical service after destroyed, including how to find the feasible scheme of reconfiguration as soon as possible [3]. It shows that non-critical service resources can be distributed to critical service resources. It is not only a new thought and method for survivability, but also has the feather of scientific and reliable, practical, and simple.

According to some related works above, we want to create a set of recovery model to analysis network survivability. We study on how to recover the system's capability and critical services that affect the mission after fault services. By that model, we will consider survivability from the needed resources. Once the resources that critical services use are destroyed, system has adaptive abilities to redistribute resources belonging to non-critical services to critical services.

4. APPROACH

In order to achieve the goals of this research, we first propose a model to recover the system under faults by adopting the concept from both [3] and [5]. Assumed that the fault has already occurred and the critical service to fulfill the mission has destroyed, the critical service could be more than one service. Then, we create a model which can diagnose and analyze the recovery actions to improve the system survivability based on needed resources. The model includes resource allocation which is redistributed resources dynamically to the critical services, where the mission is wanted to fulfill, aiming at keep critical services running consistently. The abstract architecture of the system is shown in **Figure 1**.

Once the fault happens in the critical services resources and detected by monitoring process, performed by another process in the system (such as fault detection system), the recovery engine triggered. The engine will start with diagnosing the resources that a certain critical service uses are destroyed. This will assess the resources of non-critical service afterwards. Next, the engine will analyze the non-critical service resources to be chosen in order to sustain the critical service running. The allocation will be the last process of the engine. It allocates the resources of non-critical service to critical service as soon as possible.

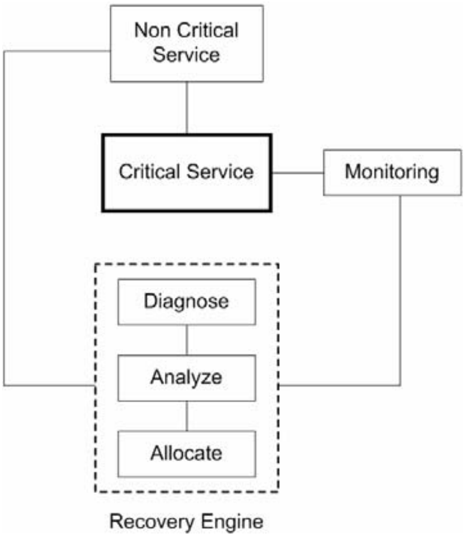

Figure 1. The abstract architecture of the recovery engine

The recovery engine will find out the feasible resource reconfiguration scheme, after diagnose and analyze the incident, from non-critical services to ensure sustainable operation of critical services. While this process running, the system will enter the graceful degradation state, means it is not totally stop functioning, but still working with less resource.

5. DISCUSSION AND FUTURE WORK

The research on survivability has become an interesting topic in the fields of security, and one of its emphases is how to improve the abilities of emergency response and damage recovery.

In this paper, we presented our preliminary attempts at defining a model to recover a critical service of system and our plan to use this model is to create a simple basis Decision Support System to manage survivability. We wish to set up a model to analyze system's survivability based on recovery process.

There are several tasks ahead. Foremost of all, we have yet to find the sets of mathematical model to specify the recovery mechanism. Other problems also arise due to the scale of information infrastructures. We are looking for some specific and small real infrastructure that our model will be applied for practical. It will be the first step of our research before we apply it on the bigger infrastructure.

REFERENCES

[1] R. Ellison, D. Fisher, R. Linger and etc, “Survivable network systems: An emerging discipline”. *Technical Report*, CMU/SEI-97-153, 1997. Revised 1999

[2] Jha S, Wing M, “Survivability Analysis of Networked Systems”, *ICSE 2001*, Toronto, 2001.

[3] J. Wang, H. Wang, G. Zhao, “ERAS – an Emergence Response Algorithm for Survivability of Critical Services”, IMSCCS 2006, IEEE, 2006.

[4] R. Westmark, “A Definition for Information System Survivability”, *Proceeding of the 37th Hawaii Internal Conference on Systems Sciences (HICSS'04)*, IEEE, 2004.

[5] J. Park, P. Chandramohan, “Static vs. Dinamic Recovery Models for Survivable Distributed Systems”, *Proceeding of the 37th Hawaii Internal Conference on Systems Sciences (HICSS'04)*, IEEE, 2004.

[6] S.D. Moitra, S.L. Konda, “A Simulation Model for Managing Survivability of Networked Information System”, *Technical Report,* CMU/SEI-2000-TR-020, 2000.

[7] G. Zhao, H. Wang, J.Wang, “A Novel Quantitative Analysis method for Network Survivability”, *IMSCCS 2006*, IEEE, 2006.

[8] A.M. Christie, “Network Survivability Analysis Using Easel”, *Technical Report*, CMU/SEI-2002-TR- 039, 2002.

[9] J. Koroma, W. Lei, D. Kazakos, “A Generalized Model for Network Survivability”, *TAPIA 2003*, ACM, Atalanta, 2003.

[10] A.W. Krings, M.H. Azadmanesh, “A Graph Based Model for Survivability Analysis”. *Technical Report*, UI-CS-TR-02-024, 2004.

[11] X. Lin, M. Zhu, R. Xu, “A Framework for Quantifying Information System Survivability”, *ICITA 2005*, IEEE, 2005.

[12] J. Caldera, “Survivability Requirements for U.S. health care Industry”, Carnegie Mellon University, 2000.

[13] D.A. Fisher, “Design and Implementation of EASEL – A Language for Simulating Highly Distributed Systems”, CMU/SEI, 1999.