

Survivable network systems: An overview

M. Keshtgary A. H. Jahangir

Department of Computer Engineering Department of Computer Engineering
P.O. Box 11365-9517 P.O. Box 11365-9517
Sharif University of Technology Sharif University of Technology
Azadi Ave., Tehran, Iran Azadi Ave., Tehran, Iran
Phone: 98-21-6005616 Phone: 98-21-6005616
Fax: 98-21-6012983 Fax: 98-21-6012983
keshtgar@mehr.sharif.ac.ir ijahangir@sharif.ac.ir

Abstract

Society is growing increasingly dependent upon large -scale, highly distributed systems that operate in unbounded network environments such as the Internet with 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 efforts of security practitioners, no amount of hardening can assure that a system that is connected to an unbounded network will be invulnerable to attack and intrusion. The discipline of survivability can help ensure that such systems can deliver essential services and maintain essential properties such as integrity, confidentiality, and performance, despite the presence of intrusions. Unlike traditional security measures, which require central control and administration, survivability is intended to address unbounded network environments. Here we describe the survivability concepts and also its relation and distinction with dependability, fault tolerance and security.

1 Introduction

Survivability is a fairly new discipline, and viewed by many as distinct from the traditional areas of security and fault-tolerance. It is defined as the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents. We use the term system in the broadest possible sense, including networks and large-scale systems of systems. The term mission refers to a set of very high-level requirements or goals. Missions are not limited to military settings, because any successful organization or project must have a vision of its objectives whether expressed implicitly or as a formal mission statement. The best example of implemented survivability research is combat aircraft that can still fly despite extensive underlying system damage.

Timeliness is a critical factor that is typically included in (or implied by) the very high-level requirements that define a mission. However, timeliness is such an important factor that is included explicitly in the definition of survivability.

The terms attack, failure, and accident are meant to include all potentially damaging events. Failures and accidents are included in the definition of survivability. Failures are potentially damaging events caused by deficiencies in the system or in an external element on which the system depends. Failures may be due to software design errors, hardware degradation, human errors, or corrupted data. The term accidents comprise a broad range of randomly occurring and potentially damaging events such as natural disasters. We tend to think of accidents as externally generated events (i.e., outside the system) and failures as internally generated events.

It is also important to recognize that it is the mission fulfillment that must survive, not any particular subsystem or system component. Central to the notion of survivability is the capability of a system to fulfill its mission, even if significant portions of the system are damaged or destroyed. We use the term survivable system as shorthand for a system with the capability to fulfill a specified mission in the face of attacks, failures, or accidents. Again, it is the mission, not a particular portion of the system that must survive.

On [12] and [2], survivability concepts and characteristics are presented. A formal definition of survivability is presented in [6] and related it to the field of dependability and the technology of fault tolerance. They claimed that the specialized requirements of critical information systems require a new facet of dependability and that the survivability as they have defined it is different from reliability, availability, safety, and so on. To illustrate the formal definition of survivability, they present an example based on a hypothetical financial payments system. They summarize the environment for the example by assuming that all of the expected elements are defined and that the identified hazards include: major hardware disruption in which communications server machines become non-operational; coordinated security attacks in which multiple commercial bank regional processing centers are penetrated; and regional power failure in which either many banks are disabled.

Defining essential and non-essential services are the requirements of survivable network systems [1]. In this paper, authors define the survivability, three phases of intrusion (penetration, exploration and exploitation) and five principles for survivable system development and testing practices:

1. precise specification of required functions in all possible circumstances of use
2. correctness verification of implementations with respect to function specifications
3. specification of function usage in all possible circumstances of use, including intruder usage
4. testing and certification based on function usage and statistical methods
5. establishment of permanent readiness teams for system monitoring, adaptation, and evolution

Two master thesis [9], [10] in Carnegie Mellon University Pittsburgh, Pennsylvania are done on two different cases: the U.S. Health Care Industry and the U.S. Electric Power Industry. They show that traditional computer security is not adequate to protect the mission-critical requirements and that a survivability approach is required.

Survivability of a network that nodes have different physical layer and network layer are discussed in [3]. They address the issue of survivability due to physical attacks that destroy links and nodes. Their goals are: 1-Development of network design models/algorithms to provide a quality of service (QoS) specified under any failure condition. 2-Development of network management algorithms, which make optimum use of network resources after a failure. 3-Studying the transient network congestion that occurs after a failure and its effect in the design of the network and the traffic restoration algorithms. A new simulation Tool (MOMARS) has been developed to study a link failure for multi-layered network. In next sections we describe survivability relation and distinction with dependability, fault tolerant and security.

2 Relating Survivability and Dependability

From the perspective of the dependability framework, survivability is dependability in the presence of active faults. Dependability and survivability are actually very close to each other [13], especially when looking at the three R's, resistance, recovery, and restoration. Dependability focuses on random faults but survivability focuses on coordinated attacks by intelligent adversaries. Clearly dependability and survivability both go beyond the traditional approaches, based on fault avoidance, and have recognized the necessity of fault tolerance.

3 Survivability and Fault Tolerance

The basic goal of fault tolerance and survivability are essentially the same [14]. One main goal of fault-tolerant system design is to mask hardware faults, such that a failure of a component does not affect the ability of the system to perform to its specifications. So many solutions found in fault-tolerant system designs are suitable for adaptation in order to increase survivability. Examples of such solutions are the introduction of time and information redundancy as well as spaced redundancy. However, in fault-tolerant systems, malicious faults are the least likely, in network security/survivability the attacker is expected to behave maliciously. One large class of fault-tolerant techniques uses a set of redundant components to determine the "correct" information; examples are TMR and N-version programming. Such a technique implicitly assumes that some distinguished element of the power set of the redundant components are trustworthy and a majority of components will function correctly. In the presence of an attack and induction of deliberate faults in these components, this assumption fails.

Survivability is a dependability property; it is not synonymous with fault tolerance. Fault tolerance is a mechanism that can be used to achieve certain dependability properties. In terms of dependability, it makes sense to refer to a system as reliable, available, secure, safe, survivable and so on, or some combination using the appropriate definition(s). Describing a system as fault-tolerant is really a statement about the system's design, not its dependability. While fault tolerance is a mechanism by which some facets of dependability might be achieved, it is not the only mechanism. Other techniques, such as fault avoidance, can be used also. Thus, for example, by careful component selection it might be possible to reduce the rate of hardware failures in a given system to an negligible level, and by suitably restricting system access it might be possible to eliminate certain types of security attacks. In similar ways, fault elimination and fault forecasting can be used as mechanisms to improve a system's dependability.

4 Survivability and Security

Security attacks are a major concern for critical information systems, and in some discussions, survivability is viewed as synonymous with secure operation. Yet experience to date is that most significant service failures of critical information systems have been caused by things like erroneous software upgrades, operator mistakes, common-mode software faults, and not by security attacks. The damage that can result from a security attack can, of course, be tremendous but this is true with other types of faults also. This is not making these security less important, clearly security attacks (i.e., deliberate faults) are a serious concern. What matters, however, is to address all anticipated types of faults including deliberate faults since it is the maintenance of customer value that we seek in survivability.

A survivable system is expected to continue to provide one of the forms of tolerable service after many different forms of damage have occurred. The anticipated faults for a given system frequently will include various types of malicious faults as well as all the other types, and so in developing the survivability specification and the associated system design, it is essential that a comprehensive approach be followed. A system that is secure yet is unavailable excessively because of hardware failures is not survivable.

Security is impacted by some aspects of design for dependability since the introduction of redundancy makes protection of a system from deliberate faults more difficult. For example, replication of data so as to provide a means of tolerating certain faults provides multiple opportunities for malicious data access.

Current security approaches to protect information systems have focused on preventing attacks from being successful by hardening defenses with authentication, encryption, and a variety of layered-violating network devices (i.e., firewalls, network address translators, intrusion detection systems) [15]. What is not being captured is the survivability of an entire system to failures or attack. While security approaches may protect one layer of a network system they often introduce vulnerabilities in other layers. There are many examples: authentication schemes that introduce a single-point-of-failure (certificate authority). There is a research group called Survivability-Over-Security (SOS) [15] that their goal is to increase the survivability of information systems using innovative techniques which simultaneously reduce network vulnerabilities and increase restoration flexibility. While security is one technique to protect system components, they feel that survivability is a higher goal over security since survivability encompasses the functionality of an entire information system and not individual components.

5 Conclusions

Survivability is a new approach to the design and protection of the systems. A survivable system fulfills its mission, in a timely manner, in the presence of attacks, failures, or accidents. Here we described the survivability concepts and discussed its relation and distinction with dependability, fault tolerance and security.

REFERENCES

- [1] Linger, R.C., Mead N.R, and Lipson H.F., "Requirement Definition for survivable Network Systems", Carnegie Mellon University., Proceedings of the 1998 International Conference on Requirements Engineering (ICRE'98)
- [2] Mead, N.R., Elison, R.J., Linger, R.C., Longstaff T., McHugh, J., "Survivable Network Analysis Method", CMU/SEI - 2000-TR-013 ESC-TR-2000-013 September 2000
- [3] Medhi D. and Tipper, D., "Multi-Layered Network Survivability -- Models, Analysis, Architecture, Framework and Implementation and Overview", to appear Proceedings of DARPA Information Survivability Conference and Exposition, Hilton Head, SC, Jan. 25-27, 2000
- [4] Jha, S., wing, J., Linger, R., and Longstaff, T., "Survivability Analysis of Network Specification", Proceedings of the International Conference on Dependable Systems and Networks, Workshop on Dependability Despite Malicious Faults, New York City, NY, June 25-28, 2000. 2000 IEEE
- [5] Felekis, A. and Milis D., "Emerging Technologies for Fiber Network Survivability" http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol4/af5/report.html
- [6] Knight, J.C. and Sullivan, K.G., "On the Definition of Survivability", University of Virginia, Department of Computer Science, Technical Report CS -TR-33-00
- [7] Lipson, H.F., Presentation: "Survivability - A New Security Paradigm for Protecting Highly Distributed Mission Critical Systems". 38th Meeting of IFIP Working Group 10.4 on Dependable Computing and Fault Tolerance. Kerhonkson, NY, June 28-July 2, 2000
- [8] Lipson, H.F. and Fisher, D.A., "Survivability - A New Technical and Business Perspective on Security", Proceedings of the 1999 New Security Paradigms Workshop. Caledon Hill, ON, September 21-24, 1999. New York, NY
- [9] Caldera, J., "Survivability Requirements for the U.S. Healthcare Industry", master thesis, Carnegie Mellon University Pittsburgh, Pennsylvania, May 2000
- [10] Byon, I., "Survivability of the U.S. Electric Power Industry", master thesis, Carnegie Mellon University Pittsburgh, Pennsylvania
- [11] Elison, R.J., Fisher, D.A., Linger, R.C., Lipson, H.F., Longstaff T.A. and Mead N.R., "An Approach to Survivable Systems", <http://site02.mirror.edu.cn/easel/nato1.doc>
- [12] Mead, N.R., Elison, R.J., Linger, R.C., Longstaff T., McHugh, J., "Definition of Survivability", <http://www.sei.cmu.edu/publications/documents/00.reports/00tr013/00tr013chap02.html>
- [13] Avizienis, A., Laprie, J. C., Randell, B., "Fundamental Concepts of Dependability", ISW-2000, www.cert.org/research/isw/isw2000/papers/table_of_contents.html
- [14] Krings, A., Harrison, S., Dickinson, J., Mequeen, M., "Survivability of Computers and Networks Based on Attack", ISW-2000, www.cert.org/research/isw/isw2000/papers/table_of_contents.html
- [15] Yurick, W., Doss, D., Kruse, H., "Survivability-Over-Security: Providing Whole System Assurance", ISW - 2000, www.cert.org/research/isw/isw2000/papers/table_of_contents.html
- [16] Bishop, M., "Information Survivability, Security and Fault Tolerance", ISW -1997, <http://seclab.cs.ucdavis.edu/projects/vulnerabilities/scriv/1997-isw.pdf>