Title:
What Are Survivable Computer Systems

Word Count:
1221

Summary:
An article about survivable computer systems, high availability, fault tolerance, and events such as attacks, accidents, and failures that can cause computer systems to fail

Keywords:
Survivable Computer Systems, Business Continuity, Disaster Recovery, Fault Tolerance, High Availability

Article Body:
Definition Of A Survivable Computer System

A computer system, which may be made up of multiple individual systems and components, designed to provide mission critical services must be able to perform in a consistent and timely manner under various operating conditions. It must be able to meet its goals and objectives whether it is in a state of normal operation or under some sort of stress or in a hostile environment. A discussion on survivable computer systems can be a very complex and far reaching one. However, in this article we will touch on just a few of the basics.

Computer Security And Survivable Computer Systems

Survivable computer systems and computer security are in many ways related but at a low-level very much different. For instance, the hardening of a particular system to be resistant against intelligent attacks may be a component of a survivable computer system. It does not address the ability of a computer system to fulfill its purpose when it is impacted by an event such as a deliberate attack, natural disaster or accident, or general failure. A survivable computer system must be able to adapt, perform its primary critical functions even if in a hostile environment, even if various components of the computer system are incapacitated. In some cases, even if the entire "primary" system has been destroyed.

As an example; a system designed to provide real-time critical information regarding analysis of specialized medications ceases to function for a few hours

because of wide spread loss of communication. However, it maintains the validity of the data when communication is restored and systems come back online. This computer system could be considered to have survived under conditions outside of its control.

On the other hand, the same system fails to provide continuous access to information under normal circumstances or operating environment, because of a localized failure, may not be judged to have fulfilled its purpose or met its objective.

Fault Tolerant And Highly Availability Computer Systems

Many computer systems are designed with fault tolerant components so they continue to operate when key portions of the system fail. For instance; multiple power supplies, redundant disk drives or arrays, even multiple processors and system boards that can continue to function even if its peer component is destroyed or fails. The probability of all components designed to be redundant failing at one time may be quite low. However, a malicious entity that knows how the redundant components are configured may be able to engineer critical failures across the board rendering the fault tolerant components ineffective.

High availability also plays a role in a survivable computer system. However this design component may not maintain computer system survivability during certain events such as various forms of malicious attack . An example of this might be a critical web service that has been duplicated, say across multiple machines, to allow continuous functionality if one or more the individual web servers was to fail. The problem is that many implementations of high availability use the same components and methodology on all of the individual systems. If an intelligent attack or malicious event takes place and is directed at a specific set of vulnerabilities on one of the individual systems, it is reasonable to assume the remaining computer systems that participate in the highly available implementation are also susceptible to the same or similar vulnerabilities. A certain degree of variance must be achieved in how all systems participate in the highly available implementation.

What's The Difference Between An Attack, Failure, And Accident?
How Do These Differences Impact A Survivable Computer System

In many cases when I am discussing the security of systems with customers, the question of business continuity and disaster recovery come up. Most companies that provide a service that they deem critical just know the system needs to be operational in a consistent manner. However, there is typically little discussion about the various events or scenarios surrounding this and that can

lead to great disappointment in the future when what the customer thought was a "survivable computer system" does not meet their expectations. Some of the items I like to bring up during these conversations is what their computer systems goal and objective is, what specifically does continuous operation mean to them, and specifically what constitutes an attack, failure, or accident that can cause loss of operation or failure to meet objectives.

A failure may be defined as a localized event that impacts the operation of a system and its ability to deliver services or meet its objectives. An example might be the failure of one or more critical or non-critical functions that effect the performance or overall operation of the system. Say, the failure of a module of code that causes a cascading event that prevents redundant modules from performing properly. Or, a localize hardware failure that incapacitates the computer system.

An accident is typically an event that is outside the control of the system and administrators of a local / private system. An example of this would be natural disasters such as hurricanes, if you live in south Florida like I do, or floods, or wide spread loss of power because the utility provider cut the wrong power lines during an upgrade to the grid. About two years ago, a client of mine who provides web based document management services could not deliver revenue generating services to their customers because a telecommunications engineer cut through a major phone trunk six blocks away from their office. They lost phone and data services for nearly a week.

An now we come to "attack". We all know accidents will happen, we know that everything fails at one time or another, and typically we can speculate on how these things will happen. An attack, executed by an intelligent, experienced individual or group can be very hard to predict. There are many well known and documented forms of attacks. The problem is intelligence and human imagination continuously advance the form of malicious attacks and can seriously threaten even the most advanced designed survivable computer systems. An accident or failure does not have the ability to think out of the box or realize that a highly available design is flawed because all participants use the same design. The probability that an attack might occur, and succeed may be quite low, but the impact may be devastating.

Conclusion

One of the reasons I wrote this article was to illustrate that it's not all about prevention. Although prevention is a big part of survivable computer system design, a critical computer system must be able to meet its objectives even when operating under hostile or stressful circumstances. Or if the steps

taking for prevention ultimately prove inadequate. It may be impossible to think of all the various events that can impact a critical computer system but it is possible to reasonably define the possibilities.

The subject of survivable computer systems is actually one of complexity and ever evolving technology. This article has only touched on a few of the basic aspects of computer system survivability. I intend on continuing this article to delve deeper into the subject of survivable computer systems.

Original URL (The Web version of the article)
---
http://www.defendingthenet.com/NewsLetters/WhatAreSurvivableComputerSystems.htm