

## Ten Challenges in Information Survivability

Jeffrey Voas  
Cigital  
21351 Ridgetop Circle, Suite 400  
Dulles, VA 20165, USA  
Phone: 703.404.9293  
Fax: 703.404.9295  
[voas@cigital.com](mailto:voas@cigital.com)

### Abstract

Information survivability is the complicated notion of providing reliable/accurate, secure/private, and timely information. This information may be provided to humans, other software systems, or hardware machines and physical devices. To provide reliable/accurate information, issues such as system reliability and software reliability must be considered. Fault tolerance techniques also play a role here. To provide secure/private information, technologies such as encryption, intrusion-detection, and malicious code detection are needed. And to provide that information in a timely manner, tools that monitor performance, increase uptime and availability, and reduce time-to-recovery are needed.

Therefore to achieve the goal of information assurance, numerous, diverse techniques need be employed. The problem, however, is that many of these goals are fully or partially mutually exclusive. In this position paper, I will discuss my interests in these trade-offs and why I feel this is a key challenge to creating and deploying survivable information systems.

### Introduction

To begin, I agree with the statement in the call for position papers that in addition to the technical challenges of information survivability, that there are also legal, political, social, economic, and even contractual challenges. I will now go through a listing of 10 challenges that I consider to be some of the more interesting ones and then talk a bit more about the key challenges from this list that I am interested in discussing at the meeting.

[1] In my opinion, there is still no well-formed definition as to what information survivability is. Connecting the term “survive” to the term “ability” clearly creates an intuitive definition, however when applied to information systems, the term is still quite abstract. And just as with software requirements, the more vague they are, the more confusion that arises during development. Further, there are QoS “ilities” that must be viewed as key components of information survivability, such as fault tolerance, reliability, availability, security, safety, performance, etc. But without a sound definition as to what information survivability is, it is difficult to argue in any convincing manner as to how these other “ilities” fit in.

[2] Because of the aforementioned definitional problem, we are then automatically stuck with the additional problem of quantifying the degree of information survivability that any given system has. And if we cannot quantify survivability, then how will we know whether the methods we apply while attempting to boost survivability succeed? So the assessment issue is a key challenge that can only be solved (if it ever can be solved) after a sound definition is found.

[3] Survivability is not all or nothing. There are different degrees to which you can achieve it. Therefore there is no way to simply stamp a survivability score on a particular system and assume that the system will always provide that level of survivability. Survivability is highly context-sensitive and environment-sensitive. Thus for system A, the survivability of A in environment B may or may not equal the survivability of A in environment C.

[4] Survivability is highly dependent on issues related to interoperability. In today's highly networked world, probably the only truly survivable systems are those that are disconnected from the world. Therefore this results in the "weakest link in the chain" problem. However knowing where the weakest link in the chain is is non-trivial. And without knowing that, all of the effort to make one part of the system survivable can easily be undone by another component that was left vulnerable.

[5] The threats that can undermine survivability are not well defined and many are unknown. Because of this, adequate protections will likely not be built into the system. Therefore to begin, we need to bound a set of threats and work from that set to design in enough features to disallow those threats from disrupting service. But note that that does not guarantee that threats outside of that space are protected against.

[6] Speaking only with respect to the US Government, there is no unified plan to address this problem. There is, of course, the Critical Information Assurance Office, but any expectation that a government agency will even begin to solve this problem is wishful. Most US Government agencies can barely lock their machines down from small hacker attacks, let alone tackle a challenge this large and at an infrastructure level.

[7] The ROI question is a very large question concerning survivability. What would the cost be to retrofit many of our critical information infrastructures in a manner that truly made them highly capable of surviving an attack? Almost certainly, that figure would be in the billions of dollars. Further, a successful attack on those systems would also cost billions of dollars in lost resources. But the real question is how great is the threat. Locking down these systems to a level of high tolerance to attack and failure is foolish (given the enormous costs) if the potential of the threats cannot be determined first. So until we can quantify with some degree of certainty what the threats are, their probabilities, and their consequences, it is difficult to convince the stakeholders of this problem that their investments in improving survivability are worthwhile. Therefore I believe that cost-benefit analysis is needed for partitioning the problem into scalable subproblems.

[8] Politically speaking, information survivability is not a very "sexy" problem. Few politicians would even know what you were talking about if you mentioned this to them in an effort to gain research dollars. Admittedly, politicians would understand the issue if you put it into a context such as the ATC system collapsing. But even so, they would almost certainly argue that such a problem would be a DOT issue or someone else's problem. To my knowledge, there is no one on Capital Hill (i.e., no elected officials or staffers) dedicated to seeing this problem brought to a greater awareness and tackled in a unified effort (all agencies working together).

[9] Another problem is solving this equation:  $A \text{ units of security} + B \text{ units of fault tolerance} + C \text{ units of reliability} + D \text{ units of safety} + E \text{ units of performance} + F \text{ units of availability} + \dots = ? \text{ units of survivability}$ . Can we? If not, problems 1 and 2 will remain.

[10] Other minor challenges I believe are related to the perception that encryption solves all worries, that good software processes guarantee good software, the fact that most of our

infrastructure is built on top of either Unix or Windows (both of which have retrofitted and buggy security models), and the time-to-market concerns of the software industry that does not allow them the luxury of delaying releases for quality improvements.

### **My Interest in This Workshop**

My key interests are in problems 1, 2, and in particular, 9. I believe that we must take the existing “ilities” that we know how to achieve some degree of, and determine a scheme for being able to combine them into this new “ility”: survivability. Therefore my interest is not as much in the interoperability of the components of a system, but instead in the interoperability of the “ilities” that are needed to create a survivable system. This does not mean, however, that the interoperability of components problem is a huge issue, but simply something that I do not think we are ready to at all discuss yet. Getting one survivable component in isolation is hard enough at this point. Hopefully someday we will be able to then perform calculations something like:

If component  $\xi$  has the following properties:

A units of security + B units of fault tolerance + C units of reliability + D units of safety  
+ E units of performance + F units of availability

And component  $\psi$  has the following properties:

M units of security + N units of fault tolerance + O units of reliability + P units of safety  
+ Q units of performance + R units of availability

Then  $f(\xi \circ \psi)$  will have a system survivability of Z.