

Dave Farrell - Dave.Farrell@sri.com

Research Red Team - Cyber Defense Research Center - SRI International

6501 Americas Parkway - Suite 500

Albuquerque, NM 87110

voice: 505-830-6800

Please consider this a request for invitation to the Fourth Information Survivability Workshop (ISW-2001) "Impediments to Achieving Survivable Systems". I feel I am uniquely qualified in that I portray the adversary most seek to defend against. One of the many things we now do is assess the survivability of information systems in ways defenders typically have failed to address. Our goal is to improve the system assurance overall by pointing out potential vulnerabilities, ideally before the system is deployed, but oftentimes in a live environment. I am actively involved in studying and understanding the cyber adversary (tools, tactics and procedures) across multiple environments and industries. I have been putting together a comprehensive adversary model that may eventually be used by researchers in the area of information assurance which will allow them to focus on their research and avoid creating naïve models based on minimal sample sets or worse, outdated stereotypical portrayals of "hackers". This leads to false claims and a false sense of security when using the developed system. The use of labels such as script kiddie, cyber vandal, hacktivist, cyber criminal, cyber terrorist and others cause each individual to conjure up many different attributes as they all interpret the words slightly differently based on their backgrounds and experiences. We need not only to provide specific definitions for clarification but also to understand the attributes (similarities and differences) across the spectrum of adversaries. It is my assertion that we can improve the security posture of a system and thus its survivability by understanding the adversary in accordance with a given threat profile.

Generating an appropriate threat profile based on the understanding of your system and the environment in which it is employed is imperative to minimizing the risk and exposure of your system in accordance with your security policies. Note also that security enforcement mechanisms are only as good as the policies that govern their use and can be rendered useless (and actually consume resources with no benefit in the worst case scenario) if not configured properly.

Many e-commerce sites choose, through risk management techniques, to ignore potential problems, as they may not exceed a given dollar threshold. It is a choice made purely of economy where the money gained, even though risk and exposure may be high, is enough to overcome the loose statistics used to justify this decision. I believe this to be an example of clearly not understanding the real threat.

In mission critical systems the threat may manifest itself through various means. We must be prepared to defend the threat independent of its source, be it adversary or natural causes. A failure is a failure and in some cases cannot be tolerated whether its cause is a programming error an intentional attack utilizing malicious code. The results may be just as devastating and appear to have taken the same path when viewed after the fact with the minimal data typically collected in an attempt to perform forensics.