

ISW 2000 Position Paper
Stephen R. Hanna and Radia J. Perlman
Sun Microsystems, Inc.
steve.hanna@sun.com, radia.perlman@sun.com

A Commercial Perspective on Network Survivability

As the popularity of the Internet grows, it is quickly becoming an essential part of our culture and commerce. New businesses are developed, based on quickly assembled electronic commerce systems. Existing businesses rush to get on the web, lest they be left behind. Even governments, utilities, and safety-critical services have moved quickly to the Internet.

But is the Internet ready for this transition? Until recently, the Internet was a research and academic network. While survivability was part of the design goals for the Arpanet, it has not always been foremost as a design criterion since then. Especially in the last decade, performance and functionality have often overridden survivability as a design goal.

We believe that a reexamination of the Internet's most basic protocols (especially routing and naming) from a survivability perspective is in order. An examination of commercial Internet protocols, applications, and service models is also useful.

Current Internet routing protocols are too fragile. Interdomain routing is a mix of static configuration (unable to adapt to component failures) and dynamic configuration (unprotected against compromise of a trusted node). Intradomain routing protocols is commonly handled with link-state protocols, which are completely susceptible to compromise of a trusted node.

Internet naming is handled by the Domain Name System (DNS), which resolves queries in the hierarchical domain name space using a hierarchy of servers that roughly matches the hierarchy of names. DNS Security (DNSSEC) allows DNS data to be signed with a private key and provides a mechanism for securely establishing the public key associated with a particular domain. This corresponds to a hierarchical PKI model and shares all of the weaknesses of that model. Compromise of the private key associated with the root domain (or important top level domains) can cause compromise of the security provided for all (or a large part) of the name space. Although the DNSSEC model allows for cross-certification between domains, there is no provision for indicating which domains have been signed by a particular issuer. So this feature is not very useful in its current form.

At commercial sites, the application architecture is rarely designed with survivability in mind. The "moat model" depends on building a secure "DMZ." Security resources are focussed on the servers in this zone, which provide restricted access to critical resource within an inner network. This fails to account for the likelihood that servers within the DMZ will be compromised. Servers in the DMZ must be treated with the same suspicion as outside requestors. And we must explore the use of delegation to limit the authority granted to the DMZ servers (and other middle servers in an n-tier environment).