Intrusion Tolerant Web Servers via Network Layer Controls
Secure Computing Corporation

Existing information systems’ security measures are limited because even if a component failure due to an intrusion is detected, there are few mechanisms for effectively isolating the corrupt component. Attacks tend to spread unchecked, hopping from one host to another. The typical response, to turn off the corrupted service, results in denial of service that is often as damaging as the attack itself. This demonstration shows the approach taken on the Intrusion Tolerant Server Infrastructure (ITSI) program to identify and isolate intrusions, prevent them from freely spreading, and continue to provide service to benign users while recovering from the intrusion.

The distinguishing feature of the ITSI approach is the use of “smart NICs” to help identify intrusions, and, once an intrusion has been detected, to contain it and ensure that service is uninterrupted by providing a failover capability. These smart NICs are based on the distributed firewall technology developed by Secure Computing on DARPA’s Autonomic Distributed Firewall (ADF) program. The ADF NIC has been enhanced on the ITSI program to support multi-server load sharing, to enable load shifting in the face of attacks, and to provide an alert capability when unauthorized traffic is detected.

The demo prototype uses two heterogeneous web servers: Apache running on SELinux and IIS running on Windows 2000. The demo will show how various attacks are detected and how the smart NICs can be used to respond to an attack in a manner that ensures that the web service will continue to operate.