Survivability & Trust

L. Jean Camp
ljcamp@ca.sandia.gov
(v) 510-294-3396
(f) 510-294-1004

David A. Evensky
evensky@ca.sandia.gov
(v) 510-294-3689
(f) 510-294-3422

Infrastructure & Networking Research
MS 9053
7011 East Ave.
Livermore, CA94550

Survivability is a critical research topic for the Next Generation Internet. Specifically, the survivability implications of the of distributed trust mechanisms now being established for commerce and resource sharing must be subject to investigation through modeling, risk analysis, and simulations.

In the Next Generation Internet security will be a cumulative, distributed, and probabilistic. The approach to security as survivability reflects the need of a Next Generation Internet where robustness must compensate for lack of hardening; and denial of service or disconnection are not acceptable defense mechanisms. In sum, the Next Generation Internet has to have survivability as a whole, as well as secure at the end points.

Traditional security, based on orange book notions, is binary. A system has a security feature, or it does not. A hole either exits, or is does not. A traditional approach to computer security assumes centralized control, and uses logic to build provable statements. This is not compatible with the current Internet, and will be less so in the next generation.

The Next Generation Internet needs to be safer as well as faster. Safe computing implies more than secure endpoints -- it requires that such security not come at the expense of Two of the greatest strengths of the Internet are that it is distributed and exhibits graceful degradation. Graceful degradation means any person can connect to the Internet without altering others' access, and the loss of one machine should not effect those not using its services. Even during the most effective assault to date on the Internet, the Morris worm incident, staying connected proved to be the best strategy for recovery. Obtain defense against the worm, and information regarding these defenses, required remaining connected. Those who disconnected were isolated, with only their own resources to develop defenses. The ability of the Internet to degrade gracefully rather than suffering catastrophic failure is now recognized as a critical component in survivability.

The Next Generation Internet will be a platform for sharing and selling resources. In order to share and sell resources, there must be distributed trust. Mechanisms for evaluating trustworthiness of requests and claims of authorization currently being proposed are centralized hierarchies, often using public key certificates. The implications of adding a trust layer or trust infrastructure to the Next Generation Internet need to be thoroughly evaluated in the earliest stages.

Proposals for trust include short-lived attribute specific certificates, long-lived multipurpose certificates (Sirbu & Tygar, 1995) certificates signed by multiple parties (Visa, 1995; Mastercard, 1995; Mastercard, 1996) , a Web of Trust (Garfinkle, 1994) and combinations of these. There is no doubt that these mechanisms will vary with respect to their ability to recognize an attack, reduce the damage of any attack, and subsequently recover. These mechanisms should be tested, possibly subject to concentrated attack, and this is possibly only in a testbed.

To illustrate the importance of survivability of distributed trust mechanisms, consider two application areas which will require high speed networks with distributed trust: electronic commerce and health care networks.

The effect of subverting a key on a root or certificate server must be tested in a highly distributed environment. An experimental subversion of an on-line SET gateway is as irresponsible as real time testing of denial of coolant to an on-line nuclear plant. The Next Generation Internet offers an opportunity for interdisciplinary and cross-institutional testing of trust loss in a contained but not classified environment.

Electronic commerce is being built upon a certificate infrastructure that will be implemented as a network of partially trusted servers. For example, the Bankers Trust gateway will extend trust to other SET gateways. This approach, effectively a Web of Hierarchies approach, of electronic commerce has not been subject to a systemic evaluation. Some common assumptions may prove to be unfounded. For example, the use of multiple keys, one for signatures and one for payment authorization, is valuable in theory. Yet how does this practice affect survivability when a consumer's entire machine is subverted? Could one key and two PINs be better in practice? Is there a threshold for a number of keys and certificates above which consumers have difficulty re-establishing themselves after their local machines have been subverted?

Health care systems have different priorities than electronic commerce systems in terms of service needs. In the military computer security paradigm loss of information is often preferable to exposure. In electronic commerce, it is reasonable and possible to freeze funds while disputes are resolved. However, in health care information system availability is the greatest priority. In health care confidentiality is desirable, but availability and integrity are critical. Emerging concepts of survivability are particularly important for health care information systems as critical decisions require constant availability. Failures and attacks of medically critical software have already caused deaths.

The high bandwidth of the Next Generation Internet is extremely important for delivery of health care. Distributed availability is not only necessary because of the increasing use distributed systems, within a single health care domain but also because an increasingly mobile population requires information transfers across domains. Such information transfers require distributed trust.

Mastercard, 1995, Secure Electronic Payment Protocol Specification Draft Version 1.1, http://www.mastercard.com/Sepp/sepptoc.htm, November, Part 2.

Mastercard, 1996, Secure Electronic Transaction Technology, Draft., http://www.mastercard.com/SETT.

Sirbu, M., and Tygar, J. D., 1995, ”NetBill: an Internet commerce system optimized for network delivered services,” IEEE ComCon, San Francisco, CA. March 6

Visa, 1995, Secure Transaction Technology Specifications Version 1.1, http://www.visa.com/visa-stt/index.html, November.

Garfinkle, 1994, "PGP: Pretty Good Privacy", O'Reilly & Associates, Inc., Sebastopol, CA, pp. 235-236.