Panel on Security Issues for Mosaic and the World Wide Web

Fred Avolio, Chair
Trusted Information Systems
3060 Washington Road
Glenwood, Maryland 21738 USA
avolio@tis.com

Overview

The Internet “killer application of the 90’s” may end up being Mosaic and the World Wide Web. WWW gives to an Internet novice the ability to seemingly effortlessly traverse the Internet retrieving information with a few simple mouse-clicks. Many organizations are considering WWW as a means of providing organizational presence on the network, and others are using it for electronic commerce.

To quote from CERN, the creators of the Web, “The World Wide Web (WWW) is the universe of network-accessible information, an embodiment of human knowledge. It is an initiative started at CERN, now with many participants. It has a body of software, and a set of protocols and conventions. WWW uses hypertext and multimedia techniques to make the web easy for anyone to roam, browse, and contribute to.”

As is often the case with systems that provide a high degree of data sharing, there are a number of security issues for sites that want to take advantage of the web. This panel brings together WWW experts who are dealing with these security issues.

This panel presents some of the research and provides a forum for discussion, debate, as well as questions and answers. Specific topics include:

An overview of WWW and its components. The mechanisms and methods employed by WWW servers and clients will be introduced and discussed. Included will be HTTP, URLs, HTML, and Mosaic, and the threats and various countermeasures to employ.

HTTP through a firewall. As firewalls are being used with greater frequency, the need has increased for allowing HTTP requests, and related services accessible via WWW, through a firewall while preserving the security policy the firewall implements.

HTTP authentication, confidentiality, and integrity. For electronic commerce each of these areas is vitally important. Parties involved must be able to authenticate themselves and servers to which they are connected; they must be assured of the privacy of their transactions; and they must rely on the information passed being protected against accidental or intentional modification.

End system security. As Dave Dalva wrote in the paper Security and the World Wide Web, “The major security issue with running client software comes about given the nature of the web: client programs interpret data that is downloaded from arbitrary servers on the Internet. If there are no checks on the contents of this imported data, there exists the potential for this data to subvert programs running on the client systems. These ‘Trojan horses’ may take several forms, from malicious URLs to rogue code that is run through interpreters (such as PostScript) on the client system.”

WWW wish list. What is needed or desired in future versions of the protocol, clients, and servers to make a security implementor’s job easier?