Internet Essay, Research Paper

Unfortunately, there’s a lot to worry about. There are security risks that affect Web servers, the local area networks that host Web sites, and even innocent users of Web browsers.

The risks are most severe from the Webmaster’s perspective. The moment you install a Web server at your site, you’ve opened a window into your local network that the entire Internet can peer through. Most visitors are content to window shop, but a few will try to to peek at things you don’t intend for public consumption. Others, not content with looking without touching, will attempt to force the window open and crawl in. The results can range from the merely embarassing, for instance the discovery one morning that your site’s home page has been replaced by an obscene parody, to the damaging, for example the theft of your entire database of customer information.

It’s a maxim in system security circles that buggy software opens up security holes. It’s a maxim in software development circles that large, complex programs contain bugs. Unfortunately, Web servers are large, complex programs that can (and in some cases have been proven to) contain security holes. Furthermore, the open architecture of Web servers allows arbitrary CGI scripts to be executed on the server’s side of the connection in response to remote requests. Any CGI script installed at your site may contain bugs, and every such bug is a potential security hole.

From the point of view of the network administrator, a Web server represents yet another potential hole in your local network’s security. The general goal of network security is to keep strangers out. Yet the point of a Web site is to provide the world with controlled access to your network. Drawing the line can be difficult. A poorly configured Web server can punch a hole in the most carefully designed firewall system. A poorly configured firewall can make a Web site impossible to use. Things get particularly complicated in an intranet environment, where the Web server must typically be configured to recognize and authenticate various groups of users, each with distinct access privileges.

To the end-user, Web surfing feels both safe and anonymous. It’s not. Active content, such as ActiveX controls and Java applets, introduces the possibility that Web browsing will introduce viruses or other malicious software into the user’s system. Active content also has implications for the network administrator, insofar as Web browsers provide a pathway for malicious software to bypass the firewall system and enter the local area network. Even without active content, the very act of browsing leaves an electronic record of the user’s surfing history, from which unscrupulous individuals can reconstruct a very accurate profile of the user’s tastes and habits.

Finally, both end-users and Web administrators need to worry about the confidentiality of the data transmitted across the Web. The TCP/IP protocol was not designed with security in mind; hence it is vulnerable to network eavesdropping. When confidential documents are transmitted from the Web server to the browser, or when the end-user sends private information back to the server inside a fill-out form, someone may be listening in.