Dimitra Samara
B" semester MIS 1998-99
Sociologist
Grammou str 121
52 100 Kastoria
Greece 0467 82722

This paper introduces frequently asked questions on security . It is attempting to answer most of those questions concerning the security implications on running a web server in the web enviroment.

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results can range from the merely embarassing, for instance the discovery one morning that your site's home page has been replaced by an obscene parody, to the damaging, for example the theft of your entire database of customer information.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.

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.

Exactly what security risks are we talking about?

There are basically three overlapping types of risk:

1. Bugs or misconfiguration problems in the Web server that allow unauthorized remote users to:
   - Steal confidential documents not intended for their eyes.
   - Execute commands on the server host machine, allowing them to modify the system.
   - Gain information about the Web server's host machine that will allow them to break into the system.
   - Launch denial-of-service attacks, rendering the machine temporarily unusable.
2. Browser-side risks, including:
   - Active content that crashes the browser, damages the user's system, breaches the user's privacy, or merely
   - creates an annoyance.
   - The misuse of personal information knowingly or unkowingly provided by the end-user.

3.Interception of network data sent from browser to server or vice versa via network eavesdropping. Eavesdroppers can operate from any point on the pathway between browser and server including:

The network on the browser's side of the connection.

The network on the server's side of the connection (including intranets).

The end-user's Internet service provider (ISP).

The server's ISP.

Either ISPs' regional access provider.

It's important to realize that "secure" browsers and servers are only designed to protect confidential information against network eavesdropping. Without system security on both browser and server sides, confidential documents are vulnerable to interception.

Protecting against network eavesdropping and system security are the subject of sections 1 to 5 of this document. Client-side security is covered in sections 6 and 7. Section 8 deals with security alerts for specific Web servers.