JDH TECHNOLOGIES

White Paper

Web-4M™ Security

Basic Security

There are four areas of basic security within Web-4M that we address in this portion of this document: password security, link security, access control, and security for the Browseable Document Library™.

Password Security

Passwords are doubly encrypted (with a one time key) using the NIST standard Secure Hash Algorithm (SHA-1). This ensures protection against password sniffing as data is transferred between client and server in the login process.

Link Security

Almost all Web-4M interactions between clients and the server are messages sent via socket connections on the intranet or the Internet connecting the computers (the one exception is the document library, discussed below). This includes the chat, whiteboard, slideshow tools, email, news, and calendar functions. These messages can be sent unencrypted over the network, meaning that if the network itself is insecure (as are most networks and certainly the Internet), the messages are vulnerable to being sniffed and read by machines on the same networks, or by any machine in the end-to-end path between the two machines.

Web-4M offers a "secure link" mode of operation to avoid this problem. When the secure link option is turned on, the client randomly chooses a 128 bit secret key, using the timing of the login keystrokes as the source of randomness. This secret key is then communicated to the server using the El-Gamal public key encryption algorithm. The client and the server then set up links to use the Blowfish algorithm for all data passing between them. The Blowfish algorithm was developed by Bruce Schneier, author of "Applied Cryptography," and in studies so far, no known weaknesses have been found.

The Web-4M administrator controls whether encryption is always on, always off, or can be turned on and off by users. By forcing the encryption always on, users cannot intentionally or inadvertently turn off encryption and make insecure transfers.

Access Control

When utilizing collaboration software, it is common that many different groups of users will be using the same software at the same time. This could cause a problem if there are documents and information that only one group should have access to. For this reason, Web-4M allows administrators and room owners to specify exactly which users have access to particular material. For example, a room owner can limit access to the room. Users without access permission, will not see the room listed in the room list. A room owner can also create a project, containing a document folder, newsgroup, and calendar, connected with his/her room and may limit which users can view and post material.

In addition to managing the access of typical users, Web-4M also provides a way to control anonymous guest users as well. Room owners can associate a conference ID and time restrictions to a conference. When a guest logs in during the set time frame they use the conference ID as their password. When they log in they are taken directly to the room in which the conference will be held. By utilizing this method, guest users will be prevented from using many typical user functions, such as peer-to-peer tools. They will, however, still have full access to the room, including conferences and projects, although they will not be able to start conferences.

Browseable Document Library™ Security

In the document library, documents are accessed via an html request. The default configuration of Web-4M uses the existing webserver to access documents. This webserver is the same one that provides access to the Web-4M applet itself. Since anyone accessing the webserver can potentially access the data in the library, Web-4M hides the document library directory structures by appending a 32-bit number to the directory names at the top level of the document library.

Advanced Security

The advanced security features in Web-4M are realized with the addition of Secure Access-4M, JDH Technologies' firewall tunneling solution.

Many businesses and organizations today have firewalls to protect themselves against unwanted cyber-attack. Additionally, many individual users have personal firewalls as well. Firewalls can be configured to block all network communications or allow particular classes of communication on specified ports. Furthermore, firewalls can limit communications based on the initiator of a connection, that is, whether the connection is started from inside or outside the firewall. Although Web-4M can be run safely through a firewall with appropriate ports opened, some network administrators or security supervisors are reluctant to change firewall rules. Fortunately most firewalls today are configured to allow web traffic (http) and secure web traffic (https) to pass through them. Secure Access-4M acts as an alternate route for Web-4M traffic by using the SSL web server port and protocol. Secure Access-4M can be run on the same machine as the Web-4M server, if port 443 (or whatever port you wish to use for the SSL connection) is free, or it can be run on a second machine, in the manner of our older, non-secure tunnel, Access-4M. The advantage of running it on the same machine is that Web-4M can be configured to use it for authorization and secure access of files in the Browseable Document Library. An added bonus of using the firewall tunnel, Secure Access-4M, is that it encrypts all messages traveling to the Web-4M server. This means that your audio, video, appshare, whiteboard, etc are all encrypted and secure.

For more information about Secure Access-4M, and all its features, as well as configuration information, refer to the "Secure Access-4M Firewall Tunneling Solution" whitepaper and manual.

JDH TECHNOLOGIES WHITEPAPER

Web-4M Security

? JDH Technologies
12388 Warwick Blvd • Suite 302
Phone 757.873.4747 • Email info@jdhtech.com