



Security White Paper



Data Center where Maintenance Connection servers reside

Maintenance Connection Inc.

Corporate Headquarters
1947 Galileo Ct. Suite 101
Davis, CA 95616

Toll-free: 1-888-567-3434
Fax: 1-888-567-3434

Email: info@maintenanceconnection.com
<http://www.maintenanceconnection.com>

COPYRIGHT 2000–2003 Maintenance Connection, Inc. All rights reserved.

This publication contains confidential and proprietary information, which is protected by copyright. No part of this publication may be reproduced, transcribed, stored in a retrieval system, or translated into any language or computer language, or transmitted in any form whatsoever, without prior written consent of Maintenance Connection, Inc. For information, contact:

Maintenance Connection, Inc.
1947 Galileo Ct. Suite 101
Davis, CA 95616
ATTN: Technical Publications
1-888-567-3434

Disclaimer of Warranties and Limitation of Liabilities

The staff of Maintenance Connection, Inc. has taken due care in preparing this white paper. However, nothing contained herein modifies or alters in any way the standard terms and conditions of any Maintenance Connection, purchase, lease, or license agreement by which the product was acquired, nor increases in any way Maintenance Connection's liability to the customer. In no event shall Maintenance Connection or its subsidiaries be liable for incidental or consequential damages in connection with or arising from the use of the product, the accompanying manual, or any related materials.

All Maintenance Connection publications and computer programs contain proprietary confidential information of Maintenance Connection, and its possession and use are subject to restrictions set forth in the License Agreement entered into between Maintenance Connection and its Licensees. No title or ownership of Maintenance Connection software is transferred and any use of the product and its related materials beyond the terms of this license, without the written authorization of Maintenance Connection, is prohibited.

Maintenance Connection reserves the right to revise this publication from time to time and to make changes in the content hereof without obligation to notify any person of such revisions or changes.

Restricted and Limited Rights Notice

Use, duplication or disclosure by any agency of the U.S. Government licensed with respect to this documentation is subject to restrictions, as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013. Maintenance Connection, Inc., 1947 Galileo Ct. Suite 101, Davis, CA 95616.

© 2000-2003 Maintenance Connection, Inc. All rights reserved. *Maintenance Connection; the Maintenance Connection logo; and maintenanceconnection.com* are trademarks or registered trademarks of Maintenance Connection Inc.

All other commercial names mentioned herein are used for identification purposes only and may be trademarks of their respective owners.

Maintenance Connection Security Whitepaper

Document Number MC-2003-01-0301

Table of Contents

- Introduction 4
- Security Levels 4
- Browser Security 7
- Server Security 7
 - Certificates 7
 - Encryption 8
 - Firewalls 10
 - Operating System Security 10
 - Database Security 10
- Physical Security 10
- User Security 10
 - Do not reveal your password 10
 - Create a password that is hard to guess 10
 - Do not leave your session unattended 11
 - Log off when you are done 11
 - Choose your browser wisely 11
 - Use caution when printing 11
 - Upgrade your browser 11
- Security Concerns 11
 - Unauthorized Data Access 11
 - Unauthorized Information Sharing 12
 - Unauthorized Data Changes Outside Of Process Boundaries 12
- Conclusions 12

Maintenance Connection

Introduction

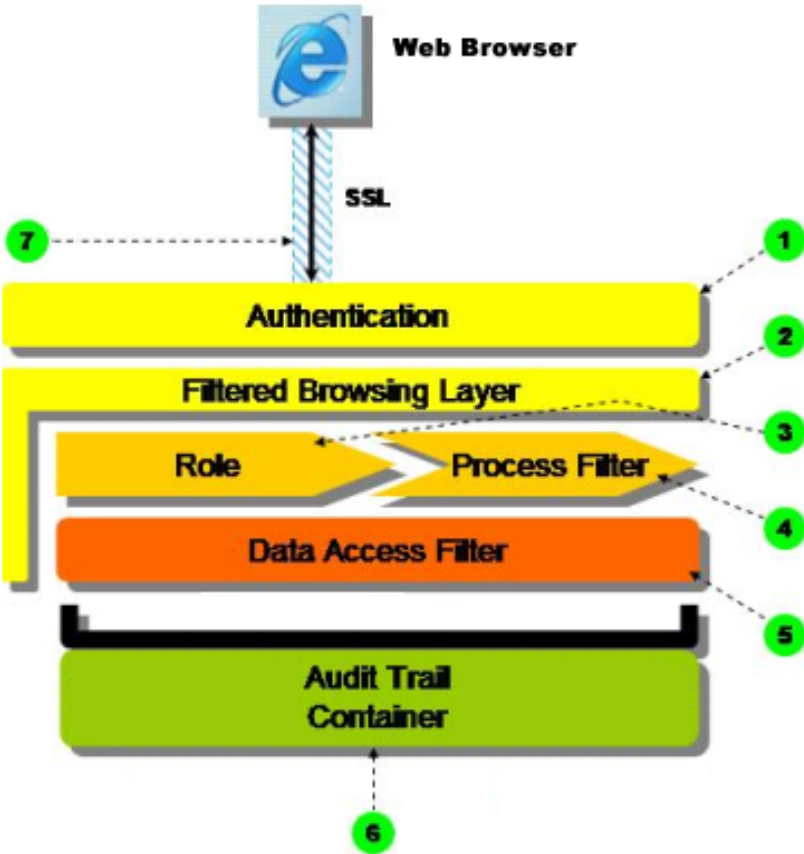
Maintenance Connection provides Web-Based Maintenance Management (or Web-Based CMMS Software) for organizations needing Equipment Maintenance, Building Maintenance, Facility Maintenance, Plant Maintenance, or School Maintenance solutions.

Features include Work Order Tracking, Preventive Maintenance / PM Software, Asset Management, Built-in Procedure Libraries, Inventory Tracking, Purchasing, Scheduling, and Service Requests - all available by simply using a web browser.

Security Levels

Maintenance Connection uses Internet security technology to provide a secure, immediate, and efficient means of access to information while employing maximum security for all data that exists on the Maintenance Connection servers. Because Maintenance Connection uses the Internet to exchange information between users and Maintenance Connection, an additional level of security is added by supporting the highest level of browser encryption, 128 bit.

The Maintenance Connection security architecture employs 7 layers and modules to accomplish a highly reliable, fine-grained multi faceted security platform.



Maintenance Connection Security Levels Architecture

Each layer is optimized for the enforcement or management of specific security detail:

1. **Authentication** – most basic and top layer of defense which establishes the identity and credentials of the user who wishes to access the system by requiring users to enter a member name and password. Every request is re-authenticated automatically given the user credentials that have been validated and secured on the first-time login. Maintenance Connection utilizes session time-outs, therefore the user might be asked to re-authenticate in mid-session if expiration timeout has been detected.

In order to protect user identity and access to records, Maintenance Connection requires that users have a unique user-defined Member ID and password when logging on to the application. Even before the user can log onto the system, they must go through the sign-up process to establish their account. Only when this account is approved will the user have access to the Maintenance Connection applications and data.

Maintenance Connection security policies and procedures provide authentication by:

- Establishing an unapproved account during the sign-up process
 - Allowing managers to approve or reject user accounts
 - Allowing user-defined Member IDs and passwords that can be changed frequently
2. **Filtered Browsing Layer** – is the extension to the authentication mechanism, enforcing each web page access to use valid credentials. This layer detects whether a user has a valid session, and therefore it will direct users to a login step if either session or credentials have been deemed invalid. This mechanism prevents unauthorized users who might have a bookmark or URL link from gaining direct browsing access to any parts of the system.
 3. **Roles** – provide a dynamic grouping function of permissions associated with data manipulation or specific application level functions. Maintenance Connection has a rich support for user level role definition (defined in the application as access groups), giving managers a fine-grained capability to grant permission to specific features of the system to any users of the Maintenance Connection application. The manager can assign an access group to any individual, thus easily expanding or narrowing access rights as necessary. The built-in access groups can be used, or new ones can be created. Since this security layer is dynamic and real-time, changes to the details of a particular role will take effect immediately. Several functions of the Maintenance Connection application are controlled by means of access groups, therefore users who do not have the appropriate permissions, will not be even aware of the existence of certain features, since the tabs, icons, or buttons will not be present in their view of the application.
 4. **Process Filter** – provides a workflow-based security framework, through which managers can enable and disable application level functions at any given step in the business process flow. For example, a manager may allow a user the ability to create a work order, but not approve, issue, or close it out.
 5. **Data Access Filter** – layer enforces data access policies of the Maintenance Connection application. All data access requests pass through system filters and only allowable data sets are exposed and returned to the user.
 6. **Audit Trail Container** – is the central repository of the history of all changes made by all users of the Maintenance Connection system. The audit log helps reconstruct with accuracy the changes made to any specific data item. The audit log contains the date, time, user who made the change, the value before the change, and the value after the change so that information related disputes can be corroborated.

- 7. Encryption** – is the methodology by which information sent between a browser and web server is scrambled through various algorithms in order to prevent someone from eavesdropping (or sniffing) in the communication and potentially observing the transmitted information. Clearly this is a major issue for communication over public networks, since there is no control over who can see the information on the open net. To combat this issue, the Maintenance Connection architecture fully supports and utilizes the industry standard SSL (Secure Socket Layer) protocol.

Secure Socket Layer (SSL) is the software protocol used by both the browser and the web server to implement the highest possible security levels. The Maintenance Connection server requires that the user's browser be configured to support both SSL2 and SSL3 protocols (in the security options of the web browser) so that it can encrypt communications with the web server and ensure that information between Maintenance Connection and the user cannot be read by outside parties.

Web servers that run secure sessions require browsers with a *minimum* of 40-bit encryption to generate session keys used to encrypt/decrypt transmissions between browser and server. Maintenance Connection uses 128-bit encryption whenever possible to ensure privacy. Encryption capabilities are built into most Internet browsers and can be enabled by users. The larger the number of bits contained in the session key used for encryption (40-128 bits), the more difficult (exponentially) it is for an unauthorized person to unscramble the transmission. The 40-bit encryption is known as international level or *export-grade* encryption. The stronger 128-bit encryption is referred to as U.S. and Canada-only level, or *domestic-grade* encryption. Until recently, no encryption requiring a key greater than 40-bit was permitted to be exported outside of the United States and Canada.¹

This restriction has now been partially lifted under certain trade conditions,² but 40-bit encryption is still used by many companies doing business internationally.

The Maintenance Connection servers support connections from browsers that employ 40-bit, 56-bit and 128-bit encryption. The stronger 128-bit encryption method may impose performance degradation on less powerful PCs running the browser. Maintenance Connection continually evaluates commercial browsers to ensure that they meet strict security standards. For browser requirements for Maintenance Connection, refer to *Maintenance Connection Minimum Requirements* at <http://www.maintenanceconnection.com>.

Maintenance Connection has implemented a rich security architecture to satisfy the most stringent needs of any organization and it is under management control how much or how little security is applied, and therefore, administration can selectively enable or disable the various security measures to tailor security constraints to the organization's needs.

¹ The following quote was taken from the Verisign website (February 15, 2001): "Until recently, strong 128-bit encryption was not exportable. The United States Department of Commerce has approved VeriSign to issue certificates for 128-bit encrypted communications, the highest level of encryption ever allowed across United States borders. With a Veri-Sign 128-bit Global Server ID, available from VeriSign as part of its Secure Site Pro and Commerce Site Pro Services, your 128-bit customers can now enjoy unparalleled security when visiting your website."

² The following quote was taken from the Netscape website (February 15, 2001): "Browser software contains encryption technology that is subject to the U.S. Export Administration Regulations and other U.S. law, and may not be exported or re-exported to certain countries (currently Afghanistan (Taliban-controlled areas), Cuba, Iran, Iraq, Libya, North Korea, Serbia (except Kosovo), Sudan and Syria) or to persons or entities prohibited from receiving U.S. exports (including Denied Parties, entities on the Bureau of Export Administration Entity List, and Specially Designated Nationals). For more information on the U.S. Export Administration Regulations (EAR), 15 C.F.R. Parts 730-774, and the Bureau of Export Administration ("BXA"), please see the BXA homepage."

Browser Security

Because Maintenance Connection is a web-based application, a user's browser is an integral part of the application. The browser supplies base functionality by displaying application information while providing a convenient means of interaction between both. Because the web server *requires* secure Internet sessions to prevent unauthorized users from seeing data sent to and from a web server, browsers that will connect to the Maintenance Connection web servers must be configured to support the recommended secure session security protocols.

Browsers can be configured to notify employees when they are about to do something that might pose a security risk. For example, if the site claims to be holding a secure session but its security credentials are suspect, the browser can warn users that the site might have been tampered with or might be misrepresenting itself. This option can be configured to meet the organization's requirements for warning users about specific security options.

When a user is viewing a page from a secure session, the browser displays an icon (typically a lock icon) on the status bar indicating that the session is secure.

Server Security

The Internet sends information originating from a browser from computer to computer until the information reaches its destination website. Without imposed security, there are many ways that hackers can infiltrate the information. Intruders can fool the browser by impersonating the web server. Unauthorized users may try to gain access to other resources inside the organization providing web site access. Maintenance Connection has incorporated integrated levels of server security to counteract these and other security threats, and to ensure confidentiality.

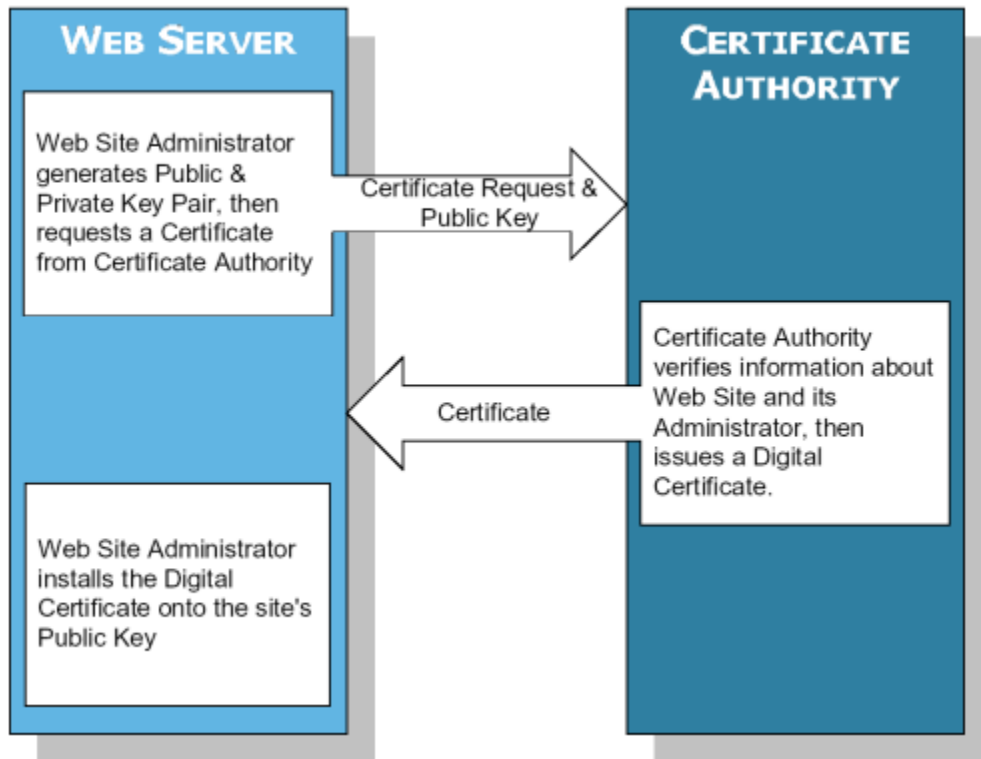
Certificates

Authentication is a process that verifies the integrity of a request, and ensures that when a user requests information from a web server, only that user receives the information. Authentication guarantees that when the user receives a response, it could have been sent only by that specific web server. A web site certificate, issued by a Certificate Authority (CA), is a means to achieve this.

This computer-based certificate will:

- Identifies the CA issuing it
- Is digitally signed by the CA
- Identifies the subscriber (such as Maintenance Connection)
- Is attached to the subscriber's public key
- Identifies the certificate's operational period
- Contains a certificate serial number

The following diagram shows how Maintenance Connection obtains a certificate for its public key:



Maintenance Connection uses Comodo as its CA and their web site can be found at <http://www.instantssl.com> Both Microsoft and Netscape browsers integrate support for verifying digital certificates issued by Comodo.

When users try to connect to a secure website, the browser verifies that the Internet address stored in the certificate issued to that web site matches the address users are connecting to, and that it has not expired. If not, the browser displays a warning to users regarding the authenticity of the web server. The authentication process ensures that no other web site can assume the identity of the original certified site.

Web server certificates also play a role in providing data privacy between the server and browser. The certificate, coupled with a key pair, is part of the encryption level of security.

Comodo has stated that if a Microsoft or Netscape browser, even an exported version, connects to a server with a Comodo 128-bit certificate, the browser will “step up” to 128-bit encryption automatically.

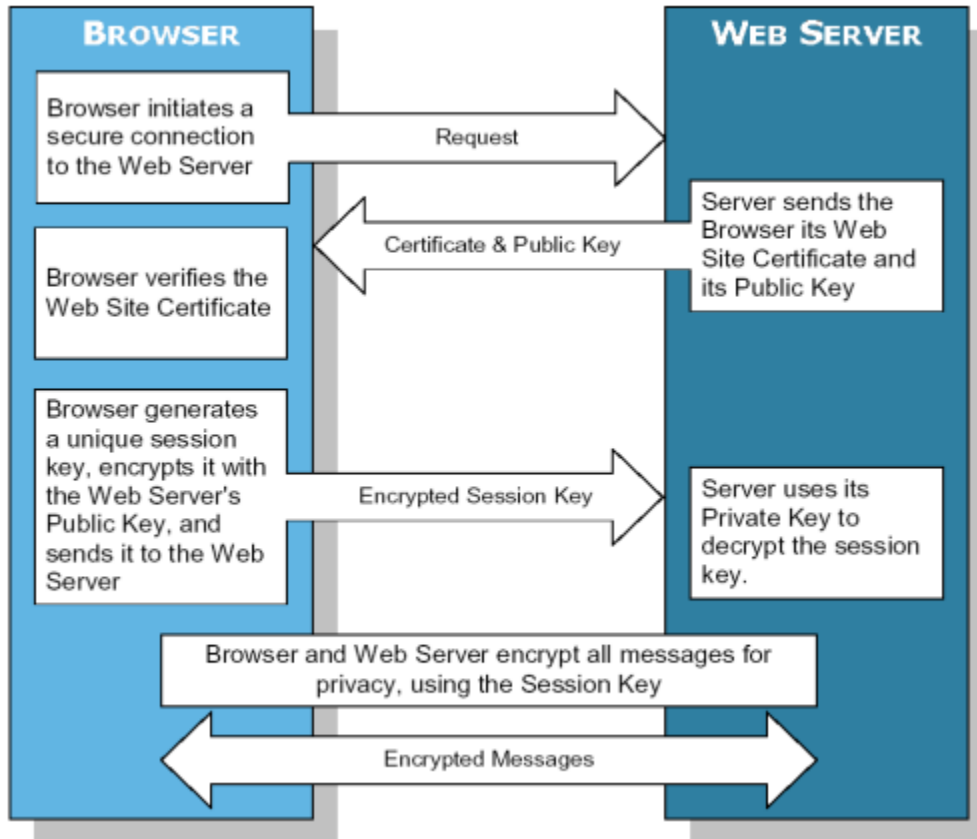
Encryption

Encryption is the translation of data into a form that can be read only by using a special key to decrypt the data. This technique, used at web sites that require secure sessions, protects private information exchanged to and from a user's browser so that it cannot be read by a third party.

Cryptographic keys encrypt and decrypt private information. In asymmetric, or public-key, encryption, data encrypted with a public key can be decrypted only with the corresponding private key. In symmetric, or single key, encryption, data encrypted with one key can be decrypted only with the exact same key.

Web servers that run secure Internet sessions, such as Maintenance Connection, use public key *and* private key encryption. The server is issued a public/private key pair via a certificate. Unlike the public key, the private key is not made accessible to the outside world, but is securely stored on the server.

The following diagram shows the series of events that occur as the browser authenticates the website and establishes a private, encrypted communications session.



The following interaction occurs for each secured session between the browser and the server:

1. The browser requests a connection to the web server, which then provides its web site certificate and public key to the browser.
2. The browser generates a symmetric key that encrypts each transmission.
3. The browser uses the server's public key to encrypt the session key and sends the encrypted key to the server.
4. The server uses its private key to decrypt the session key sent by the browser.
5. From that point until the end of the session, the server uses the session key to encrypt data sent to the browser and decrypts any data received from the browser.
6. Similarly, the browser uses the session key to decrypt the data coming *from* the server and to encrypt data sent *to* the server.

Through this interaction, the only way to expose the contents of a transmission is to decrypt it with the session key. Only the browser and the server know that key, preventing unauthorized users from violating the privacy of the data. In addition, session keys expire as soon as the user terminates the online session, or after 24 hours, whichever occurs first. In the unlikely event that a hacker could decode the session key, it would be useless in future online sessions.

Firewalls

A firewall is a security mechanism that provides limited access to a site, such as Maintenance Connection, from the Internet. A firewall allows approved traffic in and out, according to the requirements of the applications at the site. This approach lets Maintenance Connection select the services appropriate to its business needs, while preventing others that may pose significant security risks. Firewalls are implemented both at the hardware and software level as required.

Maintenance Connection's network routing hardware protects Maintenance Connection systems by routing the secure transactions to a specific server and refusing all unauthorized data packets. This packet filtering prevents external sources from directly accessing any databases containing user data.

Operating System Security

Maintenance Connection's application servers run on a hardened operating system that provides user-based access control to resources.

Database Security

The Maintenance Connection application uses a relational database server as the database engine. The database server software runs on separate servers than the web servers with internal (or non-routable on the Internet) IP addresses. These database servers are not directly accessible from the Internet. Access to the data in the database is controlled by database user groups and enforced by defined internal business rules.

When users log on to Maintenance Connection, their identifying information (Member ID and Password) are checked against the database records. If no match is found, access is denied. The application restricts administrative functions to only those users with the appropriate database access level. The database also maintains a log of user connections to the Maintenance Connection web server.

Physical Security

As an additional measure of protection, all hardware and software used for Maintenance Connection's production systems are housed in a physically secured environment. All Facility Network Systems are constantly monitored 24x7x365 in an outsourced state of the art Command Center.

User Security

While Maintenance Connection works to protect a user's privacy, the user plays an important role in protecting data. Users of web-based applications should take the following measures to ensure that an online session experience on the Internet is safe and secure.

Do not reveal your password

A password is designed to protect the privacy of your session information, but it will only work if it is not divulged. Once established, you should protect your PASSWORD. You are solely responsible for maintaining its confidentiality.

Create a password that is hard to guess

Ideally, a password should be easy for you to remember, while also being difficult to guess. It should not need to be written down. It should not be something obvious such as "password," your last name, names of family members (or pets), a license plate, or any sequence of numbers contained in your

SSN, SIN, or driver license. Good passwords contain a combination of characters, numbers, and special characters. While this is criteria for passwords is not absolutely required, it is recommended for any web-based application password you may have.

Do not leave your session unattended

Another person could use your computer while you are not at your desk. You should log off the application before leaving your desk.

Log off when you are done

Click the **Log Off** link and close your browser to ensure other persons do not have access to your information.

Choose your browser wisely

You should select a browser employing the highest level of encryption your system will allow to conduct secure transactions over the Internet.

Use caution when printing

Online information, including your pay advice, and other personal data, may be printed from your browser to a local or network printer. If you print on a shared/network printer, you are responsible for maintaining the confidentiality of your pay information, it is important that you immediately retrieve this information from the printer.

Upgrade your browser

It behooves the end user to use current browsers, as they are less susceptible to intrusion and typically support higher levels of encryption. The current, prevalent browsers from both Microsoft and Netscape both support 128-bit encryption. It is the responsibility of the client and/or end user to ensure that the browser being used provides the level of encryption desired.

Security Concerns

Information is the key asset to any organization, and therefore protecting this asset is of paramount importance to any organization regardless of industry. While in theory, outside threats present a general concern, internal security leaks are the most common way sensitive information leaves the organization. With the proliferation of ubiquitous high-speed connectivity and the need to have integrated organization information readily available and easily accessible, the internal information leakage is easier than ever, whether on purpose or even accidental. Therefore, strategic applications, which provide such sophisticated information integration, need to take special measures in lessening the ease of such security breaches.

There are several categories of business level security concerns the Maintenance Connection security architecture targets and solves.

Unauthorized Data Access

This is the most common and obvious line of defense. Management decides what person in what role (or access group) has the responsibility and the accountability to access and change specific organization information. Nobody outside those authorized should have access. Maintenance Connection enforces this policy by employing several layers of security measures as described in the previous sections:

- Authentication admits only users who have the appropriate credentials
- Filtered browsing eliminates the sharing of bookmarks or the inadvertent system access through long forgotten open sessions
- The role (or access group) assigned to the user enforces that only the designated Maintenance Connection features can be invoked and only specific data manipulations are allowed
- The data access filter defines the data realm in which the user can operate, given all the above conditions have been satisfied

Unauthorized Information Sharing

Despite all access security measures, authorized users can willfully or accidentally share sensitive data. Email systems offer the easiest method of information sharing. Sensitive information can be forwarded through file attachments or URL links. While data copy cannot be completely prevented, Maintenance Connection puts a roadblock in the way of unauthorized data or access sharing:

- Filtered browsing eliminates the possibility of someone forwarding a bookmark deep into the system and someone else being able to browse any Maintenance Connection pages without proper authorization.

This measure make it harder to share, but does not completely eliminate the possibility of someone taking a print-screen of sensitive information and sharing those with unauthorized users.

Unauthorized Data Changes Outside Of Process Boundaries

In highly structured and process driven operations environments, certain data changes and data access should be completely under management control.

For example, a manager may need to allow a user the ability to create a work order, but not approve, issue, or close it.

Maintenance Connection provides the capability to access at the process level.

Conclusions

The Maintenance Connection system has been designed with security as part of the foundation architecture. The combination of the 7 layers of security measures target specific security areas and in conjunction with one-another these layers address several high level organization related security concerns.

Maintenance Connection provides a rich environment and security foundation to allow organization's to control the granularity and severity of the security measures. With minimal configuration, Maintenance Connection can satisfy the most imminent security concerns.