jBASE Web Builder Security Features

INTRODUCTION

jBASE web builder is designed to enable developers to design and deploy secure and robust end-to-end transactional web applications in a short timescale. Security is of particular concern when applications are exposed on the world wide web, and several security features are built into web builder with this in mind.

WEB BUILDER ARCHITECTURE

Most application servers enable applications to store state and session information needed by their applications, and web builder is no exception. Many applications store their state by passing information via the URL or by the use of client side files called cookies.

Web Builder stores all state and session information on the server side in a powerful jBASE database to ensure rapid retrieval. The key needed to retrieve this information is a pseudo random hidden field which is passed to the user as part of the web page.

The hidden session key is a constantly varying value which is based on a PIN number stored on the server. The session key is completely unpredictable for any unauthorised user, and almost impossible to reverse engineer even if the server PIN number is compromised and the encryption algorithm is known.

On top of this, when a session is initiated in a web builder application, web builder captures the IP address of the client machine. This IP address is checked on every interaction with web builder so that it is difficult to 'hijack' the session.

Web Builder may be configured so as to block any caching of the pages that are produced. This means that no copy of a web builder page is stored either on the client machine, or any machine in between the client and the server. It is also possible to disable the forward and back buttons in the web browser itself, thus plugging a further loophole.

Full 128 bit PKI encryption is built into web builder and available for use by web builder applications. In addition, SSL can be installed on the web builder server adding a further layer of security.

APPLICATION SECURITY

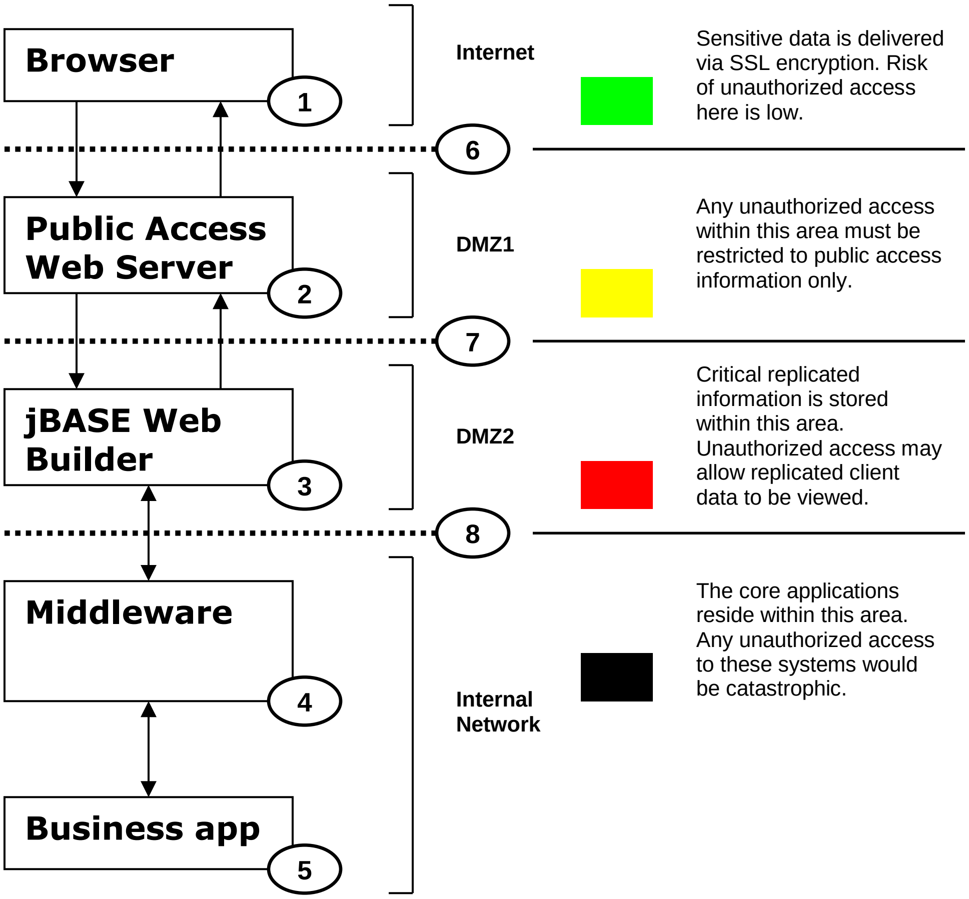
Web builder comes with user management built in, but also allows any third party repository or application to hold user information. In this way, operating system user credentials may be used or an LDAP store can hold the details of authorised users for the web builder application.

Each user is assigned a password which is encrypted by web builder. This password can be configured to time out after a period of time, and a fixed number of retries may be set up for incorrectly entered passwords.

Users are assigned to groups which helps to orgainise the privileges allowed for each user on each application. Every element of the application from a page, through collections of objects right down to individual components can be assigned a level of security. If a user does not have the correct credentials, the relevant elements of the page will not be downloaded to them.

APPLICATION SECURITY

For maximum security, it is recommended that web builder applications are implemented in the following manner



🟩 Sensitive data is delivered via SSL encryption. Risk of unauthorized access here is low.

🟨 Any unauthorized access within this area must be restricted to public access information only.

🟥 Critical replicated information is stored within this area. Unauthorized access may allow replicated client data to be viewed.

⬛ The core applications reside within this area. Any unauthorized access to these systems would be catastrophic.

Key elements

1. **Web Browser**

   Web browsers within the public Internet must be capable of running Microsoft Internet Explorer 4.0 or better, and must be capable of supporting 128bit SSL encryption.

2. **Public Access Web Server**

   This server acts as the public Internet site. This server must only contain static / non-critical information – and should not process any scripts related to the business logic.

   This server must be configured with a 128bit SSL certificate. All script calls to this server must be proxied to the jWB server. Proxy re-direction through the secondary firewall can be through any configurable TCP/IP port number. SSL encryption through the secondary firewall is an option – but will require an additional certificate for the jWB server.

   This server does not materially participate in the jWB submit / result cycle, other than to support SSL encryption and decryption of HTTPS traffic.

3. **jBASE Web Builder Server**

   This server must include web server software (unless configured for jWB Servlet interaction). The web server technologies for this server are as per the public access web server.

4. **Middleware**

   This server acts as a message re-director between the jWB server and the application server.

5. **Application Server**

6. **Internet Firewall**

7. **jWB / DMZ Firewall**

8. **Intranet Firewall**

Document Created 3rd January 2002
Author: Martin Bailey