INFOTEST EPR PROJECT: APPLICATION SECURITY

White Paper

The InfoTest Enhance Product Realization (EPR) Project

The InfoTest Enhanced Product Realization test-bed project was created to evaluate the business value of secure collaborative engineering over the Internet. The goal of the project is to demonstrate how collaborative technologies can enable an organization to streamline the product realization process by working more closely with its supplier and customers. In the project, WebEnable provided the secure dealer automation system through which customers and dealers participated in this product realization process – delivering "the voice of the customer" directly to the manufacturer's marketing and engineering organizations.

The Application Security Challenge

When considering security one often thinks only of network gateways to control Intranet access and machine user accounts to control system access. In the past even sophisticated security merely added control over network services and access control over entire files. When trusted employees were the only users allowed into your systems this level of security was sufficient. However, in this new age of Extranet access by third-party trading partners and collaborative supplier engineers, simple gateway and system security is necessary but not sufficient. To provide proper control over proprietary Intranet-based information we must also control access to individual applications, individual records within application databases, and even individual fields within those records.

WebEnable's Solution

WebEnable delivers Java-based web applications for sales and marketing automation. We specialize in supporting manufacturers who sell through dealers, multi-tier distribution chains and OEM relationships. For each of these types of sales channels the trading partner driving the sales process is a third-party organization only loosely associated with the manufacturer through contracts and business agreements. Yet, to optimize sales through those trading partners the manufacturer must be able to exchange a large amount of information. In the past this information has been exchanged as hard-copy catalogs, purchase orders, invoices, etc. This hard-copy information is not only expensive to generate, but also difficult to analyze and manage. This difficulty and expense limited the amount and value of the information exchanged.

The advent of Extranet technologies makes it possible to offer traditionally Intranet-oriented sales and marketing automation applications to Extranet trading partners. But, this can succeed only if there is sufficient security control over the applications and information the trading partners can access.

WebEnable's Sales Channel Automation System is built on a highly secure proprietary web application framework. This framework includes the following features:

WEB ENABLE

Application login security: WebEnable comes with simple username/password login security. However, we recognize that many companies have requirements for more sophisticated authentication mechanisms, including "single login" mechanisms. So, in addition to our native authentication we support plug-in authentication mechanisms allowing the customer to tailor authentication sophistication to their individual needs.

Application access: The WebEnable Server uses information in its user database to determine which applications an authenticated user is allow access. The user interfaces and associated application functionality for WebEnable applications are defined in meta-data that is interpreted by the WebEnable Application Display Applet. The WebEnable Server determines which applications the user is allowed to access and which user interface for each application the user is allowed to use. Only the meta-data for those accessible applications and their user interfaces is then downloaded to the users browser.

Record access: The WebEnable Server also uses information in its user database to determine which records the user is allowed to access. This record level access control not only constrains users from seeing inappropriate information, but also allows the customer to "personalize" the information display to the needs and desires of the user. (We use this feature for example to target the "specials" list in the Welcome application and to manage Workflow items.)

Field Access: The WebEnable application user interface meta-data includes the queries that deliver the application content to the browser. This query meta-data allows control over the fields to be returned in queries, and where and how those fields are to be displayed. For most users if you can't display it you can't access it.

InfoTest Details

For InfoTest, WebEnable has integrated the DASCOM WebSEAL authentication mechanism with the WebEnable Secure Application Framework. This allows the user to log in once to get secure access to both WebEnable and other DCE-enabled applications. DASCOM passes pre-authenticated username and group-name information to the WebEnable server at the time the user session is started. The WebEnable server then delivers the necessary application user interface and content information to the user's browser for their use during this session.

For the InfoTest project we have defined the following users and their individual access rights to applications and content:

Customers: The user "customer" has the least access to the WebEnable suite of applications, having access only to the Product Encyclopedia application, and within the application being shown only 4 of the many potential product property sheets ("tabs"). Any "unauthenticated" user is logged in with this level of access. This ensures that unauthenticated users are limited in their ability to discover what information they are *not* allowed to see. If you don't know it exists it is much harder to infer proprietary information.

Dealers: The user "dealer" has access to Welcome, Account Management, Opportunity Management, Sales Management, Cooperative Marketing Management, Product Encyclopedia, and Problem Management. Within the Product Encyclopedia the dealer has access to all product property sheets.

Marketing: The user "marketing" has access to Welcome, Account Management, Opportunity Management, Sales Management, Cooperative Marketing Management, and Product Encyclopedia. For demonstration purposes marketing does not have access to Problem Management.

Engineering: The user "engineering" has access to Welcome, Product Encyclopedia and Problem Management applications. The engineer also has access to the technical specifications associated with all parts (which is denied to all other users).

Supplier: The user "supplier" has access to Product Encyclopedia and Problem Management applications, but only has access to those products that the supplier supplies through the manufacturer. So, the supplier has access to problems with a specific part they supply, but not access to problems with the entire assembled product that contains that part.

Conclusions

The InfoTest project has successfully demonstrated the integration of multiple disparate secure Extranet applications to deliver collaborative solutions to customer requirements. In addition, it has shown that multiple organizations can exchange often proprietary information over the Extranet with fine grained control over who can access that information.