Hypothesis Eight

Is technology for security adequate?

Background

Shopping, requisitioning, and ordering in the EMall take place over the public Internet utilizing browsers and servers. It follows that ensuring the security and integrity of all activities and transactions is key to acceptance and widespread adoption of the EMall concept by all parties involved. Further, given that Users are conducting real buy-sell transactions during the EMall pilot, strong security is a prerequisite to the states' ability to exercise their fiduciary responsibilities to taxpayers.

Security Requirements for the EMall

There are two major categories of security requirements for the EMall. The first category includes the requirements specified by the Open Buying on the Internet (**OBI**) standard v1.1. The second category includes all the pre-existing security requirements encompassed by the business processes and systems infrastructure. These two sets of requirements are discussed briefly below. The EMall Operating Rules document provides a greater level of detail about these security requirements.

The OBI v1.1 specification requires the use of X.509 v3 digital certificates for certain communications between Buyers and Sellers. Specifically, authentication via digital certificates are required for Shopping sessions, also referred to as Requisitioning, and for Ordering, or sending back approved Orders to a Supplier. Specifications require that Communications during these sessions are secured via SSL3 encryption.

The business processes automated by the EMall and the network infrastructure within which the EMall exists have various pre-existing security requirements that must be integrated into the application. The business process security requirements encompass many business rules and internal control principles that assure the privacy and legitimacy of transactions conducted via the EMall.

Following are examples of business process security requirements:

- Shoppers can only view those items in a Supplier's catalog that correspond to the contracts and pricing agreements which the Supplier has with the Shopper's state.
- Only authorized Shoppers can complete Order Requests with Suppliers.

- Before an Order Request, or Requisition, can become a transmitted Order, it must be forwarded to and approved by as many authorized Approvers as each state's internal control procedures dictate.
- The application must maintain an audit trail of provable events to assist in any Order dispute resolution.

Participating states access the EMall server via the Internet. To maintain the security of the Commonwealth of Massachusetts' internal networks, the EMall application must comply with the Commonwealth's Public Access Architecture. Compliance with these requirements also insures that the EMall database is appropriately secured from possible infiltration from the Internet and other unauthorized users. Finally, the application must also take into account various security and internal control requirements dictated by back end systems such as payment and accounting applications.

Results

This section describes the actual security implementation for the pilot and identifies some of the major issues encountered. For ease of discussion the security implementation is divided into three categories – user authentication and authorization, server authentication and transmission security, and data security. It should be noted there is considerable overlap among these areas.

User Authentication and Authorization

User authentication ensures that access to the EMall is restricted to only authorized users. Authentication is also an integral part of access control or authorization that limits the types of activities individual Users are allowed to conduct, as well as insuring that unauthorized visitors are not allowed access to privileged information. However, it's important to remember that authentication and authorization are not the same thing and that one should not be confused with the other.

Authentication for access to the EMall server is implemented via browser certificates, also referred to in this document as client certificates, and via user ID and Password. This implementation provides "two-factor" security since it requires something you have, that is, the individual certificate, and something you know, that is, the user ID and Password. Authorization is handled by the EMall application utilizing the user ID and Password in combination with the access control database where roles and permissions are specified for each user.

Motorola provided client certificates for EMall users in its capacity as Certificate Manufacturer. The EMall project manager served as "Registrar," or the person from whom authorized users request certificates, and forwarded requests for certificates for authorized users to the Certificate Manufacturer. The Operating Rules, Section C, describes the Certificate Policy in detail. The Operating Rules are available at http://emall.isa.us/operatingrules.asp.

Following are the major user authentication and authorization issues encountered during the EMall pilot implementation.

- The public/private key pairs corresponding to the Motorola certificates were generated off site at Motorola and not on the User's PC. Consequently, Users with Microsoft Internet Explorer browsers were not able to employ the security feature that prompts a User for a password before they can access the certificate. For enhanced security, it is preferable for the keys to be generated and stored in the individual User's PC.

- The Motorola client certificates were sent to users in floppy disks via mail. A letter containing the access password was forwarded to the user separately. A faster and less costly solution is to provide an online request and access mechanism. This would improve not only the security of the certificates which can get lost on route or be delivered to the wrong recipient, but also would facilitate the management of users and certificates.

- A number of installation problems were encountered when loading client certificates into PCs. Most of these problems could be traced back to browser versions and, in the case of Microsoft Internet Explorer, the need for registry edits. To enhance security and for compatibility with the Motorola certificates, specific versions of 128 bit browsers were required. This meant that most users had to upgrade or reload browsers. Microsoft Internet Explorer further required that edits be done on the system registry after browser installation. All this required system staff intervention, thereby increasing resource costs as well as creating another potential security problem. In some states, after securing the correct browser environment, system staff went on to load the certificates for users compromising the secrecy of the user's certificate password.
- The IEC application version used for the EMall does not have password expiration parameters nor does it have rules regarding minimum password length. Both these features would enhance authentication and authorization security.

Server Authentication and Transmission Security

In order to ensure message and session privacy, server certificates are installed in the EMall server and Supplier servers to enable Secure Sockets Layer (**SSL**) encryption. To ease implementation on the part of Suppliers, a Certificate Authority (**CA**) whose root is widely recognized by most browsers issued the EMall server certificate. Likewise, it is expected that widely recognized CA's also issue certificates installed in Supplier servers to avoid having to import special roots into the EMall server. While these so-called "public label certificates" do ease distribution of the root certificate, they also raise concerns regarding bounding the community of trust among business partners (see Hypothesis Nine).

The OBI v1.1 specification requires that communications during certain sessions between Buyers and Sellers be authenticated and encrypted via SSL3. SSL3 requires mutual authentication between browser and server (please see http://home.netscape.com/eng/ssl3/ for more detailed information). The sessions that require SSL3 are Shopping sessions and Ordering. Because the EMall server is accessible to Users in participating states via the Internet, the initial user log-in session is also authenticated and encrypted using SSL3.

A number of issues were encountered in the implementation of server authentication and transmission security. These issues could be traced back to a lack of documentation and functionality regarding the IEC Enterprise software version used in the EMall's handling of SSL3 sessions as dictated by the OBI specification as well as customization required by the EMall's need to secure user log-ins via SSL3. In addition, some of the issues encountered were due to the idiosyncrasies of the various Web servers used by Suppliers and their varying treatment of CA roots. Following are the major issues encountered:

- The EMall implementation of the IEC Enterprise application was the first instance where a server certificate was utilized with this product. The implementation was problematic requiring Internet Explorer v3.0 for installation while Internet Explorer v4.0 was required for the operation of the IEC application.

- When a user attempts to log into the EMall, the application takes the client certificate's common name and matches it against a valid user name in the application database. However, initially the application did not check the CA name to verify that the EMall authorized certificate issuer supplied the client certificate. This functionality had to be programmed.

- There was one instance in which a Supplier used a server certificate that was issued internally and not generally recognized by the EMall server. The certificate's root had to be imported into the EMall server.

- The implementation of SSL3 for Order transmissions from the EMall to a Supplier was very problematic. It was assumed that the presence of server certificates on both the EMall Server and the Supplier server would be sufficient to establish the SSL3 sessions. However, after several weeks of unsuccessful transmissions and trouble-shooting with the Suppliers involved, it was discovered that the IEC application on the EMall server needed a client certificate in addition to the server certificate. This undocumented requirement necessitated the creation of an "Intelysis Service" user account to associate with the client certificate and the creation of a new NT user profile.

- Motorola manufactured the User certificates employed in the EMall. Since Motorola's root is not generally available in browsers and Web servers, Suppliers had to install the root in their servers. Some early versions of Web servers could not install the subordinate EMall root and instead required installation of the original Motorola root. This highlighted the importance of specifying baseline Web application versions for Suppliers.

- SSL3 sessions by themselves do not verify identity or authenticate users. Once the client and server recognize each other's certificates as being "trusted" and keys are exchanged, the encrypted session can begin. To verify identity and use other information contained in the client certificate, the application on the server must be programmed to "parse" the certificate. OBI recommends that the Supplier use the common name and organization information to authenticate Shoppers and establish the appropriate catalog profile. The majority of EMall pilot suppliers chose not to incur the additional development costs entailed by parsing certificate information. Only four EMall Suppliers are parsing the certificate information during the pilot. Instead, User information contained in the IEC application database is used to identify users and to route them to appropriate catalog profiles.

- A similar issue was encountered during SSL3 sessions established to secure the sending of transactions between Supplier servers and the EMall server. Suppliers should be parsing the EMall client certificate to authenticate the identity of the server. No Supplier is parsing certificates for verifying server identity as part of the transmission of transactions during the pilot.

Data Security

The EMall databases are stored in a server located inside the internal firewall that does not permit in-bound HTTP traffic from external sources. These databases are physically separate from the EMall application server located in the DMZ. One issue of concern was identified through the pilot experience and is described below. We believe this issue is now satisfactorily addressed in a subsequent version of IEC Enterprise:

- Changes made by administrators to the databases are not audited by the application. This affects both our ability to execute change control and to create an audit trail of changes to the databases.

Was the security implementation adequate?

Before this question can be addressed fully it is important to remember that the EMall pilot implementation utilized two layers of often-redundant security. The first layer was provided by the security features of the IEC application such as user IDs and passwords, access control lists, and hidden code transmitted during transactions. The second layer was provided by the use of client and server certificates as specified in the OBI v.1.1 specification.

Given this scenario, we can say that the security implementation was adequate with a few issues identified above concerning functionality limitations of the IEC Enterprise application version used in the pilot. Given the closed nature of the EMall community and the identification of identities and roles for each EMall participant within the IEC application databases, the use of client and server certificates, other than for the establishment of SSL2 encryption, seems a bit redundant. In fact, during the pilot only four of the participating Suppliers chose to parse client certificates for identity information and state affiliation.

The most significant security flaw encountered during the pilot involves the possibility of internal threats due to the fact that the application does not audit administrative changes. As mentioned previously, this limitation has been addressed in subsequent versions of the application.

Summary

While the OBI v.1.1 specification requires the use of certificates during Shopping Sessions and Order transmissions, the value certificates add above and beyond the security features of the IEC application is questionable. The authentication and access control features of the application appear to be sufficient to satisfy the identified security requirements. The only exception to this is the encryption function (SSL2) that server certificates make possible which is crucial in securing transmissions that are conducted via the Internet. This function, however, does not require the use of client certificates.

Our experience with certificates during the EMall pilot has reinforced several impressions from previous experiences with pilot certificate implementations to date:

- The operating environments within which certificates function are of prime importance. Browser versions, Web server software versions and application characteristics all play important roles in determining whether certificates will load and operate as intended.
- The application programming required to parse certificates so that their contents can be used for authentication and other purposes is not trivial and requires additional resource commitments on the part of business partners.
- The management of certificates (including request, issuing, installation, revocation and audit trails) is also not trivial. Management overhead is eased to the extent that processes can be automated.
- The amount of support required by users and business partners during certificate implementations is considerable.

In conclusion, while the non-certificate technology for security is adequate for the implementation of the EMall, the use of certificates for security (other than SSL2 encryption) is a resource-intensive endeavor, is not seamless and requires considerable custom programming. Further, the authentication functionality provided by certificates appears to be redundant with the security functionality available in the application.

Recommendations

1.Security Administration Should be Decentralized

The administrative approach to security was very centralized in the pilot. The management and technical aspects of security administration will have to be distributed in a production system in order to make it more manageable and efficient. Specifically,

- The EMall production system's technical architecture should reflect distributed responsibilities for user authentication.
- A set of flexible but minimum standards for user identity proofing should be made part of the Operating Rules.

2.Client Certificate Implementation Should be Reconsidered

Given the onerous nature of implementing client certificates, as evidenced by the need for increased local technical staff support, inordinate central administrative support and significant additional custom coding needed to provide core functionality, the advisability of end-user certificate implementation as part of the EMall should be re-considered. The following issues should be kept in mind:

- In the context of a sound, distributed organization-to-organization security system utilizing protocols such as IP-Sec, client certificates to authenticate individual Buyers to external Suppliers may be unnecessary.
- The cost of a full-blown client certificate "solution" must be weighed against both the benefit provided by this redundant level of security and the business and legal risks resulting from breaches to authentication mechanisms. It should be noted that other potential benefits derived from client certificates such as confidentiality, non-repudiation, and message integrity are provided in the EMall by a variety of other application, system and legal rules.
- Should the EMall production system continue to support the OBI standards, the Commonwealth, as a member of the OBI Consortium, should communicate the potential need to revise the certificate requirements in view of our difficult experience in implementing this aspect of version 1.1 of the OBI standard.