



Wednesday, March 13th, 2002

Accelerating Security Policies thru Middleware

by Robert Lendvai

As the lines dividing intranets and extranets continue to blur, companies like yours are rushing to expose private network applications and information assets to customers, business partners and employees.

In many cases, your need to share applications and services extends beyond simple web applications to legacy services running on mainframes. Your company has invested in applications accessed with TN3270, Oracle SQL*Net applications, Microsoft NetBIOS applications like Microsoft Office and Lotus Notes, or any other TCP/IP or UDP application. Additionally, your business needs to support a broad mix of application server operating system platforms comprising mainframes, UNIX servers, and Novell and Microsoft.NET servers.

Exposing your private network to the Internet introduces a number of new issues for organizations. To address these, you need to consider a common set of security policies.

Historically security technologies, both physical and virtual, essentially operated as a perimeter defense to corporate resources. In contrast, Internet security policies can act as an e-business-enabling technology that assumes open access to corporate resources but provides the following seven essential security requirements.

- Strong three-factor user authentication (possession, knowledge, third-party verification).
- Digital signatures on transactions (business transactions, administration transactions, file operation transactions, object transactions, etc.).
- Confidentiality of information being transmitted.
- Integrity of information being transmitted.
- Monitoring and logging of network activity.
- Certificate validation.
- Authorization of specific users to specific applications and resources.

Enter PKI

It has been widely accepted that currently, public key infrastructure (PKI) is the only technology that can provide the necessary foundation and building blocks to implement all seven of the e-security policies for e-business applications. But as the name suggests, PKI is just infrastructure and by itself does not enable trusted e-business. This sets the stage for new e-security models that are being developed in an attempt to unlock the power of PKI to enable the delivery of successful e-business applications.

You'll need to decide between two fundamental strategies to securing your e-business - secure the network or secure your applications.

Securing the E-Business Network

IP security, or IPsec, is the industry standard protocol for securing the IP network between two points, more commonly referred to as a virtual private network (VPN). IPsec provides crypto-based authentication, integrity and confidentiality services at the IP layer. IPsec does not concern itself with, and is transparent to, the users, applications and protocols being used for e-business. IPsec provides protection for all client protocols residing above the IP layer.

Your company probably uses IPsec to create low-cost secure networks over the Internet. Common applications include employee remote access or inter-branch communications. Since IPsec is not cognizant of users, applications, and protocols, IPsec is not able to support some of the fundamental e-security requirements necessary for many e-business applications. In particular, IPsec is grossly deficient in the following areas:

- cannot provide digital signatures for transaction non-repudiation;
- cannot perform content inspection for interpreting an application's datastream for policy implementation;
- cannot authenticate individual users as required by an application operating within the VPN;
- cannot authorize specific individuals to specific e-business applications or other IT resources.

Securing Web Applications

The de-facto standard for providing security for web-based applications is the secure sockets layer (SSL) developed by Netscape and now supported by all popular browsers. SSL provides the following security features:

- confidentiality;
- integrity;
- server authentication (optional);
- client authentication (optional).

SSL is best applied when an e-business service provider does not need to have a great deal of trust in a user. A credit card is usually the means of validating a user for e-commerce purchases, thus client authentication is rarely used. When authentication is required, it is typically implemented by a username/password. The use of digital certificates within the browser is currently a complex process requiring significant knowledge on how they can be used. Protection of the private network is obtained by isolating the web servers from the private network in a demilitarized zone, so authorization, monitoring and logging is also less significant.

As is the case with IPsec, SSL within the browser is not able to support some of the fundamental e-security requirements necessary for many e-business applications. In particular, SSL is deficient in the following areas:

- Client authentication requires a user to engage in the complex process of using certificates within the web browser.
- SSL does not provide digital signatures for non-repudiation of e-business transactions.
- SSL certificate validation is not widely supported. Standard browsers rely on non-standard proprietary certificate extensions to facilitate certificate validation that is not widely supported in the industry.
- Most web servers do not provide the monitoring and logging and access control authorization protections required for e-business.

To effectively implement all seven of the e-security requirements within the web model, first, some form of client software is required in addition to the web browser to provide a more transparent use of digital certificates for client authentication, and to provide a capability for use of digital signatures. Second, some form of server software is required in addition to the web server to provide certificate validation, monitoring and logging, and granular access control down to the page or URL level.

At its simplest, you can accomplish this with a proxy or java applet on the client desktop to perform the certificate authentication for each connection and a digital signature on every http "post" command. A web proxy or java applet on the web server can perform certificate validation, and monitoring and logging of web connections. When combined with a simple database of usernames and permissions, authorization can be implemented.

Securing Non-Web Applications

SSL support within the web browser, although limited, provides the basis of an e-security infrastructure for your web applications. It is much more difficult to provide e-security for non-web or legacy applications, since alternate client software is required in the absence of the web browser. You can PKI-enable non-web applications two ways - with PKI toolkits from vendors such as Entrust, Baltimore and VeriSign that require you to make extensive and costly changes to your applications so that they'll can provide support for SSL support directly from within the application, or use PKI-middleware to provide the SSL support on behalf of the application.

Although toolkits appear to provide the most flexibility, there are several disadvantages to this approach.

- They are labor intensive - both the initial implementation as well as ongoing support. In fact, some companies have reported that some applications have required more than a year's work to be PKI-enabled.
- Time to market is usually delayed as compared to alternate approaches.
- It requires PKI and security development expertise on staff.
- Toolkits are generally not available for mainframe legacy applications.
- Applications are bound to a particular PKI vendor, their licensing, standards interpretation, interoperability and support strategies.
- It requires access to source code, so commercial applications cannot be supported without the vendor involvement.

Therefore, toolkits are best used by large software vendors to PKI-enable their commercial application or in some cases pilot projects. Toolkits are not well suited for wide-scale enterprise deployment.

Tying it Together with Middleware

E-security middleware is a similar approach to using a browser to implement SSL security services on behalf of web applications. However, the middleware client software is providing the SSL services on behalf of all applications, including web applications. Well implemented e-security middleware will require no user configuration or training, will provide all essential e-security services for all application protocols including Microsoft networking applications (NetBIOS) like Microsoft Office and Lotus Notes, and will support the use of digital signatures and content inspection policy extensions for any application on the desktop.

E-security middleware relieves you from having to deal with the complexities of PKI integration and development using toolkits. In most cases, middleware ensures that not a single line of code needs to be developed. All applications, both legacy and commercial, become PKI-neutral, allowing the use of digital certificates from any combination of PKI vendors and delivering the foundation and building blocks to implement all seven of the e-security policies for e-business applications.

Robert Lendvai is vice president of marketing at Kyberpass Corporation. He can be reached at rlendvai@kyberpass.com



Copyright © West Coast Publishing. All rights reserved.