

Wed, Jun 6, 2001

SEARCH

advanced | help

mobile | subscribe | about | contacts

TOP ISSUES

- E-business
- Integrating IT
- IT Infrastructure
- Network Technology
- Voice, Data and IP
- Intranets/Extranets
- Data Management
- Skills Management
- E-Government

RESOURCES

- Bookstore
- White Papers
- Product Reviews
- Online Store
- Job Universe

PUBLICATIONS

- CIO Canada
- CXO.ca
- ComputerWorld
- Network World
- Lac Carling
- IT World Print

EVENTS

- ITX Awards
- Network World ~Live!
- Computerworld ~Live!
- WhitePaper Seminars

NEWS

- Daily ITwire
- Global Newswatch

COMMUNITY

- Industry Calendar



[Main](#) | [Current Issue](#) | [Archives](#) | [Editorial Calendar](#)

Making it safe to do business on-line

By Kevin Reeks

As the global market evolves towards a more comprehensive e-business environment, companies must open their private network applications and information assets to customers, business partners and employees. This e-business environment is commonly referred to as an extranet. To have true impact within most organizations, the extranet must encompass more than just web applications. A company may have investments in mainframe applications. The extranet must also support a heterogeneous mix of application server operating system platforms.

Opening up a private network for e-business introduces a number of new issues for organizations. In the past, traditional security technologies, both physical and electronic, essentially operated as a perimeter defense to corporate resources. In contrast, e-security is an e-business enabling technology that assumes open access to corporate resources but provides the following essential security requirements:

BULLET: Strong three-factor user authentication (possession, knowledge, third party verification);

BULLET: Digital signatures on transactions (business transactions, administration transactions, file operation transactions, object transactions, etc.);

BULLET: Confidentiality of information being transmitted;

BULLET: Integrity of information being transmitted;

BULLET: Monitoring and logging of network activity;

BULLET: Certificate validation; and

BULLET: Authorization of specific users to specific applications and resources.

It has been widely accepted that 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 elements for e-business applications. But PKI by itself does not provide e-security. 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 e-business applications.

Organizations must decide between two fundamental strategies to secure e-business: securing the e-business network or securing the e-business applications. The choice will depend on their e-business requirements.

SECURING 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 cryptographically based authentication, integrity and confidentiality services at the IP layer. IPSec does not concern itself 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.

IPSec is typically used to create secure networks between two computers or networks over insecure means of transmission such as the Internet. Typical applications are connecting branch offices over the Internet, or employee remote access using Internet Service Providers (ISP) rather than long distance dial-up lines. Using VPNs, companies can save money in terms of the costs of leased lines and dial-up lines while maintaining the confidentiality of corporate information.

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.

SECURING APPLICATIONS

The de-facto standard for providing security for Web-based applications is the Secure Sockets Layer (SSL) developed by Netscape. The Internet Engineering Task Force (IETF) protocol is currently standardizing version 3 of SSL as the Transport Layer Security (TLS). SSL is the mechanism supported by most web browsers and servers including Microsoft Internet Explorer and Netscape Navigator/Communicator.

SSL is best applied when an e-business service provider does not need to have a great



Sign up now!!

Subscribe to your choice of our print editions.

It's easy and It's FREE!!!

POWER PURCHASE

\$159

LG Electronics - MP3 Player 32MB with Remote

COMPARISON PRICING:

- Onvia = \$209
- Software Online = \$208
- NCIX.com = \$202
- Power Purchase = \$159

Average Savings: **\$47 or 23%**

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.

To effectively implement all seven of the e-security requirements within the web model, some form of client software is required to provide a more transparent use of digital certificates for client authentication, and to provide a capability for use of digital signatures. 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.

In the simplest form, this is accomplished with a simple 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. This is the easiest form of market entry.

It is much more difficult to provide e-security for non-web applications, since alternate client software is required in the absence of the web browser. There are essentially two approaches:

BULLET: Use PKI toolkits from vendors such as Entrust, Baltimore and VeriSign to write the software that will provide SSL support for the application directly; or

BULLET: Use PKI-middleware to provide the SSL support on behalf of the application.

Although toolkits provide the most flexibility, there are several disadvantages to this approach. It is labor intensive - both the initial implementation as well as ongoing support. 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. Access to source code is required, so commercial applications cannot be supported without the vendor involvement.

Therefore, toolkits are best used for PKI-enabling a vendor's commercial application (e.g.: Lotus Notes), experimentation, and pilot projects. Toolkits are not well suited for wide scale enterprise deployment.

E-security middleware is a similar approach to using a browser to implement SSL security services on behalf of web applications. However, in this case, the middleware client software on behalf of all applications, including web applications, is providing the SSL services. 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 the customer from having to deal with the complexities of PKI integration and development using toolkits for their applications, acquiring PKI-enabled commercial applications they may be using. 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 PKI vendor, or combination of vendors.

- 30 -

Kevin Reeks is director, Product Management, for the Ottawa-based Kyberpass Corporation which has won an award for e-security infrastructure for e-business and legacy applications. www.kyberpass.com

CUTLINE:

E-security involves a set of seven fundamental e-business security requirements.

