



INTERNET SECURITY

Introduction to Internet security standards

By [Ron Herardian](#)

As businesses move to take advantage of collaborative computing and electronic commerce on the Internet, data security has been a growing area of interest. Although there are undoubtedly more data security related products and services available today than ever before there are also more security related incidents each year. The rapid growth of the Internet and the constant introduction of new technologies, while creating new opportunities for businesses, also create new opportunities for hackers.

For the Internet, security was an afterthought. It is often said that the Internet was not designed with security in mind. The Internet is composed of many different technologies and is inherently open. Openness was one of the design goals behind basic Internet technologies like TCP/IP, which is a hardware and network independent protocol. While this enables any computer or network to be connected to the Internet it also makes it easy for hackers to attempt break-ins while at the same time making them hard to trace.

The rise in the complexity and diversity of the Internet has caused the need for security expertise to exceed the supply. As a result, inexperienced technical staff often implement security measures that are vulnerable to hackers.

On the Internet, hackers don't always need to break in to access confidential information since much of the traffic on the Internet is not encrypted. Encryption has been a growing area of activity in the past few years and today intranets, extranets, and email all involve some type of security. Developing Internet standards have come to drive security technology.

The purpose of this article is to familiarize you with the basic Internet security technologies. Over the next few months we'll look at Domino's historical security model and contrast this with the emerging Internet standards-based security technologies that will be integrated into Domino 5.0 and beyond.

Encryption

The best place to start is with encryption. Encryption means that information is scrambled so that only authorized people or systems can understand it. Understanding encrypted information requires decrypting it. For example, substituting numbers for letters is a primitive form of encryption. To decrypt the information you have to know what numbers represent what letters. In this example, the mapping of letters to numbers is a simple encryption key used to guarantee the privacy of information.

An encryption key is information (a string of alphanumeric characters) that is used to encode or decode information. The difficulty lies in telling people who need to decrypt information what the encryption key is. The most secure way of handling this is to use a public encryption key to encode information in such a way that only a different, private encryption key can decode it. In other words if I send a note to you, I encrypt it with your public key which is available to everyone but only you can decrypt the note using your private key. This is called Public Key encryption. Public Key encryption is good because public keys can be made available over the Internet and through directory services.

Deploying and managing public and private keys requires a framework for managing security information. Such a framework is called Public Key Infrastructure or PKI. For several years Domino was practically the only messaging and groupware system providing a PKI and PKI management tools, but it was implemented with

proprietary RSA technology. The Notes ID with which all Notes administrators are familiar is actually a form of digital certificate containing public and private encryption keys. The most popular implementation of Public Key encryption for email is Secure Multipurpose Internet Mail Extensions or S/MIME.

S/MIME provides end-to-end Public Key encryption for email messages. A message encrypted by the sender can only be decrypted by the recipient. At no time during the transmission or routing of the message is the message stored unencrypted nor does any user or administrator have access to the content of the message. Through digital signatures, S/MIME also provides sender authentication and tamper detection.

Today, Internet standards-based security technologies dominate the market. Vendors which had previously lacked a security model equivalent to that of Domino have now implemented similar security models using Internet standards-based technologies. At the same time, competition is taking shape around the business of providing enterprise (intranet) and inter-enterprise (extranet) PKI management facilities. In a sense Domino has a head start but Lotus faces the challenge of integrating Internet standards-based security technology with its existing security model.

Digital certificates

Digital certificates are widely used for Internet applications and I mentioned that the Notes ID is a proprietary form of digital certificate. The Internet standard for digital certificates is X.509. Like the Notes ID, the X.509 certificate contains a user's public and private keys. Certificates are used in several ways including Public Key encryption, digital signature (a way of verifying the originator of information), and to establish trust between applications or organizations based on the issuer of the certificate (the Certificate Authority or CA). A certification authority (CA) is a trusted third party authorized to issue digital certificates.

A certificate consists of a public key signed by a trusted third party or Certificate Authority. Certificates make it possible for different users to trust one another's public keys. X.509 certificates are an electronic credential like a government-issued ID or passport. A certificate can be used to access an intranet or extranet application. For example, in order to log in to a system a client application such as a web browser presents the user's certificate to the system and uses it for authentication and access control. Information for external users, such as a business partner, can be made available to users whose certificates were issued by the organization for that purpose.

Certificates can be revoked or they may expire. Key escrow entrusts certificates to the third party so that an organization can retrieve information that may have been encrypted maliciously.

Secure sockets layer

On the web, the most popular type of encryption is the Secure Sockets Layer (SSL) which encrypts data within the TCP/IP protocol. Published by Netscape Communications, SSL provides secure web client and server communications including encryption, authentication, integrity checking for a TCP/IP connection.

Conventional intranet and extranet applications typically use a combination of security mechanisms that include:

- Encryption
- Authentication
- Access Control

Authentication means there is a mechanism in place to verify that an entity accessing information is permitted to do so. The best example is a login ID and password but there are other types of authentication. One example is verifying the network address of a connecting host. Authentication is like a gate. Once a user passes through the gate there are secondary controls (Domino Access Control Lists or ACLs) that determine what information may be accessed or manipulated.

In summary, encryption applies to the connection or transport (such as SSL) or to other data (S/MIME for email). A document or application may be digitally signed to prove the identity of the originator. X.509 certificates provide Public Key encryption and digital signatures just as the Notes ID does within the proprietary Notes and Domino security model. Authentication provides a gate through which only authorized users may pass and access controls determine what information may be accessed or manipulated by a given user.

Playing a key role in the proliferation of PKIs is the Lightweight Directory Access Protocol (LDAP). LDAP directories are used to provide a facility for access to the Public Keys of users and to store access control information. The Domino Name and Address Book (NAB) is accessible through LDAP. In coming version we can expect to see tighter integration of the Domino NAB with LDAP and integration of X.509 certificates with existing Domino PKI. Since Domino provides a complete PKI management solution extending this technology to fully embrace Internet security standards is a natural step.

Ron Herardian is CEO and Chief Technical Consultant at Global System Services (GSS). You can reach him via E-mail at rherardi@gssnet.com. Visit his web page at <http://www.gssnet.com>.

Copyright © 1998-2008, [ZATZ Publishing](#). All rights reserved worldwide.