Notes.net

Iris Today

by
Katherine
Spanbauer

Level: All
Works with: All
Updated: 09/04/2001

Right from the start, security has been a integral part of Notes and Domino. Here's a quick history of the evolution of security features.

1989: Notes Release 1.0

From the first release, keeping data secure was a priority. The security features introduced in this release were made possible by the incorporation of public key technology, licensed from RSA Security. Notes uses ID files and certificates to manage the identities of certifiers, servers, and users. These ID files are protected with passwords. Based on a user's authenticated identity, access to data is then controlled at the server, database, view, document, and field level. Privileges, defined within a database ACL, allow you to further refine access based on roles. Use of public key technology enables the use of mail signing and encryption, as well as encryption of traffic over the network.

The security features of the first release of Notes included:

- User IDs with passwords
- Public and private keys
- Certificates
- Mail signing and encryption
- ACLs/privileges
- Port encryption

1991: Notes Release 2.0

For the second release of Notes, security enhancements focused on extending the encryption technology. The use of secret key (or symmetric) encryption enabled the use of encryption for documents stored in databases in addition to the use of public key encryption supported for mail encryption. Key features included:

- Document encryption
- Secret encryption keys

1993: Notes Release 3.0

As Notes developed into a scalable, cross-platform product, security features were added to support deployment across an organization. To improve manageability of the Notes public key infrastructure, hierarchical certificates were introduced. These certificates allow for the definition of distinguished names based on X.500. For workflow applications, the ability to design forms to support multiple user signatures was added. Access controls were extended to the document level and allowed for more granular control over reading and editing documents in a database. Roles superseded privileges in the database ACL and allowed the definition of 75 roles per database (versus 5 for privileges).

Key features included:

- Hierarchical certificates
- Distinguished names
- Multiple signatures
- Roles
- Reader Names/Author Names fields
- Read and Compose Access Lists

1996: Notes Release 4.0

Delivered in January 1996, Notes Release 4.0 was a quantum leap forward both in terms of a completely redesigned user interface and because of new Web technologies incorporated into the server. Security developments focused on securing copies of local databases and enhancing protection for ID files. The ability to access servers via Notes anonymously was added to allow public access to Notes databases over the Internet without the need for cross-certification between organizations. The ability to encrypt database designs was introduced to allow developers and partners to protect their intellectual capital.

New security features included:

- Local database encryption
- Database design encryption
- Multiple passwords for IDs
- Password guessing evasion for IDs
- Anonymous access

1996: Notes and Domino Release 4.5

By the end of 1996, the evolution of the Domino Web application server was complete, allowing for development of both Internet and intranet applications. New security features to support this functionality were added while existing security features were enhanced and fine-tuned. Support for SSL was added to both the client and server. The Notes authentication protocol was enhanced to allow for password checking, password expiration, and the locking out of user IDs. In addition to the option for using secret keys to encrypt documents, encryption using public keys was supported. This reduces the requirement for managing keys. Execution Control Lists (ECLs) were introduced to protect workstations against the execution of potentially malicious code. In order to enable this feature, all design elements are now digitally signed when saved. The ECL limits the actions of formulas and scripts when they run on a workstation, based on the rights assigned for that signature.

Key features included:

- SSL (Secure Sockets Layer) 2.0 support for Notes client and Domino server
- Execution Control Lists (ECLs)
- Public key encryption in documents
- Password checking and ID lockout
- Password expiration

1997: Notes and Domino Release 4.6

Release 4.6 focused on enhancing Internet standards support. SSL support for the Notes client and Domino server was upgraded to SSLv3. The Domino Certificate Authority application gave administrators the option to issue standard X.509v3 client and server certificates.

- SSLv3 (HTTP)
- Certificate authority application

1999: Notes and Domino Release 5.0

With R5, security continued evolving to keep pace with changes in technology, including support for up-to-date standards and the needs of those administering global enterprise systems. Web server authentication was enhanced by adding options for session-based authentication and the Domino Web Server API (DSAPI). Session-based authentication uses cookies to manage authenticated user sessions and allows for the use of custom login forms and session time-outs. DSAPI filters can be developed to further customize authentication with the Web server. SSLv3 support was extended to all the Internet protocols that Domino supports: LDAP, POP3, IMAP, NNTP, and IIOP, in addition to the existing support for HTTP.

S/MIMEv2 support was added to the Notes client to enable mail signing and encryption to other users of other Internet mail clients. Password quality replaced password length for determining acceptable passwords. This algorithm was designed to help users choose better passwords to protect their Notes ID file. To ease administrative burdens when users forget their Notes ID passwords, a method for the recovery of user ID files was added.

New security features in R5 included:
- S/MIME
- SSLv3 for all Internet protocols
- ID and password recovery for Notes users
- Password quality
- Session-based Web authentication
- Web server authentication interface (DSAPI)

1999 to 2001: Notes and Domino R5 maintenance releases

Throughout the R5 maintenance releases and updates, particular security features have been fine-tuned in response to user's needs. For more information about any of these features, see the appropriate **Release Notes**.

1999 (Q3) Release 5.0.1 features included:
- Importing of Internet X.509v3 certificates into the Notes ID file using PKCS#12
- Dual key support of Internet certificates

1999 (Q4) Release 5.0.2 features included:
- Exporting of Internet X.509v3 certificates from the Notes ID file using PKCS#12
- More restrictive ECL permission defaults

2000 (Q2) Release 5.0.4 features included:
- Notes and Domino consolidated to a global encryption as export regulations are relaxed by the U.S. Government

2000 (Q3) Release 5.0.5 features included:
- Workstation ECL Refresh button added to User Preferences
- Single sign-on across Domino Web servers
- Single sign-on with WebSphere Application Server 3.5

2000 (Q4) Release 5.0.6 features included:
- Option in the Sign a Database tool to sign databases with the server's ID file, using the Administration Process

Coming soon: Notes and Domino Rnext

The next major release of Notes and Domino is well under way. Here are some of the security-related features planned for Rnext:
- User Security dialog box, which consolidates security preferences and options
- Logout screen, which appears when a user locks their ID file
- Notes client support for the PKCS#11 standard for smartcards
- Support for S/MIMEv3 capabilities
- Integrated Certificate Authority for registration of Notes and Internet users
- Enhanced password management features for both Notes and Internet passwords
- Synchronization of Notes ID and Internet passwords
- Dynamic update of ECLs

ABOUT THE AUTHOR

Katherine Spanbauer is the Product Manager for Security, primarily focusing on Notes and Domino. Her current responsibilities include representing customer requirements to development, triaging critical issues, and communicating product features both within Lotus and to customers. Since joining Lotus in 1992, she has held various roles in the Technical Support, Professional Services and Product Management organizations. Katherine is a graduate of the University of Wisconsin, where she earned her Bachelor of Business Administration degree.

