Domino and Notes Security

Session 8651

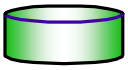
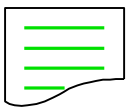
SHARE Nashville - 2002

Patricia Egen
pregen@egenconsulting.com

Agenda

- Notes security hierarchy
- Authentication
- Userids
- Certifications
- Access Control (ACL's)
- Application security
- Encryption

Layers of Security

Network		Firewalls
Server		Server ACLs
Database		Database ACLs
Forms/Views		Form/View ACLs
Documents		Reader/Author Fields
Fields		Encryption

Authentication (Who Goes There?)

- How can a Domino server learn who you are?
  - User Name and Password
    - Notes and Internet
    - Internet password is different than the Notes password
    - The Notes password is full RSA encryption
  - Certificate and Cryptographic Exchange
    - Notes Certificate from a Notes Client
    - X. 509v3 Certificate from a Browser

Notes uses two kinds of keys - Notes and Internet.

Why Passwords can cause problems

- Server must have (or be able to access) a database of passwords
- Passwords can be sniffed from the wire or stolen from servers
- Passwords can be guessed
- Hard to guess passwords are also hard to remember

Authentication

- ID file contains:
  - User/server name and password
  - Creation/expiration info
  - License number
  - Certificates
  - Public key
  - Private key
  - Encryption key(s)
- ID files whose certificates share a common ancestor can authenticate with each other

Public keys are not secret. Any user may look up another user's public key and use it to send encrypted mail to or authenticate the user. It is important that someone looking up a public key learn it reliably since Domino uses it for identification. Users must be able to obtain the public key of the certifier that issued the certificate before they can authenticate the certificate's owner. If a user has a certificate issued by the same certifier as another user or server, the first user can verify the public key for the certificate and then reliably know the public key associated with the server or user name. If a user doesn't have a certificate issued by the same certifier, the user needs a cross-certificate for authentication.

When you register users and servers, Domino automatically creates a Notes certificate for each user and server ID. In addition, you can create Internet certificates for user IDs using a Domino or third-party certificate authority (CA). Domino creates Internet certificates using the x.509 certificate format.

Notes certificates have expiration dates. Therefore, you must recertify Notes IDs when their expiration dates approach. In addition, if a user or server name changes, you must recertify the corresponding Notes ID so that a new certificate will bind the public key to the new name. However, changing a name on a user ID does not affect Internet certificates.

How certificates work

- Every user and server has an unguessable "private key" - "I authorize and trust you"
- A user's private key is stored in a Notes ID file or Browser Keyring encrypted with a password
- A certificate associates the user's "public key" with a name
- Your password never leaves your desktop, and is useless without files stored on your desktop
- A Domino Server can learn your name with no database other than the certifier's public key

A certificate is a unique electronic stamp that identifies a user or server. Server and user IDs contain one or more Notes certificates. In addition, user IDs may contain an Internet certificate that identifies users when they use SSL to connect to an Internet server or send a signed or encrypted S/MIME mail message. A certificate contains:

The name of the certifier that issued the certificate.

The name of the user or server to whom the certificate was issued.

A public key that is stored in both the Domino Directory and the ID file. Notes uses the public key to encrypt messages that are sent to the owner of the public key and to validate the ID owner's signature.

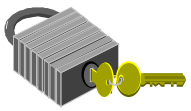
An electronic signature.

The expiration date of the certificate.

Certificates are stored in ID files and in Person, Server, and Certifier documents in the Domino Directory.

Securing Applications

- Set Anonymous access to NO for critical site files
  - Domino configuration file (domcfg.nsf)
  - Domino Log file (log.nsf)
  - Catalog file (catalog.nsf)
  - Name and Address book (names.nsf)



- Restrict access to sensitive views
  - Set Reader and Anonymous access to none
- Use $$ViewTemplateDefault to block anonymous access

Use a $$ViewTemplateDefault to block anonymous access to internal database views. Set key databases such as domcfg.nsf, domlog.nsf, log.nsf, catalog.nsf, and names.nsf set to No Access for anonymous users.

Even with general security in place, all sensitive views (such as those listing documents containing user information) should be set to 'no access' for readers and anonymous users. To prevent misuse of database searching create a $$SearchTemplateDefault with no $$ViewBody field

ACL's

- Control who can read/write/create/delete from a database
- Determines rights of Anonymous users
- Can be people, groups, other servers
- If you are using groups as part of Roles, the group name must be in the Master Catalog

Right click on databases or bookmarks or use File Database Properties to see who has access rights on a database. Note, you must have read authority in order to view this information.

ACL Types

- Types of access
  - None
  - Anonymous
  - Reader
  - Author
  - Editor
  - Designer
  - Manager
  - Depositor

Author security can create documents and delete their own

Editors can create document and delete their documents as well as others

Designers can change database design elements

Managers are the only authenticated user type that can set user security

Depositors can create a document, but then can not read it. This is useful in mailin databases for surveys

Reader Fields

- Field added by a developer to help control and limit who can read documents created with forms
  - Can be programatically set
  - Works in conjunction with ACL
- Entries in a Readers field cannot give a user more access than what is specified in the database access control list (ACL)
- Users who have been assigned No Access to a database can never read a document, even if you list them in a Readers field.
- Users with Editor access or above in the ACL can be restricted from reading documents if they aren't included in a Readers field.

Domino provides a layered security model that allows you great flexibility for controlling access to all or part of an application. The highest level of security is managed through the database access control list (ACL). Using ACL settings, you can carefully control who has access to an application and specify the type of access allowed. For example, one user might have access to read, create, and edit documents in a database, while another can only read documents.

You can restrict access to documents in the following ways:

Create a read access list for a view or folder that restricts who can see the view or folder.

Create a write access list for a folder that restricts who can update the contents of a folder.

Create a form access list to specify who can create new documents using that form. This setting also restricts who can read the documents created from the form.

Create Readers and Authors fields to limit access to specific documents created from a form.

Author Fields

- Defined by a developer and helps control who can create or edit specific documents with forms
  - Can be programmatically set
  - Works in conjunction with ACL
- Users with Editor access are not affected by the Author field

Use author fields to specifically control who can create documents on a database.

Encryption

- Using keys to provide ultimate security
- Encryption protects data from unauthorized access. Using Notes and Domino, you can encrypt messages, network ports, SSL transactions, fields, documents and databases
- If you send a key, the recipient then uses that key to view your information
- In a domain, you only need one key

The database designer can create a secret encryption key and then use that key to encrypt fields in a database. Then, only users who have the secret encryption key can read the fields. For example, a designer can encrypt a field containing salary information to prevent all but authorized users in Payroll from seeing the field. The database manager is usually responsible for distributing secret keys.

What's SSL

- SSL = Secure Socket
  - It basically means you trust the person coming through and grant them access to your databases - even across the Web
  - Notes thinks these are other Notes users
- Data is encrypted to and from clients, so privacy is ensured during transactions.

When SSL is the security, an encoded message digest accompanies the data and detects any message tampering. The server certificate accompanies data to assure the client that the server identity is authentic. The client certificate accompanies data to assure the server that the client identity is authentic. Client authentication is optional, and may not be a requirement for your organization.

You can use SSL security for Internet clients who use any of the following Internet protocols to connect to the Domino server:

Web server and Web Navigator (HTTP)

Network News Transfer Protocol (NNTP)

Post Office Protocol 3 (POP3)

Internet Message Access Protocol (IMAP)

Lightweight Directory Access Protocol (LDAP)

Simple Mail Transport Protocol (SMTP)

Internet Inter-ORB Protocol (IIOP)

The Java applet that uses this protocol must be set up to use SSL.

Simple Authentication and Security Layer (SASL)

AS400 and Notes Security

- Simple
  - Use AS400 security for AS400 functions
  - Use Notes/Domino security for Notes functions

Both AS/400 and Notes security coexist in the same physical box. At times both security mechanisms have to be satisfied when doing certain functions. Neither security system will violate the other. When Notes users want to access AS/400 data; they will need to specify userid and password.

In order to use or change the data stored in a Notes database, the access is via Domino. A Lotus Notes client will obey the authorities for those users recorded in the database's Access Control List (ACL).

Questions