


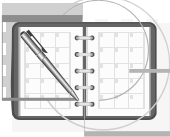
JMP104 IBM Lotus Domino Security Features - A to Z


Gabriella Davis – The Turtle Partnership
Andrew Pollack – Northern Collaborative Technologies

Lotus software 


Agenda

- Working with IDs
- Getting Access to data
- Securing your environment
- Workstation Security
- Policies
- Application Security
- Trapping Security Holes
- Summary and Discussion




Lotus software 


About the Speakers



- Gabriella Davis is a leading expert in IBM Lotus Domino and its integration with Sametime, Blackberry, and dozens of other products. She is personally responsible for hundreds of servers and many thousands of end user accounts. Her firm, The Turtle Partnership, provide the highest quality services available for these and other products.





- Andrew Pollack is an expert in IBM Lotus Domino and its integration as part of multi-disciplinary solutions to the biggest challenges faced by the information technology needs of internet generation businesses around the world. He is also a practicing fire-fighter; serving his community of Cumberland, Maine as the Lieutenant of Engine 1 and member of the Rapid Intervention Team and Special Operations Division.

Lotus software 

Working with IDs

- Public / Private Key 101
- The Notes ID and certifier
- Cross certification
- X509 Certificates
- The Certificate Authority process
- Password recovery
- Password & Key checking



Lotus software 

Public / Private Key 101

- Also known as asymmetric cryptography
- The Private Key is kept secure and not shared. Only the owner of the private key has access.
- The Public Key can be widely shared.
- Data encrypted with a PUBLIC key can only be decrypted with the matching PRIVATE key.
- Used for three distinct purposes
 - ▶ Sending data across unsecured media in a secure manner – like a diplomatic pouch
 - ▶ Providing credentials – like a passport document
 - ▶ Verifying content – like a wax sealed envelope

Lotus software



Public / Private Key 101 - Uses

- **Encrypting Data**
 - ▶ The content is encrypted using a public key in which the matching private key is held only by the intended recipient
- **Providing credentials**
 - ▶ Credentials are digitally signed using a private key known only to a certificate authority recognized by both part parties
 - ▶ In Lotus Notes, this is the root certifier or a cross certificate
- **Verifying signed content – like a wax sealed envelope**
 - ▶ An encrypted validation or hash which can only be created with a private key, but which can be verified against a combination of the exact matching content and public key associated with the private key used to create the signature.

Lotus software



The Notes ID and certifier

- Every user & server has a unique identity
- Credentials are stored in the .ID file
- The Notes password is used to OPEN THE ID file, not necessarily to access the server
- Once the ID file is opened using the password, credentials can be presented to the server

Lotus software



An Introduction to Certifiers

- Certificates are hierarchical – A certifier can be used to create sub-certifiers (called organizational certifiers) or users
- Any certificate can be validated by a server which has a higher level certificate in common
- These are all versions of the same name:
 - ▶ Common Name: Andrew Pollack
 - ▶ Abbreviated Name: Andrew Pollack/Users/TheNorth
 - ▶ Hierarchical Name: CN=Andrew Pollack/OU=Users/O=TheNorth
- These are all versions of the same name:
 - ▶ Common Name: Igloo
 - ▶ Abbreviated Name: Igloo/Servers/TheNorth
 - ▶ Hierarchical Name: CN=Igloo/OU=Servers/O=TheNorth
- Igloo and Andrew Pollack validate each other because:
 - ▶ Both have a common certificate called "TheNorth"
 - ▶ Both can verify that their certificate from "TheNorth" is identical
 - ▶ Both can verify that the common and organizational certificates of the other were created using the common certifier "TheNorth"

Lotus software



Risk!

- Certifiers are used to create IDs. Lock them up tight.
- If I have control over the /TheNorth certifier, I can create "Anything/TheNorth"



Lotus software



Cross Certification

- A Cross-Certificate creates commonality where it otherwise does not exist
- If these two need to connect:
 - ▶ Igloo/Servers/TheNorth
 - ▶ Wigwam/Servers/ThePlains
- Igloo and Wigwam cannot validate each other because they have no common certificate
 - ▶ "/Servers" is not a valid certificate in common because each was created using a different root certificate – thus they are not the same
- You can cross certify using a safe id or a supplied (as text) key

Lotus software



Risk!

- You can cross certify a user, a server or an entire OU or O – once you do that you are implicitly 'trusting' anyone within that hierarchical tree
- Don't cross certify at a level higher than you need. If Gabriella Davis/Turtle needs to access a database on Igloo/TheNorth then only cross certify:
 - ▶ Gabriella Davis/Turtle (user id) with Igloo/TheNorth (server id)
 - This limits Gab from going anywhere other than that server
 - ▶ If you cross certify /Turtle with /TheNorth you have granted anyone in Turtle and all Turtle's servers access to any TheNorth server
- Closing that security loophole is simply a case of deleting the cross certificate document that was created



Lotus software



Public / Private Key 101

- Each user and server has a private encryption key and certificate stored in their ID file and a public encryption key stored in the Domino Directory
 - ▶ Andrew/Users/TheNorth tries to access his own server to read mail
 - ▶ During the initial authentication stage, the certificates are exchanged and verified to ensure trust is met
 - The server generates a random number challenge and sends it to Andrew's workstation
 - Andrew's workstation encrypts the number using the private key in his id file and sends it back to the server
 - The server decrypts the received message using the public key it previously established for Andrew and generates the original number it sent
 - The whole process repeats with Andrew's workstation sending a random number to the server, the server encrypting it and returning it and Andrew's workstation decrypting it using the public key it knows for the server

Lotus software



Secure Client Messaging

- To send an encrypted message to a Notes user with a person document and public key in a directory you have access to is very easy
- To send an encrypted message to an Internet user requires you to have an Internet certificate you can share with them which will perform both the encryption at your end and the decryption at their end
- Your own internet certificate is stored in your ID and is in addition to whatever Notes certificates you have
 - ▶ You can have multiple internet certificates in your id file to separate encryption from signatures and client authentication
- The internet certificate is sometimes known as X.509
- For you to decrypt an encrypted message sent to you by an internet user they must have sent you their certificate in advance via a signed message and you must save that in a person document for that user in a Domino Directory

Lotus software



Working with IDs - CA Process behaviour

- The existence of physical certifier id files with shared passwords is in itself a security risk – if these get compromised
- The CA Process is designed to allow you to secure your physical certifiers and remove the need for certifier passwords by using id authentication instead

Lotus software



Working with IDs – CA Process Steps

- When generating a certificate using the CA process the following occur
 - ▶ A request is logged in admin4 for a new certificate to be issued by the CA process
 - ▶ Assuming the CA process is running and the certificate 'activated' the CA process validates that the certificate requester has RA privileges for that certifier and issues the certificate
 - ▶ A new admin request is added to update the newly issued certifier into the person or server document
 - ▶ When first accessing the server with the relevant id the certificate is automatically installed into that id and the process complete

Lotus software



Working with IDs - Migrating to the CA Process

- The properties of the physical certificate (e.g. password recovery) are migrated to the CA certificate when it is first set up but not kept in sync thereafter
- You can only migrate a certifier once to the CA process on one server in your domain only.
- If you want to 'move' the designated CA server you must first mark each certificate to say it hasn't been migrated

Lotus software



The Registration Authority

- The RA authority grants rights to users to request certificates using that certifier
- if someone requests a certificate from that certifier and is not an RA the certificate will be rejected.
- You will need to configure DDM to be notified of these rejections or monitor the Certificate Requests view in admin4
- The Certificate Authority (CA) can update the certificate properties itself and add / remove RAs

Lotus software



Risk!

- Don't try and manually edit the ICL databases , the documents or their ACLs – always modify the certificates via “Modify Certifier”
- Secure the migrated certifier with the server id so it is automatically activated when the CA process is started on that server
 - ▶ Never secure the migrated certifier with a physical id which would require that id to be physically located with a non changing password somewhere accessible to the server
- Secure O certifiers at least with a password so they must be 'activated' before issuing a requested certificate

Lotus software



Working with IDs - Setting up Password Recovery

- Password recovery is configured per certifier
- You need to specify a recovery authority (a user or multiple users) and a mail in database to use for sending the backups of each id used for recovery
- As of R7.x you can now specify the recovery password length
- Password recovery settings are updated into the user id when they access their home server

Lotus software



Risk!

- Local users working entirely in local replicas and only replicating with their home server will not receive password recovery updates or be able to send their updated id into the mail in database for recovery purposes
 - ▶ These people must do at least a File – Database – Open or other direct server activity (not replication) to participate

Lotus software



Working with IDs – Recertification

- When created, each id has a default expiry length:
 - ▶ Default for user ids is 2 years
 - ▶ Default for server ids 100 years
 - ▶ Default for certifier ids 10 years
- Expiring the certificates that have been issued limits the usefulness of old, compromised, or forgotten ids

Lotus software



Recertification Practices

- Opening the Domino Directory via a Notes Client you can use the “Certificate Expiration” view to show which ids are about to expire and automatically renew them as a batch
- User’s get prompted starting 90 days before expiry – do your renewals prior to that and the user’s won’t be aware of their ids expiring
- Recertification doesn’t affect encryption as the encryption part of the key issued is unaffected
 - ▶ DO NOT Re-Register a user who uses encryption or they will lose their encryption key and all access to encrypted data

Lotus software



Securing Identities - Password Checking

- Password Checking is enforced on a server by server basis
 - ▶ Configured on the Security tab of the Server document
 - ▶ This can then be managed per user in the person documents
- The password digest “last known password used to access this server” is stored in encrypted form in the user’s person document
 - ▶ This is compared with the password being used to access the server with that id
 - Remember the password unlocks the id and is not normally presented to the server
 - ▶ If the user forgets their password and needs to reset it you can clear the password digest field on the person document
- Using Policies is the most efficient way of managing password and security options (more on this later)

Lotus software



Securing Identities -Public Key checking

- Public key checking is enforced on a server by server basis
 - ▶ It is configured on the Security tab of the Server document
- It applies to all users accessing that server – the public key stored in their id will need to match the public key stored in their person document
- The public key in their person document is automatically updated during recertification if it is done correctly
- You can choose to not check public keys or check them only for trusted directories or all directories
- You can choose to log public key failures even if you don’t enforce checking

Lotus software



Risk!

- If you don't enforce password checking on your mail servers at least then a compromised id which has been stolen or shared and the password known can be used to access the server
- If you're not using public key checking then you have no way to lock out an existing id that has been compromised completely
- Owning an id with a valid certificate and knowing its password will not grant you access to a server with these settings enabled.
- If your certifier id is compromised, password and public key checking are only effective if you also prevent access to modify the "Person" document in the address book
 - ▶ An unscrupulous person with a phoney ID file could go in after hours, change the stored password or public key, access the content they want, and restore the original values before the actual user is aware of the issue.

Lotus software



Securing Identities - Rollover keys

- Many companies are not in position to force public key checking as the public keys stored in the Domino Director(ies) are missing or out of date – in these cases it is possible to reissue new keys to everyone via a security policy
- Create security policy or policies and apply to users for force key rollovers and updates into their ids and person documents without them being aware of it
 - ▶ Keys can be issued over a series of days so they don't all expire at the same time for instance
 - ▶ You can use this for putting new public keys in place prior to turning on public key checking or for forcing increased key strengths for ids created in older environments
 - ▶ You can also set how soon the user is notified their certificate is due to expire
- All this can be done without the user knowing
- Remote users MUST access the server to get this policy applied

Lotus software



Securing Identities - Deploying larger keys

- If your ids were created pre R6 they may use the original 630 bit keys and not the new 1024 keys available in R7
- A higher key encryption value may not be a requirement in all instances
- You may decide to issue new keys as 1024 and leave old keys on 630 until they are ready to renew
- You can use the security policy to force all keys to be updated to 1024 if they aren't already

Lotus software



IDs

- Simple security practices to adopt
 - ▶ Don't be tempted to keep backup copies of ids 'somewhere safe' with default passwords
 - They'll just get out of sync when you recertify or name change anyway
 - ▶ Migrate your certifiers so you don't have to distribute either them or their passwords
 - If they get compromised there's no way back
 - ▶ If you have to cross certify do so at the lowest possible level – only cross certify a user to access a server if that's all that's needed

Lotus software



Getting Access to Data

- Physical / Network Security
- Server Access Authority
- Database Access Control
- Reader & Author fields
- Encryption

Lotus software



Getting Access to Data - Server Security

- Server Access is granted in the order
 - ▶ Certificate Authentication
 - ▶ Deny Access Lists
 - ▶ Server Access Lists
 - ▶ Public Key Checking
 - ▶ Password Checking
- Complete the security tab of the server document carefully

Lotus software



Getting Access to Data – Who Can Do What

- Who can do what?
 - ▶ Allowed to Access the Server
 - ▶ Don't leave it blank, use */org
- Allowed to create new databases and replicas
 - ▶ This should be limited
 - ▶ Can fill your server, or deploy bad code that crashes your it
- Allowed to run Unrestricted Agents
 - ▶ Ouch – they own your server
 - ▶ Can run OS commands, etc.
- It's better to restrict access and then open up as required than to leave a possible security hole

Lotus software



Admin Roles in Version 6.x+

- Version 6.x added granularity to "Administrator" access
- Allows you to delegate specific areas of responsibility without giving complete control to junior administrators.
- Using the administrator task, you can allow area managers to register users without giving them a certifier.

Lotus software



Admin Roles in Version 6.x+

- Full Access administrators
 - ▶ Able to leap tall ACLs
 - ▶ Impervious to Reader-Names
- Administrators
 - ▶ Use all the power of the administrator tool, but subject to database and document controls
- Database Administrators
 - ▶ Manage databases, but not the server itself

Lotus software



Admin Roles in Version 6.x+

- Full Remote Console Administrators
- View-only Administrators
- System Administrators
 - ▶ No database controls, but plenty of server setup access
- Restricted System Administrators
 - ▶ Restricted System Commands

Lotus software



Limit Use of Full Access Administration

- Full Access Administration should only be used rarely, when a need to override ACL or Reader Names is required.
- Grant this only to specific ID files. Make the administrator switch to this ID file when needed.
- Create an "Event" notification to notify management any time this level of access is granted.
- Use secret key encryption on databases you don't want full access administrators to read.
 - ▶ If you use public key encryption there's a chance your admin can get hold of the user id and password

Lotus software



Using SSL

- Protocols SMTP, HTTP, POP, LDAP and IMAP can all use SSL for port activity
- To use SSL you must have a keyring file created by a certificate authority which is used to encrypt the traffic
- If you are using r6.x and Internet Site documents you can use different keyring files for different Sites or Protocols
- You can be your own Certificate Authority or use an external CA such as Verisign but either way you will need to create your own keyring file using certsrv.nsf on the Domino server
- If you are using an external CA you will need to generate a certificate request using your new keyring to send to the CA and they will return a certificate to you which you can merge into your existing file

Lotus software



Getting Access to Data - ACLs

- ACLs control database security
- There are 7 levels of ACL access as a minimum but additional settings under each level you can control (such as denying rights to delete or create)
- Roles defined within ACLs don't control database access
- ACL settings can be changed en-masse through Domino Administrator
- ACL "Type" adds an additional level of security

Lotus software



Risk!

- If you run HTTP ensure "Anonymous" is set to "No Access" on any database you don't want public
- Don't be tempted to use –Default- to control database access
- "Opt In" Security is a good model to adopt – people gain access because they are in an explicit group not just because they exist
- Servers replicating a database must exist in the ACL with enough rights to allow them to replicate the changes being made on their copies

Lotus software



Getting Access to Data - Reader / Author fields

- Author fields determine who can edit a document, regardless of who the original author was.
 - ▶ This security setting only applies to users with Author access – users with Editor access override the Author fields
- Reader fields determine who can actually see documents
 - ▶ In categorised views a user will still be able to see the category header even if they can't see any of the documents within it, unless you set the view property otherwise
 - ▶ A field value of empty means ANYONE can read the document provided they have read-access to the database
 - ▶ Servers have to be in Reader fields to replicate the documents between them

Lotus software



Getting Access to Data – Encryption

- You can encrypt documents so they can only be read by certain users
- You can encrypt at Form or Document level using
 - ▶ Public keys - only named users with keys stored in the Domino Directory can decrypt
 - ▶ Secret keys that are added to the form
 - ▶ Secret keys are created under User Security – Notes Data
 - The database manager should create and distribute the secret key(s)
 - The secret key is added to your user id
 - If emailing the secret key(s) for distribution mark the message so it cannot be forwarded printed or copied
 - Secret Key distribution messages generated by the secret key management dialog box can also be encrypted to a specific recipient

Lotus software



Risk!

- If you encrypt a document or field using a secret key and lose that key you have lost access to the document or field
- If someone has the secret key and has Author or Editor access to an encrypted document they can remove the encryption you have set

Lotus software



Securing your environment - Physical security

- Unless you're encrypting your databases locally AND password protecting your server's ID, you need to protect the data from local access
- Network admins may very well have rights to "map" to your Notes data directory
- In Linux, /local/ generally is set with read access enabled – that means people with access to ftp or other services may be able to read those files

Lotus software



Getting Access to Data

- Simple security practices to adopt
 - ▶ Create AccessServer and DenyAccess lists to control server access
 - ▶ Opt-In Security
 - Use explicit groups or names instead of -Default- access. Set -Default- to No Access
 - Enter Anonymous with No Access in any ACLs if you are running HTTP or allowing Anonymous Notes access
 - ▶ Assign Full Access Administration to a reserved id that generates a notification if it is used
 - ▶ Use encryption for local databases
 - ▶ Review Groups and Databases periodically as part of a regular process. Remove old names from groups, and old databases from the server, and old content from databases.

Lotus software



Securing your environment

- Network ports and network access
 - ▶ Disable any ports or protocols not in use
 - ▶ Disable any shares or browsing to the server
 - ▶ Consider using port encryption especially on public ports

Lotus software



Securing your environment

- SMTP relaying
 - ▶ Only turn on SMTP Listener on a server if it's receiving inbound SMTP
 - ▶ Complete the Global Domain document with valid domains that you will accept mail for
 - ▶ Complete a Server configuration document specifying which addresses will allow to relay if necessary
 - avoid using wildcard addresses
 - avoid using addresses that may apply to multiple machines such as a firewall address representing all machines behind a single firewall
 - ▶ Complete the SMTP Inbound tab on the Server Configuration document
 - ▶ Test relaying yourself

Lotus software



Workstation Security

- ECLs
- Encrypting Local Databases
- Multi-user Installations
- Roaming Users
- Port Encryption
- Single Sign-on

Lotus software



Workstation Security – ECLs

- These are NOT Extended-ACLs (also sometimes referred to as ECLs)
 - ▶ **Execution Control Lists** are designed to protect workstation activity
 - Each user has an ECL matching their id on a particular Notes installation
 - When you get prompted to 'Trust Signer' to do something that updates your ECL
 - You can set an administration ECLs for your entire organisation in Domino Administrator
 - ▶ Choose Actions – Edit Administration ACL
 - ▶ The ECL is sent to the workstation when it is being set up
 - If you later update the ECL you will need to redistribute it to users via a Security Policy
 - ▶ Use Security policies to create customised ECLs for applying to certain users or groups – the customised Administration ECL replaces the Default Administration ECL

Lotus software



Risk!

- Don't build an ECL that makes your life easier but leaves the workstation exposed
- Don't grant access to unsigned content
- Don't let users modify their ECL by deselecting "Allow user to modify" that way they can't create a security hole themselves
- To remove a group, wildcard or specific user access in an ECL – leave the entry in the ECL but deny it all rights

Lotus software



Workstation Security - Encrypting local databases

- When create a local database or local replica you have the option to encrypt that instance of the database using the public key of the user id doing the creating
- Encrypting a database locally ensures that even if you don't have disk encryption turned on the data is protected by the Notes ID
- Simple Encryption – fast access, limited protection, able to be compressed
- Medium Encryption – good access and security but no disk compression
- Strong Encryption – slower document access but highest security
 - Should only be used when the data requires it

Lotus software



Risk!

- If you create a database with encryption turned on – no other id will be able to access that database even if they are in the ACL – it is encrypted for the user that created it only
 - That user and id can disable the encryption

Lotus software



Workstation Security - Multi user installations

- Multi user installation is a Notes client install option that creates multiple data directories
- A data directory is created for each Windows user / profile that logs onto the workstation
- It relies on Windows security and database encryption to protect one users data from another
- If a user 'hotdesks' the multi user installation can be combined with 'roaming user' setup to ensure the data directory can travel and is cleaned up

Lotus software



Workstation Security - Roaming users

- Enabling a user to 'roam' stores their local data (notes.ini, names.nsf, bookmarks id file) on a server
- When a roaming user logs in their data is downloaded to the data directory for their Notes client
- If they aren't using a multi user install client then the roaming user settings will overwrite the Notes client settings permanently
- You can set clean up options for roaming users to determine how often the roaming data is removed from the local pc

Lotus software



Risk!

- Having roaming users and not cleaning up the data means you risk sharing user A's information with user B
- Using a multi user install and roaming users without effective cleanup results in large amounts of possibly unused data taking up Windows space under Windows Documents and Settings

Lotus software



Workstation Security - Port encryption

- Encrypting network traffic ensures the transmission of data is protected against network sniffers
 - Although the data is unencrypted once saved to the file system
- Encryption only needs to be enabled at one end of the network connection
 - If your server port is already encrypted you don't need to encrypt the workstation port
- Encryption will slow down traffic and especially replication but it can be a good option for laptop users if the server port isn't set to encrypt

Lotus software



Workstation Security - Single signon

- Enabling single signon means the user only has to login once
- The AD or Windows credentials are kept in sync with the Notes ID password and so one is passed to the other
 - once a user has logged into Windows they are not asked to log into Notes
- There are other 3rd party syncing tools that will integrate with a variety of applications and databases
- Your users will be thrilled to have only one password to remember and only be prompted for it once
- Your Auditors will be HORRIFIED!

Lotus software



Policies

- Registration
- Desktop
- Security
- Mail

Lotus software



Policies - Registration

- Registration policies can be combined with the CA process to enforce corporate policies for new users and provides centralised federated management of id creation
- Registration policies can be per user or per OU / O
- Security Settings include
 - ▶ Password lengths, internet passwords
 - ▶ ID type, expiry and location
 - ▶ Group memberships

Lotus software



Policies – Desktop

- Security Settings include
 - ▶ SSL Options for working with site certificates
 - ▶ Applet Security
 - ▶ Proxies
 - ▶ Network Ports
- Policy settings can be set to overwrite user choices and prevent users from amending

Lotus software



Policies – Security

- Password quality, expiry, ability to change
- Synchronisation with HTTP password
- Force password expiry
- Certification key length, expiry, forced renewal
- ECL Settings

Lotus software



Policies – Mail

- Security Options under Mail Policies include
 - ▶ Access and Deletion for sharing mail and calendar information
 - ▶ Soft Deletions timeout
 - ▶ Message Disclaimers

Lotus software



Policies

- Simple security practices to adopt
- Combine policies to have basic corporate settings added to specific local or user requirements
- At minimum use a security policy to ensure the ECLs are set and locked to protect the workstation environment

Lotus software



Directory Security

- Directory ACL
- Author access plus roles
- Document "Owners" / "Administrators"
- -Default- / Anonymous NO ACCESS

Lotus software



xACL Security – Over the top complexity for control freaks

- Extremely granular controls
- Little or no documentation tools
- Very difficult to manage
- Look for 3rd party products to integrate if you need this kind of control



Lotus software



Extended ACL Basics

- Something more granular and sophisticated
- Directory specific only can't be applied to other databases
- xACL is in addition to the db ACL and any document security – it adds on and enhances in a more detailed way but can't increase the level of access just define it

Lotus software



Elements of the xACL

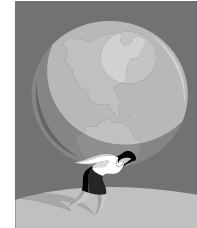
- The elements of an extended ACL are:
 - ▶ Access settings -- the allowed access
 - ▶ Subjects -- the users and groups whose access you control
 - ▶ Targets -- categories of documents or specific documents to which access settings apply
 - ▶ For each access choose Allow or Deny.

Lotus software



Application Security – It is not just about ACLs!

- Change Controls
- Risk Classification
- Signing
- Ownership
- Access Group Management
- ACL Management
- Readers fields
- Encryption



Lotus software



Application Security - Change Controls

- Do not allow developers to manage the deployment of their own code
- Common coding mistakes – especially in Java agents – can really crash a server quickly

Lotus software



Application Security - Application risk classification

- Develop an assessment guideline that requires application content owners to assign a security and privacy requirement level to each application
- Develop a checklist of security processes and features to match each privacy designation level
- Commonly this process happens in meetings between application owners and developers – without a set of standards
 - ▶ Requires every developer to have a complete understanding of all the possible security implications and features available
 - ▶ Requires end users and developers to stand up for what they believe are best practices in the face of time and budget constraints

Lotus software



Application Security - Signing with production IDs

- A limited and controlled set of "production" IDs should be used to sign code before it is deployed
- Different IDs can be used for different levels of security requirements.
 - ▶ Server Based Agents
 - ▶ Server Based Agents running with enhanced access
 - ▶ Admin Role IDs – for recovery of mismanaged reader names
- Specific signing ids for each of the most critical applications from a privacy or security perspective

Lotus software



Application Security - Application ownership, periodic review, and sun downing

- Create a database which registers each application on the server to a designated owner, contact point, and responsible developer
- Review databases periodically and remove any which are not 'owned' by anyone willing to be responsible for them.

Lotus software



Application Security - Access Group Management, review, and sun downing

- Do not give database owners manager access in the ACL. Create groups for each database and give database owners the rights to manage those groups
 - ▶ E.g. "Public Sales Tools – Author Access"
- Review groups periodically and remove any which are not 'owned' by anyone willing to be responsible for them. Make group owners attest to their contents on a periodic basis.
- Third Party Tools – both Domino Specific and more general – exist to help manage access groups and sun-downing

Lotus software



Application Security - ACL Management

- Developers and Database owners should not have designer or manager access to production databases on your key servers.
- Remove manager access from mail files
 - ▶ Mail files are where developers "test" new ideas.
- Review your CATALOG.NSF file. It can be a shopping list for penetration testers or sneaky end users.

Lotus software



Application Security - Reader Names vs. Hidden Views – security vs. obscurity

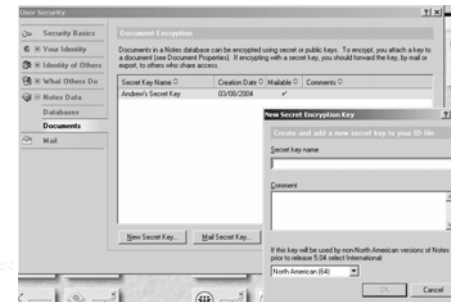
- Excluding documents from a view does not secure them. Any user with a Notes client or a browser may be able to gain access to them.
- Real security is as simple as putting your name on a document
- 1st Grade Security still works.
 - “It’s mine!” says Peter.
 - “Prove it!” responds Sarah.
 - “It has my name on it!” answers Peter triumphantly.

Lotus software



Application Security - Application Encryption with shared keys

- Create in your own ID file
- Mail to other users – can be encrypted, and even created for use only with specific IDs
- Add to FORMS or DOCUMENTS using the Properties Dialog Box



Lotus software



Application Security

- No Designer Access to the Server
- Separate Developer and Administrator rights on the servers
- Use Sun-Down Rules for Databases, Groups, and Content
- Use real security, not obscurity
- Assume everyone can get a Domino Designer client

There are only two levels of paranoia, according to internet security professionals. Complete, and inadequate.

Lotus software



Trapping Security Holes

- Designing 'Good' Security
- Monitoring
- Administration

Lotus software



Trapping Security Holes

- Simple security practices to adopt
- Are there security Best Practices?
- Defining your security best practices – it's not as hard as you think
- Once you have agreed policies use DDM to set them up and monitor any variations
- Security Probe in Domain Monitoring

Lotus software



Trapping Security Holes - Designing 'good security'

- Define internal procedures that you can follow – don't make it up as you go along or everyone else will too. You need
 - ▶ Password Quality and Expiry Policies
 - ▶ Server access Policies
 - ▶ Database and Replication Policies
 - ▶ User Registration Policies
 - ▶ ACL Policies
- Build yourself one server configured the way you would like all others configured (do you password check, who has Full Access rights). Use DDM to monitor that server document and its configuration for any changes

Lotus software



Trapping Security Holes - Monitoring for security holes

- DDM has a built in "Good Security" monitor – give it the details of a server whose configuration is 'right' and it will notify you if any other server strays from that configuration
 - ▶ Someone in Timbuktu decides to turn off public key checking on their server document for their server and you get to hear about it
- Always set up event notifications against the Directory ACLs – you want to know if someone decides to change those
- If in doubt use DDM to produce a report on "Best Practices"

Lotus software



Trapping Security Holes - Distributing administration

- Don't share certifiers or certifier passwords
- Use Directory Security to restrict what changes local admins can make
 - ▶ Just because someone needs to register users doesn't mean they need to modify server documents or configuration documents
- Monitor ACL changes via DDM / Event Monitoring
- Use DDM to monitor security or server document changes
- Set up a Security Policy to enforce workstation ECLs

Lotus software



Summary and Discussion

- Ask now, don't wait for the end and ask quietly at the podium



Gabriella Davis – The Turtle Partnership

<http://www.TurtleWeb.com>

Andrew Pollack – Northern Collaborative Technologies

<http://www.TheNorth.com>



Lotus software



© IBM Corporation 2007. All Rights Reserved.

The workshops, sessions and materials have been prepared by IBM or the session speakers and reflect their own views. They are provided for informational purposes only, and are neither intended to, nor shall have the effect of being, legal or other guidance or advice to any participant. While efforts were made to verify the completeness and accuracy of the information contained in this presentation, it is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this presentation or any other materials. Nothing contained in this presentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

IBM, the IBM logo, Lotus, Lotus Notes, Notes, Domino, Domino Doc, Domino Designer, Lotus Enterprise Integrator, Lotus Workflow, Lotusphere, QuickPlace, Sametime, WebSphere, Workplace, Workplace Forms, Workplace Managed Client, Workplace Web Content Management, AIX, AS/400, DB2, DB2 Universal Database, developerWorks, eServer, EasySync, iSeries, iSeries OS/400, Passport Advantage, PartnerWorld, Rational, Redbooks, Software as Services, System z, Tivoli, xSeries, z/OS and zSeries are trademarks of International Business Machines Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Lotus software
Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.



Intel and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.