Notes on Domino

Black Hat – Las Vegas 2003
Aldora Louw
PricewaterhouseCoopers

Lotus Domino is inherently secure……………..

…..a Misconception!!!

Security is Not Automatic!!!!

Security Requires

- Planning
- Design
- Implementation
- Enforcement
- Maintenance
- Review

Areas of Security

- Physical
  - – Physical Data Center
  - – Physical Machine
- Logical
  - – Network Security
  - – OS Level
  - – Application Level

Server ID Password?

	Password	No Password
Pro's	• Server ID Protected. • Mitigates some risks that OS and network insecurities might cause.	Server can restart without intervention.
Con's	Server cannot restart without intervention.	• Server is vulnerable to server ID being exploited. • Server relies on OS and Network Security.

No Server ID Password

Demonstration

1. Server ID is not password protected.
2. Domino is running on Windows 2000.
3. We have obtained file level access to the Windows 2000 machine.
4. Demonstrate Domino manipulation.

Protecting the Server ID

- Password protect the Server ID.
- Harden OS and prevent file access to application files.
- Strengthen network security.
- Implement fault tolerant technologies.

Domino Interfaces

Original Notes Client Interface

Notes Client Interface

- Two Factor Authentication
- Public Key Type Infrastructure
  - Root / Organizational Certifier (O)
  - Pubic and Private Keys

PKI Type Infrastructure Allows

- Global trust based on a common root certifier.
  - Most Notes client activities
- Specific user identification based on public and private keys.
  - User access servers
  - Encrypting email

Which Trust?

	Global and Specific	Global Only
Pro's	• User's identity is verified. • Confidentiality of email.	• Easier to manage. • A user id can be recreated.
Con's	• A user id cannot be recreated. • Email can only be read by the intended recipient. • More difficult to manage.	• A user may be impersonated. • Email may be viewed by unintended readers.

User Recreation

Demonstration

1. Certifier ID is obtained.
2. Certifier ID has no password or a weak password.
3. Recreate admin user and access the Domino system.

Trusts Solutions

- **Utilized Global and specific user identification.**
  - Compare public Keys. (Server Doc)
  - Check password on ID. (Server and Person Docs)
  - Encrypt incoming email. (Person Doc)
- **Protect Certifier ID's.**
  - Physically protect (Domino 6).
  - Logically protect with a strong password.
  - Require multiple passwords on higher level certifiers.
- **Utilize ID storage database (Domino 5 and 6).**
- **Set Access control list securely.**

Web Interface

Web Authentication

	Less Name Variations	More Name Variations
Pro's	• Users are more accurately identified. • More difficult to guess a user name and password.	
Con's	• May have unpredictable results in older applications.	• Users are less accurately identified. • Easier to guess a user name and password. • Confuses users.

More Name Variation Authentication

Demonstration

1. Web server authentication is set to less secure.
2. User: Joan Smith/User/BlackHat.
3. Joan’s password is default01.
4. Demonstrate how password guessing is made easier.

Less Name Variation Solution

- Set Web server authentication setting to: Less Name variations more security.
- Enforce complex passwords. (Domino 6)
- Enforce password changes. (Domino 6)

Users are often the weak link in systems security.

Technology can be controlled………..

Users need to be managed.

Password Encryption

- Utilize the more secure version of encrypting passwords (Salt Hash vs. Hash).
  - Example of a Domino Hash: (63E4BD1FEFD8913B15A5EF484A3F6B06)
  - Example of a Domino Salted Hash: (GYDKg6JZt/w6rx7w3aQk)
- Do not rely entirely on password encryption technology.

Relying only on Technology

Demonstration

1. Domino is accessible via the web interface and the Notes Client interface.
2. User has reader access to the Domino Directory.
3. User gains administrator password hash via “viewer”. (Domino 5) or User gains administrator password hash directly off of the person document. (Domino
   - Administrator password is cracked.
   - User logs in as administrator via the web interface.
4. User gains administrative access to the Domino environment.

Restricting access to data in fields

Hiding Information

Demonstration

1. Demonstrate the method for viewing all form fields including hidden fields.
2. Discuss where this has been used in real life applications (Domino Directory, HR applications etc.)

Really Hiding Information

- Field encryption vs. field hiding
  - – Demonstrate an encrypted field in the Shadow database.
- Utilizing Extended Access (Domino 6)

ECL -
Execution Control List

Clear ECL

Demonstration

1. The Notes client does not have an ECL set.
2. Show how an “innocent” email can be used to extract valuable information from the client machine.
3. Note that an ECL does not prevent unauthorized access if the user chooses to ignore the warning messages.

ECL Solution

- Set ECL’s on each Notes workstation. (Security Profiles – Domino 6)
- Have a “Process Signer” ID.
- Sign all tasks with the “Process Signer” ID.
- Train users to read and evaluate ECL messages.

Domino Design

- Business needs should drive the Domino design.
- Domino smart install.
- Limit enticement information.
- Keep different levels of data protection in mind, separating public/semi-public and private data.

Domino Smart Install

Limits the effectiveness of many directory transversal and other attacks by:

- Using different partitions
- Avoiding default install locations.

Enticement Information

- Examples of enticement information are:
  - Banner info when viewing page source
  - Banner info received when telnetting to port 80.
  - Banner info when telnetting to port 25.
- Correct this by adding the following lines to the notes.ini file:
  - DominoNoBanner= 1
  - SMTPGreeting="*string* %s"

Defeating the Firewall

Demonstration

1. DMZ servers and internal servers are in the same domain.
2. Administrator access is gained to a DMZ Domino web server.
3. Obtain command line access via a “NetCat” response.

Design Considerations

- Do not place web servers and other servers in the same domain.
- DMZ and other external servers should have their own organization certifiers.
- Configure the firewall to not trust all internal traffic.
- Utilize strong passwords on DMZ servers.
- Where feasible disallow all users access to the Domino Directory.
- Use varying levels of administration (Domino 6).
- Limit changes being made to databases via the Web (Utilize maximum internet access allowed setting).

A higher level of security is possible ……..

but not automatic.

Questions?

Contact information:

aldora.louw@us.pwc.com