

## ID218: Help Protect Yourself with New Security Features in IBM Lotus Domino 8

*David Kern*

*Peter Mierswa*

*Lotus Software, IBM Software Group*



### Agenda and Goals

- IBM Lotus Notes/Domino Protocols
  - ▶ Larger Keys for Notes Protocols
  - ▶ Certifier Key Rollover
  - ▶ ID File Recovery APIs
  - ▶ Local Database Encryption
- Internet Protocols
  - ▶ Certificate revocation checking via OCSP
  - ▶ Internet Password Lockout -- "3 strikes" for http
  - ▶ Smartcard enhancements
  - ▶ AES for SSL
  - ▶ SSO using LTPAToken2
- Domino Security Futures



### Security Improvements in IBM Lotus Domino 8

*Notes/Domino Protocols*



## Larger Keys and Key Rollover for Notes Protocols

- Larger Keys in Review
  - ▶ Large Internet keys supported since R4.x
  - ▶ Support for Notes Keys larger than the "classic" 630 bit keys has been phased in gradually starting in ND6
  - ▶ ND8 adds support for 2048 bit keys for users and servers and 4096 bit key for certifiers
- Tools for Administrators
  - ▶ Option to specify key size during registration (ND7)
  - ▶ User key rollover controlled by security policies (ND7)
  - ▶ Server key rollover controlled by server document (ND7)
  - ▶ Certifier key rollover controlled in administrator client (ND8)

Lotus



## Cost of Cracking – How Strong is Strong?

- Guessing a...
  - ▶ Coin Flip: 1 bit key
  - ▶ Spin of a Roulette wheel: 5.25 bit key
  - ▶ Birthday: 8.5 bit key
  - ▶ Specific person in the US: ~28 bit key
  - ▶ Specific person in the world: ~32.5 bit key
- Most well known cracks are due to weak protocols, short keys, or both
  - ▶ DVD encryption (CSS)
    - 40 bit disk keys, attacked as a 25 bit keys
    - Stream cipher attacked as a 16 bit key
    - "Hash" of disk key broken in less than 20 sec on a 450MHz PIII.
  - ▶ 802.11 encryption (WEP), etc.
- 40 bit keys: "Export grade"
  - ▶ Order of weeks or less on an ordinary personal computer
  - ▶ RC5-40 cracked in less than four hours in 1997 by a network of about 250 workstations

Lotus



## Cost of Cracking Symmetric Keys

- 56 bit keys: (Single DES)
  - ▶ Electronic Frontier Foundation (EFF)'s DES cracker
    - Less than \$250,000, including design costs
    - Took 56 hours in July 1998
  - ▶ Distributed.Net
    - EFF's DES cracker plus 100,000 PCs on the Internet
    - Took 22 hours and 15 minutes in January 1999
- 64 bit keys (RC2, RC4)
  - ▶ Distributed.Net cracked a 64-bit RC5 key in 2002
    - 331,252 people working together for 1,757 days
    - Equivalent to 790 days at an artificial peak rate equivalent to 46k 2GHz Athlon CPUs
    - RC5-72 crack started in 2002, and still in progress
- 128 bit keys (RC2, RC4, AES)
  - ▶ A machine that could crack a 56-bit key in 1 second would take approximately 149 thousand billion years to crack a 128-bit key.
- Additional limits set by the laws of thermodynamics
- Then why use 256 bit keys?
  - ▶ Could guard against future attacks, such as quantum computing

Lotus



## Cost of Cracking RSA keys

- General Number Field Sieve (GNFS)
  - ▶ Sieving is compute-bound and distributable
  - ▶ Matrix row reduction blocked on memory and communication
- RSA-640 factored November 2005
  - ▶ 640 binary digits or 193 decimal digits
  - ▶ German Federal Agency for Information Technology Security (BSI)
  - ▶ Sieving: 3 months on 80 2.2 GHz Opteron CPUs
  - ▶ Matrix: 1.5 months on a Gigabit cluster of 80 2.2 GHz Opteron CPUs
- RSA-200 factored May 2005
  - ▶ 663 binary digits or 200 decimal digits
  - ▶ German Federal Agency for Information Technology Security (BSI)
  - ▶ Sieving estimate: appx 55 years on a single 2.2 GHz Opteron CPU
  - ▶ Matrix step: 3 months using cluster of 80 2.2 GHz Opteron CPUs
- 640 to 663 bits approximately doubled the time to crack

Lotus



## Cost of "Cracking" Hashes

- What makes a hash strong?
  - ▶ Not reversible (one-way)
  - ▶ Collision resistance
  - ▶ Changing one input bit should change about half of the output bits
- The Birthday Attack
  - ▶ Finding two people with the same birthday is easier than finding one person with a specific birthday
- Collisions have been found in MD5, SHA-0
  - ▶ Currently known techniques generate carefully sculpted pairs of messages
  - ▶ Cannot be used against existing signatures
- Notes hashing (MD2\*)
  - ▶ Most hashes are based on repeated calls to a compression function
  - ▶ MD2 includes a checksum that is appended to the end of the message

Lotus



## Interoperability

- 6.0
  - ▶ Can use 1024 bit RSA keys, but will not generate them
  - ▶ Can use 128-bit RC4 keys, but cannot use 128 bit RC2 keys
- 6.0.4/6.5.1
  - ▶ Can use 1024 bit RSA keys, but will not generate them
  - ▶ Can use 128 bit RC2 keys, but will not generate them
- 7.0
  - ▶ Can generate and use 1024 bit RSA keys
  - ▶ Can generate and use 128 bit RC2 keys
  - ▶ Adds underlying support for 2048 bit RSA keys
- 8.0
  - ▶ Can generate and use 2048 bit RSA keys for users and servers
  - ▶ Can generate and use 4096 bit RSA keys for certifiers
  - ▶ Adds underlying support for 4096 bit RSA keys for users and servers
  - ▶ Adds underlying support for 8192 bit RSA keys for certifiers

Lotus



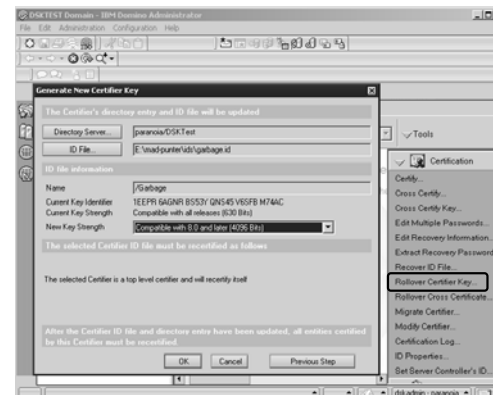
## Why use Key Rollover?

- All Notes users and Domino servers have public/private key pairs stored in their ID files
- Key rollover needed:
  - ▶ periodically as a precaution against undetected compromise of the private key
  - ▶ as a remedy to recover from a known compromise of the private key (e.g. ID file is stolen)
  - ▶ to increase security by updating to a stronger key

Lotus



## Certifier Key Rollover in 8.0



Lotus



## Certifier Key Rollover Tips

- Recertification of users and servers is not automatic to avoid an admin replication storm
  - ▶ Existing ID files will continue to work without recertification for a period of time
  - ▶ Good opportunity to roll over user and server keys
- Start at the root of the hierarchy and work your way down
  - ▶ After rolling over Os and OUs, roll over servers then users
  - ▶ Can do one branch of the hierarchy at a time or do everything
  - ▶ Wait a week or so between rounds of recertification or key rollover
  - ▶ Good idea to at least recertify users and servers beneath a CA with a new key

Lotus



## APIs for ID File Recovery

- New APIs enable customers and partners to integrate the security of ID File Recovery with the convenience of custom organization-wide management systems
- Why use ID File Recovery?
  - ▶ Forgotten passwords
  - ▶ Lost or corrupted ID files
  - ▶ Automatic ID file backups
  - ▶ Automatic recovery information updates starting in ND6
  - ▶ Enhanced logging and configuration starting in ND7
- Functions defined in kfm.h:
  - ▶ SECGetRecoveryInfo
  - ▶ SECImportRecoveryInfo
  - ▶ SECMailRecoveryID
  - ▶ SECRecoverIDFile
  - ▶ SECExtractRecoveryPassword
  - ▶ SECBuildEncryptedBackupIDFile

Lotus



## Local Database Encryption Enhancements

- Weak and Medium encryption options removed
  - ▶ Existing databases using Weak or Medium encryption still supported
  - ▶ No actual known problems with Medium encryption, but Strong uses more standard techniques
- New local database replicas encrypted with Strong when created

Lotus



## Security Improvements in IBM Lotus Domino 8

*Internet Protocols*

**IBM**



## Certificate Revocation Checking via OCSP

- Online Certificate Status Protocol, RFC 2560
  - Determine the revocation state of an X.509 certificate
  - More timely information than CRLs, no CRL cache required
- Enhances security for:
  - S/MIME signature verification
  - S/MIME encrypted sender verification
  - SSL certificate verification
- OCSP client support, not an OCSP responder
  - Third-party OCSP responders can be configured to return information from CRLs issued by the Domino CA
- OCSP must be enabled to be used
  - Security policy for the Notes client
  - OCSP\_RESPONDER, OCSP\_LOGLEVEL, OCSP\_CERTSTATUS notes.ini variables for a Domino server

Lotus



## OCSP Policy Configuration

Security Settings - OCSP enabled

Basic | Password Management | Execution Control List | Keys and Certificates | Signed Plugins | Portal Server | Corr

Default Public Key Requirements

Inherit Public Key Requirement Settings from Parent  Enforce Public Key Requirement Settings in Children

Minimum Allowable Key Strength: No Minimum

Maximum Allowable Key Strength: Compatible with Release 8 and later (1024 bits)

Preferred Key Strength: Compatible with Release 8 and later (1024 bits)

Maximum Allowable Age for Key: 36500 days

Earliest Allowable Key Creation Date: 08/01/87

Spread new key generation for all users over this many days: 180 days

Maximum number of days the old key should remain valid after the new key has been created: 365 days

Certificate Expiration Settings

Warning Period: 21 days

Custom Warning Message:

Enable Certificate Status Protocol (OCSP)

Enable OCSP checking

Always use Default OCSP Responder: http://ocsp.opnvalidation.org/80

Permitted Certificate Status: Allow use of all certificates

Level of Detail recorded in the Client Log: Log everything

Lotus



## Internet Password Lockout – “3 strikes” for http

- Lock out the user after “X” incorrect login attempts
- Enable feature and configure defaults for one or more servers at a time in a server configuration settings document.

Workspace | DSKTest's Directory - Server | Configuration for paranoia

Edit Server Configuration | Cancel

Configuration Settings: paranoia/DSKTest

Basic | Security | Client Upgrade | Router/SMTP | MIME | NOTES.INI Settings | Domino Web Ace

Internet Lockout

Enforce Internet Password Lockout:  Yes

Log Settings:  Lockouts  Failures

Default Maximum Tries Allowed: 5

Default Lockout Expiration: 2 Hours

Default Maximum Tries Interval: 15 Minutes

Lotus



## Internet Password Lockout – User Configuration

- Can override server default settings with user security policies
  - Special rules for CEOs or other users with special needs
  - Only applies to servers with Internet Password Lockout enabled

Workspace | DSKTest's Directory - Server | Security Settings: Hard Lockout

Edit Settings | Cancel

Security Settings: Hard Lockout

Basic | Password Management | Execution Control List | Keys and Certificates | Signed Plugins | Portal Server | Comments | Administration

Password Management Basics

	Inherit from parent policy	Enforce in child policies
Use Custom Password Policy for Notes Clients	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Check password on Notes if the	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Allow Clients to Change Internet Password over HTTP	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Enable Internet Password Status: Note Client Password Changes	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Enable Note Single Logon with Workplace Work Client	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Password Expiration Settings

	Inherit from parent policy	Enforce in child policies
Enforce Password Expiration	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Required Change Interval	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Allowed Grace Period	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Password History (Notes only)	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Warning Period	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Custom Warning Message	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Internet Password Lockout Settings

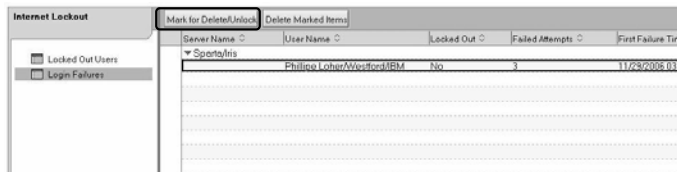
	Inherit from parent policy	Enforce in child policies
Override Server's Internet Lockout	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Inherit
Maximum Tries Allowed	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Lockout Expiration	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Maximum Tries Interval	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Lotus



## Internet Password Lockout - Inetlockout.nsf

- ▶ Created automatically on each server when Internet Password Lockout is enabled; can take up to 10 minutes without server restart
- ▶ Contains current lockout state, not history
  - Lockout history logged via DDM
- ▶ Each database has the same replica ID, but replication is disabled by default
- ▶ Replication will not sum lockouts across different servers, but can be used to easily view the lockout state across multiple servers
- ▶ Deleting a user's entry in inetlockout.nsf on the correct server will unlock



Lotus



## Internet Password Lockout - Tips and Notes

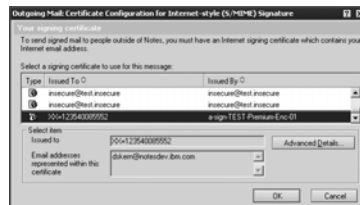
- Strikes are logged per-server, not per-domain
  - ▶ Avoids replication storm
- Custom Login Forms can be created for locked out users with single or multi-session authentication
- Use "Fewer name variations with higher security" name mapping to minimize the harm caused by an attacker
- SSO ignores all internet password policies, including Internet Password Lockout

Lotus



## Smartcard Enhancements

- Check release notes for list of newly supported tokens
- Using X.509 certificates preconfigured on smartcards:
  - ▶ Import not required
  - ▶ Lock ID not required
  - ▶ No information from smartcard stored in ID file or visa-versa
- New dialog to dynamically pick S/MIME signing certificate
  - ▶ To pick X.509 certs that exist on a smartcard but are not in the ID file
  - ▶ Can switch signing certs without changing the default signing cert in the USD

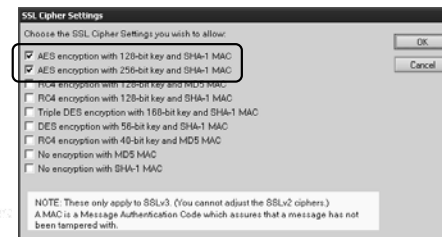


Lotus



## AES support for SSL

- Advanced Encryption Standard (AES)
  - ▶ Symmetric algorithm chosen by NIST after a five-year long contest
  - ▶ US FIPS PUB 197
  - ▶ Intended to replace the Digital Encryption Standard (DES)
- New cyphersuites supported by Domino SSL server:
  - ▶ RSA\_WITH\_AES\_128\_CBC\_SHA
  - ▶ RSA\_WITH\_AES\_256\_CBC\_SHA



Lotus



## SSO using LTPAToken2

- New token format added for Websphere 6.0 interoperability

Lotus



## Domino Security Futures

*Peter Mierswa*

IBM



## Domino Security Futures

- Single Sign On improvements
- Password and ID file recovery improvements
- Lower costs to manage ID files
- Help in meeting regulatory compliance issues
- FIPS 140-2
- Modest improvements in security administration

Lotus



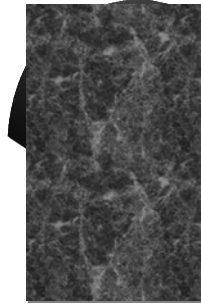
## Links

- Lotus Security Homepage – bulletins, articles, redbooks, doc
  - ▶ <http://www.ibm.com/developerworks/lotus/security/>
- Domino Blog
  - ▶ <http://www.dominoblog.com/>
- Redpaper: Security Considerations in Notes and Domino 7
  - ▶ <http://www.redbooks.ibm.com/abstracts/sg247256.html>
- Lotus Security Redbook
  - ▶ <http://www.redbooks.ibm.com/abstracts/sg247017.html?Open>
- Policy-based system administration
  - ▶ <http://www.lotus.com/idd/today.nsf/Lookup/policy>
- Domino CA & CPS
  - ▶ <http://www.lotus.com/idd/today.nsf/0/d3646dc17bea0b200256c410049d8d5?OpenDocument>
  - ▶ <http://www.ibm.com/developerworks/lotus/library/article/domino-cps/>
- Secure Messaging
  - ▶ <http://www.ibm.com/developerworks/lotus/library/article/securemessaging/>
- Security APIs in ND7
  - ▶ <http://www.ibm.com/developerworks/lotus/library/nd7-security-api/>

Lotus



Q&A – In The “Meet The Speakers Room”  
(Or Please Come Talk to Us In “Meet The Developers”)



Lotus



© 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, i5/OS, IBM Virtual Innovation Center, Series, 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.

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.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

All references to Acme, Renovations and Zeta Bank refer to a fictitious company and are used for illustration purposes only.

Lotus

