



Lotus Security in the New World of Collaboration

by John Roling

Brought to you by Voltage Security

(inside front cover is blank)

Executive Summary

Business today is increasingly global, with documents traveling between partners, sales channels, supply chains, outsourcers, and contractors. Having a trusted means for exchanging sensitive files and documents with parties outside the protected network is essential to ongoing business. For organizations with a distributed business model where internal and external parties come together as a single work community, remote collaboration is essential.

Author, blogger, and certified IBM Lotus Administrator and Developer John Roling explores why Lotus Administrators should be thinking about protecting sensitive files both inside AND outside the enterprise, and how native Lotus security can be extended across Lotus applications and beyond. Lotus Administrators will gain insight into why providing persistent protection to documents, even after they leave the Lotus environment, safeguards intellectual property and thereby solidifies consumer confidence, competitive advantage, and brand integrity.

Voltage is excited to work with IBM Lotus Quickr, the solution that provides a trusted working environment for colleagues and partners to create new ideas. Voltage SecureFile for IBM Lotus Quickr extends the security and privacy provided within the Quickr Place to the non-Quickr environment (laptops, USB devices, etc.). Using Voltage together with Quickr, sensitive information remains encrypted and private even after the files leave the Quickr Place and can be safely stored anywhere.

(this page is blank)

Lotus Security in the New World of Collaboration

By John Roling

Things are changing rapidly when it comes to collaboration. It seems like there is a hot new social network or collaborative product launch every week. People are connecting in ways unimaginable 20 years ago. It's an exciting time for everyone involved in this technology, but as our connectivity options grow, security becomes increasingly important.

Threats to Data

You can look for proof no further than the recent data breach in the UK where information on 25 million Britons (including

addresses, dates of birth, Child Benefit numbers and National Insurance numbers) were lost as two discs containing the information disappeared.

That is a data breach on a very grand scale, but smaller problems occur every day in normal businesses.

*“...as our connectivity options grow,
security becomes increasingly
important.”*

What if your head of HR accidentally sends an email containing personal employee data to someone outside your company? How about if your lead product manager has their laptop stolen with all of your company's top-secret product details in files on the hard drive? What if a salesperson's home computer gets hacked and all of your company's sales data for the last four quarters becomes exposed? I've actually seen incidents of all of these.

When I started managing Lotus software installations over a decade ago, the world was a much simpler place. Not all businesses had email, and some had simple text-based systems that wouldn't allow attachments. The web had just started to take off, but it was mainly static text-based pages. There wasn't the plethora of options to send and receive information as there are today. That said, Lotus was ahead of the game when it came to security.

Lotus Notes Data Protection

Lotus Notes has had encryption built into the core product since the Lotus Notes 1.0 release in 1989, this allowed encrypted email between users internally on the Lotus Notes network. It was simple; Notes ID files contained private key information that allowed a public/private key exchange when sending and receiving email within Lotus Notes. The reason it was so successful was the ease in which it was implemented. All an end user had to do was check the Encrypt delivery option and the message would be encrypted when sent. When the user received the email, it would be automatically decrypted and an almost unnoticeable status message would let them know that the email they had received had been encrypted.

This ease of encryption was one of the main reasons for the explosive growth of Lotus over the years. Establishments that needed the security jumped on board. Banks, Pharmaceutical companies, and government agencies could all see the need for the enhanced security that Lotus Notes could provide out of the box.

In addition to encryption, Lotus relied on a feature we all know as Replication. Replication allowed exact replicas of databases to be stored in different locations (on servers or locally.) This innovation allowed data to live wherever it needed to be. Individuals in different cities could collaborate on the same information. Mobile users could take information on the road with them. Couple this with local encryption of databases in Lotus Notes and Lotus retained its high security image.

“...ease of encryption was one of the main reasons for the explosive growth of Lotus over the years.”

This model has served Lotus very well over the years. Lotus has increased levels of encryption along the way and implemented features like Execution Control Lists to keep things like worms from spreading within Notes mail infrastructures. On the other hand, Microsoft had several highly visible instances of mass-mailing worms infect Exchange and Outlook installed bases over similar time periods.

Exponential Increases in Data Sharing

As time has gone by, users have become increasingly mobile. Hard disk capacity has grown exponentially while prices have plummeted. Networking has gone from dial-up modems to near ubiquitous high-speed access. As a result, users are more easily sharing data than they ever have. Email users think nothing of sending a large attachment. Instant Messaging clients can

allow users to transfer data back and forth easily.

Online team rooms can facilitate document sharing and collaboration.

Lotus has answered these needs by releasing software to address each niche.

Quickr allows teams to

share information in online team rooms, Sametime is one of the leading Enterprise instant messaging and web conferencing platforms, while Connections lets users interact and share data much like current social networking sites do. Notes still does enterprise-class email, and with the recent Notes 8 facelift, does it better than ever before.

“These new avenues for sharing data make for an empowering shift for the end user, but it is now causing huge problems for businesses trying to protect their data.”

Security Headaches

These new avenues for sharing data make for an empowering shift for the end user, but it is now causing huge problems for businesses trying to protect their data. Users expect access to data anywhere at any time. And while all of these products offer some levels of encryption (such as SSL protected web sites) it's not going far enough. It's too easy for a departing employee to copy sensitive documents and take them with as they walk out the door. It's also easy for a user to fire off an email to someone outside their company with an attachment that is no longer encrypted and protected via Notes.

The marketplace is getting more crowded as well. Microsoft's answer to Quickr is Sharepoint. It answers Sametime with Live Communications Server, it even can easily add internal email encryption via add-on products. Also, there hasn't been a widely publicized Exchange email worm as of late. This gives the perception that Microsoft indeed is beefing up security.

Microsoft has done quite a bit in the Outlook client to prevent similar email outbreaks, and have touted security as a top priority across their product lines. Also during this timeframe Microsoft has been aggressively pushing SharePoint as an alternative document store to Lotus Notes. The initial SharePoint offerings were fairly weak when put up against Notes and its capabilities, that is, until recently. With the release of SharePoint server 2007, IT managers are starting to take more notice of it as an actual alternative.

Security, which was once a major differentiator for Lotus, is now becoming more of a moot point. Since users can get data out of Notes (and likewise Quickr, Sametime and Connections) and send it anywhere, it seems no more secure than offerings from other companies.

Differentiation Opportunity for Lotus

I believe that Lotus now has an excellent opportunity to focus on one of its core differentiators again. Instead of just touting all the new features on each of the products they have out, they need to beef up security across all of their lines. Anti-spam, Anti-virus, Encryption, Content Filtering. These are all things Lotus can do, or at least work with

partners to make happen far more affordably and easily.


I also think they need to extend Encryption outside of the enterprise.

*“Simple encryption that extends **outside** of the enterprise and stays with documents is a sweet spot that could really differentiate Lotus from Microsoft and other competitors.”*

Microsoft already offers anti-spam and anti-virus offerings as installs or via

hosted services. Lotus needs to do the same, or partner closely with someone who can. This will keep Lotus from being exposed when Microsoft comes calling on their customers.

That just puts them on the same playing field. Where Lotus can really benefit themselves (and end-users) is focusing on encryption and document protection outside of the enterprise.



What I mean by that is simple: Make documents and attachments in Quickr, Connections, Sametime and Notes encrypted, and allow that encryption to travel outside of the company. Make it as simple and as easy as checking the Encrypt box in a Lotus Notes email. Make it so Lotus products treat all attachments the same way they treat Lotus databases. Encrypt them and enforce access control lists, no matter where the document travels.

This would benefit Lotus in a number of ways. First of all, it really solidifies the Security message that has always been one of the strongest bullet points in the Lotus list of advantages. Secondly, the branding opportunities will help their visibility in non-Lotus shops. For example, if I send an encrypted attachment to the CEO of a company using Exchange, and the CEO can open the attachment easily, and possibly see an “encrypted by Lotus” message, the question then becomes “Why can’t Exchange do that?”

Simple encryption that extends outside of the enterprise and stays with documents is a sweet spot that could really differentiate Lotus from Microsoft and other competitors. If Lotus re-focuses on security and gets that message out, they can maintain the momentum that all of the recent product releases have started.

The past year has seen Lotus really go on the offensive with their new web 2.0 technologies, a re-designed Notes client, and a renewed focus on Sametime as a platform. Lotus needs to keep that pressure on, and the best way to do that is through security. Trust me, all the features in the world won't matter if your former head of Sales sends all of your company's leads to your main competitor. I'm sure it didn't matter when personal info on 25 million end users went missing either.

This is the inside back cover.

Can't add only one page; we'd have to add 4 pages for printing.

About the Author

John Roling is a technology journalist, blogger and certified IBM Lotus Administrator and Developer. He's been professionally writing about IBM Lotus technologies since 1999 and has appeared in several technology publications. You can keep up with him at his blog at www.greyhawk68.com.

About Voltage Security

Voltage Security, Inc. is the global leader in information encryption. Based on next generation cryptography, Voltage solutions protect sensitive information wherever it goes. Voltage delivers the lowest total cost of ownership through the use of Voltage Identity-Based Encryption™ (IBE) and Format-Preserving Encryption™ (FPE). Offerings include Voltage SecureMail™, Voltage SecureFile™, the Voltage Data Protection System™ and the Voltage Security Network™ (VSN), a Security as a Service (SaaS) solution for the extended business network. Customers include over one million deployed users at Global 1000 companies in banking, retail, insurance, energy, healthcare and government. For more information visit <http://www.voltage.com/lotusphere>.

Voltage Security, Inc

1070 Arastradero Road, Palo Alto, CA 94304 USA

WWW.VOLTAGE.COM/LOTUSPHERE

TEL: +1.650.543.1280