Notes.net

Iris Today

Notes and Domino security: Past, present, and future

Interview by
Laura
Rutherford

Level: All
Works with: All
Updated: 09/04/2001

Security has always been a cornerstone of Notes and Domino. Here, three members of the Notes and Domino security team—senior consulting engineer Alan Eldridge, security architect Charlie Kaufman, and senior product manager Katherine Spanbauer—discuss the role security has played in the product over the years, what factors have influenced its evolution, and how the Notes/Domino security team participates in security standards. They also talk about the challenge of creating a secure product in today's environment and what to expect for Rnext security.

Why was security a fundamental concept of Notes back in the early days?
Alan Eldridge
Notes is a product aimed at sharing information. Anytime you share information you have to control who can access what—and so the need for a good security subsystem was evident from the start.

Notes was envisioned early on as being distributed in small shops where people knew each other—but it was always assumed that the small shop audience was not going to be the only target audience. And as it turned out, Version 1 was sold mainly (perhaps exclusively) to large organizations—in part because Lotus lacked the resources to support a large number of small customers. For large organizations, security was more important because you couldn't assume that all the Notes users in an organization were authorized to see and manipulate all of the documents.

What made you decide to use public key technology?
Alan Eldridge
In 1984, one of the scientists at MIT, Ron Rivest (Rivest is the *R* in RSA), founded a company based on the RSA public key encryption algorithm. The company had a right from MIT to market RSA. They wrote a bunch of routines to provide the encryption algorithms and they shopped it around. They banged on Lotus's door and asked if there was anything we were doing that might be able to use their encryption technology.

It was at about that time that Ray Ozzie was forming Iris, with a bit of help from Lotus, to build Notes. Because there was an obvious need for security in Notes and because it seemed like Ron Rivest's company came to us at the right time, we looked into the public key technology. We wanted mail signing and mail encryption. You can accomplish mail encryption in various ways, but really the only way you can reasonably implement mail signing is to use public key technology. And at that time RSA was really the only game in town.

Can you give a brief summary of how Notes security has evolved over time?
Charlie Kaufman
The biggest evolutionary step—starting with Release 4 and just after—has been the migration to Internet standard protocols. Notes was originally developed between 1984 and 1989, and at that time, there were no standards, certainly not for security. All this stuff got built up in a way that followed what the standards bodies were doing, but there was nobody to interoperate with. But starting with Release 4.5, we wanted to interoperate both with other mail clients in terms of encrypted mail, and we wanted to deal

with peoples' browsers connecting to our servers in a secure fashion. We had to start implementing—in addition to our own security protocols that we keep doing for backwards compatibility—all of the protocols that everybody else did in order to get interoperability.

One of the big challenges is maintaining those two streams. There are two things that make that difficult. One is backward compatibility, but we can deal with that. The more serious one is the fact that Internet standards are still immature and there are a bunch of things that you still can't do with them that you can do with the Notes infrastructure. And until either we can figure out, or the standards can figure out, a way to make those enhancements, we can't convert over because our customers won't accept the security getting worse when we do an upgrade.

Charlie Kaufman

How do you think about and address all the levels and types of security necessary in a product like Notes/Domino?
Katherine Spanbauer
We think about security from different access points. We think about how data is going to be used and who needs access to it and how to protect it from people who should not have access to it. Security is a process of evaluating the importance of the data you want to protect and how much you are willing to spend to protect it. And Domino has the features that make that easy. You can apply the features as you need them.

The advantage we have with Notes/Domino is that security was one of the key components of the architecture from the very beginning. In Release 1.0 we had the Notes public key infrastructure (PKI) and the multi-layered access control model as the foundation. These strengths have given us the flexibility to adapt over the years as security needs have changed.

Katherine Spanbauer

What Notes/Domino security features do you think are most noteworthy?
Alan Eldridge
I would say the Notes public key infrastructure. In the beginning, Notes was based on a fairly simple flat naming model. I think the idea for using that was that since we were imposing this new technology on people, we wanted to keep it as simple as possible. But the Notes networks started to grow, and the number of servers and the number of people at a given Notes site started to increase. And managing the issuing of certificates became a difficult task. For example, certificates issued by one certifier to one set of users weren't recognized by other users who were certified by other certifiers.

In Release 3, we tried to make certificate management easier with the introduction of hierarchical naming. Then in later versions, to make it easier to reissue certificates (because certificates typically have a lifetime of two years or so), we gave tools to the administrators to automatically renew certificates without the users having to initiate the renewal request. Administrators would just go to the Domino Directory and select a bunch of users and issue commands to reissue certificates to those users. And then when the users accessed their servers during the network authentication phase, those certificates would automatically be passed from the server accessing the directory directly to the workstation. And they would be stored in the user's ID file.

The result is that many users today may not even realize they are using certificates. They are given an ID file that has certificates in it when they start using the product. Administrators periodically renew those certificates, and as users use Notes, their ID files are automatically updated. The user never even notices that they are using a complex public key technology. I don't know of any other product that makes it as easy as that. There are a number of reasons why. The PKI is a core part of Notes, and so we had better do a good job on it, otherwise it is just going to be a constant nuisance to people trying to use the product. And we've been doing it for so long, it has had a lot of time to evolve.

What happens when a security problem is uncovered? How do you stay ahead of the problems?
Katherine Spanbauer

I'll start with the second part of that question first. We stay ahead because security is always a consideration. It is part of our test plans. We do rigorous QE testing. During the normal development process, we continually evaluate the product for potential security problems and we address them as we find them—ideally before anyone else does.

On occasion, a security problem is uncovered externally. These reports come to us from different sources, so the procedure for handling an incident can vary. No two are ever alike. Basically, what happens is that we verify the problem and we move very quickly to address it. If we can publish a workaround, we do so immediately. If it requires a code fix, we use the existing maintenance release process. The severity of the problem and the availability of a workaround determines where it fits in the maintenance release cycle.

We take security very seriously here. It's always a top priority and everyone works together to fix these problems. We encourage responsible reporting of security problems. Please let us know. Customers are encouraged to use the support process whenever possible. We also maintain a mailbox for reporting potential vulnerabilities at **security-alert@lotus.com**. And we work very closely with industry security organizations such as CERT. It's important that customers let us know directly of any potential vulnerabilities.

What are the main security threats today and how have they influenced what the security team is doing?
Katherine Spanbauer
There are very visible security threats that make the headlines, such as viruses and denial of service attacks. And while those can certainly be very destructive, they are not the only security threats you need to be concerned about.

Many breaches of security are done by insiders. You can't think that just because you have a firewall you are safe. Security is a process and it is all about balancing the importance of the data against the steps you can take to protect it. And not just at the application level, but at the network and operating system levels and with physical security to the systems. The technology alone is not enough. You need policies and procedures. You need to apply the right features—and that does not mean that you have to use every single one. Sometimes that's overkill and can make the system unusable in the process. You need to be able to balance ease of use and the need for confidentiality and security. So, one of our goals is to make our security features easier to use, and to give administrators better options for managing the Notes and Domino environment.

Were there security threats in early versions of Notes? How did you handle those?
Alan Eldridge
In the earliest versions, an active content attack—you know viruses, that sort of thing—was pretty much impossible because the features of Notes back then didn't provide much support for active content. At that time, one of the primary threats was assumed to be people masquerading as other people. This particular type of attack has always been very difficult in Notes unless you could actually steal someone's ID file and learn their password—just a simple password attack would not do it. The reason is because the network authentication protocol doesn't use the password directly. Instead, it uses a challenge-response protocol employing the RSA keys that are stored encrypted in the ID file. The password is used to decrypt the RSA keys, and those keys are used to encrypt and decrypt random numbers exchanged between the user machine and the server. The RSA private key never goes over the wire, and the password never goes over the wire.

For confidential data, we had two levels of protection. We had the ACL that would protect reading data that was unencrypted. And in Release 2, we extended mail encryption so you could encrypt any document in any database. So keeping confidential information confidential is something that we've always done a very good job of.

The threats that are more difficult to protect against emerged as we added more sophisticated features, in particular features that support active content. To defend against active content attacks, we added ECL [Execution Control List] support in Release 4. There is an escalating war right now between people trying to invade your system using active content and us providing features to defend against it. Active content attacks aren't just happening in Notes; they're happening all over. Every couple of months there seems to be a new virus in the news.

Have people's expectations or involvement in security changed?
Katherine Spanbauer
I think people are more aware of the need for security now. Security vulnerabilities have permeated peoples' awareness—they know it is a threat and are thinking about it more.

People are more interested in how they can effectively use security features. For example, ECLs have been in the product since 1995, but only in the last couple of years have customers thought "How can I implement this? How can I make this work?" The more open networks become, the more you communicate with people outside your own network, and the more tightly integrated products are, the greater the opportunity for security issues to arise.

Are more people skilled at breaching security today?
Charlie Kaufman
There are more people who are skilled. But the biggest thing we have seen is that there are a whole lot more people who are not particularly skilled but who are trying to do it—often times successfully. Often times a few people are clever and they will write tools, and anybody can pick up the tools and use them to go try to break into things. The mail viruses that are going around today are fairly sophisticated and it would take a fairly clever person to do them, but it does not take a fairly clever person to take one that is going around and modify it in such a way that it does a slightly different thing than the other one does and will evade the defenses that people have put up against the old one. So one of the things we are seeing is different strains of similar attacks.

We're also seeing things less in the form of break-in attempts and more in the form of viruses and worms. Break-in attempts are typically easier to conduct. There are many more exposures systems have to break-ins than to viruses and worms. However, when somebody has broken into a system, they have broken into one system and it does not make the news. When somebody launches a virus, it affects enormous numbers of people and that's what gets the press. That's an example of when a little bit of expertise can cause enormous amounts of damage.

What impact has the Internet had on security?
Charlie Kaufman
It has made security much more important because it has made all systems much more attackable from anywhere. Most systems used to be internal corporate systems, and you only had to worry about people trying to break into them from inside the company—you could deal with the physical security of your building and the trustworthiness of your employees; whereas now everything is connected to the Internet and that means people can poke at it from anywhere. Not only people from outside, but sometimes people from outside the country, from jurisdictions where first of all, nobody is motivated to go try to find them and if they did find them, it's not clear the government would be cooperative. Different governments have different policies on these things, and those that have that a lot of people who are starving can't get too

interested about somebody breaking into somebody's Web site on the other side of the world.

The other thing that's different is the motivation of the people doing this. In the past, people were trying to break in because they wanted to get something off a system. A lot of the attacks you hear about now occur because people are actually seeking publicity. Most criminals don't want to get caught, but the people who are attacking things on the Internet often times may not want to get caught but certainly want people to know that they did something.

How have security standards evolved over the years? What have been the major influences on the evolution?
Charlie Kaufman
In some sense, security standards have not evolved as much as grown to cover more areas. Once something works, there's motivation on all sides to stop changing it. In the early days, there were no security standards. The only one I can point out as having evolved is the cryptography that we use. That has evolved because the U.S. government and certain other cooperating governments around the world placed restrictions on the use of cryptography because they did not want people to interfere with their ability to wiretap.

There used to be laws in the United States, in the form of export control laws, that if you build encryption software that was good enough that the government could not do wiretaps, then you were not allowed to ship it outside the country. And this caused all kinds of complexity. Notes for a while had three versions of its cryptography. It had a version that it sold inside the United States and Canada. It had a weaker version that it sold outside of the U.S. And then it had a weaker-still version that it sold in France because France would not let us import the version that the U.S. government let us export. Some companies would go to the least common denominator and ship worldwide what they shipped to France. But we did not do that. We didn't regard the security as being acceptable, so we jumped through various hoops with multiple versions. Most of those restrictions have gone away, so now we can ship a single version—one that has the strongest cryptography—worldwide. Cryptography is the thing that has really evolved. Other than that, it's really what standards have developed.

Can you talk about some of the standards that have developed and how they have developed?
Charlie Kaufman
There have been standards bodies standardizing things as early as the 1980s. For example, the first version of X.509 public key certificates were standardized in 1984—but that was not when people started using these things and deploying them. SSL [Secure Sockets Layer] came out around 1994 or so. It was a Netscape development and it sort of became a de facto standard that now everybody, including us, runs and operates. S/MIME came even later but is now emerging as the interoperable standard for encrypted and signed mail.

We need more standards. We need standards for how to do strong password-based authentication, for example. Right now, even though people within their organizations can use cryptography to do things, most systems across the network either are authenticated with a credit card number and expiration date or with a user name and password. Getting people certificates and getting them enrolled in public key infrastructures so that others who eavesdrop on their conversations can't go back and impersonate them is a real important thing that is still developing.

Also, there are two kinds of standards. There are the standards that are sort of what some committee has said the world ought to do. Then there are de facto standards that everybody have accepted and used—usually because someone designed something and published it and others copied it.

Sometimes, a standard can be both. For example, TCP/IP is both a written standard and the standard everybody uses to talk to each other. But there are a lot of standards that a committee has blessed but nobody deploys. And if you want actual security, you often have to go out and do the thing that is not legally a standard but is the thing that everybody implements and uses.

The other thing that is happening now and is becoming important is IPSec, which is a security standard for encrypting network connections. SSL was designed to encrypt connections between peer applications, and IPSec is designed to connect whole networks to each other. So you can encrypt connections between the firewall of your company and the firewall of another company to encrypt all the traffic that goes over the Internet. Applications like Domino implement SSL because nothing like IPSec was available. If IPSec becomes universally deployed in networks and operating systems, applications won't need to do their own connection encryption, which will make it a lot easier to deploy them.

How does the Iris security group participate in security standards?
Charlie Kaufman
There are a number of ways in which we participate. The IETF is the standards body that does the most in the Internet space—although there are other things that are important—and they hold periodic meetings that I usually attend and sometimes other people from Iris attend. I've participated in various standards efforts both by writing proposed text for some of the standards and by talking with the engineers from other organizations trying to find designs that will meet both our goals and their goals.

Standards work in both a formal and informal process. The formal process is where you go to meetings and agree on things, but what is actually more valuable is the informal process that often happens in the same venue. For example, when I get to meet my peers at other companies who are trying to solve the same problems we learn that "Yes we are going to try to work on a standard, but that is going to take years. So what are we doing now and how might we be able to make things work better together?" A lot of things really involve three- or four-wise vendor cooperation in order to get things to work. SSL is a beautiful example that Netscape rolled out. They published the specification and then everybody else implemented it and tried to interoperate—and now it's being proposed for standardization. Someday it will officially be a standard, but in the meantime everybody is using it and has been for years.

Have products like iNotes Web Access presented different security considerations? How about the browsers themselves? How do you address these various scenarios?
Katherine Spanbauer
When we talk about security considerations for these products with our existing customers, they are familiar with the features they have had in Notes for years. They rely on them. So when we bring access to Domino servers from a different client environment, where we only really control half of the equation, it presents some interesting challenges. We have to take into consideration what the browser capabilities are and realize that we don't have control over how the browsers handle certain things. It just means we need to be little more creative about how we bring some of the Notes features to a non-Notes environment. It also means we need to find ways to off-load client functionality to the Domino server in order to provide similar features.

For example, Notes has the Execution Control List to protect client workstations from potentially damaging code from executing—something a Web browser doesn't offer. So for iNotes Web Access, we designed an Active Content Filter mechanism to remove potentially malicious code before delivering it to the client. The feature doesn't yet offer the same level of granularity that Notes does, but we've taken our experiences with Notes and applied them to new client models.

What about wireless? How do you think that will influence what we do? Can it be secure?
Charlie Kaufman
Wireless is not inherently any easier or any harder to secure than what we are all using now. What it does do is increase motivation to implement security because the ways of attacking the system are so much more obvious. We can leverage the investment we've already made in security to our advantage in the wireless world.

A phenomenon that people associate with wireless, but which is really a separate challenge, is that wireless devices tend to be small and have limited user interfaces and limited computational capacity. The limited computational capacity will be fixed by Moore's law, but handheld devices require new approaches for simplifying user interfaces. There's simply no way users can manage complex configuration decisions—or at least we can't expect them to get them right. So we will have to rethink some of our designs and in the process we have the opportunity to make the systems more secure. Unfortunately, what we've seen so far has been a lot of systems rushed to market without adequate thought to security. But I'm still holding out hope that this will change.

Can you talk about Rnext security features?
Katherine Spanbauer
We have some great features on the horizon. I'll highlight a few of them. We have introduced a completely new Certificate Authority (CA) application, which supports the PKIX Internet Standards and which allows administrators to use a single interface to manage both Notes and Internet certifiers. The CA process can be used to manage the issuance of certificates without needing direct access to the certifier itself. An enhancement to Notes certificates is the ability to issue certificates that support longer key lengths of 1024-bits and are in X.509v3 format.

Some of the most popular requests from customers have been around password management. We are introducing new features that enhance the ability to manage both Notes and Internet passwords. Let's talk about the Notes enhancements first. For example, password strength is stored in the user's ID file and is set when a user is registered. If you have been deploying clients for years, your password policies may have changed over time. Currently, the only way to change this setting is by manually recertifying the user's ID. With Rnext, administrators can use policy documents to specify password settings. Administrators can choose between password length or password quality for validating password selections and setting the strength. The next time the user authenticates with their home server, their ID file will be updated with information from the policy document.

The Internet password management features are new to Rnext, but they are based on functionality you have with Notes. So, you are going to be able to define expiration intervals for Internet passwords. You can apply either password length or quality—just like you do for Notes—to the Internet as well. Also, we've added an administrative option to synchronize the Notes and Internet passwords so that when a user changes the Notes password, the user's Internet password will be updated as well using the Administration Process.

Another major area where we have made enhancements is in managing ECLs. Administrators will be able to dynamically update users' workstation ECL settings based on policy documents. These policies will enable administrators to define a schedule for updating users' ECLs. This enhancement will make effective ECL policies easier to deploy and enforce.

We've also made enhancements to agent security so that the administrators can be more restrictive about the types of agents users can run. For example, we've made the distinction between activating agents versus enabling agents. This may not seem all that significant, but what it means is that users will not need designer access to their mail files or have access to run LotusScript agents on the server to use the Out of Office agent in their mail file. And of course, this feature can be used for customer-designed agents as well. It's a great enhancement.

We have also updated the underlying S/MIME library to add support for S/MIMEv3. And we've added support for PKCS#11 in the Notes client, which means you can use smartcards to protect your Notes IDs. That's totally brand new and another layer of protection.

About Alan Eldridge
Alan has had the good fortune to be a software developer with Iris for 15 years, working mostly in the areas of networking and security. He was the principal designer and implementer of the Notes public key infrastructure. Prior to joining Iris, Alan worked for Digital Equipment Corporation writing networking and clustering software for the VMS operating system. When he is not working, he can usually be found with his wife Susan either travelling or at a Bob Dylan concert.

About Charlie Kaufman
Charlie works for Iris Associates as Security Architect for Lotus Notes. He was a member of a National Research Council expert panel on Information Systems Trustworthiness that produced the report "Trust in Cyberspace." He participates in a number of IETF standards efforts and is chair of the Web Transaction Security working group. He is coauthor of the book *Network Security: Private Communication in a Public World*, published by Prentice-Hall. Previously, Charlie was Network Security Architect for Digital Equipment Corporation. He holds over 25 patents in the fields of computer security and computer networking. He holds a B.S. from Bates College and an M.A. from Dartmouth College, both in Mathematics.

About Katherine Spanbauer
Katherine is the Product Manager for Security, primarily focusing on Notes and Domino. Her current responsibilities include representing customer requirements to development, triaging critical issues, and communicating product features both within Lotus and to customers. Since joining Lotus in 1992, she has held various roles in the Technical Support, Professional Services and Product Management organizations. Katherine is a graduate of the University of Wisconsin, where she earned her Bachelor of Business Administration degree.

About Laura Rutherford
Laura worked as a user assistance writer for Lotus until she had her daughter, Kate, in January, 1999. Since then, she had another daughter (!) Maggie, born in September, 2000. Now Laura spends most of her time taking care of her two daughters, two dogs, and one husband (basically in that order). In her free time, she loves to read, run, and, believe it or not, write articles for *Iris Today*.