Authenticating Today's Distributed User With Consistent Sign-On Technology

BY RARES PATEANU

It's becoming increasingly difficult to keep track of all the entry points into your systems and to secure all of them in a consistent, easy to use and cost-effective way. Single sign-on is an attractive alternative, but it is falling short of initial expectations. A more practical approach for today's data centers is consistent sign-on.

SECURITY has always been the Cinderella of the IT industry. It stays hidden somewhere in the corner, does not get to go to the ball too often, and usually gets noticed only when something has gone wrong.

What does it take to put security issues in their rightful place among the priorities of your business? There are several factors that will change the way security is looked at in the enterprise:

- The good old cost/benefit ratio (or rather cost/loss ratio in this case):
  - Simply put, as the cost of lack ofsecurity increases, so will the attention level given to security issues up there in the rarefied atmosphere of the boardroom, where big bucks spending decisions are made.
- The increased vulnerability of corporateassets coming from the diversification of the IT infrastructure:
  - More entry points, more technology and a wider distribution of computing may bring about a lot of business advantages, but also carries an increased security exposure.
- Last but not least, help is coming from a very unlikely source, the auditors:
  - A number of the big audit firms have started to offer security assessments as part of their annual audits. Believe me, you don't need a better attention getter than board members reading the one document they really pay attention to each year, which says that the company has substantial security exposures in its IT department.

But surely all these people making billions in the remote access and Internet commerce business will give the network and security administrators all the security tools they could dream of. That's the good news. But that's also the bad news. Explosive growth has never been very conducive to standards and convergence, quite the contrary.

The bottom line is that networks have more entry points, spread over ever larger geographical areas. At last count, a large IT infrastructure could have a few mainframes, maybe an SNA network, some Novell networks, a few NT domains, remote access servers, web servers,proxy servers, firewalls, routers, etc., in various shapes and sizes, each with its own idea of what security should look like.

THE SECURITY CHALLENGE OF A WIRED WORLD

With every computer connected in some way with just about every other computer, it is becoming increasingly difficult to keep track of all the entry points into your systems and more importantly, to secure all of them in a consistent, easy to use and cost-effective way.

A friend of mine recently complained to me that he has at least eight distinct passwords. That got me counting! Now, I am the consolidator type. I have tried over the years to minimize the number of passwords I need by using the same one whenever possible. Yet, including credit card and bank card PINs, all kinds of access codes and computer passwords, I have 11 distinct passwords, several of them being reused multiple times. That does not include the password to my bank's safe deposit box. I have not used it in years, and I could not remember it if my life depended on it. (Thank God, I still have the key!)

Of course, all these passwords expire at different times, have different lengths and structures, and present a substantial challenge to my memory. So, the time has come to reveal my one and only shameful secret: Yes, I do write my passwords down! Now, my bank account is not worth breaking into (I can't find money there even with properly authorized access), but maybe your corporate data is worthy of a bit more care, not to mention that ounce of prevention!

The risk of password disclosure is not the only problem: Different security systems and databases imply different administration procedures, meaning more training, more personnel, and higher cost. Removing authorization is hard to do in a timely and consistent manner, possibly leading to serious risk of unauthorized access (I personally know people who left their former company months or even years ago, but they still have a way to sign on to some of the systems). Audits are difficult to do and even more difficult to correlate. Forgotten passwords require frequent resets, adding to administrative burden and costs. So, is there a solution?

The Growth in Internet Commerce

Consider these conclusions reached by the International Data Corporation based on their Internet Commerce Market Model (all numbers are world-wide, from year-end 1995 to year-end 2000):

The number of devices accessing the web will grow from 12.6 million to 233.3 million (the .3 is the part that baffles me!) The remote access business will grow from $1 billion to $4.9 billion. Commerce on the Internet will grow from $100 million to $3 billion (a staggering 3000 percent growth!) … and the numbers go on and on … !

SINGLE SIGN-ON: MYTH OR REALITY?

The obvious solution to the long list of problems mentioned is known as single sign-on. The idea is simple and beautiful: one user, one sign-on, no matter where you are, how you are signing on, which resources and how many of them you will access. Sounds a bit like one person, one phone number, anywhere, anytime. And, unfortunately, it is just as unlikely to happen! For something like single sign-on to happen, three factors have to come together:

- a standard set of credentials that are:
  - reasonably easy to issue and administer
  - fully secure and capable of authentication and non-repudiation
- an ubiquitous mechanism for verifying the credentials
- wide acceptance of the credentials as adequate

This can be compared to the credit card system. The credential is the credit card itself. As with anything else that has a financial value, theft, fraud, misuse, and counterfeiting are an issue, and an expensive one at that (some estimates put it in the billions of dollars a year). However, overall, considering the amount of business that credit cards bring, they are an acceptable credential.

Dial-up devices and phones have made the verification of a credit card at least as ubiquitous as a phone line and the acceptance rate is also extremely high. As a result, in most of the industrialized world, just about everyone has at least a credit card, and "Single Buy-On"is a reality. How does the IT infrastructure measure up to these criteria?

The Credentials

A lot of work is being done, but we are not there yet! Digital certificate technology and smart cards seem to be a match made in heaven. Digital certificates can be extended with any kind of digitized information, including biometrics, so storing an enhanced certificate on a smart card that requires a PIN will combine all three traditional authentication criteria: something you have, something you are, and something you know.

The trouble is there is no complete standard. The X.509 standard defines what a basic certificate looks like, but as to how to use them and how to extend them, every vendor is on the "BYO (Build Your Own) and get it to be the de facto standard" track. Can you imagine the credit card scenario with every bank issuing credit cards in their favorite size, shape, thickness, and information recording technique? And that's exactly where we are today with certificates. It's as if we basically agreed that all credit cards should be made of plastic, but nothing more.

The Verification Mechanism

Assuming we lined up all the ducks with the credentials, we now have to do the same with the verification devices. Most key players in the hardware business have plans in place to build smart card readers in all the PCs over the next few years. This trend is more advanced in Europe, where the use of smart cards for various purposes has taken off a lot faster than in North America. But when you add the time to roll out the new technology to the time it takes to make the enormous number of PCs already out there obsolete, it is going to be a while before the smart card reader will be as

Computer-Related Crime

If security is not at the forefront of your shop, it may be understandable. It's not sexy, more often than not it annoys users rather than excites them, it is a cost center (hardly anybody will pay you more for what you are giving them because it is more secure). In brief, it's like life insurance: You buy it reluctantly and hope to never really use it! But is it ever costly when it fails! In 1997 the Computer Security Institute and the FBI conducted a study of computer-related crime. Here are some of their findings:

- More than 50 percent of the companies surveyed experienced unauthorized use of computer systems during the 12 months preceding the survey — this is 7 percent higher than in the previous year.
- total known losses from security incidents over one year: $100 million
- average loss per fraudulent use of computer systems: $957,384
- average loss per theft of proprietary information: $954,666
- average cost per system penetration: $132,250

much a part of your home computer as the diskette drive is today. And that's only for vanilla certificates. If you want biometrics, add to that the need to roll out the devices required to support that side of the equation.

> With every computer connected in some way with just about every other computer, it is becoming increasingly difficult to keep track of all the entry points into your systems and more importantly, to secure all of them in a consistent, easy to use and cost-effective way.

At this point, you may ask: What if we take the simpler approach of vanilla certificates, without smart cards and biometrics? Browsers already deal with certificates, so haven't we solved all the problems? Unfortunately, not quite. The crux of the matter is that single sign-on requires changes to every client. Something has to be there to intercept the request for presenting credentials and present them to you the second and all subsequent times. With user ID and password combination, that "something" is usually some script. With plain X.509 certificates the browser does the work. In the future, hardware will do it (and that is part of the beauty of the smart card solution). But something has to be done on the client. And that adds complexity and cost to the single sign-on solution. What would credit cards be worth without all those devices you insert them into to make purchases, obtain cash, etc.

The Acceptance

And if all this is not enough, what about acceptance? After all, the reason why credit cards are so useful is because they are accepted just about anywhere. Authenticating a user by way of user ID and password is done from many security- sensitive applications today through the use of application programming interfaces (APIs). Using any kind of new credentials would require all the applications to change, not unlike the way businesses that want to accept credit card payments must adjust their processes to handle this new form of payment.

ARE WE EVER GOING TO GET SINGLE SIGN-ON?

I wish I knew! Many companies have bet heavily on it. Some have their entire futures riding on it. Maybe that is why they keep saying that it's here, only to put the brave souls attempting it through a lot of pain and disappointment. Notwithstanding some uncommonly simple scenarios, I have yet to see anyone who claims to have a successful single sign-on implementation. One thing I do know: Even if we do get single sign-on some day, that day is not any time soon.

However, that does not mean there is no solution for the security problems discussed earlier in this article. If we reexamine that list of problems, two ideas spring to mind:

1. Since multiple security databases cause much of the problems, we could achieve a lot just by eliminating the need for multiple security databases (or at least eliminating some of them).
2. If multiple security databases were required for some reason, synchronizing passwords across them would at least eliminate the need for multiple passwords, even if multiple sign-ons were required.

This approach is referred to as consistent sign-on. It works like this:

First, eliminate as many of the multiple security databases as possible or practical. This can be done if the network component doing the security administration can be configured to relegate authentication and authorization to a third party. Fortunately, in many of these cases standard industry protocols such as RADIUS and TACACS+ are used, and these protocols allow such a third-party authentication scheme. Ideally, a single security server (with appropriate redundancy and back-up provisions) will be in charge of authorization and authentication.

Second, implement password synchronization procedures to ensure the consistency of password across the remaining security databases. In order to make this a really effective solution, the synchronization must be achieved in real time. Any change in the user's password or status must be immediately reflected in all the relevant databases.

The beauty of this approach is that it does not preclude the use of new authentication technologies, such as certificates. These new technologies can be integrated as long as the single security server can be configured to accept the new credentials. And of course, you need to make the changes to a single environment. The benefits of this approach are many:

- reduces administrative complexity and cost
- leverages existing investment in equipment and skills
- substantially lowers implementation costs:
  - no code needed on the client
  - no changes need be made to the applications
- integrates new authentication technologies

Typically, the security application used would be that on the mainframe (or host). Security tools like RACF are considered practically impenetrable, so not only are they trusted, but they are also well known and most companies already have the required skills. Because neither applications nor clients have to change, the implementation costs are substantially reduced. Ongoing support costs are also reduced because of less administration and fewer password reset requests — some security administrators claim that up to 70 percent of their help desk calls are related to passwords, so you can see why this would be a benefit.

OK, so what's the catch? Nothing is that good without a price to pay! Well, yes, there are drawbacks, too.

First, a single security control, administration, and audit point is wonderful in its simplicity, but what happens when the security server or the communications to it are down? To take care of those circumstances, one can usually do some or all of the following:

- use the most reliable equipment for this task (uptime for mainframes is usually in the 99.9 percent range)
- have several security databases and configure authentication with secondary (or more) IP addresses for the security server
- build redundant access paths into your network topology

In my opinion, you have a choice between waiting for an expensive pie-in-the-sky or going for a reasonable, cost-effective and easy-to-implement solution today. How much longer can you afford to be vulnerable? The answer to this question will lead you to the choice that's right for you.

Secondly, password synchronization is less valuable if users have different IDs for different network entry points. There is no simple solution to this problem, but there are at least two things you can do to help. To the extent that is possible and practical, implement a consistent user ID policy. Although doing it 100 percent is in my experience rarely possible, some degree of consistency is usually achievable (not to mention desir-able). For those cases when consistent user IDs cannot be achieved, you must select a synchronization tool that can provide a customizable user ID mapping table. The user would still have several IDs, but at least the passwords would be the same and more importantly, they would be synchronously updated, revoked, reinstated, etc.

Last but not least, consistent sign-on does not eliminate the need to sign-on repeatedly (as single sign-on promises to do when it grows up). However, depending on the cache capabilities of your security server and the other components of your system, the number of sign-ons may be reduced. For instance, using certificates for web resource authorization will make use of the browser's built-in certificate handling features and will effectively submit the user's certificate automatically every time the web server requests credentials. But your payroll application is still going to ask for a user ID and password every time you want to use it and there is very little that can efficiently be done to improve on that.

In brief, consistent sign-on is not perfect, but it is a reasonable approach with a very good return on investment (ROI). It gives you today most of the benefits that single sign-on promises for tomorrow and does it at a fraction of the cost.

In Meta Group's words: "Bottom line: For users that cannot afford to wait for true single sign-on products, we believe consistent sign-on (a.k.a password synchronization) is a viable alternative. We believe the related benefits of simplified logon, consistent security, and ease of administration justify its acquisition based on a three-year cost of ownership."[1]

In my opinion, you have a choice between waiting for an expensive pie-in-the-sky or going for a reasonable, cost-effective and easy-to-implement solution today. How much longer can you afford to be vulnerable? The answer to this question will lead you to the choice that's right for you.

Rares Pateanu is director of marketing for Blockade Systems Corp., Toronto, Ontario, Canada. He has been involved in the data processing industry for more than 20 years, in R&D, system software development, applications development, security, customer service, management and marketing. Rares teaches a variety of Computer Science subjects at York University in Toronto, and is an award winning frequent speaker at computer science conferences all over the world. His articles on various data processing technologies have appeared in many prestigious computer publications. He can be reached at rpateanu@blockade.com.

[1] Enterprise Data Center Strategies, File 709 dated January 8, 1998. © 1998 META Group,Inc.