TRANSCRIPT

PROOF POSITIVE:
NEW DIRECTIONS FOR ID AUTHENTICATION

PANEL 4

APRIL 23, 2007

>>AVIVAH LITAN

Hi, I just wanted to point out that the session starts at 2:15. The printed schedule says 2:00, but it ended up that we're starting at 2:15. So just in case you're wondering why we haven't started yet. All right. Thank you very much for cooperating with the delay. And we will begin now with our next panel.

Thank you very much for coming back from lunch to hear about authentication technologies. Quite often, people mix up identity proofing and authentication. We've heard about identity proofing in the previous panel especially. And, assuming that you know who you're dealing with, then you give them an authentication credential. So we're talking about after you've proved the identity, now you want to give that person a credential so that when they come to your branch or they come to your Internet site, they can prove that they are who they said they were when they enrolled. So authentication is different than enrollment and identity proofing, although they go hand-in-hand.

We're gathered together with a very distinguished panel that represents all the different gamuts, not all of them, but many different gamuts of authentication technology. And we'll hear from each of them and then we'll open it up to questions and hopefully you'll participate. You can interject at any point after the presentations. So I'm just going to run through the panelists, their names and titles, but their bios are in the handouts if you want to learn more. On my immediate left is Victor Lee. Victor is a senior consultant for the International Biometric Group and he'll be discussing the different methods of biometrics. To his left we have Phillip Hallam-Baker who is a principal scientist for Verisign, for security at Verisign. And then next to Phillip, we have Neville Pattinson to talk about Gemalto and their perspective. He's Vice President of government affairs and standards. And then to his left is Marc Gaffan from RSA Security, which is now the security division for EMC. Marc is director of the consumer solutions business unit. And to his left is Micheline Casey, who is senior director of identity management at ChoicePoint government services. So we've got biometrics, we have PKI and SSL security, we've got risk-based authentication, we've got smart cards, we've got knowledge-based authentication -- all that knowledge is here on the panel. So we'll start with Victor and he'll give us a short presentation.

>>VICTOR LEE

Just to see if you're on your toes after lunch, if you can identify which one's actually mine. All right. Here we go. So, first, I'd like to thank the organizers for inviting me and for

vulnerable point on how a person could trick the system into believing they are somebody else.

Let's get more to the issue of biometrics and how they help. One of the main points that we had discussed earlier, or that some of the panelists had mentioned this morning is the issue of convenience. And oftentimes there are ways in which biometrics can be deployed to facilitate a process such as transaction. There is a company such as Pay by Touch which has been going around and their basic concept is let's utilize a fingerprint so that you can tie it to your checking account. When you want to go to the cash register, you put down your fingerprint, it automatically deducts whatever you purchased. No need to bring a card with you, no need to bring any type of other device.

But the trick with this is that convenience is going to be inversely proportional to security. When you try to move towards one that's a little bit more favorable of reducing the number of things that you have to bring with you, you may reduce the amount of security that you have available. And we have to be careful because there's a lot of times when security is often let loose as the result of trying to push people through increased through put, through again the payment solution, the payment terminal area.

Think about the last time somebody actually took out your credit card when you are making a purchase and compared that signature on the back. If you're like me in the last 20 years, I haven't had it done a single time. That aPbofsuu of thi018 -1.15 TlTT0 1 Tf0y2 0 Td[(b,J0.0001 Tc -0.0

We have to focus on distinct personal user ch

when you're talking about an issue such as identity theft, you're going to need a tradeoff between convenience and security, and I would personally urge a direction more in the line of security. What that means is let's try to aim for, what I call, the identification trifecta. By that I mean, we have, what you have, proximity cards, swipe cards, keys, fobs things of that nature. We've had things that you know. PINs, passwords, but now we also have this tool. Over the last decade we have developed this technology called biometrics that enables us to have not only what you have, what you are but also what you know. This combination of three very important factors, multi-factored solutions, if you would, can really lead to what I feel is going to be an efficacious counter identity theft system.

But we've got to be careful, and this is where I'll conclude, because biometrics are not a fool proof guarantee. We still have to use common sense; we still have to use good practices.

So, first of all, what RFID isn't, or, rather, something that is often talked of as being RFID but really isn't, and that is you can take a smart card of the type that Neville is going to be discussing later with really strong security protections and you can add a wireless component and you can end up with a contact list. Smart card that some people will call a RFID card. What I'm going to be talking about is an EPC global RFID tag. The two are not the same. The contact-less smart card is to provide you security inexpensively at low cost. The RFID EPC global tag is designed to be negligible cost. We're talking about cents. Small number of cents. And they're designed to be produced in very, very large volume. We're talking about 100 billion a year. There are two manufacturing plants already set up to manufacture these tags at the rate of 100 billion a year. So that means that everybody in this room is expected to be having 20 of them a year. That's a lot.

So what are they for? They're all about supply chain automation. And here we have containers. Container ships are the reason why we have the quality of life we do today. If you look at the growth that we have in the western world, it's because of globalization, it's because you can now ship anything from anywhere to anywhere else on the planet cheaply and economically without having your ship tied up in port for days or weeks on end when you're unloading and loading it. The idea of this EPC global RFID tag is to enable a similar transformation of commerce by automating the supply chain at a deeper level further on down the line.

Now there's a problem here from my point of view as security advocate and that is that the security model of RFID tags is a security model of the bar code; i.e., anybody can read the bar code on your book or your product. There's no confidentiality there, and also, anybody can go to a photocopier and they can make you a bar code. Or, you can go to a site on the web and it

supply chain so you can't attempt to introduce fakes? It's a very challenging problem. Eventually you get to the idea of, well wouldn't it be nice if you could have that 5 cent tag have similar security capabilities to the $5 tag? Which means that you have to have a public key cryptography algorithm that you can describe in 20,000 gates or one slide. I'm not going to do it to you. I'm not going to give you an elliptic cryptography primer one slide. The technology is possible there, and if you're going to be thinking about schemes that involve people carrying around these RFID tags please, please talk to the technologists who are developing the next generation of RFID tags. We're not just the only folks who have a dog in this race but there are solutions. You don't need to be stuck with MIT's 10-year-old design now. There is another generation of technology. And you really need to be looking at it.

And just one final observation. You may know this guy. This is Victor Thurman. And he invented the first RFID tag. He did it under very specific circumstances. He invented it in Moscow after he had been kidnapped off the streets of New York by Stalin's secret police. And it was invented as an espionage tool.

So don't be ashamed of saying there are security and privacy implications. This is a technology that could be abused. What I'm saying here is that do allow us technologists a say and we can prevent some of those abuses. So on to my second point, which is extended validation certificates.

We have a problem with SSL certificates today. And some of you probably know about it. It's obvious. Not big enough for you? Well, that's the infamous padlock icon which appears in your browser. That's the only security information you get these days. That's the problem. It just isn't obvious enough. The other problem is that the user looks at that and thinks "it's safe for me to do e-commerce," and actually technically what it's saying is the communication between you and the server is encrypted. But are you talking to the right server? Are you talking to the bank you think you are?

And here is another problem in that when the SSL certificate was first introduced and Verisign introduced the first public SSL certificate, Verisign class 3, we were authenticating specifically the bank, the organization behind it. Since then there's a new type of certificate that's come along where they authenticate the ownership or rather holdership of the domain name. So instead of authenticating Busy Bank Incorporated, we're authenticating busybank.com. And there are legitimate reasons why you might want to have that. If you want to have a web cam in your house, you want to encrypt the communication between your browser and the web cam when you're looking to see what's going on in your house or maybe in the yard or whatever. You want encryption there. But you probably don't want to be authenticated to the same level of assurance that you'd want someone to authenticate your bank.

So these problems led a group called the CA Browser Forum to come into existence. And it's a group of CAs [certificate authorities], all the leading CAs, about 20 of them at this point and the major providers of browser clients. And they have been working on a set of criteria called extended validation. And at this point it is not an agreed standard. We're hoping to come to it. However, it is now deployed.

If you have the latest version of Internet Explorer 7, you get a new user experience if you

this afternoon is my opinion and not the opinion of the committee. Okay. Disclaimer over.

the card visually.

Smart card security is all about trust. It doesn't trust; this little chip doesn't trust anything until it proves what's going on in the world about it. It needs to know that there's somebody here that should be using it. It needs to know that it's communicating to a terminal that it should be allowed to talk to. This physical security is in the silicon. The way it's designed, the silicon vendors spend a lot of time creating all sorts of sensors and counter measures at the silicon level to start people probing and taking them apart. We have hardware security mechanisms. Tamper detectors and scrambling of buffers on the CPU. We have card package security mechanisms where you can't peel them apart or dissolve them and get back at the chips.

Operating system. As I mentioned this is the strength of our own company where we

transportation worker identification credentials 5201 registered traveler, first responders, these are all in place today and many of you have probably seen these or used them.

Let's move on to the second subject. Public infrastructure. The easiest way…I'll let you read this. The easiest way to describe this is PKI is a way of life digitally. Verisign are one of the key providers in this area of certificates, which I'll discuss shortly. PKI is about trust. How do we dis-establish between one person and one other entity? How do we form trust? And that is by having certificates which are a digital representation of how we're going to validate and authenticate each other.

So PKI infrastructure is a closed system of certificate-based credential management. Everybody has a certificate. Everybody is going to have keys associated with that. You have physical security for buildings that you might be able to use within your PKI. Logical security to log into your desktop to secure your email by digitally signing your email and doing encryption by key exchange using digital certificate technology. Secure websites through SSL that you're familiar with the little lock that was described and further on for the extended authentication that we now see. Remote access through VPN and dial-in are all part of certificate-based technologies to allow you to authenticate yourself securely to those services. File encryption and so on. And we don't need certificate authorities to manage these trust chains of these certificates to work back who we can trust and where we're going to get them from.

Identity management systems are incredibly important to PKI. You need to know who you have in your system and who they are therefore going to be trusted to communicate with. Obviously, if you involve cards, there will need to be a card management system to support that, too. The certificate is a question of trust. How do I trust the credentials of the other party? Well a certificate is your public key of a key pad. For PKI folks, you have a one time generation of two pieces of information, a public key and a private key. Two mathematical related keys. One key you keep secret; the other key you keep public. And by making a certificate out of the public key, you can allow people to communicate with you and you can communicate with them with a deal of trust.

Certificate authorities are used to create the certificates to then provide them and to the public key infrastructure. You have to publish a public key and a certificate in order for people to be able to receive it and to validate your communication with them. There are standards involved on certificates. The X509 standard is the core of that. Certification authorities are those entities that are presenting themselves to provide that root of trust. How does an enterprise, for example, get their own root certificate? They go to a certificate authority. They get issued that and then they start to create certificates with their own certificate of authority and so on.

There is a tree of trust that comes from fixed points within the infrastructure. So common PKI cryptographic services provided by a combination of smart cards and PKI, authentication i.e. establishing trust. How do I know who am I dealing with right now? Can I trust them? What is the purpose of the communication? Is it valid? Is it authentic? You can do that with PKI and with certificates. You can perform bulk encryption for disks and so on communication. Digital signatures, as I said, for signing and verifying the integrity on

PKI-based authentication and authorization mechanisms to ensure that only trusted devices can access the network. Implement strong encryption protocols for data in transit and at rest to protect sensitive information from unauthorized access. Regularly update and patch all network devices to address vulnerabilities and maintain the integrity of the network. Implement network segmentation to isolate critical assets and limit the potential impact of a security breach. Deploy intrusion detection and prevention systems to monitor network traffic for suspicious activities and respond to threats in real-time. Conduct regular security audits and vulnerability assessments to identify and remediate potential weaknesses in the network infrastructure. Provide security awareness training to employees to educate them about best practices and potential threats. Establish incident response procedures to quickly and effectively handle security incidents and minimize their impact. Implement multi-factor authentication for remote access to the network to enhance security. Regularly review and update network security policies and procedures to adapt to evolving threats and technologies.

that unique device ID or not, is that still my device?

Another thing I'm looking at is a networking infrastructure of sharing information among institutions. Today there's a network in place that shares real time information of fraudulent activity such as IP addresses and device IDs that have been used previously to commit fraud. If you have insight to that type of intelligence, you can make smarter decisions on when to authenticate people.

Think about if we had no Secret Service, if we had no underlying intelligence, what type of screening we'd have to go through to get into buildings, to get through airports. The reason

individual. Is this person claiming to be Micheline really Micheline Casey? And how we do that is through a generation of what's called a smart quiz. The smart quiz typically can be anywhere from 3 to 7 questions based on historical data about that person's identity. Those questions are culled from a combination of public record sources, proprietary data sources and private data sources that perhaps our customer or the government agency owns. The level of authentication is dependent on the risks associated with that particular application. And so the smart quizzes themselves are extremely customizable depending on what the client's needs are and again the level of fraud and also the demographic base of their typical target population.

Once we've authenticated that the person who is claiming that identity truly does own it, then the client can go ahead and grant the authorizations, the rights, the privileges, et cetera, that the person is trying to get. The next thing about knowledge-based authentication is it's an extremely flexible and complementary technology to any of the other technology that the other panelists have talked about today and some of the others that haven't been mentioned, but where our primary focus is again on that upfront identity authentication piece. It is the most critical piece in an enrollment process or credentialing initiative.

today. So we are making progress, but these technologies are much easier said than done. And there's still a lot of implementation issues. So I'm going to ask the panelists to summarize the strengths of their technology in one minute, 60 seconds. You maybe could even go to 90 if you really need it. And then we're going to go through the challenges of the technologies. So we'll spend a minute each on the strengths. Just summarize what your technology does and why it's the best or why you promote it. And in your case, Phillip, I would talk about extended validation certificates as opposed to RFID, but it's your choice. And also understand that Marc's not really talking about a specific technology. He's talking about risk-based authentication. So they didn't really have time to prepare for the 60-seconds piece. But that's one thing I learned in business school, not that I went that long, but if you can't tell your value proposition in the elevator, then you don't really have a good clear value proposition.

Thank you. And Micheline?

>>MICHELINE CASEY

I'll address authentication. Strengths of KBA and identity proofing, again going back to -- going beyond the acceptance of breeder documents or sensitive personally identifiable information. Secondly, it is device diagnostic. It can work in conjunction with any of the technologies that are up here. There's limited vulnerability to hacking or phishing. The questions that are asked are pooled from an extremely deep pool, wide and deep pool of information going back up to 20 years and for multiple, multiple data sources. So, it becomes extremely hard to guess which questions are going to be asked each time you come back or which series of answers are going to appear. Additionally, you don't have to have multiple smart cards or other authenticating devices that you would have to carry around with you.

>>AVIVAH LITAN

Okay, thanks. So that's a summary of the benefits. I'm going to play devil's advocate and ask each of you about one weakness that I perceive in your different technologies. But first let me just see if you have any questions in the audience or if any come up? Yes, sir.

>>AUDIENCE MEMBER

One question that I would have or one thing that pops to mind with a lot of the technologies you presented is the privacy issue and data protection issue because I look at for instance biometrics or the knowledge base authentication and to a certain extent also risk-based authentication you will be storing additional attributes about your user base in order to be able to actually authenticate them. So that additional information, like for instance the data going back 20 years, or additional biometric information is exposed in some sort of an attack, you will probably be liable, to a certain extent be liable, for that additional information being dispersed. So I would like to get your comment on how to address those things.

>>MICHELINE CASEY

With regards to knowledge-based authentication I think we're talking about two issues, privacy and security. With regards to the privacy aspect of it, we make sure that no information is actually returned to the customer or to the consumer as part of that quiz process. We pass flags back or identity scores back. The other thing is we don't allow the clients to know which questions the consumer actually got wrong, which helps to alleviate insider identity theft. Secondly, there is no kind of great database in the sky with all these questions or with all the answers. So it becomes extremely -- if you're talking about hacking, there's no single, central repository to hack into. Harvesting becomes extremely difficult.

And with regards to the security of our data and our systems, we're audited annually as part of a SAS70 audit. Our data centers require biometric access actually to get into those data centers and since our data breach in 2005, we've had over 40 or 50, I'm sure my senior

government affairs person back there could answer that better, independent audits from government agencies and commercial entities, and we've passed every one with flying colors.

>>AVIVAH LITAN

You're speaking about ChoicePoint. I just want to bring up that there are other data brokers that are not getting audited 50 times a year and there's no regulation on them. Yes, sir?

>> AUDIENCE MEMBER

Antiquated nature of –

>>AVIVAH LITAN

We can't hear you.

>> AUDIENCE MEMBER

Given the antiquated nature of a SAS 70 evaluation, and audits traditionally being only checklists, when was the last time you underwent a penetration test?

>>AVIVAH LITAN

So let's start with Phillip and then Marc.

>>PHILLIP HALLAM-BAKER

There's something called I defense which provides a very comprehensive intelligence service on electronic threats, Internet threats across a broad range. They use a large number of techniques to monitor those threats, including the obvious ones of observing public sources such as what viruses are in the wild, but also going into the chat rooms and other techniques. It's a very comprehensive service. Working out -- actually there's one thing I'd like to put to rest here and that is the silly notion that it takes a thief to catch a thief. It doesn't. The best way to catch them is to get a bunch of thieves together and bug the room. (Laughter.)

>>AVIVAH LITAN

Good point. Marc, do you want to follow-up?

>>MARC GAFFAN

take the effort of going ahead and making a model of their friend's hand just so they can get an extra 5 bucks on whatever minimum wage is today, 7.32 whatever the case may be an hour. It's not worth their time and worth their effort. So it's a reflection also of the context in which the technology is going to operate.

And then I guess the other final point I want to bring up is that in many ways, again, I hesitate to say any technology is perfect, but the question is how can we create as many deterrents as possible? And, look, essentially people who are trying to penetrate a system are going to look for the weakest point. The idea is if you can create more and more road blocks so that that weakest point is hard to get to, whether it's using multiple levels of technology, multiple combinations of technology that might facilitate the ability for a deployer to have a robust system without being too afraid of the vulnerabilities inherent.

might work perfectly fine within their limited environments may not be able to work well with multiple other systems that exist across the nation. That could be a good thing. That might mean that a breach is going to be limited to one particular area, but it also can be a problem in so far as systems never really learn from the mistakes that perhaps other systems have encountered. In and of themselves, the biometrics have the ability to make it more difficult for a person to break into a system and to be able to do much once they have broken into it. The challenge is going to be, as somebody said before, that if somebody is successful in breaking into a system, how do you go about actually changing your biometric.

As a gentleman had mentioned earlier today, there is a concept of say cancelable biometrics, where before you actually create that new template from an image of a biometric that's captured, you do a little distortion on it so that it gets compromised. No problem we change the encryption method and you get a new sort of pseudo biometric. The problem with that is somebody comes out with a fake finger again. They're just going to go ahead and reauthenticate themselves and they're just going to create the new re encryption. You're in the same problem, the same hole you were in before.

>>AVIVAH LITAN

Basically, you're saying it would limit access on the systems where you implemented it.

>>VICTOR LEE

Both logically and physically, yeah.

>>AVIVAH LITAN

How about you, Phillip, do you want to add to that?

>>PHILLIP HALLAM-BAKER

Well I told the wife not to shop at TJ Maxx anymore, after all her credit cards had to be reissued.

Well firstly they were going into a legitimate authentic TJ Maxx. So obviously EV is not an issue there. However, there is an accountability issue. Can I mention my book?

>>AVIVAH LITAN

Sure.

>>PHILLIP HALLAM-BAKER

In my book on Internet crime which should be coming out in the fall, I identify accountability as the key deficit behind almost every Internet crime. Here the accountability issue was why on earth were you storing all that data in the first place?

In the credit card rules, tell you that if you divulge that information, you are fined 50 bucks per card that you've divulged because the bank that issued that card now has to reissue it and there's cost there. So the merchant that disclosed the data is charged for the cost that they've incurred. And so there is accountability in the system, which I would guess is about to hit somebody in that company. You shouldn't have had that data unencrypted on your disks. As soon as you took the data at the tills, it should have been encrypted and the decryption keys should have been held offline if you needed to keep the data at all.

>>AVIVAH LITAN

Good point. Neville?

>>NEVILLE PATTINSON

I think a little bit can be augmented onto what Victor was saying about biometrics, about physical and logical access. Smart cards can provide that linkage between the human and the biometric, the system. I'd like to think of it as a trust triangle that we're looking at here. The triangle being on one point the issuer who has given you the credential and issued you the smart card for you to bear as the user. So the user's on the second point of the triangle, and the person who's receiving it or the server or whatever is the third part of the triangle. So we're trying to create trust in that triangle that the issuer is authentic, that the card is authentic. That the relationship between the card and the user can be proven.

So we know who should be bearing this card, that the card is good and that it can now be accepted and trusted by the receiver. So without this, you're left with biometrics or you're just left with other things. The card provides that little computer to do that authentication. It can verify the user's present by biometric or by PIN. It can then verify to the servers, or the receivers, or the issuer as well to prove that it's authentic. On this basis you get the chain of trust and essentially the trust triangle between these three elements. So by having this, accessible information is protected, by having to physically use these, by physically having to authenticate to them, and for them to have to validate to the equipment. So you create lots of steps and checks and balances of authentication before you can get at information. If you don't protect it with technology such as biometrics and smart cards and PKI, it's not protected sufficiently in my view.

>>AVIVAH LITAN

I just want to stop on Neville because I would agree that if the U.S. banks had smart cards, it wouldn't matter if they stole data. It wouldn't work at the point of sale.

So given that, why is there so much reluctance to upgrade to smart cards in the U.S.?

>>NEVILLE PATTINSON

I wish I knew the answer to that. That seems blatantly obvious to me they should.

Do we have a microphone? We want to hear what you're said because you're sparking a good debate.

>> AUDIENCE MEMBER

The problem is that the costs and the benefits are not precisely aligned here. And in

The other thing that comes up in these discussi

>>MICHELINE CASEY

It does vary depending on volume of transactions but on a typical implementation, it would be somewhere between $1 to $1.50 per consumer. Plus you have no maintenance cost or replacement cost. If you lose a card, obviously you're going to have to replace that. You don't have that same issue with KBA.

>>AVIVAH LITAN

But as a practical matter, and I'm here to be devil's advocate, if you stop someone in a