TRANSCRIPT

PROOF POSITIVE:
NEW DIRECTION FOR ID AUTHENTICATION

DAY 2 OPENING REMARKS & PANEL 6

APRIL 24, 2007

>>JOEL WINSTON

Good morning, everyone. Thanks for coming back this morning. You hearty souls who arrived at 8:30. And I wanted to talk a little bit about what's happened so far and what's going to happen today. We covered a lot of ground yesterday interspersed with the press conference announcing the release of the President's Identity Theft Task Force Strategic Plan. And for those of you who have had a chance to leaf through the Strategic Plan, you will see a lot in there about authentication and the vital role it plays in the fight against identity theft. So this is really good timing.

Today we have a lot more to cover, but before we begin let me try to summarize what happened yesterday. We started with some opening remarks by Chairman Majoras who, among other things, talked about what we can learn from the Social Security number experience. How the SSN's use as an authenticator has led to increased identity theft. She then challenged us to think about how government, industry and consumers can work together to build better identification and authentication systems.

Simon Davies and Gus Husein started things off with their now famous five D theory even though no one could seem to reme

Then moving from the development of

statements and to be mindful of time when answering questions so everyone can express their views.

I'd also like to call your attention to the four break-out sessions we have this afternoon, they're listed at the back of the agendas you all received. Joel went over them during his recap but I want you all to know these are designed to be a round table discussion so that everyone who attends is able to participate. Although we have set out these topics, they are meant to be a place to start and we've tried to structure them so that the group can move the conversation forward in whatever way they see fit.

Lastly we hope to draft a report based on this workshop so we'd be interested in any comments that any of you have. You can submit your comments via the workshop web page which you can find at www.FTC.gov and you can also mail in comments if you prefer to the address listed on that website. And actually one last thing was that there is material out on the information table outside, including a paper that was written by the first two panelists yesterday, Simon Davies and Gus Husein, as well as the presidential task force report that was issued yesterday.

Then just a couple of housekeeping notes. If you leave the building for lunch, just be aware you're going to have to be screened through security to reenter so please leave enough time to do that. Please wear your name tags at all times. If you notice anything suspicious please report it to the guards in the lobby. Please turn off or set to vibrate your cell phones and please don't use them in this room. It does interfere with our video equipment. Also try not to use them out in the hallway because it was loud and I think some people were having trouble hearing yesterday when people were on the phone. If you would like to use your cell phone there is a telephone room right over here on the side, and if you go in and shut the door or go out into the lobby outside the conference center that would be very helpful.

We ran out of the WiFi brochures but if anyone wants to connect to WiFi the code

And third we have Yukiko Ko, who is a Policy Advisor at the law firm of Alston and Bird. She advises companies on electronic commerce, related policies and laws, including data protection, Spam control, Adware control and electronic transactions in Asia and Latin America. She has extensive experience in providing intelligence and analyses on e-commerce policies and laws and in identifying key policy makers and law makers for multi-national companies. She'll be speaking about some of the new technologies and how security and authentication issues are being addressed in Japan. So we have got I think we have the world pretty well covered. Stacy, are you with us?

>>STACY CANNADY

Yes, I am. Can you hear me?

>>JOEL WINSTON

We can hear you just fine. We have I guess your power point –

>>STACY CANNADY

Yes.

>>JOEL WINSTON

-- set up. If you would just let me know when you would like the next slide.

>>STACY CANNADY

So I expect you have got the title page up right now?

>>JOEL WINSTON

Correct.

>>STACY CANNADY

Please go to the next page titled most computer products are very insecure. All right. So the topic today is authentication, and I will be talking from that point of view, but let's begin very early in the process fobutbuiw -datab2 Tw-1.15 Tdin very earl14c -0.0(butbuiw -oper 0 T

Let’s talk about this a little bit more. Software companies, hardware companies, all of these companies have limited resources. It’s necessary to constrain available resources in order to ensure profitability of the company. Therefore, it is typically unusual to find someone with security expertise in a company that is not directly related

So now there is a retrofit action going on as the people who develop the standards are in the process of trying to invent security features to build around the VoIP standards. Are they going to be successful in the first round? History says no. If we look at the evolution of wireless data communication, what we see is the same pattern. Wireless was invented because they wanted to communicate without wires, were they successful? Oh yeah. Did they put security in it? No. So they went back and they tried to retrofit security into the early standards and did they succeed? No. They failed miserably. It took three or four rounds of wireless standards before security was present and effective in the standards. Is that going to happen

>>JOEL WINSTON

I'd say about 90%.

>>STACY CANNADY

So I drive down your home street and I check the mailboxes and I see one of these. So I take it out and I take it home and I open it up and I see here is a credit card in your name with call from my home number. I know what your name and address is because I found it on the letter on the envelope that this credit card came in. I look in the telephone book and I get your phone number. Now I use free software that I downloaded from the Internet, this is VoIP software that allows me to mask my phone number and make that phone number any number I want it to be. I know what your name is, I know what your address is, I know what your phone number is.

I call the credit card number with your home phone number, listed for caller ID on my VoIP software. The person at the other end picks up the phone and says may I help you? I say I'm you and I'd like to activate my card please. The person at the other end of the credit card company checks caller ID, sees that the phone number is correct, activates the credit card, I sign the back, and you're screwed.

Next, we have hacking VoIP networks to access company data networks. As I said, companies large and small know how to tie up data security, data networks pretty securely. They have been doing this now for over ten years. There are fine products out there, so there is an opportunity for corporations to put genuine security in place on their data networks and they often do. This is a good thing.

What's happened is that the corporations have decided we want VoIP. And they slap the VoIP in because the return on investment is so high. And the IT people, they don't know anything about this VoIP stuff. They do know something now. They know there's no security built into it. And they are running the VoIP on top of their data networks.

As an attacker, I know of a list, actually, a long list of standard attacks that can be used to bridge from a compromised VoIP network into what had been a secure data network. Why would I want to do this? That's where the money is. So those are three examples of how VoIP can be exploited for personal gain at the loss of someone else.

May I have the next slide please? How about another example – Bluetooth. All right. The original Bluetooth specification did make an effort at security. This was security designed by engineers who had no idea what security meant but they figured hey, we're engineers, how hard can it be? So they published their specification, they were proud of the job they had done. The security people saw it. After they got through laughing at the toy security that was built into the specification, they commenced to howl about how miserable it was and how bad it was going to be for all of us.

So, once again, we go through the evolution of toy security to somewhat half-baked security to security which is pretty good. It's good enough for Bluetooth, I think. And that sounds good, right? We have got that solved. So there's real security in place. But then why in the attack community do we have these slang phrases, toothing, Bluetoothing, blue snarfing? This is a hobby activity at this time in the attack community. There are people that engage in these actions to compromise Bluetooth devices. First of all, who cares? Well, look at the picture. Do you have one of those devices? Probably so. If you're a European you bet your life you have one of those devices and you have a whole bunch of other devices that are Bluetooth enabled.

Let's go to the next slide. What is the risk with Bluetooth? Once again, the primary risk associated with Bluetooth is you. You didn't set it up right if you tried to set it up at all. That is almost always the point of attack that attackers are relying on. You did not set it up or you did not set it up correctly. So what does this mean? I'm in an airport waiting area as I was this morning for some time, in fact. I'm in the waiting area, I have nothing to do, so I open up my lap top and plug in a little device. You may know that Bluetooth is supposed to have a range of about ten feet. But with my device and a little antenna on it I have got a range of 200 feet. So that basically makes it possible to pick up everybody in that waiting area. I get a constellation of Bluetooth devices, I start scanning each device to see which one is misconfigured, probably around two-thirds of them are and I engage in what's called a Bluetooth pairing operation.

Once I have paired with it, your Bluetooth device thinks I'm God and it will do anything I tell it to do. If your Bluetooth device is your telephone, I can ask for all the phone numbers that you have in your phone. If your Bluetooth device is your PC, I can ask for any file on your PC. Now, I don't know what phone numbers you have got in your phone and I don't know what data you have on your lap top. Do you want me to find out? And finally, my favorite for Bluetooth attack devices is something called a blue sniper rifle. It's an antenna, a Bluetooth antenna, mounted on a rifle stock which has a range of over a mile.

All right. That's about it. I think -- yes, that's the last slide I have on my presentation. I think I'm right about on time. Are we handling questions now or at the end of the session?

>>JOEL WINSTON

I think we're going to do them at the end.

>>STACY CANNADY

All right. So I'm done. Thanks very much for listening. (Applause.)

>>JOEL WINSTON

Thanks.  Ok, Hanne?

authentication methods accepted by Norwegian banks for securing the debit transaction that all Norwegians are very accustomed to. So in 2001 Telenor launched an electronic PKI based ID for mobiles to be used for Telenor customers with a bank account in Norway's largest bank. It was a very secure but extremely user unfriendly solution. And nobody wanted to use it. There's just no Norwegian that wants to go to the post office, show his passport and other form of identification and in addition go through a complicated procedure on his mobile to get an electronic ID. It just doesn't work.

So what we did then, we thought we'll have to work on the usability part. So we went back to the drawing board and made an identification and authentication system based on mobile subscription data in combination with Social Security numbers. And we used this for Visa and MasterCard payments because no way Norwegian banks would accept this kind of authentication for their debit card scheme. So we got a very easy solution to register for, a two-minute process. But it was only for our own customers. So

Japanese government is prone to consider more usability first rather than protection. This is not to say that the Japanese government does not care about privacy. They really do. I will explain about the government's initiatives on personal data protection and information security later on.

that coupon, it's actually like a barcode, and give it to the restaurant. So you get not just a pleasant meal but reasonable dining deals, so I love it.

Cell phones are used as electronic wallets. For instance, some cell phones allow subscribers to use a national electronic card cash network called EDY. E-D-Y, EDY. How it works is that RFID is embedded in the cell phone that transforms the device into a credit or debit card. I think we use more for debit card use. Credit card we don't have a well grounded credit card culture so we prefer to pay in advance, prepay. But that's EDY card. This electronic wallet, the customer swipes the phone against a vending machine -- we're also a vending machine culture. If you have prepaid EDY cash network downloaded in your cell phone, you want just a coke, you swipe your cell phone and you get a coke. Also ATM as well. If you swipe on train tickets dispenser, you can get the ticket if you don't want to buy a pass.

A recent interesting trend in Japan is what we call toilet traders. They're a growing number of mobile phone users that take a restroom break and invest and trade stocks using mobile phones in a very private setting. (Laughter.) I have to say that the high volume of mobile phone use contributes to the recent surge in the number of individual investors in Japan. Now, so much for showing off our mobile phone culture.

Let's move on to some of the risks and threats that we face. All these mobile phone-based services involve some kind of financial transaction. This is why it tends to alert criminals, naturally. That most of the ID theft cases stemming from mobile phones in Japan are caused by lost or stolen cell phones in Japan, so it's more conventional. You lose your device and maybe you get a high bill. So what it tends to be is that instead of storing data in your cell phone you tend to store all the data on the network server. And if you lose your cell phone then you remotely control and delete everything or just shut down. But the data is not lost because it's on the server.

Other type of threats risks include one-click fraud, which is kind of phishing. Criminals send emails to your cell phone and then

What are the policy responses?  There's a laundry list of legislations available to protect consumers from online fraud including that of by mobile phones.  Personal information protection act to specify commerc

What we’re doing when we are introducing an electronic ID for everyone is that –

>>JOEL WINSTON

Closer to the microphone please.

>>HANNE SJURSEN

consumers are going to be so afraid and so turned off by this process they're just going to pull the covers over their heads and stop using these technologies?

>>STACY CANNADY

This is Stacy – that's already happening in the space. There are surveys that indicate that people are less and less willing, certainly in the United States, to engage in online shopping. For a decade online shopping went up year by year. It's not any more. At least the inflection point has been reached and the rate at which it's going up is declining. The percentage of people who are engaged in online banking, it's about 42% right now, and the growth rate for online banking in the United States is 1% per year visioned to cap at 48 or 49% and the reason is that most of the people beyond that just

That raises one other question I have which is, what is the impact of cultural

Why don’t we open it up to the audience now. We have got microphones so if you could raise your hand and introduce yourself, why don’t we start here.

>>AUDIENCE MEMBER

I’m John (indiscernible) from Hampshire Research. Can we go upstream a little bit in the process whereby an account or a devi

and what are the fear factors in -- particularly on the banking side in terms of who owns the customer for the long term?

>>HANNE SJURSEN

Trust, building trust, and that's time consuming. We talked for two, three years. We also used the CEO of our company together with the CEO of the new -- the largest Norwegian banks. And the continued sort of -- stating that Telenor is not becoming a bank and also the banks were telling us that they're not becoming service providers in the Norwegian market.

The ownership of customers, that's a discussion that if you sort of start to discuss that you're in great trouble. It's not a discussion that you can sort of conclude on. So what we said that we would together deliver services -- services based on electronic ID to the Norwegian market, and that's an interesting discussion, not who owns the customers. But lots of people wanted to make that discussion. I had hard time just getting them to go away. Yeah. But I think senior involvement and our CEO stating I want to do this, I want to do this together, we're not going to become a bank. That's important.

up and announce 3 million customers were compromised last night because they're going to be heading to the door and the revenues are going to drop and that's what I have been concentrating on for my contract. Are you -- I'm at the point where I'm saying that really the security element is totally outside of the market stuff. It just is not a market incentive. It's in the category, yeah it's leprosy but I may never get leprosy and I got a lot of other things to work on with regard to budget and objectives of revenue and customers. Are you ready to move to that area and say that perhaps government has to put in the curbstones? And is it possible in the security area or -- excuse me, the technological area for the future that those curve stones could be continually moved forward by government? Because I don't see any other incentive within the private side or the revenue and marketing side in order to come up with and make the security part. But it's devastating if I get that leprosy and I have to announce that 20 million customers were compromised last night. And I'll take anything from Hanne and Yukiko on the same matter.

>>STACY CANNADY

I think I'll stick to my guns for a least a while longer on this issue. We're in a capitalist society and corporations make decisions based on money. As a consumer of security technology you're in a situation where if your security technology fails you, there are dire consequences. You have established that. You can express that to your vendors in service level agreements and in selection of partners and in other ways that can influence the vendor behavior. If you're relying on a database for your application, for example, it is possible for you to place requirements on which vendor you choose and on the chosen vendor for security performance in that regard. Your insistence and the insistence of others in your position will modify the behavior of corporations. We have seen that and it can take time, maybe you don't have time. But I still think that voting with your dollars is a powerful incentive.

If you're going to influence with the lever of policy, then you're going to have to be very artful in the construction of your policy so that the policy can endure in spite of the evolution of technology. So for example, if the policy says, this technology is what you must use to provide security, that's almost guaranteed to fail after 18 months, the next generation of computing technology. If on the other hand, the policy reads, you must use a NIST, a National Institute of Science and Technology, approved encryption algorithm for encrypting your data, that's much more interesting. So policy can work but you better be really careful in how you construct it.

>>JOEL WINSTON

Other questions?

>>AUDIENCE MEMBER

I'm Richard Dick with You Take Control. First of all I just want to comment about this last gentleman's statement. All I can say is if your business is on the front of

the Washington Post, you're toast. That's it. It's over. And if you don't understand that, if you don't understand what's at risk, then I'm just feeling sorry for any businessman who doesn't really understand that. We are so vulnerable today. I come out of the healthcare space. Healthcare is running naked. I mean, just flat naked. The emperor has no clothes and doesn't know it.

>>YUKIKO KO

In terms of the last question, I briefly touched upon biometric authentication. Multi-factor authentication may be the most robust way is to -- just a fingerprint is also risk to forging so that's why we in Japan try to do R&D on the finger patterns of the vein inside and then you combine with one time passwords and J passwords. The language one. So we have in theory it's very robust. But I haven't seen all those features combined in one because of the user friendly issue that Hanne explained.

>>JOEL WINSTON

We have time for maybe one or two more. Way in the back.

>>AUDIENCE MEMBER

(indiscernible). We seem to be looking very much at the high end of security and authentication here rather than authentication in general and I think that's important to note in that if you look at government mandates and the history, if you get it wrong you

insurance company you need to use, we specify a minimum level of protection that you need to have, but not the maximum.

I'm interested in exploring the role of government. I think I was hearing those gentlemen say that you know, government needs to establish standards through its purchasing policies. Then he was talking about if you're going to establish a policy specifying NIST standards which would evolve over time. So I guess my question is, is it the role of government if there's not enough incentive? I understand that's a point of debate in the private sector to employ sufficient security, is it the role of government to say you must have, if you're going to roll out the service over the Internet, you need to have protection for others just like you need to make sure that somebody can drive or that somebody has insurance in case you hit them? Is there a role for government without specifying a particular standard because I think -- or a particular technology -- because I think we all know that that's not a go proposition. But is there a role for government here in setting some kind of level? And maybe there is, maybe there's not. I mean we're very market sector driven here. But what I'm hearing is this maybe a place where we're seeing some market failure.

>>JOEL WINSTON

I think we're going to be talking about this at the next panel but it's a good segue. We're out of time. We're going to go to a break now but please thank our panelists for a terrific job. (Applause.) Stacy, you can hang up now.

>>STACY CANNADY

You bet. Thank you very much.