Real-World Identity Authentication: Simplicity on the Internet

Recorded October 9, 2013
Discussion Transcript*

To download or listen to the audio podcast version of this discussion, visit:

Real-World Identity Authentication

***Jim Cavanaugh,* Webtorials**
Security Analyst

***Andre Boysen,* SecureKey**
Executive Vice President of Marketing

***Thom Hounsell,* SecureKey**
Director of Product Marketing

Patte Johnson: Thank you for joining us for this Webtorials Thought Leadership Discussion. I am Patte Johnson. It is my pleasure to introduce Jim Cavanagh, our Webtorials Security Analyst. Jim will be speaking today with Andre Boysen, Executive Vice President of Marketing at SecureKey, as well as Thom Hounsell from the Product Team at SecureKey. The subject of our discussion today is "Real-World Identity Authentication: Simplicity on the Internet." Jim, I will let you take it from here.

Jim Cavanagh: Welcome. Andre, in plain language, what is your underlying thesis?

Andre Boysen: Hi, Jim. Thanks for the invite today. The Internet is a great technology and it's allowed us to accomplish a lot of things; but the challenge has been that we're getting more and more user IDs and passwords. We need to manage

our online life, and it's gotten to the point that most users can't cope with the number of user IDs and passwords that they need to manage.

And so, we need to get to a simpler scheme. And that's really what our model's all about, allowing users to accomplish their tasks on the Internet with having fewer user IDs and passwords to do it.

Jim Cavanagh: So, what forms of authentication should one look for in a product or service?

Andre Boysen: Today, the Internet is entirely based on user IDs and passwords. Basically, it's all secrets. And they have their place. But what we've realized now is that secrets are easy to compromise, and it's hard to detect when they've been compromised. So, we need to move to something that's stronger. As an example, my Facebook account has access to nothing that's important to me. It has a crazy set of password rules, like many services do, and it has the eight-character password.

By contrast, my bank card, which has access to all my money, has a four-digit PIN. On the surface, that sounds kind of crazy. But the reason the bank can put a four-digit PIN on your account is because you have a card that's attached to the account, and what we know about you, the user, is, if you lose the card, you're going to call the bank and say, I lost it. Which means the bank can turn it off, and that's no longer a vector of attack.

So, that's the insight. If we can start anchoring the Internet on stuff, instead of on passwords, we can make the user's life easier, and at the same time make security stronger. So, certainly, things and people are definitely part of the authentication mix in the future; as will biometrics, I think, play a role at some level.

Jim Cavanagh: So, everyone talks about the cloud these days, but a lot of services are still implemented via the appliances or virtualized. What are your thoughts for the best, simplest implementation of authentication?

Andre Boysen: Everyone has six cards in their wallet that they can use to accomplish real-world tasks. I can use my cards in my wallet to purchase things; I can get onto an airplane; I can get a new bank account; I can get a new cell phone; I can buy cigarettes - all these things - with these cards in my wallet. Six cards; all my destinations.

Yet, on the Internet, every single destination I go to, I get a dedicated user ID and password. And we've kind of reached the point that that's not scalable any more. So, what we need to get to is the concept of credential federation, so the user can use a smaller set of credentials to reach all of their online destinations. That's really what we're talking about here.

Jim Cavanagh: So, am I correct in assuming that SecureKey has achieved these goals?

Andre Boysen: Yes. We've actually got several instances operating now, where we're running credential federations for consumers to access online services. The biggest project that has been in the market longest is something we've got running in Canada called SecureKey Concierge, where Canadians can now use their bank accounts to reach government destinations for things like getting access to tax accounts, or reaching information about their benefits. They can use something they use every day, which is their bank account, to access these services now.

Jim Cavanagh: Let's dig into that a little deeper. How does SecureKey Concierge work?

Andre Boysen: SecureKey Concierge is a service that is used for government. The challenge government has is, they want to serve online, but they have this challenge that I don't go there very often; and because my transaction velocity is low, they have a hard time getting enough business assurance to know it's really me, to serve me in the online channel. And so, they have a valuable service to offer, but because I don't go there often, they have a hard time serving me there. And that's what they're really searching for, is a mechanism to do that.

And so, when you think about it, you use your bank account, as an example, every single day. And so, you're not likely to forget the user ID and password. But if you did, there's a bank branch that you can go to, or you can call them on the phone and easily get it reset. By contrast, government has a hard time doing that same thing, because they don't have that transaction velocity with their customers.

So, one of the opportunities here, then, is to allow government to piggyback, if I can use that word, on a credential or a thing that a user already has, as a mechanism to get access to government.

Jim Cavanagh: Well, I think piggyback is actually a good choice of words, because that's exactly what's happening. So, not only do you actually have fewer accounts and passwords to remember; you also have fewer accounts and passwords that are used rarely, often maybe one time, floating around the Internet. And if a website has a trust relationship with an entity you also trust, such as your bank, it is one more step in establishing with a website what your identity is, and the fact that you are trustworthy and the website is highly unlikely to be part of identity theft or something else.

Andre Boysen: That's exactly right. What's important here is that the user has a trusted and ongoing relationship with the bank, and that's something that the government would like to be able to take advantage of. In doing this, we've got to have all the right provisions in place so that the government can get the business assurance it needs, but we can still maintain user privacy. So, we're looking out for services where we can increase trust online, but still keep proportional balance on privacy, so users can protect their information and be in control of what's going on.

Jim Cavanagh: That's great. Does SecureKey actually negotiate a separate and secure password with each partner entity, or is…?

Andre Boysen: It actually functions like a two-sided marketplace. So, today, in payments world, the payment network will typically have two sides. They have the issuing side, where people issue cards and put cards in wallets —credit cards, as an example—and then they have the acquiring side that sets up relationships with merchants. And so, typically, merchants are signing an agreement with the payment network, as is the issuing bank who gave you the credit card. Each side only has signed one agreement, but yet you can get a many-to-many network created by having each of these relationships set up.

Jim Cavanagh: Hmm. Interesting. Well, let's go through the process again in a little more detail. Our Webtorials audience, I'm sure, is intrigued at this point and wants to know a little bit more about it. And certainly, we haven't heard from Thom yet. So, Thom, if you want to jump in and add some comments to Andre's explanation in a little bit more detail, feel free to do so.

Thom Hounsell: I'll do that.

Jim Cavanagh: Great.

Andre Boysen: So, let's examine how a user's going to get access to a service online, then, using a service like this. Say I want to get access to agency.gov, because I want to get access to my account. So, I'm going to go to www.agency.gov to access the service. At this point, agency.gov doesn't know who I am. So, they're going to give me the option of using a service called SecureKey Concierge, where there's an established list of trusted sign-in partners that I can choose from. So, agency.gov does a handoff to SecureKey Concierge to do the authentication of the user.

So, now I'm talking to SecureKey Concierge. I choose somebody I have a relationship with. I see Bank.com on the list, which is who I bank with. So, I select Bank.com from the SecureKey Concierge menu. The next step is, the SecureKey Concierge redirects me over to Bank.com. So, now I'm at Bank.com, and I log in to Bank.com the same way I would every single day if I wanted to get access to my online banking services.

And so, I've logged in, and this is where it gets interesting. What Bank.com does is – now, is produce an anonymous security token. In technical terms, it's a SAML assertion, basically saying that the person enrolled for this bank account is here now. SAML stands for Security Assertion Markup Language, and that's the protocol that we're using to do the handoff. So, Bank.com produces an anonymous security token based on SAML and gives it back now to SecureKey Concierge.

Thom Hounsell: At this point, SecureKey Concierge gets involved and says, well, thanks very much for that assertion. Maybe it's given something like number 1234. But

SecureKey Concierge isn't going to want to pass on 1234 to the agency. We want to anonymize it yet again. So, we take that 1234 number and we change it into ABCD. And that's when we pass it off to agency.com.

Andre Boysen: The reason we've done the rewrap is that we're trying to preserve the user privacy. This is an anonymous authentication service. SecureKey Concierge doesn't know the identity of the user, but did know the identity of the bank. So, what we're doing is now shielding the identity of the bank from agency.gov so that the user privacy is preserved.

And so, now what we have at agency.gov is an anonymous security token based on SAML. And what the agency does now is look at this anonymous token. And there'll be one of two conditions. Either they see this anonymous security token and they know who I am, so they'll just say, hi, Andre, welcome back today; or, what they see is that this is actually an enrollment, because they've not seen the token before, and they proceed to ask me a set of questions to establish my identity and confirm who I am.

And once they've achieved comfort that I am Andre Boysen, they're going to take that anonymous security token and bind it to my account so that I can use that every time I show up in future. And so, that's how the process works.

Thom Hounsell: We've already taken the token from Bank.com, which maybe said 1234, and changed it into ABCD. And we store that relationship. But we don't give ABCD to every agency that comes along. We further diversify it. So, every agency that gets this token is getting a different identifier. So, even if you've got access to databases from multiple agencies, you wouldn't be able to put the story together and tie it back to a user.

And that's the way the system is basically enabling privacy by design. There simply is no point in the system where there's a treasure trove of data that you can get at. So, it's not just done through encryption; it's done by design.

Andre Boysen: Thom's hitting an important point here. One of the important principles of privacy is to minimize surveillance. And so, by giving each agency a different handle for the same user, they're not able to correlate my behavior across agencies. The additional benefit is that the underlying bank account is protected, because the agency who has the handle for the user is not the same information that the bank has. And so, getting access to agency.gov, as an example, doesn't give any clues as to what the bank account information that originally provided access to the account is.

Jim Cavanagh: The example was for government agency, which is more, I guess, of a consumer-based type of example. Is there a plan for managing the authentication within a corporate structure as well?

Andre Boysen: That is something we've definitely talked about, and we see it on our roadmap. It's not something we're doing today. But the same techniques

and principles, and our technology, could certainly do that. As we go to market, we're focused on consumers today, but we do see helping inside the enterprise is something that we'll likely get to in future.

Jim Cavanagh: Wow. That's great. Well, that really delivers on your original promise of being simple as possible. What needs to be done to see widespread acceptance and usage of this technology?

Andre Boysen: The most important point is making sure users have comfort that the service works as advertised. The first part, is communicating about what's going on here. When you first hear about the idea of using your bank account to get access to government, sometimes people's hackles get up, worrying that they're going to lose control, and there'll be collusion between government and banks. Once consumers get comfortable that that in fact is not the case, and this is just a convenience mechanism to allow them easier access to government, people will kind of get it.

I can take my Bank.com bank card to any ATM on the planet and pull money out. So, if I went to another country, like the UK – if I go to Barclays and I pull money out of Barclays via a Bank.com card, users kind of get that Barclays doesn't get to look at my Bank.com account. We want to use those same notions that people have about how networks work, to apply to identity and authentication. And that's really what we need to do here, so people understand what's going on.

And then the next part is to allow both sides of the marketplace to flourish. So, we add more credentials providers, so consumers have more choice how they identify for service, and then to add more destinations, so users can accomplish more of their online passwords or credentials that they have already.

Jim Cavanagh: You're absolutely right. That is very important. And what should the Webtorials members do next to learn more about this and to become involved in this process?

Andre Boysen: We have lots of good information available on our website at www.securekey.com, where we describe what we call our briidge.net Exchange platform, where a lot of these capabilities are present. So, that's the first thing.

The next piece is to get active in the identity and the access management community, where we start pushing this idea that dedicated authentication schemes for every service is not a good idea, and federated credential is really the way this thing needs to go. And that's where we should be pushing all of our online services, is that they should be using a strong credential provider rather than trying to develop their own authentication scheme.

Jim Cavanagh: Very good. Well, Andre and Thom, thanks for joining us today and sharing your insights on this very important and current topic.

Andre Boysen: Thanks so much for the invite today.

Thom Hounsell: Thank you.

Patte Johnson: Well, thank you, Jim, Andre and Thom for another informative, thought-provoking discussion. We remind our listeners and readers to share your questions and comments at the Webtorials website. And again, thank you.

** The discussion has been edited slightly for clarity and length.*