SECURITY NOW!

Transcript of Episode #98

# Internet Identity Metasystems

**Description:** Steve and Leo discuss the user experience and operation of Microsoft's "CardSpace" technology which hopes to completely change the way users identify themselves on the Internet by doing away with traditional usernames and passwords.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-098.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-098-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

**Leo Laporte:** Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 98 for June 28, 2007: Internet Identity Metasystems.

Time for a little security. It's always nice to have a little security when you go out on the 'Net.

**Steve Gibson:** You can never have too much security, Leo.

**Leo:** Our security blanket, Mr. Steve Gibson. Some call you a wet blanket because you sometimes take the fun out of our surfing. But it's always good to know what the dangers are. Mr. Security Blanket, Steve Gibson. Hey, you're actually not here right now.

**Steve:** Let's hope that moniker doesn't stick.

**Leo:** You're at Harvard right now.

**Steve:** Yeah, they asked me to come out and keynote the kickoff of a conference/symposium there that's being hosted at Harvard Law on spyware. And so I said, yeah, that sounds like fun. I'm going to be on a panel and start off the conference...

**Leo:** What day is that?

**Steve:** ...on Wednesday. So it's...

**Leo:** It's already happened.

**Steve:** Yeah, it's already happened. But of course Wednesday is the day you and I are normally recording our podcast for airing the following Thursday. So we're recording this one early.

**Leo:** But that's fine. Well, you will have already given your speech and have been a great success. But I'll tell you now, have a great time and - you know, I think Harvard's doing a lot of really - they have the Berkman Center, which is an amazing center for the Internet. They're doing a lot of really good stuff in that area. Good for them.

**Steve:** Well, the Internet turns out not to be a fad after all, Leo.

**Leo:** Amazing. Who'd a thunk it?

**Steve:** It's here to stay.

**Leo:** Now, today, and I don't want to scare anybody away, we're going to talk about Internet Identity Metasystems.

**Steve:** Yes, that's a mouthful. But actually it plays perfectly into the idea that the Internet is not a fad, and it also follows on what we've been talking about recently about the issues of authentication because this goes sort of the next step in that chain is sort of more robust identity, and even identity with content, which we alluded to a little bit before.

**Leo:** Do we have any letters or email you'd like to take care of, addenda, before we get to the meat of the matter?

**Steve:** We do. I've got a couple interesting notes in the mailbag. Matt Sharp in, okay, now, I assume that his hands did not slip on the keyboard when he was typing where in the U.K. he is: Aberystwyth.

**Leo:** Wait a minute, I have to write that down.

**Steve:** Aberystwyth. Give it a shot, Leo.

**Leo:** Why, of course, that's Abery-saint-eeth.

**Steve:** I'll buy that.

**Leo:** And it is a very well known, it’s probably - I don’t know where it is. It’s probably Welsh.

**Steve:** You could probably put it in Google and be looking down at the top of his head.

**Leo:** Yeah, right, because it’s probably just him. You know, I’m going to put that in Google and see. That’s very interesting. Aberyst...

**Steve:** Meanwhile...

**Leo:** What does he say?

**Steve:** He says, "Hi there, Steve and Leo. I love Security Now!, and I’m a regular listener. I believe in one of your recent shows you mentioned how to ensure that the web page you are visiting is secure by checking for https, the padlock, and that the signing authority is trustworthy. However, I have a question about that last detail. How can the average user know whether the certificate is signed by a proper authority? I have seen..."

**Leo:** Aha.

**Steve:** Aha. He says, "I have seen IE7 showing its green bar on eBay and PayPal, which is great because you know you really are safe. But what about all other sites that are signed by Authority X? Is there...." Well, I don’t think X, well, anyway, you know, of course he didn’t mean "X" literally. "Is there any good way to know who is trustworthy and who isn’t?"

**Leo:** Good question.

**Steve:** Well, it’s a great question, but this really brings home a peeve that I have. That green bar is really cool. And it costs any site that wants to provide it $1,500 a year.

**Leo:** You won’t be seeing it on my site.

**Steve:** It really - that really frosts me, Leo. VeriSign has what they call their 128-bit SSL with EV. You know, it’s like Techroline additive.

**Leo:** With EV. Now with EV.

**Steve:** Exactly right. It stands for Extended Validation. And all it is, is nothing. All it is, is a certificate that they rake you over the coals...

**Leo:** Because if you were a hacker, you wouldn’t have 1,500 bucks to pay for this.

**Steve:** Well, and Leo, I would buy it if I had to buy it once. But that's a one-year certificate.

**Leo:** Every year. Absurd.

**Steve:** If you go for two years, oh, they give you a discount, it's only $2,695, that is $2,695 for two years.

**Leo:** That explains why you're not seeing a lot of green bars on the web.

**Steve:** It just really bugs me. It's like, hey, I want that, you know, I've got a 128-bit certificate. But it won't light up green unless I pay them a lot of green.

**Leo:** That's a scamola.

**Steve:** It really - it is such a scam. That just really bugs.

**Leo:** And by the way, I completely mispronounced it, and I'm not going to try to mispronounce it.

**Steve:** Oh, believe me, I...

**Leo:** It is Welsh, though. It's mid Wales's main seaside resort, Aberystwyth or something. It's in the heart of Cardigan Bay, and it is the town of 50 pubs. So there you go.

**Steve:** Aberystwyth. I think that's exactly how you would say that.

**Leo:** It looks like Aberystwyth. But it's in Wales, and nobody can pronounce - only the Welsh can pronounce Welsh names, I'm afraid, so I'm not going to attempt it.

**Steve:** Well, you did a good job.

**Leo:** They have a website.

**Steve:** To actually answer Matt's question, having gotten my rant off my chest - god, that just bugs me - essentially the way certificate chains work is that the root certificate, which is the signing authority, has to be installed in your browser. It's funny that he mentions this also because about a week ago, I don't remember what led me to it, but I looked through under XP with IE7 the list of signing authorities. Oh my god, Leo, the thing just scrolls on forever. It's phenomenal.

**Leo:** Who certifies the certifiers?

**Steve:** Well, exactly. I mean, certainly Microsoft is ultimately in control of the certificates for their browser. Presumably the guys behind Firefox are gathering those together, and Opera and Safari and everything. I mean, the browser vendor can set up the certificates that they want their browser to accept. So to answer his question, you just can't normally get a random bogus certificate into a browser without deliberately installing yourself. And I have never heard of a situation where malware goes about doing that. One hopes that the operating system and browser take some pains not to allow that to be an automated process, or you could imagine that you could start getting bogus root certificates.

On the other hand, there's a mechanism called a CRL, Certificate Revocation List, which, if such a bogus certificate appeared, there are mechanisms for causing them to be revoked as soon as they are found. So basically that part of our connection, the whole SSL stuff has been engineered very well by our vendors. So it's really not a big problem. But boy, it bugs me that I can't have a green bar without spending ridiculous amounts of money.

**Leo:** Well, and I'm thinking only the biggest merchants are going to have green bars. And I have to say it's going to really eliminate the usefulness of this. You know, I talked to somebody at Yahoo! the other night at a party, and they are implementing a SiteKey system, much like the Bank of America's SiteKey system. And I said, well, you really ought to listen to our podcast. There seem to be some issues with the usability and - not merely usability, because I hate SiteKeys, but, frankly, the security offered by a SiteKey. That's the image that your bank displays, and you're supposed to recognize it and so forth. Fortunately Yahoo! is not going to make it a must. But I'm a little disheartened to see them adopting - you know, the bank has to do it, I guess, just by law. But Yahoo! doesn't. And I'm a little disheartened to see them adopting stuff like that.

**Steve:** Well, what you're bringing up, this issue of a SiteKey, plays right into today's topic, as it happens.

**Leo:** Oh, good.

**Steve:** But I wanted to mention, we had another reader - another reader - another listener, Richard Collette in Beaumont, California. He said, "Hi, Steve. I was just listening to you and Leo on the Tech Guy podcast." So I'm sure he means - I guess you do a podcast of your Tech Guy show.

**Leo:** It's the radio show. And since you appear every week on the radio show, he's hearing your segment on the radio show, on the podcast.

**Steve:** Right. And so he says, "I heard you guys talk about passwords. I thought I would share with you how I create passwords." And the reason I'm bringing this up, Leo, is here's one I've never heard before. And he says, "I take the model number and serial number of my monitor, put them together, and I have a very unique, complex, and unforgettable password. If I forget it, I just turn my monitor around. This can be done with any device that is within arm's reach of your computer. If you want a unique password for each site, you can put the domain name part in the password, as well." He says, parens, "(I put it between the model and the serial number.) As long as you don't forget the device you have used as the root of our password, you will never lose the password. Just don't tell anyone what the device is."

**Leo:** Yeah, because they can just look on the back.

**Steve:** And actually it is pretty - it’s pretty neat because, you know, not that passwords have to be absolutely unique, but serial numbers are going to be unique within a given family and model number of a monitor. So he’s come up with a way of creating a complex, unguessable, probably alphanumeric blob which, if he should forget it, he can always recover it again.

**Leo:** Right.

**Steve:** So I thought that was kind of neat.

**Leo:** Very clever. Very clever.

**Steve:** And then I have, speaking of clever, I have one very short little blurb that I just got a kick out of this guy. He’s a listener, Harvey Russ. And he says, he starts off, says, "Okay, this was an emergency. My TiVo puked."

**Leo:** Oh, no, that’s terrible.

**Steve:** And I loved it that he’s like, okay, you know, his TiVo dying is more of an emergency than his PC dying. He says, "My TiVo puked. The WeakKnees tech support page said that the problem with my TiVo looks like a disk failure. Well, I have the fix, SpinRite 6. Yes, I resurrected the pair of disks in my Series 2 TiVo using the handy-dandy trusty SpinRite. Steve, thank you for your knowledge in hard drives and technology in general. I’ve been using SpinRite since v1.0. Your faithful follower in technology, Harvey Russ."

**Leo:** Lovely. Lovely.

**Steve:** So I thought that was neat. And I just got a kick out of, help, my TiVo puked. Forget about my computer, I need my shows recorded.

**Leo:** Now, that’s a Linux disk. So it works fine on Linux.

**Steve:** It does. In fact, what happens is, on Series 1 TiVos - and I’m not sure about Series 2, but I think it may be the same. Those are byte-swapped systems, meaning whereas on Intel-based systems we have what’s called "little Indian format," where the least significant bytes come first, certainly on the Power PC that was used in the original Series 1 TiVo, and I think also in Series 2, those are "big Indian systems" where the most significant byte comes first. This is important because, when SpinRite looks at the partition table on the drive, it will not find it on TiVos because the special signature word at the end of the partition table, which is a 55AA, will be swapped, and it’ll be AA55. So SpinRite says, well, your disk is blank. Shall I go anyway? And so obviously Harvey said, "Please." And SpinRite took off and just did the whole drive from front to back and resurrected his TiVo.

**Leo:** Very interesting.

**Steve:** So, yup, works on TiVos.

**Leo:** All right. Now, you’ve got me with this title, and I have no idea what it means. So maybe you’d better - maybe you’d best explain.

**Steve:** I’m going to ‘splain.

**Leo:** ‘Splain to me.

**Steve:** It turns out that Microsoft has a guy whose title is

Identity and Access Architect.

**Leo:** Well, there you go.

**Steve:** His name is Kim Cameron. And he wrote such a nice setup for this that I’m just going to read it. This is in one of his blog postings. And as I was doing some research for this, I mean, I could hear my own voice saying these things. These will not be unfamiliar concepts for anyone who’s been listening to our podcast for a while. But he just does such a beautiful job with it that I want to lead in with that. He says, "The Internet was built without a way to know who or what you are connected to. Since this essential capability is missing, everyone offering an Internet service has had to come up with a workaround. It is fair to say that today’s Internet, absent a native identity layer, is based on a patchwork of identity one-offs," as he puts it. You know, everyone just doing their own thing, basically.

**Leo:** So this is exactly what we’ve been talking about, the authentication issue.

**Steve:** Yes. He says, "As the web increases, so does users’ exposure to these workarounds." I’m sorry. "As use of the web increases, so does users’ exposure to these workarounds. Though no one is to blame, the result is pernicious. Hundreds of millions of people have been trained to accept anything any site wants to throw at them as being the ‘normal way’ to conduct business online. They’ve been taught to type their names, secret passwords, and personal identifying information into almost any input form that appears on their screen. There’s no consistent and comprehensible framework allowing them to evaluate the authenticity of the sites they visit, and they don’t have a reliable way of knowing when they’re disclosing private information to illegitimate parties, i.e., like phishing exploits. At the same time, they lack a framework for controlling or even remembering the many different aspects of their digital existence.

"People have begun to use the Internet to manage and exchange things of progressively greater real-world value. This has not gone unnoticed by a criminal fringe that understands the ad hoc and vulnerable nature of the identity patchwork and how to subvert it. These criminal forces have increasingly professionalized and organized themselves internationally. Individual consumers are tricked into releasing banking and other information through phishing schemes that take advantage of their inability to tell who they’re dealing with. They are also induced to inadvertently install spyware, which then resides on their computers and harvests information in long-term pharming attacks.

"Other schemes successfully target corporate, government, and educational databases with vast identity holdings and succeed in stealing hundreds of thousands of identities in a single blow. Criminal organizations exist to acquire these identities and resell them to a new breed of innovators expert in using them to steal as much as possible in the shortest amount of time. The international character of these networks makes them increasingly difficult to penetrate and dismantle. Phishing and pharming are now thought to be one of the fastest growing segments of the computer industry, if you can call it that, with an annual compound growth rate..." get this, Leo, "...of 1,000 percent."

**Leo:** Oh, man. That makes sense, though. It’s growing outrageously.

**Steve:** It absolutely does. He says, "For example, the Anti-Phishing Working Group Phishing Activity Trends Report of February 2005..." so this is...

**Leo:** Two years old.

**Steve:** ...two and a half years ago, yes, "...cites an annual monthly gross rate in phishing sites between July through February of 26 percent per month, which represents a compound annual growth rate of 1,600 percent. Without a significant change in how we do things, this trend will continue. It is essential to look beyond the current situation and understand that, if the current dynamics continue unchecked, we are headed toward a deep crisis. The ad hoc nature of Internet identity cannot withstand the growing assault of professionalized attackers. A deepening public crisis of this sort would mean the Internet would begin to lose credibility and acceptance for economic transactions when it should be gaining that acceptance."

**Leo:** That’s the big cost of this stuff is email and the Internet become less useful.

**Steve:** Well, in fact, I’m sure - I’ve heard reports, I’m sure you have, Leo, and our listeners probably have, or know people who have stopped using the Internet because they’ve been put off by it as a consequence of all this.

**Leo:** Yeah. Very scary.

**Steve:** And so he concludes by saying, "But in addition to the danger of slipping backwards, we need to understand the costs of not going forward. The absence of an identity layer is one of the key factors limiting further settlement of cyberspace. Further, the absence of a unifying and rational identity fabric will prevent us from reaping the benefits of web services. Web services have been designed to let us build robust, flexible, distributed systems that can deliver important new capabilities and evolve in response to their environment. Such living services need to be loosely coupled and organic, breaking from the paradigm of rigid premeditation and hard wiring. But as long as digital identity remains a patchwork of ad hoc one-offs that must still be hard wired, all the negotiation and composability we have achieved in other aspects of web services will enable nothing new. Knowing who is connected with what is a must for the next generation of cyber services to break out of the starting gate."

**Leo:** Now, this is coming from Microsoft. I hope that this doesn’t mean another proprietary single sign-on initiative from them. They’ve said they’re supporting OpenID, haven’t they?

**Steve:** Well, that’s where we’re going today with the podcast. Because of course many people will be familiar with exactly what you were alluding to, which is the hopefully defunct, if not still on its way toward defunction, and always having achieved dysfunction...

**Leo:** Passport.

**Steve:** ...Passport. I mean, I tell you, for a while there was a - you had to create a Passport account to be an MSDN subscriber, which I am. You know, I pay my 2,500 bucks a year to receive DVDs of Microsoft's latest and greatest. And it just irked me. And...

**Leo:** That's still true, by the way.

**Steve:** Yes, exactly, although I guess I just must have one installed now...

**Leo:** It's automatic, and it just signs you in.

**Steve:** ...and it's automatic. But, I mean, talk about a dead-on-arrival solution. The problem, of course...

**Leo:** But not misguided.

**Steve:** No, no, not misguided at all. Microsoft was right. The problem is, thank goodness there are some things which are proving to be bigger than Microsoft.

**Leo:** Right.

**Steve:** And of course...

**Leo:** Thank goodness is right.

**Steve:** Yes, you know, even we were talking last week in one of our errata about SPF. Or was that today earlier? The Sender Provider Framework.

**Leo:** Yeah, that was, I think, last week's podcast, yeah.

**Steve:** Okay, right.

**Leo:** I can't remember, you know, it's blurring together.

**Steve:** The whole SPF deal. Microsoft tried to come out with their own that they were going to license and said, oh, well, but it'll be a free license. And fortunately the industry, again, you know, email is bigger than Microsoft, and Microsoft ended up having to compromise and basically, you know, meld their solution in and sort of, they never really wanted to admit it, but, you know, they ended up adopting that protocol and saying, okay, fine, you know, we'll do something that is interoperably compatible.

Now, the real catalyst for today's topic was something that has appeared in Vista which has the strange name of CardSpace. And in fact, I say "strange," I think it's a bad name, especially when it was originally named InfoCard. For several years during development it was called InfoCard, which actually I think is a better name for it. Maybe it wasn't available, they couldn't get a trademark, or who knows why they ended up changing it from InfoCard. That was the internal project name. But it's called CardSpace. What it is, is essentially Microsoft's version of what we talked about a couple weeks ago with OpenID. You'll remember that OpenID promises, and the good news is it is delivering on this promise because this is so cool, it promises to allow people a means for having a single authentication system which is completely open source. And, in the case of OpenID, it is URL based. You give your identity as a URL to a page which you control. Either an identity provider provides it to you, you have your own page on MySpace, or what's the one you like now? Facebook?

**Leo:** Oh, Facebook, yeah. What's the one I like now. Let's see, what week is it? Who knows by the time this airs. It could be anything.

**Steve:** And so the page you control is looked up, and the identity server you have assigned, the URL for that is obtained. The site you're wanting to authenticate with then sends your browser over to there, along with some other information that it provides. You authenticate with that third-party service. Then it sends you back to the original site you wanted to authenticate to, having signed essentially the package that that first site provided. And so that's a way of using a single point of authentication among many different services. And it's very cool. The problem is, it really doesn't provide a mechanism for providing those sites with granular information about you which you are able to control. And it's sort of inelegant. Your browser's bouncing around the Internet, and it's not quite as seamless as it could be. There are means to cache credentials and to involve more scripting to make that process more transparent, but still it's really not seamless.

Well, what Microsoft has done, and the reason this is called a metasystem, is they learned from their mistake with Passport. They said, okay, oops, why did that not work? Well, everyone would immediately say, well, because it was yours. You know, and sorry, Microsoft, we're sort of stuck using Windows and other stuff that you provide, whether we like to or not. And a lot of Microsoft stuff is as good as anything else, but we don't want to have to. We want choice. And so what Microsoft did was they created a metasystem which explicitly allows other sorts of authentication frameworks to be put underneath the users' experience. And I would be less enthusiastic about this if it were only on Vista because, you know, I'm not there yet, and I know a lot of the world is waiting for the first Service Pack or longer. The good news is, it will be - this CardSpace technology will be back-ported to IE7 on XP. And there's already support for it, for example, in the open source community on Linux and in Safari and coming for Firefox.

So what is it? Okay. What this thing essentially does from a - let's talk about the user experience first, then we'll talk about what's going on underneath. In a CardSpace environment, that is to say, running on Windows or in Safari - and by the way, it is Safari on the Mac that there is a CardSpace-compatible experience now.

**Leo:** Yeah, 'cause there's no IE on the Mac anymore, so they don't...

**Steve:** Correct. So say that I'm an eBay auctioneer, and I have an eBay auctioning client that I use for managing my multiple auctions on eBay. So I want to authenticate myself to eBay. So I launch my client, this eBay-aware client. It connects to eBay and gets from eBay a list of authentication parameters, given that eBay were a system that supports this technology. So essentially it says, what protocols do you support for authentication? It asks, what trusted ID providers do you support, like Thawte, VeriSign and so forth; and what information would you like from us? So there's a protocol established that allows a client running on my system to basically sort of get an authentication requirement package back from somebody we want to authenticate with, all transparent to the user.

What happens then is there is a hardened, secure UI system or subsystem in Windows called CardSpace, which the client is able to hand this packet to. CardSpace then presents essentially a very simple and elegant UI to the user. It pops up, and it looks like a series of credit cards. These are cards that - and so think of cards as an abstraction for an identity that contains some information. So what happens is the packet goes to CardSpace. CardSpace looks at all the cards that reside on this user's computer. These may be cards that were issued by the government, by banks, and even by the user themselves. You're able to create your own cards. They don't have to come from some certifying authority somewhere.

So this packet says, okay, eBay trusts Thawte and VeriSign and Equifax or something, and would like to have our email address as the token it uses to identify us. You know, for example, logging into eBay now you give it your email address and your - or your username and a password. So CardSpace looks at the cards it has, finds the intersection between those cards and what eBay has said it wants, and presents that subset to the user. The user is able then to choose the card that they use for logging onto eBay, which will be among those in the subset. What then happens is that the CardSpace system goes to the provider, like Thawte or VeriSign, and sets up a secure connection, and says please get the user's email address associated with this credential.

So this is a key aspect of this, that personal information doesn't even reside on the user's computer. That's held securely, and doesn't have to be held, but in this case is, by the provider of the identity. So the bank or the government or whoever has issued this credential actually has the information. All that's in the card are some tokens saying, basically, the user's email address, maybe your street address, your mailing address, your phone number, basically any information that you want associated with that credential can be. But the content of it is kept outside the machine. So it is not available for compromise because it's not stored locally. Merely sort of a tokenized representation is.

So the provider sends this back to the user's machine. Now, at that point - and here's one of the critical aspects - the user is always provided with a screen showing essentially which information is going to be disclosed. In this case it would just be his email address. But one of the requirements for the system is that users always have complete control, the idea being this is not a system designed for the other party's benefit. This is designed for the end-user's benefit. The end-user selects the card and sees what information is going to be disclosed before anything that identifies them leaves the machine.

So essentially, although there's a lot going on behind the scenes, it's a very simple transaction. You fire up your eBay client. Up pops a screen with a few cards on it. You click on the one that you use for logging into eBay. Next thing you see is a confirmation screen saying is it okay for us to send the following information to eBay. Oh, and get this, there's even now an RFC, an Internet Request for Comments document, for how to securely embed logos, that is corporate logos, in X.509, which is the standard for security certificates. So that you also see eBay's logo with enough crypto wrapped around it that there's no way for it to be spoofed.

**Leo:** The logo helps a lot. I think that's important.

**Steve:** I really do, too, yes. Because, I mean, it's sort of like what you were talking about with SiteKeys, the idea being that it's something visual that the user can lock onto and remember and just sort of expect. He wants to see eBay's logo when he's about to click on a card and say, yes, I want to send this information to eBay. So he just says, yes, send it. So CardSpace returns this to the client, that returns it to eBay. All of this, of course, is wrapped in seriously strong crypto. We've covered that aspect of these transactions many time in our past podcasts, so that our listeners understand that all of that is possible. It's very possible to authenticate and to protect this stuff so that the channels at each stage of the protocol are secure. So from the user's standpoint it's a very straightforward transaction.

What this does more than OpenID in its basic form - OpenID, as we've talked about before, merely authenticates you. But it does provide you the luxury of not having to create individual credentials on every site you want to visit. You have a single point of authentication, and it's all under your control. Well, the good news is, Microsoft formalized their endorsement and support of OpenID as an underlying protocol for the so-called metasystem.

**Leo:** Good. I'm really glad to hear that.

**Steve:** Well, it's perfect, Leo, because what it means is that we get, I mean, OpenID is already taking off, and CardSpace was just born. And it would likely again be stillborn, much as Passport was, if they hadn't learned their lesson and really taken their hands off this thing and did the right thing.

Now, you'll remember that we've talked, I think it was on the Tech Guy podcast and your show last week, I mentioned how I prefer Google Checkout to PayPal from an ease-of-use standpoint because Google Checkout does contain and provide to the vendor my whole little packet of information that I have authorized them to make available so that I don't have to fill out the form. Well, this is the same sort of benefit here. You can create your own info cards and say, okay...

**Leo:** That's where CardSpace comes from, right, you have a space of cards.

**Steve:** Yes, exactly. And I've seen it. Microsoft has a nice little animated Windows video file that shows you this thing in use. I mean, it is really a nice user interface, if this thing succeeds, and because it's built on top of open source and OpenID. And in fact, this thing is open enough that there is an Apache module in full open source, I mean, everything sitting there that allows it to be a client of Microsoft Windows CardSpace system. So nothing has been, I mean, they've really learned their lesson. Nothing has been kept away from the open source community, so that I really am excited about this. I think this has a very good chance of succeeding.

**Leo:** So it doesn't supersede anything existing, it just coexists using OpenID as kind of the underlying common core.

**Steve:** Well, it doesn't actually use it. It can use it.

**Leo:** It supports it.

**Steve:** Yes, exactly. The idea is they've defined a number of things. For example, they call the relying party, or RP, the relying party is the entity that wants to receive the credentials. They call the identity provider, or IP, that party that provides the identity. And of course you have the user sort of in the middle there, which is arbitrating the conversations that go back and forth. And the crypto is used in order to allow all the parties to authenticate each other and to provide this in a secure fashion.

But it turns out that, thanks to the evolution of XML, there's something called SAML which is another open standard, the Security Assertion Markup Language, which is an XML-derived protocol, essentially, that allows this information to be conveyed and encrypted in a secure fashion that allows these parties to conduct open source dialogues of this kind of information. So essentially what it will mean is, as this spreads, as IE gets an add-on - I'm sure it'll be an ActiveX add-on to IE, and there exists one now for Safari running on the Mac, it's available under Linux, Apache's got a module, Firefox will have one - this will provide a very clean sort of a front end which is arguably easier to use from a user standpoint than having to have sort of a funky-looking URL that you use to identify yourself. And it sort of manages multiple identities at the same time. There's nothing that says you always have to authenticate with the same identity. You could just, you know, since users are able to be their own IPs, or identity providers, you're able to create an identity, you know, for example, over on Slashdot or over on eBay or over in random bloggings.

And so, you know, again, the beauty of this is that we stay in control, but there are things that are very powerful. For example, eBay, that is a so-called relying party, that RP, it could also be an identity provider if, for example, we wanted to prove how trustworthy and what our eBay integrity is. Remember that eBay has that whole voting system and feedback system where sellers are able to demonstrate what good sellers they are, and buyers are able to demonstrate what good buyers they are. Well, imagine that you'd like to establish your identity as someone trustworthy over on eBay, over on some other site. This system essentially allows eBay to securely package your credibility, your identity that you have earned over time there, and export it to any other site that you ask them to export it to. You can have them create the credential, which they're standing behind, to allow you to essentially not have to have your identity fragmented all over the Internet, but be able to pull it together.

**Leo:** Well, it seems like a good solution, especially since it's integrated into Vista. It makes it a lot easier.

**Steve:** Yes, exactly. It'll just be built in. And what I like about it is we don't have to, given that this takes hold, we don't have to move to Vista for it because we will have it in IE7 running under XP, which is, you know, where I'm finally comfortable, and I'm in no hurry to go to Vista.

**Leo:** It does concern me, though, because I'm, as a Mac user, kind of left out in the cold. Well, I guess I can use Safari, that's right, you told me that.

**Steve:** Yes, you absolutely will. And there is, I've seen screenshots of the Safari plug-in, which is in beta now, but is running and is successfully processing credentials.

**Leo:** I hope they put that on the iPhone.

**Steve:** So it's going to be another step forward, Leo.

**Leo:** Yeah, yeah, very good. So CardSpace, that's what Microsoft calls it. But Steve just likes to call it Internet Identity Metasystems. And I hope you've enjoyed this trip down Metasystem Lane. If you want to know more, of course, go to Steve's website, GRC.com. You can get a 16KB version of this show for the bandwidth-impaired, and transcripts, along with Steve's great program SpinRite, the ultimate disk recovery and maintenance utility, and of course all his free software. So, Steve, have a great time at Harvard.

**Steve:** I'm going to. We're going to, a week from the time people are listening to this, we're going to answer for Episode 99 the intriguing question, are you human?

**Leo:** Aha, and how do we know?

**Steve:** Exactly.

**Leo:** That's great. I love it. All right. We'll talk again next Thursday and every Thursday. Coming close to Episode 100, just a couple more to go. For Steve Gibson, I'm Leo Laporte. Thanks for joining us.