



RUNAS RADIO



<http://www.runasradio.com>



Richard
Campbell

RunAs Radio is a weekly Internet Audio Talk Show for IT Professionals working with Microsoft products. The full range of IT topics is covered from a Microsoft-centric viewpoint.



Greg
Hughes

Text Transcript of Show #012
(Transcription services provided by [PWOP Productions](#))



Richard Turner Checks Our Identity!
June 27, 2007



[Music]

Carl Franklin: From runasradio.com, you're listening to RunAs Radio, the weekly Internet audio talk show for IT professionals with Richard Campbell and Greg Hughes. This is Carl Franklin, introducing show #12, with guest Richard Turner, recorded Monday, June 11, 2007, at TechEd 2007 in Orlando, Florida. RunAs Radio is produced each week by PWOP Productions, offering professional media and podcasting services online at pwop.com.

Richard Campbell: Hi. You're listening to RunAs Radio and this is Richard Campbell, your host, and with me my co-host, Greg Hughes.

Greg Hughes: Hi Richard and everybody.

Richard Campbell: So, here we are, working on this again. I got another email.

Greg Hughes: We like the emails.

Richard Campbell: I do like the emails and if you'd like to send us an email, send it to info@runasradio.com. This email says, "Disk-based Backup," the subject keeps coming back. "Hi y'all from England." Can you say "y'all" if you're from England?

Greg Hughes: "Y'all" from England? How do you say "y'all" with a British accent?

Richard Campbell: I don't know. It doesn't work.

Greg Hughes: Hello y'all.

Richard Campbell: Hi y'all. "I've been listening to the PWOP Productions podcasts for over two years now."

Greg Hughes: I heard they're pretty good.

Richard Campbell: Apparently. Then he says, "More Mondays please," so now I question his taste.

Greg Hughes: You know, when we were at TechEd and you were mentioning Mondays and I had gone back and listened to #1.

Richard Campbell: And you met Mark Miller!

Greg Hughes: I met Mark Miller.

Richard Campbell: For your first time in your life.

Greg Hughes: Oh my God. That guy is so funny.

Richard Campbell: And now you understand, don't you?

Greg Hughes: He is hilarious. I'm going back and listening to every single Mondays that I can get my hands on.

Richard Campbell: Mondays is a geek comedy show. For those who haven't heard it, it is at mondays.pwop.com. It is not safe for the office.

Greg Hughes: No, it's very colorful, so be warned. If you don't like colorful, then just stay away.

Richard Campbell: You're not going to enjoy this. Nothing is out of bounds for Mondays. It's a little out of control.

Greg Hughes: Yeah.

Richard Campbell: But you can see Mark Miller is the center of that show.

Greg Hughes: Yeah, and he is a character.

Richard Campbell: He's really like that when you meet him in person.

Greg Hughes: He really and truly is.

Richard Campbell: Oh, let's get back to Matt's email here. Right.

Greg Hughes: Yeah.

Richard Campbell: "You asked in your latest podcast if people wanted to hear a podcast on disk-based backup and, yes, please. I'm in a situation where I'm looking at this for a client. Well, I'm looking at backup in general for clients quite often. For me, the new Windows Home Server looks very nice for this and it could be used for small offices too. Also look into Internet-based backup. That would be cool too. Regards, Matt Peters." Thanks for your email, Matt.



Greg Hughes: Yeah, Windows Home Server is very cool. For people who haven't had a chance to look at it, it might be something that would be worth looking at. I use a couple of different Internet-based backup for home computers and we actually do some disk-based backup here at Corillian, the company that I work at, but we sure have had a lot of interest and request just in the disk-based backup.

Richard Campbell: Yeah, I think we hit a button and that was show #1, Pat Hynds show, right off the bat where we talked briefly about disk-based backup and it keeps recurring. I've been doing some research and there is some cool stuff out there. I'm just trying to figure out what the best way to tackle the topic is, but do you know Quantum makes a whole array of disk-based backup solutions? All kinds of big, multi-drive gear, specifically ordered on backup.

Greg Hughes: Oh yeah. The drive manufacturers, Quantum included, do make specifically designed gear and combinations of drives and what-not just for doing that particular type backup.

Richard Campbell: It's just that I see a lot of systems here where they're backing up their production drives, two disk drives, so that it's fast and then backing that up to tape because they need the persistence.

Greg Hughes: And you also keep that fresh copy around, your latest backup, available for a fast recover or a fast search if you need it for that reason.

Richard Campbell: Right, rather than digging through the tapes.

Greg Hughes: Absolutely.

Richard Campbell: I still don't see a great solution, but I agree. We've got to do some shows on Internet-based backup and disk-based backup and I'm working on it. I've just got to find the right people.

Greg Hughes: You know what I'm wondering? Is there anyone listening in our audience out there that's already doing disk-based backup that would like to let us know about it?

Richard Campbell: Yeah, absolutely.

Greg Hughes: We don't just bring on people that are thrown at us by PR firms. In fact, we really don't even do that at all.

Richard Campbell: Not at all.

Greg Hughes: We talk to people that we know are out there in the field or that we hear about or, like when we were at TechEd, people that are very clearly very smart people who were doing cool stuff.

Richard Campbell: For sure.

Greg Hughes: So, if you're doing something cool out there, especially if it's disk-based backup, drop us an email and let us know.

Richard Campbell: That's at info@runasradio.com.

Greg Hughes: That's right.

Richard Campbell: So, Greg. This is another show we picked up at TechEd.

Greg Hughes: Yeah, a friend of mine, a professional acquaintance there, Richard Turner at Microsoft.

Richard Campbell: Yes. We had Richard on the identity panel for .NET Rocks!

Greg Hughes: That's right. Richard's one of those guys that -- well, first of all, he's got a great accent.

Richard Campbell: Oh yeah. He's English, so he sounds fabulous.

Greg Hughes: We should have asked him to say "y'all." That would've been great.

Richard Campbell: If only I'd known.

Greg Hughes: That's right, but seriously, Richard is in the product management side of things and specifically around .NET framework, right?

Richard Campbell: Right.

Greg Hughes: And has a very special focus on CardSpace and I had the opportunity at a Security



Summit for the company that I work at a few weeks ago to have Richard and Kim Cameron, who is an architect at Microsoft around Identity, they both came and spoke. Richard was at TechEd and we sat down with him and talked about CardSpace and Identity and what they've done and what's coming.

Richard Campbell: CardSpace is one of those fascinating products, definitely straddles the line between the developer audience and the IT audience.

Greg Hughes: I think you're absolutely right. One of the things that we asked Richard to do throughout our conversation was to talk about how does this really apply to the IT pro.

Richard Campbell: Absolutely. Hey Greg. Here we are at TechEd again. We're in the fishbowl this time.

Greg Hughes: Yeah. Not drowning. We're doing pretty well.

Richard Campbell: Yeah. This is the backside of the virtual TechEd stage. We have a recording studio and then we also have the editing studio, but we're actually in the editing studio because the recording studio is busy and we're sitting with Richard Turner. Hi, Rich.

Richard Turner: Hi. How are you doing?

Richard Campbell: A fine name too, I might add.

Richard Turner: Fine name, yes. All the best people are called Richard.

Richard Campbell: So, tell us a little bit about yourself, where you work at Microsoft.

Richard Turner: I work in .NET Developer Marketing and I own the marketing for Microsoft's Identity Developer Platform, which includes Windows CardSpace, ADFS, etc., etc.

Richard Campbell: So, I really wanted to jump into where CardSpace is going because CardSpace is really shipped with .NET 3.0, which meant when Vista came out we had a version, which was really version 1.0.

Richard Turner: Yeah.

Richard Campbell: And that has been out a little bit. We've had some other conversations offline and in other shows, I might add, about what the developers are doing with it. I really want to talk about where IT folks want to go with it. In the other conversations we've had about CardSpace, the first thing that came up was, "So, what's the story between CardSpace and Active Directory?"

Richard Turner: Always a good question. Maybe it's worth winding the story back a little bit so we can get a good understanding of what CardSpace is, what it's for, and what kind of scenarios that fits into both on the web and inside your enterprise potentially.

Richard Campbell: Absolutely.

Richard Turner: Yeah? So, I think the easiest way to describe CardSpace is that CardSpace is an application that runs on the client machine, which helps users better manage and control their different digital identities that they might need to use to identify themselves most safely and easily online and potentially to also allow them to perform things like authorizing tasks to happen or authorizing events to kick off, etc., etc.

Richard Campbell: Right.

Richard Turner: Windows CardSpace as you've just mentioned ships as part of the .NET framework 3.0. It is built into Windows Vista and it's available as a download for Windows XP. If you're going to be deploying the .NET framework 3.0 to your users' machines, you now have Windows CardSpace installed by default and you can find it on the Control Panel if you want to go and have a quick play with that.

Greg Hughes: What are some examples of, say, for a corporate IT shop or a business IT shop, where might they use CardSpace in the environment?

Richard Turner: This is a really interesting side of the story. When we explain the CardSpace story, we're usually talking to people who own or operate public-facing websites, websites that interact with people that you don't already have a strong established relationship.



Greg Hughes: The company that I work for does online banking sites and we've been working with you for a year and a half now on CardSpace...

Richard Turner: Yeah, too long almost.

Greg Hughes: And enabling that, right.

Richard Turner: Yeah, absolutely. CardSpace has very, very strong story for public relationships with people that you may have some knowledge of, but they are not, for example, part of your corporation. They're not part of your group of corporations or your group of partners that you interact with.

Richard Campbell: This is your customer or maybe your vendor, that sort of thing.

Richard Turner: Yeah, maybe your loosely affiliated partners and so on and so on.

Richard Campbell: So, they probably wouldn't have a domain account per se, but they have one step below that.

Richard Turner: Yes, absolutely. Interestingly, CardSpace has a number of scenarios that it provides great value into the enterprise as well. We're speaking to a lot of companies right now who have through acquisition or through other means have grown and spun up new organizations or acquired new organizations and haven't yet got to the point of integrating all of those organizations into a cohesive whole, so they haven't got 180, they've got 5. Maybe they've got a couple of other directory systems as well, etc., etc. Maybe they also have a bunch of partners who they regularly interact with and with whom they share information, they might share processors, etc. Now, one of the problems that we've seen repeatedly in these kinds of organizations is how, if you're the operator of your corporate purchasing system, let's say, how do you partner with your close business partners and allow them to access the information inside your organization?

Greg Hughes: I think there are two key things. You mentioned customers of like a bank or ecommerce site. There's an IT pro running an IT shop. I have customers, that's all the people that work at the company that I work with and, as you say, the partners that we work with. I'm primarily concerned about really two things that are somewhat

related to each other. Authentication is one of those, how do I know it's the right person, but also authorization, right? What is this person authorized to do?

Richard Turner: Absolutely.

Greg Hughes: What I authorize them to do could be based on the type of information that I receive from them.

Richard Turner: Absolutely. And, wouldn't it be great if when a user turns up at your extranet portal, if they were able to provide you a cryptographically strong token containing a set of information that allows you to not only identify who that person is and that they are coming from an organization that you're willing to trust, but also that the organization they're coming from is willing to say to you what kind of rights and roles that person has in relation to the information that they're trying to process.

Greg Hughes: Sure, right.

Richard Turner: A good example is a banking scenario whereby let's say your bank owns all your business accounts, but only executives of your company are allowed to get access to their accounts. Now, today, what usually happens is the bank has to set up an individual account for each person who is allowed to access the system.

Richard Campbell: Right, and immediately I'm thinking the average executive immediately shares that with their administrative assistant...

Richard Turner: Absolutely.

Richard Campbell: And circumvents all of those roles.

Richard Turner: Absolutely. At some point, the executive gets a better offer from someone else, disappears, and then who decommissions the account that now lives at the bank.

Greg Hughes: Right. On paper, it always happens. In the real world, it practically never happens.

Richard Turner: Absolutely. So, how long does that account stay open for? Oftentimes, we're hearing



these accounts often stay open for two or three weeks, which means the executive leaves and he still has access to the online banking account for the business two or three weeks after he's actually no longer an employee of the company. That's frightening from a corporate compliance perspective at very least.

Greg Hughes: This is interesting. It sounds like CardSpace and similar types of technologies really could be used not just to identify yourself and to present claims, but on the back office side could actually be used to help invoke a set of IT controls.

Richard Turner: Absolutely, yeah.

Greg Hughes: Do you consider this a multifactor type of credential? I guess you could use it in a multifactor environment, something I have, which is to have the actual card or the digital card, I have to present that to you, but I suppose you could also layer that with something I know or other types of information so that you could actually do a multifactor type of authentication.

Richard Turner: Sure, absolutely.

Richard Campbell: Are we talking about a PIN then?

Greg Hughes: Well, I don't know, Richard. What do you think? I could see where you could have a Smart Card. It could be something else I have, two things I have. You could still use a username and password and require an InfoCard on top of that or perhaps some type of other information that I provide. It could just be a username and an InfoCard. I could see a variety of different ways that I might present it. Is InfoCard still the correct term, by the way, for the card itself?

Richard Turner: InfoCard was its codename back in the dark old days. It is now called Windows CardSpace, so we try and stick to names that people recognize right now.

Greg Hughes: Right, absolutely.

Richard Turner: You should know better by now, Greg. Come along.

Richard Campbell: You've been doing this for 18 months, the dark old days being...

Richard Turner: Eighteen months ago.

Richard Campbell: Last year.

Richard Turner: Yeah, exactly. How fast does this industry move.

Greg Hughes: And as slow as the brain moves.

Richard Turner: Absolutely. What you've just described is exactly the kind of scenarios that we're seeing. So, imagine an alternative to the scenario we just discussed whereby instead of the bank creating an individual account for each user that comes in, the bank instead sets up a trust relationship, we'll talk about the details of that a little bit more later, but sets up a trust relationship with that client, your company. Let's say, for example, your bank configures its service to accept some kind of cryptographic identity token issued by one of their clients. Now, when the client user, so an employee of, let's say for example, Corillian. Well, I can't use Corillian because you're in banking, but let's say you work for...

Greg Hughes: Contoso Company.

Richard Turner: For Contoso.

Greg Hughes: There we go, okay.

Richard Turner: You as an employee of Contoso get given a username and password to log in to your machine or maybe you've even been given a Smart Card to log in to your machine at work.

Greg Hughes: Not likely.

Richard Turner: Not likely? Well...

Greg Hughes: Maybe in the future.

Richard Turner: You'd be surprised how many people actually are doing that now, but, yes, certainly in the future.

Greg Hughes: Okay.



Richard Turner: Now, you log on to your machine and via your extranet, you would browse to your partner's website. Now, your partner's website needs you to authenticate. Essentially, they can do one of two things, well, one of three things at this point. They can say "enter username and password," which, let's be honest, no one really likes because we all end up with too many usernames and passwords we can't remember.

Richard Campbell: Not me. I use the same one everywhere.

Richard Turner: You use the same one everywhere? Fantastic!

Greg Hughes: Yeah, he's our best friend.

Richard Turner: We'll find out what that username and password is at the end of the show.

Greg Hughes: I think we can all agree that usernames and passwords pretty much suck.

Richard Turner: Yes.

Greg Hughes: And that there are many, many problems with relying on them to do anything where you want to put real security around.

Richard Turner: Absolutely. So, an alternative thing that the organization might want to do is to prompt the user to provide a cryptographically strong token.

Greg Hughes: Okay.

Richard Turner: Now, you could very easily add Windows CardSpace support to your external extranet portal to say to the user to sign in to the site, you must provide me a card, which has either been issued by your organization or you must provide a card, which has been issued by the bank itself in order to sign in to the site. So, when you click the Sign In button, the website will send back a little blob of information to your client machine and your browser will detect that and then spin up Windows CardSpace asking you for your corporate ID card, let's say. Now, your corporate ID card might say about you what your first name is, what your last name is, what your position is, and what your role is.

It might say general dogsbody, cleaner, handyman, chart assembler, senior executive, chairman.

Greg Hughes: Gotcha.

Richard Turner: What happens with that is that when you submit that card to the website, to the banking website, what will happen is the CardSpace will obtain a signed encrypted token from your own employer containing the information that the website has demanded and CardSpace will relay that information via a secure communications link to the website that you're trying to access. The website can then decrypt that information, check has it been tampered with in any way, and can then look at the information being presented to make sure they are happy to accept these statements from this organization and that they're happy that this user has sufficient rights to get into the system and that they know what kind of capabilities to give that user within the system because they know what kind of role the user might have.

Greg Hughes: Or one or more roles effectively. For example, I could think of customers where maybe you have an extranet site and you might have customers that would have multiple customer roles.

Richard Turner: Absolutely.

Greg Hughes: The way I understand it, the CardSpace card, which is an electronic virtual card...

Richard Turner: Yeah, it's a digital card.

Greg Hughes: Has a set of fields in it, some of which can be optional. You can make them mandatory or optional, those are called, and the data that goes in there called claims, was that accurate?

Richard Turner: Yeah.

Greg Hughes: Am I able to specify what those claims are?

Richard Turner: If you are an issuer of an identity, yes, you can create entirely your own schema describing exactly what information you are willing to release about your subjects.



Greg Hughes: So, I could have a partner set to true or false, customer true or false, or that type of thing and then I can make decisions based on those claims as they're presented to me, but they're presented to me in a cryptographically strong manner that I can validate and verify and trust.

Richard Turner: Yeah. The strength of the token is in the fact that the token itself is encrypted so that only you can read it. The token is signed so that you can check that it hasn't been tampered with and because it's signed by the identity provider, you could also check the signature to see who issued that token making those statements about the user.

Greg Hughes: So, how do identity providers work? Are we talking about identity providers third parties that are out on the Internet somewhere and I can sign up with an identity provider or do I act as my own identity provider?

Richard Campbell: I think my reflex on that would be the bank issues the card.

Richard Turner: Could well do. The problem is the bank then has to manage all those cards.

Richard Campbell: Right, and maybe they don't want to. It's sort of I think the credit union scenario where there is a collective group that represents a bunch of different credit unions that does the card issuing.

Richard Turner: Sure. Yeah.

Greg Hughes: NCUA.

Richard Turner: Very possible.

Greg Hughes: NCUA or something similar to that, right, yeah.

Richard Turner: Very possible. All these scenarios are entirely possible. It just depends upon the scenario and who's comfortable with doing what.

Greg Hughes: Let's open a can of worms then. What about what used to be Passport is now called Windows Live ID.

Richard Turner: Yes.

Greg Hughes: What's the story with that and CardSpace, if there is one, and where are the two going to meet? I've heard a rumor that there will be some kind of a meeting of the two. Has anything fundamentally changed between Passport and Windows Live ID and where do you think that might be going in the future?

Richard Turner: Well, the Windows Passport, which is now called Live ID as you pointed out, has a long and checkered past. It was essentially created back in the late 1990s with the recognition that if Internet usage explodes, then people are going to end up having to create multiple usernames and passwords at hundreds of different sites that they might interact with.

Greg Hughes: And we've seen that happen.

Richard Turner: And we've seen that happen.

Greg Hughes: The problem is that people quite often use the same username and the same password...

Richard Turner: Absolutely.

Greg Hughes: Across those hundreds of sites.

Richard Turner: Yeah, and if someone managed to steal that, then they can replay that across 10,000 websites and find where you've used that same username and password.

Greg Hughes: And then find the person that's done that, which I wouldn't do, but if I chose to use the same username and password across many, many sites, I think most people do actually, at least in my experience in speaking with them, in order to actually solve that problem I now have to go to each of those hundred different sites that I have interacted with and I have to know what those sites are.

Richard Turner: Yes.

Greg Hughes: Good luck with that.

Richard Turner: Absolutely. The password management problem is a big, big issue, which we recognized back in the late 1990s, which is why we created Passport. Passport was all about a username and password that you would use to



authenticate the Passport and Passport would tell the website you're trying to access that you have successfully authenticated.

Greg Hughes: But the problem with Passport is that when I was using Passport to log in to a few different sites, it was also very expensive to get involved, but as I was using it to log into those different sites, I really didn't have any control over the information. In fact, I don't even know what information that I would have in my Passport. Maybe it's being provided to, at the time, eBay or whatever other site that I was logging on to.

Richard Turner: Absolutely. You touched on a couple of points there, one of which was that Passport at the time charged a fee to websites that wanted to adopt Passport and many websites just weren't interested in paying the money and didn't see the point in it and so created their own username and password and drove the users into the quagmire we now have. The other side of it is that, yes, you're absolutely right. The user isn't necessarily in control of their information because when you sign in to Passport, how do you know what information Passport is telling the website about you? Luckily, there are safeguards in place there so very, very little about you is actually transmitted.

Richard Campbell: Except I'm thinking that I gave an awful lot of information to Microsoft when I set up Passport, so using it elsewhere you presume, my automatic reaction is all of that information went across.

Richard Turner: That might be the first assumption. In fact, very, very little of that data at all goes across. It's pretty much used as a unique identifier for you with maybe your display name that actually gets sent to the partner website.

Greg Hughes: Part of creating trust though is if I can actually see what is going, then I know that I can trust it and I don't even have to worry about it and I don't have to think about it anymore. That ability to visualize what it is that I am sending whether it's somebody else sending it for me or if I'm doing it directly, there's real value with that just in terms of building trust.

Richard Turner: Absolutely. That's one of the very, very core features of Windows CardSpace is in

fact the first principle, which is the user must remain in control of the exchange of their digital identity information at all times. With CardSpace, when Windows CardSpace pops up, you get to see the cards that you own. When you choose to submit a card, the first time you submit the card, we show you a preview of what information is going to be submitted to the site before it leaves your box and if you want to on subsequent submissions, you can click the Preview button instead of the Send button so that you can see what data is about to be submitted.

Richard Campbell: So, I get a chance to be reminded of what's being sent each time.

Richard Turner: Absolutely.

Richard Campbell: But that doesn't necessarily mean you can control -- the only control you have over what's being sent is saying, "I'm not going to send that."

Richard Turner: Absolutely. That's a brilliant function essentially.

Richard Campbell: Because the host site is saying, "I require the following information."

Richard Turner: Absolutely.

Richard Campbell: That's fair. They're saying, "You got to give me this." "I don't wanna give you that." Well, then, we're done.

Richard Turner: We're done. Absolutely. Just like meeting someone you really don't want to interact with in a bar somewhere, you can walk away from the conversation.

Greg Hughes: Now, my bank or other company could have optional fields that are not required like maybe they don't require my cell phone number, but they could make it optional and in that case, if it is an optional claim, then I can choose whether or not I want to provide that.

Richard Turner: Absolutely. By default, we err on the side of minimal disclosure, so by default we don't enable the optional fields. If a website says, "You must give me your first name, last name, email address, and if you want to, you can tell me what country you live in." Then, when Windows



CardSpace shows you the preview of the card itself, the user will see that CardSpace has only selected first name, last name, email address, and there's a little button down the bottom left-hand corner that says, "Include optional fields," and then the user can choose if they wish to send also the country that they live in, which might help them in terms of just not having to fill in these many fields when they're registering on the site. It's a useful feature for those kinds of scenarios.

Richard Campbell: All right. Let's get back to the original question, which was, so, how am I going to tie the information I already have in my Active Directory stores to this kind of CardSpace store as well.

Richard Turner: Absolutely. If you are going to be an identity provider, you are going to be an organization that issues cards to your employees perhaps or even to your partners or to your customers or whoever it happens to be, you need to have a piece of software, which allows the user first of all to walk up to your site and, for example, answer sufficient questions that you're comfortable that they are who they claim to be and then you issue them a managed card. A managed card doesn't actually contain any data. What it contains is, essentially, a URL to the security token service that will actually issue the real token when requested. It will also contain the names of the fields that the card represents, so this card represents first name, last name, email address or this card represents position, title, years of service with the company, whatever it happens to be. It also contains a description of how the user must be authenticated because when the user selects their managed card and hit submit, CardSpace must reach out to the identity provider and ask for the real token, the actual data itself. How does the identity provider know who the user is? Now, in Windows CardSpace v1.0, we support essentially whatever WF Security supports, which means X.509 certificates, maybe on SmartCards or even software certs built into your client machines, Kerberos tickets which is great for corporate enterprise scenario because then we don't have to prompt the user for another form of credential. We can just pick it up off the wire. We can use a shared key value and, in fact, in CardSpace, we can use a shared key value, which is the value of another personal card that you create yourself on your local machine that generates a unique ID for that card.

The final one is username and password, but we'd like to try and avoid that wherever possible.

Greg Hughes: Sure.

Richard Campbell: I guess that's basically a backward compatibility element there.

Richard Turner: Absolutely.

Richard Campbell: People are still using these and they can't migrate everybody at once so have some kind of mechanism.

Richard Turner: Absolutely, but even that is better than asking for username and password on the website because CardSpace runs on a very secure environment, which makes it much harder for hackers and malware to get into. So, typing your username and password into the environment within CardSpace itself is safer than typing it into a website, which is open to all the keystroke loggers and...

Richard Campbell: And you're only doing that once and then it's in the card so you are more likely to be unique username, unique password, you don't have to remember it, it's in the card now and protected in other ways.

Richard Turner: Sure. So, the beauty with this is, is the user experience is almost identical apart from maybe an extra authentication step like "insert your Smart Card and type your PIN" when you use the card. It's identical for personal cards, which you create yourself on your own machine and managed cards, which you obtain from third parties. The user experience is use your master, click the Login button on the page, up pops Windows CardSpace, you select the particular card that you're interested in submitting to the site, you click Submit, and at that point you might be prompted for a PIN and a Smart Card, for example, or it might automatically pick up your identity from the wire or from the self-issued card on your machine and then requests the token from the identity provider and posts that token via HTTPS to the website that you're visiting.

Richard Campbell: What about the roving user? So, I have a bunch of machines. Anybody can use them. I want you to take your identity and your info with you and be able to sit down to any machine and authenticate successfully. For the most part, I've just



heard CardSpace is this highly encrypted chunk of data living on a machine. Can I put it somewhere that I can carry it?

Richard Turner: Absolutely.

Richard Campbell: How am I going to protect that?

Richard Turner: Very good question. The portability of cards is an imperative for CardSpace because as you've just said, all the information about your cards and the data associated with personal cards is all stored locally on your own machine. The data behind the managed card is stored by the identity provider, but you need, for example, to back up your card so that if your machine toasts, then you can get them back again. Or if you maybe move machines or if you want to take some of your cards and copy them onto your machine at home so that you can also sign in from home to websites and be known as the same person. We need some way of exporting those cards and we provide an export-import mechanism in CardSpace v1.0 today. You choose the cards that you want to export. You provide a password, which encrypts the exported file, and it exports an encrypted chunk to your hard drive or to USB stick or whatever it happens to be.

Greg Hughes: And then I can pick that. I can take that over to another computer and I can use it there.

Richard Turner: Absolutely. You can import it to the next machine, yeah.

Greg Hughes: You sort of blew right by something, which piqued my interest a little bit. I think it's important, especially if we're talking about the gals and guys that work in IT departments in companies or if it's the one-person IT department. Some of the things that they are charged with worrying about, you said something along the lines of, I'll paraphrase, basically that you don't have to worry so much about the keystroke loggers.

Richard Turner: Yes.

Greg Hughes: You were talking about usernames and passwords and the way we've always done things, so what's the difference?

Richard Turner: Keystroke loggers and mouse loggers essentially come in two flavors, one is the user mode piece of malware and the other is a kernel mode piece of malware. Either of them use various mechanisms within the operating system to essentially record and trap the different keys that you press and the mouse movements that you make so that they can perform algorithms against the keystroke stream to synchronize with events that they see happening on the screen itself, so they recognize the IE 7 comes up and then they recognize that IE navigates to a particular page. They start recording the keystrokes because you're probably just about to type in your password to log in. That's how they can capture your username and password and they can either record it or transmit it to a malicious site that then uses that username and password to log in as you. Now, one of the beautiful things with CardSpace is, as we just described, the user experience typically is click your mouse on a button, up pops the identity selector, click the card that you're interested in, click the Submit button, and you're done. There are no keys to log. There are no mouse movements that they can synthesize.

Richard Campbell: The logging opportunity came a long time ago when you set the card up in the first place.

Richard Turner: Well, if it was a personal card, then possibly, but you need to have a kernel mode keystroke logger in order to break that mechanism because CardSpace itself actually spins up an entirely private desktop separate from your logged in desktop session, which means that in order for a piece of malware to watch the keystrokes happening in their separate desktop, they'd have to watch them from the kernel, which means that to get into the kernel, they got to be in a kernel mode hackery, they've got to get past the Vista protection mechanisms like UAC or if you're on XP and hopefully most users and enterprisers at least will be running non-admin then they won't be able to install those kernel mode drivers.

Richard Campbell: Even then, creating the card is a totally separate chunk of code from the webpage requesting it as opposed to the existing mode where everything is in IE, you only have to get through one thing to capture it's this site, this username and password, so that disconnect is going to impair things a great deal.



Richard Turner: Absolutely. We've erected a couple of fairly seriously large walls now around this stuff so that we've raised the bar away from simple script kiddie or trivial hack to something requiring a great deal more effort and a great deal more experience and knowledge essentially changing the economic model of hacking CardSpace entirely compared to the economic model of phishing people.

Greg Hughes: And by raising the bar, when you raise the bar and you change the landscape, the threat landscape somewhat, it also means that if somebody does eventually get over that bar, that the threat is probably pretty high.

Richard Turner: Yes.

Greg Hughes: Hopefully, you all are thinking about that.

Richard Turner: Oh, we're painfully aware of that stuff, yeah.

Greg Hughes: Do these protections that you've put in place and these walls that you've built, they apply to everything we do in CardSpace so not just using the cards to do the logins and what else, but also the creation of the cards and the exporting of the data if I want to move it to another computer, all that is also in a separate process.

Richard Turner: Absolutely. When CardSpace is running, it's not just in a separate process, it's in a completely separate desktop. So, you are running applications, running on Windows, unless they can get to the kernel, can't even see there is another desktop.

Greg Hughes: Right, gotcha.

Richard Turner: Yeah. It's essentially the same mechanism that Ctrl+Alt+Del uses to drop you back to the secure desktop, which is where all the Winlogon and GINA infrastructure runs protecting your logon infrastructure from malware as well.

Richard Campbell: Jumping back to that roving profile, we really talked about being able to export the CardSpace data on to a key and then import again to the machine. Is there no way for me to keep my

profile mobile so that I don't have to keep copying things back and forth?

Richard Turner: This is actually something we're focusing a great deal of effort on for future versions of CardSpace for vNext and vNext beyond that and so on and so on.

Richard Campbell: You're not going to talk about V2 yet, just it's only vNext?

Richard Turner: Internally now we have a naming strategy, which is if you've released a product before, the next version of the product is the next sequential number in quotes, so it's CardSpace "2," whatever that happens to be, or CardSpace "3" or CardSpace "4." In whatever versions of CardSpace we can fit these capabilities into especially when it comes to roaming identity information, you're not just going to want to store that information on some old random USB key that you got free with a box of cornflakes. You're going to want to store that information on a strong cryptographically protected device such as a Smart Card or an intelligent USB device, which are easily available today, but will require a little bit of work to add a few capabilities to enable CardSpace to not only store the cards on the portable device as well, but also perhaps act as a security token service, allowing you to use the secure authentication mechanism offline or in non-Internet connected environments.

Greg Hughes: Yeah, I think for big businesses whether it is big banks or corporations or what have you, usability drives supportability and the cost of supporting something whether it's because it's new or because it's complicated or what have you is a pretty premium concern. What is there now for the people that need to manage all of this, say, in a corporate environment or in a financial services or similar type of environment that's likely to use this and what do you see coming in the future?

Richard Turner: The enterprise story is definitely something that's coming in the future, in a very near future. We're not talking two to three years out. We're talking within the next 12 to 18 months or so. You're going to start seeing stuff rolling out of Microsoft to provide you with that security token service, for example, that performs the functions of issuing cards to authenticated users and then when the cards are used, issuing the tokens that are



requested. So that security token service will integrate with the AD infrastructure so that if you got users in AD or in ADAM, then that will simply plug into this STS infrastructure and allow you to control which users you're going to provide access to cards to, what information goes into those cards and so on and so on, all the usual management tools and so on.

Greg Hughes: You see this replacing the RADIUS server at some point in time?

Richard Turner: I think RADIUS will still be there for some time to come. None of this stuff suddenly just stops on the day that we ship something. It takes time for these things to move forward, but who knows what will happen moving forward with some of these technologies. Some of this stuff's going to be around for decades and decades, but the general notion is that we're providing the service side technology for you to become an identity provider using the Microsoft platform and as per usual try and make it as easy as possible, as manageable as possible, and as performant as possible within the constraints of time resource and everything else that everyone else has to fight with as well. We're doing our best to come up with a decent strategy and a decent set of technologies and products and you will start to see some of those coming out from Microsoft late summer/early fall onwards. That's one part of how to become an identity provider. On the other side of it, what happens if you want to accept information cards? Now, we already shipped a bunch of helper classes and utilities for your developers to take advantage of to easily add CardSpace support to your site.

Greg Hughes: Right, a bunch of widgets, if you will.

Richard Turner: Absolutely. Just a bunch of stuff they can slap on their website and add CardSpace support very quickly. In fact, we found out this morning that a challenge was made last night to one of the guys here at the conference to go and add CardSpace support to his site.

Richard Campbell: That was the folks at CriticalSites.

Richard Turner: It was, absolutely.

Richard Campbell: Patrick Hynds and Duane Laflotte.

Richard Turner: Absolutely. They took up the challenge with gusto. They went off and bought themselves an SSL certificate, which is required to protect the website and the information it's exchanging with CardSpace and to identify the website to CardSpace. They went and bought an SSL cert for their domain online, they obtained the certificate, they installed it on to their machine, and they configured the certificate appropriately. That took them about two hours and it took them less than an hour to write the 12 to 15 lines of XML on their login page and the five or six lines of code to actually process the token and make a small database modification. And, within literally two or three hours, they were done. They have CardSpace support on their website.

Richard Campbell: Yeah. I think the toughest part of the whole process was getting the SSL cert installed in IE 6.

Richard Turner: Absolutely. Getting the cert in the first place and having to provide the right complements and so on and so on. Absolutely.

Richard Campbell: All those hoops to get that stuff together. The code side of this doesn't look too painful. I think the challenge is going to be managing the keys well when you're an identity provider.

Richard Turner: Absolutely, but it's the same old SSL certificates that we all know and love already. If you already have an SSL certificate for your site, you can actually use that to protect your site with and to identify it to CardSpace. If you are an entity that does anything serious, i.e., you're not just using this for personalization, you're actually maybe storing sensitive information or performing financial transactions behind the scenes, we do strongly encourage you to take the hit and go buy an EV certificate, an extended validation certificate.

Richard Campbell: Back in show #8 with Brian Komar, we spent a good long time talking about EV certs.

Richard Turner: Wonderful.



Richard Campbell: Yeah, I was just thinking exactly that. I don't think I'd want to use a managed card from anyone that didn't have an EV cert backing it.

Richard Turner: Precisely.

Richard Campbell: Am I going to as a user be able to see that or even better as an IT manager? Am I going to be able to set group policy on my machines to say, "If there's no EV cert here, forget it! You don't get that card."

Richard Turner: You absolutely could. There's nothing to stop you. You could use your management tool of choice to scan your websites and if you see anything that says X information card and the website and it's got a standard SSL certificate on it, raise the vent somewhere and have someone come down on that team like a ton of bricks. Getting an SSL cert requires a longer process. It means you have to go and prove that you're an officer of the company, the company exists, and so on.

Greg Hughes: For the EV cert.

Richard Turner: That's for the EV cert, yeah, absolutely, but in exchange you get back a certificate that lights up the address bar green in IE and importantly, when the users who use CardSpace come to your site to sign up, we show them a nice shiny page with your company's name, its location, state and country, your corporate logo, as well as the logo of the certificate authority that actually issued the cert to you. It gives the user a much nicer experience, a much higher level of confidence that you are who you claim to be.

Greg Hughes: Yeah, it's good validation to let me know that I'm on the right site. You said light up the address bar in green in IE.

Richard Turner: Yes.

Greg Hughes: What if I don't use IE?

Richard Turner: Mozilla does the same, Opera does the same.

Greg Hughes: And if I don't use Windows?

Richard Turner: If you're running Firefox on Linux, it will still light up green. It has to be a fairly recent version of Firefox, but, yes, it will.

Greg Hughes: Right. Now, there's a pretty strong open source and a community movement in this whole area.

Richard Turner: There is. That's one of the most exciting things actually about working in the CardSpace project is we've been able to foster wonderful relationships with many people out there in the open source community, on Linux platforms, on Mac platforms using PHP, Ruby, Pearl, Python and everything else. And, we have a great relationship with these guys because many of these guys are, how do we say it, much more technically adept than your typical general office-based PC user. They really get the problem, they understand the issue, and they've taken to CardSpace very, very well indeed. We're working wonderfully with Novell and with IBM and with Oracle and with Ping ID and a bunch of close compatriots in this space.

Richard Campbell: So, we're actually at the point where someone in a Mac OS X is going to be able to pop up that CardSpace window, too?

Richard Turner: Actually, they can go into it now.

Richard Campbell: Really?

Richard Turner: It's not actually CardSpace they pop up. They can go to Chuck Mortimer's blog and they can download a -- I think Chuck's is for Linux. I forget which way around it goes, but one of Chuck's colleagues actually wrote the -- I think Chuck's is for Linux and I think one of Chuck's colleagues actually wrote the extension for Safari so that it pops up a simple identity selector for those platforms. Now, this is just a proof of concept to prove that it can work and they're working on improving this slowly as time goes by, but Novell is actually sponsoring Project Bandit as well, which is an open source framework for identity selectors and that's being contributed to Project Higgins, which is Novell, IBM, Social Physics, Red Hat, and a bunch of other guys who are building the relying party codes to the code at your website that you need to accept cards, an identity selector that the user runs, and the



security token service for their platforms and technologies as well.

Greg Hughes: Is there a drive towards standards in this area?

Richard Turner: Well, CardSpace only speaks standard protocols on the wire. That's one of the other great things with this thing is that when it speaks to the website, it does so over HTTPS. It's just HTTPS H post again. In terms of talking to the identity provider, it's pure WS-STAR over HTTPS again. We use WS MetadataExchange policy and security policy to hook up a secure conversation to the STS itself and we use WS-Trust embellished with WS-Security headers to request the security token from the identity provider and it sends back the response via WS-Trust response message. So as long as you can speak WS-STAR, you can become an identity provider and as long as you can speak HTTP you can become a consumer.

Richard Campbell: I find myself almost unable to conceive of the idea that we might actually have a common strongly authenticated login mechanism across platforms and across software.

Richard Turner: Isn't it a frightening concept? This has come about so amazingly quickly. It really does shock you sometimes. When you look at it, you go, "Oh my God. It's so simple. Why didn't we do this 20 years ago?" Kim, if you're listening, you should've done it earlier.

Greg Hughes: The real difference is that companies, Microsoft included, but also others really have opened the doors and have started to have conversations.

Richard Turner: Absolutely. This is nothing but goodness for the whole industry because, let's face it, you're prone to phishing regardless of what platform technology or device you are on.

Richard Campbell: Without a doubt. You're talking about, yeah, Kim should've done this 20 years ago, but the reality is this has been really built on the back of all of that W3C work development in WS standards. We wondered if it was worth it at the time because there was a lot of arguing, but this looks like one of the strongest manifestations we could hope for, at least in the security authentication area.

Richard Turner: Absolutely. This really is a trailblazer I think and real validation as to why WS-STAR is so important because now it gives us a Lingua Franca on the wire to do the kinds of things that we would never have been able to do with any of the individual proprietary technologies that we've seen from many, many vendors in the past. Now, we have an open, intra-operable communication fabric that lets us do really interesting things like this.

Richard Campbell: And funny that the codes suddenly get simple when the specs are good.

Richard Turner: When the specs are good, you know how to write the frameworks that use those specs, making it easy as heck for the developer to consume those libraries.

Richard Campbell: Rich Turner, it's been a lot of fun talking to you.

Richard Turner: Absolutely, you guys, too. Thanks very much for the opportunity.

Richard Campbell: Going a long way from CardSpace all of a sudden.

Richard Turner: Wonderful.

Richard Campbell: And we'll talk to you next week on RunAs Radio.