RunAs Radio

http://www.runasradio.com

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.

Text Transcript of Show #078
(Transcription services provided by PWOP Productions)

Wes Miller Enables Windows Rights Management Services!
October 8, 2008

[Music]

Brandon Wenn: From runasradio.com, you're listening to RunAs Radio, the Internet audio talk show for IT professionals with Richard Campbell and Greg Hughes. This is Brandon Wenn, announcing show #78, with guest Wes Miller, recorded Thursday, September 25, 2008. RunAs Radio is produced each week by PWOP Productions, providing professional media and podcasting services online at pwop.com.

Richard Campbell: You're listening to RunAs Radio. I'm your host, Richard Campbell. With me as always my co-host, Greg Hughes.

Greg Hughes: Hey everybody. Richard, how is it going today?

Richard Campbell: Well, it's raining in Vancouver. I bet you it's raining in Portland.

Greg Hughes: Nope.

Richard Campbell: Oh come on.

Greg Hughes: It's a little; it's cloudy. It's kind of gray today but no, it's not raining.

Richard Campbell: All right. Well, fall is fall and of course fall means conference season and probably when this show is running, I'll be in Europe or something. My fall is insane this year.

Greg Hughes: Yeah, it's a lot more insane than mine. That's for sure. You got a lot going locally but you seem to, as usual, have a lot of going on all over the world.

Richard Campbell: But you and I are going to be together in Barcelona TechEd Europe.

Greg Hughes: Yeah, I'm looking forward to that. I know we say that every week but every time you mention it I get a little bit more excited.

Richard Campbell: They changed things around this year. Our stage, the community stage where we're going to do Speaker Idol and our panel discussion and so forth, is dead center of the floor this year instead of off to the sides.

Greg Hughes: Yeah, it's a pretty cool layout they got down there in the hall.

Richard Campbell: Yeah, it's exciting. I'm really looking forward to it.

Greg Hughes: I've been looking at the sessions that are listed and a lot of the content for this TechEd EMEA. It's going to be a really good show.

Richard Campbell: If you're a listener to RunAs, you probably want to give a listen to .NET Rocks! and .NET Rocks is running the sweepstakes right now for a free ticket, airfare, hotel, and admission to TechEd Europe. You can use it this year or next year.

Greg Hughes: Right.

Richard Campbell: That's at dotnetrocks.com.

Greg Hughes: So when does that end? When does that contest come to an end?

Richard Campbell: That's like the week before TechEd actually goes they're going to end the contest to pick the winner and that's one of the reasons they offered the second year so if you can't actually tell your boss a week before, "Hey, I won a trip to TechEd. See ya," you can go the following year.

Greg Hughes: Yeah.

Richard Campbell: Which isn't in Barcelona. I think it's in Germany. I think it's in Berlin but we don't know for sure.

Greg Hughes: That would be pretty darn awesome so if you're either unemployed or if you're a consultant that has nothing to do, then you can certainly take advantage of it this year, otherwise, we'll be more than happy to see you next year.

Richard Campbell: Absolutely and any questions, comments, shows you'd like to see, send us an email info@runasradio.com.

Greg Hughes: It's your input that makes the show what it is.

Richard Campbell: All right, let's jump to our guest, the one, the only Wes Miller. What can you say about Wes Miller? Ex-Microsoft, ex-Winternals, runs with tech fellows like Mark Russinovich, and now with CoreTrace?

Wes Miller: Uh-hmm.

Richard Campbell: Yeah? Tell us a little bit about CoreTrace, Wes. Welcome. Glad you're back.

Wes Miller: It's great to be here. We'll have to try not let 72 shows run between the next time I get back and talk to you guys again.

Greg Hughes: Show #6 was the last time that we talked to you.

Richard Campbell: Yeah, back when we were just figuring this stuff out.

Wes Miller: It's been a little bit. So yeah, yeah, basically during that timeframe you guys were doing that, I took a year. I was working in a little startup here in Austin and along came another startup that is much more security focused and much more really right up my alley and basically beginning with a project they've started in 2001. One of the founders had started creating a platform for application whitelisting, something that you may recall from my time at Winternals. It was something I pretty fundamentally believe in. I chatted with them, found out we have a lot in common and so I've been serving as their product manager since last December so going on a year now and it's been a blast. Actually, we just got back from a conference. We were at DEMOfall two weeks ago, one of the 72 companies that had the coming out party and it was phenomenal so it's a great experience and pretty jazzed about where our products go.

Richard Campbell: It's a great area of thinking. I don't want us to go deep into whitelisting right now but if you haven't thought about this, it's the same basic concept of getting a fingerprint for your app and that's a good way to stop non-authorized apps from running on your machines.

Greg Hughes: Yeah, that would be a great show in and of itself. We'll have to have you back to talk about that sometime.

Richard Campbell: I'm with you. That's a good idea. I'll stick that in the hopper here and let's come back in a few weeks and really do dig into white listing some more.

Greg Hughes: Yeah, but today...

Richard Campbell: Yeah, what is today?

Wes Miller: I was thinking maybe we could talk about information rights management.

Richard Campbell: Oh my goodness. All right, security show, Greg, it's your game.

Greg Hughes: Okay. So if you bring up rights management, the first thing that we have to do is we have to talk about what we're not going to talk about because rights management, just those two words have been applied to a lot of different products, technologies, add-ins, downloads or whatever at Microsoft. Maybe we should define the big picture. What different rights management stories there are and then drill down on maybe the Windows Rights Management or Active Directory Rights Management or the topic that we want to talk about today.

Wes Miller: Sure, yeah. It's like the Fight Club. The first rule of rights management is you don't talk about digital rights management.

Greg Hughes: Or never say the words digital rights management, right?

Wes Miller: Yeah. Fundamentally, the topic that's been of interest to me for a while and really of late, actually I have an article that run a couple of months here in TechNet that is specifically talking about Windows Rights Management Services, so RMS as it's usually abbreviated, and Office Information Rights Management or IRM as it's usually abbreviated.

Greg Hughes: Got you.

Wes Miller: The two, though their separate technologies integrated into separate pieces of Microsoft infrastructure, are completely interrelated.

Greg Hughes: Got you. So what does that mean?

Wes Miller: So what it means is if you actually look at the two pieces of technology and it's funny because usually people tend to disassociate IRM and RMS as not being DRM, but you know, at a fundamental level that's what they are because DRM is all about having content be owned and protected and having it not go where it's not supposed to go.

Greg Hughes: Right, controlling access and disclosure if you will, right?

Wes Miller: Exactly, exactly and so what IRM does is it works to protect the content from within Office and Windows then services the proxy agent to say, "All right, you've protected the content. Now who should actually have access to it?" and between your domain infrastructure and your local machine then it will actually proxy that and say, "All right, this user has permission to see this content. Let's go ahead and allow him to view it or print it."

Greg Hughes: Let's talk for a minute about the problems that we're trying to solve. We have a tendency as IT guys to sort of dive into technology and then try to find a problem to solve once we've discovered some cool technology. Let's take the other route.

Wes Miller: Sure.

Greg Hughes: Talk about business problems before we really dive into the technology side.

Wes Miller: Absolutely. Well, you know it's funny because I wound up on several calls. When we

go out and talk to customers, we have a really great solution for stopping the bad stuff coming in and they'll often turn to us and say, "That's great. So that solves most of my problems but I have this other problem. How do you keep the good stuff from getting out?"

Greg Hughes: Right.

Wes Miller: That's the fundamental problem. There are sort of two approaches to this and one of them which had been the industry approach for years is make my USB ports go away.

Greg Hughes: That's what Epoxy is for. Hooks it together.

Wes Miller: It's funny you mentioned that. I remember at Microsoft we actually had a government, I won't name the country and I won't name the division of the government, but they came in and they actually said that this was their technique to protect rights.

Greg Hughes: They are not the only ones. I've worked with financial institutions in the real world who, the company that I worked at in the past doing security audits and they would send their auditors in and they literally have their USB ports Epoxy'ed. I mean it was a clear Epoxy and it was filled up.

Wes Miller: While a great one-off solution, it doesn't scale real well and doesn't really solve the actual problem because as soon as the user draws in a CD-RW and you haven't done device control to that level which was hard until Vista, then you've lost control of the content again so the problem is you're stopping the guy after he has left the gate and saying, "Hey, you probably shouldn't be taking that right now." That's really what rights management in the IRM world is all about is protecting the content within your infrastructure so things that used to happen at Microsoft where you see a great email in the morning from Steve or Bill when I was there in 1997 to 2004 and the great email would, you'd see it and you're like, "Oh, this is awesome news," and it would say Microsoft Confidential Right at the top and at the bottom in really big red fonts and somebody...

Greg Hughes: Right. Then it's on a thousand blogs by 3:00 p.m., right?

Wes Miller: Exactly. It was on the Seattle Times in an hour.

Greg Hughes: Yup, right, and probably crossed posted to my blog, who knows? I mean...

Wes Miller: Exactly which is fine as long as you get the traffic but...

Greg Hughes: As long as I wasn't first, that's it, yeah.

Wes Miller: Exactly.

Greg Hughes: This technology that Microsoft has put together, we should dive in to what it does but it's really transformed and changed over time. I can remember the first iterations of this in Office and dealing with attachments to email for example and how you could protect stuff inside of Microsoft realm but once you took stuff outside of Microsoft's software, maybe it wasn't quite so protected. Has that changed or am I even accurate in that regard?

Wes Miller: You're close and actually there's a couple of things that come into play here. You'll recall there's been a big contention that happened in the DRM for a second. There was a big contention back when they were building Vista about Microsoft building in the HDCP, the high def copy protection, that went all the way up into the analog layer so you had to have a special monitor, yada, yada, yada.

Richard Campbell: Right.

Greg Hughes: Sure.

Wes Miller: Well, that whole idea eventually fails even there because of the problem referred too often as the analog hole and that fundamentally means that anytime something gets rendered to a screen or piped out to an analog output, you've lost control of it because it's no longer digital.

Greg Hughes: Right.

Wes Miller: So if you think about this virtual world we're living in where people have VPCs and VMware installs where they've got Windows running out of there, it's easy enough to capture a screenshot of whatever is running on that screen so the problem is you have to understand whenever you approach rights management like this that there are some cut off points where you say it's good enough and I have to think for me at least IRM going that much farther is a lot better than me saying, "All right. I super glued all 60 of my desktops. We're secure now."

Greg Hughes: Right, that's a good point.

Richard Campbell: So I think about protecting at the file level but actually stopping an email from opening?

Wes Miller: What it's actually doing is it's encrypting the content itself. It's all about the content and instead of trying to use permissions to control

access to it like you would traditionally, you know, Office for years has had generally unbreakable password protection for documents and the document wasn't literally encrypted with that. It was a password. Now you can think of IRM as an encryption layer on the document itself so if you don't have the key literally to unlock this document, the document is useless to you. In fact, if you open up an IRM protected office document, you can look at it like in Notepad, you can look at it, you can actually see that the document is formatted differently because it's encrypted and so the guy who gets to open it first is IRM, not literally in Word.

Greg Hughes: Windows Rights Management or Active Directory Rights Management as they call it now, are we able to do this at the file system level or are we talking just Office documents? Can we apply it to other types of documents, any file on a file system? Where are we at today?

Wes Miller: So where we're at today is actually Microsoft did a couple of really neat things. They've actually begun licensing the technology so I've seen a couple of vendors without naming names or some people who have extended this story above and beyond to other platforms, other document types, other scenarios that they're amazing and the neat thing is most of those interoperate with ADRMS although some them actually take it a step further and do some things on their own with their own management, but what you get into today with IRM in Office and RMS in Windows is you get the ability to protect what honestly is going to be the majority of your infrastructure content. You can go and you can protect all of your Office documents. My article actually is a link to a table of literally all the file types that you can protect this way now, but all of the Office document types and Outlook email so you can protect emails from themselves. You can't protect an email with as an attachment within another email. It's kind of a encrypted thing, but you can protect a ton of Office content this way and the neat thing is it's not system specific, that protection roams wherever the document roams since the document is encrypted itself. If it leaves your Office, it doesn't matter.

Greg Hughes: Sure. I can see examples where maybe I would want for anybody within my organization to be able to see it or forward it, maybe not forward it. Can we control at that level? I mean if someone sends an email but I don't want anybody to be able to forward it to anywhere except for maybe a very small group of people that I specifically allow to do that.

Wes Miller: So, there are a couple of neat things you can do. You can definitely do with an email you can say basically you got to do not forward. So, in order to open the content -- we'll take a step back for a second, in order to actually open the content, the person opening it has to authenticate and that usually means providing either Active Directory credentials or if you've extended it a little bit further, a Windows Live Passport that allows them to go through and do that same pass through authentication.

Richard Campbell: I'm sorry. Did you say passport?

Wes Miller: Yes I did.

Greg Hughes: Windows Live ID?

Wes Miller: Did I say Windows Live? Yeah, excuse me, I'm sorry. If you recall, I left in 2004. The branding has changed a little bit. Sorry, Windows Live ID.

Richard Campbell: There you go.

Greg Hughes: Right. So we're talking about federation, right?

Wes Miller: Yeah, you're definitely talking about federation and there is even some really cool across the name scenarios that are in ADRMS now. If you've got Dell and Microsoft exchanging documents, for example, those can actually stay encrypted and have RMS working across them.

Greg Hughes: So it will go across for us as well as across domains. Interesting.

Wes Miller: You can assign it on a user basis, on an OU basis, group basis, etc. It's pretty flexible. The key thing is there's not much of a learning curve for a viewer. You sort of think of it as most publishing metaphors. For the viewer, you've got to teach him how to put in credentials. The key and the double details is in the sender where they've got to sit there and say, "All right, now how broad do I want this to go; and do I want an expiration on it, either a terminal expiration or the content can be free after this period of time?" So that's another neat thing about RMS is it can actually if you got a press release you don't want to go public, you can have an expiration date that it literally kills the document regardless of who gets it, it dies on this day, or you can say, "You know, after that day I really don't care. Anybody could view it."

Greg Hughes: I think about protecting sensitive information or intellectual property. Office documents and emails are great and if you have to name names, I think that's okay but I mean I think about things like source code or files containing data, it could just be some kind of a text flat file or something that contains sensitive information. It

could be banking information. It could be anything. I always go back to that example because that's my experience, but you can apply it to a wide variety of compliance oriented information and controlling and monitoring and protecting access to that in a guaranteed way is a really difficult thing to do so I'm trying to figure out where are we today but also where can we go in the future and how can we do that, how can we better protect sensitive information? With a really high level of confidence from a technology standpoint to compliment our process requirements that we have from a security approach but technology wise, can we leverage this to do some of that?

Wes Miller: Sure, yeah. It's definitely something that's possible. I haven't looked into the specifics about pluggability but I know that the functionality exists that if an ISV wanted to come along with, say, like AutoCad and they wanted to Autodesk if they want to actually make AutoCad work within an IRM infrastructure, they can do that. It just takes work on their part and I guess sort of the traditional Microsoft story, if we build the infrastructure and then it's up to the ISVs to realize the value of adding it in. You know, IRM, Rights Management, as a whole is one of those things that you sort of have to explain if tech guys like us are in here talking about it and sometimes we all even scratch our heads when you actually go out to a company. Let's take In2It as an example when you're describing to them, "Well, you know, you really want to encrypt your content using this kind of thing because data at rest is only at rest for so long. When it starts flying over the wire, you're not really protecting it. So there is ability to plug into it. I'm not seeing many other ISVs do that piece of it which is really unfortunate but one company I actually get jazzed every time I talk to the guys from there, I met them for the first time at RSA this year at Liquid Machines and they've taken Microsoft's IRM to a whole other level and they protect the content while it's moving around so if you copy and paste from a protected document if you're allowed to, the new document inherits that protection, so some really rich scenarios.

Richard Campbell: Interesting.

Wes Miller: That's sort of I think the direction you'll see over the next couple of years as compliance collides violently with what I would refer to as true security and I had posted recently an article about how compliance and security aren't necessarily the same thing. I think we'll see this more over the next couple of years.

Richard Campbell: Yeah, if you go down that path, it's just sort of a recognition of -- compliance, we've done some shows specifically on compliance is really can you pass the audit.

Wes Miller: Absolutely.

Richard Campbell: That's a totally different can of worms per se.

Greg Hughes: That's one way of looking at it. Compliance and security are two different things. Compliance is do you need these thresholds? Is that what you're saying, Richard, I think as opposed to security which is more of a way of doing things and it's measured in similar ways but at the same time maybe has loftier goals and certainly brought her in more complete goals than specific compliance review.

Wes Miller: Right as I to say basically compliance doesn't generally beget security but security does begets compliance.

Richard Campbell: Right.

Greg Hughes: Right, right.

Richard Campbell: It clarifies motivation too, pretty much folks understand why we need to secure things, the fact that it happens to support compliance which more people question the value of.

Wes Miller: Exactly.

Greg Hughes: Quite often we see compliance requirements that are simply thrust upon organizations driving security initiatives though so it does go both ways but they are not one and the same.

Wes Miller: Absolutely. I guess if you got to sort of answer your question if you take a step back and you look at what IRM does, you think about the life of a knowledge worker during a typical day. You know probably 60% to 80% of the documents in a typical office, if not more, are going to be office documents so what Microsoft has gotten is a good initial stab and then you can look at other vendors. I honestly haven't seen another solution like IRM that takes it any further that protects other document types unfortunately, but you can look at local disk encryption to protect the content while it's at least at rest but then you sort of miss it if it flies off the system.

Greg Hughes: Yeah.

Richard Campbell: The trick here, I don't know if we've really delved into this, the implementation side of this thing is, if I'm able to because this is all Active Directory driven, I've got people assigned to groups and so forth so that's where their permission source comes from, it's their relationship in AD.

Wes Miller: Absolutely.

Greg Hughes: So we have permissions and then we have rights. Permissions being file systems permissions versus rights which is -- I guess I'm thinking I can have permission to get to where the file is but have the rights that are required in order to actually open and view it.

Wes Miller: Exactly and that's actually an important delineation that Microsoft put literally in the product by referring to it as Microsoft's Rights Management product and that's the exact idea that I've got. Everyone in my company may have access to the share but I may have an executive directory that only executives can get into or it just is importantly, you know, *Sarbox* type review. You may have one that's honestly only the CFO and her team or his team can get into and actually do their work so rights takes you one step further than permissions. The problem is if you have just permissions plus take that share metaphor and I have permissions on just an ACL on that share, just an ACL.

Greg Hughes: Right.

Wes Miller: But if I had an ACL on the chair or something comes loose because somebody sets a poor ACL, then that file which is sitting out there on its own and someone can either a compromise it intentionally or accidentally, you know, it goes both ways.

Greg Hughes: Yeah, accidentally it's pretty common.

Wes Miller: What RMS does, what rights management does is a whole concept to say, "Listen, I don't care where this content is. It's more than permissions. I want only these people, these principles, this OU or my people on my domain to ever actually see this content. It's that private and I want it to keep it private."

Greg Hughes: So, technically, talk about how this works. There is a server role. Is there a client that needs to be run?

Wes Miller: Yeah.

Greg Hughes: I guess in the real deep technical part of it does this require a certificate services or is there some kind of a PKI infrastructure that's going on in the background and how does it all work?

Wes Miller: Sure. So Microsoft, I have to, you know, kudos to the team. I recently needed to install this in order to get the whole, you know, I'm familiar enough with the back story about it but I want to get it on installs so I could do my article about it and honestly I installed this on my Windows Server 2008 box and it was one of the most pleasant experiences I think I ever had. It just went through, you told it I want to install ADRMS and it installed all of the subcomponents that it needed to and in the backend, you honestly probably don't want to know the dependency stack it installed but it's things like IIS, it's things like MSMQ is actually a critical part of this. It actually installs the message queuing service as well but the Wizard is phenomenal about doing all the configuration for you so I'm actually encouraging anybody out there who has thought of playing with it to do it because it's a ridiculously simple install to do, you can be up and running in a matter of minutes. Then there is a client piece as well. The client piece, obviously we're talking about a service ID who is in Active Directory as well. So you have to have a domain controller up and running for that work and to have one lying around. On the client side, there is a standalone client that goes back, if I recall correctly, goes back all the way to Windows '98 but they count support beginning with Windows 2000 all the way through Windows XP, actually Server 2003, excuse me. Beginning with Vista, the client actually integrated into the product so it's a native part of Windows Vista and Windows 2008. You don't even have to do a client install, you just have to say here's your arm as content and it begins to do initialization.

Greg Hughes: Got you.

Wes Miller: You could sort of say that there's a two-piece process to it because you've got the RMS client then on the Windows machine but you obviously need a copy of Office that has the actual IRM piece in it so since Office and Windows are two separate products, you've obviously got to have Office here to install it too and this is beginning with, if I recall correctly, Office 2003, it was the first version that offered it and it came forward into Office 2007 so it's in both of those versions. If you have one of those, it just works.

Greg Hughes: So what is the mechanism to actually identify if a user is using Windows digital certificates or how is that happening?

Wes Miller: It's traditional like if you're used to user manager style picker, it's not too far from that and again it's sort of a let's separate the experiences. You've got a producer of content and a consumer of content so let's take a step back and look at the guy or gal who is actually producing the content that they want to share but not to share too liberally. So what they do is they actually go in and they create the content they want, lay it out, set it out, get it ready to send off and they can just select the option to protect the content in Office itself. So the option is there and it will tell them if they don't have RMS installed on older versions of Windows and install it and actually

give them a URL to direct it to, great experience there too. Once they've done that, there's actually a dialogue which pops up which allows them to apply the appropriate protections that they want, things like again the expiration date, can people print this, there's the analog hole again, what kind of things can they do with it, and in there they can actually select the user's groups or use what that they want to apply to the content itself as far as protections.

Richard Campbell: Is there a mechanism to create policies for like minimum security requirements?

Wes Miller: Yeah, there is the ability within the RMS piece itself, you can actually create initial profiles and those are shared out so you can have a profile that applies to the RMS users and see if you can have a company, all company, you can have this subsidiary, only that kind of a thing, so you can so some pretty neat subdivisions within RMS itself and users get to take advantage of that.

Richard Campbell: I'm just thinking from the context of I mean it's one thing to have the rights to actually get in and access the document as well, but I'm also thinking about configuring the rights of what options document creators are allowed to set. It's like I'm sorry, under no circumstances can these things be copied. You have the choice to, you know, you can adjust who can read it and who can't.

Wes Miller: Yes, so Microsoft stuff is pretty much a Boolean unfortunately. It's been sort of a print or not, so you can view it or you cannot view it and you can set the option to print or not, but good machines has been neat and they took it one step further and do allow you more granular copy but keep protecting copy allow to break that kind of a thing but what they do have is within Microsoft, there's a couple of different classifications of author like creator/owner kind of a thing and then you have editors and then you have consumers. So the editor people can actually sit there and make some modifications to it but they still can't print the document.

Richard Campbell: Right. So you do have that.

Greg Hughes: I'm curious what the transaction looks like in the background. Obviously you have to authenticate the person who's doing the read or the view or the print and then something is happening behind the scenes...

Wes Miller: Yeah. If we talk about the consumer experience here, once I've produced that content and I had emailed it out, I could email it to everybody and only to the people I want to and I'll be able to actually consume it. The consumer side, what you get is you get Windows Live experience where basically are challenged for some credentials and you're asked to provide your authentication. You can basically say either I've got a Windows Live ID or I'm going to use my corporate ID, generally corporate being your preference because you're going to keep it all into internal league organization and that's generally how it will be set up.

Greg Hughes: If it's corporate, is it a pass through thing and all sort of trans-parent me or do I have to interact?

Wes Miller: As a user, you have to interact, you have to actually type in credentials, it's one of those classic, more like a basic authentications that happen in the background Kerberos authentication if you are still using Kerberos to do it instead of doing it a prompt which I've been doing automatically. You do have to have a prompt and you'll interact with it typing your regular domain credential and password and click okay and then the content literally just renders and so I'll sort of gloss over the transaction just because I'm not intimately familiar with all the pieces over the wire that are going on but basically those credentials, you can have an internet facing RMS as well so you can just be roaming and actually connect up if you're remote but generally this can be connecting up to the RMS server. It was told to authenticate to and that RMS server is going to do its own polling for Active Directory to find out if she's allowed and actually go to RMS and say, okay, they are, and then proxy that back. Generally, I'm relatively certain that's where MSMQ gets involved in the transaction. There's a lot of that communication back and forth to their client.

Greg Hughes: Sure. You just mentioned internet facing server, so I guess one question was so if I'm not on the corporate land and I can't talk to my, you know, I'm not talking directly to the main controller and whatnot, my pre-provisioned, already provisioned client knows to ask for a server by name that's accessible on the internet. Is that what's going on?

Wes Miller: Yeah, you're basically going to tell it this is the machine that the FQDN to connect to and it's going to go through that fully qualified domain name to say, "Here is my preferred RMS guy and okay, he knows me and we're good to go here." So, again, they've built a really good experience and it's really the default tolerant that you don't have some initial hangs setting it up, you know, hang-ups getting it set up but once it's actually up and running telling it which server to go to, then it's actually very robust.

Richard Campbell: I love the fact that this is, you know, as soon as I hear Active Directory, I think, "Okay, the network better be right. It's all internal. Branch offices need not apply." Then you start thinking about what happens if this doc actually gets

out in the wild, what authentications seems to be at work, but it looks like they've worked that stuff out.

Wes Miller: No, I think it they really did a good job. One of the ironic things is years ago when trains were first coming in the vogue in the United States, you know the story about they used to have it where the break system would stay open if it didn't have pressure holding it shut.

Richard Campbell: Right.

Wes Miller: You know, the other way around, and not it obviously clamped shut unless it's got a pressure applied to it so it stops the train that's a runaway instead of the other way. The beauty of the RMS stuff is that if it doesn't work and you're too far away, there is a chance that the content is going to stay protected like it should, but that said, you know, I actually had, like I said, a great experience setting it up and it works really well and I used it at Microsoft for several years before I left and its relatively robust.

Richard Campbell: And you bring up a valid point which is this isn't one of those classic Microsoft dog food moments. They have this problem. This is a tool they developed for themselves that now they've turned into a product and they've really beaten the snot out of it.

Wes Miller: Absolutely. If it weren't working, it wouldn't have worked within Microsoft but this is used extensively within Microsoft control content from getting out because there is just some information that's the kind of stuff you need to protect that way.

Richard Campbell: Absolutely.

Greg Hughes: Very, very cool.

Richard Campbell: I mean if you're an all Windows 2008 Vista shop, you've got this.

Wes Miller: Plug and play.

Richard Campbell: Then if you're lesser versions, lesser versions, it's just a download.

Greg Hughes: Previous versions, yes.

Richard Campbell: Right.

Wes Miller: In the spirit of a lot of the stuff that was done for Windows Server 2003 after the team shift in like 2002, there's a free download so if you're still running Server 2003, it's still gratis but you do have to install it after you've downloaded it from the internet and in the 2008 version, again, it's a little bit more full featured and you've just done a better job of integrating it overall so it's an easier setup, etc.

Richard Campbell: Yeah, it took me a second to find it on the Microsoft site, Windows Rights Management Services, it's in SP2. It's click and download, 64-bit and 32-bit clients, that's good. So they've definitely -- it looks like a mature set of software.

Wes Miller: It's been really neat learning about the internals of it because it's a very functional piece of software. You know, occasionally companies will come up with software that, gosh, I don't understand why I need that, but once you really start explaining the whole rights management problem to people and why you're not protecting it if you've got shares, you're not protecting it if you've permissions as we were talking about earlier.

Richard Campbell: Right.

Wes Miller: The key thing is it's about protecting the content itself.

Richard Campbell: Yeah and I like the fact that the file is encrypted. If you've used the software, it will be easy to decrypt but you don't have to, it's going to be tricky to circumvent. You could pound your way through the decryption by hand if you really, really want to; but good luck.

Wes Miller: Right.

Greg Hughes: That does help to solve one of the classic problems of Joe calls me because Joe doesn't have ACL permission access to a file and says, "Hey, can you grab that file for me and email it to me?" If there is a reason that Joe shouldn't have access to it, whatever that reason is then it certainly helps prevent that.

Wes Miller: Sure. It's actually kind of interesting too because while I was at RSA, one of the things that's attracting me to a couple of companies there in talking to them and realizing that we're on the same page was thinking about security from a proactive versus a reactive perspective and I saw a lot of companies out there who will attempt to help you find shares that aren't secure or attempt to do stateful email inspections so they'll look at every single email that goes over the wire and someone will try to look at IM traffic but that doesn't scale. It doesn't protect you and so you have to come up with something proactive and that's really what's neat about RMS is it's a proactive way to protect your content.

Greg Hughes: There's another whole other show we could have is proactive versus reactive

security and maybe we'll do that someday but that will definitely be a different conversation.

Richard Campbell: Gentlemen, I think we're about out of time.

Wes Miller: All right.

Richard Campbell: Another half-hour flies by. I didn't know that I wanted to know this much about Rights Management actually.

Greg Hughes: Very interesting. I'd be curious too, Richard, if any of our listeners are using or have used Windows Rights Management Services, drop us a line, info@runasradio.com. We'd like to hear your experiences and what you've used it for.

Richard Campbell: That's great. Wes, thanks so much for coming back on the show.

Wes Miller: Thank you so much for having me, guys. It's been a lot of fun.

Greg Hughes: Take care, Wes.

Richard Campbell: We'll bring you back next year. Actually, I think we should get into whitelisting so, you know, call back to the beginning of the show. I'll ping you in a couple of weeks and we'll put another show together.

Wes Miller: Wonderful.

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