



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 #030
(Transcription services provided by [PWOP Productions](#))



Brien Posey Secures Exchange!
October 31, 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 #30, with guest Brien Posey, recorded Thursday, October 11, 2007. RunAs Radio is produced each week by PWOP Productions, offering professional media and podcasting services online at pwop.com.

Richard Campbell: Hi there, welcome to RunAs Radio. I'm your host Richard Campbell. Here with me always, Greg Hughes.

Greg Hughes: Howdy everybody.

Richard Campbell: Hey, it's Halloween.

Greg Hughes: Yeah, it's kind of scary. You know, what's scary is how fast the year has gone by. It's just amazing.

Richard Campbell: Wow. We started back in April. This is show #30.

Greg Hughes: Yeah. Seriously, if I sit back and think, you know, 30 shows. I'm like, "Wow." It's just really pretty amazing.

Richard Campbell: I still feel like we've got so many topics to go. We're sitting on a goldmine here of things to discuss.

Greg Hughes: Oh yeah. There are so many ideas for shows and whatnot. You know, one of the things of course is we always want to hear the listeners, you know, what do you want to hear? If you have ideas or topics or you if you think maybe you're the person, let us know.

Richard Campbell: Yeah, by all means, info@runasradio.com. Send us a mail. Let us know what you're thinking and we're happy to make a show out of it one way or the other.

Greg Hughes: Yeah, that's a whole lot of fun. We enjoy it. We hope you're enjoying it too. We've got some pretty important stuff coming up in the next couple of weeks.

Richard Campbell: The live stuff. I love getting in front of an audience and doing the show in that context. We're going to get a couple of shows done at Dev Connections in Las Vegas next week.

Greg Hughes: Right, RunAs on the road.

Richard Campbell: Yeah, got to love it, and the week following that, IT forum, TechEd Europe, Barcelona.

Greg Hughes: Barcelona, Spain, yup. We'll be over there and doing quite a bit of the IT forum. I think it's going to be an awfully busy week for us, but it's going to be a lot of fun, looking forward to Speaker Idol among a bunch of other things.

Richard Campbell: You bet, and if you haven't already entered the contest over at our sister's show, dotnetrocks.com, they have a contest for Barcelona where you can answer questions about the show and win yourself a 24-inch LCD monitor. So, take a look over there at the Barcelona contest and we'll see you in Barcelona as well. I hope you're coming out, happy to talk to you, and so many things going on there. I can't keep track of them all.

Greg Hughes: If you're there, then please stop by and see us and say hi.

Richard Campbell: You bet. All right, Greg, let's introduce Brien. Brien Posey is a freelance technical writer who has received Microsoft's MVP award four times for his work with Windows Server, IIS, and Exchange. Over the last 12 years, Brien has published well over 4,000 technical articles and whitepapers, and has written or contributed to over 30 books. Prior to going freelance, Brien served as CIO for a nationwide chain of hospitals and healthcare facilities. He has also served as a network administrator for the Department of Defense at Fort Knox, and for some of the nation's largest insurance companies. You can visit Brien's personal Web site at: www.brienposey.com. Four thousand articles?

Greg Hughes: Wow.

Brien Posey: Yeah.

Richard Campbell: I thought I did -- I've done over 300. I thought I was prolific. How do you do 4000 articles?

Brien Posey: I don't know. It's just one of those things that really come easy to me. I try and crank out about two or three every day.

Richard Campbell: Wow, that's amazing.

Greg Hughes: You know, Brien, I've read your stuff over the last several years on MSD2D and just a variety of different locations and so it's really actually pretty cool to talk to you.

Brien Posey: Oh, thank you. But, you know, I'm no different than you guys. Just a geek. I just happen to write, that's all.



Brien Posey Secures Exchange!

October 31, 2007

Richard Campbell: I understand the concept of being a prolific writer. I think I hit my peak as a writer around 1997-1998 where I remember writing like two articles in a day, but it passed for me. I got over it. Apparently, you're still doing it.

Brien Posey: Yeah.

Greg Hughes: We all have our addictions I suppose.

Richard Campbell: Yeah, that's a ton of typing. Boy, oh, boy.

Greg Hughes: What about repetitive stress injuries? Have you ever had that kind of problem?

Brien Posey: Yeah, actually I have. I try to use Dragon Naturally Speaking as much as I can.

Richard Campbell: Really?

Brien Posey: Yeah. There are some articles that use a lot of acronyms or words that are spelled together that it kind of makes it hard to use it, but I'd say 70-75% of my articles I dictate instead of typing.

Richard Campbell: That's pretty cool too. Boy, that would be a whole show all by itself just somebody who actually uses the voice dictation system in a real way.

Brien Posey: Yeah, I tried it, gosh, I guess around 1996-1997. I think it was IBM's ViaVoice at the time and it just wasn't really up to the job and I forgot all about it for a long time and about a year ago, I started really having a lot of problems with arthritis in my hands and I knew I was going to have to do something, so I gave it another shot and lo and behold, it actually works.

Richard Campbell: Wow.

Greg Hughes: That's interesting.

Richard Campbell: Yeah, I guess that makes more sense now. I'm feeling better about it that you could put out -- you're not wearing your handset anymore.

Brien Posey: Yeah.

Richard Campbell: I have so many possible topics here, but I think we've sort of narrowed in on -- you've done a lot of work in the Exchange Space and so we're going to dig into sort of the security issues around Exchange. Do we need to talk about a particular version? Are they really different from version to version?

Brien Posey: Yeah, there are a lot of differences. I would say if you're going to pick one, probably the best choice would be 2003 because that seems to be what most people are still using.

Richard Campbell: Yeah, it seems 2007 adoption hasn't gone as quickly as Microsoft may have wanted.

Brien Posey: I don't want to do Microsoft bashing or anything.

Richard Campbell: Of course.

Brien Posey: And I don't believe in biting the hand that feeds me, but really I think that Microsoft rushed 2007 out the door too soon. I mean that's evidenced by the features that are going to show up in the first service pack that just weren't included in the initial release, things like tools for managing, public folders and stuff like that.

Greg Hughes: Sure.

Brien Posey: I think that is a big part of why it hasn't been more heavily adopted.

Richard Campbell: My first guess was that the 64-bit requirement might have been onerous for some folks.

Greg Hughes: That was going to be my point as well.

Brien Posey: Maybe, I don't know, but I mean pretty much all of the hardware that's being released anymore is all 64-bit.

Richard Campbell: That's true, yeah.

Brien Posey: I know it was kind of tricky to get drivers for a while but...

Greg Hughes: What's interesting though is -- I know I've heard a lot of people say that that 64-bit requirement is what stopped them because they don't even realize that the equipment they have can do it. They don't have a 64-bit operating system installed typically, but they could rectify that.

Richard Campbell: Yeah, they don't know the license for the OS. Maybe that's it. It's an interesting problem, but it's not what we're here to talk about today. I agree with you. Let's go with 2003, that's the server I'm care and feeding for the most. Actually, to be perfectly honest as we're being honest today; it's the one server that scares me the most.

Brien Posey: Really?



Richard Campbell: I mean I'm not afraid of SQL Server. I'd do anything with SQL Server. I'm not even afraid of Active Directory, but I fear Exchange.

Brien Posey: Why is that?

Richard Campbell: It's a complicated beast. I think the integration of the different pieces between AD and the mail store; I think the security model is very challenging. I have been bitten by the open relay, you know, I'll admit it. Once in my life I was in open relay. I got blocklisted and had to clean up the mess.

Greg Hughes: Yeah, that happened to me on a UNIX server. They were on a BSD server.

Richard Campbell: So, take us away, Brien. Tell us what the challenges are here.

Brien Posey: Oh gosh. Are we talking about security just in a broad sense?

Richard Campbell: Yeah or, you know, specific techniques. What do you do when you set up an Exchange Server? What are the right things to do?

Brien Posey: Well, the instant relay for one.

Richard Campbell: Yeah. Is it correct to answer just securing SMTP requiring people to authenticate SMTP?

Brien Posey: I think that's a big part of it. I mean really, I tend to think that -- I mean don't get me wrong. It's definitely important to secure Exchange, but I think that not nearly enough emphasis is put on securing the underlying infrastructure though because if Windows doesn't secure, then Exchange isn't going to be secure.

Richard Campbell: Right.

Greg Hughes: Right. You know what worries me the most about email security and so it directly impacts Exchange is it's not just the infrastructure but -- I mean email is inherently a fairly insecure medium and it's not just viruses and whatnot, but it's also what people put into emails. What kind of devices or what methods are they using to access Exchange? All of those things are pretty critical security questions.

Brien Posey: Yeah, you're absolutely right.

Richard Campbell: It makes me think we should -- I mean, can you really set those kinds of lines down and stuff like you must access Exchange through Outlook? Is that the right way? Then it gets into the whole thing of Outlook over HTTP or should I use a VPN. What are the right ways to connect to the stuff?

Greg Hughes: Or OWA and Outlook Web Access and Outlook Mobile Access and all of those different systems. What kinds of controls can an enterprise or can a company put around that kind of access?

Brien Posey: Well, for starters, you have the option of completely disabling them if you don't want to use it. I've known plenty of organizations that simply don't allow OMA to be used. Incidentally, OMA was completely dropped from Exchange 2007.

Richard Campbell: Wow. So, how do you do support for your Windows Mobile device in 2007?

Brien Posey: The primary method for using mobile devices with Exchange 2007 is just to use direct push.

Richard Campbell: Oh, okay. So, they just didn't need OMA anymore? This is a better way?

Brien Posey: Yeah. I actually talked to somebody at Microsoft a while back and I asked them why it had been dropped and their answer was that nobody uses it.

Richard Campbell: Interesting. I mean I'm not using it right now, but I think it's more just that my Exchange isn't set up properly for it, but I'm fascinated by the prospect of actually getting my BlackBerry-like effect without using a BlackBerry or BlackBerry's connector.

Greg Hughes: Now, Outlook Web Access or OWA, that's widely popular and pretty widely use.

Brien Posey: Yes.

Greg Hughes: What are some of the controls if you will or the security lockdowns that an organization can do on Outlook Web Access? I guess the question is what are some of the important things to be thinking about if you run Outlook Web Access in your environment and it's available on the internet?

Brien Posey: Well, Outlook Web Access if it's deployed correctly in all the service packs and all that are in place. That in and of itself is fairly secure. The biggest things to keep in mind are not to be dumb about deploying it and you don't want to put it in a place where it's sharing a server with some other application because you are exposing it to the Internet even though it should be behind a firewall and all that.

Richard Campbell: Right.

Brien Posey: You don't want to risk that box being compromised. My personal thoughts on OWA



is that by far the most important thing that you can do to make sure that's secure is to secure the machines that people are accessing OWA through the workstations.

Richard Campbell: So, you're thinking in terms of, of course, it's probably a laptop, right?

Brien Posey: A lot of times, but not always. There are plenty of people that get on their desktop machines at home and log in after hours.

Richard Campbell: Oh right. Yeah, of course.

Brien Posey: I think Microsoft is kind of starting to see this as being a big deal too because if you look at Windows Server 2008, the Network Access Protection feature...

Greg Hughes: Right.

Brien Posey: It's something they've been playing around with for years, but it's just now kind of finally become practical, but it's set up to where when somebody VPNs into the network, you know, there is no reason that something like this couldn't be applied to OWA even though OWA isn't traditionally accessed through a VPN. You can set it to where people have to have the latest service packs. They have to have up-to-date virus protection. Windows Firewall has to be on that sort of thing.

Richard Campbell: Yeah, you have to set policy on the client machine. We did a show on NAP which I'm really excited about the technology. I think it's wicked cool, but I figured if you've got a VPN connection to a network, you should be using the Outlook Client.

Brien Posey: Yeah, I agree.

Richard Campbell: Because you just got so much more of it and so much of a better -- I mean, don't get me wrong. OWA blows my mind. I think it's the single biggest cause of people building web apps today is that their CTO has OWA as well. This is web and it's great. You make an app that good.

Greg Hughes: Yeah, it was the pre-web 2.0, web 2.0.

Richard Campbell: Yeah, it's always been so far ahead of its time, but I'd still rather use Outlook if I had the choice.

Greg Hughes: Yeah. I guess more accurately you can say it was the pre-AJAX AJAX is really what it was.

Richard Campbell: Yeah, that's right because it had that whole effect going on. Do you feel you have

to have a VPN connection? Like if you're going to use a laptop out in the field, VPN is what you need to get connected to the network to get access to these resources properly and securely?

Brien Posey: That'd be my first choice, definitely. I don't want to turn around and say that no other method is secure because that's just not the case, but I think your chances are better using a VPN.

Greg Hughes: Yeah. I think there are certainly methods to lock down OWA if you want to, to jump in there and add on, so that only certain machines could actually gain access and do some checking, but it isn't built that way out of the box.

Brien Posey: Yeah, but again that kind of goes back to what I was saying earlier about securing the underlying infrastructure because those settings that you're mentioning, those are all in IIS.

Richard Campbell: So, am I going as far as putting client certs on all the laptops and only those machines can speak to that Web Server which is hosting OWA?

Brien Posey: Yeah, that is another way you could do it. When you said that initially, I was thinking about the settings in IIS where you can restrict a site to people with specific IP addresses or things like that.

Greg Hughes: Right.

Richard Campbell: Yeah, the only thing I'm going to run into is I'm the world's traveler here. I never know where I'm connecting on.

Greg Hughes: Yes, and having done the certificate authority, the internal certificate authority, and restricting access to those types of resources of certificates, I can say it does work. I think that is one viable way among several and I really like the network access protection, the future of that and the ability to maybe leverage a deeper set of capability and provide a more robust protection, maybe even in addition to the certificate-based restrictions that you can put in place for access to resources like that.

Brien Posey: Yeah. I still think that worth facing itself is probably a much bigger threat than what is thrown at the server. I mean how many machines out there that people are still using Windows 98, that's infested with all kinds of Trojans and things like that. None of these automated Trojans are probably going to turn around and launch an attack against an OWA Server and actually be able to break and instill things, but it's very common for those to steal information off of the PC that's infected, you know, so if somebody is accessing their email and sending and receiving sensitive



information, who knows where that information is going to get sent.

Richard Campbell: Yeah, because you've got control of that workstation, you're watching that data stream. I guess that sort of goes into, if you're going to use OWA you better be using SSL.

Brien Posey: Yes.

Greg Hughes: You know, one of the things that, you know, and it's been on my mind a lot lately because I broke down and bought one is like an iPhone, which allows me to do email and connect to different types of servers. I'm not using it for any corporate stuff of course, but I use it for personal mail, but there's a lot of companies out there despite warnings to the contrary that are allowing devices like this one and others access to corporate systems and there are really no controls around the devices themselves. Is there anything that an administrator can do on an Exchange machine to try to help beef that up with those handheld mobile devices?

Brien Posey: Well, Exchange 2003, when Service Pack 2 was released, there were a whole bunch of settings that were put in that allow you to enforce passwords on mobile devices and remotely wipe the device after a number of failed login attempts and things like that, but the problem is it doesn't work on every device, but there is a setting that you can enable that will allow you to prevent anybody who has a got device that won't accept those settings from connecting.

Richard Campbell: So, that's sort of the NAP for mobile devices.

Brien Posey: Yeah, kind of.

Greg Hughes: Interesting. So is that part of the 2003...?

Brien Posey: Service Pack 2.

Greg Hughes: Right, part of the OMA settings then?

Brien Posey: No, it is not really a part of OMA. It's just kind of part of Exchange as a whole.

Greg Hughes: Interesting.

Richard Campbell: Like you said, as of Service Pack 2, we've got that capability now to put those...

Brien Posey: Right.

Richard Campbell: It's just a policy restriction on client, right?

Brien Posey: Yeah, exactly.

Richard Campbell: Okay.

Brien Posey: Because OMA is nothing but a generic web application that provides access to the stores on the back-end.

Greg Hughes: Gotcha.

Richard Campbell: Yeah. Okay, now, I'm starting to understand why you think it's not a big deal that OMA has been dropped. We didn't drop support for mobile.

Brien Posey: No, not at all.

Richard Campbell: We just didn't need a separate service for it.

Brien Posey: Yeah. I mean, you know, what about you guys? Have you all ever used OMA?

Richard Campbell: No.

Brien Posey: I think I've played around with it once or twice in a lab environment, but I've never once seen it used in the real world.

Greg Hughes: Used it briefly for a little while when it first came out to play with it.

Richard Campbell: Yeah, I guess it was a solution to a problem that didn't exist.

Brien Posey: I think it was kind of ahead of its time. At the time that Microsoft released it, the idea was to be able to use it with a PDA that had a very unsophisticated web browser to access email, but the thing about it is at that time, there weren't really a lot of PDAs that were web enabled.

Richard Campbell: Right, and now once you have a PDA that's got a decent feature in it, it is running Windows Mobile and it has the full Outlook client on it.

Brien Posey: Exactly.

Richard Campbell: So it's just connected to Exchange as if it was Exchange. It was definitely a solution to a problem that didn't actually exist. When you talk about Firewall and Exchange, do you think NAP is the way to go, like literally doing address translation or is it just poor filtering? What is the right way, how hard can we lock down Exchange? Do you think the box should have a live IP?

Brien Posey: Interesting question. I tend to prefer to use NAP just the live IP to the net router and



use a private IP on the Exchange box and use port forwarding.

Richard Campbell: Right. My preference too, uses fewer IP addresses that way.

Greg Hughes: Right, I would agree to that.

Brien Posey: Yeah, that's true.

Greg Hughes: Maybe a side question to go along with that one is what about front and back-end servers and what's the real value in that and when should that be done?

Brien Posey: I think that if you're using OWA, a front and back-end is essential because you want to keep that front-end Outlook Web Access Server running only OWA, nothing else, and you don't want to run any risk of exposing your back-end servers to the web.

Richard Campbell: So now you are talking a DMZ architecture. The OWA server is in the DMZ, the mail server is behind inner firewall.

Brien Posey: That's one way of doing it. I would almost think it will be better thought to go ahead and place the OWA server in a DMZ but behind a corporate firewall or your perimeter firewall but then have a separate firewall that further isolates it from the back-end just as a precaution.

Richard Campbell: Oh, I see. Well, the big thing being port 80 is the hacked half.

Brien Posey: Oh, the universal pass support.

Richard Campbell: Yeah, the universal pass support, so I don't want port 80 opened on my mail server, so I have a separate server that's the OWA server and it's got the pass through port open and then it's speaking in a much more secure way to the mail server.

Greg Hughes: Well, if I'm doing it, I don't want port 80 open to that one either. I want 443 only.

Richard Campbell: Right, of course.

Greg Hughes: That's what I'm good for.

Richard Campbell: Ah, yes, Mr. Security.

Greg Hughes: Yeah, let's do SSL. I'll preach for five seconds, well, I already have, but I'll do it again which is if you are running OWA or you're running this on the Internet and you are not having SSL certificate over it, bad, bad for you. Fix that now.

Richard Campbell: You are asking for it and there is really no excuse. The certs are cheap. You just got to go do the homework.

Greg Hughes: Right and if you're doing RPC over HTTP instead of HTTPS, and this is where you can allow Outlook to remotely connect without using a VPN, but still use a secure connection with some of the controls that we've been discussing allow it to connect directly to the Exchange front-end server so you can use Outlook on the internet, then HTTPS is equally or even more important in that case.

Brien Posey: You know, earlier you made a statement that if you're using OWA, you better be using SSL which I would completely agree with. I don't think SSL by itself is enough to get the job done. That will stop somebody from snipping the wire and getting data; but it doesn't offer any protection if your machine's already infected with a key stroke logger.

Greg Hughes: Right, or if you're using weak passwords or if somebody attacks and tries to find some other way to get in, it's simply the transport, encrypting the transport.

Richard Campbell: And so to your point, Brien, just because you're using SSL, don't think you're secure?

Brien Posey: That's exactly it.

Richard Campbell: Are there things we should be doing in an optimal OWA config then?

Brien Posey: I still say that the absolute most important thing to do in a work configuration is to take ownership of the workstations that clients are using whenever possible and make sure that those machines are up-to-date and secure.

Richard Campbell: But in order to enforce that, which you're really talking about NAP, we've got to be using a VPN, the whole NAP negotiation happens over the network connection.

Brien Posey: And I realize that right now doing it that way isn't practical, but still one thing that you can do is -- I've always kind of had a philosophy that if a company doesn't own the machines that are being used, then there's really not a lot that you can secure them. So, go ahead, fork out the extra expense, get laptops for people who have legitimate good access while on the go and use things that are available to you right now like group policies to make sure that those machines are good and locked down. Make sure the virus definitions are up-to-date and that all the latest Windows updates are in place on those machines.



Richard Campbell: Right. All right, so if we're controlling the machine to that point, the workstation to that point, why would we ever use the OWA? Shouldn't we be just using RPC over HTTPS and let them use Outlook because we could control it.

Brien Posey: There certainly is an argument that could be made there.

Richard Campbell: Yeah.

Greg Hughes: There are probably arguments both ways. I think in the bandwidth constricted environment, you know, if you have somebody overseas over a connection that maybe it's not real reliable, that may be able to get a lot more done quicker with OWA, but the most cases you're right. I think with that RPC over HTTPS capability, that really solves the biggest chunk of the problem, doesn't it?

Brien Posey: Yeah, it does.

Richard Campbell: Although, again, you don't even need to do if you're going to get a VPN working properly.

Brien Posey: Another option that I've started seeing people do too is to just to completely forget about OWA and use terminal services instead.

Richard Campbell: Really?

Brien Posey: Yeah, I've seen two or three cases lately where companies have just gone ahead and implemented a Windows Terminal Server and run OWA on that and then the client just establishes an RDP session to the terminal server and then access the mail that way.

Richard Campbell: Wow. That is an interesting way to lock it down. I had not thought of that.

Brien Posey: Yeah, but I haven't studied it to know how effective it really is, but it is something that I'm starting to see.

Richard Campbell: Other than attachments, the ability -- in the end, all you needed to do is be able to see your email and respond, that's going to work. The only place I see it stumbling is if I need to get a Word doc onto my machine to work on it.

Brien Posey: Right.

Greg Hughes: I guess you can do the proxy copy, you know, you copy it to the desktop of the terminal services and then, you know, if you're RDP'd into that terminal server, you do have the ability to copy and paste it on your own machine.

Richard Campbell: Right.

Greg Hughes: So, it is possible, but it's probably a little kludgy. Sounds like there's really a lot of different options for different vectors for getting access to a lot of different interfaces, all of which have their own proper use and maybe are the best choice. So, really it's what are you going to choose and then whatever you choose, securing it is just really critical.

Richard Campbell: Let's keep dancing around VPN a bit here. I think I want to dig in to it a little. I have had messed around VPNs running on Windows Servers and I've never been widely happy with the results just in terms of network share behavior and so forth. Brien, what's your position on VPN end points? Is it best handled as a network device or is it okay to run it on the server directly?

Brien Posey: I've seen it run on the service directly and find that, again I tend to think that if you're going to do that, it's probably best to isolate that server in terms of not running anything else on it.

Richard Campbell: Right, you need a dedicated machine as an endpoint for VPN.

Brien Posey: Yeah, absolutely.

Richard Campbell: And if you're going to do that, why not make it a device, something a little simpler.

Brien Posey: Yeah, and easier to maintain.

Richard Campbell: Right.

Greg Hughes: And often a little more robust and flexible as well.

Brien Posey: Yeah, that's true. I mean anytime you got a device that is solely dedicated to a specific task and design from the get go to do that task, it's probably going to perform better than a server that was designed to do whatever and you just happen to custom-tailor it to act as a VPN endpoint.

Richard Campbell: There was a time when we simply admitted these were general purpose machines, right? From my point of view, I've always preferred dedicated hardware for dedicated tasks.

Greg Hughes: I know I've done a lot of work with Cisco's VPN concentrators and their software, VPN Client, that's the one that I found has been the most reliable in terms of giving good secure access, but also allow you to do literally everything that you need to be able to do as if you're on the network. Brien, what kind of VPN technologies have you played with and what's been your experience?



Brien Posey: As much as I hate to admit this, I work out of my house, so I really don't do a whole lot with VPN and my experience has just revolved around using Windows Remote Access Services and configuring that as a VPN.

Richard Campbell: So, your usual approach has been to run VPN services on the server and work with that?

Brien Posey: Yes.

Richard Campbell: It's true that the dedicated hardware for VPN gear can get really expensive when the seed count climbs. One to one is pretty easy in this -- the number of times I've bumped into people who were buying paired VPN connections for branch offices, two boxes, and all they're good at is talking to each other and nothing else. Very different from a product where I can have workstations connecting to it.

Greg Hughes: Doing remote endpoints that are in large numbers quite often.

Richard Campbell: Yeah, it gets more complicated than that. What haven't we dug into? Open relay? Yeah, Secure SMTP, that's all. Well, if the only way you can get connect to that Exchange server is through some kind of secure connection, you've solved the problem anyway, right?

Brien Posey: Yeah.

Richard Campbell: If you're opening port 25 to the world, well, you have your own problems.

Greg Hughes: And so does the rest of the world.

Richard Campbell: Why can't we fix the mail protocol?

Greg Hughes: Because once you've put something out there, it's there. That's just the way it is until something substantially better is there, there's no fixing to be done. Replacement is difficult, but how do you fix email?

Richard Campbell: Well, there are always mail certification services, right, where you have -- and every so often, I get a mail from someone who is a certified mail junkie and they've got their little symbol on their email that shows it's secure. That just never seems to have taken off.

Greg Hughes: Well, the problem with email is that it's an inherently insecure mechanism for getting things to you and so how do you know whether you can actually trust what you see in the email message?

It's one of those darned if you do, darned if you don't things, unfortunately.

Richard Campbell: Did you ever play with any of the secured mail service, Brien?

Brien Posey: No, I really haven't played with much of the secured mail services, but what you were talking about how do you know if you can trust somebody? I had a really interesting conversation with somebody at Cornell earlier this year. They were using a service where they send out large amounts of, I think it was newsletters or something like that they were sending out to subscribers, and they had basically registered themselves with some service basically saying, "Okay, we are who we claim to be. We're legit. We're not spamming people," and all that. I think one or two people ended up out of thousands and thousands flagging that as spam and all of a sudden, their reputation gets trashed and they're not allowed to send stuff out anymore without jumping through a bunch of hoops to get their name cleared back up.

Richard Campbell: You know, I think we're almost back into this topic, which is a terrible thing for an Exchange show, which is, is email dead. The reality of spam is such a huge problem that when you are sending at a legitimate newsletter to a group of people who have asked for it and they still report it as spam, because, really, they're overwhelmed. It's just too easy and then the spam reaction to the legitimate mailer is so severe that your ISP is being assaulted about it, all hell breaks loose, because a couple of people accidentally clicked the button saying, "Oh, that's spam." They may not even have meant it, but it's too late now. It just makes me wonder if mail is broken. You know, I'm going out -- Brien, you and I, just trying to get in contact with each other. I mean I'm a reader of your stuff and I wanted to bring you on to the show. It was very challenging for me to get a message to you to say, "Hey, would you come on the show?"

Brien Posey: Really?

Richard Campbell: And I think we ultimately connected through LinkedIn, didn't we?

Brien Posey: Ah, yeah.

Richard Campbell: So, email did not connect us together. We couldn't make that happen and it's this third party social web stuff like LinkedIn and Facebook that seems like it's replacing email. I'm having conversations with folks on Facebook now instead of an email.

Brien Posey: Hmm. I never thought about that, but you may have a point. I can run into some



more problems emailing people. What happens with me is I live out in the middle of nowhere in South Carolina and we've just got a local mom and pop ISP who has a total monopoly on phone Internet and cable and the thing about having a company like that is that some people apparently use some of their IP addresses to send spam and they used dynamic IP addresses which change every few hours, so that full range of addresses is blacklisted by a lot of anti-spam providers.

Richard Campbell: Right, and us as fairly technical people want to do things like run our own mail server, that's really difficult to do because these larger infrastructure companies are doing everything they can to try and mitigate spam to the point where your mail server just won't be able to send mail out, can't do it.

Brien Posey: Yeah, you're right. I used to own a company that send out newsletter on a periodic basis, and this was a few years ago, but Server 2003 was the current operating system at the time and actually ended up to be able to pull it off, I had to go back and install Windows 2000 Server and write a special web app that would interact with the component of that that was taken out of 2003 to be able to basically do a mail blast.

Richard Campbell: But still you get into this whole what's the protocol, how do I identify myself as not spam.

Brien Posey: True.

Richard Campbell: Yeah, I know, and it comes down to the individuals always have that power and yet they feel so powerless at the same time.

Greg Hughes: Might be a good point at which point out SPF records or Sender Policy Framework records for anybody who is running a mail server. If you are in the business and you haven't set one up, then you need to get on Google there and put in Sender Policy Framework and it's pretty simple to do, but pretty critical in terms of making sure that all email that you're sending is being received and validated.

Brien Posey: Yeah, that really seems like something that's been underutilized.

Greg Hughes: Yeah, I would agree.

Richard Campbell: Sender Policy Framework?

Brien Posey: Yeah.

Richard Campbell: Tell us about it Brien. Obviously, Greg knows, but I don't.

Brien Posey: Sender Policy Framework, basically, and Greg help me out here if I mess this up. It's been a while since I have done much with it, but the basic idea is that you can set up a special DNS record, so when you send out an email to somebody, it looks at the IP address that the mail came from and compares it with this record and make sure that the addresses match, so they can tell that a message bearing your domain name really did come from your mail server.

Richard Campbell: Right.

Greg Hughes: That's exactly what it is, sort of a DNS record, so for greghughes.net, for example, I can have a list of one or more IP addresses that are sort of white listed as allowed to send mail from or on behalf of greghughes.net. There are actually a lot of corporate systems out there that are checking SPF records to find out whether or not they should even accept email in the first place. Unfortunately, I don't think there's quite as many that actually have the SPF record set up to make sure that email is actually going to be able to reach its destination.

Richard Campbell: So, on their incoming side, they're checking it, but they're not using it on their outgoing side.

Greg Hughes: Well, they may not even know they're checking on the incoming side because some mail systems are doing that automatically for them without setting it up.

Brien Posey: Yeah, pretty much all of the anti-spam products out there now can at least be configured to check SPF records, but a lot of them do it automatically.

Richard Campbell: SPF isn't the be all, end all of anything. This is just making sure that the IP address that that email is coming from is actually the right IP address for that domain of mail.

Brien Posey: Exactly.

Richard Campbell: Okay, I get that. That's a good idea. You know, what's interesting here is it's a patch to a broken protocol, but that doesn't make it a bad idea, you know. If the protocol worked right, we wouldn't need this, but since the protocol doesn't work right, we have these other resources to try and find a way to resolve it.

Brien Posey: It's still not the be-all end-all because you can spoof an IP address.

Richard Campbell: Sure.



Greg Hughes: Absolutely. There is some good information about SPF on the internet. One location for that is openspf.org, which is the project there.

Richard Campbell: Of course, the moment you said Sender Policy Framework, and I went, "What the heck is that?" I googled it and ended up at Wikipedia, which seems to be the center of all knowledge anyway, but it has a pretty good entry on that too.

Brien Posey: Is it a reliable source?

Richard Campbell: It is a reliable source.

Greg Hughes: It is and it's not the same thing as the sunscreen.

Richard Campbell: No, it's a different SPF.

Greg Hughes: It's a different SPF.

Richard Campbell: Oh. Do we even want to tip over the can on spam some more? What do you use, Brien? How are you filtering spam? Is the Exchange Spam feature sufficient?

Brien Posey: I actually use that in conjunction with GFI's MailEssentials

Richard Campbell: Okay.

Greg Hughes: That's a good product.

Richard Campbell: I'm using Mail Route as well as the Bayesian stuff in Exchange and that seems to be helping.

Greg Hughes: You know, I have a lot of experience, really good experience with Mailfrontier Gateway, which was acquired a little while ago by a company called SonicWALL. It does a terrific job of catching spam as well, sort of at an enterprise level.

Richard Campbell: I have a domain I've owned since like 1990 and that thing gets hammered with millions of emails a month, literally millions. I use it as my spam test because there's only one valid email address in the whole domain and nobody knows it. Every time someone tells me they have a good spam solution, I said, "Okay. Take on this domain. See what you think." I think last month there were seven million emails sent to it and none of them deliverable.

Greg Hughes: You know, one other that's out there is called ASSP and it's free. It's open source type of thing, Anti-Spam-SMTP-Proxy, and that's at assp.sourceforge.net and I've used that on my own email server and I got to say that of all the stuff I've used, that's actually been the most accurate and a

great performing system as well, so that that project at assp.sourceforge.net is another good one to look at if somebody is interested in sort of getting their hands into it and really seeing the underpinnings of what it is that happens in a spam engine.

Brien Posey: Oh, I'll have to check that out.

Richard Campbell: Cool stuff. All right, gentlemen, it sounds like we're coming to about the end of our time. Any last words, Brien?

Brien Posey: No, just thanks for having me and I really enjoyed chatting with you all.

Richard Campbell: That's great. Where can we read your stuff? What's your main conduit of writing these days?

Brien Posey: You know, I'd love to give you one, but there really isn't one. It's scattered all over the place.

Richard Campbell: Google Brien Posey. You'll find him. I guarantee it.

Brien Posey: Exactly.

Greg Hughes: Brienposey.com.

Brien Posey: And that's Brien spelled with an E, B-R-I-E-N.

Richard Campbell: Right, B-R-I-E-N P-O-S-E-Y.

Greg Hughes: dot-com.

Richard Campbell: All right, thanks very much Brien.

Greg Hughes: Thanks Brien.

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