



<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 #031
(Transcription services provided by [PWOP Productions](#))



Randy Smith Helps Us Secure Vista!
November 7, 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 #31, with guest Randy Smith, recorded Thursday, October 18, 2007. RunAs Radio is produced each week by PWOP Productions, offering professional media and podcasting services online at pwop.com.

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

Greg Hughes: Hi everybody.

Richard Campbell: So here we are in Las Vegas.

Greg Hughes: *Lost Wages*, Nevada.

Richard Campbell: Yes. We're at DevConnections right now and through the magic of radio still coming to you with a show.

Greg Hughes: That's right.

Richard Campbell: Next week, Barcelona. So, lots of travel for us.

Greg Hughes: In fact, I'm flying on Friday. I believe the day has changed and things and I'll be getting there a day early, get settled in, and then I think we have a long week ahead of us?

Richard Campbell: Oh, we sure do.

Greg Hughes: But looking forward to it.

Richard Campbell: The 64-bit Question on Monday, Speaker Idol runs Tuesday, Wednesday, Thursday, as many panels and interviews as we could squeeze in.

Greg Hughes: Absolutely.

Richard Campbell: I really liked what we did at TechEd US with the shows and I want more, more, more.

Greg Hughes: It was a lot of fun and we really hope to see people there. If you in the audience are going to be in Barcelona at the IT Forum Week of TechEd Europe, please stop by and see us. Send us an email at info@runasradio.com. Let us know what you'd like to hear. Let us know if you're going to be there.

Richard Campbell: Hey, if you're in Las Vegas right now, come and see us, we're around.

Greg Hughes: Yeah, come say hi.

Richard Campbell: You bet.

Greg Hughes: In fact, I think this is released on Wednesday on our show. I'm sorry, our session is actually on Thursday.

Richard Campbell: Right, so you'll have a chance.

Greg Hughes: So, stop on by.

Richard Campbell: All right, Greg. Let's introduce Randy. Randy Franklin Smith runs UltimateWindowsSecurity.com web site and is an award-winning writer, consultant and trainer on Windows Security topics. Welcome Randy.

Randy Smith: Thank you.

Richard Campbell: So, I know UltimateWindowsSecurity.com just fine. It's a great place to sort of get summaries around security bulletins.

Randy Smith: Thank you. We try to update that the same day with Independent and pithy Analysis Bulletins, the same day they come out from Microsoft.

Richard Campbell: Yeah, your usual recommendation is patch *after* testing.

Randy Smith: Yeah that's true. However, that may be my usual recommendation, it may not be what I would like to recommend every time. I strongly believe that if you can avoid loading a patch for stability's sake, all the better. Oftentimes, if a company is doing a few basic best practices, you can eliminate the need to load a lot of those patches by just attack surface reduction and stuff like that and



that way you have what we like to call automatic immunity, autoimmunity, and less time and effort and resources spent on testing patches and deploying them and following up and all that stuff.

Greg Hughes: I know that in the online banking space where I've worked and actually running our systems all on Windows Server platform that patch testing is pretty important, but not all patches necessarily apply to that environment. To give an example and tell me if this is what you're alluding to, if you have a Windows Server that's running in a secured data center and you're not allowing outbound access to the internet by the web browser and not allowing it to run at all, then an Internet Explorer patch doesn't necessarily have to be applied in that environment.

Randy Smith: Yeah, exactly. In fact, that's why one of the columns on our chart is, I think we call it principal type of system impacted and we separate between servers as opposed to workstations/terminal servers and by terminal servers, we're referring to those terminal servers that deliver end user applications, but that's right. If you're refraining from browsing the internet or opening up files from the internet with Internet Explorer, there's a whole slew of patches that you can just avoid loading on your servers.

Richard Campbell: It strikes me that Microsoft really doesn't do this work. They want you to load everything. If you've got auto patching on, your machine is rebooted every Wednesday or at least you discovered every Wednesday, and everything has been loaded.

Randy Smith: Yeah. I think that's more of a consumer small business issue and for those folks, they probably are safest just going that route, but as you guys would imagine and priority appreciate, if you've got hundreds or thousands of computers, it's going to hurt you a lot more if you happen to load a patch that does cause a problem in your environment. It goes the same way. There are a bunch of patches, I mean fewer, but there's still a significant number of patches that really only apply to servers and there's no need to load them on workstations, but over the past year it's been mostly a workstation-centric list of patches that have come out.

Greg Hughes: Also interesting is that Microsoft provides for that corporate or that business environment that needs to exercise some control over patching and as much as I hesitate to focus on patching right upfront because that seems to be kind of the cliché of Microsoft security discussion, but we're talking about it, but they provide like the Windows Server Update Services, the tools that can be used to control the rollout of the patches and I guess put some standards and controls around that.

Randy Smith: Yeah. Giving credit where credit is due, Windows Server Update Services, the latest version of that, it does a really nice job of letting you divide computers up into different classes or groups and then roll out patches appropriate for each one of those.

Greg Hughes: So, if I had some kind of a farm of web servers that I wanted to treat differently than my workstations and differently than my database servers, then I guess I'm able to do that?

Randy Smith: Yeah, exactly. The other thing, while we're still on the subject of patches to look at is whether there are any what I call practical comprehensive workarounds and oftentimes for vulnerability there are and you can maybe just tweak a particular registry setting or something like that. I call it comprehensive because it plugs all of the probable vectors. For me to recommend it as practical, it has to be something that you can easily do through group policy or through a really simple script and you have to be careful because a lot of the workarounds that Microsoft offers are not practical, meaning there's something you have to do manually on every computer or they're not comprehensive, meaning they only plug one particular vector of infection or attack.

Richard Campbell: Changing gears a little bit. I know you've worked a lot on the area of locking down Vista, not to be cliché, let me just set you up here, I thought Vista was locked down?

Randy Smith: Well, it's got a lot of new security features, most of them I'm not real excited about. The one that I am excited about is BitLocker, it's the first time native to Windows you have the capability of fully encrypting your drive volume. To me, from a security point of view, that's pretty much the only big motivator in my mind. There are other



Microsoft Security MVPs and whatnot that might take issue with me on that but that's a big one there. It really solves the problem of stolen laptops. The other feature, stuff like user account control and the enhanced security configuration for protected mode of IE and whatnot is a step in the right direction, but especially like with user account control, that's the new feature that they refer to as least privilege. Well, that's another story in itself, but that's a semantic story. Anyway, user account control is the feature that allows you to run without full admin authority even if you are an administrator. So, even if you allow your end users to be admins, normally, under UAC, they're running without Admin authority and that way if they happen to execute some kind of malware that tries to do something that would require admin authority, you get that little dimmed out screen and the little sound effect and a console that says, "Hey, you've got a program that's trying to do such and such, do you want to allow that?" That sounds great on the surface because it protects the operating system, but I think this is a great illustration of how in information security we can kind of start concentrating on trees and lose sight of the forest.

Richard Campbell: Right.

Randy Smith: What we're really trying to prevent is business information from being compromised, right? Or business transactions from being compromised and the fact of the matter is you can do that without admin authority. If you've got somebody trying to look for credit card information on a computer and steal it and send it back, it can do that without admin authority. Malware, as long as it runs under the user's account can access any information or transaction that user has access to without triggering any admin level requirements.

Greg Hughes: Right.

Randy Smith: So, that's kind of my take there.

Greg Hughes: Yeah, it's interesting to talk about this. The title of our show is RunAs Radio, which is really touching on that least privileged user and the classic RunAs capability, RunAs admin or RunAs a more privileged user. Tell me what you think here. My experience so far has been that user account control is something that people are turning off, good, better or otherwise, I'll probably say unfortunately. Number two is that using the RunAs

capability, for example, in Windows XP, my experience is primarily in software development shops where running as admin the application that you're developing you don't want to run it as admin, but that is very difficult to do and to make it work well. That doesn't mean that it can't be done well. It means that it's difficult to do and that there are some impediments to making it cost-effective and affordable. I also don't think that's necessarily a good reason or excuse, but it's a fact. What's your experience in that and what are your opinions around that? I think that this is something that we've been talking about for years now and we still don't have a very solid story around.

Randy Smith: As I said, I think it's a step in the right direction. You don't want malware to be able to leverage admin authority whether you're running with admin authority or not, but it only plugs a few of the holes and it doesn't directly address what I'm most worried about, which is confidential information on that computer getting out.

Greg Hughes: Right.

Randy Smith: Hey, if user can't control work and was not intrusive and it didn't break things and for some environments it may very well be that way, I would say yes, definitely turn it on, you are safer with it. In my experience as a user and I'm not necessarily an example of how end users should be configured, it breaks too many things for me. Constantly, there's software that won't install while it's on and so on and so I was forced to turn it off. I kind of found the same way, I mean there are so many websites that do not work with Vista's IE 7's default configuration.

Greg Hughes: Sure, even software that won't install. Yeah.

Randy Smith: Yeah, yeah.

Richard Campbell: I think that UAC also has the problem that it's simply pops too much. People aren't reading it anymore. If you don't turn it off then you're just agreeing with anything it says. So, the effectiveness of the security is pretty much obviated. I think one other layer of this is that the average person who's got a UAC dialogue in front of them doesn't know the answer to yes or no.



Randy Smith: This is straight from the mouths of Microsoft researchers at a couple of years ago MVP event and that was when you give users a dialogue box, they will always select the option that allows them to move forward with whatever they're trying to do.

Richard Campbell: Right.

Greg Hughes: Right.

Randy Smith: So, again, we're getting back to one of the other complaints I have about a lot of workarounds in Microsoft Security Bulletins is that it leaves the decision in the hands of the end user and we all know what that is.

Richard Campbell: The choice is always going to be which one of these gets my work done.

Randy Smith: Exactly.

Richard Campbell: Damn any other consequences, I got to get my work done.

Randy Smith: I'm much more intrigued by some of the other technologies like white-listing. I think that sort of stuff ultimately is going to be a much more proactive and effective solution to malware than this reactive thing of "Hey, are you sure you want this to run?"

Greg Hughes: So, let's build on that. What do you mean by white-listing in that particular context?

Randy Smith: Yeah, I know. White-listing can mean different things in a different context. I'm referring to software, it's available from third parties right now, where instead of identifying "here's all the bad things that we don't want to happen," "here's all the bad programs and virus signatures and stuff like that that we don't want to execute or open," instead let's go completely from the other direction and say, "Here are the only good things that we want to happen and the only good programs we want to allow to run."

Richard Campbell: And so much more of a known list. I know what I'm supposed to be working on.

Randy Smith: I mean it's hard because you think you know that answer, but when you have an

enterprise of lots of users and occasionally, maybe you've got a user out there, a knowledge worker, that needs to install SnagIt and that sort of thing, you start running into issues there and support issues.

Richard Campbell: Right.

Greg Hughes: Right.

Randy Smith: But, yeah, it can be a manageable problem if you have the right technology and if you take the right approach and if you can overcome the end user political/expectation challenges.

Greg Hughes: That's a whole different conversation is that who really owns security and whose responsibility is it? I mean I think my position has always been that everyone's job is to be an information security employee, if you will, or a worker and that everybody have their own responsibility. It sounds like what you're saying is what we really need right now is user account control and you almost need that type of control and maybe an interface to do that, but a better way to do that maybe at the enterprise level or across the network level.

Randy Smith: That and just the overall idea of white-listing is pretty cool. In fact, in a conversation I had just a couple of days ago, a good size enterprise claimed that they were ready to pull out their antivirus software on their desktops because of the success of white-listing. They had a couple of insurance-related things that had to be addressed to make sure their insurance company recognized white-listing as an antivirus solution.

Greg Hughes: Sure. Well, then the idea of allow nothing by default and then only specifically allow that which I have already researched or approved is a pretty powerful way to control to put around the information resources to make sure that they're only doing what I want to allow them to do. It's really exactly the opposite of the classic, which is allow everything and then have to go in and block things after the fact. Isn't that really kind of one of the reasons that you know the RunAs approach hasn't worked very well? Everybody is already developing stuff. They're already admins. They're already building software. The systems are already setup. Now, you want me to change what I'm already doing?



Randy Smith: Yeah, exactly. I think that's a lot of it.

Richard Campbell: Another angle that I worry about when it comes to enterprise level machines is removable media, the floppies, the CD burners and the USB keys. When it comes to *infosec*, that just seems like a huge leak and I just can't seem to banish them from all my computers. Well, usually I don't want it, especially USB, I need it, but how do I stop the keys?

Greg Hughes: Yeah. I know organizations that have, it sounds funny, but literally they epoxy the USB ports on their desktops and they just plug them up with hard epoxy.

Richard Campbell: Just as an aside to give us some more fear, then they did this great psychology study where they dropped USB keys in parking lots and watched what happened to them and in like 80% of the cases people picked them up and stuck them in their machines.

Randy Smith: Well, I think that speaks to the growth in companies that make endpoint security solutions.

Greg Hughes: Well, there's a few out there that are pretty strong now.

Randy Smith: Yeah. In fact, one of them was pretty cool. You can go and get a free report. It's a utility. It's a loss-leader for their solution, but nevertheless it's pretty cool. You download it, you run it, it scans whatever workstations you specify, and it gives you back a report showing you all of the removable media devices that have been plugged into said computers.

Greg Hughes: So, why don't you go ahead and share the one that you were referring to in that case?

Randy Smith: That's GFI EndPointSecurity and I don't remember the name of the utility, but it's there prominently on their website and it was pretty revealing when I just ran it on my own network. I mean I recognized the devices that it came back with whether they were iPods or USB flash drives or whatever.

Richard Campbell: But the fact is, all this is logged so you can know basically after the fact what's happened.

Randy Smith: But you don't know what's being copied back and forth at least with native Windows functionality. Vista has some removable media controls there, but it's pretty rudimentary and basically helps you put it on the bullet list of marketing collateral, but I don't see it being a real solution except at companies that are actually willing to go the epoxy route, but only through software.

Richard Campbell: So, software-driven version of epoxy. I banish the USB ports.

Randy Smith: Yeah.

Richard Campbell: Can you block down the USB ports so just it won't run drives? Can you still plug a mouse into it?

Randy Smith: Yeah, you can do that. You're blocking out classes of devices.

Richard Campbell: Right.

Randy Smith: But there is still not enough granularity for what I think the typical company is going to have to face. "Well, my executives need to be able to plug in Blackberries. Oh, I have this one executive that has sufficient clout to not have a Blackberry, but to have a mobile Windows device or a Symbian device, all the things that happen in the real world.

Richard Campbell: Right.

Greg Hughes: Removable storage as a generic class is really where the difficulty is.

Randy Smith: Yeah.

Greg Hughes: Now, some of the companies, I think about Pointsec, for example, I think they were actually recently acquired by Pure Security, but they have some endpoint encryption software as do others as well as whole disk encryption and I know you mentioned whole disk encryption earlier as kind of solving the laptop theft problem. What's available on that? You talked about BitLocker but there are also some third party solutions out there. What do you



think the real value is there and what should people be thinking about?

Randy Smith: First and foremost, if you're going to encrypt the entire drive you need something that gets along well with the operating system and the reason I never got real enthused about third party stuff for XP is whenever I talk to any of my clients that used that sort of stuff, they complained about the speed and stability issues, which in fairness to Microsoft, I can say those are not present with BitLocker if you have a processor intended to run Vista why it's quite transparent to the user, but you have more flexibility with the third party solutions with regard to type of encryption key strength, but I don't think that is that important. The other flexibility that I think is a lot more important is what are your pre-boot authentication options? With BitLocker Vista, that's very limited to just two, either you have a TPM chip, Trusted Platform Module Chip on the motherboard of the laptop or workstation or if that's not present or if you don't want that option, then you have a USB flash drive that you have the encryption key stored on. With these other solutions, they can be smart cards, tokens, certificates. You've got lots more options with regard to that.

Greg Hughes: And often, BIOS integration for boot passwords which may or may not be tied into your Windows domain passwords is also possible. I know Pointsec does that, for example.

Randy Smith: Yeah, TPM itself is a good idea, the way that it takes measurements of all the hardware on the system and helps to detect anybody tampering with it and so on.

Richard Campbell: Sorry, *acronym police*, TPM.

Randy Smith: Trusted Platform Module.

Richard Campbell: Right.

Randy Smith: It does two things. It takes various measurements of the configuration of the PC and if those things change, it refuses to boot. It also has a secure storage similar to the tamper resistant storage of a smart card storing private keys or secret keys and that's ultimately where the key to encrypt the BitLocker drive is. Now, the other really bad decision that Microsoft made with BitLocker is they limited it as

a feature to the Enterprise Edition and the Ultimate Edition.

Richard Campbell: Right.

Greg Hughes: Yeah, I was actually very surprised about that.

Randy Smith: It blows my mind that they didn't put it in the Business Edition. What are they saying to small business people and where does that sit with the whole trusted computing initiative? To me, it's such a fundamental important security. How could you be in business and buy the Business Edition of Vista and not want that?

Greg Hughes: Yeah, it does boggle the mind. It really just doesn't make sense.

Richard Campbell: Well, here's to hoping they rethink that a bit as it moves further down. I mean they hit two important editions. The Enterprise Edition is the one that the big shops are using as part of their volume license agreement.

Greg Hughes: Right.

Richard Campbell: It almost seems like an afterthought in the Ultimate. While we put everything else in there, we'll put this in there too.

Greg Hughes: And Ultimate being everything that's in business plus a bunch of that other stuff, it's sort of the uber geek's version of Windows.

Richard Campbell: Yeah, I get Media Center as well as BitLocker.

Greg Hughes: Right.

Randy Smith: Yeah, I can encrypt my music, wow.

Greg Hughes: I run the 64-bit Ultimate on my machine and I like it because it does have all those things, but Windows without the option to use BitLocker for me I think would be pretty frustrating.

Randy Smith: Now, some of these solutions out there that you're referring to give you encryption not just the hard drive on the laptop, but also give you control over removable media and encryption of the



removable media also, all manageable through the same platform.

Greg Hughes: Right, and in some cases even port level control so that you can exercise new layers of control over what gets plugged in where and how it can be used.

Randy Smith: I think that's pretty compelling. The other that I think is compelling is USB flash drives with fingerprint readers on them. I was pretty jazzed about that for non-TPM-enabled laptops where you want to use BitLocker, but then you start worrying about the BitLocker key sitting on that USB flash drive probably stored despite your policy in the laptop bag along with the laptop, right?

Richard Campbell: Of course.

Randy Smith: It doesn't do you much good then. I was able to go out there and find a couple models that have a fingerprint reader built into them that don't require any special software and I thought that was a really nice solution, but one of the companies has since stopped selling and I haven't really been able to get much traction out of the other company with showing them this potential value-add out of their product.

Richard Campbell: It seems to me that fingerprint readers have really taken a beating over this whole idea that you can always lift a fingerprint off the laptop.

Randy Smith: Yeah.

Richard Campbell: I don't know that's necessarily true like it's not that easy to do and I think it's back to the old sufficient security model like putting the club on your car, it doesn't make your car impossible to steal, it just makes it harder to steal than the other guys. So, isn't this enough?

Randy Smith: Yeah. Well, that's the way I look at it. I mean my policy with my employees is, "You don't store the key with the laptop."

Richard Campbell: Yeah, don't store the key with the lock.

Randy Smith: Yeah, exactly. You put it around your neck or else you put it on your keychain

and we check that periodically. So, I have confidence with my employees that that hardly is ever going to happen, but when it does happen someday like it's left on the dresser in the hotel room along with the laptop over on the desk, at least we have some kind of compensating control.

Greg Hughes: The usability of all these different controls whether it's Smart Cards that you have to have with you, USB drives which has a whole slew of issues around, you know there's even things where you plug a little device that you have to have with you, that something I have type of factor into a microphone port or a soundcard port. I've really sort of liked the of multi-factor authentication for any computer, but the thumbprint or the fingerprint is something that I'm always going to have with me and if I combine that with something that I know, maybe it's a passphrase or some other piece of information that only I know and I require those two things in combination, that could create a pretty strong authentication mechanism including unlocking the encrypted drive. So, I don't just need the fingerprint that I could lift off the laptop as Richard alluded to as possibility, I think it's an unlikelihood, but it's a possibility, I would also have to know something in addition to that.

Randy Smith: Yeah, for the folks who are always pointing out the way to get around something and use that as an excuse for never doing anything, I refer to those people as security cynics and I like to point out and remind people in my classes, "We're in business to do business, not to be secure." When you look at these thefts of data that make the news, you have to ask yourself, "If we'd taken those steps, whole drive encryption, the key on the USB flash drive or something like that, would these data thefts from laptops have actually occurred? It might have been stolen, but would the data have been compromised?"

Richard Campbell: Right.

Greg Hughes: Right.

Richard Campbell: It's getting back to the reality of this whole situation. Since we're spending some good time on BitLocker and this whole concept of whole disk encryption, what about the backups? The drive is encrypted, but now I need backup, so when it fails I have some other way to get to it. Are they encrypted as well? How is that handled?



Randy Smith: Well, I think there are two issues there. One is the laptop hard drive backed up and most of the time it's not anyway, but I'll come back to that. The other backup issue is that the backup of the key. So, let's say the hard drive is not destroyed, it's still viable, but the key is lost through the flash drive is lost or whatever.

Richard Campbell: Right.

Randy Smith: Or the TPM chip goes bad. They did a nice job on that and that is you can flip the switch pretty easily in group policy that says, "Do not allow BitLocker to encrypt the drive until it first make sure that it has backed up the BitLocker key for that computer to a special property on that computer's object and Active Directory." So, then you'll always be able to get back to that key unless you happen to lose Active Directory along with your laptop.

Richard Campbell: Right, so there is a copy of the key in the Active Directory store of its home network.

Randy Smith: That's right and the permissions on the property are what you would expect in order to protect it. It is limited to domain admins being able to read it.

Richard Campbell: Right.

Randy Smith: Now, as far as backup of the data on the laptop, if you have any laptop backup solution in place at all, that's going to continue to function because BitLocker operates at a very low level and does not interfere with any software that's reading those files.

Greg Hughes: Right. So, if I have a service that's running on my laptop and backing up over the network, streaming information as it changes to a centralized backup authority of some kind, then that will still work because that service will still be able to read the drive.

Randy Smith: That's right.

Richard Campbell: and then it's up to you to secure the backups.

Randy Smith: Yup. I'll tell you what I think is a pretty elegant solution is the combination of

BitLocker and offline folders. It works pretty well. We just point everybody's My Documents folder to a share on the server, mark it as available for offline, and what that accomplishes for us is a backup of the data on their laptop whenever they connect to the network.

Richard Campbell: Yeah, that's the way I run my laptop as well. There's always a central store of everything and anything you write into that machine is going to get synched up there. You don't even think about it. The moment you're plugged in, you're backed up.

Randy Smith: That's right. "Laptop stolen? I got BitLocker." You can keep going.

Richard Campbell: The machine is secure and the data is already here, so we just set up another machine.

Randy Smith: Yup.

Richard Campbell: Randy, I hate to tell you this, but a half-hour has gone by already.

Randy Smith: Oh well, we got all kinds of things we can talk about next time.

Richard Campbell: You bet. I'm glad we got a chance to drill into this angle of BitLocker and securing Vista effectively because it's certainly something that people need to think about. Not everybody has moved to Vista yet oddly enough, but there are definitely some distinctive features that we can take advantage of when we do.

Randy Smith: It was a pleasure talking to you both.

Greg Hughes: It was good to speak to you and hope to talk to you again sometime soon.

Randy Smith: Okay.

Richard Campbell: We'll see you next week on RunAs Radio.