UAC in Depth

Description: Steve and Leo wrap up their quest to get Windows Wi-Fi to 'Maintain Full Radio Silence' by adding one additional important tweak to Windows settings. Then they discuss the detailed security implications, now and in the future, of Vista's new and powerful user account control (UAC) system.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-083.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-083-lq.mp3

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

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

This is Security Now! with Steve Gibson, Episode 83 for March 15, 2007: Vista's UAC.

Security Now! is brought to you by Astaro, makers of the Astaro Security Gateway, on the web at www.astaro.com. And by Nerds On Site. Looking to grow your IT service business? Find out how Nerds On Site can help. Visit Iwanttobeanerd.com.

Time for Security Now!, our favorite security podcast. Well, frankly, my only security podcast. But it's still my favorite. And my favorite security guru is here, that's for sure, and that's Mr. Steve Gibson from GRC.com. Hi, Steve.

Steve Gibson: Hey, Leo, great to be back with you.

Leo: We are, of course, going to talk about something new in a moment. Actually I'm very excited about this, the user access control, the UAC feature in Vista, and whether it really does protect you. But before we get to that, do you have anything from previous episodes you'd like to...

Steve: Believe or not, yes. We've basically snuck in an entire show on maintaining full radio silence on Windows Wi-Fi.

Leo: Well, it started when we were talking about this Free Public Wi-Fi that pops up on Windows from time to time, and what it was, and how now Microsoft has offered a fix but

never told anybody about it, and you have to explicitly download it. That's what we talked about last week. And if you didn't hear last week's episode, you should absolutely download that update.

Steve: Right. So that was our second mention. Then the week before, Episode 81, we talked about – we actually showed the dialogues required to turn off the functionality, just sort of this promiscuous connect-to-anything-that-I-hear, and also this idea of broadcasting the names of any networks you had connected to before, which by default Windows tries to do. It turns out that it's trying to do that still, even after you've got the update, because Microsoft added a checkbox to one of the configuration dialogues which is checked by default, and you have to go turn it off. So here in our fourth serialized How to Get Wi-Fi Just to Shut Up, we have additional instructions. People can, if they go to the show notes for this Episode 83, I've got a link back to the new and enhanced instructions that are over now on Episode 81's notes. So Episode 81's show notes are enhanced with this additional information, and this episode links back to those.

Leo: So this is if you installed the patch that Microsoft offered in November to fix wireless zero config, it's still promiscuous unless you uncheck this box.

Steve: Yes. There's a box which enables it to connect to networks which are not broadcasting. And so if the networks are not broadcasting, then your computer does. And it's just like, okay...

Leo: Is this ad hoc only? Or is it infrastructure networks, as well?

Steve: It's both. And so anyway, the idea is – in fact, I realized, okay, I started using the term "maintaining full radio silence."

Leo: Yeah, that's a good way to talk about it, yeah.

Steve: As the famous jargon. And that's what we want. We want to be able to carry a laptop around. If we forget to disable our Wi-Fi, we don't want it sending out stuff of any sort. We want full radio silence. And so it turns out that following the instructions that are now on the show notes for 81, with the update which we talked about in 82, which we're all pulling together now in 83, when we first opened the topic in 80, we basically snuck in a whole Security Now! episode on maintaining full radio silence for...

Leo: I should just take those chunks and edit them together, and we'd have Episode 84 ready to go.

Steve: And then the other news is, we had a second Tuesday of the month with no major Windows security updates.

Leo: Wow. Now, that doesn't mean there were no major Windows security flaws, we've learned. And often Microsoft will just say, well, a patch isn't ready, or we're not going to elect to ship it out. As I remember, I saw that in fact there were several critical flaws in XP, at least, that Microsoft wasn't ready to patch yet. So those flaws are still there. Presumably it'll be patched next Tuesday. But I don't think anybody has said there are any flaws in

Vista. And that's actually very encouraging news.

Steve: Well, and I don't think they'll be patched next Tuesday because – oh, you meant...

Leo: Next month.

Steve: ...next Patch Tuesday, right.

Leo: Yeah, Microsoft's doing it the second Tuesday of every month now. Unless there's something really serious going on, and sometimes they'll do a quick patch.

Steve: And of course several times, I guess it was last year, we saw them do that, where they would catch up. They said, okay, this will not wait for our standard monthly cycle. We've got to get this done now.

Leo: Well, I have to say, and we're going to talk about it today, a little bit about Windows Vista security. But I am encouraged. Vista's been out now officially for more than a month, almost a couple of months, and I haven't seen any major exploits. Of course people have been attacking the Windows authentication. But I don't care about that so much.

Steve: Well, in fact, I think it was on one of your other podcasts you were talking about – or it might have been Diggnation. Anyway, so one of these podcasts I heard mention that there was now a tool that would generate valid keys for installing Vista, and that it was possible that somebody else could come along with a correct key which Microsoft would say, oh, I'm afraid that's already been used. You can't use that key.

Leo: Yeah. I'll update you on that. We were talking about that on Windows Weekly.

Steve: You and Paul, yeah.

Leo: It turns out that was a scam, bogus. It was phony. And the people who claimed to have actual keys generated by this thing were either lying – and the guy who wrote it admitted it. He said, you know what, 25 characters, a mix of alpha and numeric, too big for any brute-force key cracker to solve. So I lied to you. However, that doesn't mean that the hacks don't continue. There's now a BIOS hack to disable authentication. So the hackers go on trying to crack into Windows Vista. And everything I've heard about this latest one is that it does, in fact, work. And it doesn't have that really – somebody pointed out that this key cracker, if it had worked, wouldn't be stealing from Microsoft, it would be stealing from other users because you'd be coming up with a serial number that these other users might in fact legitimately have.

Steve: Right.

Leo: Anyway, that's where the hacking seems to be going on. But so far I haven't heard –

I don't know, have you? – of any exploits against Vista, which is very encouraging.

Steve: Well, okay, yes. It's encouraging. But it's also predictable. For example, we know that so many problems we had with Windows 2000, well, certainly 95, 98, Windows 2000, I don't even want to talk about ME, and even XP were due to the fact that Microsoft just seemed so slow about getting a clue about how to make a Windows system safe on the 'Net. All you have to do is have a firewall. And as we know, XP had it, but it was disabled by default. Finally, with Service Pack 2, they turned it on. It's funny, I'm seeing this pattern, and I'm recognizing, though, what the pattern means. The pattern is a means for sort of slowly but surely creeping forward with good security.

Leo: Hallelujah.

Steve: Yes. And this actually feeds directly into today's topic because I spent a lot of time researching something that I promised that we would talk about because I knew there was a lot there, and that's the UAC, the user account control. Because it's more than just the annoying dialogue that pops up. There's a ton of stuff going on back there. And when I look at what Microsoft had to do to implement the solutions they have, I can understand why Vista took so long. Even though they threw out all the other goodies that they were promising to have in so-called "Longhorn," which was the backroom codename for a long time, there's really a lot there.

But, for example, Vista of course maintains XP Service Pack 2's default enabling of the firewall. Well, that means that you don't have this problem of open ports that we've always had until, well, a router would be in front. That would be a solution. But obviously lots of people several years ago during all of the worms on the 'Net, they didn't yet have home routers. And in fact, I don't know at the time whether we were yet promoting the idea of a router as an affirmative hardware security measure. I think still then we were talking about software firewalls. So certainly people who added software firewalls to their system or made sure XP's disabled-by-default firewall was enabled, they were much more secure.

Well, finally we got that built in with Service Pack 2. And essentially that whole set of problems is resolved now. That's just not going to be a problem. But what's interesting to me is that this is sort of the trend that we see with Microsoft, where new, better technology is put in, but it's not enabled initially, sort of because they want to warn everyone, this is coming.

Leo: Right. They don't want to break everything, but they do want to implement it. So they give you a little heads□up.

Steve: And a perfect example, we've talked of course extensively about hardware DEP, data execution prevention, that I'm so bullish about, which now exists both in XP and being given a lot more attention in Vista. What I've seen as I've looked at it more is, for example, a very popular image-viewing program called IrfanView, it turns out it won't run with DEP turned on. It's because it uses an EXE packer, an executable compression program called ASPack. And it makes sense that it wouldn't because naturally an executable compressor has got to decompress the executable, so it allocates a bunch of data memory into which it decompresses the compressed executable, and then it runs it. Well, it's running a data allocation, which is exactly what DEP is designed to stop. On the other hand, UPX, which is actually the leading and most popular EXE compressor, it's DEP-compatible because those guys realized, hey, when we allocate this memory, we should mark the pages as executable. In which case, DEP has no problem with it. So that's a great example of how a program might stumble over DEP, but how it's also possible to do the same thing in a DEP-friendly fashion.

Leo: Now, why doesn't a hacker just mark his pages executable and avoid the problem himself?

Steve: Well, because he's got to be running in order to mark them.

Leo: So he can't run the code until he can run the code.

Steve: Exactly. Exactly. So it's the perfect example. And in fact we see this a lot. For example, when Vista pops up the user account control screen, the whole screen darkens, and you get this highlighted dialogue that you have to say Continue or Cancel on in order to allow this permission or not. Well, it's been noted that malware could fake that screen in order to get users to type in administrative credentials. And so from that standpoint it sort of represents an Achilles heel of user account control because with user account control you're constantly, if you're not running as an admin user, you're constantly having to type in your admin credentials to prove that you have admin rights that are just you're not flexing those muscles right now, which raises the exposure of those credentials. But then the counterpoint to that is, well, yes, but malware has to be running in your system in order to allow it to spoof user account control. And what user account control prevents is the inadvertent installation of malware in the first place.

Leo: Hey, before we get too far into the discussion of user account control, because I'm very interested in this, should we pause for a station break?

Steve: Sure.

Leo: And we'll get back to it in just a second. But I do want to mention our sponsors since we are talking about security. Astaro Security Gateway's Version 7 has come out. And, man, what a major update. I mean, a lot of neat new features you're going to take a look at. Of course you know the Astaro Security Gateway is a device that runs software that gives you a complete solution, soup to nuts, for security. I mean, everything from VPN to hacking intrusion detection. You get email security, antivirus, antispyware, you get web filtering, you get spam protection, all of that in an easy-to-use device; and all, of course, the network protection stuff that you'd expect. But now with Version 7 there's some new features – a centralized email encryption strategy, which means you get email encryption and decryption at the device instead of at the desktop, so your users, it's completely transparent for them. A great way to implement S/MIME or OpenPGP standards. It now has SSL on VPN, yay. Scaleable via clustering so you can get as many as ten Astaro Security Gateways working together to really give you, without load balancing, to really give you some powerful growth capabilities.

And this is the thing for home users that I'm very excited about. In the past you've always offered the Astaro Security Gateway software so you could put it on your own beige box machine. It's an open source distribution. And in the past, what they've done is they've charged you 79 euros, and you'd have a subscription to all the other features – the web filtering, the spam, the updates for the antivirus and the antispyware. Well, they've waived that subscription fee if you're ten users or ten IP addresses and up to a thousand concurrent connections. So for home users it's now completely free for all of the goodies Astaro can offer. This is really a great deal.

If you want to know more about Astaro, visit their website, Astaro.com, or call 877-4AS-

TARO, and they'll schedule a free trial of an Astaro Security Gateway in your business. We thank Astaro for their support of Security Now!.

So some people complain sometimes about that user account control screen, the fact that it's a separate screen. For instance, I notice some programs don't work. I use a program called Synergy that allows me to share my mouse and keyboard over the network. And it's befuddled by that screen. I guess that's also to defeat some hacking.

Steve: Yes. In fact, it's much more going on there than meets the eye. Let me finish with sort of the concept that I was...

Leo: I'm sorry, I didn't mean to interrupt you.

Steve: No, it's fine. Irfan of IrfanView fame is now under tremendous pressure to get IrfanView to be compatible with DEP. So even though it's disabled by default, some early adopters, like all the people we're preaching to, are turning DEP on. They're discovering IrfanView is incompatible. They're sending him support email saying, hey, this doesn't work.

Leo: Something he could fix easily, I'm sure.

Steve: And it's funny because I saw – someone forwarded me his response. And I'm not sure what his native language is, but it was pretty clear it's not English. And he was like, what's going on? All of a sudden everyone's complaining about this. And I'm thinking, well, can you say Security Now! and the importance of turning on hardware DEP?

So this is an exactly analogous thing to certainly what happened back in the early days of software firewalls. Early adopters who were security conscious turned this on. And they were the people who were aware enough to understand sort of the UI complexity and sort of the downside of being an early adopter. They put pressure on anything that was incompatible to get it fixed. So essentially the way was paved for Microsoft then to come along later and do a firewall built into Windows that would just be able to be turned on.

So similarly, here Microsoft has DEP. And thanks to us bringing it to attention, and of course with Vista's increased security, there is now pressure on developers of applications which are not DEP-friendly to fix that. So what I can absolutely foresee is that some point in the future DEP will be enabled by default. But it won't be until all of the early adopters have put pressure on applications and sort of moved incompatibility from more of the, well, yeah, that's another problem so it's not worth turning DEP on, we've essentially moved it to where DEP-incompatible or unfriendly programs are enough in the minority that it's sort of more their fault for being un-DEP-friendly rather than expected.

And as we talk here about user account control, there's all kinds of aspects of what Microsoft has done in Vista which, as I have explored it, I've come to the conclusion that, slow as Microsoft is – glacial, in fact – in moving, it's very clear to me with Vista that they really got it. I mean, the light finally lit up and said security is the big deal. We have got to resolve this. And this was essentially Jim Allchin's final gift to Microsoft. He was there for 17 years, and he resigned the moment Vista went out the door. He said, I am done. Because he was the head of this project with a long, deep career in networking and understanding this stuff.

And what we end up with is essentially a system which throughout the system it's putting pressure on developers. It's doing it gently, just as the existence of DEP does, sort of in the

background. But there is pressure nonetheless. A perfect example is what you were just saying about how people are upset or complaining about this UAC, the user account control permission dialogue popping up so much. It turns out that an application developer can completely control that so that it isn't popping up when it's not necessary. But by default, unless you mark your application as UAC-aware, then Microsoft falls back to the default behavior of essentially popping it up too much because your application hasn't provided the granularity which is available in Windows.

A perfect example is my little SecurAble app that I wrote a couple months ago. I made it Vista-compatible by specifically appending what's called an "application manifest" to the executable to declare that this thing needs administrative privileges. Because, as we'll remember, I am installing explicitly, briefly I'm installing a kernel driver in order to access the chipset's hardware directly in order to get underneath any disabling that the BIOS or Windows may have done. I want to actually see what the hardware is telling me. The only way to do that is from ring 0 in the kernel. So SecurAble announced right upfront, hey, I'm going to need admin privileges. So anyone attempting to run SecurAble in Vista is immediately presented with this UAC dialogue.

Well, it would be possible, and Microsoft provides complete documentation, for making that more granular so that, for example, you could run SecurAble, and if there were more to it, basically you run SecurAble and it simply shows you the results, so there was no UI process to go through, which is why I have that dialogue, the user account control dialogue presented right upfront. But, for example, it's very possible for a more complex application not to show you that dialogue until you actually do something that will, in that user interface event, will need those kind of privileges. A perfect example is setting the clock. If you look under Vista at just the standard old clock setting dialogue, the button that you have to push to change the time has a little shield on it. That shield over time will come to be associated in users' minds with, oh, this is user account control. So Microsoft has designed an icon which can be attached to buttons, just to sort of show users, if you push this, we're going to ask you. And so it creates a little bit of sort of interactivity, even pre-pushing interactivity, because the user can adopt the expectation that they're going to be asked for credentials if they're logged in as an admin user.

So the idea is that all of these things, they put pressure on the developers. Your application can be more friendly if you do the following things. Well, in the process it is substantially more secure also. And so what'll happen is, this behavior will end up over time pervading applications which become Vista-aware. And so this whole notion of needing admin privileges will be diminished.

The other thing is that, because now even people running as admin users are being prompted to confirm, again, the application experience is the motivation that developers have to minimize their use of admin privileges. It turns out Microsoft's analysis of many applications showed them that most apps really don't even need admin privileges. It's just they were inexpertly, or I should say casually, written so that, well, you know, what the heck. I'm running as an admin. We know most users run as an admin. So we won't pay much attention to that.

Well, thanks to Vista not even running admins as admins, which I'll talk about in a second, it turns out that all applications which were sort of assuming admin privilege even when they didn't need it, they're now popping up these dialogues which can be easily prevented just by having the developer pay more attention to whether admin privileges are really necessary or not. And just that simple, this little bit of pressure is going to end up changing the experience. It's going to make applications more friendly under Vista by essentially never showing this user account control dialogue because there was a little pressure on the application writers to do the right thing.

Leo: So by default the application, if the application writer doesn't do anything, opts for the highest level of security, just assumes that you have no access to do anything.

Steve: Well, yes. And Microsoft recognizes that there are apps, old apps, for example, that are no longer being maintained. Companies have gone out of business. You still want to be able to run those securely. So if the application doesn't identify itself as being Vista-aware, then Microsoft defaults to the behavior we're seeing from most existing applications at Vista launch time, which is this is a lot in your face...

Leo: It's not too bad. I have to say it isn't too bad. I think, though, that really it does respond to a problem that I've seen in both XP and Windows 2000 of applications not running at all if you're not an admin.

Steve: Yes. And in fact that was what SecurAble was doing. When I was first running SecurAble, it was failing silently. And I thought, wait a minute, that's not good. So it didn't have admin privileges. And rather than asking for them, I was performing some calls. What Microsoft has done is a little bit of a problem because they are silently failing some low-level calls without letting the application know that this thing it tried to do didn't work. I guess they're trying to be a little bit tricky or clever in order to prevent malware from knowing that something it wanted to do hasn't happened.

There are many layers to this. They've got something called UIPI, the user interface privilege isolation, which is another new thing in Vista. We've never had it before. It's, again, really a long time in coming, but will do a lot to enhance desktop security. The idea is that they've added a new abstraction for applications called "integrity levels." You can have low, medium, high, or system integrity. And many things that go on in terms of the system communication depend upon the level of integrity. For example, a lower integrity process cannot validate a window handle, which is something that goes on in the API of a process with higher integrity. You cannot send it a message or post a message to a process with a higher integrity level. There are other things that hackers often do known as attaching a thread or a journal hook to an application, and injecting DLLs is a common means for sticking one of your own DLLs into a privileged application and getting it to run there. All these things were fundamental, I mean, long-standing, fundamental, serious security problems in Windows.

So Microsoft is sort of inching forward. They couldn't turn that stuff off because it would break too many things. So they said okay, let's create a new abstraction, this notion of how much we trust applications. And so, for example, Internet Explorer runs at the lowest level of integrity, as does email applications, because they're communicating, and they're more potential vectors for trouble. So those programs have absolutely no need to be reaching out and touching other applications on the desktop. But by default Windows was designed, for example a macro recorder could attach to another process and send it keystrokes. That's how macro recorders and macro playback operates is you're able to sort of send messages to a program as if you were the user typing things or clicking the mouse. Well, malware is able to do that also in order to cause obviously malicious things to happen. So this longstanding behavior, again, Microsoft is slowly tightening the screws on this saying, wait a minute, for things that we don't trust as much, we're going to limit their ability to access other programs.

Well, now, this will break some things. Microsoft is unable, as we've seen, for example, with the kernel patch protection, they're unable to simply shut down all kernel modification in 32-bit Windows as they have for 64. So they're saying, look, we're going to be really resistant to this kind of behavior and sort of try to moderate how much they push back. But what's very clear as you look at what Microsoft has done throughout Windows Vista is there is finally some real pushback from the OS onto applications, saying, look, it's time for us all to clean up our act. It's time for us to start behaving ourselves. And you can read the handwriting on the wall that this is going to be increasingly enforced over time until eventually, Leo, I can say, I can foresee the time when Windows ends up being the most secure operating system around.

Leo: What I'm really hearing you say actually explains a lot. People like Chris Pirillo who have decided to go back, they don't want to use Vista, they're going back to XP because so much stuff doesn't work, what they're really running up against is what we've always said all along. It's a tradeoff, security for convenience and security for compatibility. And in a way it's encouraging to me that Vista is not compatible with some of these applications. It can't be if it wants to be secure.

Steve: Well, yes. And in fact we also hear – I did a lot of research. I've heard, in fact, even our friend Joanna Rutkowska, who created the Blue Pill system, she's poked around at UAC some. And she commented that initially, well, first of all, one of her main systems she's using all the time is Vista. She's moved over to it. And she was seeing that she was getting the UAC pop up a lot initially, and that it quieted down. It stopped being a problem. And so I think it's clear that it's also a function of what kind of user you are. Certainly Chris is a power user. He's installing things all the time. He's experimenting with stuff. He's a different profile than your typical, buy a new Dell laptop at Circuit City and basically take it home and plug it in and don't do anything with it because it's got all the stuff in it already that you need.

Leo: Well, and that's what I've been saying. If you're getting a new computer, and you don't have legacy hardware and software, absolutely go with Vista. And if you're not, if you're upgrading, you might want to wait just because of these compatibility issues.

Steve: Well, again, for myself, I'm happy at XP. And I also saw...

Leo: Well, you were happy at 2000 until about a month ago.

Steve: That's true.

Leo: In fact, you still run 2000, don't you.

Steve: In fact, I'm sitting in front of 2000. I was a little annoyed that Microsoft chose not to update the time zone change during our recent daylight savings time shift. Windows 2000 is still under their critical care, whatever the heck they call it, where major security things get fixed, but non-important things don't get fixed. Which they could have easily done, but I think it's some pressure from Microsoft to say, okay, they're not telling me to move forward, but they're telling the industry it's time to start moving away from Windows 2000.

Leo: Although there's no technical reason. All that daylight savings time update is simply changing a setting for when summertime begins. There's no need to vet that or test it. It's just push it out. So it's very blatantly, if you ask me, commercial pressure to upgrade, for no good technical reasons.

Steve: I think that's clearly what was going on. But again, just to make sure I made myself clear, I could see Chris backing away from Vista and essentially allowing other people to get the arrows in their backs and essentially solve these problems. It makes sense to wait for applications to mature for the Vista environment.

As I really came to understand, as I looked at what was going on here, I realized, you know, these are deep changes. When we talked about the incompatibility you experience with remote

control of the secure desktop, it is explicitly the case that the secure desktop, even though it sort of just looks like the desktop got dim and a dialogue was allowed to run, sort of like in the foreground, what's actually happening is that desktop bitmap is copied, and the desktop is switched to a secure environment where nothing but system code is able to have any contact with that desktop. So application code, which is normally what you have running, for example, keystroke macro recorders and playback and so forth, that are using Windows hooks in order to control applications remotely, and certain keyboard and mouse remoting, those things lose – they have no connection to this secure desktop. And the reason Microsoft did this is they wanted to prevent obviously malware from clicking Continue before the user is able to click Cancel if this has been presented by malware trying to install itself. So it really is a substantial change.

Now, Joanna, in examining this user account control stuff, she spotted something which really annoyed her, which was in order for Microsoft not to break installers, they've done this bizarre stuff, Leo. Literally, if you run any program that contains the word "install" or "setup" or "update" in the filename, Vista looks at the filename, the executable filename. And if it has "install" or "setup" or "update" or many other things, like specific vendors or company names, product names, keywords in the executable, specific strings in the environment, any of these things will trigger Vista to decide you're running an installer which should have admin privileges.

Leo: Now, it's funny because I don't expect a hacker to put the word "setup," "update," "install" into their software, or even name it such. Do you?

Steve: Well, again, it's a perfect door for a trojan to basically trick somebody into running a trojan program.

Leo: Oh, you make it look like a standard installer, of course, yeah.

Steve: Exactly. And essentially, for anything that looks like an installer, Vista completely drops its guard. And Joanna's complaint was anything with those words in the name, for example, can install drivers in the kernel. And so it's like, well, okay, but that's what a setup program may need to do. It may need to legitimately install drivers in the kernel. And so I guess Microsoft's response again is, well, wait a minute, we asked you if you wanted to run this program. So we've prevented it from happening behind your back, and that's the whole point, is we're going to prompt you to make sure this is what you want to do.

And again, it's Microsoft fighting the need to not break old things while waiting for them to catch up. For example, once all the installers and installer systems around have been caught up, Microsoft can quietly back off on this sort of flaky heuristic approach to solving the problems of the past and, again, putting more pressure on these things to update in order for those programs to identify themselves as installers that explicitly need admin privileges in order to run. So essentially I'm very impressed with what Microsoft has done. Even, you know, we've also commented how even users who do run Vista as an admin, your typical I-don't-need-no-stinking-limited-account guys, even they...

Leo: And that's the default, by the way, it encourages you to make a user account, but it doesn't require it.

Steve: Actually the way it works by default, Leo, is the first account you create is one of these sort of limited admin accounts. Successive accounts are user accounts.

Leo: Right, users, right.

Steve: By default. So...

Leo: And most people just create one account, though, that's my point. And that account will be an admin account.

Steve: Yes, it will. Now, what's interesting, though, is at log-on, two separate tokens, two separate privilege tokens are actually created by the operating system. It creates a privileged user, but it also creates what they call a filtered standard user. And that's what everything you do runs under.

Leo: So you really aren't running as an admin, even if you're running as an admin.

Steve: Yes, that is what's so cool. And it's one of the things that I didn't understand is that you absolutely are not running with admin privileges. Even when you log on as an administrator, you get this filtered, limited, standard user token. And that's the privilege under which Explorer.exe, not Internet Explorer, Explorer.exe, the main desktop shell, which is the parent process for everything else you do, that is running as a standard user. And it's called a filtered token because what happens is Windows is watching for things asking this token for heightened privileges. And so the more privileged admin token, the real admin token, does still exist. And that's what Windows will switch to if you satisfy it by saying, yes, I want to proceed with installing whatever it is you're doing. But by default, even an admin user under Vista is running as a standard user.

Leo: Do you know of any attempts to hack UAC to get around it? It sounds like UAC provides a very good barrier. But of course, with any barrier, it might be possible to just ignore it to get around it.

Steve: Well, and certainly that is the attack surface that we can imagine hackers will be going after.

Leo: They're not going to go straight in. They're going to have to go around.

Steve: Exactly. One of the things that I have seen as I've looked at what Microsoft has done is that all the things that all of us have known have always been wrong with Windows, they have fixed. This notion of the too easy inter-application communications, well, they've created this integrity level concept to mitigate that threat and to prevent DLL injection. While still not breaking it completely, they've made it less accessible. And certainly data execution prevention, and the address space layout randomization, ASLR, to make things load in unknown, uncertain locations to prevent hackers from being able to jump to code at known fixed locations in the system.

I mean, basically they've sat back, and they've looked at everything wrong. And with Windows Vista they said, okay, we can't just lock down on this because things will break. But we're going to make it very clear that we are in the process of locking down on these things. Which is why I'm so encouraged. I mean, as you know, I've been very rough on Microsoft historically about their lack of care and lack of concern. I was pulling my hair out with raw sockets, and for so

long they kept running with no firewall enabled and active exploitable services, open ports exposed to the Internet. Those things are fixed.

What Vista represents is a major psychological mindset change about where Windows is going. I'm not surprised that Chris Pirillo has backed off from it because it's so new. What he's feeling is he's feeling that pressure. I expect that three or four years from now it'll be a much – when I'm ready to move to it, it'll be a much better experience because that pressure will have rippled backwards through the application community; and application providers, wanting their stuff just to work seamlessly, they will have fixed things to be Vista-compatible. And in the meantime I'm happy with XP.

Leo: Now, let me ask a question, because a couple of podcasts ago you were worried about Vista's virgin stack, that completely rewritten stack that at least in beta was making some mistakes that had been fixed in earlier versions of Windows. Any evidence that the stack is providing a weakness?

Steve: Well, it's not providing a static weakness, by which I mean because of the firewall in front of it there's no access to it. There is still the problem that, once you've got a connection opened, there could be some packet-level connectivity problems. But we haven't heard of anything yet. I wouldn't be surprised if we end up with some funky way that a malicious server could send you bad packets. The problem is, they couldn't be unsolicited. They have to be solicited. And so that's a much lower attack surface than what we saw before, for example, with UNIX, with no firewall running by default and just all these services running in the very early days of the UNIX stack, where all these exploits and mistakes were first being made. So Microsoft, even though they've got this unproven stack, which worries me, it's much less easy to get access to it from the outside.

Leo: Well, I have to say I'm excited. And I've been very happy running Vista both in emulation on my Mac and on at least one of my PCs. I can't run it on another one because Adobe Audition does not work with Vista, and it doesn't seem to have any timeline when it will. Somebody told me that...

Steve: Well, and you know, Leo, it totally makes sense, too. Because as we know, Vista completely revamps the whole audio subsystem in order to add DRM.

Leo: I'm sure it's a major thing to rewrite. And it's based on old code, Cool Edit Pro. So I have a feeling that maybe, in fact, some have indicated that perhaps Adobe won't even do an Audition for Vista, but just start a whole new application like Soundbooth from scratch.

We do want to thank right now our great friends at Nerds On Site who are celebrating, I'm sad to say, their last episode with Security Now!. If you are a nerd, they need nerds to service their customers. Visit Iwanttobeanerd.com. Nerds On Site are looking for nerds with all competencies and skills from PC and Mac experts to specialties like Siskel – not Siskel, Cisco, Siskel's a movie reviewer – and Oracle. Actually I think I combined Cisco and Oracle to make one thing. You name it, they need it. Fix-it technicians, web designers, programmers, project managers, even you could be a sales nerd, a trainer, a security expert like Steve. Antivirus gurus, the list goes on.

They especially love nerds who like to troubleshoot, tear apart, and rebuild their own systems in their spare time. Nerds are independent contractors. You're in business for yourself, but not by yourself. And that's what's so cool about Nerds On Site. You could focus on your passion and not the burdens of running a business. All over the world, seven

countries, 256 different competencies and that University of Nerdology. Visit Iwanttobeanerd.com and register for a nerds-only meeting in your area today. Great people. We really are glad that they stopped off and spent some time with us on Security Now!. We wish them all the best in the future. Iwanttobeanerd.com.

Boy, I have a feeling Microsoft is going to want to publish this podcast on their website. If you go to GRC.com, Microsoft, you get a transcript. You can also – everybody can do that. A 16KB version for the bandwidth-impaired. I know Bill Gates doesn't yet have broadband, so maybe you want to go to GRC.com. That's also where Steve stores all his great security programs like the new SecurAble, DCOMbobulator, UnPlug n' Pray, and of course ShieldsUP. Have you crossed 50 million users yet?

Steve: No, but we're approaching that. That's going to be a big event.

Leo: We'll do a party, yeah. GRC.com. And of course that's where SpinRite lives, too, everybody's favorite, my favorite disk recovery and maintenance utility. If you've got a hard drive, you need SpinRite at GRC.com. Next week it's question-and-answer time.

Steve: We'll do a dozen of our listeners' questions and answers. And to answer the question that they ask, how to send that, you go to GRC.com/securitynow. That brings up our main and growing Security Now! page. Scroll all the way to the bottom, and there's a web form. Just fill it out. You can put a name and tell us whereabouts you're calling from, click the Send button to post it to me, I'll receive it, and we'll get to it.

Leo: Next week. Thank you, Steve.