SECURITY NOW!

Transcript of Episode #197

Windows 7 Security

Description: This week, Steve and Leo discuss the changes, additions and enhancements Microsoft has made to the security of their forthcoming release of Windows 7.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-197.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-197-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 197 for May 21, 2009: Windows 7 Security. This show is brought to you by listeners like you and your contributions. We couldn't do it without you. Thanks so much.

It's time for Security Now!, the show that covers all things secure and insecure. We actually cover insecurity more than security. Privacy, too. Steve Gibson is here. He is the guru of security and privacy, the man who discovered spyware, coined the term, wrote the first antispyware program. He's also famous for [SpinRite], still the world's best disk maintenance utility. And he is here every week talking about security issues, answering questions. Hey, Steve.

Steve Gibson: Insecurity issues.

Leo: It really is.

Steve: You're right. Security is boring. It's the insecurity that's exciting.

Leo: Yes.

Steve: And trying to get there from here, or here from there. Or somewhere.

Leo: So this week, what insecurity will we be discussing?

Steve: The source of the world's greatest lack of security, Windows.

Leo: Oh.

Steve: We're going to talk about Windows 7 security, what they have done since Vista in their now more than half-hearted attempt, I mean, I think they're wholly hearted, to get Windows security cranked up. They're basically still trying to recover from years of really not giving a damn. And now that they do, they've got all these legacy problems. And so they're continuing to move forward. We're going to talk about the things in Windows 7 that Microsoft has deliberately continued to work on since the big changes that they made in Vista.

Leo: I'm really liking 7, and I'm hoping - my sense is it's more secure. But I'm hoping that you will give it at least a qualified thumbs up.

Steve: The short version is: Yes.

Leo: Oh, whew. But we'll get the long version in a moment. I want - we want details. Yeah, I want details.

Steve: That's why we have listeners.

Leo: Also I'm sure we have some news and errata from the world of security. So what's new in the world of security?

Steve: Well, the good news is it's been a surprisingly quiet week. Only one thing happened that is of potentially substantial note. It is of course with Microsoft. And that is that they've been informed of a defect in IIS, their main web server system, in the WebDAV protocol. WebDAV is the technology that essentially uses HTTP to connect to and allow directories to be viewed and modified remotely. So, for example, it's a way, for example, that people could edit the pages on remote servers. The traditional way has been to use FTP, File Transfer Protocol, where you'd work on a page, and then you'd FTP it up to the server in order to make it go live. WebDAV, for example, is what Jungle Disk uses. It uses that protocol in order to create folders on your local system that are actually files remotely located at Amazon in their S3 service. So it's a useful and sort of increasingly popular protocol.

Well, Microsoft, it turns out, has a Unicode parsing problem in their password handling for their WebDAV adjunct component to IIS, both 5.0, 5.1, and 6.0. So that's a problem. There aren't - they don't know yet of any exploits to it. But potentially this allows any WebDAV services that are exposed to be exploited. And it's not good. So I would imagine they'll have this fixed for the June patch because it's potentially really bad. I wanted to let any of our listeners know who do have WebDAV running, since it's running over the same port, that is, it runs over port 80, you can't just close the port. What you have to do is shut down that service and not use it. And that's Microsoft's recommended workaround for this. I mean, this is bad. So I just wanted to make sure that our listeners who are using IIS, if we have any, who also have the WebDAV component actively used, since it's available to anyone who has access to your web server, a mistake in its password processing is bad. And so this is.

Leo: I saw that Ball State University actually fell prey to this on Monday.

Steve: Ooh, already.

Leo: And so it's, yeah, it's out there.

Steve: Okay.

Leo: It says - this is from the Register. Hackers have wasted no time targeting a gaping hole in Microsoft's IIS server, according to administrators at Ball State University, who say that servers that use the program were breached on Monday. So as of this morning web accounts at Muncie, Indiana-based university remain inaccessible. And the service isn't expected to be restored till tomorrow or the next day, so...

Steve: Yeah. In fact, I think it was Monday that this was announced because I knew - I've known about it for a couple days, and I've been waiting for this podcast to update our listeners. So, yeah, people jumped on it immediately.

Leo: You know, there's one that also is breaking this morning. You probably didn't see it. But according to SecureMac they issued a critical warning for an unpatched Java security vulnerability in OS X on the Macintosh, including - remember we talked last week about that half-gigabyte update.

Steve: Oh, the mega patch, yeah, 13,000 files updated?

Leo: Even in the mega-patched Macs, the vulnerability could be used to perform something they call a "drive-by download," the ability to infect a computer by visiting a web page. The flaw allows malicious code to run commands with the permission of the current user. So you have to say yes, apparently. But Landon Fuller, who discovered this, is a little upset. He says, you know, they've known this exploit has been around, and they didn't patch it. So he released - he said, I've got to release code just to prove that it exists.

Steve: Yup. It'll get fixed now.

Leo: It'll get fixed now. He says the workaround is to disable the use of Java applets in your web browsers.

Steve: Imagine that.

Leo: Yeah, and turn off Open - this is something that Apple does called "open safe files after downloading." And I wish they'd put "safe" in big old quotes.

Steve: Believed safe.

Leo: Yeah, because this was a problem before with I think dashboard items just opening and running and installing, you know, presuming that they're safe. And really that should be turned off on the Mac. It's a convenience, but it's a bad idea. So something to be aware of. And since we're going to cover Windows security, I didn't want anybody to think that we were biased.

Steve: Especially you, Leo. No one would think that you were a Mac fan boy.

Leo: Not now, because I'm telling the truth. I want everybody to know.

Steve: Well, I have two other little blurbs of errata. I discovered the other day, searching for a solution, another little add-on for Firefox. I know from talking to a lot of the people in our newsgroups that many of them use Windows large fonts. Just because their screens are high resolution, the fonts end up being too small. When I'm at Starbucks I'm using this tablet, and the tablet has a lot of resolution relative to the screen size. It's a 1400x1050...

Leo: Oh, it's big. How big is the screen?

Steve: It's a 12.1 diagonal screen.

Leo: Oh, that small. So you really have little dot pitch there.

Steve: Yes. And what I was noticing is I was - I've got old person eyes now. So even though I've got my left contact lens is focused for reading close, and my right one is focused for distance, so that I'm not having to do the whole reading glasses thing, even so, I was noticing that lots of websites and even Microsoft's MSDN help file stuff is really small. Well, so I thought, gee, you know, is there, like, some way to, in Firefox, to change the font size? Well, first of all, Ctrl+ and Ctrl-, that zooms a site in and out. And it zooms the text and leaves everything else the same, which is very nice. And Firefox even remembers, I notice, what your zoom settings were per site. So when you go back to something where you've been before, it's the size you left it, which is...

Leo: I use that all the time.

Steve: ...very nice. What's missing from Firefox 3 is a default zoom factor, which would be very nice. I've put in about:config to bring up the private config page. And I got a little prompt saying, are you sure you want to go there? This is, like, for people who know what they're doing. Wind up your propeller. And I said, yes, I'm sure. And I think it had an option not to be harassed with this extra little intercept every time. And then I put in z-o-o-m. And I found, like, five entries under the about:config that were about zooming. And like there was, like, what - it had a list of zoom factors, minimum and maximum, some cool things, but no default. It's like, why not give me a default entry which would default to, like, 1.0, meaning 100 percent, and then I could change it. But no. So it turns out, naturally, there's an add-on. It's called NoSquint.

Leo: Not NoScript, NoSquint.

Steve: Exactly.

Leo: I love it.

Steve: It's NoSquint. No S-q-u-i-n-t. So I wanted to share that with our users, our listeners, who are also maybe 40-plus age and who are finding themselves squinting. What this does...

Leo: So it still zooms, but it jumps to, like, a zoom that you like.

Steve: Well, it does even more. You are able - it's got both this notion of zooming the whole page versus zooming the text...

Leo: See, I like that. Safari does that. And for, well, for TV, for what we do, it's great because the pictures get bigger, too..

Steve: Right.

Leo: So you don't lose formatting. You just kind of are zooming in.

Steve: Right. So you have independent control of those two factors. And what Firefox 3 doesn't offer is a default.

Leo: Right.

Steve: So I set mine to 130, to 130 percent. And so now it's just the size I want. So I wanted to notify users I found - our listeners that I found something else that's cool, NoSquint for Firefox 3.

Leo: Now, do you still do Ctrl+ or...

Steve: I haven't had to.

Leo: Oh, it just does every page 130.

Steve: Yes.

Leo: Ah.

Steve: Although then it will also do the per-site exceptions. And so it's able to memorize anything that you do aside from that.

Leo: That looks great.

Steve: So it's just, you know, for me it's just what I want. And I thought, hey, cool, I'm going to share that with people. The other thing, there was a - I've had a huge, tremendously positive reaction to the little KatMouse utility. That's the thing that allows your mouse's scroll wheel to scroll whatever you're over, even without having to click on it to make it the active window. And, I mean, an amazing amount of mail came back saying, my goodness, I really like this. Well, I wanted to tell people about a mouse which works really well with this. And actually it's the whole family of Logitech mice that have - and I don't know how they do this - a virtually zero friction mouse wheel.

Leo: Ooooh.

Steve: So that you can spin this wheel...

Leo: Oh, yeah.

Steve: ...with your finger.

Leo: Yeah, I think it has, like, a clutch; right?

Steve: Well, it's got two modes. When you push it in, it goes into, like, the traditional kind of click-click-click-click detent mode. But if you push it again it, like, toggles back and forth. It puts it in this zero friction mode. I mean, this thing really spins. So that now you're able just to kind of give it a flick and, like, literally zoom, I mean, like, scroll all the way to the top or all the way to the bottom. But I'm noticing that it works well enough, you can spin it like the speed you want. And then as soon as you get to where you want to be, you just put your finger down on it, and it freezes the window.

Leo: Which mouse is this, Logitech mouse is this?

Steve: Well, I'm actually using their Nano VX, which is...

Leo: Oh, yeah, I have that. I love that mouse.

Steve: That's my - it's the mouse I'm using.

Leo: It's designed for laptops.

Steve: Yes. It's the mouse I'm using at Starbucks. It's got a little tiny, I mean, a super tiny little transmitter that's - literally it's the size of the USB plug with a little tiny head on the top of it, just enough...

Leo: I was so sad because I lost my transmitter.

Steve: Oh.

Leo: It's this small. You can eat it.

Steve: Well, in fact, me, I'm sort of a battery fanatic. So when you put it back into the mouse, it stores inside the battery compartment of the mouse. And of course in the process of plugging it into, like, returning it to its storage position, it disconnects the battery so that your mouse is turned off. But I think they think in terms of, like, leaving it sitting there on your laptop all the time.

Leo: [Indiscernible]. It barely protrudes.

Steve: Yes. And the mouse knows when it's not being moved, and it goes into an idle mode anyway.

Leo: Do you prefer that to using Bluetooth for - I do. Bluetooth seems to drop out, and it's just...

Steve: I agree. I've not had success with Bluetooth to the degree that I have with this thing. But they do - I can't remember. They have a trademark name for this style of wheel. And many of their mice, they don't have a Bluetooth mouse with this, but they have a whole range of, like, larger desktop mice, as well, that have this same zero-friction wheel. And I tell you, when you combine that with the KatMouse, you know, just hover scroll thing, it's just a - it's a hot setup. So I just wanted to pass that on to our listeners as something that I found.

Leo: I think that this Nano VX is good for these Netbooks because they really have lousy track pads.

Steve: Well, they don't have room for a full-size track pad.

Leo: Right. So you almost need a mouse. And something this small, it's perfect. It's just right for it.

Steve: Yeah, I like it. And in fact I'm seriously, I mean, I'm liking the wheel so much, I've got the big Microsoft ergonomic mouse under my hand, my right hand right now. But it's got the traditional sort of stiff wheel. And I'm seriously considering moving over to a Logitech mouse just to have this zero-friction wheel because it just - literally, you just kind of give it a kick, and it zooms up. And then when you see where you want to be, you just stop the wheel, and the scrolling stops.

Leo: Like a fishing pole.

Steve: Lets you jump - yeah, exactly. And we did get a really nice note from a listener, Mac Morris, who wanted to share a SpinRite testimonial, which he named as such. He said, "I recently downloaded SpinRite 6 to fix a hard drive at my workplace. The hard drive would attempt to boot and then give the famous Blue Screen. I ran SpinRite and received a clean bill of health. However, the clean bill of health led me to the real problem, which was a corrupt Windows installation." So it wasn't a problem with his drive at all.

He says, though, "After repairing the installation, all was well. Well, my boss decided not to let SpinRite go to waste. I have since used it to successfully recover two dead hard drives, and have two more on which to run it. I think we need new hardware," he says. "Thank you for such a great product, and thank you and Leo for Security Now!. I hope to catch up on the episodes soon. Luckily the CD player in my car plays MP3 files."

Leo: Well, you'll be able to catch up. Just take long drives in the country every once in a while.

Steve: Exactly.

Leo: Listen to all the shows. All right. We're going to get to Windows 7 security issues. I think this is a great topic. I'm dying to hear this. I've been saying, and I hope that you're not going to prove me wrong, that this is the best version of Windows ever.

Steve: No. Well, okay.

Leo: We'll see. I know that there's qualifications and caveats and so forth. But I don't have your depth of knowledge on the security side, so that's what I really want.

Steve: For the typical user I think it is the case. I'm not going to contradict you.

Leo: Wow.

Steve: But I'm not going to go there for a year, either.

Leo: Yeah, I understand that. This is a guy who was using Windows 2000 for the last eight years.

Steve: My XP installation is still fresh.

Leo: So let's talk about - I am excited about this conversation - Windows 7 security. Now, remember Vista, they said we're going to rewrite everything from scratch. And you were very worried, the TCP stack, brand new.

Steve: Well, yeah. And Vista had fewer problems than XP. Remember that it added kernel patch protection, where it was not going to allow things to go hook the kernel, which was controversial because many third-party products did rely on patching the kernel in order to function. It hardened services and drivers by requiring that they be signed, which was arguably a good thing. Worked more for data execution prevention, DEP. Also offered Address Space Layout Randomization, ASLR, where it would deliberately load the various subcomponents of Windows at random locations in order to make it harder for malware to jump to a specific location in the kernel, which was one of the approaches that malware depends upon, for example as part of an exploit using a buffer overrun. You would jump into some place in the code that just happened to execute a few instructions that had a side effect of, for example, turning off User Account Control or something.

So they did a lot in order to improve the security when they went to Vista. Now, of course they also, talking about User Account Control, which was very controversial, they arguably maybe went too far. I think we could now say clearly and confidently that they did because they have backed away from some of the annoyance factor. But the good news is they really - they've done so in a way that is some reengineering rather than just turning things off. So they really haven't backed out of the security that they were offering. So, but Windows 7 offers, running through the list briefly, and then we'll go back and look at it in depth, is something called a "biometric framework" which is currently only supporting fingerprint readers. But it offers some good features. They have extended authentication protocols for small networks. They've improved BitLocker so that it may actually be useful. They've added BitLocker support for removable drives. They've really made some changes to User Account Control. There's something new called AppLocker. They've fixed firewall policies to make them better. They've got DNSSEC, that is, DNS security support in the client. They've fixed autoplay so that it defaults in the right way. And they've got something called Direct Connect that works with their built-in VPN client stuff.

So a bunch of things which they have - they've basically gone into, they've looked at. I would sort of call this, you know, like major improvements to - mostly major improvements to the security, to the existing functions in Vista. This is like Rev. 2, or Round 2. We're going to - they took all the feedback and problems people had, and in many cases did some real reengineering of it.

Now, one thing that's new that I talked about first was the so-called "biometric framework." They call it WBF, Windows Biometric Framework. It's in response to the fact that an increasing number of machines, probably primarily principally laptops, have built-in fingerprint readers. I know that both of my ThinkPads do, as does this new tablet that I got, all have fingerprint readers. Under XP, which is what I'm using, it's necessary for the vendor to basically bring along a whole collection of add-ons to make the fingerprint reader work.

And in fact one of the problems I had, remember we talked a while ago that I had my two employees, Sue and Greg, were out roaming around and wanting to get secure access to the GRC network. Well, I ended up doing the whole Perfect Paper Passwords technology to create a paper-based, one-time password system that would allow them to do that securely. But that was only after a great deal of frustration trying to figure out how I could write an application to use the fingerprint reader that we all already had in our laptops because I set them both up with these nice IBM Lenovo ThinkPads, all with fingerprint readers. Yet there's no API, no Application Programming Interface, that would allow me in any way to say swipe your finger on the reader now, even though I'm running, swipe it again to prove that this is really you at the keyboard. Well, we get that in Windows 7. So...

Leo: Ah. But that was kind of inevitable; right? I mean, that's been - these biometrics have been built into machines for a while now.

Steve: Yes. And so Microsoft is responding, so...

Leo: Finally, yeah.

Steve: And what it also means is that we'll see shareware and freeware applications using the fingerprint in different ways. I mean, I'm, as we know, I'm a fan of the YubiKey. It offers the ability to - it's different because it allows you to authenticate yourself wherever you are. Inherently you're authenticating your fingerprint to your own machine. On the other hand, you've always got your fingers with you, hopefully, so that's convenient. So what this does is this essentially turns the fingerprint reader from a proprietary device only supported by manufacturer-specific drivers and, like, some third-party glue that, like for example, Lenovo provides their own third-party stuff and keeps it very closed. This opens it up. And I think we'll end up seeing lots of good use for it.

For example, my own forthcoming VPN will certainly leverage that API when it's available as one of the many means that it will have for authenticating. So when you want to create a connection it'll say, okay, you've told the server that you want to make yourself swipe the fingerprint right now. So do that right now. Prove that it's you who's doing this.

And so that's going to be - that's a nice step forward. I consider that a good thing. And I think we're going to be seeing, then, as a consequence, much more use of this kind of inexpensive pervasive biometrics where it's available.

Also, because Microsoft has carefully engineered this with security in mind, we noted - and we've talked about how, for example, that a problem with biometrics is that unlike, for example, a password, you can't change your fingerprint. The fact that you can't change it means you don't want it to get away from you. It's one of the reasons that we've had listeners write in during our Q&As saying that they object to Disneyland Florida using their fingerprint as getting into the turnstile at Disneyland. It's like, uh, no, I'm not - this is where you give them your knuckle instead because you want to keep control of your fingerprint.

So one of the things that the Windows Biometric Framework does is it encapsulates that knowledge and prevents any application from having access to the fingerprint. It gets a token that represents you, but absolutely cannot access that biometric information, which you really want to protect because it's something about you that you can't change. So that's new in Windows 7, and that's a hundred percent good news. I mean, as long as they didn't screw it up somehow. I mean, it certainly represents a nice move forward for security, and something I'm glad to see. I mean, I will absolutely take advantage of it.

Leo: Are they tying it in to TPM or any of the hardware...

Steve: Oh, yeah, yeah. It's absolutely based on the Trusted Platform Module to do authentication and storage of stuff. I mean, as is, for example, in the ThinkPad, and even in my tablet, all of these things do use the TPM. But there isn't an application-available API. Just adding that hugely opens this up to the ability for all kinds of applications to say, hey, let's have you reauthenticate right now before we proceed.

Oh, in fact, User Account Control can be tied to the fingerprint reader now. So, for example, in a home environment, the kids would be running as a limited user. And you can then put parental controls on things which are tied to the fingerprint reader. So that in order to do something, the box comes up, and the kids have to say, hey, Mom, can you come here for a second, I need permission to whatever it is, charge a micro payment on your credit card or something. Mom comes over, scans her finger, and bing, it works.

Leo: That's good. I like that.

Steve: So, yeah. We're going to see - this is just like, you know, lots of good move forward. Traditionally in a home network you log onto your own machine. Or if you're doing filesharing, and you have different credentials on another machine, you have to - you put those credentials in, in order to map a network drive. Microsoft has done something that they call "extending the authentication protocols" with what they call "home group authentication." And with home group authentication, essentially it's a little bit like sort of a mini enterprise. You know, in an enterprise you authenticate to the domain. And so that allows an individual to be in various parts of the enterprise. And when they authenticate on a machine where they happen to be, they're authenticating against their credentials that are stored on the domain controller.

Well, Microsoft has sort of juniorized that and created this notion of a home group authentication, where the idea being that it essentially creates peer-level authentication providers that will allow you in a home network environment to authenticate against another machine on the network, which is a whole new level of sort of flexibility for what home networks are doing. And I don't really have a good sense yet for how that will be applied. But I'm glad that that foundation is there because it makes sense in a home network environment. I'm the only one in my home. So I've got credentials synchronized among my different machines. And so connecting to them is transparent. Really in a more heterogeneous environment, where you've got different log-on users and passwords on all the different machines in the environment, it'd be nice to have, to be able to authenticate as Mom or Dad on your kids' machine, depending upon how you wanted to set up filesharing and media sharing and so forth. So we get that.

Now, BitLocker. I've never been impressed, and many people have never been impressed with BitLocker, only because, unlike TrueCrypt that I am very impressed with, BitLocker has traditionally been a big pain to set up because, as we'll remember from our podcast on BitLocker, you need to create a separate system partition, separate from the main system partition. That is to say that Microsoft didn't do the sort of boot sector intercept approach that TrueCrypt took, where you're able to just do an in-place encryption of the whole drive and add that after the fact.

And so the problem with Vista was that Vista came with the whole drive partitioned as the C partition. And the problem is you couldn't just say, oh, I want to add BitLocker to this because it needed repartitioning. And sure, you could use some third-party tools to do that. But that was enough of a barrier that lots of people didn't. So two main changes to BitLocker in Windows 7. The first is that Windows 7 setup itself, by default, creates a separate active system partition. So it sets itself up so that it is ready to be BitLockerized if you decide you want to do that.

And if you are upgrading from Vista into 7, of course you wouldn't be running Windows setup from scratch on an empty drive. The whole drive would already be a C partition. So Microsoft has taken responsibility for essentially allowing you to retrofit the BitLocker-required partitioning into any non-prepartitioned drive. That is, literally it comes up with a dialogue, and it shows you shrinking drive C, which is what's necessary in order to create some empty space where it can set up its separate active system partition. So that means that you are for the first time able to, without using any third-party repartitioning tools, and the potential concern of, like, okay, well, which one do I use, how do I do it, how much space do I need and all that, you're able to just tell, in Windows 7, you're able to tell BitLocker, okay, I want you to install on this drive, even though it's not ready for you.

So BitLocker will shrink the partition, create the new system drive, set itself up, and then prepare to encrypt the whole drive, which is very cool. And of course the flipside of the overhead that this represents is that you end up with an arguably much more capable authentication environment. For example, I wish that I could use biometrics to authenticate with TrueCrypt, or I wish that I could use my YubiKey to authenticate with TrueCrypt. TrueCrypt right now only allows you to enter a password. And so the advantage of the more heavyweight Microsoft approach is you've got a Windows system there running, so you can take advantage of much more powerful authentication technologies in order to say, for example fingerprint reading, in order to say yes, this is me, unlock my BitLocker partition.

Then the next thing that they did is that they call BitLocker to Go, which short version is it's BitLocker for removable drives. Which is very cool. One of the things that they have done that I think is really a tremendous improvement is there is - when they added BitLocker to Go, meaning that you had BitLocker for - you had encryption of removable drives, meaning USB solid-state drives or removable hard drives, they said, okay, we're going to enforce that. So there is now, for the corporate environment, a group policy setting that says any removable drive is read-only unless it is encrypted with BitLocker.

Leo: That's great.

Steve: Yes. So, now, they did have to do a little bit of a kludge in order to retrofit this into FAT file systems because of course most removable drives, in fact I don't think I've ever seen one that came preformatted as NTFS because of course you don't have...

Leo: Compatibility issues.

Steve: Exactly, compatibility issues across Mac and Linux and other OSes, whereas they all support the FAT file system without any problem. So Microsoft has this weird sort of virtualization overlay that they create on top of the FAT file system. They realized that's not a problem because only they and BitLocker can read it. So they were able to sort of kludge up the architecture of the FAT file system.

The other thing that they had to do was they said, well, okay, we're doing BitLocker to Go in Windows 7. But we can't get away with only having Windows 7 work with these things, that is, at least being able to read them. We need a solution for XP and Vista. So they do have, when you set this up, there is a reader which is installed on that removable drive which both XP and Vista are able to invoke in order to have access to the FAT file system. So it creates sort of a little decryption system which is XP and Vista compatible so that the drive that you create under Windows 7 with BitLocker to Go can be read by XP and Vista. So it's a nice solution.

They also have, in existing BitLocker systems, every single volume you created needed a different recovery key. And they realized that was too burdensome for keeping track of all this. So it is now possible, for example, in a corporate IT environment, to have a single recovery, a single master recovery key that will work across all the BitLocker drives in the organization, which makes doing data recovery, they have something called a "data recovery agent" in Windows 7 which they actually - they got this technology from EFS, their Encrypted File System, and set that up. So essentially they've made this portable in a way that's useful. And I think this solves a lot of problems. And as you said, there's group policy enforcement, the fact that they're able to say removable drives you plug in are read-only unless they're encrypted. Again, that's a major step forward for Windows 7 and long-term security enhancement.

Leo: You could disable that.

Steve: Yes. Oh, absolutely, yeah. Oh, yeah.

Leo: But it's the right default behavior.

Steve: Yes. And it is not the case normally. So it would be something that corporate IT would say we're enforcing this. So that you can plug drives in, your thumb drives, without encryption, and you can read from them. But you can't write anything to them.

Leo: Right.

Steve: Well, speaking of that, the other thing that they did - yay - is autoplay. Autoplay...

Leo: Yeah, this is the problem.

Steve: Yes, is now disabled by default on everything except removable optical drives. That is to say, CDs and DVDs.

Leo: And this is in response to Conficker, basically.

Steve: Yes, essentially, yeah. Well, and in general. Microsoft actually did a study which showed, I think it was 17 percent of viruses, yes, 17.7 percent of malware was propagating through autorun. And so they said, okay, this is wrong, let's turn that off. So that's another improvement. So CDs and DVDs by default will still launch when you install them. But no other removable drives will. You don't even get the pop-up that prompts you for what action to take because users tend to take the wrong action. It's just silent. It's like, nope, we're not going to have that. That does mean, though, that simulators of CDs and DVDs, like U3, they do still work. They look like a CD, like a removable optical drive, specifically in order to get that autoplay functionality. And so those will still work.

Leo: That's too bad. But I guess that's...

Steve: Yeah, but again, security-conscious users can disable that themselves. So that won't be hard to fix, either. User Account Control. This is, of course, the very controversial pop-up which has been the bane of Vista users for so long. Several things have happened. The good news is that User Account Control was such a problem that a great deal of pressure was put back on application writers to make it work right.

For example, I remember when I wrote SecurAble, I thought, okay, I want to make SecurAble work correctly with Vista. So there is a means for an application to declare its need for administrative privileges right upfront, right in the loader, essentially, so that Microsoft asks you preemptively, hey, this program wants administrative rights. Do you want to allow that? And then you're able to give it to the program and never be harassed later, like downstream when you're doing specific things that require the rights. Most applications traditionally, well, first of all, this didn't exist before Vista, so of course no applications were doing it then. So it would be when the application stepped into a directory or tried to touch the registry or did these things that you'd get the pop-ups.

And so the problem was you could get them all over the place in a single application, rather than just permitting it once. So what happened was, or what has happened over this span of time, from the time that Vista happened until Windows 7 is threatening to happen, is that put back pressure on application writers to make their applications quieter, and/or to make them run as a standard user. As we know, traditionally, because this whole notion of running as a non-admin, a non-superuser is relatively new. Certainly it wasn't new in the UNIX world, but there wasn't any concept of it for a decade of Windows use.

So as security advice began to be don't run as the admin user, people were saying, yeah, but it's a pain in the butt not to run as admin because nothing works. I mean, all my applications are, like, causing all these problems. So in addition what's happened is this migration away from running as admin has also put pressure on developers not to assume admin privileges, only require them if it's really necessary. And typically it's just the installer. It's just the setup process that needs to put something on the machine, install device drivers, have access to privileged directories or the registry during setup and install. And after that you don't need that so much.

So one of the changes that's happened is just natural, and that is these sorts of - this evolution in security policy toward being more secure is never painless. And so we've seen some pain. Over time that's been getting better because applications are evolving not to assume that they're going to have admin privileges. Okay, but Microsoft also responded, and they made some major changes, two real major changes to the way UAC works. One is that prompting for standard admin tasks has been removed. Things like changing the screen resolution. I mean, Vista used to require you to say yes, it's really me wanting to change...

Leo: Yeah, that was silly.

Steve: ...my color depth. Okay, that's just dumb.

Leo: Yeah.

Steve: Exactly. And so that they removed. The other thing is that they've better aggregated the way things trip User Account Control. So for example when you were installing an add-on in IE, for example, there would be an initial prompt when something tried to sort of look like it was about to do it. Then you'd say yes. And then when the add-in then tried to do something itself to install, you'd get another one because you'd get blocked again based on the add-in's behavior. So what Microsoft did was they said, okay, this is really annoying for people. Let's create sort of an encapsulation of that, that is, we'll recognize when something is going to install.

One of the other problems was that some of these, many, actually, of these User Account Control pop-ups didn't give you much information at all. It said, do you want to install this add-on? Well, okay. I'm trusting the site that I'm going to that's telling me I need this add-on to be installed. But I'd really like to know more about the add-on because I'm not sure how much I trust this site. Can't you tell me more?

Well, the original architecture didn't have any more information. The new architecture does. So that the process that presents you with the permission query reaches into the ActiveX control that you're trying to install, extracts its name, publisher and so forth, and presents that to you; and then permits it to do - given that you have said yes, of course - permits it to do whatever it wants to do. So you're not getting multiple successive pop-ups after you've said yes, I want to install this. Essentially you're saying, I want to install it, and you've told me enough that I'm going to trust everything that it does while it installs. And that's the decision I've made. Don't keep bugging me about this. So that's been fixed.

Leo: Good.

Steve: And Microsoft is trusting themselves, that is, their own code which is making changes they trust. They don't trust foreign code. And of course that's the activity that you want. Now, they of course made one famous screw-up, and that is, one of the pop-ups that they decided not to have require User Account Control was User Account Control itself.

Leo: Right.

Steve: Where a couple clever guys figured out that we could use the Send key's technology to essentially pretend to be the user, turning off User Account Control, and the act of turning off User Account Control would not ask you for permission because Microsoft just deadened all of those permission queries, including that one. So they said, whoops, good point. It's interesting, too, because their initial reaction was, no, that's by design, go away. And then they started to actually listen to what people were saying; and they said, oh, yeah, that's a good point, maybe we ought to ask for permission if we're going to be turning off all asking for permission.

So there's now a slider, a four-level slider in Windows 7 where the default setting is level three. One, two, three, and four. Level three is not quite as onerous as level four. Level four is essentially the same as we had in Vista, that is, you're notified when programs install software or make changes or change Windows settings. You're notified, and you are required to reply. So that's pretty much the same as what we had in Vista. Three, level three gives you the notification, but you're not being forced to respond. It's just sort of a notification, and then it's like, okay, fine, we wanted to let you know that this is going on, but we're going to move on.

Level two is a little bit of a concern, but a little bit less visually jarring. As we know, every time User Account Control comes up the whole screen behind it goes dark, and it's sort of the only thing illuminated. Well, this is actually a different desktop. It's a security-enforcement desktop which prevents any software that's running in the normal environment from being able to see and reach into the User Account Control dialogue. So this darkening of the desktop is a visual metaphor for something that's actually happening in the architecture. Normally, and this is a fundamental security problem with Windows, different windows running on the same desktop are able to see each other. They can enumerate them, they can get all their names, they can send them keystrokes. And that's how macro programs work. A macro program is sending keystrokes to another window which is emulating what the user is typing. Well, you wouldn't want to emulate User Account Control receiving the click of Okay for permission. So this darkening of the desktop is a security feature that is creating an isolated environment for the User Account Control dialogue to pop up. But it turns out that some video drivers are very bad about implementing this switchover. Some of them blank off completely for a while and then click back on, which is...

Leo: I've seen those. It's really annoying.

Steve: Yeah, it's really annoying. So what Microsoft again, trying to respond to this, created level two, which is not as secure because it does not invoke the secure desktop.

But it's way less visually disturbing. So the User Account Control dialogue will come up, leaving, you know, it's on the same dialogue. So there's the concern about, okay, something bad could click on the buttons. On the other hand, and this is a point that I'm going to bring up here in a second, by that time it's too late. That is to say, you've already got something on your computer if it's able to click the button. So you could argue, okay, well, if we're compromised, we're compromised.

And level one, lastly, does nothing at all. If you go to level one, it will warn you that you are about to disable User Account Control, and you're going to have to reboot your machine because, you know, we've wired this all in so deep that we can't turn it off on the fly, like making major intrinsic changes to Windows settings. So that's the way those four settings lay out. So the point I want to make, and I know, I mean, I've heard you say this, Leo, on other podcasts and on The Tech Guy radio show, that by the time your computer is infected, it's too late. And it's a funny concept that people have a hard time grasping, but...

Leo: Well, we've been trained that, you know, antiviruses can remove this stuff for years.

Steve: Right, right. And of course there's still the hope that that can happen. But we know that with the growth of rootkit technology, I mean, basically malware has gotten much worse in terms of what it does to your system once it gets in. It's not just, oh, look, it's in the Startup group, let's take it out. Or it's in my Run key in my registry. I mean, that's just - none of that stuff is the case anymore.

So the point I wanted to make, though, I wanted to, I mean, you're exactly right when you say that - and I've been sort of trying to figure out how to make a really clear distinction. The idea is that, if you've got a castle with a moat and a drawbridge that's up and high walls, the idea is that there really is a useful function to keeping things out. That is, inside the castle walls you can have all kinds of secrets, and you can be doing anything that you want to. And the moat and the walls keep the bad things out. And there's a fundamental change when those walls are porous, the moat is filled in, the drawbridge is down, whatever, when something is able to get in. Now it's on the inside.

Well, I mean, I guess the point I want to make is everything changes at that point. We're hardening Windows to be better at this. We're trying to keep things out. So User Account Control is trying to make users more aware of typically the things that they do. But it also could just be, you know, drive-by websites. You go to a website that is trying to, for example, run Java in order to install something on your computer. Well, if your computer never told you when something was being installed, then you're in trouble. But if the computer is able to say, wait a minute, something is trying to install itself, do you want to allow this to happen, it's very much like you've got a door through your castle wall, and someone's knocking on it. And it's like, someone's knocking on the door. Are you going to open it and allow whatever happens to happen?

But I guess the point is that it seems to be a difficult concept for people to grasp that having the bad stuff outside the castle is just fine as long as you don't let it in. Once you do let it in, really, the jig is up. I mean, Windows is trying to be hardened against ever letting it get in. But once it's in, all software is being run by the operating system on pretty much even basis. Now I'm about to talk about something that changes that a little bit called AppLocker, which is another really good improvement in Windows. But again, this notion of before and after and the value of User Account Control is that it helps with notifications. I really think Windows 7 is an improvement because it's going to be in your face a lot less. It's been - people that have incorrectly criticized what Windows 7 has done to User Account Control say that Microsoft has neutered it, they've turned it essentially off, or down to a point where it's not nearly as useful. And that's a complete misunderstanding of the changes that have been made.

Microsoft has - basically this is Rev. 2 of User Account Control. It's much quieter. It's much saner in terms of, as we said, lots of little things aren't going to be in your face. You can go weeks at a time without ever seeing any UAC pop-ups. When you get them, you're not getting a flurry of them, but you're getting one. And they're also containing more information. So, I mean, I think this is...

Leo: All that's good.

Steve: ...really a good - this is really a big improvement.

Leo: The real problem, as you say, is user fatigue. Well, first of all, lack of information about what the pop-up means. And then there's user fatigue, where they just go yeah, yeah, yeah, yeah, yeah.

Steve: Yeah, exactly. If it's coming up all the time, and the thousand times they've given it permission nothing bad happened, then they get trained into, like, oh, this is just, this is what I have to do now with this darn operating system.

Leo: Right, I just say yes and get it over with. And of course that's exactly what you don't want to do.

Steve: So AppLocker, A-p-p as in application locker, AppLocker, is another refinement to something that we've had for a long time which was called Software Restriction Policies, or SRP. This is something that unfortunately really upset users and really upset IT. The IT in the corporate environment, well, they wanted to bring software restriction policies into play because they wanted some control over what employees in a corporate setting were running on their workstations. The problem was, the software restriction policies were based on sort of a very low or non-granular security certificate, if it existed, and hashing of the EXE. Well, what that meant was any change of the security certificate because of, well, the security certificate or the executable file as a consequence of, for example, updating, completely broke the hashes. And the program was no longer recognized as permitted, just because you went from version 1.0.297 to 1.0.298. And so it was a huge problem for actual deployment and use because it was far too brittle.

So what Microsoft did was, thank goodness, they made it smarter. They actually call it, the information is called SRPv2, which is stored in the registry as an XML format file off a registry key. But they're now formally calling it AppLocker to sort of give it a more friendly name. What it allows IT to do is to create rules that are based on the certificate that comes with the application. So, for example, you're able to say, I want to trust all applications by this publisher. Or I want to trust this publisher's application named this for all versions later than that.

And so the beauty of that, given that applications are digitally signed, and we understand how signing processes and certificates work, I mean, they are bulletproof and robust and provable, now using AppLocker you have sort of a much more working the way it should always have system for software restriction policies, allowing the corporate environment to say this is the set of software we want to run, and this is going to be a robust rule set even in the face of software being changed and updated. So this is - I expect that as a consequence this will end up being much more feasible to use than it ever has been before. And as a consequence it'll get used.

Now, employees are going to be annoyed because they're not going to be able to install their own software and run them on corporate desktops. But you could argue that's a huge source of security problems, and in a corporate environment the company has a right to control what runs on their desktop. Overall, though, this means more security. And that's a good thing.

Leo: So it'll be even in the home versions.

Steve: Yes. It is built into the kernel in a new driver. It's called...

Leo: That's where it should be, isn't it, yeah.

Steve: Yes, appid.sys driver, and it does kernel mode rule checking at process creation and DLL loading. It also is able to individually manage executables, scripts, installers, and DLLs so that - to provide corporate IT a lot of control. I don't know that an end-user would use this. Maybe really security-conscious people would. It does have an audit-only mode which might be very interesting. That is to say, you're able to say audit but don't enforce, and then you're able to look at your audit trail to see what has been run.

And I know that sometimes I'm interested to know what's been going on. I associate a sound in Windows when an application starts, and one when it stops. Under the little sound applet in the Control Panel you're able to create sound associations. Many of the themes that Microsoft has bring a set of WAV files for sound associations. And I've always had something that I can hear when an app starts and when an app stops. And so sometimes I'll be working away, and an app, something will run. And it's like, whoa, wait a minute, that wasn't me, what was that? I'd like to know. And so this audit-only mode that AppLocker now adds will allow you to look at essentially an audit trail of everything that's been going on in order to answer questions like that, which I think will be very useful from a security standpoint, as well.

Also, we now have the first client in Windows 7 which understands DNS security certificate records. We did a podcast a while back on DNSSEC, as it's called. But it hasn't been natively enforced at the client end. And with Windows 7 we have that. So it will be able to validate DNSSEC signatures in the data returned from DNS lookups.

Leo: Excellent. So now everybody can go out and implement this.

Steve: Yeah. Well, I mean, it starts to be time to get serious about this because this absolutely, this allows intermediate DNS servers like ISP servers to accept the DNSSEC data and then to cache it and then to make it available to clients. So it solves the spoofability problem completely. You're no longer dependent upon just making - you're no longer dependent upon the ISP's server not having been hacked or having it set up in a secure way because the data itself carries its own validation. And so you're able to, with Windows 7, to say, okay, I want to make sure that this is safe. And no doubt the browsers will surface that information at the UI so users will see, in a way that today we see when we've got an extended validation certificate, and so the URL bar turns green or something to say this is an extended, an EV certificate, and we've verified it, which is a nice thing to see. You can imagine at some future point saying we have verified the credentials of the DNS data that we just received so that we know this is the IP that you think you're going to.

Leo: Excellent.

Steve: Which is again very cool. And then I got a kick out of one thing that they added in Windows 7. They call it Direct Connect. I got a kick out of it because it's a feature that CryptoLink has always been able, or always had planned, and Microsoft has added it to their VPN solution. The idea is that it makes VPN tunnels essentially automatic so that whenever you connect to, like your laptop if you're out roaming around, it automatically and silently reconnects your VPN back to corporate headquarters so that your corporate assets are just always there. That's something that I had in my notes a long time ago for CryptoLink because it's an obvious missing piece for just VPN ease of use. And so Windows 7 adds that.

Now, theirs, of course, is still an IPSec and PPTP VPN. So you've got all the problems associated with inaccessibility of the VPN in an environment instead of blocking VPNs deliberately. But given that you've got a VPNable location, Direct Connect will be nice in that it will allow you to sort of maintain a persistent connection back to home base. And I certainly think that's the future for people who are roaming.

Leo: Yeah, no kidding.

Steve: And the last thing that I wanted to mention was Brian Krebs, who writes one of my favorite security columns for the Washington Post, he noted that in Windows 7, unfortunately file extensions are still hidden.

Leo: Oh, that makes me so angry.

Steve: I know. It's funny, too, because, I mean, it's one of the first things I have always done in Windows is, when I'm setting up a new version of Windows, is to turn that off because it is so prone to exploitation. You know, Microsoft says, oh, but the file extension, even if you can't see it, you can tell by the icon because extensions are associated with icons. So you can tell, like, when a file is a text file because it looks like the little Notepad icon. The problem is that if you name something malware - well, you wouldn't call it malware, you would call it happyware...

Leo: Happy, good stuff for you.

Steve: ...good stuff for you.txt.exe, and only the .exe is being hidden, then what you see is happy stuff good for you.txt. Well, EXEs carry icons with them. And so all that malicious happy good stuff.txt.exe file has to do is put the Notepad icon in itself, and that's what the user sees. They see the Notepad icon, and they see the .txt confirming that that's what it is. But in fact it's an EXE with a hidden file extension. I mean, it's just nuts. I don't think we're ever going to succeed in getting Microsoft to change that. But I appreciated that Brian said, well, he was hoping maybe that users would get to see what the actual file type is. But nope, we're still not going to get that from Microsoft.

Leo: Why do they do that?

Steve: I just think they're worried about confusing people.

Leo: Yeah, but that doesn't - it's the opposite of confusing.

Steve: It is. I mean, I want to see .doc or .pdf. And, you know, maybe - I think Brian's right. In this day and age people know about documents and about PDFs. They know they have to have a PDF reader, not some magical link between this unextensioned file.

Leo: Yeah, they've figured it out.

Steve: Yeah.

Leo: And that's how it used to be. In DOS we had it.

Steve: Yup, and we survived that, yeah.

Leo: Oh, well. It really does make it hard to solve this.

Steve: So overall I'm bullish on what has been done in Windows 7. I think they've done a lot for UAC. They've made BitLocker far more feasible and useful and usable. I mean, basically making it a pleasure to use and deploy. And they've allowed it to work in a useful fashion on FAT devices to be backward compatible to XP and Vista, and a group policy that will allow corporations to enforce that removable drives are read-only unless they carry encryption with them, so we ought to see much - ultimately. This will take years to happen. But you've got to start somewhere. And these things always take years to happen. So we'll see five years from now problems with lost thumb drives containing the corporate records or all of the identity information for hundreds of thousands of medical records that'll be - at least it'll be encrypted. It won't be just sitting there for anybody to pick up and exploit. So these are really good changes.

Leo: How about - what is your sense overall of the code? I mean, a lot of the problems that we have with Windows these days is because the code has exploits in it. Have they done anything to clean that up? I mean, it's still Vista, I think.

Steve: Well, yes, it's still Vista. And the problem is they're still human, and security is still hard. And so that's why, no matter how good this looks, I'm waiting a year. I mean, I'm in no hurry to, I mean, none of this particularly affects me. I mean, it's like, okay...

Leo: Yeah, none of these things, you know better. You turn on extensions, you don't need AppLocker, you know how to do security with the...

Steve: And I'm using TrueCrypt. I'm using TrueCrypt on my drive, yeah.

Leo: You don't have - you turn off autorun. All of these things you've done anyway.

Steve: Right.

Leo: And frankly, anybody who listens to this podcast has done, and most people who are sensitive to security have done.

Steve: Yup.

Leo: So but what we're talking about is making it - I mean, look, if you're sensitive to security, XP's safe.

Steve: Yes.

Leo: What we're talking about is making it safe for the people Microsoft is selling hardest to, which are novice computer users, people I think probably shouldn't be using Windows. But those are the people that Microsoft needs to make Windows secure for.

Steve: Well, and these are the people who have Conficker running on their machines.

Leo: Precisely.

Steve: And this none of our listeners probably do. So this is for them. And that's good. We want them all to be more secure because it makes everything more secure.

Leo: Right, exactly. We all suffer from the stuff that happens because novices aren't secure.

Steve: Yup.

Leo: Well, Steve, that's reassuring. I'm excited. I believe, having now put Windows 7 on many machines, that it really is a much better way. It's faster, it's lighter, it's cleaner in the UI. It seems to be, from the outside, more stable and secure. I'm hopeful.

Steve: You probably know from talking to Paul, and I haven't done the research, what's the status on - because we're not yet at final...

Leo: This is release candidate, yeah, right.

Steve: ...RTM. And I do think I remember reading something about some changes to RC1. Where are we relative to upgrading from this beta 7 install, I mean, I heard you say you put it on all those machines.

Leo: You should be using RC1 now, which is Build 7100. That's the last officially released one.

Steve: But I guess my question is, once they finally release it, is the beta upgradeable?

Leo: Yeah.

Steve: Okay.

Leo: But you know what we say, what Paul's been saying, and I have to agree with him, is clean install each time. And so that's kind of one of the drawbacks that people should be aware of if they want to run this beta, is when the final version comes out you're going to want to upgrade. Now, I have to say, for a beta, even the last beta, very, very, very robust and reliable.

Steve: Well, again, because it's mostly just Vista.

Leo: It's Vista. It's Vista with the knobs, you know, the rough spots polished off, that's what it is.

Steve: Right.

Leo: A little tweaking here and there. Yeah, of course it's got - it's going to - what's interesting, I find really interesting - this doesn't really address security - is it's much faster. So they clearly were able to tune Vista to get better performance out of it.

Steve: Well, yes. And apparently there is a technology also where it's much better about not bringing the kitchen sink of device drivers along with it.

Leo: Yes, yes. Which may be why it's more reliable.

Steve: Yeah.

Leo: It also - and faster. And also at some point I'd love for you to address the virtualization capabilities because I think they've enhanced - they're really moving towards this hypervisor idea. And I think that's, I mean, they've already announced that if you get Windows 7 Ultimate or Business, whatever it is...

Steve: It will include an XP VM.

Leo: Right, right. And I think we're moving towards really running in virtualization all the time. Which would be more secure; right?

Steve: Yes.

Leo: Hypervisor mode.

Steve: Yes. I can easily see the day where applications are actually in their own virtual machines, where everything is just - where there's much more control. And again, from that vantage point we'll look back at these Wild West days with viruses jumping around and sending keystrokes to other applications and all this and think, wow, how did you guys even survive that?

Leo: I hope you're right on that one. I do. Steve's at GRC.com. That's his home, the Gibson Research Corporation. You can go there yourself. And you'll find wonderful stuff. SpinRite, of course, the world's finest hard drive maintenance and recovery utility, that's a must-have. There's a lot of free stuff, too, like Wizmo and ShieldsUP!, Shoot The Messenger, DCOMbobulator, and of course the Security Now! forums, the security forums are there. If you have a question for Steve, we'll be doing questions next week. Go to GRC.com/feedback, and you could leave a question or a comment or a suggestion. 16KB versions of the show are there, as well as the full 64KB, full-quality audio and transcripts, too, so you can read along as Steve speaks. All at GRC.com.

Steve, have a great week. Enjoy your programming at Starbucks. I think that's great. Are you getting close to the end?

Steve: Yes. It's funny, I'm now adding CSV, Comma-Separated Value, export and import. This is going to be a great little utility. I think it's going to really - it's going to be significant for us. And so I've just decided - I'm actually doing a bunch of things more for it than I really need. But it's technology which will also be part of CryptoLink. So I figure, well, I might as well put that in, get it developed now. That'll just make CryptoLink development go that much faster. So it's got a whole bunch of nice things that we'll be talking about here soon as I get it done.

Leo: I can't wait.

Steve: We're getting close.

Leo: Thank you, Steve Gibson. We'll see you all next time on Security Now!.

Steve: Thanks, Leo.