SECURITY NOW!

Transcript of Episode #66

Windows Vista Security

Description: Steve and Leo describe the new security features Microsoft has designed and built into their new version of Windows, Vista. They examine the impact of having such features built into the base product rather than offered by third parties as add-ons. And they carefully compare the security benefits of Vista on 64-bit versus 32‑bit hardware platforms.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-066.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-066-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 66 for November 16, 2006: Vista Security.

Security Now! is brought to you by Astaro, makers of the Astaro Security Gateway, on the web at www.astaro.com. And by Dell. For this week's specials, visit TWiT.tv/dell.

It's time to talk security with our favorite security guru, the man who keeps us all safe and sound. Last week we were not only talking about computer security but security worldwide. We're talking about homeland security.

Steve Gibson: Yup.

Leo: Steve Gibson. It's good to have you back on Security Now!. How's your week been?

Steve: It's really been good, Leo.

Leo: I'm in Canada right now, where it's freezing. I want to come home to California.

Steve: Well, I'm going to be up there joining you in December, so I guess...

Leo: Oh, good timing. Should be much warmer then. You nut. All right. What...

Steve: So, Leo?

Leo: Yeah, what can we talk about today? What's the hot topic?

Steve: Since we last talked, I have installed Vista.

Leo: Oh, good.

Steve: I decided, okay, it was at RC2, and it's probably RTM by the time people are hearing this because it was supposed to be around – last I heard it was November 8.

Leo: It did, in fact, the last – I just heard, now, it's an unconfirmed rumor, but I heard a rumor that it in fact was certified and went to master about a week ago. So it's official.

Steve: Well, I hope they made some changes to it.

Leo: Uh-oh. You're using – what build are you using?

Steve: Okay, I'm using the RC2 build. I think it was, like, 5766 or something.

Leo: Okay, okay.

Steve: I mean, it was a late build. And all kinds of things crash. In fact, it was behaving so badly that I thought, okay, maybe this is a system problem. So I ran the Memtest86 for, like, four days, never had a single problem. And Windows XP runs on this system like a bat out of hell. I mean, I've got to say, okay, this is a 3.06 GHz hyperthreaded Pentium 4. It's got 2 gigs of RAM. And because I was going to run Vista I bought a brand new NVIDIA, it's the GeForce 7600 GS board. You know, it's one with a blower on it, and you've got to give it a hard drive connector, you know, it can't – it wants so much power that the bus won't power it. You've got to plug hard drive connectors into the edge of – the back edge of the card in order to get this thing powered up. But Leo, Vista is slow.

Leo: Really.

Steve: Oh. And in fact, I mean, I've got the glass UI, which, okay, you know, I mean, I'm – it's attractive, but not at the expense of all this performance. I mean, I'm – frankly, I'm – the more I look at the Mac, the more impressed I am with this nice brushed-aluminum look that, you know, the first thing I did with Vista, because, I mean...

Leo: I kind of like how Vista looks. You don't like the new Aero Glass interface?

Steve: It'll be interesting to see what people think. It's not that I don't like it. It's that I think they could have done something better with all these display and processor cycles that they are apparently consuming. Now, I turned it off just to see if I could get the display performance up because, I mean, really, it is just dog slow.

Leo: Yeah.

Steve: And also, even with this card, they have something that they call the "Vista Experience Rating"...

Leo: Right.

Steve: ...which, you know, where it ranks your processor, your display card, your RAM, your hard drive speed, and other stuff. Basically what they're doing is they're saying, it's not our fault. They're, you know...

Leo: You don't have enough hardware.

Steve: It's giving me a rating of 2 for this display – for my graphics performance. I think...

Leo: Out of what? What's the top?

Steve: I think it's out of 5. Because the hard drive I'm getting a 4.9. The processor I get a 4.2. And everything else is in the 4.something. But I get a 2 with this screaming, you know, GeForce 7600. It's like, okay, what do you want from me? How can I get more? You know, it's a 512MB graphics card. It's just, I mean, but Leo, grabbing the lower right corner and stretching a window out, it's just like it refreshes so slowly. And, I mean, this is a fast machine that I'm using it on. It's, you know, 3 GHz P4 with 2 gigs of RAM. It's like, okay, well, I hope this thing works. I mean, I just, I don't...

Leo: I think what you're using is fairly close. But again, it's not the final version. The final build is, I think, build 6000, although it's pretty close to what you've got.

Steve: And in fact, all of Sunday – well, it didn't take all of Sunday. But I decided, okay, I've got to find out what you and Paul are talking about.

Leo: Right.

Steve: So I downloaded the four episodes so far of Windows Weekly, of course, with Paul Thurrott. And I got a kick out of the fact that somewhere in the fourth one he said – you guys were sort of talking about Vista and security a little bit. And he said, "Do I remember you saying that Steve Gibson is still using Windows 2000?"

Leo: Yes.

Steve: It's like, yes, and I'll be moving to XP soon.

Leo: But not right away.

Steve: No. I mean, I'm getting ready to move to XP. It's stable enough now. It's mature enough, you know.

Leo: Okay. Well, that should give you some idea. Now, how – it's hard to judge security, though; right? Because, well, frankly, nobody's attacking you yet.

Steve: Well, actually there are – I want to talk about today the architectural things Microsoft has done in the name of security. Now, we've already talked about – we had a prior episode about Vista's Virgin Stack, I think we called it.

Leo: Right, right.

Steve: And I was shuddering over the idea that Microsoft is bragging about the fact that they rewrote the networking from scratch and that Symantec's early pokings at it discovered many problems that are critical security vulnerabilities that were fixed decades ago...

Leo: Right, right.

Steve: ...in early UNIX stacks, that are all – all these problems are back again. So it's like, oh, boy. I mean, this is typical. This is not an architectural thing. This is a, you know, brand new code that just hasn't had the debris pounded out of it yet. And it's why I'm now five years late getting ready to move to XP, because it's had the debris pounded out of it. And, I mean, even XP was a direct descendant of Windows 2000, so it had the advantage of Windows 2000's maturity. Anyways...

Leo: So I gather what you're saying is, if you want real security, use XP.

Steve: Okay. What I'm – we're going to draw some conclusions once I've laid enough foundation. But I'll tell people, the bottom line is, don't buy any more 32‑bit systems.

Leo: Oh, interesting. Oh, interesting.

Steve: And that's freaky for me to say that. But I'm going to explain why. Because what Microsoft has had to do is, in order to make the next move forward in security, they've had to make a conscious decision to break major things that have always been done in the past. This was the right decision to make. I fully endorse it. But it means that the 32-bit platform is going to sail on mostly unchanged, and only the 64-bit platform will be secure and will receive the benefit of these security design changes Microsoft has chosen to make.

Leo: Interesting.

Steve: So, you know, for people who are security conscious, I want to, you know, you're hearing it here. There is a huge difference in Vista's 64-bit security, that is, security on a 64-bit platform as opposed to anything Microsoft is able to offer and has chosen to offer on the 32-bit platform. But stepping back from that, I will again say, boy, you know, any hardware you have that can run Vista will run XP like a bat out of hell. I mean, the system I'm using where Vista is just painfully slow just on a UI standpoint, I mean, Leo, moving a window around pegs the processor.

Leo: Yeah.

Steve: It goes to 100 percent just moving a window around. It's like, okay, what are they doing? That's nuts.

Leo: Well, again, you're using beta code. Maybe there is, in fact, often the case with beta code, there's debugging code still in there, there's other stuff.

Steve: Well, pre-release code. I mean, they were calling it RC2. But as I learned from listening to you and Paul, and I would encourage our listeners to start, you know, if they're interested in Vista, certainly add Windows Weekly, your Windows podcast with Paul Thurrott, to their podcast lineup.

Leo: Thank you. And I'm telling people who listen to Windows Weekly to listen to you because basically both of these shows are covering Vista from different angles. I mean, Paul's not a security expert, but he certainly talks a lot about, you know, things to keep in mind with XP. And I think Paul will actually be very interested to hear what you have to say. Because truthfully we haven't recommended 64‑bit Windows, either XP or Vista, for the very reason you just quoted. It breaks a lot of things, including drivers...

Steve: Yup.

Leo: ...antiviruses, and security software.

Steve: Yup. Yup. Now, okay. So stepping back from that, I just want to say, again, I've got Vista installed. I really do, I mean, it's a pretty OS. It's got a nice sort of flat look. I'm not that impressed with the translucent, you know, window headers that blur what's behind them. It's like, okay, gee whiz, you know, whoopy-do, I mean...

Leo: Yeah, and you can turn that off. You're not...

Steve: And I did, I did get a more – I've got better graphics performance that way.

Leo: Yeah, yeah.

Steve: So I've created two users, one where I bolted down the UI as much as possible. But even so, you know, it's really slow. So yes, I'm hoping what they're shipping is going to be faster. Although notice that RC2 was not much earlier than the RTM. I mean, what, it was like two weeks.

Leo: Right.

Steve: So it's not like the one I'm using was from six months ago.

Leo: No no no no no.

Steve: The one I'm using was from late October.

Leo: Right, right.

Steve: So, you know, again, I'm the reverse of an early adopter because, yes, I'm still on 2000, and I'll be moving to XP, you know, one of these days. But, okay. So, and I have to say also that IE has crashed. Any time I log out of the system, it crashes. It just drops right out for the BIOS and reboots. I mean, I've gotten a whole bunch of crashes of this code which, you know, was supposedly pretty mature. And this is on a system that as far as I can tell is just working perfectly. So, you know, I'm not blaming my hardware.

I also want to mention before I forget that I have been using Parallels on the Mac with an XP install, and I am really impressed. I'm becoming more and more impressed with Parallels the more I use it. You know, we've talked about this before and how Mark Thompson was saying that, you know, he thought Parallels' performance, even on a PC, on a standard Windows host platform, far exceeded what VMware was doing. So really I think VMware's advantage is the stuff they've got locked up in patents, you know, all of the incremental snapshots and rollbacks and things which they clearly have a patent on, and which no other VM application is able to do because of infringement against that.

Leo: Right, right.

Steve: But, you know, but just in terms of running Windows on a Mac, as far as I can tell it runs absolutely full speed. I don't see any difference. However, I was unable to install the RC2 of Vista. Apparently it's still very finicky. RC1 of Vista would install under Parallels, but only after the Parallels guys, like, fixed it so that it would work. And I was getting blue screens when I'm – oh, that reminds me, Leo. Vista has removed the blue screen by turning it into a dialogue. Instead of...

Leo: Instead of blue screen of death.

Steve: And it even says "blue screen." They, like, kept the term. It pops up a dialogue. And in there in the dialogue text it says...

Leo: It says "blue screen"?

Steve: ..."You've just had a blue screen." It's like, okay.

Leo: Uh, wow.

Steve: Yeah. So...

Leo: That's like when Apple took out the Error 11 by just renaming it. We don't have to fix this software, just take out the error message.

Steve: Yeah, because we don't want to see that anymore.

Leo: No, we don't want to see that.

Steve: So anyway, I like the – I like the Vista UI. I like the decisions that Microsoft has made from a policy standpoint. I'm scared of what they've done recoding huge network-facing, you know, Internet-facing aspects of Vista. We don't even know about the whole peer-to-peer thing yet. But so let's talk about what Microsoft has deliberately done in terms of Vista security, you know, what's new. We saw in the release of Service Pack 2 with XP the so-called Windows Security Center, which sort of continuously monitors your security-related things, like your firewall, automatic updates, and antivirus. That aspect has been expanded in Vista to include Windows Defender, which is Microsoft's malware scanner. And I've got to say, you know, as you and I have said before, you know, we don't run anti-spyware stuff. I discovered from the log that this Vista system was running Windows Defender scan in the wee hours of the morning on the days that I left it on...

Leo: Right.

Steve: ...all by itself. So it was performing this sort of scan. And it's, again, it's pretty nice to have a scan built into Windows, not some third-party add-on which is sinking its tendrils down deep into the kernel and who knows what, slowing things down and just, you know, basically having a problem coexisting with everything else Windows is doing. So, I mean, I imagine that, you know, ten years from now when I actually upgrade to using Vista myself, that I'll be very happy just using the built-in malware scanner that Vista has.

Leo: Yeah, I've been pretty happy with it. Of course you and I both know what to do not to get the malware in the first place, so...

Steve: Right.

Leo: ...we're not really taxing this thing.

Steve: So we haven't – exactly. We have not been having that problem. Certainly, though, users who have not been doing anything proactive like that security-wise, and who are picking up malware that Microsoft knows about, I mean, this thing updates itself continuously so it's being kept apprised of the latest problems. You know, this is going to be really helping people. So I think this is a very, you know, proactive major good thing.

I mean, a perfect example is that, even though personal firewalls existed way before Windows

XP Service Pack 2, even in the era of personal firewalls, we were getting all those worm wars, Code Red and Nimda and Blaster, because people had them turned off, or they had been subverted, or they just weren't using them. As soon as Service Pack 2 happened, where the firewall was part of the OS and turned on by default, all of that problem went away.

Similarly, as soon as Vista happens, with Windows Defender built in, able to and doing automatic background updates and scanning for the user in the background, I think we're going to see a sea change in the whole spyware/malware problem. I mean, I think it's going to make a huge difference for this thing to be built into every version of, I mean, every version and copy of Windows that ships. So, you know, I take my hat off to Microsoft. Certainly the people who are competing with Microsoft in this space, in this application space are not happy about this. But they had many years of, you know, of lots of profit and a good long run. And it really is a pro-user thing that Microsoft is doing, much as adding, you know, an always-on firewall to the OS has been a very pro-user thing.

Leo: Right, right.

Steve: So one of the other things that Microsoft has done is Vista incorporates something called BitLocker. It's sort of – I like sort of the double entendre of that. It's locking your bits, and it's also storage. It's a locker that stores your bits.

Leo: Oh, I get it.

Steve: It, yeah, it is built-in whole volume encryption that can work two ways. If you've got a TPM, a Trusted Platform Module, built into your system, you know – and we've talked about TPM before, how it's sort of controversial because, you know, from a privacy standpoint, basically what TPM does is it's pre-boot technology that was going to solve a lot of problems. And in this case the TPM system is able to authenticate you through the operating system and enable on-the-fly decryption of the main OS volume. Now, BitLocker requires its own partition because it has to run prior to installing on-the-fly decryption. But this is very much like built-in TrueCrypt sort of technology, where everything written to the drive is encrypted on the fly. Everything read from it is decrypted on the fly.

The reason, again, that this is a good thing is that, because it's there by default and from Microsoft and present, it'll probably see more use. The great use, of course, is on laptop systems, and we've talked about this often, the problem of them being stolen. Now, the problem, of course, is systems that don't have the TPM, the Trusted Platform Module, installed, you know, present in their system, they need to fall back to a secondary but still sort of elegant solution, and that is the decryption key can be stored on a USB, a small USB drive. And you must then, for example, on a laptop that was set up, or on a main desktop, you must have that USB key installed, and your BIOS needs to be able to access that USB key at boot time.

So there are some requirements. But most motherboards and laptops made in the last few years have been able to boot from USB and access the USB device in the BIOS and not needing, you know, fancy Windows drivers in order to do that. So essentially your USB dongle becomes your key. And you boot your laptop with the key in place, and Windows will perform on the – this whole BitLocker technology will cause Windows to perform on-the-fly decryption for you, and, you know, you're good to go. And this, of course, can also be used with a desktop. Because it requires two partitions, it's not as easy to set up as it could be. But you can imagine that in the short term, maybe from the beginning, laptops and new desktop systems shipped from OEMs will be partitioned to be BitLocker-compatible in this fashion. So I would imagine that they should work without any trouble.

So it is nice, on-the-fly decryption technology. And what it prevents is the problem of, for example, removing a drive from a system and putting it into another drive and using, you know, NTFS-aware drivers to access a drive underneath the security system. You know, it's one thing not to be able to access the drive if you're a non-privileged user. But it's always been the case that you could access the drive from outside the operating system, and that's always been a problem. This basically encrypts the entire system volume, with all your apps and all your data, you know, basically giving a complete wrapper around the system in Vista. So again, hats off to Microsoft. This is a really good thing.

Leo: Although, I mean, we still probably would recommend TrueCrypt. It's just nice to – once it's built into the OS, more people will use it, I guess.

Steve: Well, and that's exactly my point. And corporations will be far more...

Leo: They'll feel comfortable with it, yeah.

Steve: Exactly, far more enabled to have this technology running and working on those laptops. But again, it requires Vista, and I'm not going to be there anytime soon. I don't know about the rest of our listeners. But, you know, not me.

Leo: I'll be there. Don't worry, folks. Steve can hang out. He's still running Windows 2000. I'll be running Vista the minute I can buy it. Although now you're making me think about how to buy it, whether I should buy 32 or 64. But we'll get to that.

Steve: Okay, let's talk about that now.

Leo: Okay.

Steve: Several major new security systems in Vista to protect the kernel. We've talked about rootkits. We know how big a problem rootkits are. We've talked about Blue Pill, the idea of running a program that just silently subverts your OS by sort of slipping in a hypervisor shim that the system doesn't even know about. Nothing hiccups, nothing happens; but, you know, your system's been taken over. Of course, the famous Sony rootkit DRM issue that we talked about a long time ago, where it turned out it had a problem that was allowing malicious exploitation of it, in addition to being a bunch of software that was being installed and then using rootkit technology to hide itself. So, you know, we've talked many times from different directions about kernel modifications. And we talked recently a couple weeks ago about the issue that the AV vendors like Symantec and McAfee and others were having over the news that the tricks they were using would no longer be permitted. And there was some confusion at the time about, well, was Microsoft going to create an API that would allow them to modify the kernel, that is, you know, give them, like, somehow some means of authenticating themselves in order to allow those modifications. The good news is, no.

Leo: Rightly so.

Steve: No.

Leo: Stay out of my kernel.

Steve: Now, one of the things that has been...

Leo: Now, that's true only in 64-bit, though; is that right?

Steve: Yes, that's where I'm going right now.

Leo: Yeah.

Steve: One of the things that's always been true of Microsoft is they have gone out of their way for forward compatibility, or reverse compatibility, whichever direction you're looking. That is to say, as they come out with new stuff, they really go to extreme lengths not to break old stuff.

Leo: Right.

Steve: In fact, one of Mark Thompson's complaints about Apple is that Apple is far more willing to break older things and say, well, sorry, we broke that, so upgrade your software or stop using that or something. Microsoft really, really tries desperately hard not to break anything that they've ever offered.

Leo: Which is why your 15-year-old copy of Wizards of Might and Magic still works on Windows XP.

Steve: And interestingly, it's why them removing full raw sockets from Windows XP, as I was begging them to do, it took them several, well, it took them two service packs and several years because they realized, I mean, and even then it was controversial because they were taking something out that was going to break software, and a bunch of software did break. But...

Leo: They don't like to do that, yeah.

Steve: But they really don't want to do that. So two things have appeared in 64-bit versions of Vista and only 64-bit versions. And that is, all kernel drivers must be signed. Now, signing kernel drivers is always a good thing because it's just nice, it's nice to see where stuff that's down in the kernel, I mean, that has installed itself and become a part of the operating system, you know, you'd like to know that it really came from NVIDIA or from Microsoft or from Symantec or whomever. And an unsigned driver is always suspicious, especially since Microsoft signs all of theirs. You're able to look at the version information and verify the digital certificate of any of the drivers coming from Microsoft.

The problem is that with – and driver signing appeared in and began to be really active in Windows 2000. But it was not enforced. It is possible to use what's called a "group policy editor" to enforce only the loading of signed drivers, and for Windows, even Windows 32-bit Windows, you know, current Windows XP and 2000, to refuse to load unsigned drivers. The problem is you can't do a lot of things because, since by default Windows 32-bit Windows, all versions of 32-bit Windows will load unsigned kernel drivers without complaint, most manufacturers never bothered to sign them. And in fact...

Leo: Does it cost them money to sign it? To get them signed?

Steve: Yes. And it annoys me that, you know, for example, I've got Authenticode credentials that allow me to sign all my apps. And my older ones are not signed. My newer ones are signed. And I think it's, like, $700 a year that I have to pay for that privilege. And, you know, it's just for some bits of code that goes directly, you know, and the dollars goes directly into Microsoft's pocket. So it annoys me. But at the same time, I want that Authenticode signature to mean something. And in order for it not to just be spoofed and made up, Microsoft goes to some measures to verify that I am who I am. And so you could argue, well, that takes, you know, time and effort on their part. So they're getting – they are doing something for the money that I'm paying them. So...

Leo: Well, that's a good thing.

Steve: But largely, largely code is not signed.

Leo: Right.

Steve: And increasingly there will be pressure on people to have their code signed. You may remember...

Leo: As absolutely should be. I mean...

Steve: Yes. You may remember that one of my comments about MojoPac that I made back to the MojoPac people was, hey, this is not signed. It's dumb for any high-volume downloadable software not to be signed because IE will bring up a dialogue and say this is an unknown publisher. That is the only way for software to prove its publisher is for that publisher to obtain Authenticode credentials and to take the trouble and time to sign their code.

Leo: It's funny, this has been around something like ten years.

Steve: Yes.

Leo: And it's about time they kind of enforced it.

Steve: Well, what's going to be enforced finally is this functionality for the 64-bit kernel. Now, as you mentioned, Leo, XP 64-bit has been around for, what, a year and a half or so? And because they are enforcing signed drivers, a lot of publishers just said, oh, well, we're not going to do 64□bit support right now. So it hasn ’t really taken off because, as you said, it's a problem.

Well, Vista is going to require signed drivers. And there is no exception to it, no way to turn it off, no way to circumvent it. So, and Microsoft's thinking is this, okay, 32-bit applications will still run fine on a 64-bit platform, in the same way that 16-bit Windows applications worked fine under, you know, Windows 95 and 98 and so forth, and of course NT and all of its children. So there isn't an application portability problem because you're able to emulate the prior API set on top of the operating system. You cannot do this with kernel code. Kernel code inherently has to be rewritten from scratch. So no 32-bit drivers can run. No 32-bit kernel drivers can be used in a 64-bit kernel. So Microsoft's feeling is, okay, we're not breaking anyone's existing drivers. We're simply saying you're going to have to get your drivers signed in order to load them in the kernel.

Leo: Now, just to clarify, the signing is required for 64□bit Vista, not for 32 -bit Vista.

Steve: Correct.

Leo: Okay.

Steve: Correct. So from the start, what this means is that the 64-bit kernel will be protecting itself by requiring signing. Now...

Leo: It also means that a lot of things won't work.

Steve: Well, no, because...

Leo: You'll have to get 64-bit specific drivers.

Steve: Which you would have had to get anyway.

Leo: Anyway, okay, okay.

Steve: I mean, and that's my point is that this isn't breaking anything.

Leo: Got it.

Steve: This is...

Leo: It just means a lot of hardware won't work because there'll be no driver.

Steve: Exactly. But again, it wouldn't work anyway until the hardware had 64-bit support.

Leo: Right, right.

Steve: Because 32-bit support won’t work...

Leo: Wouldn’t do it, okay.

Steve: ...in a 64-bit platform.

Leo: Got it, got it.

Steve: So, and it’s certainly the case that 64 bits is coming. Now, here I am, you know, and when I started thinking about this it’s like, okay, wait a minute. 64 bits. I mean, 32 bits seems like ought to be plenty. But we’d like to have more RAM because there are big server applications, and there are, you know, big iron applications where four gigs of directly addressable RAM is beginning to be not a lot anymore.

Leo: That’s the current limit for 32-bit platforms.

Steve: Yes. A 32-bit word, or dword, as it’s called, a double word, 32 bits has four billion different bit combinations. And so that allows you to access four gigabytes, four billion bytes of RAM. And that’s the limit for 32-bit direct addressing. Now, sure, we could play games the way we once did in the old days when we, you know, when we had 640K limit on memory with...

Leo: You could page stuff in and out and...

Steve: Exactly, expanded memory and extended memory and all that. But that’s just not going to happen anymore. I mean...

Leo: Well, so what else do we get from 64 bit? We get four gigs, more than four gigs of memory.

Steve: We get more than four gigs of memory. And the other major feature is what’s called “Kernel Patch Protection,” or KPP. And this is really controversial. But it’s controversial because it is so important and so powerful. What this means is that the 64-bit kernel will no longer ever allow itself to be patched. Now, every personal firewall is doing this now in 32 bits. It’s the only way personal firewalls are able to hook into the network layer where they need to in order to block incoming traffic because applications don’t have that ability. So every personal firewall, the AV programs that have taken advantage of this kind of access, which has always been unfettered in all prior versions of Windows, 16 and 32 bits, Microsoft has flatly said that ends now. That ends at the 64-bit switch into the kernel.

Leo: I think that’s fine.

Steve: It is.

Leo: Now, this is the thing that Symantec and Adobe were complaining about; right?

Steve: Yes. Because they would like the freedom to do this. And they've proposed various ways of, like, signing their privileges, I mean, basically using some sort of...

Leo: It's okay, it's us.

Steve: ...crypto – exactly. The problem is, any – and this is what we said when we talked about this a few weeks ago for the first time, Leo, is, you know, it was just like, oh, no, don't, I mean...

Leo: Don't let 'em.

Steve: Don't let 'em. Because there is no way, if you create exceptions, that the hackers will not find a way around those exceptions.

Leo: And Microsoft seems to have come up with a good compromise, which is, okay, 32 bit, we won't enforce kernel patch protection. We'll just do it in 64 bit.

Steve: Well, because they can't. They literally, they can't do it in 32 bit because...

Leo: Oh, I didn't know that. Oh.

Steve: Well, because it would break everything.

Leo: Oh, yeah, yeah, yeah.

Steve: Nothing would work.

Leo: But they kind of hinted that they would at first, it sounded like. And then they backed off.

Steve: Well, what they've done is they have created a new set of APIs. There is – the really new thing, they call it WFP, the Windows Filtering Platform, is a way for applications to reach down and get legitimate access to the raw network traffic. So that, for example, personal firewalls, they'll need to be redesigned around this new API. But it's a completely clean, non-kernel patching way for those applications to function. So basically the manufacturers are complaining because they would like to continue breaking the rules. I mean, and this...

Leo: Ha ha, you can't.

Steve: Any, you know, this is rootkit technology.

Leo: Right.

Steve: And what this means is that 64-bit Windows will be rootkit safe. It will be rootkit protected. People will not...

Leo: Well, be careful when you say that.

Steve: I know. You will not be able to modify the kernel. Now, the next thing that Microsoft is going to do, and this is not happening now, but because they've made this rigorous, no-exceptions policy, it means that they will be able to seamlessly create a hypervisor when they bring out their forthcoming hypervisor technology and use the chip's hardware to enforce a non-modified kernel by absolutely locking down the writability of pages. So anyway, this is all really good news. But it does mean that people may want to consider whether it's worth holding off for 64 bits, because 64 bits...

Leo: Now, there aren't that many 64-bit processors. AMD has a few. In fact, I'm running on my Shuttle PC the 64FX. And then there's the Opteron and Sempron. And Intel has the Xeons. But these are workstation-grade computers. These aren't in widespread use yet.

Steve: Right. And so it's certainly going to take some time for these things to come down. So I guess I'm saying, if people are wanting – if they try to run Vista on their current hardware, I'm going to be very surprised, if it's what I've been seeing in RC2, if it provides acceptable performance. That's going to induce people to say, well, boy...

Leo: They're going to upgrade anyway.

Steve: ...I guess I need, exactly, I need more hardware. So I'm hoping that this will also – this will create a market for 64-bit systems which will begin then to – and so the software manufacturers will start supporting 64-bit drivers, we'll start seeing some volume of 64-bit chips. That'll inevitably bring the price down, you know, and...

Leo: Yeah, because I just spec'd out a Dell server, workstation, 64-bit Xeon workstation, and that was four grand by the time I was done.

Steve: Yes. Yes.

Leo: Yeah. And of course I'm not going to order it because I'm waiting for Vista to come out. But as soon as Vista's out, I have to say, Steve, I'm probably going to do it. And now you've convinced me that I should go with a Xeon or a 64-bit AMD.

Steve: Oh, boy. From everything I've seen – and again, I'm glad you kept reminding me about the caveat that this was RC2. This was not final code. On the other hand, it was only two weeks old. And, you know, this thing did not seem very stable. And it, boy, did it not seem very fast. So, you know, I'll have it, too. I'll have Vista running. We'll be able to poke at it. And, you know, we need to be able to talk to our listeners about it. But in terms of me using it on my main system, no. I'll be moving to XP.

Leo: Also something to be aware of, you may be getting new peripherals because, if the manufacturers of those peripherals don't do 64-bit Vista drivers, you won't be able to use them. So if you're going 64 bit, we're talking a fairly steep expenditure. And not just a new computer, but you may be getting new printers and scanners and so forth, as well.

Steve: Yeah, so looking at this the other direction, for people who are still wanting to run Vista on 32-bit systems, there is not a huge change in what Microsoft was able to do in terms of really improving the system's security. Yes, you've got your firewall. Yes, you've got malware scanning built in now. Yes, you've got the equivalent of TrueCrypt in what they're calling BitLocker to do on-the-fly decryption of the whole volume. But there's no kernel protection and no driver signing that Microsoft is able to bring into the 32-bit Vista world because so many people have unsigned drivers and are messing with the kernel that it would just break too much. And Microsoft said, no, we're not going to be able to make that change.

Leo: You might frankly want to think of Vista 32-bit as compatibility-mode Vista, and 64-bit as incompatibility, but secure-mode Vista.

Steve: Right. And, I mean, it's necessary to break some eggs to make the omelet.

Leo: Well, and that's why Mac users have benefited a little bit. Now, ironically, I'm using a 32-bit OS on a 64-bit Xeon on my Mac. But Leopard will be 64 bit, fully at 64 bit. So right about the same time Vista comes out, just shortly after that. We'll all be going 64 bit someday.

Well, Steve, thank you very much. We want to thank also our major sponsors who provide funding for this show: Astaro Corporation, makers of the Astaro Security Gateway. If your small or medium business network needs superior protection from spam, from viruses, from hackers, complete VPN – I use the VPN all the time, it's really nice to have VPN – intrusion protection, content filtering – very important in small business – and an industrial-strength firewall, all in a simple, easy-to-use, high-performance appliance, great power at a great price, contact Astaro, Astaro.com. You can call 877-4AS-TARO, and they'll schedule a free trial of an Astaro Security Gateway appliance in your business. I recommend them. I'm using the 120 and love it. Also, frankly, if you're a non-business user, you can get the software absolutely free at Astaro.com and get many of the benefits on some old beater that you've got lying around. Just put Astaro on it. Thank you to Astaro for their support. Astaro.com.

Also thanks to Dell. I've been pricing them out. I'm going to have to put a 64-bit Dell system now in the Leo's Picks page at TWiT.tv/dell. And I will, I'll put a – you know, I was – I told you last week I'm getting an XPS 700. You just convinced me, Steve, not to. And I'm going to go with a Xeon because I want to have that 64 bit.

Steve: I think it's worth being on the leading edge in that case.

Leo: Yeah. Oh, and I'm going to tell you, these are nice machines. They're not as inexpensive. But, you know, you get good Dell quality. If you want to know more, I'll put my pick for a 64-bit machine, along with some other more affordable prices, affordable choices for desktops and laptops on the Leo's Picks page. It's TWiT.tv/dell. And if you're about to buy a Dell, want to get a new Vista Windows machine, make sure you go through that link so that we get credit for you. TWiT.tv/dell. We thank Dell and Astaro for their support of this podcast.

Of course, Steve's website is the place to go for show notes, 16KB versions of this program, and of course full transcripts for those who like to read along while they listen, thanks to Elaine. GRC.com, the home of SpinRite, everybody's favorite disk recovery and maintenance utility. Any interesting SpinRite correspondence?

Steve: I've got another really fun story, but I'm going to save it for next week, Leo.

Leo: Okay. Okay. I understand, Steve. Hold out on us. If you want to read some of the older ones, though, SpinRite.info is the place to go for that. I just – I think everybody who has a hard – if you have a hard drive, you ought to have SpinRite.

Steve, it's been a great pleasure. We will see you next week for another edition of Security Now!.