SECURITY NOW!

Transcript of Episode #67

Kernel Patch Protection

Description: Steve and Leo first discuss errata from previous episodes, correcting, among other things, Steve's first poor impression of Vista's performance. Then they discuss the results of Steve's in-depth research into the inner workings of Vista's Kernel Patch Protection (aka PatchGuard) to uncover its limitations, benefits, and real purpose.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-067.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-067-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 67 for November 23, 2006: The Problem With PatchGuard.

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.

Well, the turkey dinner's over, the football game's done. Maybe it's time to turn on a podcast or two. And you've made the right choice, my friend, because it's time for Security Now! with Steve Gibson. Hello, Steve. Happy Thanksgiving Day.

Steve Gibson: Hey, Leo. Great to be here. This is our Thanksgiving Day edition. On Thursday.

Leo: Yeah. I always think of the big, you know, football game, and the snows were coming down at Lambeau Field when the – you know. And I really feel like this is it. This is a – we have to have some dramatic music [singing]. Or maybe not. You know, and it's only in the United States. And they've already had Thanksgiving a month ago in Canada, and the rest of the world they're going, Thankswhating?

Steve: Yeah, yeah.

Leo: So we must go on. We must soldier on because we are an international podcast. No U.S. holidays for us, my friend.

Steve: Yup.

Leo: What is our topic of the moment?

Steve: Well, we got – I want to talk about, well, that we've got a bunch of errata stuff. And I want to talk about, in general, I want to really focus this week on Vista's Kernel Patch Protection.

Leo: Okay.

Steve: Because believe it or not, it's already been hacked, and it doesn't work.

Leo: Oh, boy. All right. Well, we'll get to that in a second.

Steve: Yeah.

Leo: But let's start by clearing up any issues from previous episodes here.

Steve: Yeah, a bunch of stuff. One thing that happened was last week I mentioned – or maybe it was the week before – that very cool little freeware utility, allSnap. Unfort-...

Leo: Which we killed.

Steve: Which we completely killed. Unfortunately there's a – most of the Google links point to an old site, which is on GeoCities. And almost immediately we – our mention of allSnap burned up the bandwidth, and they shut down the site. You know, they got slashdotted, essentially. I wrote to the author. I started serving the file myself so that we wouldn't zap GeoCities. Bunch of people downloaded it. And he explained, the author explained that he'd actually moved it. He's Canadian, I can't – I think at, like, University of Toronto or somewhere.

Leo: Oh, neat.

Steve: I don't remember exactly where now. But anyway, so it's back up and around. And I just wanted to mention to anybody who might have tried to go there following the podcast and not been able to get it that I will on this week's show notes continue the link to the most recent version myself, and also put a link to the original site. Because it is just a really cool little gizmo.

Leo: I was amazed because to me it's like, okay, fine. But obviously you are not alone in your love for this program.

Steve: It's just cool to have the windows lock themselves to the screen borders. I just really like that.

Leo: Okay.

Steve: Also I misspoke – again, it was either last week or the week before. Because we recorded two together, I'm sort of muddy in my mind which one was which. But I mentioned that – confirmed that accessing Gmail remotely over a secure SSL connection worked, and you could set up an email client that way. The problem was, I stumbled over the issue of anonymity. And it's really dumb, too, because you may remember, Leo, that I – one of my trips to Toronto I talked about the three main browser-based email systems, Yahoo!, Hotmail, and Gmail; and that only Google mail, when you accessed them through a web browser, was anonymous; that if you sent email using either Hotmail or Yahoo!, in the headers of the received mail was the IP address from which the user was accessing Hotmail or Yahoo!'s website, making it not anonymous in that sense.

Leo: It puts that in the headers. Wow.

Steve: Yes.

Leo: Wow.

Steve: Just sort of embeds it gratuitously. Now, Gmail doesn't. And so I got that backwards because I said that using a remote SSL connection you still had the benefit of that anonymity, and you don't. So if you are using an email, a regular email client – Outlook, Eudora, you know, whatever – and accessing Gmail and assuming that you are maintaining that IP-level anonymity, that's not the case. In order to get that with Google Mail, and it's the only one of those three that does, you need to access it through a web browser and do your work there, if you don't want the recipient to be able to easily see what IP address you were at when you sent the mail. So I wanted to correct that.

Leo: It's really – it is counterintuitive because you'd think, if you're not using a browser, why would it do that? If you're using a standard POP client, why would it embed the IP address? But...

Steve: Ah. Well, actually the reason is it has to. And the whole reason these IP addresses are embedded is that headers are appended as mail moves from one SMTP server to the next. And you need to prevent routing loops, or email forwarding loops. So, and when mail arrives at an SMTP server, it checks all of the received headers which are appended as the mail is moved from one server to the next to see if it has already received that mail. So it is necessary as a precaution for Gmail to do that, so it makes sense. I just wanted to make sure, you know, that I corrected that because I wouldn't want people to think that they were more safe than they are. They're not as safe using Gmail through a remote client as they are from an anonymity standpoint of masking their actual connection IP when they use Gmail through the web browser.

Leo: And you'd need to use HTTPS through the web browser, and not just HTTP.

Steve: Well, yeah. That won't affect your anonymity. But of course you'd just as soon have a secure connection so nobody could be, you know, eavesdropping on you, your connection to Gmail.

Leo: So it doesn't embed the IP even if you're using the standard nonsecure Gmail.

Steve: Correct.

Leo: Okay.

Steve: Also we talked several weeks ago about that new exploit and vulnerability which was being exploited in the XML, the Windows XML core services. I did want to confirm to people that that was patched in Microsoft's Second Tuesday of November patch cycle because we were telling people, you know, if they were at high risk of that kind of exploit, to, you know, you might want to set that kill bit. So people could go back now and remove it. On the other hand, you know, invoking this particular ActiveX control through a web browser is a purely exploitive thing to do. It's not functionality that you could conceivably even need through your web browser. So you could probably just leave it there if you wanted to.

Leo: Harmless to leave the change.

Steve: But what's interesting is there's a new exploit, not in a Microsoft ActiveX control. And this is sort of – this is a scary sort of thing to come in the future. Get this. The WinZip FileView ActiveX control has a vulnerability, and in the same way that this non-browser-oriented XML core services ActiveX control which was exploited a few weeks ago and we talked about, in the same way that it can be invoked through the browser, so can WinZip's vulnerable FileView ActiveX control.

Leo: Don't you get a certificate, though, a permissions request?

Steve: Not that I've heard of. Apparently it...

Leo: I thought that was what was supposed to protect you against these ActiveX controls, is if you go to a website with an active – embedded ActiveX control, it asks permission before running.

Steve: Ah, but that's where it's providing you the control. Here...

Leo: Ah, the control's not coming from the website, it's coming from your system.

Steve: Exactly. And that's a problem. And that's a problem with widely deployed third-party software like WinZip. I mean, WinZip is very popular. I've got it on all my machines. And so, you know, here's WinZip bringing along an ActiveX control which has a vulnerability. So, I mean, this is really sort of the next generation of problems we're going to be facing is, you know, once Microsoft gets themselves all battened down, unfortunately the technology Microsoft has created is so powerful that now websites are able to reach through your browser into – literally into the guts of Windows and invoke other components of Windows that were never intended to be used through the Internet.

Leo: Wow. Oh, so this file browser wasn't intended to be used that way.

Steve: No.

Leo: Oh, interesting.

Steve: No, it's just a random ActiveX component that someone found a vulnerability in, which you can ask Internet Explorer to invoke for you.

Leo: Just launch that for me. Do we still have this bit that we can set to prevent that?

Steve: Yes, there is a kill bit. And in fact, it's any version of WinZip 10.0 prior to build 7245. It's important to note that they've already fixed this. So the best thing to do is just to update yourself. Anyone using WinZip, update to the latest version of WinZip, and a build from 7245 or later, and you'll be okay.

Leo: Got it. Great. Okay.

Steve: Now, another thing is that we were talking last week about 32- and 64-bit stuff. And many people wrote to both you and me...

Leo: I got a lot of email, a lot of email. Holy cow.

Steve: Yeah, well, I listened to TWiT on Sunday, Leo. And so I heard you, you know, early in the show you talked about, oh, yeah, I'm going to have to talk about this. And then you got around to it later on.

Leo: Yeah.

Steve: What I wanted to make clear to people was that it's not just these Xeon, you know, the high-end, server-level processors that have support for 64-bit technology.

Leo: Pretty much it's any modern processor now; right?

Steve: Yes, for a number of years many of the – the Pentium 4, the Celeron D, the Pentium D processors have included this technology. Intel calls it EM64T, which stands for Extended Memory 64 Technology. And so basically it's, you know, it is full 64-bit technology running inside of the chip that can be turned on. And in fact, you know, 64-bit Windows, 64-bit operating systems are now able to use that. And of course Vista, the 64-bit version of Vista, if you happen to have one of these late-model Pentium 4, Pentium D, or Celeron Ds, and it's not all of them, it's only some of them...

Leo: Also the AMD chips, the Turions, many...

Steve: Yes.

Leo: In fact, I have – I'm sitting right next to an AMD FX64, which I knew was a 64-bit chip. I don't know what – I was just having a brain seizure.

Steve: Well, I mean...

Leo: I mean, I've had this 64-bit chip for a year. Really the point, though, of compatibility is not so much the chip. I mean, yes, you have to have a 64-bit chip. But then everything else has to be compatible. It's not enough just to say, well, does it have a 64-bit chip.

Steve: Well, actually you also have to have a 64-bit-aware BIOS. And so if you took an older BIOS and put a newer chip in it, that is, you happened to have a chip with this EM64T technology, if the BIOS wasn't aware, then you still, you know, Vista would still not be able to work on that. So, you know, and exactly as you said, it's – I mean, the real thing that's slowing down the adoption of this, and the reason people aren't just turning on the 64-bit emulation instruction set within their chips, is that there's a real dearth still of 64-bit drivers...

Leo: It's all about drivers, yeah.

Steve: ...for, like, you know, all the hardware. It really is.

Leo: Yeah, okay. Well, thank you. I was a fool. I was a fool. And I learned very quickly. I was told many times.

Steve: Well, I was first going to call this episode "Embracing Vista," before I really took a look closer at kernel patch protection. But we also need to revisit – and this is still in the errata category – the performance of Windows Vista.

Leo: Because you were saying you had terrible performance.

Steve: Well, and I did have terrible performance on RC2, which was the – as I mentioned at the time, I wasn't sure if it was RC2-ness or if it was the fact that I was using an MSDN download that was just loaded with...

Leo: The debugger download.

Steve: ...the debugging code.

Leo: Yeah.

Steve: It turned – okay. So I wanted to absolutely and officially correct the record. Vista flies on this machine.

Leo: Okay.

Steve: I mean, it is...

Leo: Faster than XP?

Steve: Probably not faster than XP. It is bigger. But, I mean, it is fast enough on that machine that I built, that, you know, the Pentium 4, 3-gig, with the NVIDIA display, the machine I described a couple weeks ago, where I was just moaning and groaning and saying, well, who cares if it even works, it's so slow you can't even use it. All of that was due to RC2 and the fact that I was using the so-called "checked build," a debugging build.

Leo: Yeah.

Steve: I mean, it runs absolutely acceptably fast.

Leo: Good.

Steve: I am, I'm completely pleased with it. I even installed it, because I knew I was going to be, you know, correcting this presumption and this whole notion that it was so slow on this show, I installed it on my older HP Compaq TC1100 tablet. And it runs fine there. I don't get the fancy blurry interface, which, you know, the UI which I really dislike anyway. But, I mean, it runs at full speed. And even they do a bunch of really cool things for tablet PCs where, like, it gives you this little twinkly star cursor since you really don't need a cursor because you're using a stylus on the tablet. And when you touch it, a little ripple kind of comes out from the point.

Leo: Oooh.

Steve: Oh, I mean, it's just wonderful. So I don't know, I'm really happy with it from that standpoint. And as I laid the groundwork, I'm very happy with the security-related things Microsoft has done. So I want to talk about that.

But in my last little bit of errata, we got a really neat piece of email that talked not only – it was from a Security Now! listener – that talked not only about SpinRite, but believe it or not about Astaro. He said, "I subscribed to the Security Now! podcast a while back, and some of the information I've received as a result has been fantastic. Like many others, I have purchased a copy of SpinRite as a way of saying thank you for the real information you and Leo impart every week. Shortly thereafter I found myself in a situation where I had a dead system on my hands." He says, "I popped in the SpinRite CD, and 45 minutes later the system was back to its old self."

Leo: Yay.

Steve: Then he said, "I immediately purchased an additional three licenses to bring my office up to site-license status," which of course allows, you know, his whole office to use SpinRite whenever something like this happens. And he says, "Any product that can deliver that well is a must-have resource in my opinion." Then in his next paragraph he says, "I'd also like to thank you for allowing Astaro to sponsor your podcast. I have approximately 30 small satellite offices..."

Leo: Wow.

Steve: "...and was at my wit's end trying to gain control of inappropriate web surfing, as well as providing some form of firewall IDS solution," you know, intrusion detection solution, "I could manage from one location. After hearing their name over several episodes of Security Now!, I contacted Astaro and arranged for a demo box. Within a couple of weeks I had all the evidence I needed to make a case for their product."

Leo: Oh, good.

Steve: "We have 13 of the devices deployed already and will be rolling out an additional 18 over the next few weeks. Had I not heard their name on Security Now!, they would likely have never come to my attention, and we would have missed out on a great product. Thanks again for all the hard work."

Leo: Two great products, I've got to say.

Steve: Isn't that great?

Leo: So more at SpinRite.info. And of course SpinRite's available through Steve's site, GRC.com. It's a disk recovery and maintenance utility. Did I say "a," it really is "the" disk recovery and maintenance utility and is a must-have for anybody who wants to update their hard drive, keep an eye on it, maintain it, or very often recover it when the worst happens. As long as we're mentioning Astaro, let me do the Astaro ad, and then we'll get into our Vista kernel patch protection and how hacked it is. Oh, you scare me when you say that.

But we do want to thank Astaro for supporting the show. The Astaro Security Gateway is their product. If your small or medium business network needs superior protection from spam, from viruses, from hackers, complete VPN capabilities – which is how I use it, that's fantastic – you've got intrusion protection, you get content filtering, as you heard, and an industrial-strength firewall, all in a very easy-to-use, high-performance appliance, contact Astaro, that's Astaro.com, or call 877-4AS-TARO to schedule a free trial of an Astaro Security Gateway appliance in your business. There is, by the way – and I really do want to emphasize this, in fact I should put the link in the show notes because I think people have said it's kind of hard to find – a free download for non-business users. So you could put it on your – actually, if you go to freshmeat or SourceForge, I think it's on there, too – you could put it on your, you know, beat-up PC, you know, and use that as a firewall, and it does all the same thing. In fact, if you pay the subscription, you even get the antivirus and the antispam and all the other commercial features. So, and it's a very reasonable deal, I think. The yearly price is very, very affordable. Astaro.com. We thank them for their support of the podcast.

So now let's talk about the Vista kernel patch protection. This is the thing that's been controversial up to now. Isn't this the thing that Symantec...

Steve: Yup.

Leo: ...and Adobe and others were complaining that they didn't have access to the kernel?

Steve: Yup. Now, I want to make sure people understand that I am pro Vista from a security standpoint. I mean, I'm worried about the fact that apparently they rewrote the network stack from scratch. We've talked about that, you know, in our episode called Vista's Virgin Stack, because it's so easy to recreate errors which have been resolved years before and to reintroduce these old problems. But the thing that encourages me about Vista, and we're going to be talking about it I'm sure, you know, off and on here now because, you know, it's important, is Microsoft has done a number of things which are policy-wise really pro security. You know, the best example of that that we've seen is when they finally turned on XP Service Pack 2's firewall by default. The moment that happened, the world changed. Because, you know, even though XP was out and XP had a firewall, and there were even third-party providers of firewalls, you still had all those worms. And the way the worms worked was having access to open incoming ports.

Leo: It's really becoming obvious that, in the Windows world, that inexperienced novice users are the real threat. If you're sophisticated, you know how to protect yourself. So having something be on by default is so important because it's not the experts we're worried about.

Steve: Yes. And so, for example, that's why I think it will clearly make a huge difference that Windows Defender is built into Vista, that is, that Windows will have a malware scanner built in. It'll update itself. It'll scan by itself. I mean, all that's turned on when anybody buys one of these new Vista machines in '07. So, I mean, it's really a good thing. Now, what's always been the case, unfortunately, since the very first version of Windows, is that Microsoft themselves used undocumented APIs that existed in their operating system that only they knew about. The developer community figured that out and started doing the same thing. And in the case of even later operating systems, for example...

Leo: You mean using Microsoft's undocumented APIs, not creating their own undocumented APIs.

Steve: Yes, correct. Yeah. Thank you for the clarification. Yes. Using Microsoft's – doing the same thing Microsoft was and using their undocumented APIs.

Leo: Which Microsoft said don't do.

Steve: They said don't do.

Leo: Don't do what we do.

Steve: Well, and they said, you know, we know what we're doing. So if we were to change the operating system so that those things went away, then...

Leo: We'd know.

Steve: We would know, so we would change what we were doing. Anyway, what has happened is there's been this – over the years a culture of the kernel has developed which just shows the kernel no respect at all. And...

Leo: Do you want to explain what the kernel is, how important the kernel is?

Steve: Well, I think we've really talked about that a lot.

Leo: Oh, okay.

Steve: And I want to – there's a lot of ground I want to cover here. So I don't want to diverge too much.

Leo: Suffice to say it's the basic part of the operating system, the most important part of the operating system.

Steve: Well, yeah, I mean, exactly. It is, you know, if you were to divide the operating system into the actual OS and then a lot of applications that come along with it. And then, of course, device drivers that are – that sort of become part of the OS. You know, this is what you get from Microsoft before you start adding applications. The problem is – and it provides all the fundamental services that make the computer go.

Well, the kernel has never gotten much respect because it hasn't protected itself from change. And even though Microsoft has said do not change, do not hack the kernel, Symantec and McAfee and Zone Labs and Kerio and literally everybody, you cannot build a personal firewall without breaking those rules. Because Microsoft until Vista has never given us the ability to hook into the operating system deeply to allow us to implement our own firewalls. So, for example, the only way to do a personal firewall has been to break the rule, break the official rules, and ignore Microsoft's admonishments about not hooking the kernel.

Now, the problem is that it's not just good software that hooks the kernel. It's, as we know, malware, you know, formerly known as rootkits. The famous now Sony DRM rootkit disaster, where they were installing – where Sony was secretly installing a rootkit when someone just played a Sony-published audio CD in order to enforce their DRM, that was doing the same thing. It was...

Leo: You had to modify the kernel to do that.

Steve: Yes, it was hiding itself by essentially hooking into the kernel and filtering, that is, you know, like looking at every single action that the OS was doing. And, for example, if you tried to do a directory listing, it would skip over the listing of itself. Well, the problem is, first of all, not only can this stuff be malicious, rootkits use this technology to hide themselves; but, if not properly implemented, they really can destabilize the operating system. You know, the classic case was, you know, the spyware that I first found, the [Aureate] spyware. It was badly written, and it hooked into Internet Explorer. And it damaged Internet Explorer. That is, Internet Explorer – it was so poorly written that it broke the OS. But because it was installed secretly, no one knew what had happened to their computer. It just, you know, Windows sort of started having a hard time.

And so I never expected that when I produced OptOut, my little free program to remove it, that we'd be getting mail back saying, well, you just fixed my computer. It was like, what? That's not what it was supposed to do. But it turned out that by removing this spyware which was secretly damaging their computer, their computer got better.

So what Microsoft has done with the 64-bit version of Vista, as we talked about before, is they have implemented something that they call their kernel patch protection, which has the nickname of PatchGuard. Now, they would desperately love to give this technology to the 32-bit platform, that is, to the Windows, you know, XP and Vista that runs on 32-bit hardware, but they can't. Because, exactly as I was saying, there is such pervasive use of this rule-breaking, kernel-modifying behavior that it would just, I mean, it would just scrap, I mean, even, you know, not even device drivers from Symantec and McAfee, but random printer drivers. I mean, obscure things you would never think would have any reason to modify the kernel turn out to have, just because the kernel has had no respect at all, they just go in and make little changes here and there. And, you know, mostly this stuff works. But it turns out it is implicated in destabilizing Windows.

Leo: Well, you could see what a mess this would make.

Steve: Well, and, I mean, it's phenomenal actually that it has worked as well as it has because, you know, people want their machines to work, and you put something in, and it breaks it, you take it out, and it fixes it. So it's like, okay, well, I'm not putting that in again. So what Microsoft has decided to do is they have said enough is enough. We are, with our 64-bit version, since that requires brand new kernel mode drivers, device drivers and code anyway, we are going to proactively enforce our statement that no one can modify the kernel. And that's...

Leo: We're going to keep you from doing it.

Steve: That's the difference, yes. We are going to proactively enforce it. Now, here's the problem with doing that. And this bears on a lot of the things we've talked about before. The kernel itself is trying to protect itself. That is, it's running at the same level of protection, the same protection domain, as the code which it's trying to protect against. This is fundamentally impossible to do.

Leo: Oh, no.

Steve: You can't – yes. You know, we...

Leo: That sounds bad. I don't know what that means, but it sounds bad.

Steve: Well, and a perfect example is, you know, like SSL, the Secure Sockets Layer, it's a public spec. Everybody can know exactly how it works. And knowing how it works doesn't allow an attacker to circumvent it. Okay? Knowing how PatchGuard works, that is, the Vista kernel patch protection, knowing how it works allows it to be circumvented. And so what – and again, Microsoft knows this. And so they've gone to extremes to obfuscate and to misdirect. They've got deliberately misnamed labels that are labeled something innocuous looking. They've got routines that do – that say they do one thing and actually do another. They create – they have a pseudorandom number generator that they initialize from something called the RDTSC, The Read Time Stamp Counter. That's a very high-resolution timer. Basically it counts every single clock cycle the processor had. So it creates a nice source of randomness. They use that to randomly scramble the PatchGuard data structures so that they can't easily be found in memory. But all of this exists in memory, and there are already white papers on the 'Net with sample code which circumvents PatchGuard.

Leo: This is what they call "security through obscurity." And...

Steve: Well, it is exactly security through obscurity.

Leo: And when you're a prime target like Windows, you can't expect that to hold very long.

Steve: Well, so here's what this means. And I want to – again, this is a tricky conceptual issue that I want to make sure I get really clear. The fact that it can be circumvented means a few things. But the fact that it's there at all means something else.

Okay. So first of all, Microsoft is proactively enforcing to publishers of commercial software like Symantec, like McAfee, like Zone Labs, like, I mean, anybody who in the past has been a deliberate kernel modifier, Microsoft is saying no, no more, it stops here at the 64-bit kernel, as we, you know, we wish we had done this when we went from 16 bits to 32 bits. We didn't. Well, we're doing it now. And so it's just like no more, we are going to proactively prevent this. Essentially what this means is anybody who does deliberately circumvent the PatchGuard does so truly at their own peril. And...

Leo: And you could presume that Symantec's not going to do this, McAfee's not going to do this, Zone Lab's not going to do it.

Steve: Exactly. I mean, what I like...

Leo: But guess who is going to do it?

Steve: Yes. But what I like about this is that it raises the bar to a point where the good guys really won't do this. The reason this is important is that this is not the end of kernel protection. What Microsoft will next do, and this is just sort of a stepping stone, is they will implement their own Blue Pill. We've talked about the Blue Pill before, how it essentially slips in a hypervisor that runs underneath the kernel in order to be, you know, like be a super rootkit. The next thing Microsoft will do is they will add hypervisor technology into some future version of Vista, which will finally then make this kludge which is PatchGuard unnecessary. The reason PatchGuard is a kludge is it isn't actually kernel patch prevention. It's kernel modification detection. What it does is it runs every five to ten minutes, randomly timed off of a timer in the kernel. One of the attacks of that is just to turn off the timer. And it turns out you can.

Leo: Oh.

Steve: You can find the timer...

Leo: You just in one sentence blew the whole thing, Steve.

Steve: ...and you can just turn it off. And there's...

Leo: Well, that's pathetic.

Steve: There's sample code on the 'Net for doing that.

Leo: And that works?

Steve: It works. It's been proven. It's been tested. It just turns off PatchGuard. Thank you very much. One of the other things that happens...

Leo: So it's very clear Microsoft must have known that this is not in any way secure.

Steve: Oh, absolutely.

Leo: This is just a way of saying to the good guys, you can't do this anymore.

Steve: It's a way of saying...

Leo: You'd have to be a bad guy to do it.

Steve: Yes. It's a way of saying to the good guys, we are really, really, really, really, really serious about thou shalt not touch the kernel. And so, from this position, Microsoft is now free to make kernel changes. See, they've been locked up in the past because everybody was going digging into the kernel, doing their own thing down there. Microsoft in the name of compatibility could never make any changes. Even though they said, please don't mess with the kernel, we want to be able to make changes, Microsoft couldn't. Because nothing is more important to Microsoft, bless their hearts, than keeping compatibility as they move forward. So now by doing this, by being proactive this way, they're able to say, you know, if you do anything like this, don't come crying to us because we guarantee you we will break things in the future. So what they've done is they've really created a boundary, and they've enforced it in a way that, yes, it can be defeated, it has been defeated.

Now, the other problem is that we really can't look at this today as really strong malware prevention. We can look at it as really strong good guy prevention, that is, it's going to prevent the commercial guys from making changes.

Leo: It's like putting a fence around a new lawn, saying "Keep Off the Grass."

Steve: Yes. And so...

Leo: And if you get on the grass, you're breaking that law. You can do it, but that makes you a bad guy.

Steve: And ultimately Microsoft will be able to leverage the hardware. See, again, we've got – we've talked about, like, ring 0 and ring 3, ring 0 being very privileged, ring 3 being where the user mode code runs. Code in a different privilege ring can be controlled. But we're talking about code, you know, device drivers modifying the kernel when the device driver is in the kernel. So by using, in the future, by using hypervisor technology, you know, virtual machine technology to supervise the kernel, it will be possible to lock down the kernel. But you could only do that if you knew the kernel had never before been modified. Because locking it down, if somebody were depending upon it being modified, that would render their software useless. So Microsoft is saying...

Leo: So baby steps. We're taking baby steps.

Steve: We're going to make it really, really, really hard to modify the kernel so that, if you do, you know, you have at your own peril. And then in the future we're going to really lock it down using hardware technology we have not yet deployed, which will not allow it to be modified. And that's where we'll get real malware prevention. We don't quite have it yet, but we're on our way. This is like an incremental step towards that. And again, I salute Microsoft. This is a really good thing they have done.

Leo: Kernel PatchGuard is not in 32-bit, though. It's only in 64-bit? Or is...

Steve: It's even been in – you're correct. It's even been in the 64-bit version of XP.

Leo: Oh, okay.

Steve: And so it's been running there. And in fact the...

Leo: That's why we know how it works, probably, yeah.

Steve: That's why it's been, exactly, so carefully looked at. And I'm sure, I mean, this is literally – it's cat and mouse. I'm sure when these papers came out Microsoft said, oh, let's work around those workarounds.

Leo: Right.

Steve: And then, you know, these guys just re-reverse engineer it and work around the workaround workarounds.

Leo: But let’s not get around to that because this is only an hour-long podcast. We’re not going to go on forever.

Steve: As a matter of – and our hour’s up, Leo.

Leo: Hey, well, that’s a really great explanation. And it does give me hope that not only is Microsoft, you know, understand the problem, but they’re, you know, it doesn’t happen overnight, but they’re making progress.

Steve: Yeah. I thought it was important not to oversell what PatchGuard does because I felt like I did that a couple weeks ago. I told people, oh, this prevents the kernel from being modified. I did a lot more research, and it’s like, well, okay, no...

Leo: Only by the good guys.

Steve: Exactly. I mean, it really raises the bar. And it does allow Microsoft to alter the kernel as they really need and ought to have the right to do for our own sake in the future.

Leo: Well, I know that I am actually now looking at Vista-capable hardware because it’s really time. And that’s why I’m going to Dell. And I encourage you to do the same. I’ve got my XPS 700. We got that for Call For Help. And now I’m looking for laptops. Almost all the Dell stuff now has that Vista Capable and Vista Premium Ready sticker, so you know what you’re getting. And the Vista Express Upgrade means you can upgrade to Vista the minute it’s available, January 30th. We encourage you, if you’re looking for a Windows machine, to go to TWiT.tv/dell to Leo’s Picks Page, click the links there. Whatever you buy once you go through that page we get credit for. And we do appreciate that. And we also appreciate the support of Dell for this program. That’s TWiT.tv/dell.

Steve Gibson’s website is GRC.com. That’s where of course you’ll find SpinRite, as we’ve mentioned. But not just SpinRite. Also the show notes, the 16KB versions of each episode for the bandwidth impaired, transcripts thanks to Elaine, a lot of useful information, and of course Steve’s wide-ranging list of free programs for your security. It’s GRC.com.

Steve, have a great Turkey Day.

Steve: Yes, Leo. I may have a surprise for people next week, speaking of my list of free programs.

Leo: Oh, he’s been working.

Steve: I’m really bad about pre-announcing things, so I’m not going to say anything. We’ll see what happens next week.

Leo: Steve’s been in the lab. We’ll find out what he’s got next week. We’ll see you next Thursday on Security Now!.