Vista's Virgin Stack

Description: Steve and Leo discuss the revelation, courtesy of a Symantec study and report, that Microsoft's forthcoming Vista operating system has a brand new, written from scratch, networking stack supporting old and new network protocols. They consider the sobering security consequences of Microsoft's decision to scrap Window's old but battled-hardened network stack in favor of one that's new and unproven.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-051.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-051-lq.mp3

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

This is Security Now! with Steve Gibson, Episode 51 for August 3, 2006: Vista's Virgin Stack.

Security Now! is brought to you by Astaro, makers of the Astaro Security Gateway, on the web at www.astaro.com.

It's time to talk security with our maven of security, the man who coined the term "spyware," wrote the first anti-spyware program, created ShieldsUP! and, of course, SpinRite, the ultimate disk maintenance and recovery utility. And now, ladies and gentlemen, he's become the security guru for many people.

I have to, before we get started, Steve, I have to tell you a little story.

Steve Gibson: Cool.

Leo: I got an email from a guy who is a chief security officer of a major Israeli corporation. I won't say the name. But it's big. So if you're the chief security officer for a big Israeli corporation, you're a big security guy, right?

Steve: And probably at the moment you're down in a bunker.

Leo: Well, you're not happy, but you certainly know how to keep your – it's a financial institution, so you know how to keep your stuff safe.

Steve: Oh, wow. Cool.

Leo: Occasionally the board of directors will bring in a consultant to kind of watch him, you know, just to kind of double check it. And he says there have been eight consultants in the last couple of years. These guys always come in cock of the walk and, you know...

Steve: Wow, they're really serious, then, about their...

Leo: They're very serious, yeah.

Steve: Yeah.

Leo: And they always think, you know, they're the new guy, they're going to be here for years; and I always have to explain to them, no, no, you're here for a minute. I'll be here a lot longer than you.

So they brought this new consultant in, and he said we usually just let them, you know, scan the network and just kind of put them off in a corner, say go ahead, do – you know. And he starts coming back with very voluminous emails that seem very erudite and very intelligent. And he's, you know, my correspondent's a little puzzled because he talks to the guy, and he seems to know – he seems like an idiot, right, he can't put two sentences together. And he's, where is he getting this good stuff? So at one point he sends them, he says, well, I've scanned, and there's a port open here. And he sent him a screenshot, clipped carefully to avoid certain telltale information. But the security officer looks at it, and he figures it out. It's ShieldsUP!. And he says, hmm. So he goes to ShieldsUP!, you know, he figures this out. He starts listening to the podcasts, and he realizes the security consultant has effectively just been parroting back the contents of the podcast to him. He in fact knows nothing aboutsecurity, but he has used Security Now! to get the job.

Steve: He's got a good memory.

Leo: He's got a – well, not good enough, because he can't do it in conversation. But he's good at cut-and-paste, I guess.

Steve: Right. He's not understanding it, but he's listening to it.

Leo: Right, he's listening to it. So anyway, I just want you to know we reach far and wide...

Steve: What a kick.

Leo: ...with this podcast. And if you are a security – if you're pretending to be a security expert based on what Steve says, it's good material, but you might want to do some extra research to really bolster your knowledge, you know.

Steve: Or maybe listen to each one a few times.

Leo: A few – memorize. Memorize. That's the key. Understand. So it – go ahead.

Steve: When we did our one about the Netstat, how the Netstat command works, there was a bunch of dialogue in various forums and things that I happened to see, saying, you know, you'll get much more out of it if you sit down in front of a computer and type along with Steve and Leo.

Leo: Type along with Steve. Well, people used to do that, we know, when they were watching TechTV, when they were watching the screensavers, because we'd have to be very careful not to give out the URL of a site until we'd actually loaded it.

Steve: Well, mine, you know, whenever you would talk about ShieldsUP!, it would just – back in the old days, when my bandwidth was only on a couple T1s, it would just, I mean, it was the so-called "slashdot" effect, where it would just collapse my site. Which, you know...

Leo: People were watching and typing in those URLs as we said them.

Steve: Yup.

Leo: Which is very interesting.

Steve: Well, because you never know how long they're going to stay on the screen. They're like, oh, my God, I'd better type that in, you know.

Leo: That might be. So last week we started a series on virtualization, and we really kind of more talked about the history and the concept behind virtualization and modern applications. And we are going to get back to that. But...

Steve: Well, actually there's a little bit of errata from last week, too. Some sharp-eared listeners caught me in a mistake that – this really made me grin.

Leo: No.

Steve: Because whenever I'm talking about hard drive sizes, I have to consciously say, like I'm talking about, you know, old school, I have to consciously say 10 megabytes.

Leo: Right.

Steve: Because I'm just, you know, everything is gigabytes now.

Leo: Right.

Steve: You know, we're three orders of magnitude beyond where we were then.

Leo: I slip like that all the time. Anybody who's been around for a while is going to make that slip.

Steve: Well, and I did, because I was talking about how Bill Gates, you know, was quite sure when he released, you know, the original DOS and was working with IBM on the design of the first PC, that we would never be needing more than 640 megabytes.

Leo: Oh, no. He said...

Steve: Oops.

Leo: ...640K.

Steve: Exactly. 640K, you know, which was ten times what the Apple II had, the Apple II, of course, being the competition at the time.

Leo: 48K, that's right.

Steve: It was 48, but then you could add, like, a soft card and some RAM expansion. So it sort of had a 64K addressing space. And so, oh, ten times that, 640K.

Leo: No one will ever...

Steve: Who would need more?

Leo: ...need more than that.

Steve: Right, right. And then the other thing I forgot was that – someone refreshed my memory. We talked about a couple of the early DOS-based, sort of VM-ish utilities, Quarterdeck with DeskView and...

Leo: And QEMM – oh, you mean the...

Steve: The actual applications.

Leo: Applications, yeah, yeah.

Steve: And then of course IBM had TopView, which really never got off the landing pad, or launching pad. But someone reminded me of the utility that was the one that I actually used, which was called Software Carousel.

Leo: Oh.

Steve: And it was – I used it because it was even cleaner than the other two. All it did was I think you did, like, Alt-2 or Alt-3, and it just instantly swapped you to, like, a brand new DOS.

Leo: Wow.

Steve: And, you know, it used all the memory mapping that we had at the time, with extended and expanded memory, and just gave you just the ability to just completely switch DOSes. And so you'd have different things running in different ones' and you could, like, preload them at boot. And it was just a great little utility, so...

Leo: It's so cool. It's so cool.

Steve: ...you know, harkening back to the old days.

Leo: Yeah, yeah.

Steve: But anyway, as you were saying...

Leo: We're not going to do that today.

Steve: Exactly.

Leo: We're going to save that for next week.

Steve: Actually the week after.

Leo: Or week after because we have to do a...

Steve: Next week is one of our Mod 4.

Leo: Q&A.

Steve: In fact it's a very – it's a special Mod 4.

Leo: It is.

Steve: Because it's number 52.

Leo: Oh, and why is that? Because there's 52...

Steve: It's our anniversary.

Leo: Oh, it's our one-year anniversary.

Steve: Yeah. 52 weeks in the year.

Leo: We're not taken a single week off. Wow, that's amazing. So, okay, yeah, next year, one-year – next week, one-year anniversary, and questions and answers. And then, events allowing, we'll do – continue virtualization the following week in Episode 53. But this week there's something a little more topical that you wanted to cover, and...

Steve: Yeah, I really, you know, as we've said before, when something comes up that is, you know, within our purview, even though we've got some plans, we'll catch back up with those plans. Something really caught my attention this week. I mean, it really flabbergasted me. Back when I was originally reading Microsoft's Vista plans, you know, their marketing sheet about, you know, all the new stuff – and, you know, you do that with each Microsoft OS that's coming out. One of the items there, one of their bullet points, was, you know, brand new networking stack offering support for new protocols, blah blah blah. Well, I mean, okay. I just blew that off. You know, they always say that, and it's never true. You know, I mean, remember...

Leo: Maybe we should explain, before you go too far, what a networking stack is and what it does.

Steve: Well, we'll definitely do that, but...

Leo: Okay, we're going to get to that, all right.

Steve: Yeah. But, for example, you know, with Windows 2000, and mostly with XP, you know, they had the same sort of thing. But it was clear to any of us who know Microsoft and know Windows that XP was, you know, just – it was Windows 2000, and they added some nice green rolling hills and a blue-and-green candy coating. But, I mean, it was obviously still Windows 2000. I mean, they really hadn't changed that much. And of course that's where the raw sockets happened was the Windows 2000 raw sockets, you know, they put the candy coating around it to give it to my mom, but left a bunch of other stuff there.

Leo: Right.

Steve: So I just – I didn't think twice about Microsoft's claim that Vista would have a brand new networking stack. Well, until I discovered a report from Symantec, where two of their engineers took a look at, like, four, I think three or four different beta versions of Windows – actually it was three different beta versions, and there was a fourth one since – and poked at it and discovered it really is brand new, written from scratch. Now, that's significant.

Leo: It seems like a good idea, especially given all the problems we've had with the old one.

Steve: Well, people are generally of the feeling that something new is good.

Leo: New is better.

Steve: But – exactly. It's like, you know, oh, let's upgrade. Well, of course patching is a good thing to do.

Leo: Right.

Steve: But the problem with security is that fresh is really not what you want your code to be...

Leo: Fresh code.

Steve: ...when it needs to be secure.

Leo: Right.

Steve: And it's interesting because there were rumors at the time of Windows 2000's release about where did Microsoft get that stack. Because, you know, there was 95 and 98 and NT, and then Windows 2000. Well, Windows 2000 really did appear to be a different networking stack than Microsoft had. But it just – it was born fully mature. It was, I mean, it was a really good networking stack from day one. And you just don't get that. I mean, all of the security problems that have been solved years and years ago were, like, already fixed in this stack. And there were rumors that Microsoft lifted it from one of the open source BSDs.

Leo: Oh, boy.

Steve: That that's where it came from. And I can't remember where it was NetBSD or OpenBSD. I don't think it was FreeBSD. But, you know, there was a strong suspicion, just based on the behavior. You know how there are network fingerprinting tools, or OS fingerprinting tools, that will send a bunch of specially crafted packets at a machine. And based on really subtle differences in the way it responds, they're able to determine what kind of operating system is at the other end.

Leo: Nmap does that, yeah.

Steve: Exactly. Nmap is the classic example. Well, Windows 2000 was responding exactly like one of the BSDs at the time. And it worked really well. I mean, it was, like, ready to go. So it was like, okay, well, hmm, you know. And of course, as we know, Windows 2000 was the first OS that had raw sockets. And of course the BSDs, being UNIXes, have always had raw sockets. So there were just – there were many things that Windows suddenly inherited in Windows 2000. We don't know, I mean, I have no proof or evidence. But it was strange. And in fact, the lesson we're seeing with Vista actually lends more credence to the notion that maybe Microsoft got the Windows 2000 stack from somewhere because Vista's stack is a disaster.

Leo: Uh-oh. Well, let's – so that's our subject today.

Steve: Yup, yup.

Leo: Vista's disastrous stack. What did you call it?

Steve: I call – well, Vista actually has a virgin stack.

Leo: Vista's virgin stack. Now I guess we'd better step back a little bit because I don't know, I mean, I don't know exact- I've heard, you know, TCP stack. I've heard, you know, all of this. But what is it, and what does it do?

Steve: Well, the term "stack," as it sounds, refers to a stack of layers. And networking people talk about networking layers because it's extremely convenient to think of networks in terms of layers. And of course there's the famous OSI model of layers where it talks about, like, the lowest layer is...

Leo: Right, there's seven layers, and...

Steve: ...the electrical link layer, sort of a link layer. Then you've got, you know, basically a set of layers going from the electrical wire connections all the way up to high-end application usage. And basically the idea is that each layer in this stack does one sort of thing. Well, we've talked over the last – literally over the last year about how Internet packets are encapsulated within each other, how you'll have an Ethernet header which routes this packet which on the outside is an Ethernet packet. Then, inside of that, sort of encapsulated in that, you'll have an IP header with its payload. And then within that you'll have the protocol header – ICMP, TCP, UDP, and whatever. So it's sort of like nested layers of data.

Well, the stack essentially interprets those nests of buffers in exactly the same way. The lowest level of the stack deals with, in the case of an Ethernet system, deals with the Ethernet layer. The Ethernet layer takes, you know, accepts the packet, removes the envelope that it contains, and then passes that, which would be the IP envelope, up to the next layer in the stack, which says, oh, I'm the IP layer, I know how to read IP packets. It does whatever it needs to do with the information in the IP header, then takes that off and passes the internal data, the protocol, up to the next layer in the stack, which is the protocol layer. So essentially, packets are unwrapped envelope by envelope, like nested envelopes, with each layer in the stack dealing with the contents of the previous layer's data. So...

Leo: That makes sense. It's almost – so it's kind of a parallel of the stack itself.

Steve: Oh, it's beautiful. I mean, it's elegant, and it's symmetrical. So for example, the same thing happens in reverse direction.

Leo: Right.

Steve: When the OS wants to send data out, it sends the data down the stack. Each layer takes what it gets from the layer above, encapsulates that with its own layer data. So the protocol layer takes the actual data and wraps a protocol around it, TCP or UDP or whatever, hands it down to the IP layer, that adds the IP layer stuff around it, then hands it down to the Ethernet layer, the link layer, encapsulates it with Ethernet data, and finally sends it out on the wire. When it finally gets to wherever it goes, that process is reversed to essentially bubble the very, well, sort of like the inner core of the data, like these nested dolls, all the way back up to the application at the other end.

So it's complicated, but it just works beautifully. And it's very flexible because in this layered architecture, for example, you could have different specific layers if your destination was not, for example, Ethernet, but maybe Token Ring or PPPoE, Point-To-Point Protocol over Ethernet, or, you know, other protocols. So this notion of encapsulation is why we have layers. And so the layers collectively are referred to as a "stack."

Leo: That makes perfect sense. I followed that exactly.

Steve: Oh, it's beaut- I mean, it just is beautiful. And it's worked so well and stood the test of time because it's modular. It's inherently modular. And so it subjects itself to being changed and evolved very nicely.

Leo: So all networks communications goes through the stack.

Steve: Yes.

Leo: It's the portal into your computer.

Steve: Yeah. It's like one of the major – well, for any Internet-connected machine, any UNIX machine, any modern Windows machine, anything that's going to be doing Internet stuff, somewhere there's a stack. And that's fundamental to the systems operation.

Leo: All right. So it seems sensible that you'd want to improve a stack as new protocols came out, or maybe you found bugs, or maybe you could make it more efficient. So writing a new stack doesn't seem like such a big deal.

Steve: Well, the problem is, it is incredibly complex.

Leo: Ah.

Steve: And we talk, in terms of security, we talk about maturity because – there's a classic example was in the summer before Windows XP was released for the first time. Of course, I was arguing with Microsoft about the raw sockets issue. But Microsoft was saying Windows XP was going to be the most secure operating system they had ever made.

Leo: Well, that sounds familiar. I've heard that phrase about Vista, as a matter of fact.

Steve: Well, exactly. But any security person would listen to that and just, you know, roll their eyes and shake their head.

Leo: Because you don't really want new. You want proven by the test of time. You want something that's been banged on.

Steve: Well, what it actually is is that it's fundamentally illogical. I mean, it's impossible to say something is going to be the most secure.

Leo: Because you don't even know yet.

Steve: It's a non sequitur.

Leo: Right.

Steve: The way the world works is security is proven. It is not claimed.

Leo: Right.

Steve: And so claiming security means nothing. And of course we know...

Leo: Claim all you want.

Steve: Yeah. We know that Windows XP was the least secure operating system Microsoft ever produced. I mean, it was worm land on the Internet for a long time.

Leo: Well, and we've lived through that for the last five years, yeah.

Steve: Yes. And what's really interesting is, okay, finally, Service Pack 2, firewall's on, all these problems have been found. Now we can all take a big, deep breath. Well, the bad news is, Vista is the most secure operating system Microsoft has ever made.

Leo: And they're starting from scratch.

Steve: Well, and not only that, they are really starting from scratch. What the Symantec report did, these two guys at Symantec took these early betas – and I want to make sure everyone understands, we're not talking about production Vista. So this is just beta code behavior. And in fact...

Leo: And also, to be fair, Symantec has a vested interest in insecurity because they make security programs.

Steve: Well, it's worth mentioning, yes, that Symantec is not happy with Microsoft. There is a lawsuit they filed several months ago claiming that Microsoft has stolen their trade secret information. There was some sort of license deal that Microsoft had with Veritas that limited what they could do. And apparently Microsoft has used that as the foundation for new stuff in XP and in Vista. And Symantec, I mean, they've tried to resolve their problems amicably. They're going to let the attorneys do it now. So they're fighting on that front.

But also, exactly as you say, Leo, Microsoft is clearly – I mean, and this was foreseeable – getting into the anti-spyware and antivirus business big-time, which is going to be a big problem for Symantec. So, yes, Symantec has some interest in Microsoft's not being secure. But the report was very well written. I mean, these guys – and you've got a link to it on your show notes. I've got a link to it on mine also, on the Security Now! page. So people can take a look at the full PDF of the report if they're interested. And the guys were very fair, I mean, they really explained that they understand that these are betas. And they talked about problems that they watched being solved along the way that earlier betas had, that had been fixed in later betas. So...

Leo: And even the publication of this document may improve the stack because all of these issues that they raise, Microsoft can now fix.

Steve: Okay. Now, okay. For example, remember a couple weeks ago, within the last couple weeks I talked about a ridiculous, really old problem that was almost funny, where you would send a spoofed packet to Windows, claiming that it came from that same machine. It's called the Land attack, where the source and the destination IP are both the same as that machine's. And it would just cause the stack to freak out and collapse because it thought it was receiving something from itself, so it would answer to itself, and just melt down.

Leo: Right, get in a loop, yeah.

Steve: Well, Vista does that.

Leo: No. Now, was this something that was patched and fixed in XP?

Steve: No, this was fixed in Windows 95.

Leo: Oh, boy.

Steve: No, that's what we're talking about. We're talking...

Leo: Oh, boy.

Steve: That's just it, Leo. We're talking about all the same mistakes that have been fixed in all prior Windows stacks finally, and in all other mature stacks, are now back in Vista.

Leo: Why?

Steve: Well, okay. Now...

Leo: I mean, wouldn't that be kind of almost a textbook thing when you're – you know, when writing a stack, make sure you don't do this. We learned this 15 years ago.

Steve: And that's just the problem is that, yes, it's going to be pounded on. These things are going to be fixed. And in fact, this problem was present initially and was fixed in a later build...

Leo: Oh, good, okay.

Steve: ...when someone tried it. You know, the good news is we have lots of security tools now that have been developed to nail these problems. However, this absolutely proves that this is a brand new stack.

Leo: Because it would be fixed in any mature stack, would obviously not have this problem.

Steve: It is fixed in every other mature stack, yes.

Leo: Right. So they definitely didn't borrow this from somebody else. Unless they borrowed it from the Windows 95 development team.

Steve: I mean, they're saying that it was time to start over. Now, I respect that because, you know, over time code evolves, it gets very patchy, I mean, that's why the Apache Server is called Apache, because it's basically a whole bunch of patches. So it makes sense to say, okay, timeout, we need to start over. One of the things that the Vista stack incorporates is IPv6 support, natively in the stack.

Leo: Right. And no earlier stack would have that, probably.

Steve: Well, exactly. For example, XP and even Windows 2003, if you want IPv6 support, you add it as an add-on to the existing technology. So Microsoft has had IPv6 around. Now they're building it in from scratch. There are also a number of other protocols. As you may know, Microsoft's Vista will be adding native peer-to-peer support with NAT traversal built in, these

technologies that, you know, for example, Skype and other peer-to-peer technologies had been using in order to be able to get machines to talk to each other, are being built in. So there's a lot of new stuff. And Microsoft made the decision, you know, bit the bullet to say, okay, we don't want to keep dragging our aging, creaky stack forward. We're going to start again. The problem is, nothing could be worse for security.

Leo: Yeah, yeah.

Steve: For example, there are – the stack responds to unknown protocols with an ICMP message saying, I don't know what that is. For example, TCP is protocol 6; UDP is protocol 17. There's a byte in the protocol header that identifies what the protocol is. And so it's polite, if a packet is received that's for a protocol that the stack doesn't have anyone to send the packet upwards through its layers to, for it to send back an ICMP message. Remember we've talked about ICMP as sort of being like the plumbing management. So when a packet comes in that is for an unknown protocol, it's nice that the stack sends back a note saying, gee, don't know what that is, got anything else? The problem with doing that is that it means it's trivial to probe the stack to find out what protocols it does support.

Leo: Yeah, what do you do? Yeah.

Steve: Exactly. Well, the guys did that. And they found a bunch of interesting unknown protocols. So they sent some random data to one. Boom. Blue Screen of Death.

Leo: Oh, no. Oh, geez.

Steve: I mean, it's like, oh, what next?

Leo: But that's easy to fix.

Steve: And it will be fixed. You know, those are easy things to fix. I'm sure that Microsoft has read Symantec's report. And in fact, in the later developer version after the build that was made public that was the last thing these guys fixed, more of these things have been fixed. But what I want to stress here is that we now know for sure that Microsoft has written a new stack from scratch. And anyone in the industry will tell you – and this is not Symantec, you know, crying wolf or the sky is falling. Anyone will tell you that a networking stack is so complex that it takes years to mature.

And while Microsoft has the advantage to some degree of us having a strong sense for how to fix all the old known problems, we have no idea yet what new problems this stack is going to have that no other stack ever had. Not only has Microsoft recreated many known problems, but there are going to be – well, in fact there is, there is one brand new problem that never existed before. There's something called IP options, where it allows additional data to be enclosed at the IP level of networking traffic. And what you have is, in the IP options, you've got a size of the options that tells the system, okay, here we've got some option data, and it's this long. So then – so jump over that this many bytes to get to the next piece of data in the packet. Well, it turns out in Vista, if you set the size of options to zero, it says jump over zero bytes. So it lands where it is, does it again...

Leo: Loops.

Steve: ...and then lands where it is and loops permanently. It locks up the system hard and requires a full reset.

Leo: Now, Vista's – the betas that people have been using of course is full of bugs. That's why they're in beta test. So you're not saying that these problems will persist, but merely that a new stack is an untested stack. And of course there's a lot of concern about Vista's security. I mean, the spotlight is on Microsoft now. They need to put out a secure operating system.

Steve: But, see, and Leo, you can't. You...

Leo: Because it hasn't been tested.

Steve: Yes. By definition, nothing brand new is secure.

Leo: Now, they are doing the world's largest beta test. They're sending out 2 million copies of Vista. And of course most people won't be testing the security of it. But I presume some security experts will be working on it.

Steve: Yeah, oh, there's no doubt about it. I mean, I guess my point is – I'm not here, again, like the Symantec guys, to cry wolf or say the sky is falling.

Leo: We don't know yet.

Steve: Yes.

Leo: We don't know yet.

Steve: When I'm using XP on a couple laptops that I recently got, toward the end of last year – I'm still using Windows 2000 as my main platform. Windows 2000 is GRC's server platform.

Leo: And that is, by the way, running out of time because Microsoft's not going to support it anymore.

Steve: Right. Actually, I did try to consider using Windows 2003, but it was just a – well, I won't go into it, but...

Leo: You know, the interesting thing is that it was my understanding that much of Vista was based on 2003 Server. But I guess the stack is not. I guess it's...

Steve: Well, it's clear that it's not. There are so many mistakes in the current stack, in the current beta stack...

Leo: It's very discouraging, frankly.

Steve: ...that it proves – it demonstrates that this is new, that Microsoft told the truth this time when they said all new, brand new, whatever...

Leo: Shiny code. Fresh, shiny code.

Steve: Or as any – I mean, it is a virgin.

Leo: Untested code.

Steve: And so, you know, anyway, the point I was making about XP was that it wasn't until several years after the...

Leo: Yes. Took a while.

Steve: ...release of XP that – and we had Service Pack 2 that...

Leo: And it wasn't a new stack.

Steve: Exactly. And all the new stuff in XP was badly broken in ways that no beta testing found, no early testers found. Late problems were discovered by people really looking closely. So...

Leo: Well, because Windows is a natural target. It's so dominant, there's so many installations, that every hacker in the world is most interested in compromising Windows. So Vista will immediately come under attack, very serious, hard attack from top-flight hackers all over the world, the minute it ships.

Steve: Well, and I would argue that it isn't even Microsoft's fault that this is a problem. I mean, Microsoft is taking responsibility for these problems. Microsoft made the decision, I'm sure a tough decision, probably, well, I don't want to say unwise. But they made a tough decision to scrap their networking architecture and write a whole new one.

Leo: I'm sure they felt they had to for various reasons.

Steve: Yeah. I mean, they talk about performance...

Leo: It's not something you undertake lightly. I mean, they must have felt they needed to.

Steve: They talk about performance and stability and extendibility. I mean, what they had was probably getting old. Apparently, the current stack underperforms the new one. That's – maybe it's, you know, debugging code and beta code, and they'll be able to trim it and prune it and make it better. I mean, I like the idea of them making the hard choice to drop what they had. But all I want to really – the message of this episode is a couple. One is that you cannot – no one can claim something is secure ahead of time. You can say, we hope it's secure. We really, really want this to be secure. But it's only years of battle hardening that is going to make Vista secure.

So listeners of Security Now!, who are obviously on the security awareness leading edge, you know, along with us, are, I would say, will certainly want to play with Vista. I would be very careful and skeptical of it for quite a while, until we see what's going to be happening. Leo, if you and I had been doing Security Now! four, five years ago, when XP was coming out, you know, we would have been busy. And we will be doing security...

Leo: We're still busy. But we'll be busier in a couple of months.

Steve: Yes. Well, and see, that's the other horrifying thing. As I understand it, they're talking about Vista maybe January of '07. Which, as you said, in a few months. Well, in order for OEMs to happen, and we know how the whole routine goes...

Leo: We're talking a couple of months to get to the gold master, at most.

Steve: They need to – it needs to be golden and frozen in order to get into production for OEMs to have copies, for integration to happen.

Leo: Well, and they promised Enterprise that it would be available by December. So we're talking in the next two months they will freeze the code.

Steve: And Leo, just last week it was, like, locking up and going blue screen when you sent some data to a certain protocol. So it's like, okay, when, I mean, I can't imagine that it's either going to be stable or they're going to ship it on time. It almost, to me, based on the rate at which these problems are being fixed and the fact that the networking stack still has serious problems now, you think, okay...

Leo: A year?

Steve: This thing just – well, at least this part of it...

Leo: They're going to ship. They have to ship, and they will ship. And I guess the advice we're going to be giving...

Steve: We're going to be really busy. It's going to be really...

Leo: ...is to hold off. Don't be the first upgrade to Vista. We will be busy. You know, I'm going to be – I'm giving, in February 3rd through 10th, I'm going on a geek cruise. PC World is sponsoring PC Paradise. And I'm giving two classes in Vista security. So I can't hold off. Nor can you, Steve Gibson. We will be getting Vista machines.

Steve: It's funny you mention that because I was just thinking, I mean, I just ignored XP...

Leo: We can't.

Steve: ...for years.

Leo: Sorry, dude.

Steve: And you know, the only reason I had one around was so that I could do screenshots of my applications running on XP so the Windows had the candy coating on them, rather than my Windows 2000, you know, that looks more like...

Leo: You don't have that luxury this time.

Steve: No, I don't.

Leo: Nor do I. But we'll take a bullet so that you don't have to, folks.

Steve: Well, and again, I'm not saying don't upgrade, don't use it. Maybe, you know, set it up as a dual boot. And so, you know, go over, boot that one sometimes on the weekends, you know, and...

Leo: But don't shift your whole office over right away.

Steve: Oh, it's, you know, or don't do it soon. It's going to be – we're going to be busy, Leo.

Leo: We'll have a lot to talk about. Well, Steve, I really thank you for this kind of warning. And again, you know, all the disclaimers, Symantec has a vested interest in this, it is beta code. But I think you're underscoring, which is the fundamental problem that every programmer, certainly anybody who's done any network programming understands, is that this stuff is hard. It's hard to make it secure. It's hard to do it from scratch.

Steve: And they started over. I mean...

Leo: And it's not...

Steve: And they're making all the same mistakes that have been fixed...

Leo: That's a little discouraging.

Steve: Oh, well...

Leo: They should, no, there should be a manual somewhere that says, oh, by the way, guys, don't do this. They should know that. They should know that.

Steve: It's just going to be a hacker heaven.

Leo: Oh, it's scary. It's very scary. Well, you know where to go to find out what's going on. And I think, as we get closer to Vista, we're going to of course do more and more Vista coverage, not only on this podcast but on all our podcasts, and on my radio show and so forth. And we'll talk a lot more about this. And I think it's just, you know, something that maybe this podcast will become less educational in the next six months and more here's what's happening this week.

Steve: Well, you know, Leo...

Leo: But we'll do it if we have to, you know...

Steve: ...we are going to pick up our series on virtual machines. So people – and specifically on sandboxing using virtual machines to prevent bad behavior from getting out of the sandbox. That's where we're going to be going in the next few weeks. And so...

Leo: This would be the perfect way to do Vista.

Steve: Well, running Vista in a sandbox is probably going to make a lot of sense.

Leo: As far as I know, Parallels doesn't yet support Vista. I'm not sure whether Microsoft's Virtual PC, which they're giving away for free, does. I'm sure VMware will by the time Vista ships. So there will be...

Steve: Actually, we'll have to check, but I think their virtual – the free thing they're giving away is only something that runs on top of their server platform.

Leo: Ah.

Steve: I think it's Virtual PC Server 2003 RC2 or something. And...

Leo: I thought they were giving away the basic one, as well. They changed their plan. We'll find out. We'll find out. But we'll talk about that...

Steve: Yup. We will be talking about it.

Leo: ...because we're going to, yeah, we have a – in fact, we're going to interview one of the kings of virtualization, I hope.

Steve: I hope so.

Leo: Yeah, we're looking forward to that. So I hope you have learned a thing or two. My eyes are wide open here. And a little scared.

Steve: I couldn't believe it. I just thought, oh, yeah, marketing propaganda, all new stack. No, this one...

Leo: No, it really is.

Steve: This one really is.

Leo: Vista's Virgin Stack.

Steve: Lord, lord help us.

Leo: We encourage you to check out, of course, GRC.com. That's Steve's site. That's where you'll find 16K versions of the show. You'll also find transcripts, thanks to the wonderful Elaine, who does such a great job making our words intelligible. And Steve's great SpinRite, which is the ultimate disk recovery utility, and a must if you deal with hard drives. Not just for recovery, but for maintenance. I think people, you know, I think we're been underscoring the recovery because I think a lot of people use it for maintenance and didn't realize it is as good as you can get in recovery. But don't forget, it is a great way to keep your hard drives working smoothly for a long time.

Steve: Yeah. I think what happens is most people buy it because they have a disaster.

Leo: Ah.

Steve: And then they realize, wait a minute, had I been running SpinRite every, you know, quarter, for example, every three or four months...

Leo: Yes, right.

Steve: ...or when something maybe sort of seems a little strange in the computer, it's slowed down or delaying or something, they realize, hey, I could just do this to keep the problems from happening.

Leo: Right.

Steve: And SpinRite does that because it shows the drive, the problems that the drive has, and helps the drive correct them.

Leo: I was talking on the radio show the other day about SMART monitoring. And really I haven't had much results, much success with this SMART monitoring. Most drives are SMART drives now, but I don't find that those monitors are particularly useful. I suggested the best way to know if a drive is going to fail is use SpinRite. SpinRite has a really kind of fun little tool that shows how many corrections – is it per second or per minute?

Steve: It's actually per megabyte.

Leo: Per megabyte, okay.

Steve: Yeah. As SpinRite's moving along, what it does is it dynamically reads the sort of private SMART data that most drives publish to the API, the SMART API. SpinRite sees how many corrections are occurring from the time it last looked to the time it looks now. It then looks at how much data it has read from the drive and computes the number of corrections per megabyte, so that you're able to see over the long term if that number starts going up suddenly, that tells you your drive is getting into trouble way before it actually dies.

Leo: It's the best warning. And I don't know of any SMART monitor utility that will tell you this, only SpinRite.

Steve: Well, there's nothing else that can because it only makes sense to look at that when the drive is doing work. So it's only when the drive is under load, and SpinRite puts a calibrated load on the drive in order to watch how hard it's having to work.

Leo: Sometime I want to talk about it because it's fascinating. I mean, it didn't realize that the error correction technology that's built into drives is actually active all the time. Drives are making mistakes constantly. I mean, hundreds of mistakes a megabyte, thousands are normal, right?

Steve: Yeah. I mean, it used to be in the old days that ECC, Error Correction Code, was only brought into play to deal with a defect. But data is so dense now, relative to our ability to produce absolutely perfect magnetic recording services, you know, we just can't. At some level our ability to make perfect recording surfaces fails. Data, the actual bits, are down now at the size of that failure. So error correction is being employed all the time...

Leo: Constantly.

Steve: ...just as standard operating procedure, instead of being an exceptional case. And so...

Leo: It's really remarkable.

Steve: Well, I mean, look at the size, look at the incredible amount of data. There are now on the shelves at Fry's 500-gig drives.

Leo: See, I eschew those. I buy smaller drives and multiple drives rather than buy one big drive.

Steve: Actually, I...

Leo: It scares me. The areal density is too high.

Steve: We're old dogs. I'm the same way. When I call my computer guy to order drives, I say, okay, what's the smallest Maxtor drive you guys still can get for me?

Leo: Right.

Steve: Because I just, you know, it's like...

Leo: And with RAID you can combine them or whatever. But you don't, you know, it's just, I mean, 500 gigs.

Steve: It's scary.

Leo: That's very dense.

Steve: Yup.

Leo: We want to thank our sponsor, Astaro Corporation, makers of the Astaro Security Gateway. I mean, when it comes to security, as you can tell, no half measures will do. And if your small or medium business needs superior protection, based on well-known, tried and true, open source technology – you get protected from spam, from viruses, from hackers, complete VPN capabilities, intrusion protection, content filtering, and an industrial-strength firewall, all in a very easy to use high-performance appliance – contact Astaro, Astaro.com;, or you can call (877) 4AS-TARO. You can schedule a free trial of an Astaro Security Gateway appliance in your business. And of course non-business users, as always, can download the software version of ASG for home use at Astaro.com. And I do recommend that. It's a great solution. Really, really good. Astaro.com.

Steve Gibson, next week it's Mod 4.

Steve: And our anniversary.

Leo: And what are we going to do? I'll bake you a cake. I don't know. We'll have to think of something.

Steve: Maybe your wife.

Leo: Sorry? No, I'm not giving you my wife. That's...

Steve: No, no, I know. Maybe...

Leo: Oh, my wife will make the cake. Yes, she's a much better baker than – we have to draw a line somewhere. I'm sorry, Steve. This is a great anniversary, and I can't wait to celebrate it. It's been a wonderful year. And I think we now know it's going to be a very interesting year to some.

Steve: Oh, we're not going to run out of material, Leo.

Leo: Thanks, Steve. We'll see you next time.

Steve: Okay.

Copyright (c) 2006 by Steve Gibson and Leo Laporte. SOME RIGHTS RESERVED

This work is licensed for the good of the Internet Community under the Creative Commons License v2.5. See the following Web page for details: http://creativecommons.org/licenses/by-nc-sa/2.5/