SECURITY NOW!

Transcript of Episode #65

Why Is Security So Difficult?

Description: Steve and Leo get a bit philosophical this week. They discuss the broad nature of Security – all security, not just computer security. They propose a new definition of "Security" and flesh it out with examples to illustrate why security is so difficult, if not impossible.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-065.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-065-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 65 for November 9, 2006: Why Is Security So Difficult?

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.

Time to talk security with my personal security hero, Steve Gibson, a man who I trust implicitly. If Steve says do it, I do it. It's good to talk to you, Steve.

Steve Gibson: Thank you, Leo. Great to be back.

Leo: That's a heavy burden. Do you feel like that's tough?

Steve: No. Because, you know, I spend a lot of time thinking about this stuff. I'm involved in it. I love the technology. I mean, I'm, you know, I'm a technology junkie. And, you know, much as once upon a time hard drives had this problem, and I used my love of technology to deal with that with SpinRite, now, you know, the next real big deal with the Internet has been security.

Leo: Yeah.

Steve: So, you know, I've sort of rolled my sleeves up and, you know, did ShieldsUP! and, of course, you know, got into this whole spyware thing and malware and, you know...

Leo: Well, we really have to thank you. And at this point you don't make any product, which in a way – for security, which in a way to me gives you more credibility. I mean, if Symantec says viruses are on the upswing, I always have to think, well, hmm, who benefits from that? But when you say it, I know that you're not benefiting from it. This is – and I also know how scrupulous you are about facts. This is an issue. So...

Steve: Yeah, well, I love it.

Leo: The only criticism sometimes you get is that you're like Chicken Little, that sometimes you overstate the security issues. Do you have a defense for yourself in that regard?

Steve: Well, yeah. And we've sort of talked about this. When we're doing this, I'm trying to say to people, look, you know, not everybody is the same. And in fact we're about to talk about yet another Microsoft zero-day exploit which is on the 'Net, it's an ActiveX control. And so last time we talked about this I was very careful to say, and I hope our listeners heard me say, you know, if you're a person who surfs with scripting enabled, if you're using IE, if you go to, you know, random sites that you don't know often, then this is probably worth worrying about.

Leo: Right.

Steve: Whereas, you know, if any of those things are not true, you know, basically you hang out on MSN or Amazon or, you know, your breadth of reach with your browser is not extreme, then you can probably wait for Microsoft to catch up with their next security patch and, you know, when presumably they'll fix it. So, you know, as we've said before, you can be bitten by things you're not aware of. And I'm sure from, you know, looking at all the feedback we get that people want to know; and they'll let, you know, they respect the fact that we're trusting them to decide whether this is something they want to deal with or not. I mean, Leo, remember, here you and I are, not with any antiviral software on our machines.

Leo: Shhhh.

Steve: So it's not like...

Leo: Don't tell anybody. I don't want anybody coming after me.

Steve: So, I mean, which most people think is nuts because...

Leo: But we know what we're doing.

Steve: Well, yes. And so I guess my point is it's not like we're sitting here, you know, pumping out fear and worry and feeling that. The idea is to say, look, here are the facts.

Leo: Right.

Steve: As clearly and flatly as we can provide them. And we let people figure out how they feel about it.

Leo: Right, right. And then you be the judge. You decide what you want to do about it.

Steve: In errata from prior weeks, I did want to mention that – remember that we had some discussion about remote access to Gmail using POP and SMTP.

Leo: Right.

Steve: And I wanted to confirm that Google Mail does absolutely allow you to configure your regular mail client with secure connections, using SSL, to connect to Gmail servers. So you can have exactly the same experience that you would normally have with Gmail, you know, going to your web browser and opening Gmail. You get the same interactivity with your own email client, just setting up an account on your email client to go and fetch and send your mail through Gmail. So it's very cool.

Leo: Now, actually, this came up on the cruise. We were talking about SSL. Security was a big topic of discussion, of course, as you might imagine. And somebody pointed out, I think one of the editors of Macworld pointed out – probably Dan Frakes – that some online mail accounts let you use SSL to log in, but then are unencrypted once you're transferring mail. And some are not. Is that the case?

Steve: Like web browser based?

Leo: Yeah, Hotmail, that kind of thing.

Steve: Well, yes. And in fact the way Google works is, if you go to Google with a non-https URL, that is, you just say http://mail.google.com, you will briefly go secure while you're logging in. Then you'll notice in your address bar your subsequent use of Google is just over a regular connection. But you can go there deliberately with a secure https://mail.google.com, and it recognizes you've done that, and it will leave you with a permanently secure connection for all your transactions.

Leo: I'm just doing it right now. And so it stays https if you start https.

Steve: Yes.

Leo: And that's the key.

Steve: Exactly.

Leo: If you see that "S," you know you're all right.

Steve: Right.

Leo: All right, that's good to know. So and you can use it for SMTP as well, which is kind of cool.

Steve: Yes, you can, so you're not only able to remotely pull your mail, but you can send mail. And because I wanted to give this a try, I used my Gmail account from my normal Windows, you know, because I'm an old Eudora user. And they have a knowledge-base article that I'm going to put a link to on our show notes for this show that shows you, for all the different clients that they know of, and my version of Eudora 5.1, which is a bit older than where Eudora is now, it was covered step by step, screenshots showing you how to configure your client in order to do this. And then I looked at the mail that went through Gmail from an anonymous standpoint, that is, you know, was the IP from which I originated this available, and the answer is no. So it provides a nice layer of anonymity in the same way that, like, going to some location and using a browser to do the Gmail transaction would.

Leo: Excellent.

Steve: So it's very nice. I just wanted to confirm to people that, you know, remote access to Gmail is possible from an email client, and it requires you to be secure. Security is there. I don't even think you can turn it off when you're using remote access that way.

Leo: Very cool. We also have a big zero-day exploit, as you mentioned, in...

Steve: Well, I'm actually not sure how big it is yet. I dug around, and I looked, and it looks like this one is – if nothing else, this is a slower start than we've seen before. On the other hand, you know, people are actively looking, that is, hackers are actively looking for ways into people's machines. So it is certainly a concern. This is not – it's interesting. This is not an XML parsing bug in something that IE was meant to use, such as the last one. But it is an XML problem. The idea is there is something called XML Core Services, which is an ActiveX control, which Microsoft provides so that developers of Windows software can add XML awareness to their applications.

Leo: Ah.

Steve: But because it's an ActiveX control, IE is able to invoke it because IE is, you know, unless you otherwise limit IE, it's able to access any ActiveX controls in your system. So the exploit for this – and there is exploit code on the 'Net, and it is being actively exploited to install malware in people's machines. So it's worth knowing. This is a zero-day exploit, which as we know means that the first awareness of the problem occurred when someone discovered it already being used. So, you know, zero day. It was, you know, it was found out in use. And it's being used to install malware. At this point it has not seen widespread use, but we can presume it's going to be.

Now, Microsoft's second Tuesday of the month is next Tuesday, which doesn't provide Microsoft with much of a window in which to fix this, you know, based on how long Microsoft tends to take. So I don't know for sure they're going to lock this thing down next Tuesday. If they don't, then this has a much greater opportunity to grow a lot and spread in the meantime.

Leo: Now, if you use your protection technique to protect – if you still want to use IE – and Steve uses IE, but he uses the trusted and untrusted zone settings to protect himself. That would work in this case, wouldn't it?

Steve: Absolutely. I mean, and that's what I like about this so much is, you know, as I've talked about it, wherever I go on the 'Net I am locked down. I've got the Internet zone set to high security. And then I've got my trusted zone set to medium, which is the default security. And then for sites where I want them to work, that is, if I go somewhere and it doesn't work, and I look around and it's like, okay, this is worth lowering my guard for – and, I mean, that's what you're doing if you're going to allow a site's scripting to run in your browser, you're lowering your guard – then I add that URL to my trusted zone, as it's called in IE. And so what happens is, unknown sites are always maximum security with scripting disabled. And it's only sites that I have chosen to trust that, you know, where scripting then runs. And so, yes, I would be protected by default in that situation. Now, of course, if I made the mistake of trusting something that I should not, then that's still a problem. So it's not like this is – like doing this means you never need to worry about Microsoft code ever again. I mean, you still do.

Leo: It's not a panacea. And key, by the way, to this and to a lot of security settings, including firewalling, is you start by denying everything. And then you explicitly add sites, rather than vice versa, slowly taking sites off the list. You deny ActiveX to everybody at first.

Steve: It's funny because original firewall logic, when firewalls were brand new, something bad would happen, and the IT administrators would block that port or block that...

Leo: Kind of closing the barn door after the horse had bolted.

Steve: Well, I mean that the logic was reversed. It was the old-fashioned logic of block a problem rather than permitting only the things that you know you want. And of course that's completely flipped over now so that, you know, firewalls are blocking everything by default, and then only allowing traffic in which they've been – that they've been told to and configured to.

Leo: Right.

Steve: So in the case of this ActiveX exploit, there is something in IE which we've talked about before called the "kill bit." The kill bit is basically a permission for IE to access any ActiveX control. ActiveX controls are identified internally with one of these Microsoft Windows GUIDs, the GUID, the Globally Unique ID. Which is I'm sure when people see it they go, oh, yeah, I've seen those before. It's weird, too, because I'm seeing them surfacing more and more when I'm surfing around Microsoft's site. I'm, like, seeing these GUIDs printed out. And there are a lot of them in Vista also where I'm seeing them. I don't know if this is going to go away once we go to final RTM code, or if Microsoft is intending to begin exposing users to these bizarro, you know, serial number-looking things.

But anyway, the point is that there again on our show notes page for this show, No. 65, I have a link to a little registry script that anyone can download. You simply run that, it'll pop up a dialogue saying – because it says .reg is the extension – pops up a dialogue saying do you want to install this in your registry. And what this is, this little script – and this is directly from Microsoft's page, and I also have a link to that, to Microsoft's page, so people can go back to the original source also. All this does is add an entry in the registry to turn on the kill bit for IE for this particular control. There's no reason that IE would ever be expected to use this particular ActiveX control, unlike the prior, the real XML parsing ActiveX control where we had the problem last time. So...

Leo: So I'm – is this something – does this prevent all ActiveX execution? What does kill bit do?

Steve: No, it prevents IE's use of this particular ActiveX control.

Leo: Oh, just this control is disabled.

Steve: Just this control where the problem was found.

Leo: Got it, got it.

Steve: And that's why I was talking about this wacky GUID is that it's identified, the ActiveX control is identified by one of these bizarre, you know, curly brace, and then I think it's eight hex characters, a hyphen, then a couple more groups of four hex characters and so forth, in order to, like, make up this weird globally unique ID.

Leo: Ah. So each ActiveX control has this ID.

Steve: Right.

Leo: And you set the kill bit individually for each ID.

Steve: Exactly.

Leo: Got it. So you're going to find – you don't – you need to know that – it's actually a CLS ID, I think they call it, when it's an ActiveX control. You need to find that ID number and then – in your registry, and then turn the kill bit off. Or better yet, use this script. It'll do it automatically.

Steve: Well, actually, and it may not be in the registry. It may or may not already be there.

Leo: Oh.

Steve: But you do need to add a key...

Leo: I see, I get it. I get it.

Steve: ...in order to add this optional kill bit. And then that'll prevent IE from having access to it.

Leo: Got it. Got it.

Steve: And then the last thing I wanted to mention is something I've talked to you about before. This is just in the errata section. And this is a program that I just want to tell our listeners about because I'm – I can't live without it now. And I learned about it from seeing it demoed last time I was on the Call For Help show with you, Leo, up in Toronto. And that's a little piece of freeware called allSnap. AllSnap...

Leo: You're really a fan of this.

Steve: And what brought it back again...

Leo: Mike, Mikey discovered this one.

Steve: Yeah, well, what brought it back again is that I was talking to my tech support guy, Greg, on the phone yesterday. And we were, you know, covering our, you know, and sort of catching up on various GRC stuff. And he said at the end of our conversation, "And you know what I can no longer live without?" And I said, "AllSnap?" He said, "Yes." Because he's anal in sort of the way I am. You know, I was telling you that I spend all this time adjusting the position of my windows so that the, you know, they're exactly on the edge of the screen. And all allSnap does is makes the edges of windows and other application windows sticky. So that, I mean, you know, and we've seen these in some apps have a UI where their own windows will be sort of snappy. They'll, like, snap to the edge of your screen or in the upper corner, just to sort of place themselves for you. What this does is this just installs a global hook in Windows that provides this sticky functionality to your entire OS experience.

Anyway, just if anyone puts allSnap, just one word, allSnap, into Google, it'll take you to the programmer's site and to a free downloads page. And it's very clean. When I use a Windows – I have a whole bunch of Windows machines. And I think they all now – except I think I have one XP machine that doesn't yet. Whenever I'm using one and the windows don't snap, it's like, okay, you know, I'm going to install this right now before I go any further because I just – I love it so much.

Leo: We'll put a link in the show notes, too, since people obviously want this. Now I'm wondering if I need one for the Mac.

Steve: Exactly. I mean, I wish the Mac had it. So...

Leo: Well, it's probably pretty easy to write, so I'm sure somebody will do that just for you, Steve.

Steve: Well, if so, I want to know about it because it would be great if the Mac had it, too.

Leo: AllSnap.

Steve: So I wanted to talk today about something I've been – I've had on my mind for months. Because I've been trying to figure out when I'm, like, talking to my friends and family, you know, we're talking about, you know, the war in Iraq and, you know, whether it's made us more safe or less safe, and denial of service attacks and like, and why, you know, why there isn't anything people can do. We were talking about this, you know, you and I, Leo, just the other day. And also, similarly, like this new ActiveX zero-day exploit. I mean, all of this is sort of why is security so difficult? And I finally, I think, came up with sort of a way of framing an answer that I really like. Because, you know, as I'm talking to friends, you know, they know I'm into computer security. And it's like, well, you know, why is it such a problem? And...

Leo: Let me – when you frame it that way, do you mean why is it so difficult to make a secure operating system? Or why is it so difficult for end users to secure themselves?

Steve: No, why is it so difficult for the United States to be secure even.

Leo: Oh, that kind of...

Steve: I mean...

Leo: So just why is it so tough to be – to make something secure.

Steve: Yes. Why is security – and I'm glad you asked the question because I want to make sure, I mean, like, everything, you know, against terrorism, against denial of service attacks, which is sort of a form of terrorism, against ActiveX controls having bugs in them, why is this so hard? You know, what's the problem? And I, you know, I mean, I knew sort of in my guts just intuitively that I – it was interesting, I was having a hard time communicating it. And so I've spent a lot of time trying to figure out how to explain to people what the problem is. And I've come up with something that I like because I think it begins to address that. And so I define security as the absence of all insecurity. And I think that's the way to think about it.

Leo: That makes sense, yeah. So all right.

Steve: So, well, and so if you think about that. So security is the absence of all or any insecurity.

Leo: Eliminating all danger or, in the case of computers, eliminating all chances of loss of privacy, loss of integrity.

Steve: Or eliminating all bugs.

Leo: Well, that's the problem with computers, isn't it.

Steve: Exactly. And so, I mean, that begins to take us towards an understanding of why we continually have these problems is that, you know – and it's also why – I mean, I really like this because the more I think about this definition, security is the absence of any and all insecurity, it then, for example, answers Steve Ballmer's famous outrage about why do we still have all these buffer overrun bugs.

Leo: Right.

Steve: I mean, it says the only way to be secure is to have absolutely nothing that's not secure. Because anything that is not secure obviously creates an opportunity for insecurity. So, you know, it's well understood that software has bugs. I mean, you know, and I've heard – I cringe when I hear people say, oh, well, all software has bugs. Because, I mean, you know, I take it personally because I'm a software developer, and I would like to imagine that my software, at least, doesn't have bugs. But the fact is, this software is incredibly complex, as I've certainly said before. That's, I mean, you know, that's my defense for this.

But I've – in thinking about this more in the context of security, I realized there are two different classes of software bugs. There are bugs and problems that users stumble over in normal use. That is, you're using some application, and it does something wrong. And it's like, oh, okay. I mean, and frankly, I'm sure anyone who uses Windows and PCs in general has just sort of become accustomed to that. You know, the software that they use oftentimes, you know, freeware, shareware that they've downloaded that's going to perform some useful utilitarian task, there'll be something about it that just kind of doesn't work right. And it's like, okay. And, you know, you close it and restart it. You figure out a workaround yourself. Maybe you report the problem. But, you know, we're encountering them all the time. So one class of bugs are those sorts of things, the things we stumble over in normal use.

But a very different kind of bug are those which manifest themselves from deliberate abuse, that is, deliberately doing something that the software author didn't expect, didn't plan for, didn't protect against. And it's fundamentally different than – that is, to try to find problems than to stumble on them when you're not trying to find them. Because it's – there is just – the nature of the software we're using is that it is, I mean, well, to finish that sentence, that it is so complicated. I mean, and if nothing else demonstrates that, just look at the size of the code now that we're loading onto our machines. You know, it used to be, I mean, we all remember the day where you would buy a software product, and it had a couple floppy disks, you know, a couple 1.44-meg diskettes. Now nothing doesn't come on anything but CDs. And it's, you know, it's hundreds of megs. And so there's just – there's so much more code and so much more opportunity for mistakes. So this notion that software could appear to be fine if it's functionally okay, yet still have exploitable problems if someone were actively trying to find them. And of course that is what hackers are doing today.

Now, the reason we're seeing so many problems with Internet Explorer now is that there are two ways that hackers have access to us. Either they come to us, or we come to them. Now, the traditional big problems that we saw in the earlier days of Windows, actually before Service Pack 2, were, you know, were worms, Code Red and Nimda and Blaster and these big worm problems. Well, worms were things that came to us. That is, they were a real problem because they were inherently able to exploit an opening that existed in a large base of Windows platforms in order to attack the computer remotely. They came to us. The reason that XP Service Pack 2 was such a win is that Microsoft finally turned on the firewall by default, so that no longer, unless something, you know, special was done, but in any event you wouldn't, you would no longer have the default majority population of Windows machines accepting unsolicited incoming traffic. Well, in one day, I mean, in the day that Service Pack 2 turned on the firewall, the huge problem of they come to us ended. And, I mean, and things are, like, way better ever since.

Leo: Yeah, it fixed it. It just fixed it.

Steve: It just – and, you know, overnight.

Leo: Yeah.

Steve: And so, you know, as I was saying for years before that, I don't blame Microsoft for mistakes. I was upset with them for policy. And their policy was to have all these services running with open ports, I mean, literally creating the they-come-to-us trouble, which they finally, thank goodness, ended by turning a firewall on by default. And of course way before that anybody that was following along with the good idea of running a NAT router – a NAT router of course being, you know, a hardware firewall in the sense that any incoming traffic is just dropped unless it's expected – that also would have terminated the them-come-to-us trouble. But on the other hand, as the success of the worms demonstrated back in those worm years, the huge bulk of Windows machines were not behind any kind of firewall. Those Microsoft services were exposed, and they were coming to us.

Now, what we're left with then is the reverse model today. And I don't see this going away anytime soon, unfortunately. And that is the we come to them. And that of course is all the current exploits and troubles that we've been talking about are inherently we come to them. And of course the way we come is with our browser. That's the way the computer extends itself out onto the Internet.

Leo: That makes it a lot easier for hackers. They don't have to come to us anymore.

Steve: Well, it's easier from the standpoint of they lay traps which some number of users fall into. But it is certainly the case that the number of machines affected by any of these traps is inherently going to be much smaller because, you know, no super-popular, high-volume website, you know, Google, Amazon, MSN, and so forth, you know, CNET, you know, none of these big sites are under control of hackers. You know, certainly it's conceivable that they could have a problem, that a site could get some malicious code installed on it that would affect a lot of people in a short time. But that's, you know, that's the exception rather than the rule. So it is worth mentioning, especially in the context, Leo, you were saying of like, you know, us crying wolf or the sky is falling. It's worth noting that it's only people who are generally venturing out and want to poke into dark corners of the Internet that are exposing themselves.

Leo: Well, but I have to point out, there have been cases, MySpace leaps to mind...

Steve: Ah, it's a perfect example, yes.

Leo: ...where 50 million people frequent this. MySpace is one of the most popular spaces on the 'Net and is absolutely a place, a vector for infection.

Steve: Yes, that's a very good point. And so there's a place where the we-come-to-them model can still infect a huge population of users. So anyway, I really liked finally coming up with a way to explain to my non-computer-savvy friends, you know, why security is such a problem. It's that, you know, to really be secure, you must really be secure. Which means no opportunity for insecurity. And of course then computer-savvy people understand what that really means. I mean, that means...

Leo: It’s impossible.

Steve: You must have bug-free software.

Leo: Right.

Steve: And that’s just, you know, no one sees that happening in the near term.

Leo: If I were to boil this down in Socratean terms, perhaps, it’s axiomatic. Well, first of all, as you did, you defined security as the absence of insecurity. And the only way to be secure is to have nothing that is insecure, in other words, no bugs. It’s axiomatic that all software has bugs. And since bugs often create security holes, all software is inherently insecure.

Steve: Well, and it’s worth noting, too, that this recent zero-day exploit was an interesting lesson because a component that was not IE, that is, a Windows core service component that was invokable by IE, was where the problem was found. And so, again, the we-come-to-them model, which would otherwise not be useful – for example, you know, I’m looking right now at a stopwatch app sitting here telling us how long the show’s been going on. Well, it may have bugs. It may have exploitable bugs. But I’m not going out on the Internet with my little stopwatch application. So the fact that it’s got some problems doesn’t hurt me. It doesn’t represent any kind of a problem. Now, that...

Leo: It’s a problem, though, in Windows, because so much of it is available to IE. I mean, once you put the browser as an integral part of the operating system, you’re really in many ways making things worse.

Steve: Well, Windows has become componentized. And that, you know, and that’s what they call, you know, OLE then became ActiveX. And it is inherently a component-based system.

Leo: It’s designed to be a network-aware operating system. And IE is always running. You cannot not have it running.

Steve: Well, the other thing worth mentioning is that – and I mentioned my little stopwatch app that is not on the ‘Net. One of the things that we see happening is that mainstream applications...

Leo: May be on the ‘Net.

Steve: Yes.

Leo: They dial, they phone home.

Steve: More and more mainstream applications are adding Internet connectivity and Internet features because they're looking for ways, you know, as they get past Version 4, it's like, okay, how are we going to sell more of this? We need to, you know, add more features. Well, everything's networked these days. Everything's the Internet and connectivity and peer-to-peer and all that. So the next level of problem after Windows, if Windows ever really becomes bolted down enough that it's not the majority target, we're going to see the network-enabled applications which are the most popular begin to be the next round of attack target. And then it's not just Microsoft that needs to be really careful and really aware of bugs. It's all third-party programmers.

Leo: Oy, oy.

Steve: And I don't ever see that happening.

Leo: Yeah. Wow. I think, you know, for a while the Department of Defense tried to solve this problem with bulletproof languages, Ada, for instance, that kind of forced – the whole idea of Ada was a bug-free language that forced programmers to not make errors. I don't know what happened to Ada.

Steve: Well...

Leo: Maybe it was undoable, I don't know.

Steve: Next week's topic is Vista security.

Leo: Oh, boy.

Steve: I've delved in and spent some time because I want to follow up on this week's issue of like, okay, if security is the complete absence of all insecurity, where is Microsoft going with their own security initiatives, and what's been added to Vista, and what's the difference between 32-bit and 64-bit platforms. And I've got some surprising news there. So...

Leo: Good.

Steve: ...that's what we're going to do next week.

Leo: Well, now we know why security is so difficult. In fact, I think you might have said, why is security impossible?

Steve: Impossible, I'm afraid.

Leo: Yeah. And it's – and as you've always said, it's a process. There is no end to securing yourself. It's a process.

Steve: Well, and it's not like the 100,000 listeners we have of Security Now! are all going to get their machines destroyed. It's that, inarguably, some percentage of Windows users are being infected, and it's not a small percentage, every day. I recently saw something that said two thirds of average Windows computer have spyware and malware installed on them of some sort.

Leo: Yeah. I mean, I know just from doing the KFI radio show that it's endemic.

Steve: Yup.

Leo: No one has an exact number, although the study I've seen, as you say, are far more than half. And but just anecdotally, from talking to people, that's the number one concern of Windows users, spyware and viruses are. And it's not hysteria. It's a very real problem.

Steve: Yeah. And again, it's not like it affects everyone. You know, the old days with the worms, where if they weren't behind firewalls, where we had the they-come-to-us model, well, we know, you stick an unpatched XP machine on the 'Net, and it's compromised in minutes. I mean, that's the case today. But all current XP machines are behind a firewall, and hopefully behind a NAT router, so that's just not a problem. You know, they come to us is over. But we've still got this we come to them. And...

Leo: And we're coming to them more and more.

Steve: And we're coming, baby.

Leo: Hey, thank you, Steve. Want to thank our sponsors, Astaro Corporation. They know that security is a process, and they make it possible for big business, little business, and even home users to be secure with the Astaro Security Gateway. If you're a small or medium business network that needs superior protection from spam, viruses, and hackers, as well as 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. There's a link on our show notes, makes it easy to get there. Or you can call them, 877-4AS-TARO, to schedule a free trial of an Astaro Security Gateway appliance in your business. I have a 120, and I cannot tell you how fantastic it is. It is incredible. Based on open source, built to withstand anything.

And if you're a non-business user, by the way, you can get it for free, the software version, at Astaro.com. Install it and run it on any old PC box, and you'll get the same benefits. Pay a small, I think it's 79 euros a year, small fee, and you can have all of the antivirus and spam and so forth, too. I think – I want to see – I expect to see more and more people with home networks using Astaro to protect the entire network. It really is a great solution. Astaro.com. We thank them for major financial support for Security Now!.

We also want to thank the folks at Dell for providing major financial support. Dell.com. Actually the best way to go is probably to go through TWiT.tv. We have a special Dell page. If you just click the link at TWiT.tv or go to TWiT.tv/dell, we have some picks there. But don't be just limited to those. Anything you want from Dell, if you go through those links, we get credit for anything you purchase. If you're buying a Windows PC, getting ready for Vista, Dell has some great stuff. I love this XPS 700. You know, I'm just – I'm about to buy one. Now that they have the Vista express upgrades, I think it's time to pull the trigger and get that XPS 700 I've been eyeing for so long. TWiT.tv/dell. We thank them for their support.

Steve Gibson's website is GRC.com. That's the place where you can find Security Now! show notes, [transcripts] thanks to Elaine, and the 16KB versions for the bandwidth impaired. We've got a lot of show notes today, particularly to allSnap, and we'll put in a link to – I have a link, and I'm going to put it in the show notes, to "Your Guide to Using IE Safely." I wrote it up at one point with pictures and everything. So I'll put that in the show notes. And the kill bit – I want to call it Kill Bill. The kill bit – you might want to kill Bill after all – the kill bit registry patch, with apologies to Quentin Tarantino, and more at GRC.com. That's also where you'll find SpinRite. Any good SpinRite letters this week?

Steve: Actually I did get a really fun one. Some guy said he's both a loyal customer and fan of SpinRite and GRC since 1997.

Leo: Wow. When did you start making it? '95? '96?

Steve: Oh, it's 19 years old, Leo.

Leo: Oh, it's older than that, wow.

Steve: Oh, yeah, yeah. Anyway, so he says – I love this one. He says: I do volunteer work for the Alberta Diabetes Foundation. Donors have provided systems to the ADF for a number of years now. Every time one of these systems will not boot, and it appears that the hard drive has crashed, I run SpinRite.

Leo: Oh, interesting. There's a good test.

Steve: Isn't that cool? So, like, people are bringing dead computers in, you know, donating them because their computer died.

Leo: Yeah, thanks.

Steve: So this guy goes on, he says: The number of times I've been able to call up a donor and ask them if they would like to have the data off the drive is incredible. He said: And this happens after the system has been in some shop that declared it DOA. When they ask me how they can thank me, I always just say, "Thank Steve Gibson and GRC by purchasing SpinRite." He said: I have no way of knowing if this translates into any sales for you. But I will bet that GRC is who they think of the next time they get "OS not found."

Leo: Isn't that a nice – that is really a nice story. I like that.

Steve: I thought it was really cool.

Leo: Yeah.

Steve: So, you know, the person's machine dies, they go, oh, well, I'll just, you know, give it away to the Diabetes Foundation. Then a couple days later the guy calls up and says, hey...

Leo: Oh, by the way...

Steve: ...your computer was dead, but there's all this data here, would you like it? That's great.

Leo: I love it. Well, that's – SpinRite is everybody's favorite, my favorite certainly, disk maintenance and recovery utility. And that's also at GRC.com. And by the way, Steve has a lot of free security programs. It's worth browsing. People often start with ShieldsUP!, which is a good way to test your network when you install a new router or firewall. But don't stop there. There's all sorts of free software: DCOMbobulator, Unplug n' Pray, and all sorts of very useful tools. It's all at GRC.com. When's that new menuing system going in there?

Steve: I've got a little more work to do here before I get back to do that. But that's top of my list. And I did want to mention that at the bottom of the Security Now! page is a form that people can use to send questions and...

Leo: Oh, good, okay.

Steve: ...comments and notes and things. So GRC.com/securitynow will take you to the top of the page. Scroll all the way down. I'm going to have to rearrange, reorganize this whole Security Now! area because, you know, we're, like...

Leo: Well, it's growing like Topsy.

Steve: It is. We've got 65 episodes now. But all the way down at the bottom is a form that anyone can use to send questions and stuff directly to me. And I really appreciate knowing what people are thinking and what they want to hear about.

Leo: Good. And next week I know what you want to hear about: Vista security. That'll be a top topic, I know, with everybody listening. And we will see you here next Thursday for another gripping edition of Security Now!.