Listener Feedback Q&A #10

Description: Steve and Leo discuss questions asked by listeners of their previous episodes. They tie up loose ends, explore a wide range of topics that are too small to fill their own episode, clarify any confusion from previous installments, and present real world "application notes" for any of the security technologies and issues they have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-056.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-056-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 56 for September 7, 2006: Your questions, Steve's answers.

Security Now! is brought to you by Astaro, makers of the Astaro Security Gateway, on the web at www.astaro.com. And by Visa. Safer, better money. Life takes Visa.

Ladies and gentlemen, it is time to talk security once again with the king of all things secure, Mr. Steve Gibson. He was up in Canada last week with me, and we said farewell to Amber. And he sat on my bed with his sock puppet and wept his crocodile tears.

Steve Gibson: For people who weren't there, Leo, this is sounding very strange.

Leo: Yeah, you have to listen to Frank Linhares's techPhile podcast because we did a podcast in my hotel room with Steve – you were great. And Mike was there from commandN, and Amber, and Frank, and me. And it was a fun podcast.

Steve: We just talked.

Leo: Yeah, it was really a fun podcast.

Steve: We just sort of hung out.

Leo: Yeah. But it was Amber's last week. And Steve said – it broke my heart – "I'm never coming back. There's nobody to hug." You can hug me, Steve. Okay, never mind. Forget I said anything. We're going to do a Q&A. It is mod 4.

Steve: Yup.

Leo: And mod 4 means divisible by four. So Episode 56 is divisible by four, if I remember my grade school math. Lots of questions from listeners all over the world who listen to Security Now!. Anything you want to catch up with, with our sandboxing from last week or...

Steve: We're going to – next week I want to do a review, essentially a comparative review of the VMware products and of Microsoft. Several people have written in when we were talking about VMware saying, hey, what about Microsoft's Virtual PC? Because it's free, too. And it turns out that VMware has a server version which is also free, even though what I've been talking about and what I myself have always used is their VMware Workstation, which is not free. So it's like, okay, I really need to, like, figure this out because there's been a lot of interest raised in this whole notion of creating virtual machines to operate in securely.

Leo: Right.

Steve: So we're going to do one more episode on the whole sandboxing VMs for security topic.

Leo: Great.

Steve: And I got a really neat note from a listener actually about SpinRite that I want to read next week. I don't have it here in front of me. So I'll track it down. Because it was just – it was just a perfect little – a perfect little experience.

Leo: All right. Well, let's kick off with Question No. 1, John from Piedmont, California. He says: Back in Episode 51 – that was the Vista's Virgin Stack episode.

Steve: Right.

Leo: You guys were worried about bugs that Symantec engineers had found. But those had already been fixed in the later betas. And now, of course, we're in release candidate one or maybe even release candidate two. I mean, we're getting very close to the final version of Vista. And he's also read that Microsoft is opening Vista to hackers. They actually offered copies to 2,500 hackers at the Black Hat Convention, just so they could pound on the OS before it's released. Well, all OSes have bugs, says John. Microsoft's doing everything it can to remove them. Isn't that enough? Isn't Microsoft behaving responsibly?

Steve: I would say yes. I think that Microsoft is doing what it can. My concern, and really the whole thrust of our talking about Vista's Virgin Stack, was really to drive home some sort of philosophical and theoretical aspects of security. For example, I'll remind people that Microsoft opened Windows XP to hackers also. And Windows XP was a catastrophe.

Leo: Right.

Steve: From a security standpoint. So the idea of over some relatively narrow window of time of telling people, okay, everybody pound on it and see what you can find, that isn't the model for the way security problems are found. You know, they're, you know, Microsoft could do that, or Microsoft would solve those problems. The thing that finally made the difference in Windows is when Microsoft finally started running the software firewall by default. Suddenly everything changed because, even though ports were opened behind the firewall, they were no longer exposed to the outside. And, I mean, had that been done from the beginning, we would have had none of those Windows XP worms that were such a problem in the beginning. So philosophically, Microsoft finally made the right decision to be running a personal firewall that blocks incoming traffic by default. And...

Leo: But it's not, you know, that's just – that's nice. Of course there were a lot of security patches, too. But it's not just that that's going to make Vista secure or not. I'm sure the firewall will be turned on in Vista.

Steve: Well, that's what's going to make this such a party for us. For example, Microsoft has said that they're building in a peer-to-peer technology by default, which will be running by default.

Leo: Oh, that's nice. So then...

Steve: Yeah.

Leo: ...it doesn't matter if you've got the firewall turned on, you've got a server.

Steve: You'll have something that has built-in NAT traversal that allows incoming contacts. So, I mean, and we know, for example, that even if you had a connection to a remote location, if you've got a brand new stack that has not had, you know, all the bugs pounded over, pounded out of it over time, there are going to be problems. And so what was so illuminating for me was to see that Microsoft – and the reason we called that episode the "Virgin Stack" – Microsoft was repeating all the mistakes, well, many of the mistakes which had been already made and fixed 20 years ago at the beginning of UNIX Internet stacks.

Leo: So you're saying even – oh, yeah, of course they're patching those as time goes by, and a lot of them have been patched. But the fact that they even made them again is not encouraging.

Steve: Right. Well, the fact that they made those mistakes is – essentially it proves the point that a brand new stack, written from scratch, is going to be a problem.

Leo: Yeah.

Steve: Just it's going to be a problem. And we'll find that happening, I'm sure.

Leo: And we'll see how much of a problem soon.

Steve: So Microsoft says they did this because they needed to start again. I respect them for not dragging their old code along forever and, you know, adding patch on patch and feature and glomming things on. I mean, certainly starting over, knowing now what they wish they had, they can build it. So that's the good news. The bad news is there is a security cost to doing that, that we're going to be spending a lot of time talking about in the future. There's just no way around it.

Leo: That's good. Just gives us something to talk about.

Steve: Yeah.

Leo: If it weren't for that, we wouldn't have anything to talk about. Dave Rozendal asks from Michigan: Regarding Episode 45 – we were talking about the hosts file – can you password-protect the hosts file?

Steve: Yeah, I put that in because there have been a number of people who have asked the question. And I wanted to talk a little bit about the use and misuse of the hosts file. First of all, there are ways you could protect it. For example, if you used, assuming that you have an NTFS partition that supports Microsoft security policies, you could make the file writable only by the administrator...

Leo: That's a good idea.

Steve: ...and – yeah. And then, as we recommend, run as a non-administrative user. Then if something that you ran by mistake, like, you know, a script in a browser or a program that was doing something behind your back, any such program would be locked out from being able to modify the hosts file unless it went to much greater extent to acquire, you know, a so-called "privilege elevation" of some sort. And there are ways to do that. But it's just – it's much more work. So...

Leo: Now, let me ask, though. The hosts file, if you're not running as administrator on a normal operating system, you wouldn't be able to modify it anyway. You wouldn't have to change the permissions on the hosts file. It just wouldn't be accessible because it's a system file. I don't know about it on Windows. I don't know what it is.

Steve: Well, that's exactly the case. However, most people who are not security conscious are already...

Leo: Are running administrator.

Steve: Exactly.

Leo: Right, right. So don't run as administrator, for sure.

Steve: Yeah. And so the real issue is, clearly someone wants to password-protect the hosts file because they're concerned about malware modifying parts of their system. Well, if you've gotten to that point where malware is in your system, then you're really already in serious trouble.

Leo: Right.

Steve: I mean, it's like it's – I don't want to say it's too late. Certainly you can – there's malware that doesn't modify the hosts file. So having a modified hosts file could prevent that malware from looking up the domain that it's trying to find, trying to phone home to, and could confuse it and still give you some protection. On the other hand, there is malware that does know about the hosts file. And we've seen instances where malware, for example, is changing domains for antiviral companies or putting entries in the hosts file for antiviral companies. And even Microsoft trying to prevent you from updating your patterns to identify that very malware which you've just acquired in your system. So we know that there is malware that does modify the hosts file.

The best you can do is – and again, the thing that's frustrating for people is everyone wants security to be black and white. It's just not. I mean, there's just – there's nothing about security that is absolute and black and white. It's a matter of using layers of protection because it's how, for example, we've recommended multiple spyware utilities. Rather than just one, using three is better because there will be some overlap, but there'll be some programs that one will see that another won't.

Similarly, the hosts file is another – is a good thing to do, but it's not absolute protection. You know, the phrase "absolute protection" is a misnomer. I mean, it just – it's an oxymoron in security. It doesn't exist. So in general you should think of the hosts file as, like, one more useful good thing to do, but not ask it to provide more protection than it really can. Fundamentally, if there's bad software in your system, you're already in trouble. And then you really can't trust anything that happens from there on.

Leo: Art in Washington, DC, is juggling. And he's not a juggler. He's considering remote access options for his users. He writes, first of all, he's having a policy to use VNC over a VPN to securely allow access for my end users, access to their desktops from home. A good idea. And here's the details. He wants to allow a thou- he's got a thousand or so users.

Steve: Yeah.

Leo: That's a lot of seats – access to his network, a business network, from home. They have purchased a VPN, but they're concerned that their home computers might have viruses, naturally. In fact, the chances are, if you have a thousand home users, that you have a – almost certainly that there's some viruses.

Steve: You've got a few in there, yeah.

Leo: We're worried that the remote access will make improper downloads of sensitive data

too easy, because they have consultants that come and go. A nice solution seemed to be to give the users some kind of desktop sharing to their local machine from home. Since the only thing going across the network should be bits of screen pixels, it seems to be more secure, albeit slower in performance. I guess that's why he's thinking about VNC. This would also solve the issue of having to purchase and install applications on the home machine. VNC is rumored to have security flaws, and the other products – GotoMyPC, GotoMeeting – require fees. Also an interesting one is WebHuddle – I haven't heard of that. A Java...

Steve: No.

Leo: ...open source screen sharing tool. However, it seems buggy. He's got a quandary, doesn't he.

Steve: Yeah.

Leo: Since many of the users are still on Windows 2000, the Remote Desktop feature of Windows is not available. I don't know if that's the case. And we do have a hundred or so Macs. Any ideas or comments? Just to – I'll throw something in.

Steve: Yeah.

Leo: You can use Remote Desktop with Macs and Windows 2000. It's the host machine that has to be a Windows – well, in fact, if you're doing it on a network, I don't think even that has to be a Windows XP.

Steve: Well, and Windows 2000 Server will be...

Leo: That'll do it.

Steve: ...is able to run terminal services, but not the non-server version.

Leo: So Windows 2000...

Steve: Professional, I think it's called. Well...

Leo: Windows XP Professional is the server. But I think anybody can be a guest on there. Anyway, that's one...

Steve: Yes. You're able to run the client from any kind of machine.

Leo: Yeah, and including a Mac.

Steve: Yup.

Leo: So that's answer one to that. I guess really the bigger question is, is it possible to be secure doing what he wants to do, VPN to VNC.

Steve: Well, yeah. The reason I thought this long question was really interesting is that it does – it sort of morphed from a policy or philosophy standpoint. You know, the idea being, what he wants to avoid, even though he's got VPN technology already and, you know, certainly for – he's got some serious VPN technology if he's got a thousand users who are able to use this. That, you know, that's a nice big system. His idea is, he doesn't want to use the VPN simply to allow remote telecommuters to connect into the corporate network and be a peer on the corporate network, for the reasons he states. You know, if there was a virus, then the virus could, you know, crawl up that wire.

Essentially, what this means is, you know, as we know about VPNs, that anyone connected to the corporate VPN, their computer is, for all intents and purposes, on the corporate network. And so for him, he doesn't mind the machines that are physically located in the corporation being on the corporate network, obviously, that's what they're plugged into. They have to be. He's concerned, and this is a really useful concern, about too carelessly extending those corporate – essentially the corporate network through the VPN to remote machines. Now, many people do that. And, for example, you know, it's what, you know, for, like, personal users it makes a lot of sense to be able to access your home network while you're out roaming around. So his alternative is to restrict what can be done through the VPN to running VNC. And so essentially his question was, given all of that, if VNC has security problems, would encapsulating it in the VPN solve those problems? And the answer is yes.

Leo: Good.

Steve: And so...

Leo: Simple enough.

Steve: So it's a nice solution. You know, there are many different VNC variants. Some are inexpensive; some are open source and free; some are fast; some have, you know, different features. There's a bunch of them. But by running them within your existing VPN, all security issues of, like, having a VNC server that's exposed and could be logged onto by malicious people, all that goes away. So it really is a great solution.

Leo: Good. There you go. See? Fabian from Bonn, Germany says: After reading the Windows Vista Security Report by Symantec you mentioned in – again, we're talking about this virgin stack issue in Security Now! 51 – there's something I don't understand. On page 5 of the report – wow, he got farther than I did – they mention that Vista employs NAT traversal via technology called a "Teredo," or "Teredo," and that it will make your Vista hosts that are behind a NAT router externally visible. I guess that's the peer-to-peer you were talking about, Steve.

Steve: Yes, exactly.

Leo: Since this is enabled by default, does it mean a Vista machine announces itself automatically to a public server in order to provide NAT traversal?

Steve: Yes.

Leo: Uh-huh. That's how it works. They say in the paper that many, quote, "many individuals and companies use private addresses as a key part of their defense strategy and may find their Vista hosts externally reachable to an unexpected degree unless strict egress filtering is in place." In other words, unless my personal firewall blocks outbound traffic from that service, my machine will be visible on the Internet. This would mean that your recommendation and Leo's recommendation of NAT routers are practically void with Vista machines, wouldn't it? Ah, really. Or does all of this only apply once I enable IPv6 on my network?

Steve: Well, this is a perfect example of Microsoft extending the functionality beyond what's been well proven and...

Leo: Beyond what anybody's asked for.

Steve: Well, that's exactly right. I mean, you wonder why they have this thing turned on by default. And the reports have been, this is on by default.

Leo: I do want to say, though, this is still beta software. And I always hesitate to comment on beta software because you don't know what they're going to turn on or off when they ship this thing.

Steve: That's very true. Although, even if, I mean, it's worse that it's on by default. It's a concern that people may be told to turn it on when they don't need to. For example, Universal Plug and Play, you know, is, like, on all the time and...

Leo: That was on by default, too.

Steve: Even when people don't need it and aren't using it. So it's...

Leo: I think it's unlikely, I'll be honest, given how people feel about peer-to-peer and the fact that they're trying to get Vista adopted by businesses that hate peer-to-peer, that this would be turned on by default. I just don't find that likely.

Steve: Well, let's hope not because it does – from everything I've seen, it's exactly as Fabian suggests, that Windows makes an outbound call, registers itself with a server. I mean, this is the way, you know, many other peer-to-peer systems work. You know, you and I are both...

Leo: But we choose to run those.

Steve: Exactly. You and I are both using Skype. But when we run our individual Skype clients, it connects into the Skype server. Hamachi is the same way. All the Hamachi clients tie into the central server, and that's how the clients are able to find each other. Well, Microsoft has developed the same sort of approach, but now it's at the OS level. Sure, it's cool that this functionality that we're all using currently in individual applications will be subsumed by the OS as a whole. It just – it certainly is a concern from a security and privacy standpoint.

Leo: Yeah. Yeah. Wow, okay. Well, we'll keep an eye on it. But again, I find it hard to believe that they would do that by default. But you never know with Microsoft.

Steve: How many years did we have Windows running services we didn't need?

Leo: You just never know. But they've learned, I mean, I've just got to think they've learned. Dave Matthews of Richmond, Virginia, writes: I know you advocate using the administrator or equivalent account only when necessary. You did just again a few minutes ago.

Steve: Right.

Leo: I took your advice, he says, and made the change about five months ago. I'm surprised at how seldom it's actually needed. However, I did run into negative feedback around the water cooler regarding Microsoft Updates. Are security patches installed automatically under a normal level account? If so, how can I confirm this on my machine?

Steve: Well, this question had a couple points that I really liked to discuss. First, for what it's worth, the Windows Update system runs as a system-level service. It's a classic Windows service running with system-level privileges. So it's not running in the user account, it's essentially running in the background as an extension of the operating system. It's the kind of thing you can turn off if you want to, if you go into, you know, the services applet. There's a list of all the stuff that's available in the system. Some of it you can start by hand. Some is running all the time. Some you can disable, some you can stop, and so forth. But it is running with system-level privileges, which it needs because it's replacing core system DLLs and making changes to the core OS, essentially on the fly, although often you have to reboot in order to flush all the old stuff out and get the new code to load. The second part is...

Leo: I don't think security – I'll be honest. I don't think security patches are installed at all until you run as an administrator. Because no other thing can – nothing else can be installed. You can't – for instance, try to update your antivirus. Try to install software. You can't if you're running as a limited user.

Steve: Well, that's true except that Windows's own security system, you know, built into Windows, is running as a system-level service. So I'm pretty sure you can run as a non-privileged user. You'll get the little notice that Windows – that updates have been downloaded, do you want them to be installed, you say yes...

Leo: Boy, I think that's – if that's the case, then it's not very – that's not a good setup.

Steve: Okay.

Leo: I just – because it's just too easy to spoof that.

Steve: Well, and there's – that is the second part I wanted to bring up is that, you know, the concern around the water cooler, as Dave puts it, is, I mean, this is why all of us oldsters, you know, the old computer guys who've been around, were really looking askance for quite a while at this whole notion of, like, giving up one more aspect of control to Microsoft. It used to be that you could, you know, voluntarily download these updates and install them when you wanted to. And, of course, gradually we've been moved away from that model to the point now where, you know, the Windows Automatic Update is on, and you are berated if you turn it off, and you're warned and cautioned, and little shields appear on your taskbar saying, oh, no, you don't have updates turned on. It's like, okay, fine, you know, just take care of this for me. So we've been incrementally losing more and more control over our system. And so that, you know, thus the water cooler talk. You know, he's certainly right that we are now victims to what Microsoft chooses to do with our systems. And of course, many corporations deliberately have this stuff off by policy because they want to vet and verify any of these changes that Microsoft makes prior to putting them onto their corporate-wide deployment.

Leo: Here's a – this is from an MVP, a Microsoft VP for Windows security: If you set Automatic Updates to notify before downloading, or notify after downloading, no updates will be applied, and no notice will be offered to the limited user. But as soon as an admin logs on, the Automatic Updates icon will pop up. In other words, it won't install if you're a limited user. If you set AU, Automatic Updates, to the third option, that is, automatically update, right, then most updates will automatically install for a limited user, and automatic updates will also force the limited user to reboot if necessary.

Steve: Yup.

Leo: However, service packs which require a license agreement, i.e., SP2, will not automatically install for limited users. So if you want to install a service pack, you'll have to log in as admin. I think, if you run as a limited user, it would behoove an admin to come in from time to time and log in. Or it would behoove you to log in as an admin from time to time.

Steve: Yeah. I think the typical model would be, for example, in a corporate environment, if they were allowing Windows Updates to occur, and the users were running as a non-admin user on the machine, then they would be happening in the background. People turn their computers off at night and turn them on in the morning. And with that morning reboot, everything gets updated.

Leo: Except for the stuff requiring a license agreement.

Steve: Except a major service pack deployment, right.

Leo: Right. And that's, again, only if you have the full Automatic Updates turned on. If you have Notify in any way turned on, it won't do it.

Steve: Right.

Leo: So I, when I have users running as limited user, I make sure that periodically they log on and do system update and update their antivirus. Because even if Microsoft will update, nothing else will update.

Steve: Right.

Leo: So you've, I mean, a limited – that's, I mean, there are a lot of drawbacks, unfortunately, to running Windows as a limited user. It's not easy.

Steve: Yup.

Leo: But it's also the only safe way, I think.

Steve: Well, yeah, because it does restrict – not only does it restrict you – and the whole point is it restricts any programs running in your session, that is, any, for example, malware or spyware or something – they are similarly restricted to the changes they're able to make to the underlying OS. And what's really annoying is there's all sorts of ways around that. I mean, it's sort of a – it was a good idea, but it was a faulty implementation. One of the things we're really hoping for is much more robustness in this regard from Vista.

Leo: See, in my opinion, no system files should be changeable unless you have an admin log in, period.

Steve: Right.

Leo: Regardless of, I mean, I guess it's somewhat protected because it's running as a Windows process, you know, Windows own process. But I don't buy it. I think it's just – it's just not safe unless somebody has an admin password for system files to be modified. Period.

Steve: Yeah.

Leo: I think. But you're the expert. I'm just saying. And I'm looking at UNIX in particular. If you don't have an administrator log in, you can't change a system file. I don't care what happens. And the operating system can't, either. Although...

Steve: Well, and...

Leo: ...processes can run as administrator, I guess.

Steve: Yeah. The real problem is, Windows is so complex now, there are so many ways around things. I mean, the fact that debuggers are able to open up other processes and modify them means that, you know, there really is no real isolation among processes.

Leo: Right. Anish, writing from Google Mail, asks: Is it possible to use the hosts file to redirect sites to display an image file, a JPG, for instance? This would look nicer than the 404 errors in place of banners on websites.

Steve: I got a kick out of this because clearly he's implemented the hosts file approach that we've talked about. And now when he brings up...

Leo: Get big red Xs everywhere.

Steve: Exactly. And the answer is no. It's not possible. There are alternative approaches. There are various types of filters you could run...

Leo: Well, wait a minute. Now, if you – you're redirecting it typically to localhost, 127.0.0.1.

Steve: Right.

Leo: If you had a – you'd have to run a server. But if you had – but it doesn't have to be a fancy server. If you had a minimal server running, it could take that and put up a default display, yes?

Steve: Well, the problem would be that it would have to be clever enough – I mean, yes, there are ways around this. For example, that server would have to be clever enough to accept any request for an image of any name and return something.

Leo: Right. No matter what it gets it always gives you a pretty picture of a sunset.

Steve: Right.

Leo: So instead of red Xs you get a sunset.

Steve: Sized to fit the available space.

Leo: Oh, good point.

Steve: Presumably.

Leo: Yeah, it gets a little complicated.

Steve: It really does get complicated. There are filters that can be run. But just the hosts file itself, it's just going to give you little red Xs.

Leo: Scott Burr of Beaverton, Oregon, observes that: For anyone – whoops, I lost it. For anyone, like almost everyone – let me see if I can understand what he's saying. For anyone, like almost everyone, who has a lock, a key lock in a door for security, worrying about someone breaking into your computer system at home or your office becomes a secondary thought when they could break into your place and take it away with them easily. I don't understand what he's saying here. Let me...

Steve: Well, it's sort...

Leo: [Indiscernible] this?

Steve: Yeah. Actually, this is what Scott wrote. But I understood what he meant, and I liked it because it talks about the real difference with cyber crime versus physical crime. I mean, we all know that...

Leo: Oh, he's saying you could take the hardware with them.

Steve: Yes.

Leo: So who cares if you've got it secured?

Steve: Exactly.

Leo: I get it.

Steve: Exactly. And what Scott's missing is the fact that it can be done over a great distance with relative anonymity and in the dead of night – well, okay, maybe not. Or in the middle of the day, rather...

Leo: In broad daylight.

Steve: At noon, exactly. You know, it...

Leo: That's what's scary.

Steve: That's what's really the difference. I mean, we all have homes. I've got a lock on my door.

Leo: There's no such thing as a secure home, period.

Steve: I've got glass windows.

Leo: Right.

Steve: I mean, all you have to do is throw a brick through the window, and now you have gained entry. So...

Leo: It'd have to be a bunker.

Steve: Yes. And the point is, I think, that we understand the limitations of physical security. But in order for someone to be trying the front door or throwing bricks through windows, they're physically exposed to capture. They can be...

Leo: Plus it's a limited subset of the universe that can do that.

Steve: Right, right.

Leo: Your system could be broken into from anywhere in the world.

Steve: And a potential intruder can be scanning vast numbers of systems. It'd be like, you know, throwing bricks through everyone's window...

Leo: Right, right.

Steve: ...at the same time.

Leo: Right.

Steve: You know, so I guess the point is that there really is a difference in the cyber aspect of this. There was an interesting report in Government Computer News – I mentioned it to you last week when we were in Toronto, Leo – that terabytes of data have been downloaded from secure government networks by IPs in China.

Leo: Yeah.

Steve: And then like – it's like, okay, that sounds like a bad thing.

Leo: Bad thing.

Steve: Well, you know, those people get to stay, you know, behind their wall and, you know, suck our networks dry.

Leo: There's every evidence that there's vast schools of hackers in China.

Steve: Well, and apparently this notion of, you know, real cyber crime, cyber warfare teams being built...

Leo: Yeah. I think they're being trained.

Steve: And apparently we've got some in this country, too.

Leo: Yeah. Right. For them. Against the Chinese. You know, if I look at my logs, I mentioned to you the other day there's lots of people from China trying to break into my system using SSH and other servers. Always trying to crack it. Always, constantly.

Steve: Yeah.

Leo: Hundreds and hundreds of attempts, by hand, a day.

Steve: Yeah.

Leo: Now, a good point to make in this, though, is if you have a laptop that you carry around, it's a good idea maybe to secure the data on the laptop, if you have stuff that's private in there. I'm thinking the Veterans Administration specifically. Or many corporations.

Steve: Right. Well, and...

Leo: If you've got important corporate data on your laptop, encrypt it. Use TrueCrypt.

Steve: I was just going to say, yes, we've talked about TrueCrypt. It's a fantastic solution. It just needs to be done. And you keep seeing people losing laptops with unbelievable amounts of really important and private data. And it's just like, well, these tools are out there, they're free, but we're not using them.

Leo: No. So it's true, if somebody gets your hard drive, you know, a lot of the so-called encryption techniques aren't going to work very well. TrueCrypt will, though. There's no way they can get your stuff if you've done a good job of your password.

Steve: Right.

Leo: So do it. Seems simple to me. I don't know whether you – Keith Rocheck of Cleveland, Ohio, says: I don't know whether you guys plan more coverage of firewalls and routers. I was wondering what your opinion is about SmoothWall, as opposed to maybe a

router you'd pick off the shelf at a computer store. Patrick – SmoothWall, as you know, I'm sure, Steve, is a Linux firewall distribution. Patrick loves SmoothWall.

Steve: Yep, SmoothWall. And there's also m0n0wall is very similar. I liked the question because I want – and we've talked about it a couple times. Certainly the advantage of pulling a router off the shelf at Fry's or Target or wherever for $49 is that it's, you know, it's there, you plug it in, you snap your Ethernet connectors into it, and you're done. An alternative, though, that offers much greater power, is the idea of taking a retired computer, which, you know, a 486 or something old, slow, and pokey that you're no longer using, and adding a second network card to it, or maybe even a third if you want to get some true DMZ protection. And you can then download an ISO image of SmoothWall or m0n0wall, these are all open source and all free. And you boot this CD and/or install it on a hard drive, if you want to go that route. And, I mean, you've got a really full-featured solution.

Leo: Yeah, I like it. I mean, there are some limitations. I mean, but I think in general – some of these, by the way, will run off firmware, don't even need to run off a hard drive, so that you don't have to have moving parts, it'll be very quiet.

Steve: Right.

Leo: But, well, I guess there is no really, you know, limitation. You just have to be a geek and willing to put some time into it.

Steve: Yeah. I mean, I think that's exactly it. If your mode is not to play with this stuff, you just want solutions, then just buying the router appliance makes more sense. But if you want to roll up your sleeves and have more control, have, like, a powerful firewall that does everything, you know, bandwidth rate limiting and quality of service and, you know, able to log into it remotely and do all kinds of things, you know, essentially something like SmoothWall or m0n0wall is a full Linux system in which you can run anything you want.

Leo: Right. People often used to ask us on The Screen Savers, my roommates use too much bandwidth. How can I limit them? SmoothWall is great. You can run Squid or some proxy server on SmoothWall. And, oh, you can just turn them right down.

Steve: Yup.

Leo: Tim in the U.K. asks: If I want to run a web server on the, quote, "host" PC on port 80, and a web server in a virtual machine also on port 80, which server will pick up the request? Oh, that's interesting.

Steve: Yeah.

Leo: Will they be battling? Is it possible even to do this, he wonders.

Steve: Okay. No. If you have two servers, normally what happens is a virtual machine that has networking capability is – there are several ways it can be set up. One is that it's got its own

sort of local network, sort of a virtual local network within the machine, which allows the physical machine and a local machine to talk to each other. So if you ran a server in the virtual machine, then from your host you could access the web browser on port 80 in the virtual machine, using the IP address of this little virtual network that's all existing within the main host machine. To put the virtual machine on an IP that's externally accessible, then you have a collision. It is not possible to run two TCP servers that are both listening to a given IP and port at the same time. And there's something – the way the API works, when you're programming these, you say, okay, a certain process is going to be listening for incoming connections. And once that's been done, any other process that attempts to do so will return an error saying, you know, you can't listen, there's somebody already on this port listening for those connections.

So UDP is a little bit different. There is a way to sort of share notices of packets coming in because UDP, as we've talked about, is not a connection between two endpoints, it's just the flow of raw packets. So it is possible for UDP services, multiple UDP services, to get notified of incoming packets, and then, you know, for them to figure out what they want to do about it. But not in the case of a web server. Only one application at a time can, like, terminate the endpoint and receive connections.

Leo: I've actually, in a smaller way, seen this happen with Parallels on my Mac and a CD-ROM.

Steve: Ah.

Leo: When you insert a CD-ROM, if Windows is foremost, Windows grabs the CD and autoruns it, and it's not visible to the Mac, and vice versa.

Steve: Right.

Leo: So I guess kind of the generalization is, I mean, unless you have something like UDP that's specifically designed to be shared, in most cases one or the other's going to get it.

Steve: Right.

Leo: And keep it. And that's it. That's the whole story.

Steve: You know, Tim's question was which server will pick up the requests. Unless he goes to some substantial extent, the external, the server running in the host computer, the main machine...

Leo: It gets priority.

Steve: Exactly. It would be first in line. And then, you know, if he had a different IP assigned to the virtual machine's web server, then incoming data on that different IP would go to the virtual machine. So...

Leo: Right. And I think some – I don't know, but I would imagine some virtualization

programs would allow you to pass the data along explicitly and say, you know, I'm running a web server, pass the port 80 stuff along.

Steve: But one of my projects, by next week's podcast, is to nail down, I mean, I know VMware, the VMware Workstation quite well because I've used it a lot. I've never messed with Virtual PC. So I'm going to learn about Virtual PC, and we'll have a real head-to-head comparison between these.

Leo: I'm a big fan of this stuff now. You've really won me over.

Steve: Well, and Parallels...

Leo: They've done a nice job.

Steve: They've done a great job. And now that they're supporting the virtual – the hardware virtualization technology, the Intel VT technology, over on the Mac side, you know, you've got Windows running at full speed on a Mac.

Leo: I know, I love it. Yeah, I just love it. I'm really – we're looking – at Call For Help we're looking at buying, instead of buying new PCs, buying new Mac Pros, which are very, very, very fast Macs, and running Windows and Mac on the – and using virtualization, whether it's Parallels or VMware, on the same machine. It'll eliminate this whole need to switch from machine to machine. It's just all there.

Steve: Yeah.

Leo: Chris Meisenzahl of Rochester, New York, is becoming more and more annoyed with ZoneAlarm. And he blames you. Well, I don't know if he blames you, but I blame you because

wouldn't have known about ZoneAlarm if it weren't for you. You were the one who told us all about it.

Steve: Yeah.

Leo: Of course, we ever since have been telling the world about it. He writes: My question is regarding software firewalls. I have two XP machines, one Home, one Pro, behind a Linksys NAT router. In addition, I have long used the free ZoneAlarm, never had trouble with it, no malware, viruses, trojans, and so on. I also have an iBook running Tiger. But in the last few versions of ZoneAlarm they've just – it's becoming larger and more resource intensive. You've been saying that for a while.

Steve: Yup.

Leo: I'm beginning to wonder if a third-party software firewall is superfluous, as long as I have a NAT router and the XP firewall, also running AVG Anti-Virus and Ad-Aware Spybot. What is your stance on this? Chris, I'm so glad you asked. What is your stance on this, Steve?

Steve: Leo, do you run a software firewall?

Leo: No.

Steve: I don't either.

Leo: No.

Steve: No.

Leo: I say on the air all the time a NAT router is sufficient. It's not as capable as a software firewall, but on the other hand it doesn't slow your machine down, it doesn't add to the compatibility woes or the sometimes frustrating connectivity issues that a software firewall can cause. And it gives you 90 percent of the protection.

Steve: Well, no force on earth could get me to plug one of my real main machines directly into the – onto the Internet without protection. I mean, it's just – it's, you know, you measure the lifetime of a computer hooked onto the Internet without some sort of protection in minutes. I mean, it's just – there's just so much junk out there now. And it's the nature of this that there's a chance we don't know about attacks. I mean, there are – we know that there are exploits, you know, these so-called "zero day" exploits, which are discovered when they're being used, rather than beforehand.

Leo: Right.

Steve: So, I mean, I'm behind a NAT router for my entire network, and I have no firewalls on any machines. And I've also never, ever had a problem. You know, NAT really is super strong technology. Now, my tech...

Leo: We'll talk a little bit later about Astaro, which is, you know, a more secure, a more advanced firewall. But it's the same idea. I mean, it's a hardware firewall as opposed to a software on your machine.

Steve: Well, in fact, I was going to refer to Astaro earlier with our prior question, the guy who was asking about SmoothWall, because Astaro is exactly that kind of...

Leo: It's a Linux distro, yeah.

Steve: Exactly.

Leo: But so you're not – so something like that is not the same thing as a software firewall. You're not saying use a NAT router instead of a hardware firewall. A hardware firewall would be even better, yes?

Steve: Oh, I – yes. And you certainly want to have that. However, you know, when I'm roaming around the country, like coming up to Toronto, I'm absolutely behind XP's software firewall when I don't have my normal hardware firewall in front of me. The...

Leo: The advantage of XP's firewall is it's small, and it doesn't slow it down. So you get that protection without really compromising your system.

Steve: Right. Well, and, I mean, the traditional personal firewalls – McAfee, Symantec, ZoneAlarm – they really have become huge and bloated. I mean, yes, they do lots of things for you. And I don't want to suggest that people shouldn't be using them if they're comfortable with them. I would suggest, though, that people should not be afraid not to have them if the firewall is, as is the case for Chris, who asked this question, if the firewall is becoming a problem. I mean, you really don't need it.

Now, that said, the thing that the firewall does is it gives you a notification of software in your computer, notification and control over software in your computer that might be phoning home behind your back. You know, I mean, that's the classic experience I had early on with a beta of ZoneAlarm that got me excited about the idea. That is, you know, I discovered something in my machine I didn't know I had. So that...

Leo: But that was a long time ago.

Steve: It was a long time ago. And ZoneAlarm, it was version 2.6.

Leo: A lot smaller, yes.

Steve: 2.6 was the one I – that was, like, the sweet spot for ZoneAlarm. And so I would recommend, I mean, if someone wants a firewall, look at Kerio. The Kerio personal firewall is – if I were to use a firewall and install it on a machine that didn't already have one, for example if I was using Windows 2000 and wanted a software firewall because I was going to have to be using that machine out from behind some sort of NAT protection, it'd be the Kerio firewall that I would install and use.

Leo: Yeah. Yeah, we've mentioned that before.

Steve: Yup.

Leo: And it's free, too, so.

Steve: Yup.

Leo: It's a very good, very good program. Paul Sanza from Louisiana writes: Whenever a new security issue is uncovered in XP, you can always find people complaining in forums and newsgroups that Microsoft can't make a bug-free operating system. This is generally followed by a round of Microsoft bashing, with some defenders chiming in. I personally – says Paul, not me – feel that Windows XP or 2000/NT/ME/98/95 is just too big to be bug-free. Well, that I'll agree with.

Steve: Yup.

Leo: And that newly discovered flaws should be expected. Yeah, of course, everything has flaws. My question is, what's your view on this matter, Steve? Do you feel that Microsoft is lax with their OSes, or that all those naysayers are expecting the impossible?

Steve: I think that Microsoft in this instance is just the big target. I mean, they're easy to pick on. They, you know, everyone – well, not everyone, but a huge population of people on the Internet are using various versions of Windows. Microsoft, or course, has the problem that flaws are being discovered in very old versions of Windows which Microsoft is no longer fixing. So that's a concern. You know, we've seen that 95 and now 98 have gone past the horizon of critical security updates. This was an issue that we saw at the beginning of this year with the Windows Metafile exploit, which Microsoft said we're not going to fix in the older machines. Turns out the older machines didn't have this problem. It occurred in Windows NT for the first time and moved forward. But still, the point is that the older versions of Windows are not – are no longer going to be fixed for the critical security vulnerabilities. It is the case, though, that Linux has problems, too. And the Linux code base has tripled in size over the last few years as its popularity has grown and as all kinds of new features and capabilities have been added to it.

So, you know, if you look at any mature security list, you'll see problems with Windows, and you'll see problems with Linux, and with UNIX, and with OpenBSD and FreeBSD and all of these, you know, large and complex operating systems. So it really – it isn't correct, and I think therefore not fair, to single out Microsoft as being, you know, worse than any. There have been policy problems with Microsoft, and I've, you know, we've talked about this often, the idea of running unnecessary services without a firewall on by default and giving those machines to naïve users. The advantage that UNIX and Linux has is that they generally have more sophisticated users who understand what it is that they've, you know, what kind of OS they're sitting behind the wheel of. Whereas Windows tends not to. So, you know, the Service Pack 2 advancement in Windows XP that runs the firewall by default was a huge change and really made a difference for Windows security.

Leo: Yeah. But I have to say, and I don't blame Microsoft at all, but it's an old operating system now. They made decisions, as you've pointed out, back when security was not as big an issue, that have resonated throughout ever since. They can't change it because of a legacy software that, you know, requires Windows to work in a certain way.

Steve: Well, they...

Leo: It's a very difficult thing for Microsoft.

Steve: Yeah. They wrote code, I mean, a huge body of Windows code is this old code from before the dawn of security awareness at Microsoft.

Leo: It's not their fault. Now, I do think that there is a bad – there is, frankly, some pretty bad programming. I mean, the number of buffer overrun exploits in Windows is kind of staggering.

Steve: If there's a buffer, it can probably be overrun.

Leo: And I, you know, we won't ever know. But I think that there's some culpability on Microsoft's part for not having better coding policies.

Steve: Well, Mark Thompson told me something the other day. We were talking about Vista's virgin stack. And he said, well, it's not just the stack that's virgin, you know, Vista is completely rewritten from scratch.

Leo: Right.

Steve: And it's like, ohhh, what?

Leo: Well, but, you know, if, you know, for instance C#, Java, there are a great many more modern languages that are much more resistant to buffer overruns because they do range checking.

Steve: Yup.

Leo: And much of what Microsoft does is written in C++, which has no, you know, range checking. You can use a string copy and not care where that data goes.

Steve: Yup.

Leo: And apparently that happens a lot. So it's partly because they're using an older language that doesn't protect the programmers. It's probably more because they don't have good policies. I'm hoping, though, that when they start from scratch, that that's one of the things they implement, that they – there must be a switch in the compiler that says, you know, range checking is required, is mandatory. I would hope so.

Steve: Yeah.

Leo: I mean, it's possible programmatically to prevent many, many buffer overflows. I think. I mean, I may be wrong here, but...

Steve: Well, if you put enough encapsulation around the calls, you can do that. The problem is that programmers don't like to have those kinds of constraints on themselves because, I mean, and C is the classic, you know, pointer land...

Leo: You can do anything in C.

Steve: Exactly.

Leo: You can write to any part of the memory, anywhere you want, anytime.

Steve: Right.

Leo: And that's why we like pointers. Walli Fergus- and by the way, Assembly is even worse. Walli Ferguson of Athens, Tennessee – which is what you use...

Steve: I know.

Leo: ...is feeling a bit exasperated. I'm exasperated, says Walli. He writes: I've experienced quite a few problems with hackers and Internet security, to the degree that I couldn't even install and use McAfee and Norton. One problem compounded upon another, creating a third. I finally researched and cleaned my PC, finding among other things a rootkit. Gosh, Walli, I hope you reinstalled Windows from scratch. I don't think cleaning is going to do it.

Steve: Yeah.

Leo: Authorities like Microsoft OneCare offer a solution for which I am appreciative. Yet what can be done to prevent even their secondarily looking at my private files – oh, Walli. Walli, your focus is wrong here, dude – such as Word documents and personal information. This is not intended to sound accusatory, it's just an afterthought, for an enterprising engineer might decide to covertly use Microsoft capabilities for personal gain. He does raise a good point. You have to trust the security software that you use not to be bad.

Steve: Yes.

Leo: Have to trust somebody.

Steve: Well, you do. And, you know, he's sort of talking about, well, what if, you know, Windows had a backdoor installed?

Leo: Well, then you're out of luck, dude.

Steve: Yeah. Well, and, you know, and Microsoft is being sort of accused of this kind of behavior. I mean, you know, even I, at the beginning of the year, looked at the Windows Metafile exploit and said, wait a minute, you know, this allows images to run code, and this wasn't a mistake. It was, you know, it was a bad idea. We don't know that it was a backdoor; but it was, you know, clearly a facility that appears to have been deliberately put into Windows for whatever reason. And of course they've taken it out, and that's a good thing. So I don't

think Microsoft could survive a true, provable, you know, example of their code having a backdoor. You know, there's some strings in the network driver, I think it is, or somewhere, that talk about an NSA key. And it just – it turns out that NSA is a – there's, like, an acronym collision that's got everyone freaked out that, you know, Microsoft has installed, you know, a key that belongs to the NSA so the NSA can access our computers behind our back.

Leo: Bad choice of an acronym, that's all.

Steve: No, no no no no no.

Leo: All right. You know, you have to – look. You use an operating system, use any software, you're kind of trusting the vendor. That's just the way it is.

Steve: Although, again, this is the point that you often make about open versus closed source.

Leo: Ah, good point.

Steve: Because with an open source system...

Leo: You don't have to trust. You can verify.

Steve: Yeah. Now, most people don't. They, like, they don't even compile the source themselves to binaries. They just use the binaries. But the idea is there's many hundreds of eyeballs looking at this stuff and no, you know, no single Bill Gatesian sort of overlord that says, oh, let's put a backdoor over here.

Leo: Right, right, right. The truth is, I think if you're looking for security and, for instance, encryption, you've got to use open source software. It's the only way you can be sure encryption doesn't have a backdoor. But, you know, that's my opinion.

Steve: Or trust the source.

Leo: Or trust the source.

Steve: Or trust the Force, Luke.

Leo: If you dare.

Steve: Yup.

Leo: Steve, what a great round of questions. Some great stuff. Of course you continue to

take questions. What's the best way people can ask you?

Steve: The best way is to go to GRC.com/securitynow. At the bottom of that lengthening page, which I'm going to have to organize now that we're, you know, we've got 56 episodes on it, at the very bottom of the page is a form that allows someone to just put a question in and press a button, and it comes to me.

Leo: Great. And maybe your question will be next in four episodes. Next week, kind of a virtualization wrap-up?

Steve: Yup.

Leo: And we're going to take a look at maybe some of the stuff that Microsoft's doing.

Steve: Some specific feature comparisons, you know, when – people are writing in, saying, okay, Microsoft's Virtual PC is free. The server version of VMware, and we got the player, and we got, you know, blah blah blah blah blah. Which one should I use?

Leo: Okay.

Steve: I'm going to attempt to answer that question.

Leo: Fair enough. The wonderful Steve Gibson. Catch more of his stuff on his website, GRC.com. And that's where you'll find the 16KB versions and the transcripts. That's also where you'll find the wonderful SpinRite, everybody's favorite hard disk maintenance and recovery utility. It is the greatest. But if you have any doubts, just visit the testimonial site, SpinRite.info, and you'll see how many happy customers Steve has. It's a nice feeling. Of course...

Steve: Oh, I got, as I said at the top of the show, there was a neat note that I received. It's buried in my email right now, but I want to read it next week because it was just – it's from a Security Now! listener who bought a copy just to support us, you know, which is like way above and beyond, and then needed it, and it really saved him.

Leo: Good. Really neat. A nice story. And we also want to thank Astaro because they are, of course, our sponsor on this show. Astaro has been here since – they were one of our very earliest supporters. And I just think they're a great little company doing some great stuff. If you're looking for security, the Astaro Security Gateway line of network security appliances offers complete protection from network, web, and email security threats. Astaro.com. By the way, Astaro has an opportunity for everybody who listens. They're offering people who listen to Security Now! a free demo unit you could test to protect your network. You just dial 877-427-8276, or visit Astaro.com, and you'll get a free demo unit. They will ship it to your business or office in one business day. If you're ready to step up to the next level of protection, 877-427-8276, or visit Astaro.com.

And we also welcome Visa, our newest sponsor. You've heard the Visa commercial already.

You know, one of the things that's good about Visa is they're – and one of the reasons they want to be on Security Now! – is they're promoting credit card security. And I thought I'd just pass along real quickly from Visa a couple of points that they've asked us to put into the advertisements on the podcast for credit card security. Now, I mean, I use a Visa because, you know, I know that, should anything go wrong, they stand behind it. I don't have to worry. But there are some things you can do to protect yourself. Sign the card, for instance, on the signature panel. Choose a good secure PIN that's secret and memorize it. Don't write it on the card. I don't need to tell the Security Now! audience that, I don't think. Check your online and paper statements immediately on receipt, or if possible monitor your account activity more frequently online. I do that. It's nice to have the statement online now. And of course keep your financial information secure, preventing access from even family members, friends, and neighbors. It's your stuff. Keep it private. And do shred everything before discarding. You know, most identity theft occurs, not online, but from hard copy people are digging out of your trash. Shred it.

Steve: Yup.

Leo: And you don't have to worry about it. Safer, better money. Life takes Visa.

Steve, we've wrapped up a great episode. And I think it's time to say goodnight.

Steve: Once again, 58 and counting – no, 56, 56 and counting. 57 is next week.

Leo: Yup. Steve Gibson from Irvine, Leo Laporte from Petaluma. We say to you, thank you for joining us. We'll see you next Thursday on Security Now!.