Listener Feedback Q&A #8

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-044.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-044-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 44 for June 15, 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.

I smell a mod 4 episode. I do indeed. Leo Laporte here, Steve Gibson in Irvine, and it's Episode 44. And as far as I can tell, that's divisible by 4.

Steve Gibson: That's like a double mod 4.

Leo: That's a double mod 4.

Steve: Yeah.

Leo: So we get our usual 20 questions.

Steve: It's even mod 11.

Leo: Mod 11, mod 4, mod 2, mod 0...

Steve: Mod 22. Yeah.

Leo: All right. You math showoff. Let's get to the questions, unless there's anything we want to cover from our last episode, where we talked all about ports. People really appreciated that, by the way. Got a lot of positive feedback.

Steve: Yup. And in fact, some of the questions that we're going to deal with today are follow-ons from that. So we've got 12.

Leo: 12 of them, starting with Nick from New Jersey, who says he hasn't caught up with all the past episodes, so apologizes if he's asking something we've already answered.

Steve: As a matter of fact, yes. He asks:

Leo: I was wondering about this program called Hamachi. He really is far behind. It promises virtual LAN functions over the Internet, all encrypted. I'm wondering how you and Leo feel about the technologies behind it and the features included. I thought it might make a good show topic. It might.

Steve: Well, exactly. I put it in here. I got a kick out of it because he's excited about the show. I want to tell you, Nick, that there's an episode titled "Hamachi Rocks." And I love the title. Apparently Hamachi's author's wife has been giving him, back when we did the show, a hard time about us doing a podcast called "Hamachi Rocks." We absolutely love Hamachi. So Nick, if you go to GRC.com/securitynow, you'll find the archive of all past shows. Just scroll down. I don't even know what number it was [Episode 18]. But it was, you know, probably in the 20s somewhere, where I thoroughly researched, checked out Hamachi, had a whole bunch of great email with its author, Alex Pankratov, and really did a complete exposé on how it works. And we love it. It rocks.

Leo: It literally rocks. Let me see here. I think it was – no. Keep going back through the episodes trying to find which episode it was.

Steve: Yeah. How far back was that?

Leo: It goes away, away, away back. Was it 22? Let me see here. I'm looking at all of our – no. It goes back to where we were talking about VPNs, doesn't it.

Steve: Yes, it was in our whole, you know, how to securely connect yourself to other machines. And I have to say, I mean, we haven't talked about it a lot since, but there's a constant flux of Hamachi questions and accolades. I mean, people really do like it. My own tech support guy, Greg, is using – he moved from my area to Phoenix, from where he still does tech support for GRC, answering questions that our customers have who've purchased or are considering purchasing SpinRite. And, you know, he's online several times a day and gets responses back to people immediately. He had some clients that he worked with on the side who he's hooked, who he's completely Hamachi-ized in order to get into their networks and do remote management of their corporate facility.

Leo: Isn't that great.

Steve: I mean, it really is super.

Leo: Yeah. A lot of gamers use it because it's a way to create a LAN party without everybody being in the same location.

Steve: Right, and in fact I remember that one of the questions I answered when you and I were together on the Call For Help show in Toronto was a gamer wanted to be able to hook two Xboxes together. And of course the Xbox direct connection couldn't understand going across the Internet.

Leo: Right.

Steve: But by using Hamachi, you both are on a five-dot network, so it looks like a LAN to anything that you want to connect locally. And it is, of course, easy to hook two Xboxes together locally.

Leo: Right, right. And don't feel bad that you haven't heard all the episodes. We understand. There's lots of good stuff coming up. In fact, you're going to hear – if you're back there, you've got a long, long way to go.

Steve: Well, but it is worth recommending to people that, you know, they remember that the podcast, at least from our standpoint, because we've done so much sort of research and tutorial content, not just current event stuff, there's this archive of stuff at GRC that, you know, anyone can browse through. And you'll find lots of really good stuff there.

Leo: You have a list at GRC.com/securitynow of every episode, so they can just click through those.

Steve: Yeah. And of course, you know, transcripts, and a complete archive of all the past episodes.

Leo: And just so people know, I don't know, I haven't really publicized it, once we open the new site – by the way, the site redesign will happen in a couple of weeks, the new site will launch, but then it will be fairly easy. We'll have a complete episode guide. But until then you can always enter TWiT.tv/sn and an episode number, so sn1, sn2, all the way up to sn44, and that'll take you to that episode. So it's not widely known, but that is a convention I've been using.

Steve: It's funny, too. I see people, like, trying to get ahead of us, trying to pull content from the next week or the week after.

Leo: Oh, yeah, because we use the naming convention.

Steve: Because it'll pop up in my logs, and I'll go, oh, okay, well, we're not quite there yet. They must just be anxious and wondering if the content's already been posted.

Leo: It happens almost every time. In fact, I had to start moving things to a staging area before I uploaded – after I uploaded it because people were screwing up the caches, the Akamai caches. So I had to finally...

Steve: Right.

Leo: ...finally just, you know, put it somewhere hidden until the time comes. Ray from Irvine, your neck of the woods...

Steve: Yeah.

Leo: ...says: When I'm behind a corporate firewall, going through a proxy server to the outside world, how exposed am I to the IT department when I go to a secure site, an SSL encrypted site for banking or online ordering? Does the IT guy see my password, my credit card info, and so on?

Steve: Yeah, that's a great question because there are situations where corporate IT has deliberately configured their border to decrypt a person's communications, like for whatever reason. They might want to be monitoring, they might want to be filtering it, they might want to be, I mean, it might be for a benign and beneficial purpose, for example performing antispam filtering or malware and virus and spyware filtering, because people certainly can get infected over a secure connection if the secure site at the other end is doing something bad.

So what anyone can do when they're on a secure site is right-click on their page and look at the certificate. We've talked about this in several different contexts, but not exactly this context. You should see, for example, if you were at PayPal, and you had an https secure connection, or Google, if you were using Google Mail securely, or whatever, if you right-click on the page and look at the certificate, you will see the URL or the name on that certificate. If it's www.paypal.com or Google.com, whatever, then that means that you actually have a non-intercepted secure connection directly to that site, and nothing is there interposing itself.

What can happen is that corporations can install their own certificate on their employees' browsers, which will essentially allow them to intercept any other SSL connection and proxy it, meaning decrypt it, do whatever they want to with it, and then re-encrypt it, essentially breaking the security completely at the border.

Leo: Wow. I wouldn't have thought that. I would have thought that once you've established the – that you're establishing connection with your bank directly. But they...

Steve: Well, and that's the problem, is that if a – in the same way that certificate authorities can be installed on browsers, which is what authenticates certificates, it's possible for a local certificate to be created. Now, you know, users will generally see some notice of that. But that can be suppressed in browser configuration also, making this thing pretty transparent. So it is something that corporations, some corporations, do. And, you know, if you're really concerned about not having anyone able to sniff your traffic, you need to make sure that's not being done.

Leo: Wow. Wow. But again, you can check the certificate in your browser, and it will tell you whose certificate you've got, and that'll tell you who is...

Steve: Exactly. If you...

Leo: ...seeing your data.

Steve: Precisely.

Leo: Oh. I'm going to have to think about that from now on. Is that still a common technique, is using a proxy server at a corporate environment?

Steve: Actually, I think it's increasingly common as opposed to decreasingly common practice, although not necessarily for secure traffic. Generally it's for non-secured stuff. But we are seeing, as security concerns and spyware and malware concerns increase, there is an interest in filtering all traffic, even that which is secure.

Leo: Wow. James from London was wondering: In your discussion, last discussion, you talked extensively about blocking inbound access to ports using stealth and NAT techniques. But what about blocking outbound ports? Is it necessary for personal or business users to block all outbound port access and only open up the ports required?

Steve: Well, of course, this is the great question. This is sort of the issue of do I need an additional personal firewall beyond having just a NAT router or beyond having the personal firewall that's now built into and turned on by default in Windows XP after installing Service Pack 2. And, I mean, it's a good question. Neither you nor I run with them, Leo. But on the other hand, it was during beta testing of the very first version of ZoneAlarm which offered outbound port blocking, which is to say application-level port blocking, that I discovered the very first piece of spyware on my machine and coined the term "spyware." So...

Leo: So without it, it wouldn't have seen that.

Steve: I would have never known that there was something in my system phoning home. And of course Microsoft has been in the news recently because their Windows Genuine Advantage program has been caught phoning home daily, despite the fact that they did not acknowledge that that was going on in their EULA. And they're now, you know, running backwards a little bit and apologizing and saying they're going to change it and coming up with strange justifications for doing so.

Many people like the ability to know exactly what programs are communicating over the 'Net. Other people find it makes their computer too noisy. It's popping up and asking permission and so forth all the time, although that kind of facility can be trained. So I think it's really a matter of personal preference. Is it better for your security to run that kind of software which is going to give you outbound control? I think you'd have to say yes, it's better. But as always, there's a tradeoff. For more security comes more responsibility, more of your involvement in managing what your computer's doing. Many people like doing it.

So I would say maybe give it a try. You know, use, I would say, a lightweight firewall. You know, the Symantec and McAfee products, even ZoneAlarm, unfortunately, has just become so big and so kitchen sink-oriented, trying to do so much for you, that it imposes a burden on your system. In fact, it's funny, I mentioned Greg, who does my tech support, who remotely administers a client here in Orange County. He upgraded them to a newer version of McAfee which broke the function of one of their systems because it was an older computer that just no

longer had enough power to run the antivirus updates in addition to the other stuff it was doing. So the only change he made was updating to a newer version of McAfee, and finally it was like the final straw.

So, you know, firewalls like Kerio, which is now owned by Alex Eckelberry's company, Sunbelt Software, Kerio's a great lightweight firewall. And really, if I were to recommend one, that's the one I now recommend because it's just – it's smaller and tinier. And so anyway, the point is, if you're interested in trying outbound blocking, get a good outbound blocking firewall like Kerio and see how it feels, see what you think. If you like the control, then it does give you more security.

Leo: Let me ask you this. Are there any hardware routers that do this? I mean, that might be a better way to go.

Steve: It's a difficult thing to do from a hardware router standpoint. NAT, as we know, by default allows everything outbound. The problem is that, as soon as you're outside of the computer, when you're in an external router, there's no way for it to know what application generated the traffic. So you certainly could block all kinds of ports. But then basically you're shutting down services.

But on the other hand, Leo, I mean, it's not a bad idea. The classic corporate firewall of yesteryear did not allow traffic, for example, to remote servers other than those running on 80 and 443, maybe FTP on port 21. And then it was smart about handling FTP's reverse connections. So you certainly could run a more traditional firewall.

But then all the many other things that most people are now used to using and wanting to use, you know, Skype and peer-to-peer and, you know, many of these fancy servers that we have would not function unless you started then opening ports to their remote servers over the ports they want to use. And many of these are dynamic and changing and configured on the fly. So unfortunately, if you were to try that, you'd end up, you know, either having to open up so many ports that you really no longer had any security, or you could still have a case, for example, where malware was deliberately using port 80 in order to pretend to be a web browser. Thus it would go right out through an external firewall, and you wouldn't know that it was something not your browser, pretending to be a browser, using your existing Internet connection.

Leo: All right. So...

Steve: So the real advantage of the program running in the computer is it's able to backtrack through the computer, figure out which program is doing the communication, and then going – in fact, we have a question sort of about that that we'll be dealing with a little bit later in this show.

Leo: Very good. Very good. All right. Mannix of Canberra, Austria – Australia, I'm sorry, there's a little difference there – has been thinking about something he calls VM surfing: I was just listening to the episode of SPYaWAREness [Episode 7], and I was just wondering, is using Virtual PC, something like a VMware workstation – Virtual PC is a Microsoft product, but VM...

Steve: Or he says, yeah, a virtual PC...

Leo: A virtual PC...

Steve: You know, any one of them, yeah.

Leo: Right. VMware is another one, of course – for browsing high-risk sites any safer? Actually, I'm interested, too, because I'm using now the Parallels Workstation on my MacBook to run Windows. Because even if you get infected, he says, it's just going to infect the virtual PC and not the main system, right? Or can – and this is the big "can" question – the main system be affected through the virtualized system?

Steve: It's a great question. And in fact, we will be – it's on my slate of things that we're going to devote an entire episode to. This notion of VM surfing is a question that comes up from time to time. VMware was really the first high-profile company to offer this notion of virtualizing your computer. I am an owner of a current copy of the VMware Workstation system. And I've used it, for example, to set up multiple virtual machines when I wanted to test many different personal firewalls. You know, I mean, like, I have nine or ten of them, each installed in their own virtual machine, and I can jump around between them much more easily than having to install and uninstall them. The whole concept is that it creates a truly secure sandbox, basically a virtual computer that cannot modify its external environment. It actually is a very safe means for surfing. The problem is, it's not nearly as quick, easy, and transparent as firing up your web browser and doing something. So...

Leo: So it can't then cross the boundary between the virtualized hard drive and your real hard drive.

Steve: When done correctly, and we're assuming it's done correctly, that's true. It cannot.

Leo: Now, there are sometimes shared files, or you can write to the other hard drive.

Steve: Yes. And that's really what I mean about "when done correctly" is that...

Leo: So if you can do any of that, that's not good.

Steve: For example, VMware specifically supports the notion of a local network among the machines. And filesharing, you can actually use Windows filesharing to bridge your virtual machines together, in which case you're able to see each other. And there are all kinds of ways to break the containment that a virtual machine offers. But there are some exciting things happening, specifically in the world of VM surfing, where for example VMware now makes a free player. And people have put together Linuxes that are preconfigured with browsers ready to run where you can run one of these Linux VMs, a virtual machine, in the free VMware download, to go a certain distance towards creating an enclosure that is absolutely safe to surf in.

Leo: Interesting.

Steve: And that's, I mean, enough of this is happening that we're going to do at least an episode on this to talk about exactly how these things work and which one we recommend as,

like, the easiest to use, most bulletproof solution for people who want to explore this.

Leo: Well, and in fact, you know, I just started doing this on my MacBook. Now, of course, in this case I have shared folders. It can read the drive, local drive, so it's probably a little risky. But on the other hand, since it's a Mac, it's not likely to cross-pollinate from a PC. So I probably am pretty secure, yeah.

Steve: A good point, yeah.

Leo: And, you know, it's funny, given enough memory, it actually runs pretty quickly and launches pretty quickly. So it might actually be a good solution.

Steve: Well, yeah. Microsoft is promoting this. And, you know, they...

Leo: Oh, are they?

Steve: They purchased their technology, I can't remember from whom, but somebody else, and they call it Virtual PC.

Leo: Right.

Steve: They're suggesting that, for reasons I don't fully understand, that their normal server software won't completely use all the resources of a hardware server. So you're supposed to now run the server edition of Virtual PC to run multiple virtual servers in a single server. And it's like, okay, whatever. It just seems loony to me. But...

Leo: It's not too much of a burden, though, because it is running on a PC. At least it doesn't have to do any translation or anything like that.

Steve: Yeah, the purist in me wonders, you know, how you're not going to have an additional layer of something going on, context switching and virtual machine switching back and forth. I mean, apparently something about the architecture that they're normally using doesn't let them saturate the hardware resources of a server. And this is supposed to be a way to, like, do a better job of just, you know, really taxing your hardware better.

Leo: Well, one thing, I guess, is that there is hardware, support for hardware virtualization in the new Intel chip. So that's one of the reasons I think people have gotten all excited about this because at least it's supported in hardware now.

Steve: Well, actually it's been there since the 386.

Leo: Oh, it has?

Steve: Yeah, I mean, there has been this notion of VMs, you know, the old DPMI that we had back in DOS...

Leo: Well, they're somehow promoting this, Intel's somehow promoting this new virtualization technology. So they must be doing something different. Maybe not.

Steve: They just want – they want a new logo. They want a new sticker, a sticker they can put on this.

Leo: So DPMI allowed you to do this before.

Steve: It was, yeah, the DOS Protected Mode Interface was a context-switching – you remember Quarterdeck and their, I mean...

Leo: Sure, yeah, that's right.

Steve: ...that was all virtualization, yeah.

Leo: Yeah, you're right. Hmm, interesting. Dave Matthews of Richmond, VA, wonders about the alternative Linksys firmware. We've all – maybe you haven't, but I've certainly been hearing a lot about this. He wants to hear your thoughts about the various hacks for Linksys routers, particularly for the WRT54G, which is a very apparently hackable router. And there's OpenWrt, there's a lot of different forms. Are they more secure than what comes on the Linksys?

Steve: Well, that's a great question. I wanted to respond to it because, as you say, there is a continual buzz about this idea. We've talked about it, in fact, in the context of OpenVPN, our VPN system of choice, because there are some opportunities to run an OpenVPN server on a Linksys. Backing up a little bit, the idea is that, you know, as we're familiar, many of these personal routers, NAT routers, allow you to upgrade their firmware when they're – typically when they're adding features or fixing bugs. You download the latest firmware and go through some process to update the firmware that's burned in the router.

Well, Linksys, it turns out, and among other routers, is using Linux as the core OS in the router. And that brought people to say, hey, what about putting other Linux configurations into the router? Which turns out to be completely possible and is even sort of quasi-supported by some of the router manufacturers. They're not that concerned, long as you don't call them for support, because you bought their hardware, they've got their money from you, and it is sort of a more high-end advanced thing to do. But there are – it is possible to install firmware in this hardware which is substantially more powerful than the much-watered-down sort of generic feature set that Linux provides, Linux or any of these other routers that allow you to do this.

Now, the question is, are they more secure? That's a great question. When you go off the reservation and use some third-party software or firmware in your router, you're certainly taking responsibility away from the manufacturer about what this thing's going to do. With responsibility comes power, also comes of course the opportunity for something to go wrong, for you to misconfigure something, for you to have these more powerful servers or services running. If then there was a security vulnerability found in them, you might have hackers scanning the 'Net looking for these hacked Linux routers running a vulnerable version of a service that the base Linux router didn't have. So, I mean, it's the standard, okay, you want to

do something more fancy, you need to take some responsibility for it. So...

Leo: And you're trusting what others have done.

Steve: On the other hand, it's all open source. This is all open source technology. So it's inherently more trustable. So I would say, if you're wanting to do that, make sure you're paying attention to and are a member and have joined to whatever security lists or bulletin system they have, and that you are keeping that firmware up to date, because you want to stay ahead of any problems that are found because they could be then exploitable, whereas the base generic firmware would be less so.

Leo: Right, right, right.

Steve: But, I mean, you know, for – I have a WRT, is it the 54G?

Leo: 54G, yeah.

Steve: And I flashed it because I wanted to play around with SIP, with VoIP. And you can install a complete SIP system in one of these routers and...

Leo: That's pretty cool.

Steve: ...create – oh, I mean, it's amazing. And, I mean, and they got, I mean, you know...

Leo: It's really a little Linux, as you say, a little Linux computer that you can do a lot with. I mean...

Steve: It is absolutely running Linux. And there are some builds of this that are very feature packed. I mean, it's amazing, they're really building tight little systems with all kinds of cool additional features. So people could Google OpenWrp...

Leo: T.

Steve: Excuse me?

Leo: Wrt.

Steve: Oh, yeah, yeah, exactly, Wrt. It's the open – what's it stand for?

Leo: Well, Wrt is whatever Linux calls that router. Wireless Router Thingamajig?

Steve: Yeah, I thought there was some acronym for it. Anyway, yes. Google OpenWrt and...

Leo: You'll see a lot of stuff.

Steve: There's a lot of stuff, lot of resources.

Leo: Yeah, in fact, Wikipedia has an article on it with a good link to the various projects like DD-WRT and HyperWRT and...

Steve: Right.

Leo: Sveasoft's was one of the early ones that allowed you to create a wireless access point that you could charge people for and stuff. That was really cool. Hamachi user – back to Hamachi, I see – Darren Govey of Chertsey, Surrey, U.K., writes: You guys are always saying that Universal Plug and Play is a bad thing – I'm starting to sound Australian, I'm sorry – security-wise. But the latest beta version of Hamachi includes a feature for automatic UPnP configuration. They claim it poses zero risk and should be left enabled. Well, who's right? Gibson or Hamachi?

Steve: Well, this is a good question. What they say, what Hamachi says on their changes page, referring to this latest beta, is that they've added support for automatically configuring required port-forwarding rules on home routers via Universal Plug and Play. This feature is transparent in a sense that it requires no configuration and does not manifest itself in any way other than reduced number of, quote, "yellow status peers," unquote.

Leo: And it's a very easy way to do it.

Steve: He says the feature – as Alex writes, the features may be turned off completely by using respective option and preferences system. Note, however, that Hamachi does not depend on infamous SSDP Windows service, and therefore having UPnP feature enabled poses zero risk to your system. We encourage everyone to keep this feature enabled as it improves overall quality of the communications over Hamachi networks.

Leo: Wow. Hmm.

Steve: Okay, now what this – yeah, this is a problem.

Leo: You're going to have to call him.

Steve: What this really means is that Hamachi is doing what UPnP allows, which is it's configuring your router behind your back to open a static port inbound into your router. The reason this is done is that otherwise Alex's servers have to be a bridge between your connections. And Alex doesn't want his servers to be a bridge between your connections. I mean, and this exactly discusses the NAT traversal issue we were talking about before. Alex does a great job with Hamachi of doing NAT traversal, bridging two users, both behind NAT, except when they have a non-peer-friendly NAT router, again, exactly as we were talking about

in the last couple weeks. So in order to not need Alex's servers, he's opening ports through your routers.

Well, the problem is there's no security in the router for doing this. If the router somehow had a way of communicating to you and saying, hey, somebody's trying to open a port through me, should I allow this to happen, then it would be acceptable because there'd be a dialogue, and you would know what was going on. In Mark Thompson of AnalogX's research, on the routers he's seen, you can't even tell this is going on in the user interface. So you can't bring up the router's web page and see that there's been this kind of reconfiguration. It's all transparent. Which is, you know, an additional bad idea.

Now, the security risk is that, in the same way that Hamachi, without asking or being able to, or the router being able to get confirmation from you, in the same way that Hamachi is able to do this, anything else can. So it's a perfect example of how software behind your back can be bringing down the security of your router. So I still say it's a bad idea. The good news is, if you disable Universal Plug and Play in your router, then Hamachi, like anybody else, will not be able to do this. The question would then be, what do you want to do about these yellow flags, the so-called, you know, we're not able to connect you? The paid version of Hamachi, as I understand it – unless things have changed, and I haven't looked at it recently – the paid version does allow you to use Alex's servers as an intermediary if you're behind – if you have a problem with your NAT routers not allowing this kind of connection.

The better solution, and this is what I have done with Hamachi – because remember I have a NAT peer-to-peer traversal unfriendly router – is just to establish your own static port forwarding. You can tell Hamachi in the user interface to use a statically forwarded port. There's, like, a great – I think he calls it a magic number or something on the UI. What that actually is is static port forwarding. So make up a port – I think it has 1234 or something in the field by default. Don't use that. Make up your own port number. Choose something between 1024 and 65535. Put that into Hamachi. Then, on your router, go there, and instead of turning on Universal Plug and Play, which you should disable for security's sake, instead simply set up a statically forwarded port using that port into your computer's IP. That gives you the same capability of not having Hamachi give you a yellow flag on users, still allows you to connect directly. There's the minor security problem which there's no way to avoid of that port now being opened. But it's a high-numbered port. It's only going to be coming into Hamachi, and as far as we know there are no security problems with doing so.

Leo: Moving along to question 7. A sharp listener, Brian Hogan in Budapest – wow, we have listeners everywhere, it's so great – had this tip to share regarding NAT traversal. Brian says: You were saying that it's not easy for a person using Skype to determine if they have a direct connection to the party they're calling. So here's how he suggests doing it. Both parties check their, you know, public IP address by going to a site like whatismyipaddress.com, or my favorite...

Steve: Or actually GRC.com will do that for you, too.

Leo: GRC will do it. IPChicken.com will do it. Using the chat feature of Skype, both parties tell each other what their own real IP address is. Then you open a command prompt – okay, you're starting to lose me here – and you run netstat-nb. In Linux it'd be np. Netstat command is available in Windows, Linux, pretty much any operating system. This'll show the IP addresses you're connected to and the programs using these connections, and so you'll see if Skype is in fact using the real IP address. If it is, you have a direct connection. Comments.

Steve: Unfortunately, that doesn't work.

Leo: No.

Steve: It would work if we were using TCP connections. But Skype uses UDP.

Leo: Oh. So something like IP Chicken or WhatIsMyIPAddress or even GRC's not going to tell you what the UDP address is using.

Steve: Precisely. In fact, you know, you and I have a Skype connection right now directly between us. And just for the heck of it I did a netstat and looked. And there is no sign anywhere that I'm directly connected to you over UDP. We do have a TCP connection, but that's a whole different kettle of fish.

Leo: That's not where the audio is going over.

Steve: Exactly.

Leo: So but netstat can show UDP connections. You're just saying it doesn't show it up.

Steve: Well, the problem is UDP is not connections. UDP is just packets.

Leo: Of course.

Steve: And that's the problem. TCP connections you can see. And in fact I want to put this in because – I put this question in because we're going to talk about, and we'll devote a whole episode to, netstat and other connection-monitoring programs. There are a number of free ones, and they're relatively easy to use once you know what the information is. And they can be very useful for giving you some sense for what's going on in your computer right at this very moment.

Leo: Well, that makes a lot of sense. So it's a stateless connection; so, you know, you don't have any information...

Steve: Yes. You're able to see that something in your computer is listening on a specific UDP port. And in XP, that nb command will tell you what the application is. That's a new feature in XP. Under Windows 2000, which I'm still using, I use netstat-an to give myself a simplified list.

Leo: Right.

Steve: But it won't tell you which application has anchored the endpoint. There are some freeware that – our friends over at Sysinternals have a great little program, for people who want to go poke around and experiment with this, that will allow you to see what activity you actually have in real-time, and also which programs are the endpoints that are on those communications. So it is possible to do it. Netstat won't do it. And in fact you would only see that Skype was listening for UDP. I haven't looked actually to see what Skype would show us,

but we'll certainly cross that bridge.

Leo: Right. Kay Hayes of Richmond, Kentucky, wants clearer VoIP. Who doesn't? And asks: I have VoIP service through Packet8, which is actually a very good service. I've had a few blurps, hisses, and dead spots during calls here and there, which may be caused by my network setup. Some people on Packet8's forum suggest putting the phone adapter in the DMZ of the router. Is that safe?

Steve: Oh, it's an interesting idea. The phone adapter, I guess it's a piece of hardware...

Leo: Yeah.

Steve: ...which is running. And in fact...

Leo: I have a Packet8 phone. I can fill you in on that. It's exactly as you say. It's like a Vonage adapter or any other adapter.

Steve: And it turns out that because of the problems people have being behind NAT, this is standard advice is that, you know, in fact I've run across this several times where people, the support people and the official configuration suggests that you put your VoIP device in your router's DMZ. That is to say, any unsolicited packets coming at your router will be forwarded to the IP of your VoIP phone. That allows it essentially to create or to accept incoming connections from the outside world. It's relatively safe. I mean, it's a better idea to get a second IP and, if you can, if it's practical, to put a switch or a hub in front of your router, put your phone outside of your router, that is, upstream of your router, and then leave your router configured tightly without a DMZ. But it really is...

Leo: Well, what's the risk? I mean, the phone isn't going to – even if the phone's attacked, it's a dumb beast. There's not much you can do to it. Does a DMZ somehow make the network inside protection more vulnerable?

Steve: It probably doesn't. It does mean that unsolicited traffic is coming into your network.

Leo: Right.

Steve: Although, since there is no ability for any sort of ARP games to be played remotely, ARP won't cross the router's boundary, and then, you know, just isn't being sent by your ISP across from external sources. I think you're really pretty safe.

Leo: Generally Vonage recommends putting its terminal adapter, its voice adapter, outside your router and passing through to your router. Because all of these have a pass-through. So, and they say it's because they can't do quality – and this is interesting – they can't do quality-of-service adjustments if the voice adapter's inside the router.

Steve: Ah, that probably makes sense, yes.

Leo: [Indiscernible].

Steve: Right.

Leo: So it may be in fact you do get better results. I don't know what Packet8's recommendation is. In both – I use Vonage and Packet8. In both cases I put them inside the router. But you're right, you do get occasional interruptions, so I don't know if that would be any better if it were bare on the network. Al Pitchard of Wildomar California wonders: Can a virus damage a CPU?

Steve: It was an interesting question because there are – well, first of all, it brings up the interesting question about whether the virus would want to damage the CPU. As we know, the new game is to acquire computers, as opposed to just infect them for the fun of infecting them or to destroy them. Through the years we've always remarked, those of us who are focused on security, that viruses have not been more damaging than they have been. I mean, you've got code running in your machine that could do anything. Most of the time it just, you know, tries to propagate and replicate itself and tries to live, rather than destroying the machine on which it's living.

Now, there have been some notable exceptions. The Chernobyl virus, also known as the CIH virus, was something that was nasty. It didn't damage the CPU, but it did two things that were certainly damaging. It erased the first megabyte of hard drives it had access to, which was certainly disconcerting for people who had data on their drives. And the other thing it did was it flashed the BIOS with garbage, which destroyed your BIOS.

Leo: Now, that's mean.

Steve: Yeah. And so it was really a problem. BIOSes, you know, which can be reflashed will allow themselves, by software, of course, to be destroyed. The other possibility is that hard drives can have security features which can be engaged and enabled and locked. And again, that can cause problems for people. But we haven't really seen that problem. Now, the CPU itself, so far we have no technology that would allow a CPU to be changed inherently. There's been some talk about, you know, softer hardware on CPUs. But that hasn't happened yet. So no, there's no way for a CPU to be damaged. I mean, you could imagine some strange things like maybe talking to the BIOS and changing the CPU speed or voltage and things, because of course a lot of that is under control of software now. But that hasn't been done. And again, it wouldn't damage the CPU. It might just cause your system to hang. But in general, viruses are not wanting to be destructive that way because they're wanting to take over people's computers and use them for sending spam, for launching denial of service attacks on other people. Basically they're wanting to use your machine as a resource and an asset, not to destroy it.

Leo: So if it were Sherlock Holmes talking, he'd say, no, Watson, there is neither means nor motive. You can rest assured you're safe.

Steve: Well, actually I guess there is means because any virus could be, for example, deleting files. And in fact, you know...

Leo: It couldn't hurt your CPU.

Steve: Couldn't hurt your CPU.

Leo: We don't know of any way to do that.

Steve: While I'm on the topic, though, it is worth mentioning that we do have these new extortion viruses now which are encrypting your files and then holding you ransom. I think it's...

Leo: Unbelievable.

Steve: It's very clever. I don't want to give any credit to the people who came up with this because it's, you know, it's certainly...

Leo: Well, there's some flaws in the plan. You have to somehow get the money to these people, and I think that's a good way to catch them.

Steve: Yes. That, of course, is the glitch. But what I – okay, I'll say "admire." What I admire about this from a cleverness standpoint is that, if a virus destroyed the contents of your drive, well, it's hurt everybody. If it encrypts your drive – now of course this whole scenario, for those who don't know, is that the virus encrypts your drive, then tries to extort money from you in order to decrypt it. And so it's like, well, that's, you know, an interesting scam that has surfaced in the last few months. And but as you say, Leo, it's difficult for these people not to immediately get caught because they need somehow to receive money.

Leo: Raphael Wolfe of Warsaw, Indiana, has just heard about firewalking. Can you talk about firewalking, please, he says. I've just stumbled onto this. Apparently the term has been around for ten years or so. As I understand it, although I'm not sure I do, the idea is to keep pinging IP addresses until you reach a firewall, then use different tools to ping through the firewall. Is it still possible today with NAT? In other words, you look for firewalls and then exploit the holes in them.

Steve: Yeah, it's an interesting idea. We've talked about, when we covered how the Internet works, we talked about the notion of using a traceroute to determine the path your packets take. And the way traceroute works is it deliberately sets short TTLs, that is to say, the time to live in the packet. And as we'll remember from that podcast [Episode 25] – those who haven't heard that may want to listen to it because it was actually a fun series, we talked about how the Internet works – the time to live is not measured in time. It's actually measured in hops. As you move from one router to the next, each router decrements the TTL, the time to live in the packet. When that hits zero, the router will not forward the packet further. Instead, it sends back a message to the sender saying, sorry, for whatever reason this packet expired on the Internet prior to reaching its destination.

So what firewalking does, it's an attempt to find some location on, well, on the Internet or in your path between you and a remote location, anywhere between you and a remote machine, find where there's a filtering going on. And what happens is, rather than using ICMP packets, those standard sort of plumbing packets of the Internet, which is what a ping is, rather than

using an ICMP packet with short TTLs, firewalking uses protocol-carrying packets like TCP or UDP and emits them with shorter TTLs in order to find the location where something is blocking that protocol. So, for example, if you were able to get the protocol past a firewall by using a longer TTL, you would then walk that TTL backwards until you found something that was blocking it.

And so, for example, by sending packets aimed at different ports with long TTLs, you might find that they were both being blocked at some point. And then you're able to, by adjusting the time to live, you can determine where there's a difference in their being sent back, which allows you to determine where along the path something is blocking it. That gives you – essentially it gives you the IP address of the device which is doing the filtering, which you can then presumably use other tools to attack.

So it's something that, you know, it's like deep hacker firewall technology that isn't really apropos today because NAT routers are not vulnerable to any of these kinds of exploits. They're more in the older days where devices, for example, might have a known vulnerability. You might be running an old Cisco firewall that had a known vulnerability, and there was a way to, like, locate that, and then exploit it once you were able to get its IP.

Leo: Interesting. So you just don't see it very often anymore.

Steve: Yeah.

Leo: Yeah. Theoretically possible, I guess.

Steve: Well, yes, still there. And, you know, I liked it, and I wanted to answer the question because it's sort of cool leveraging of the way the Internet works, and it represents that very cleverness that we've seen from hackers of yesteryear.

Leo: Marcus Kasmeric in Kenai, Alaska, wants better Skype connections.

Steve: Doesn't it – here we are again.

Leo: Okay. Now that I've been listening from the beginning, you say that you made Skype operate over a certain port. I have it on a specific port. But is there anything more I need to do to make it work like you guys on the podcast? We get such great audio on Skype.

Steve: Yeah, we do. And the reason is we have done one thing more. I wanted to answer Marcus's question because lots of people are writing, asking how to get quality like you and I have with Skype, Leo. And so you have to do two things. He's done one. He's told Skype to use a specific port. The second thing you have to do is, and we referred to this earlier, is called port forwarding. There's tons of information on the 'Net about port forwarding. So there's – and I'm sure even on the Skype site. If you looked at something about how to configure Skype for port forwarding, and also your NAT router, what you have to do is log on to your NAT router, typically through a web page, and set it up so that it forwards that port which you have told Skype to use through to the IP address, the private IP address that that computer running Skype is on. It'll probably be 192.168.0.1 or .1.1 or something like that. And the idea being then that that allows Skype to make the same kind of direct machine-to-machine connection that Leo and I use. And that's all there is to it. So tell Skype to use a static port, a fixed port number, and then send that port number through your NAT router to your machine. That's

the key.

Leo: It can be any number above 1024. And in my case I have, let's say – this is actually not the port I use, but let's say I use 11111, easy to remember, five ones. I've gone into port forwarding in my Linksys. I say Skype 11111 to 11111, and protocol is UDP. Right?

Steve: Yup.

Leo: And then I just say the IP address of my machine that we use. Which, oh, it looks like I have it wrong, come to think of it. So I may – but does it now have to be done on both sides, or just one side?

Steve: It really only needs to be done on one side, but both sides is better. I mean, basically you've got somebody you're Skyping to. You'd like to both set yourselves up this way. You're going to get a super clean connection. And you'd also get the advantage that anyone else you connect to who is not all configuration happy, they'd get – you'd be able to get a direct connection with them, as well.

Leo: Yeah. So I'm going to now port forward it to the proper machine, which is 205.

Steve: And as you found, when you did this experiment before, Leo, it really did make a difference for you.

Leo: Yeah. We were having trouble with – you know, the other thing that you don't have any control over is how much upstream bandwidth you have. And Steve's got a lot of upstream bandwidth. And I have a business-class DSL. So we're dealing with, I don't know, I think mine's at least 386, up to the 384 upstream.

Steve: And I've got a pair of T1s.

Leo: You've got symmetric, so you've got a lot. You've got a megabit and more. So, and that's what matters, right, not the downstream so much as the upstream.

Steve: Well, of course...

Leo: Both, you know, my...

Steve: My upstream is your downstream.

Leo: Right. So your upstream and my downstream are what matter.

Steve: Exactly. And...

Leo: So there's not much people can do about that, necessarily.

Steve: Right.

Leo: For instance, with Dick DeBartolo, who has a standard DSL, simply by doing what we just described, I've really improved the quality of the calls to his system.

Steve: That is cool. And see, I had already done it on my end, demonstrating the fact that your router was not being peer-to-peer friendly, but mine was by virtue of static port forwarding. So now you've made yours so. So only one router in a connection between two needs to do this. So it doesn't have to be done at each end. Only one end will allow you to have a direction connection.

Leo: It can be done unilaterally.

Steve: If you're doing it, you know, just in general you're going to get better Skype connections with people if you take the time to do this. And again, it's better to do it manually than to turn on Universal Plug and Play and have anything do it for you because you're then opening yourself up to anything else that gets into your system.

Leo: One more question. Steve Gilliam of Pinehurst, North Carolina, wonders about email reliability. He says: You've explained that plain text email can be intercepted, read, and altered nefariously in transit. In fact, trivially done, so...

Steve: Yeah.

Leo: ...I'm wondering what percentage of email is delivered successfully, in a timely manner, assuming that both email addresses are valid. In principle, well, it should be 100 percent. In practice, how much email is dropped by the Internet.

Steve: Uh-huh.

Leo: Do we know?

Steve: Well, I liked this because it opens the discussion about the protocol reliability and other things. For example, Leo, when I sent these questions to you, you didn't see them at first.

Leo: No, because it went to...

Steve: Because...

Leo: ...the spam folder.

Steve: Exactly.

Leo: That's the real – I think maybe the most are dropped by spam filters.

Steve: Yes. In fact, that's really the number one cause now. I do a lot of e-commerce shopping. And I'm seeing more and more a warning and a caution about making sure, you know, they're wanting to send me a receipt, and they don't want my receipt, the receipt bound for me, to get blocked by anything I may have defending my borders against spam. So, you know, you'll see more and more e-commerce sites saying please make sure to allow email from, you know, boughtmycookieshere.com, whatever.

Leo: It's a real problem. I think, frankly, the reliability of email has gone way downhill, and thanks mostly to spam.

Steve: Well, in fact, thanks entirely to spam. The cool thing is that the protocol itself, and this is what I really wanted to address, was the protocol itself is absolutely reliable. If it weren't for things that are deliberately blocking email, the POP and IMAP and SMTP protocols -- basically it's SMTP that is the mail server to mail server system – it is an affirmative delivery technology. There is technology for retrying extensively, for finding another server that can accept your mail. If your inbox is full it'll fall back to a secondary server; and that server, called, you know, backup MX servers, will try to forward the mail. Basically, I mean, it's a phenomenally reliable system which, as we've just said, has been unfortunately now badly broken by the fact that spam actually has used that reliability or abused that reliability to such a degree.

Leo: Sad, isn't it.

Steve: Yeah.

Leo: I just read an article in Security Focus saying email's dead. It's not reliable; it's not usable. Spam's killed it.

Steve: Well, I can't use it myself. You know, I've got a mailing list. We're still accepting subscribers because I've got – and I've talked to you about this, Leo, I want to do one last mailing when I announce a replacement technology myself. But we've got – I'm just looking at the number here – 786,000 subscribers.

Leo: You can't send out a mailing that big.

Steve: And that's the point. What I'm going to do is I'm going to sort the list by recency, and so, you know, so send mail to the people until it just bogs down too much. But there's no way, I mean, that's more than three quarters of a million email addresses from people who've signed up at GRC over the years. And I know that the older ones are going to be dead. But the problem is, the moment I start generating email at any appreciable rate, all kinds of red flags and alarms are going to go off all over the 'Net, and I will be shut out of AOL and EarthLink and, I mean, you know, major ISPs who will immediately flag me as a spammer. And so I'm just going to have to trickle this mail out at a very slow pace and take my lumps. I want to do one final mailing to people. So anyway, that's my plan. It'll be an interesting experiment to see how well I'm able to do.

Leo: Steve is banned forever.

Steve: Oh, and I'm not doing it from GRC. I'm going to – I'm doing it from a completely disjoint IP range, and I have the domain GRCmail.com because I don't want to in any way contaminate my ability to send email receipts to SpinRite's customers.

Leo: And unfortunately that IP address will then be contaminated for years to come. I don't know what the half-life is of black holes, but it's going to be useless for a long time to come.

Steve: It really will be.

Leo: That's too bad. That really is too bad. Steve, we've answered all 12.

Steve: Perfect. And we had a nice hour show.

Leo: Good job. And, you know, speaking of spam filtering and security, I do want to mention our sponsor, Astaro Corporation, makers of the great Astaro Security Gateway. If your small or medium business network needs superior protection from spam, from viruses, from hackers, as well as a complete VPN and intrusion protection and content filtering and an industrial-strength firewall, I mean, this really does it all in a single, easy-to-use, high-performance appliance, you want to contact Astaro. It's www.astaro.com, or you can call 877-4AS-TARO, toll free, to schedule a free trial of an Astaro Security Gateway appliance in your business. And of course the home version is still available for download for free at Astaro.com.

Steve: You know, Leo, it is worth mentioning, probably, that this thing is not just a static box that sits there, but that what you get when you subscribe, whether you're a home user or a corporate user, is you get them remotely managing and updating this with latest virus and spyware signatures and everything. So, I mean, it's – the rough equivalent is running some anti-spyware stuff on your own computer, where you've got it continually phoning home in order to check for updates and new stuff. And of course what this thing does is it's an appliance that protects your entire network, but it's not just – it doesn't sit there and get old. It's being continually renewed and being maintained current. I mean, it's a great solution.

Leo: We're going to start having you do the commercials, Steve.

Steve: Well...

Leo: We are very happy. It's really nice to have a sponsor that we really can get behind.

Steve: It's cool technology, and I've been wanting to explain for some months now that, you know, that that's what this is. I mean, that it is remotely managed...

Leo: It's very sophisticated.

Steve: ...and updated and continually maintained for you.

Leo: Very good. Steve, we've wrapped this guy up, this puppy, with a string and a bow and everything. But we'll be back next week to talk more about security, the Internet, your computer. I love doing this show, and I'm so glad that we've found such a big audience, such a great bunch of people. We do thank our friends at America Online for providing us with the bandwidth, as always. And if you want to know more about the things we talked about, go to Steve's website, GRC.com/securitynow. That's where you'll find 16KB versions for the bandwidth impaired and, of course, thanks to Elaine, transcriptions of every episode so you can read them as well as listen to them. And sometimes with the more complicated subjects that's a real boon. I don't know how Elaine does it.

We also want to remind you that GRC.com is the home to SpinRite, which is the world's best hard drive maintenance and recovery utility. There is nothing better. You can find out more about SpinRite by visiting SpinRiteInfo.com. That's where you'll find a whole bunch of great testimonials.

Steve: Actually SpinRite.info.

Leo: I'm sorry, SpinRite.info. Don't go – I don't know what you'd get if you go to the other place.

Steve: Well, yeah. And you know, Leo, I was thinking about this, it really is – it is SpinRite's users and owners that support GRC and this podcast.

Leo: That's true.

Steve: I mean, it's the people who are buying SpinRite and using it to keep their drives in good health and to repair damage, I mean, they're my sponsors.

Leo: Yeah. Steve would have to have a job if it weren't for SpinRite. So we're glad that you have the time to do both SpinRite and this podcast. We really appreciate it. And all the great stuff you're doing. I know your third-party cookie stuff is coming along. I just looked at a beta page of that. That's exciting.

Steve: Yup. And I'm adding menuing to the GRC site so people will be able to find...

Leo: No.

Steve: ...all the stuff, so...

Leo: Steve. How 21st century. You're amazing.

Steve: Yeah, it's, well, and because I want to do the whole new third-party cookie stuff, and of course I've still got the OpenVPN project to get wrapped up, and...

Leo: That is not – we have not given up on that.

Steve: Nope. It's going to happen. But it's funny, as I think about adding this content, it's like, okay, how's anyone going to find it? Because my home page is kind of a mess, and...

Leo: You need some navigation.

Steve: Yeah, we need navigation.

Leo: If you want, I'll get Amber and her team to help you, if you need some help.

Steve: No, you know me, I want to row it myself. I want no JavaScript, no scripting at all. I'm, you know, I'm learning how CSS works. And, boy, what a nightmare that is, but...

Leo: Oh, Steve, Steve, Steve. Maybe we'll do a story on that.