Listener Feedback Q&A #3

Description: Leo and Steve 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 they have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-024.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-024-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 24 for Thursday, January 26, 2006: Listener Questions and Answers.

Steve Gibson: Hey, Leo. Glad to be with you again.

Leo: We're in the studio at Call for Help, so...

Steve: Yeah, physically together, rather than by Skype this time.

Leo: Steve, Steve, you just crack me up. He brought, essentially, an entire radio production studio with him in his suitcase.

Steve: It was heavy. I'm not doing this again.

Leo: Two PR40 mics...

Steve: I was dragging it through the airport.

Leo: Two arms, you have a pop filter for your PR40, I mean, we're just really - we're rocking here. So, as we do every fourth episode, we're going to answer your questions and kind of follow up on things that Steve raised in previous episodes. Shall we just get right into it?

Steve: Yeah, let's go.

Leo: A couple of questions right off the bat about Hamachi, which was the VPN client that you used and recommended. Tony from Northeastern PA said: On many forums there's been a great deal of disagreement about Hamachi and the need for hardware and software firewalls. Hamachi rocks, as you've said. But what, if any, dangers does its use open us up to? And Greg from Goodyear, Arizona kind of follows on in that. He says: If I'm using Hamachi on my laptop through a friend's open wireless

network to connect to my machine at home, how secure am I?

Steve: Yeah, those are great questions. Hamachi, I'm just so stoked that we discovered this thing because people are using it like crazy. I mean, they really love what it does because it allows them to create really secure point-to-point links between machines. However, the bit of confusion, and we talked about his when we first did our show about Hamachi, is that it's a very powerful connection. You're literally giving somebody else an IP address on your machine, and you're connecting. So it makes sense for a personal use to, like, hook your own machines together. But I was wondering, you know, like for example gamers, a lot of gamers are using this in order to create their own little five-dot LAN systems. But it does mean that other people are connecting to your machine, just like they were in the same room, plugged into a hub.

Leo: So you're on a LAN together. When you say "five-dot," that's the address range that uses five dot something dot something dot something.

Steve: Exactly. But the other thing that's important is that, even while you're using Hamachi, your machine still has its original IP. So, for example, in Greg's case, where he's at a friend's house using his laptop and using Hamachi to connect to his machine at home, he's still on his friend's wireless LAN. So he's got his wireless IP, which is still keeping him exposed from that standpoint.

Leo: So essentially what's happening is he's putting his home machine on the local LAN, as visible as any other machine; right?

Steve: Only if he had some trojan software on his laptop, that would be a problem.

Leo: It would have to be on the connecting machine.

Steve: Yeah.

Leo: Not anywhere else on the LAN.

Steve: The way to think of it is that, when you're using Hamachi, your system has its original IP and the Hamachi IP, not the Hamachi IP instead of the original IP.

Leo: I see.

Steve: So the first caller's question about firewalls, the short answer is yes, you still need a firewall.

Leo: But not to protect your Hamachi connection.

Steve: Exactly. Well, not to protect the data flowing over the Hamachi connection. But, for example, say that you were going to be using Hamachi for gaming, and you wanted to tie ten machines together. Well, it would make sense to use your firewall to only allow gaming traffic over the Hamachi IP. So you really do want to use a software firewall to protect access through Hamachi, if you don't trust somebody on the other side. That is, if you don't trust the Hamachi computers you're connecting to, you still want to keep your guard up. And so because Hamachi looks like a standard Internet interface, and most firewalls will allow you to permit traffic by interface, that is, by connection, you could say only allow the gaming traffic over my Hamachi 5.xxx IP. And you certainly still want to have a firewall to protect your non-Hamachi IP.

Leo: So, and let's say you're using a router as a firewall, and the router port forwarding - what port does Hamachi use?

Steve: Well, see, that's actually a really perfect example because, by using Hamachi, you are basically penetrating your router's inherent security when you create a Hamachi tunnel between...

Leo: Because it's an outgoing thing, you don't have to forward it.

Steve: Well, and it allows incoming traffic.

Leo: Once you've established the tunnel.

Steve: Once you've established that tunnel. So the tunnel is made outbound through your router. But once you've got the Hamachi tunnel, inbound traffic is allowed and is not...

Leo: Of any kind.

Steve: Exactly, of any kind, and is not controlled. Basically it is...

Leo: So the router and firewall don't even see it.

Steve: Exactly. Well, now, your router cannot see it. Your software firewall will see it. And so it...

Leo: Do you have tell the firewall anything particular, like watch five-dot?

Steve: Yes. In fact, normally, if you look at a software firewall, if you've got one that is about inbound blocking, for example, you may have to deliberately permit Hamachi to access out to the rest of the Internet. So...

Leo: It'll give you that pop-up most of the time that says...

Steve: Exactly.

Leo: ...Hamachi's trying to access the Internet. Do you want to be able...

Steve: Well, and for example, say that you were, like, a high-volume Windows user, as most are, using Windows XP Service Pack 2. So you've got the Windows Firewall on. You won't initially be able to get any incoming traffic. Now, the non-secure solution is to simply remove Hamachi from the firewall completely. That's okay as long as you trust the computers that are on the Hamachi network. But what you probably really want to do is to specifically allow only the traffic, like the gaming traffic or whatever, if...

Leo: Open the port that that game uses.

Steve: Exactly. Forward that port through that only the game is going to need. Otherwise, anyone who you're connecting to in their Hamachi network has complete access to your machine.

Leo: So you'll give your software firewall permission for an outbound connection to Hamachi from your system. And then you may say, but don't allow any incoming traffic except traffic over the specific port that that game or whatever thing you want to use, uses.

Steve: Right. I mean, these are great questions because this is a confusing topic.

Leo: Is it documented on the Hamachi site, or do you have to just kind of figure it out?

Steve: If someone will go through the forums. There's not a lot of documentation, like static documentation on the pages. But there's been a lot of dialogue in the Hamachi forums. And that's a great place to learn about, you know, all these Hamachi specifics.

Leo: Norbert Davis asks - is it Norbert in Davis, or is Norbert Davis his name?

Steve: I think Norbert Davis is his name.

Leo: Okay. I've loved the ZoneAlarm software firewall because I can see what programs are asking to talk back to the mothership. That's that outbound traffic protection we're talking about.

Steve: Right.

Leo: Really the only real reason to run a software firewall. However, ZoneAlarm has become bloated in its code, consumes a lot of resources, and does things I don't need. Can you recommend a good freeware or shareware software firewall? I run Windows XP and need something dependable but lightweight.

Steve: You know, it's funny, earlier on in our podcasts, and this was months ago, I referred to two firewalls that I liked a lot, and that's Tiny and Kerio. We had a lot of people who wrote back and said, wait a minute, they're both being discontinued. And it turns out that they were sort of partly being discontinued. They were changing their nature. I did some research about six months ago on the next versions of my little LeakTest freeware, going to be LeakTest Version 2 and Version 3, that were going to be looking at sort of next-generation threats, aside from what my little first LeakTest did. From looking at all the firewalls out there, my two favorites were Tiny and Kerio.

Leo: At the time.

Steve: At the time, which is what I mentioned. Okay. The really good news is, Alex Eckelberry of Sunbelt Software is a good guy. Sunbelt Software is down in Florida. They've got a bunch of security and privacy-related applications. He liked Kerio so much that he bought it.

Leo: Oh, neat.

Steve: So Kerio has a new home, a new publisher.

Leo: And they've renamed it to Sunbelt and Suspenders?

Steve: They're leaving the name Kerio because I guess he got the rights to that, too. It used to be, I think it was $44.95 or $45 or something. He's dropped the price to $19.95.

Leo: Great.

Steve: And through March of this year he's, like, having a "we bought a new firewall" special - I guess we could call it a fire sale? - firewall sale, $14.95. Now, the free version is really all anyone needs. Kerio does a

number of...

Leo: Oh, so they're still doing a free version.

Steve: Yes, and they will always do a free version.

Leo: Oh, great.

Steve: I think it's 4.1.something, you know, it's got the versionings, the changes frequently. But it's being kept up state of the art. It does pop-up blocking and cookie handling and some nice additional features. It also does something which is increasingly important, which is it deals with rootkit-type behavior. It watches processes that are trying to start other processes. And so it will catch many sorts of malicious behavior that your typical standard firewall will not catch. And I think even the free version has that. It's the cookie handling and pop-up blocking and things that you get extra in the paid version. But even the paid version is $14.95 through the end of March. So anyway, if I had to...

Leo: Are you recommending this for people who already have routers?

Steve: Well. There are, okay, routers will protect you from any external intrusion. And XP Service Pack 2's built-in firewall, which is free, protects you similarly from any external intrusion. There are a lot of people who really like knowing what's going on in their computer, and they want, when they're running a new program, they want a software firewall to alert them when this program is trying, as this caller asks, to phone the mothership.

Leo: Right.

Steve: You know, to phone home. And so, in fact, it's the way I found the very first spyware I encountered, was I was beta testing the original ZoneAlarm, and it popped up something saying that TSAdbot was trying to use my Internet connection. Well, I didn't know what that was or that I had anything like that in my machine. So, I mean, I was really glad to have it for that purpose.

Leo: Do current attacks, trojans, turn off software firewalls?

Steve: Well, that's one of the problems when you have a firewall as pervasive as Service Pack 2's firewall in Windows XP, is it's not invulnerable because any software that gets into your machine pretty much can do whatever it wants to inside of your machine.

Leo: So it could disable it.

Steve: So it certainly could disable it. And, I mean, and the firewalls have been in sort of a standard, you know, like antivirus/virus cat-and-mouse game. Here it's like the trojans versus the firewalls game, where the firewalls are continually trying to strengthen themselves against new ways to be turned off. So you really want to keep stuff out of your computer because, once something gets in, you're pretty much in trouble.

Leo: Which begs the question, what do you need outbound protection for?

Steve: I mean, I don't disagree. It is more hassle because things are popping up, asking if you want to give them permission. The firewall will learn if it's okay for this application...

Leo: Yeah, it shuts up eventually.

Steve: ...like Internet Explorer, Outlook Express and so forth, and Skype and so forth. I am not a user of an outbound firewall because I pay a lot of attention to my machine. I'm very careful with what I install. But personal firewalls are very popular. People are constantly writing, saying what's the best personal firewall?

Leo: So there it is.

Steve: So there's the answer. Is it Kerio? It's going to live on from now on at Sunbelt Software. They're great people, and they've dropped the price down, and they're going to keep it current and, you know, fix the bugs and so forth.

Leo: Excellent. Dylan in San Francisco writes: Is there anything I can do to stop recreating the same adware tracking cookies on my PC? For instance, you know, I'll run Spybot, Ad-Aware, Microsoft's Defender on one day and remove all the problem cookies. Then the very next day I'll run the same programs, and they're back.

Steve: Well, as you and I have talked about before, a lot of the so-called spyware or bad cookies are just stuff that your system collects. You know, some of these adware tools get a little carried away in trying to demonstrate their effectiveness and talking about, you know, or in discriminating what's bad and what's good. So...

Leo: It looks great if you say, "You had 60 infections, and I removed them all." But they're all cookies.

Steve: Or 432. I mean, I hear people talk about these insane numbers of stuff that was found. And it's like, okay, not all of that is bad.

Leo: So what should you do? It's kind of unusable to use the 'Net without cookies. You've got to leave cookies on.

Steve: Well, and you and I have talked about this before. We're going to talk about this in detail in an upcoming podcast. But essentially what's happening is third-party cookies are what these things are detecting, like DoubleClick cookies and...

Leo: Ad cookies.

Steve: ...ad cookies. As we have discovered, Leo, actually it's when we were doing a Call for Help show, we looked at the various browsers. All browsers today, by default, enable third-party cookies. That's what you want to turn off. In Opera and in Mozilla and Firefox, there's normally a checkbox that says "allow third-party cookies" or "foreign cookies" or something.

Leo: Uncheck that.

Steve: Yes, you want - whichever the - sometimes it's...

Leo: So cookies from originating site only is what you really want.

Steve: Yes. And Internet Explorer, it turns out, doesn't have an easy way to do that. They've got a very scary button down in their configuration dialogue that says "Advanced," as if, oh, I don't know if I'm old

enough to press that. It turns out, just push the "Advanced" button. None of their default cookie handling actually handles cookies the way you want. When you press the "Advanced" button, you get a simple dialogue where you can say, "Allow first-party cookies; deny third-party cookies," and problem over. And that's a large part of the debris that keeps coming back into someone's system after they've, like, cleaned it out.

Leo: And that's really the only risk from cookies is these third-party images or third-party cookies. Those are the real risks.

Steve: Right.

Leo: Just don't let those load, and you're fine.

Steve: Right.

Leo: And then you don't have to delete the rest. And if they come back, it's not a big deal.

Steve: Right.

Leo: Charles writes from Katy, Texas asking: With U.S. government NSA eavesdropping and spying so much in the news, do you really think that SSL, SSH and other things we think are safe are truly safe from the folks who, you know, have this high-end stuff and big computers, like the NSA? They can crack through this stuff, can't they?

Steve: No.

Leo: No.

Steve: No. The good news is, academic people and cryptologists who are not part of the NSA, with no axe to grind, have developed this current state-of-the-art crypto. We understand exactly how it works and why it's uncrackable. For example...

Leo: It just takes that long to factor prime numbers, period.

Steve: Well, or to take the log of a really huge exponent. The Diffie-Hellman key exchange operates by raising a large number to a large power.

Leo: Now, you can throw a lot of computer power at it. But if you get enough bits in your encryption, it's still going to take to the end of the universe to solve this.

Steve: Right. The beauty of cryptography is that it seems complex and, you know, mysterious to us. To the cryptographers, it's not. You take two really large prime numbers, and you multiply them together, and you get this really huge number. Now, it turns out that cracking crypto is a matter of finding out what the two primes are that made up this really huge number.

Leo: Right.

Steve: There's no fast way to do that. I mean, people have studied this thing...

Leo: Now, that could happen down the road, some brilliant mathematician could crack this by coming up with a way to do it.

Steve: There could be a breakthrough.

Leo: But right now...

Steve: But we would all know.

Leo: Yeah.

Steve: So the beauty is it's not like this is based on some reliance on aliens or something...

Leo: Or chaos or...

Steve: You know, exactly, something bizarre that we don't understand. We know why it cannot be broken in a feasible time.

Leo: Right.

Steve: And the NSA may not be happy about the fact that they would have to...

Leo: They work.

Steve: ...put on amazing supercomputers to crunch something for a year to crack it. But it really, I mean, everything we know says nobody can do this.

Leo: You're okay.

Steve: You really are.

Leo: Even the spooks can't do it.

Steve: Because, again, we know why it's safe.

Leo: Right, right.

Steve: It's not like it's safe because no one's broken it yet.

Leo: Because we say so.

Steve: Exactly. We know what it takes to break it, and it just takes too long.

Leo: What is the minimum bit length you recommend?

Steve: 128 bits now.

Leo: If it's that big...

Steve: 128 bits of symmetric cryptography. Now, we're going to be doing very shortly here a really nice podcast explaining symmetric and asymmetric and public keys and how all that stuff works. But 128 bits of symmetric crypto is plenty strong.

Leo: I'm going to throw in some of my questions here because I - when you talk about SSL, you talk about 128-bit. But when you talk about RSA encryption, you talk about 1,024 and 2,048.

Steve: Yes, yes.

Leo: Are those comparable? What...

Steve: And even SSL will have a 1,024-bit component because those protocols use both public key and private key, that is, asymmetric and symmetric crypto. So the initial key exchange, which you're using for authenticating a remote server, that uses a public and a private key pair because that type of crypto is fundamentally less secure. The way you strengthen its security is by ramping the bit depth up high. So 1,024 bits. And in fact, I'm using OpenVPN in 2,048-bit length, just because...

Leo: You can.

Steve: ...why not? Yes, exactly. And, I mean, that's just ridiculously strong.

Leo: It can slow things down a little bit, but not significantly.

Steve: Well, and the actual crypto operations, and this is what we'll talk about in detail later, the actual crypto operations for bit lengths that long are so slow that you cannot afford to do it with your actual bulk data that you're shipping back and forth.

Leo: Oh, I see. So that's just for the key.

Steve: Exactly.

Leo: And then the crypto is 128-bit.

Steve: They use the public key technology, the asymmetric key, just to exchange a 128-bit private key. And that keeps it private so that only the two of them know it. Then they get to use high-speed crypto that uses shorter key lengths and is super secure.

Leo: Now I understand. So one is for the public key; one's for the private key.

Steve: Right.

Leo: John in Sunnyvale, California has a complaint that I have, I share with John. I'm always giving you a hard time on this. He says there's no way to find your password generator page from your site. Could you please put a link on the homepage so I can send friends there?

Steve: Well, before answering this question, I have done that.

Leo: No, have you?

Steve: Yes. Our homepage has GRC's Perfect Password Page or something like that, right on the homepage.

Leo: You've always had to dig through your site to find anything.

Steve: I know. It just - it keeps growing, and I've never - you should see my closet. Or no, maybe you shouldn't. Anyway...

Leo: So there's no conspiracy theory here. I always thought, well, he just wants me to see everything he has before I...

Steve: Oh, that's good, too. Yeah, oh, that's why, Leo. Yeah, that's the reason. Actually, it's just GRC.com/passwords.

Leo: That'll do it.

Steve: That's all it takes. But for those who can't remember GRC.com/passwords, if you can get to GRC.com, it is there now on the homepage.

Leo: I know some good web designers. We're doing a redesign on TWiT. Do you want me to...

Steve: I'm getting interested.

Leo: You know, it wouldn't hurt.

Steve: It wouldn't, yeah. Maybe then I...

Leo: You could still do it all.

Steve: Maybe then I'd get lost on my own web, on my own site.

Leo: You understand how it works. Paul in Athens, Ohio writes: What's the comparative security of Windows, Linux, and UNIX Mac? This is a very common question. A lot of people say, oh, you Mac people, it's going to be just as bad as soon as Mac is as popular as Windows. They're just as insecure. Well, are they?

Steve: Okay. To do justice to this, it's worth saying that Microsoft's Windows started out being a catastrophe. I mean, it was never designed for the Internet. Apparently no one at Microsoft understood what it meant to even design an operating system for the Internet. I mean, for years and years and years they had problems that were not, I mean, like, not just bugs, not mistakes. I could...

Leo: Misunderstandings.

Steve: ...forgive anybody - yes. They were running open servers, you know, file and printer sharing, sitting there exposed for...

Leo: This was a corporate issue because Bill Gates didn't really think about the Internet until late. He came to it very late. I remember when he suddenly - the light went on, and he turned around the whole company on a dime.

Steve: Well, remember, MSN was going to be his AOL-killer when everyone was doing dial-up. He was going to have - and then the Internet happened, and he said, whoops, we need a browser.

Leo: So no surprise. But have they been able to catch up? In other words, they didn't start with good security. Have they been able to fix that?

Steve: With security, the size of your code, the complexity of the code are always killers. And Windows is huge and bloated and very complex. I mean, it's feature packed. But features are all potential security risks. In all fairness, Windows is getting so much better. I mean, the change with XP and Service Pack 2, putting a firewall in that would prevent external intrusion and having it on by default, that was a huge win. Now, the Mac, and to a somewhat lesser degree Linux, but also Linux - the Mac because, of course, it's based on UNIX. UNIX was the founding OS of the Internet. I mean, the guys who wrote TCP, they implemented it on the UNIX platform.

Leo: But I do have to point out that, even though UNIX was always a multi-user operating system and was permissions-aware, and they had passwords, they also, like everybody else, were kind of tilted in favor of openness. And some of UNIX was not designed very securely in the beginning.

Steve: Right. Well...

Leo: But it is 30 years old.

Steve: Well, and again, it's...

Leo: 35.

Steve: It's evolving. The problem is, anytime you do new stuff, you know, like PHP interpreters, PHP has had all kinds of security vulnerabilities because it was put together and put out and tested, but there were...

Leo: And then people banged on it.

Steve: And then people banged on it. So...

Leo: So what's the bottom-line answer?

Steve: I don't really think there is a simple summary. I would say that Windows is far better today than it ever has been before, that they are showing signs of finally figuring out what they need to do. And Microsoft understands security really matters.

Leo: I'm still using a Mac.

Steve: Yeah.

Leo: Angie Brae of Venice, California writes: How and why are pop-ups triggered only when I open a browser? Does a malicious software rewrite the code for IE? I've noticed when a computer is hijacked or compromised in any way, it all starts when I open up a browser.

Steve: Yeah.

Leo: What's the deal?

Steve: Well, this is Java script, or Active script, or some sort of...

Leo: Or ActiveX.

Steve: Or ActiveX, some sort of scripting technology. The problem is, and this was something really that Netscape is responsible for because that's where this all came from, was they wanted websites, web servers that you visited with your browser, to be able to make more dynamic pages than just these, you know, well, my pages on my website, which are just content and just sort of sit there...

Leo: Static.

Steve: ...and you click links, and you scroll around, but there's nothing fancy going on.

Leo: It only changes when Steve opens up his HTML editor.

Steve: And types ASCII into my - actually it's my Notepad that I do the web pages in.

Leo: But many pages are not that way. They run scripts all the time.

Steve: Well, and users want more functionality. So really our browsers are much more functional because they are running scripts which are provided to them by the websites they visit.

Leo: It's client-side scripts that are the problem, though. Server-side scripts like PHP, like Perl, like all...

Steve: That's a very good distinction, yes.

Leo: That is running on the server, not on your computer. And that's safe.

Steve: Yes. So what happens is, you go to a site, and not only are you downloading the web page content, you're also actually downloading...

Leo: A program.

Steve: ...executable script code, which runs on your browser in your computer. And if it says open a new window, that's what your browser does.

Leo: Which is why Firefox might be a little bit safer from spyware because it doesn't have ActiveX or active scripting. So it's more limited in the things it can do. It's actually a dumber...

Steve: It's got Java script.

Leo: Right.

Steve: It certainly has Java script. And Java script is able to do these things, as well.

Leo: True.

Steve: I guess the point is, in order to answer Angie's question, it's the site you're visiting that is doing this through your browser. So if you don't like that...

Leo: Don't visit that site.

Steve: ...you can either disable those features, or don't visit that site. But it's not like the Internet in general that's somehow tunneling through your browser.

Leo: Well, but if you accidentally download spyware, or if you have a ActiveX intrusion...

Steve: Oh, if you've got bad stuff...

Leo: Then you can have a program on your computer, doesn't need your browser, can pop up stuff even when you're not online. That's another - that's really spyware, and that's...

Steve: Right.

Leo: ...a whole 'nother conversation from pop-ups. Bert in Redford, Michigan asks: You mention that formatting a system and reinstalling removes most rootkits, but not necessarily all viruses, as some can reside on Track 0, or the master boot record.

Steve: Right, we did talk about that a few weeks ago.

Leo: So will a low-level format, or using the manufacturer's software to write zeroes to the drive, remove all information, including that track surfacing?

Steve: There's a very cool, free, open source tool called Darik's Boot and Nuke, DBAN.

Leo: That's a must-have for everybody.

Steve: Yes. What this does is, it allows you to burn your own CD from an ISO. You can just put DBAN into a search engine. It'll find Darik's Boot and Nuke. This thing creates a little bootable Linux that runs a scrubbing program. So...

Leo: Which will do, by the way, good disk erasing, so it's good if you want to really clear off your desk.

Steve: Oh, it'll do serious, like, overkill disk erasing.

Leo: But it also does the master boot record and all...

Steve: Absolutely. So, for example, if you want to start over from scratch and absolutely know that nothing bad at all was on your drive...

Leo: Boot and Nuke it.

Steve: Boot and Nuke it. Or if you're decommissioning a computer, you're going to give it...

Leo: Right.

Steve: ...you know, donate it to a...

Leo: That's who I'd recommend it for, yeah.

Steve: ...school or something, you know, scrub the drive with Darik's Boot and Nuke, and there'll be just nothing left behind.

Leo: Low-level format is not only not advisable, it's not possible on modern drives. You used to be able to do that; remember?

Steve: Well, true low-level format isn't. Some manufacturers will allow you to trigger a low-level format on their drive. What they're doing is they're writing zeroes throughout the entire drive. If your drive manufacturer lets you do that, that will erase the whole drive to zeroes. It won't deeply erase it. So the NSA can get the data back if it came to that. But...

Leo: You know, I asked Simpson Garfinkel this because he's the MIT graduate student who did the study of hard drives. They bought a bunch of hard drives on eBay and found passwords, ATM card information, all sorts of stuff.

Steve: Oh, just all in the clear right there.

Leo: And I asked him, I said, do you really need to do this, you know erase, rewrite ones and zeroes erase? He said no, you know, not really.

Steve: Yeah.

Leo: That's, you know, I don't know of any way, even the NSA really...

Steve: Right.

Leo: But nevertheless, Darik's Boot and Nuke does do that.

Steve: Yup.

Leo: And Boot and Nuke is free. Grant, UC Berkeley writes: I can't use Windows Remote Desktop because I don't have XP Pro. To be a host you have to have Pro. You can use it as a client with XP and 95, 98, even on a Mac. But the hosting requires Pro. He said RealVNC has been suggested on the Hamachi forums. Is RealVNC secure? I use RealVNC, as a matter of fact, all the time.

Steve: Yeah. The VNC project was, I think, started by some AT&T folks.

Leo: It's an AT&T in the U.K., yeah.

Steve: Yeah. And it's a terrific solution if you need multi-platform. It's Linux, Mac, PC, so cross-platform. You're able to run the server-side on one platform and the client-side on the other. And there's also something called TightVNC, which is a free version.

Leo: That's what I use on Windows, yeah.

Steve: Yeah. RealVNC has...

Leo: I use Chicken of the VNC on the Mac, by the way.

Steve: Chicken? Oh, Chicken of the VNC, oh, my God.

Leo: That's very good.

Steve: There are three versions of RealVNC. There's a free edition, there's a personal edition, and an enterprise edition. The free edition is not secure. It will allow you to log on in a secure fashion using a challenge passphrase handshake. But after you've done the log-on, the actual data is in the clear. It is not encrypted. So it's...

Leo: When we use this, we set up a VPN first, establishing a tunnel, an encrypted tunnel, and then use VNC over the VPN. And that's secure.

Steve: And that's exactly what I was going to say, was that if, you know, the question was, could I use this with Hamachi, and would it be secure?

Leo: Then it would be.

Steve: Absolutely. And so you could definitely use any version of RealVNC, even the free one, over Hamachi, and it's going to give you, you know, good performance, and Hamachi will provide the security. If you ever need to use RealVNC outside of Hamachi, and you certainly can, you're probably going to want to use the personal edition, which is $30, and there's a trial period and all that, because it invokes serious, state-of-the-art encryption over your entire connection, both your log-on and all communications afterwards.

Leo: Brian in Toronto says: I never give out my name online. So how do the RIAA and the MPAA find

me? How do they know my name and address? They only have my IP address. How can I hide that?

Steve: Well...

Leo: First of all, they don't have your name and address. They only have your IP address.

Steve: Well, they start out with only having your IP address.

Leo: They have to file what's called a John Doe lawsuit.

Steve: Exactly. Your ISP knows your IP address. Even somebody like AOL, who's issuing IP, if someone were to compel them, like a court order, and this is how the RIAA and the MPAA, you know, the people who are going and suing people who are doing filesharing, the way they get those is they collect all these IPs, they go, they get court orders to compel the ISPs to release the actual physical name and address of the person who had the IP either that week, in the case of, like, a cable modem that has a relatively static IP; or during a particular hour of the day if you were, like, an AOL user. So even though you feel like you've got some anonymity, your true anonymity has limits on the Internet.

Leo: When people use BitTorrent, your IP address is known. Any peer-to-peer. You wouldn't be able to do it if you didn't have an IP that somebody could hook up to. That's what it means, peer-to-peer.

Steve: And the RIAA and these other people who are trying to prevent this, they have invested serious technology in, like, creating IP-scraping systems...

Leo: Yeah, called honeypots.

Steve: Exactly, like fake BitTorrent clients and fake Kazaa and all these clients that are being used for peer-to-peer sharing, they're able to get in and harvest who's got which files and what IP they are. Now, the other part of the question here...

Leo: He says: How can I hide my IP address?

Steve: Yes, was how to hide it. There is an interesting system called the Tor system. It stands for The Onion Router. Onion routers are deliberate, like, proxy routers that allow you to send your traffic through them. If you just put Tor, T-o-r, into a search engine, you'll find The Onion Router project. There are hundreds of these routers set up all over the world. And it's actually being funded by our free speech folks, the EFF.

Leo: EFF?

Steve: Yes. The EFF is currently hosting the site...

Leo: Interesting.

Steve: ...and financing the project because they believe in free speech and freedom for use of the Internet.

Leo: Now, as long as these anonymizing servers don't keep logs, you're okay.

Steve: And they explicitly do not keep logs.

Leo: They have to destroy them.

Steve: Yeah. So and also you normally bounce through three or four or five of these things before you come out of the other end. And, I mean, you know, you're just untraceable at that point.

Leo: Anonymizer works this way, too. And that's one of the disadvantages of that is it does slow you down...

Steve: Yes.

Leo: ...because you're traversing a lot more miles.

Steve: And The Onion Router system is free, so you don't have to pay for it; whereas you do for Anonymizer.

Leo: Right.

Steve: Anonymizer, as you said, is a business specifically put on Earth here to...

Leo: To do that.

Steve: Exactly. You have to pay them some amount of money per month. But the traffic stops there.

Leo: It's not much. It's 35 a year, I think.

Steve: And they protect your identity.

Leo: I also use an iPhantom, which does the same thing. You have, instead of your IP address, you have the iPhantom IP address.

Steve: Oh, and iPig. The iPig system, the iOpus iPig client, if you are using them to route your traffic, no one would be able to know who your real IP was.

Leo: But I have to tell you that, if a court order comes down, most of these at least commercial entities are going to cave in. And if they say, who was using your system, unless these guys explicitly destroy logs so that they can't answer that court order, you're just as much at risk.

Steve: Right.

Leo: You know. So you really should ask a commercial entity, what do you do with those logs? Do you keep track of who's using...

Steve: Right.

Leo: ...what services?

Steve: And so, for example, you know, GRC.com I keep no logs. I will turn them on briefly if I'm, you know, needing to figure out something that is wrong. But I don't log any of the traffic at GRC.

Leo: I like that. We're going to get a hat for you. John's got "I Get No Spam."

Steve: I keep no logs. He gets no spam.

Leo: You can have...

Steve: "I Keep No Logs."

Leo: ..."I Keep No Logs." You know, I should do that with my servers, too. You have IIS, so I can't ask you how to do it. But I'm sure on Apache there's a way to just say, hey, that log gets turned off.

Steve: Oh, yeah.

Leo: Either doesn't get kept or gets just deleted frequently.

Steve: And it lightens the load, too.

Leo: I could do it with the kron. Yeah, because it's really...

Steve: Those logs are huge.

Leo: Huge. Last but not least, Joe from Iowa Falls, Iowa says: I have a question about wireless security. Is there a potential risk, when setting up your WPA protected network, as the key will be transmitted wirelessly? Preshared key?

Steve: Well, it's called a "preshared key" because it's not transmitted wirelessly. There is no exchange of keys in this environment. The idea is...

Leo: You have to ask me.

Steve: Well, you have to use another, you know, technically it's called a "secure channel," which is just like writing it down on a piece of paper and manually typing it into the other end.

Leo: That's the secure channel.

Steve: That's the secure channel.

Leo: Ask Steve.

Steve: No one is able to get you, you know, from anywhere on the Internet.

Leo: So the key is never sent over the Internet?

Steve: It is never sent over the Internet. And in fact, derivative keys are used and generated on the fly. This is with that TKIP, the Temporal Key Integrity Protocol that WPA uses. The idea is that only if endpoints already know the key, which they got because they were configured that way, not using any kind of radio connection or even network connection.

Leo: So it's not like this challenge/response thing, where it says, what's the password, here's the password. We're never sending the password.

Steve: Absolutely never.

Leo: Oh, that's interesting.

Steve: Yeah. And so, I mean, it has been engineered from the start the right way, unlike WEP encryption, which as we know is badly broken.

Leo: Well, I thank all of you for your questions. There's, of course, many more than we have time to answer on a single podcast. But we love doing this, and we will do it every fourth show.

Steve: Yup.

Leo: Conditions permitting. Next week...

Steve: Next week we're going to start with the long-anticipated series, "How the Internet Works."

Leo: It's only a month late. That's not so long.

Steve: It's been a busy month.

Leo: It's been a busy month.

Steve: Yeah.

Leo: There's been a lot to talk about. We're glad you listen to Security Now!. We hope you'll keep listening every [Thursday] at TWiT.tv or GRC.com/securitynow.htm. In fact, Steve, I know almost 5,000 people a day download the podcast from your site alone.

Steve: Or, yeah. Well, all of our audio files. Because I have an archive of everything that we've ever done. And here we are, we're at the end of our sixth month of doing Security Now!.

Leo: There's a lot there.

Steve: Yup.

Leo: Both in the high-quality 64KB, as well as a very low bitrate, 16KB for people who don't have the bandwidth. We also should mention that we know we are having some trouble with truncated files. This is due to the Akamai servers that our provider AOL is using. They went to Akamai because they were pushing 3.4 terabytes a day, and they had to. And we know, we're working it out, and we think that this will be solved soon. But if you have been getting truncated podcasts, just send me an email saying, you know, I'm having trouble with the Akamai. I need your IP address or your location, that'll help, and how big the file was that you did get. That will help us track down which servers are not caching properly.

Steve: And for what it's worth, I serve the low-bandwidth files from my own server.

Leo: That's HTTP, so that's always complete.

Steve: And I always make sure that that's correct. So my high bandwidth links do link to AOL. So you'll still have a problem. But if you did have a problem with a truncated high-quality file, let Leo know, and then you can always get the lower quality from me directly, and I know it won't be truncated.

Leo: I think we're going to set up a BitTorrent version, as well, so that there's at least always one good - we can't afford to provide the bandwidth for it. And thank goodness that AOL Music is there because, if it weren't for AOL, none of this would be happening. We wouldn't have TWiT, Security Now!, Inside the Net, none of these podcasts. But I think I'm going to start doing BitTorrents of everything. So should something go wrong with the AOL...

Steve: We'll have a backup.

Leo: You'll always be able to get it via BitTorrent. And I'm recommending a really neat new program for downloading these BitTorrents that makes it very easy to do. But I forgot the - I think it's [Fireant]. But you can go to the website, and there's some information on that at TWiT.tv.

Steve: Okay. And of course Mark Thompson has BitPump, which is his BitTorrent client.

Leo: A very easy-to-use BitTorrent client.

Steve: And nice file managers.

Leo: Windows only.

Steve: Oh, yeah, Windows - oh, no, Mac also.

Leo: He did a Mac client?

Steve: Yeah.

Leo: Mark "AnalogX" Thompson?

Steve: That's right.

Leo: Oh, wow. Mark's really spreading his wings.

Steve: Yup, AnalogX.com.

Leo: Now I know the world's almost come to an end. Again, transcripts, low-bandwidth versions, and lots more information about everything we talk about available at GRC.com/securitynow.htm. And by the way, while you're at GRC.com, don't forget SpinRite, the ultimate disk recovery and maintenance utility. If you've got a problem with a hard drive, you've got a file you can't recover, please, do yourself a favor, get SpinRite. I have it, and I use it all the time.

Steve: Makes it all possible at my end, Leo.

Leo: Yes, that's, well, that's our advertiser.

Steve: Yeah.

Leo: Yeah. It pays Steve's bills. We do thank our good friends at AOL Radio, who not only broadcast this on their podcast channel, but also provide us with the bandwidth for this at AOLmusic.com. And we thank you so much for joining us. See you next time.