Listener Feedback Q&A #14

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-072.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-072-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

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

This is Security Now! with Steve Gibson, Episode 72 for December 28, 2006: Your questions, Steve's answers, #14.

Security Now! is brought to you by Astaro, makers of the Astaro Security Gateway, on the web at www.astaro.com. And by Dell. For this week's specials, visit TWiT.tv/dell.

There is no rest for the security-conscious, and that's Steve Gibson, even though here we are, just a few days after Christmas, a few days before New Year's, the week that almost everybody in the world takes off, much of TWiT has taken off. No, Steve says, we must soldier on. A Security Now! every week, whether you want one or not. Hey, Steve Gibson.

Steve Gibson: Whether they want one or not.

Leo: Whether you want it or not, you're getting it.

Steve: Okay. Well, I've got to tell you, Leo, I don't know what it was about the last Q&A, but I've never had such positive feedback from people. I think it was a – now I'm a little nervous about, oh my god, I wonder if this Q&A will be as good as the last one.

Leo: We can't possibly be as good.

Steve: People loved the mixture of questions. They were giving me credit with selecting them.

It's like, well, I just select them like I always do. I don't know why those ones turned out so good. Actually this time we've got a bunch of TOR-related stuff, so there won't be quite the diversity that we had last time. I think that's one thing people liked was that there was just a really wide-ranging mix of questions. I think they also liked that you and I just sort of hung out and took our time. It was a 97□minute episode.

Leo: It was the longest podcast I've ever done, as far as I can tell. But you know, Steve, people do, they love what you're doing. And so I don't think it's – the nice thing about a podcast, if it's too long, just pause it or give up or whatever.

Steve: And I do like the way the Q&As break these episodes, you know, we have some that are highly topical, focused on just one thing. And I think that's good. I got a lot of people who said, my god, I can't believe you explained TOR with no diagrams or pictures or anything.

Leo: That is pretty amazing.

Steve: Just listening, they were able to understand the onion.

Leo: You're good at that.

Steve: Which I thought was really – it was really fun. So certainly there is a place for that kind of focus. And I think our Q&As do a really nice job of mixing that up and allowing people, first of all, to feed back. I do want to remind people that the bottom of the Security Now! page at GRC.com, just GRC.com/securitynow, the bottom of that page is where there's a form that anyone can use, giving their name and location or not – leave it anonymous in the interest of anonymity – in order to submit questions which I receive, the server sends it to me as email, they pile up, and then I go through them and pull questions for our Q&A.

Leo: And we've got a lot of good ones. Before we get to those, though, I do want to mention that SpinRite is Steve's bread and butter, and we do always want to give it a little bit of a plug. Not only because it's how Steve makes his living, but frankly because it is a must-have utility if you've got hard drives. It's really useful for people who are kind of the go-to guys for your friends and family, maybe your coworkers, when there's problems with the computer. I always have a copy of SpinRite in my possession for those emergency house calls. It is the ultimate drive recovery and maintenance utility, works with all kinds of drives. You can even – I didn't know this, but somebody sent me a note and said it works with external drives, too.

Steve: In fact, I've got a couple pieces of email from people who have USB drives that it fixed.

Leo: That's neat. I didn't know that. I thought that you wouldn't be able to get access, low level enough access to the drive.

Steve: It's very true that I don't have as low a level access to the drive through a USB or Firewire interface. And so the best way is if people can remove the drive from the case and just temporarily attach it to the motherboard. There I have a really intimate connection. SpinRite is not only faster, but it does have access then to much more about what's going on in the drive. But many times that's not possible, so SpinRite will still do the best job it can.

It's funny, here we are between Christmas and New Year's, and I've been sharing over the last weeks some of the email that we receive about SpinRite success stories. I thought, since this is sort of a special holiday episode, I would share a wacky one that I received. It's literally, the subject of this email, I just recently received this, it was "Steve, your SpinRite software got me fired." True story. The guys says it, hyphen hyphen true story. And first I was a little confused. Then I realized this was this person – I don't see his name here. But it's this person who is recounting a SpinRite 2 adventure he had. So that would make it about...

Leo: A long time ago.

Steve: About 15 years ago, yeah. Anyway, he says, "This happened in Rockville, Maryland. As a service tech in the MFM/RLL days" – so of course that's Modified Frequency Modulation and Run Link Limited are those acronyms.

Leo: I remember those.

Steve: Yeah, remember those, MFM, yeah. He says, "I was called to an old people's community organization. Their disk needed a low-level format. The nice old lady said, 'Thank God you're here....'" And actually this guy writes really well, which is the other reason I wanted to share this. Says, "'Thank God you're here,' begging me to fix her computer, and told me of all the sad terrible things that would happen to the old people if their data were lost. Being newly hired by the service company, I was accompanied by a senior tech from the same outfit. He was happy I recognized that the drive needed a low-level reformat. I got out my trusty personal copy of SpinRite 2. The other tech had never heard of nondestructive low-level formatting. 'See, this reads the track before reformatting it, then it formats the track, instead of writing zeroes as sector data. It uses the original data so they don't lose any. Isn't that cool?' I said."

Leo: It is cool. That was always the best thing about SpinRite.

Steve: It was very cool. And so he says, isn't that cool, he says, wide-eyed and innocent. Okay. "Then the other guy, the senior tech says, 'But won't that take twice as long?'" And he says, "I looked at the old lady wringing her hands hopefully on the other side of the room. She couldn't hear us. 'It will take 20 minutes instead of 10, but will save their data.' I assumed it was a no-brainer. 'No,' he said. 'This is a service contract.' 'So what,' I asked? 'So we already have their money, just format their drive, and we can bill that 10 minutes at the next job. We're not a charity organization.'"

So this guy writes, he says, "I felt like I was in the Twilight Zone. I thought about what to say. I thought about my professors at college and how much I missed them." And he says, so our guy says, "'No, I can't do that,' I said, and continued with SpinRite. It took 22 minutes."

Leo: Good for him.

Steve: He says, "After rebooting, the system was back up, and the old lady was ecstatic. 'What's your name, young man?' she asked. 'David.' 'God bless you, David,' she said. Well, get this. Afterward, out in the parking lot, we almost got into a fistfight over it, but agreed to take it to the company president. The president agreed with the senior tech and fired me on the spot."

Leo: Unbelievable.

Steve: "There was no other reason, just this. As I left, the other tech smiled smugly."

Leo: Wow, what a depressing story.

Steve: SpinRite got him fired.

Leo: Oh my god. And you know, I have a feeling that same kind of stupid shenanigans still goes on.

Steve: Well, it's funny because I read to – prior to meeting with you last week, Leo, in Toronto, I met with the Nerds On Site guys and hung out with them for a couple hours, and I shared this story with them. I didn't have it in front of me, but I remembered it because I had already put it together and posted it. And I read it, I told them the story, and they said, "Who is that guy? We'll hire him."

Leo: Yay. Now, I like Nerds On Site. They're going to buy some ads on TWiT, so I like them even more. But that's good to know, and that's the kind of thing I want to hear. I don't want to recommend a company that's going to look more toward the billable hours than toward the customer's satisfaction. That's a shortsighted way of doing business.

Steve: And wouldn't just reformatting the drive be faster than performing data recovery.

Leo: I'm willing to bet that company is out of business and long out of business. That is terrible.

Steve: We can hope.

Leo: Cool. That's really neat. I want to mention, by the way – and I forgot to mention this last week so I'll mention it again – you know SCOTTEVEST; right?

Steve: Sure.

Leo: They do great geekware, they call it "technology-enabled clothing," with lots of pockets and places to run wires for your – they call it "personal area network" – for your headphones or chargers or whatever. They're just really great. Jackets, pants, shirts and hats. And they've offered us a holiday TWiT code. Now, I know it's after Christmas, but a lot of times people buy this stuff just for themselves. So we'll put a link in the show notes. But if you go to SCOTTEVEST and you buy anything, use the coupon code TWiT. That'll save you 20 percent off, I think, or 25 percent off the cost. Just a little gift from us and SCOTTEVEST to our listeners. Now, shall we go on with the questions?

Steve: Q&A #14.

Leo: #14, starting with Dennis from Atlanta, Georgia: So, he says, I listened to Episode 69 about the social implications of Internet anonymity. Then I listened to Episode 70 about achieving Internet anonymity using TOR. Then the next episode of "Numbers" on CBS is about a vigilante – wow, this is on CBS? – using onion router networks to anonymously stalk and kill pedophiles. Seems like more than a coincidence.

Steve: It's funny, I got so many of these notes that I thought, okay, I just have to mention this. One guy said he was watching "Numbers" on CBS just after having listened to Episode #70 about the TOR network. And he said to himself, please mention onion routing, please mention onion routing. And they did.

Leo: That's so weird.

Steve: They referred to it by name as he's using onion routing. And apparently, I didn't see the episode, but they used the analogy of putting envelopes inside of envelopes and then sending them. And he said, of course that analogy only holds in the onion routing context so long as only the person to whom the envelope is addressed is able to open that envelope. And he said, wouldn't that be nice if paper mail actually worked that way. But it was just – so for all those people who wrote, it was a bizarre coincidence. We have nothing to do with the scheduling of programming on CBS or anywhere else.

Leo: No. In fact, they must have written that episode months before we did anything on it. But I think what's interesting is that this kind of advanced technology is now sneaking into mainstream programming, which just shows that people are more aware, and that mainstream media folks realize it's not the kiss of death to talk about technology. I like it.

Andy, listening from Spain, writes: This may seem a bit morbid, but I'd love you and Leo to discuss the handling of private encrypted data, passwords, and computer-based private information in the event of our death. I mean, today, while alive, I don't want to give my sensitive stuff or passwords to anyone, including my wife. But when I eventually die or become very ill, I need to make sure that my family has access. This makes a lot of sense, actually.

Steve: Doesn't that? Yes.

Leo: They're not stranded economically or practically. Also to make sure they can wind up and close down my company in a safe and good way. I've often wondered about this. And my stuff isn't even that encrypted. But I know my wife wouldn't be able to figure it out to save her life. If I have TrueCrypted all of my data, have complex unguessable password schemes and so forth, how do I unwind all of that for the benefit of other people I care about in my life?

Steve: Isn't that a great question? I mean, I thought that really was. Here we are, we spent 72 weeks now talking about privacy and encryption and uncrackable passwords and not writing them down and coming up with personal password algorithms and all this. Imagine, you know, if any of us or our listeners who were actually using these sorts of approaches suddenly, god forbid, something happened to them, they were critically ill or they passed away, here's their whole life that they've been deliberately working to keep out of the hands of bad guys. Well, inadvertently it's now out of the hands of good guys, I mean, their family, their friends, people whom they might wish had access to this. It's just no longer available. So I don't have an

answer, but I loved the question. And I thought it was worth...

Leo: TrueCrypt allows, for instance, your password to be stored in an image file, let's say. Right? And you can use that to decrypt.

Steve: Well, yes. If we wanted to provide a solution, it would be that you would have any kind of – and, I mean, TrueCrypt might be overkill. There are very nice little pieces of freeware where you can just take, like, a text file, and it will run it through symmetric encryption and just scramble it with full crypto strength. So what you could do would be give to your attorney who has your will, or in a safety deposit box, something where access will be granted in the event of something bad happening to you without your taking any action. And this is certainly not something that somebody who's 15 and listening to this is even thinking about. It's like, aw, I could live forever. But you know, you and I are...

Leo: We're thinking about it.

Steve: Exactly. So anybody who's preparing a will, who has a will, who's taken actions about what would happen in the event of their death, something to really think about is, is there any information, are there passwords to your email accounts, passwords to your drives, to your data...

Leo: Here's what I'm thinking...

Steve: Well, and to your online financial accounts.

Leo: Oh, and I've already done that. Here's what I'm thinking is that you separate the information out. So one of the things TrueCrypt lets you do is have an image file and a password. You need both; right? Maybe give the attorney the password, maybe even put it in your will, and store the image file in a safety deposit box. Separate the two, to be opened on your death or whatever. And that way – go ahead.

Steve: My only concern with that is that, from a practical standpoint, this might be a file you want to be modifying from time to time, have easy access to. The beauty of it being encrypted is that no – and you don't even need TrueCrypt, again, I mean, some little simple encryption program that would allow you to easily decrypt it, update passwords, account information and so forth. Basically it would be your whole life...

Leo: Everything.

Steve: ...in, you know, all the log-on usernames and IDs and passwords, everything you'd want someone to access if you were unable to. And then you lock it up again, you just reencrypt it, and you know what the password is, it's also stored somewhere like your attorney has it, or in a safety deposit box, so that if something happened, the directions there would be turn on my computer, run this program. And again, TrueCrypt can be a little confusing, I mean, it is a techie tool. So I was thinking in terms of a simple little simple encryption utility that will just decrypt a single file. And so the instructions could be run this program, enter this password, here's everything you need to know about accessing my personal private financial life that I want you to have access to.

Leo: Right. Jared Burford, a Security Now! listener and a SpinRite user in Western Australia, asks: On my laptop, my Hitachi 100-gig hard drive, which is a 7200 rpm hard drive, gets too hot when SpinRite is in operation. At times it reports SpinRite cannot continue due to overheating problems, proceed at your own risk. I took this seriously. However, at other times, when ambient temperature outside is cold, like when the air conditioning is on, it stays around 50 degrees Centigrade, and all is okay. I've read various posts and come to the conclusion drive temps vary with every drive, depending on size, capacity, et cetera. So my question, is 50 degrees Centigrade too high for a laptop drive to function?

Steve: That's interesting. SpinRite 6 is the first version of SpinRite where I made SpinRite aware of smart stuff. And one of the parameters that most drives make available, I think probably all of them being produced now, is their current operating temperature. What we learned during the development of SpinRite – and again I have my fantastic group in the newsgroups, we created a SpinRite Dev newsgroup where we all hung out, and I got a ton of testers – it turns out that laptops, to a much greater degree than desktop systems, really have a problem with heat.

Leo: Yeah, they've got nowhere to dissipate it.

Steve: Well, that's the problem, is that there is no space. And their super-small enclosure – any user of a modern laptop knows that, I mean, I'm impressed with battery technology because these things are generating an amazing amount of heat. Literally, you burn your lap. There are even some things for keeping your lap cool while your laptop is on top of them because it generates such a problem.

Anyway, what we learned was that, because SpinRite is using the drive continuously, that is, it's moving through the drive, and basically seeking is what generates a lot of heat because you are accelerating and decelerating the head very quickly, well, that requires a lot of energy, as anyone knows from their old days in physics is in order to accelerate something you need to apply a force, and then to decelerate it you need to apply the reverse force. So that ends up generating heat in the drive. So what SpinRite does is, if it sees that a drive, whether it's in your laptop or your desktop, is becoming too hot, it will bring up a dialogue box and say, hey, just wanted to let you know, SpinRite's going to stop now until things cool off. You can ignore this...

Leo: Oh, so that's a SpinRite error.

Steve: Yes. Well, not an error. It's like a SpinRite notification, yes. And so people can let things cool off, then proceed. I really like it, though, because many people have increased the size of their hard drives even in their desktop machines; and they didn't take account of the fact that now that they're running a 7200 rpm drive, it is drawing more power, it's generating more heat, and their system may not be designed to just move cold air through fast enough to keep the drive cold. The reason this is important is the number one killer of hard drives is over temperature. It is the number one cause of premature hard drive failure is drives running too hot, and no one's ever been keeping an eye on them. So...

Leo: So is 50 degrees Celsius too hot?

Steve: No.

Leo: That's not hot at all, really.

Steve: No, it's not. And I think SpinRite limits it at 75, if I remember. What I did was, I looked at all the manufacturer specs in the industry. And I was surprised, they were all in pretty much uniform agreement about the maximum operating temperature of the drive. And I just have SpinRite let people know if they're exceeding that.

Leo: Damon in Oklahoma writes: A previous Q&A topic of spam left me wanting more. Please talk more about what mail servers do to limit spam. Something to consider talking about in relation to these SPF records – we talked about that a little bit, the authentication records. ISPs are now filtering SMTP traffic. For example, create an SPF record for domain.com that states that SMTP traffic – that's the mail protocol, sending mail protocol – comes from, you know, 192.1.1 whatever, or mail.domain.com. This would work fine as long as your ISP allowed you to send mail over port 25 to your server. Sure, you could add the ISP's SMTP to the allowed list, but what happens when you or, more importantly, your less savvy users go on the road, you can't possibly add each mail record for all the potential addresses, the IP protocols that are blocking SMTP traffic, or all the ISPs. Nor would you want to. Doesn't this make the SPF idea almost useless? I'm not really following this, Steve. You'll have to explain. Super show, I'll buy the Dells from your link – thank you – I'll add cash to the donation bucket – thank you – whatever, keep them coming. Do both. Thank you.

Steve: Okay. So, yes. This is an interesting question.

Leo: I don't understand at all, so you'd better explain it.

Steve: Okay. And it's a perfect place for us to talk about what ISPs are doing about spam. We talked about SPF, the sender provider – oh, now I have an acronym loss.

Leo: I'll Google it while you talk.

Steve: It's funny, I'm just blanking on that...

Leo: Framework. I want to say framework. Sender something framework.

Steve: Policy framework, yes.

Leo: That's it, okay.

Steve: Yes. And it's funny, too, because they've changed what the acronym stands for several times. It's gone through a bunch of mutations which left everybody confused. So, okay. But it's a very cool concept. The idea is that we understand, we've talked extensively in the past about DNS, where anyone is able to make a DNS query saying what is the IP of this domain. Well, what SPF does is it adds another type of query that you can ask for. For example, you can ask for a so-called MX query and ask, what is the mail server for this domain? What SPF does is adds a query that says, what are the allowed IPs or machine names that you authorize as

originating mail from your domain?

So for example, GRC does have an SPF record. So when my mail server sends something to somebody else's mail server – say I'm sending mail to Google. Google has a TCP connection to me, so it knows my IP address because we know TCP connections cannot be spoofed, they have to be a real IP address. It makes a DNS query saying to – it notices that the mail is apparently coming from GRC.com. It makes a query of GRC.com asking for the SPF record, which is a text record in DNS with a specified format. The DNS server returns a text record. In there is my specification, that is, I put this in my own, in GRC's DNS, saying email from GRC will only come from this one IP.

And so what happens is, it allows the recipient to authenticate the identity of the server. That is, if anybody else is spoofing GRC, some other non-GRC server is trying to send mail to Google Mail saying, hey, this is from steve@grc.com. Then what happens is Gmail asks GRC, could this be a valid IP for mail from GRC? Well, since I control my own mail servers, I know my IPs. That's what's in the DNS record. So, I mean, it is a really cool antispam feature.

Here's the problem. The problem is – there are a couple. First of all, and we got hit by this actually just a couple days ago, Greg, my tech support guy, sent me a piece of email that he had been unable to send to somebody else. The SPF system only works for point-to-point connections. That is...

Leo: Of course that makes sense, yeah.

Steve: It does. It does. Because any relay, relays of course have traditionally...

Leo: Everything changes.

Steve: Well, and relays have been a huge spam problem, so-called "open relays" where anyone...

Leo: We don't want those to exist, yeah.

Steve: Exactly, where anyone is able to drop email on an arbitrary server, and it will forward it on their behalf. Well, that's called an open relay, which is what spammers have traditionally used. So notice in my model it had to be a direct connection, a single TCP connection between my server and Google Mail in order for Google to trust that this mail was really coming from me.

So Greg happened to send email to someone who, for whatever reason, that email server relayed it to a third. That third server used SPF to verify that that relaying server was authenticated by GRC, and of course it was not. So it bounced the mail back to Greg saying this is an unauthorized server. Greg tried it a few times, sent the mail to me saying what's going on? I said, well, this is typical. This is what you have when security tightens things up. You have problems. Like last week, Leo, we were talking about all of the controversy of digitally signing device drivers. Well, yes, more security; but, yes, it's got some problems.

Leo: So what's the solution for Greg?

Steve: Well, there is no solution. SPF has this problem. It will not tolerate the use of relays because relays are so prone to abuse. Basically we were unable to send email to this guy whose email was configured with an intermediary server.

Leo: You could have sent it directly from GRC; right?

Steve: No.

Leo: No, because of the way he was configured.

Steve: Yes. At his end, he was configured with a relay. And so it's not just us, but anyone who is using SPF. And there are hundreds of thousands of servers now. Anyone who's broadcasting these records, or is making these records available through DNS, they're not going to be able to get mail to that guy. So ultimately he'll figure out, gee, you know...

Leo: I'm not getting mail.

Steve: I'm not hearing from people that I send email to.

Leo: And is it his Internet service provider that's caused this, or is he doing it, or we don't know?

Steve: I didn't pursue it beyond seeing what the problem was. But it was very clear that there was a relay. So something's going on. Now, the related problem is another problem that Greg has had because Greg sometimes travels around and wants to keep doing Security Now! – Security Now!. SpinRite support is what I pay him for. He does tech support for SpinRite. And sometimes he's out on the road. Well, he wants to be able to send and receive GRC mail. The problem is that his ISP is blocking port 25, and many ISPs are now because this is what trojans are getting compromised. We've talked about this a lot. Trojan machines are generating a ton of spam. They're doing so by using port 25 outbound...

Leo: They set up their own servers on the zombie machine.

Steve: Essentially. And what an SMTP server does is use port 25 outbound to another SMTP server's port 25 in order to transfer the mail. So ISPs are starting to block, and many of them now do, block port 25. You are able to connect to their SMTP server. So for example my cable modem has me use smtp.west.cox.net as my SMTP server that Cox provides. So I'm able to send mail to them, but I'm not able to send mail to another SMTP server. And Greg is unable to send email as being from GRC through his Cox server because then that creates a relay. Again, there's not a misconfigured relay. The only way he can send port 25 email is sending it to Cox. But when he deposits mail from GRC, from his GRC identity within his ISP, he puts it on their server, they try to send it somewhere, now it's being relayed. The recipient checks with GRC and sees that it's not valid.

Leo: Not the same address, yeah.

Steve: Right. Now what I could do is not what I did, but I'll present this because I know that lots of people are having problems like this. I could add Greg's ISP's server to the list of authenticated sources of GRC mail. It would open up a tiny vulnerability because then anybody using Greg's ISP's server could spoof email from GRC. But the likelihood of that is very low. Anyway, it's not what I did. What I did was, because I'm controlling our email, I just made up another port. We chose some random port up in high port land. And it's another entry to our email server. So Greg has configured his Eudora client, which we're all still using, he configured Eudora not to send email on port 25, to send it on XYZ, whatever port we chose. And so his ISP is not blocking that. So mail from greg@grc.com goes directly to our server, which then doesn't have this relay problem. So it is a tricky – you can see it was a complex question and not a simple answer. But it is going a long way to solve this problem of finally creating some authenticatability in the email system.

Leo: Brad Beyenhof of San Diego, California is wondering about onions. More TOR. With the TOR network, can't the various routers know who sent them the onion package? In other words, wouldn't it be possible to use such a record to backtrack the packets' paths and find out where they were originated?

Steve: Nope, you can't. Essentially the given router receives the onion package from one other router. That is, it receives it. Now, only it can decrypt the envelope. It didn't see the prior envelopes. Remember that we build the onion, which is fully nested as it starts down the path of onion routers. Each router uses its private key to decrypt one shell of the onion – or an envelope, to use CBS's term for this, their analogy. And so when any router receives the onion, they're only receiving what's left of it. That is, the outer shells have been already removed by the earlier stages down the route.

Leo: So there's no way to backtrack.

Steve: That information is gone. Not only that, you cannot forward track because after...

Leo: That's encrypted.

Steve: Exactly. It's encrypted with, you know, the remaining shell is encrypted with the next router's private key that only the next router can decrypt using – I'm sorry, it's encrypted with its public key, which only the next router can decrypt using its private key. So basically, any router that receives the onion gets – and this is what's so cool about this notion of these onion shells – receives only the information it needs to do its one little piece. It gets the symmetric key for the upstream link, the symmetric key for the downstream link to each of its adjacent routers, and the information it needs. Then it gets this opaque blob that it forwards to the next downstream router in order to continue making this routing path. So it's just – it really does work. It's very cool.

Leo: Very elegant. Carlos J. Restrepo in Houston, Texas, is seeking some assurance about crypto. He writes: I was wondering about crypto and the protection of privacy. If I use a program like FileVault in the Mac – that's the OS X's built-in encryption, it's kind of like the encryption now that's part of Vista – or some other program to encrypt your data, can the government or some other agency order the developers of these programs, in this case Apple, help them decrypt your data? And in this case are the developers able to decrypt your data based on the algorithm they used to create the program, or is your password absolutely necessary?

Steve: Well, I would tell Carlos, if he has not gone back and listened to the series we did on crypto, we did much earlier in Security Now! a really, I would almost say, sort of a landmark series in really explaining all of the ins and outs of cryptography and how this technology works. To answer the question, any properly implemented crypto, and certainly I'm sure that Apple's is, TrueCrypt's is, you know, as it's one of the reasons, Leo, that you like open source solutions so much is because they're transparent. The technology itself has no backdoor. So while it's possible that someone could, for example, be writing your crypto key somewhere secretly on the system, that's not the way these systems work. That would be a breach of their operation, not a breach of the crypto. Crypto itself does not have a backdoor, that is, the type of crypto we've been talking about where you have public key that is asymmetric keys with sufficient length or symmetric keys with sufficient length, they're just elegantly beautiful mathematical solutions. And while no crypto expert will ever say that it cannot be broken, as we know, security comes over time from many, many people scrutinizing it and trying to break it and never finding a solution. Well, that's the case with the mature crypto we have today. Everything we believe leads us to trust that there is no quick, simple solution for cracking crypto. So...

Leo: And just because they know how it was done doesn't mean they can reverse the process because they know how it was done. It doesn't work that way at all.

Steve: Exactly. That is the heart of the elegance is you can, and everyone does, publicly disclose, publish, write it on blackboards, talk about it in Security Now!, you know, complete disclosure of how it works. There is no obscurity because, as we know, security is not generally found in obscurity. It's completely unobscured, and it is absolutely bulletproof. So I think what Carlos wanted to know was just sort of a make sure that, you know, he could trust this to keep his secret safe. And as long as he uses a trustworthy solution, he absolutely can.

Leo: And again, that's why I say open source because somebody can verify it. I'd trust Apple and Microsoft, but those are closed source solutions, so you just don't know. The only way to be sure is if you have something like TrueCrypt, which everybody can look at the code of. Somebody pointed out that you can't always assure that the code has been vetted because, you know, especially small projects, people may not be looking at the code. But I think with TrueCrypt it's pretty safe to assume that that's been heavily vetted.

Bert Keates of Sun City West, Arizona is worried about being fully stealthed or not fully stealthed with Windows 98: I was occasionally using two Windows 98SE machines in my home office LAN. I disconnected both from the network last July. There's a Netgear router between the modem and my four computers. The other two systems run XP SP2 and IE7, though I browse with Firefox most of the time. Good man. I just hooked up one of the older Win98 machines and checked it with ShieldsUP. It's all stealthed except port 113 that's closed. Since my LAN is not true stealthed, should I be worried about those two older Windows 98 machines? I want to be able to print to three printers and share files across the network. Thanks from a long-time SpinRite user.

Steve: Well, there were a couple interesting things that Bert brought up. First of all, true stealth is just the term I made up for ShieldsUP, when you do a ShieldsUP test and it absolutely never hears anything back from the remote end. I do a bunch of funky things. I send TCP packets to port 0 that doesn't exist. I send ICMP to 0 and 1. I play with different bits. Basically I send a bunch of stuff, trying to get anything back. And only if nothing comes back do I then in the ShieldsUP display say "You have true stealth."

So what Bert is seeing is he's seeing something that's very common, which is the other reason I selected this question to talk about, and that is port 113. Port 113 is the so-called "IDENT" port. It's an old technology that has not been used for years. So it isn't normally necessary to

provide any information. The idea would be, when you were connecting to a remote computer, the remote computer would send you back an IDENT query looking for a server running on your machine that was listening for incoming queries on port 113. Your machine would then send back some confirming identification information which would just sort of be a way for the remote server to check in with you, get whatever information you were making available. Some old FTP servers are apparently still configured to do this. And some, I think it's IRC servers also do, too. Anyway, it's sort of old technology.

The problem is, if port 113 is stealthed, that is, if it's not closed, if it's stealthed, then the remote side will try to open up a connection. It'll send a TCP SYN packet and wait for that to time out. Then it sends another one. Then it doubles the wait time and sends another one. Then it doubles that wait time and sends another one. It can take, like, a minute before the server finally decides either, A, you don't exist, and so it won't accept your incoming connection to it; or it'll finally allow that. But in any event, if it's configured this way, it can delay your connections by a minute. So what the Netgear router is doing is it is stealthing everything but deliberately leaving port 113 closed so that, if a SYN packet comes to it on port 113, rather than dropping it and sending nothing back, thus being stealthed, it'll at least send back a reset ACK saying, I'm here, but this port is closed. And that will cause any of those types of servers to say, to immediately say okay, no server running there, but at least we can move on. And the last thing I want to point out is that Bert talks about firing up his Windows 98 machine, which is behind a router, then using ShieldsUP to test that machine.

Leo: He's not testing that machine.

Steve: Exactly. He's testing the router. It's important to remember that his little LAN will be on a private network. It'll be 192.168.0.whatever, or .1.whatever. It'll be using the private network space. So he's testing – any remote access is testing the IP of his public-facing connection to his ISP, which is his routers. So he's actually testing his router, not Windows 98. And just so Bert knows, behind a router you can do filesharing, you can pretty much do sharing printers and so forth without any concern because the router is working as a very good hardware firewall.

Leo: And you might want to look at your router and turn – if you don't ever use IDENT, turn off that IDENT, stealth it; right?

Steve: Yes, you are often able to configure that and shut that down.

Leo: Most routers do that now.

Steve: And most people do that now, too, yes.

Leo: More TOR. Jim in Victoria, BC wonders: Would using TOR's anonymity and encrypted connection protect you on an open Wi-Fi network?

Steve: Well, that's an interesting question because the problem with open Wi-Fi, and this is something I wanted to reiterate, is that there are two problems, and they're very different. There is the problem of someone monitoring your traffic, which is the one we generally focus on. And so any time you are using an encrypted connection, that aspect will be safe.

The other problem, though, is your computer is probably – it may be behind its own firewall.

Hopefully it's behind its own firewall, running in the laptop. Certainly I would hope all Security Now! listeners know that in any scenario they need to have their local software firewall running, and that a lot of security is coming from that. So but if they did not have a local firewall running, then in an open Wi-Fi environment their machine is completely exposed. It would exactly be like allowing someone to just come along and plug a network into their computer and have access to their computer. Generally lots of ports are still open behind someone's personal firewall. And we're now trusting the firewall to keep us safe, or we're trusting our NAT routers. Many people will take a laptop from behind a NAT router out into a public Wi-Fi and have a problem if they're not running security locally on that laptop.

So I just wanted to make the point that it's not just the traffic which needs to be secured, but the actual presence of the machine. It's on the wireless LAN with everybody else. And this has been a source of continuing security problems for Windows and other OSes in the past.

Leo: So to make it clear, TOR does anonymity, not encryption.

Steve: Correct. And I address that actually in the next question, which is why I wasn't trying to go any further with Jim's question.

Leo: Well, then let's go to Vaylor Trucks of Lawrenceville, Georgia. He says: Why not use TOR instead of VPN in a hotspot? I just listened to Episode 70 in which TOR and Freenet were discussed. In discussing how TOR worked as a TCP-level redirector, which uses multilevel encryption – he said that well in a very terse form – it occurred to me that turning on TOR might serve as an alternative to using a VPN connection when using a public Internet hotspot. Aside from the issue of performance, is there any reason why I shouldn't use TOR for encrypting data going over the first hop?

Steve: I need to determine for sure, Leo, whether running a TOR client does provide encryption between you and the first onion router.

Leo: And that's what you care about, by the way, with an open Wi-Fi hotspot is you want to – you can't be encrypted the whole way because once you get to where you're going it has to be open. But you want to encrypt it at least while it's in the Wi-Fi.

Steve: Exactly. And, now, many people asked this question. So I will have an answer by the time we are next speaking for our next Security Now! And it's very clever because you could imagine using a single onion router on TOR.

Leo: Right. Then it wouldn't be so slow. It would be fast.

Steve: Exactly. It wouldn't be so slow if you're not frantic about anonymity – as most of us generally are not because we don't normally have it in the sense of what TOR provides. If you're not frantic, you could use a single hop, a single-node TOR onion router, just to use encryption to it and take advantage of it, much like any of these publicly available proxies. But, you know, here's the whole TOR network. So exactly as you say, Leo, you wouldn't have a slowdown of an extensive multi-hop TOR network. If it encrypts that first hop from the client to the router, then it really would be an interesting alternative.

Now, there's one caveat, and this is something that I did not mention two weeks ago when we talked about TOR. But it's a glitch in the issue, well, not really of anonymity, but of privacy. And

that is, the only thing the TOR network handles is TCP. I did mention that before, that is, that it's a generally TCP transport. But it doesn't handle UDP, and DNS uses UDP. Which means somebody listening to you, someone watching your traffic while you were using TOR, would still see the DNS queries your system was making. They would know what IPs your system was looking up and, obviously by inference, where you were going.

Leo: Well, that's why you use Proxify.

Steve: Exactly. You want to encrypt and proxy all of your data until it gets away from your computer and outside of your computer.

Leo: And most TOR installations, when you read the docs, they say install Proxify for this kind of protection.

Steve: Exactly.

Leo: Very interesting. We'll have to find out – I'm looking at the TOR, its documentation. It's not clear. But you will be able to figure it out.

Steve: I'm going to figure it out, and I'll have a definitive answer for everyone. Because if it turns out that that works, and you could use a single onion router as a free and always available VPN, that would be a really great solution.

Leo: Yeah. And I can't see any reason why they wouldn't encrypt that first leg unless it's overhead that they don't want.

Steve: As far as I know, they use SOX Proxy. And SOX is not encrypted by default. So need to find out about that.

Leo: Joe Campana of Ontario, California was wondering about the three- or four-digit security codes on credit cards. This always drives me crazy, too. I'm glad you asked, Joe. I know I'm a bit late for the holiday shopping season, but I was hoping you might take a moment to talk about the three- or four-digit security numbers on our MasterCard, Vista, and American Express cards. They're still very misunderstood by most consumers, and a potential major security concern. Why are they there? How do they provide an extra layer of protection against fraud?

Steve: Well, it's interesting. I actually learned more than I expected to because as you know, Leo, and as I think I may have mentioned, I wrote – from scratch, in Assembly language – my own ecommerce system for GRC a year or two before getting SpinRite 6 ready to go. I didn't want to buy anything off the shelf. I didn't trust anybody else. Nobody else, you know, there were constant security problems in people's shopping carts. My model for GRC wasn't a shopping cart model. I don't have a hundred things people can buy. I have a hundred things people can download, but only one thing people can buy. So it just didn't make any sense to me. I wanted it to work exactly the way I wanted it to, so I wanted to write my own.

What I learned is that, by law, any credit card has to have a phone number on the back that a consumer – this is like consumer protection law – that a consumer can use to call the issuing

company for help, and that it's called the CSC, the Card Security Code. It's also called a CVV or a CVV2 within the industry. And the idea is that that is a security number which has a couple special characteristics. It never is written on the mag stripe, and it is never embossed on the card. So it will never be picked up by the old-style credit card embossing deals where they stick your card in the machine with carbons and run the roller over it. And it will never be picked up by a card swipe technology.

Leo: So the theory is you have to have physical access to the card to know that number.

Steve: Yes. And it turns out that some people, sometimes that number is written in the signature area, which is a coded area of the card that can become scratched off over time, so you can lose that number. And the reason I mention the phone number is that you're always able, given that you can prove your identity to the person on the other end of the line, you're always able to get them to tell you what your code is. And it's better not to record it on the card. It's better to move that number further from the card, maybe to a secret corner of your wallet where you keep the card, just so that the two don't go hand in hand. So essentially it is another level of authentication. Also by agreement, that code, even if provided, is never – it never appears in receipts, it never appears on printed receipts, and it is never stored in a database. So essentially it is, as you said, Leo, it is a completely separate, external, non-associated token that allows something – it's like some additional level of authentication.

Leo: I have to say, though, the security card system is grossly insecure.

Steve: It's not very long. But they realized – but basically it's sort of like an ATM PIN. It's like a PIN that goes with your credit card.

Leo: But just credit, you know, credit cards get stolen all the time. You give out that number, if you buy something they'll ask you for that CSC number. And so you're giving it out, I mean, it's just grossly insecure, the whole credit card system is. And I guess until we get smartcards and bioidentification, it's probably going to stay that way.

Steve: Well, and of course this is the result of the fact that credit cards predated online commerce. But even then, remember, as we've talked before, you're handing your credit card to an anonymous server in a restaurant.

Leo: And there's no association of that card with you, really.

Steve: Right.

Leo: And I think that's the problem, there's no – but I'm sure we'll come up with better ways someday. There's not enough fraud, or the fraud is – as a user you don't mind because you're protected, if you keep an eye on things.

An appropriately anonymous sender located somewhere in Southeast England asks about TOR: Sounds like TOR is quite a sophisticated system, but there are still a few questions. You said there's no need to trust any of the routers in the chain, but what about the last router? It removes the last layer of encryption from the data packet and sends it on to the server. So if one is corrupted, say owned by the NSA, can the originating IP address also

be extracted? I mean, there must be some way for those routers to know where to send the reply; right? And isn't there some way to find out where the packet's coming from by intercepting the clear text between the last router and the server? Or just by owning the server?

Steve: He asks a bunch of questions, and we sort of have already covered this and touched on it earlier in this single episode. But I'll just answer his question because it does amplify what we said. If the last router were compromised, as he said it's receiving unencrypted data both coming out of the router bound toward where you're sending your traffic, and unencrypted coming back. Then it encrypts it. Well, the IP that it's coming back to is its own, and that identifies the channel that has been set up through the onions. So it is not the case that even a compromised last router is able to have any idea where the traffic is going. It absolutely knows nothing about it. It knows how to encrypt it and which next onion router to send it to. That's all it knows. So it does see the clear text. It is able to watch what you're doing. But remember, and you've amplified this point several times, Leo, TOR is not about security and privacy, it's about anonymity. And so it's important that, I mean, and this question brings up the point that the last router is seeing anonymous people's traffic coming in and out of it. It doesn't know who they are. So...

Leo: But if it's not encrypted, they could read it.

Steve: They can read it. And as I mentioned before, there are some hacks that could be performed against an unwitting user. For example, that router returning web pages could alter the web pages, if it were malicious, and inject some JavaScript which would follow the web page back, router by router by router, to the user's browser. If the user's browser is running scripting by default, then it's going to run that JavaScript and do whatever that malicious person told it to. Now, it's worth noting, though, that any web server can do the same thing. So it's not like this is a particular vulnerability of the onion routing system. It's if you've got scripting enabled by default, which smart people don't, then you're safe against that kind of problem.

Leo: There's a lot of information on the TOR wiki on using things like the Firefox NoScript extension to prevent that whole...

Steve: Exactly. But to answer his question, isn't there some way that the router knows who you are? And the answer is, unless you tell it, by scripting or a cookie or something, no. There is no way. Because all it knows is the next hop. And this system is now active enough, there are so many routers, there's just a blizzard of traffic – more so, actually, after we talked about it two weeks ago – a blizzard of traffic flying among these routers. There's just no way to know where it's going.

Leo: All right. Last question. Fred Barlow of Atlanta, Georgia had an interesting question about cryptography: If I generate public and private keys, and someone else generates the exact same – there's your problem right there – public and private key with messages encrypted with the public key, one, will they be able to be decrypted by the private key; and, two, vice versa?

Steve: Yup.

Leo: Yeah. But that's never going to happen.

Steve: Exactly. As we know from our episodes on crypto, because of their nature, public keys, that is to say, asymmetric keys where you have a matching pair of public and private key, they are very long. They are 1K, 2K, 4K in even more modern cases. They are generally extremely long; 2 to the 1,024 is how many different possible 1KB keys there are. Well, it's just an astronomically large number. I can't even do some quick math to give people an idea. I mean, that is just – the chance of it happening is so small that you absolutely don't need to worry about it. And there's just no way you could guess it because there are too many guesses. So even if two random people on the planet, both happen to have randomly chosen the same key, they would never know it. So the chance of one of them trying to decrypt something the other had encrypted, well, that's vanishingly small, too. These things are so large...

Leo: Don't worry.

Steve: Possibility is so low.

Leo: Don't worry. Calm down. It's okay.

Hey, a great set of 12 questions, Steve. And you've done a great job explaining them all. I do want to thank our friends at Dell for sponsoring this podcast. I do think this is the last one. I don't think they run into 2007.

Steve: Leo, I have to interrupt you for one second. I just picked up my calculator because I was curious. I tried to raise 2 to the 1,024 power using my HP11C...

Leo: It won't do it, will it.

Steve: No. 9.99999 to the 99th. Which means it just overflowed and blew the calculator's mind. So...

Leo: It's a number larger than the number of molecules in the universe. I think you're okay. We're more likely to have a positron electron explosion.

Steve, Dell is, of course, the sponsor of this podcast, their last time on the show, and we want to thank them so much for a great quarter of ads. Your last chance to get a great deal on a Dell through the TWiT.tv/dell page, the Leo's Pick Page, some great computers there. But anything you click and then buy later, anything you buy on the Dell site, if you go through that link in other words, will count towards us. And we do appreciate that, and we do appreciate Dell's support. I've always been a Dell fan. It was just a real thrill for me to kind of get Michael Dell behind us and say, hey, we believe in what you're doing on TWiT, and we want to help you out.

Steve: It's been a good year with Dell.

Leo: It has, it really has. Also a good year that will continue with Astaro. They've decided

to sign up, they're re-upping, our first sponsor. And I think they'll probably be with us as long as we're around. Astaro makes the Astaro Security Gateway. If you're in a small or medium business, and you're looking for kind of an all-in-one solution that does everything, I mean, superior protection from spam, from viruses, it's got hacker protection and complete VPN capabilities, intrusion detection, content filtering, and an industrial-strength firewall, and it's all in one simple, easy-to-use appliance, not very big, about as big as a router, but it does it all. You can get one in your business free for a trial. Contact Astaro, Astaro.com, or call 877-4AS-TARO. A free trial of the Astaro Gateway Appliance. And if you're a non-business user, you could download the Astaro version free at Astaro.com, install it on a PC, and get great protection. In fact, for a very low subscription price you can even get all of the additional features added in and automatically updated. It's really kind of a neat idea. More people should try that. Astaro.com.

For more information about this subject, and 16KB versions of the show for the bandwidth-impaired, and transcripts, too, if you like to read along while Steve's talking, go to GRC.com. It's the home of Security Now!, of SpinRite, Steve's incredible disk maintenance utility, and of course all those great free programs. SecurAble will be out very soon, and a ton of other ones that are a must-have. And let's not forget ShieldsUP, which is still, I mean, how many people have used ShieldsUP now so far? It's a huge number.

Steve: I think we're approaching 47 million.

Leo: That's outrageous. That's great.

Steve: It's wonderful.

Leo: Steve, have a very happy New Year. We will see you in 2007, one week hence.

Steve: '07, amazing.

Leo: Amazing. This has been such a successful podcast, entering now our third year of securing you, your friends and family. Since 2004...