Listener Feedback Q&A #47

Description: Steve and Leo discuss the week's major security events and discuss questions and comments from listeners of 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 we have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-156.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-156-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 156 for August 7, 2008: Listener Feedback #47. This show is brought to you by listeners like you and your contributions. We couldn't do it without you. Thanks so much.

It's time for Security Now!, everybody's favorite show about protecting yourself online with our security guru, Mr. Steve Gibson from Irvine, California. Shaky Irvine, California.

Steve Gibson: Well, yes. The earth is not moving at the moment. So that's a good thing.

Leo: It was, you know, I was watching you on video. We didn't have the ability to broadcast the video because of some technical issues last week. And you were shaking around pretty darn good. I mean, it looked like the Starship Enterprise when they hit an asteroid belt.

Steve: It was serious. In California, especially Southern California, we're sort of accommodated to earthquakes. It's not such a big deal. I know that I've talked to people sometimes - we haven't had a lot of earthquakes for a long time, too. But I'll talk to somebody who's, like, from the Midwest, where the ground is a lot more stable. And they

just...

Leo: It freaks them out.

Steve: They experience, yeah, exactly, they experience one, they're like, okay, I'm moving home. This is wrong.

Leo: But we don't have tornadoes, hurricanes. You know, there's always something. And Mother Nature never lets you get scot-free. And those of us who live in California and have been through a few of them, we're just, you know, it's just - you were very - I was so impressed. In fact, that's why I left it in the show instead of editing it out because, you know, oh, we're having an earthquake. You rode it out and said, okay, let's get going. You didn't pause a beat. It's very impressive.

Steve: Ah, well, been through a few.

Leo: We've got a Q&A show. And it was apparently - they called it a moderate quake. It was 5.8, but it wasn't...

Steve: Well, the thing that was the saving grace, apparently, is that it was a much deeper quake than normal. It was five-plus miles down instead of being up near the surface. And if it was near the surface, even that size a quake on the Richter scale would have been a serious event. But being down that deep it smoothed it out a lot so it wasn't as sharp as it would have been had it been much nearer to the surface. So that's a good thing.

Leo: Yeah, thank goodness, yeah. And as you pointed out last week, it's great to release that tension.

Steve: Got to have a tension release every so often.

Leo: Every once in a while, as we all know.

Steve: Keep us all sane.

Leo: We're going to do a Q&A session. We've got some great questions from listeners around the world, as usual. Any news in the tech - there was a big security flaw, wasn't there, Steve.

Steve: Yeah. The big - it's been a relatively calm week, thank goodness, because this DNS problem that we discussed in detail last week has really been causing problems. There are still a large number, as of this day - we're recording this on the first day of August. More than half of the servers being tested by the various testing facilities are

turning up still vulnerable. And...

Leo: Wow. More than half?

Steve: More than half. A little - it's 53, I think, 53 percent was what I was seeing.

Leo: That doesn't seem right. Holy cow.

Steve: Well, and what's going to happen is the problem is there are just so many DNS servers. And there are arguably some that are - they're not going to be big targets, but they're important targets. And so I think we're going to see the major ISPs will be under so much pressure to fix this that they're just - they're going to have to do it. But there's been a lot of reluctance shown. It's like, oh, well, do we really have to do this? And the good news is that consumers who are able to see that the DNS they're using can be too easily spoofed are really raising a ruckus. On last week's show notes, that is, the show notes for Episode 155, I've got three links now to three testing facilities that are available. And I'm working on my own. By the time we record our next episode I imagine GRC's DNS spoofing tester will be online.

Leo: Oh, neat.

Steve: It'll be another facility, very much like ShieldsUP!. I'm going to do a whole bunch of really cool stuff that nobody else is doing. So I'll be certainly telling our listeners about that as soon as it's online. And I just figure this is a big problem. DNS spoofing is a problem. This has raised sort of the - it's put back in play the whole problem of spoofing. As we know, these problems have been there for a long time but just haven't been given much attention. So this focuses the attention.

And one of the problems that people are discovering is that NAT routers, which so many DNS servers are behind, are derandomizing their random ports. So even when you apply the DNS patch, if you're behind some sort of network appliance which is not allowing the random outgoing port assignment to survive NAT translation, you lose the randomness. So that's creating some new opportunities. So it's turning out to be a problem. But what I wanted to tell people was if anybody is using the RealPlayer, any RealPlayer version prior to 11, some serious security vulnerabilities have recently been addressed and discovered in earlier versions. So absolutely make sure that you update your RealPlayer to version 11. That's really the only new news of the week. Also an interesting issue with DNS spoofing relative to testing sites arose because people realized, wait a minute, if sites can be spoofed, and my DNS server can be spoofed, then how do I know that I'm going to a real DNS testing site through...

Leo: Oh, that's a good question.

Steve: ...through my spoofed DNS?

Leo: Right.

Steve: Because one of the first things you would expect bad guys to do, or something they could certainly do, would be to set up a fake testing site to say, oh, don't worry, your DNS is...

Leo: No problem.

Steve: No problem. Your DNS is fine.

Leo: It's working great. You're safe. You're fine. Don't worry.

Steve: And the point is, I mean, it's a perfect example of a real security issue because if your DNS has been spoofed, then you can't trust the lookup. And if you can't trust the lookup, and you're using a domain name to get to the testing site, then you don't know that you've really done that. So there is an IP address for the OARC site. The IP address is 149 - actually they made this URL easy to access. It's just the IP address 149.20.3.33/test.

Leo: So if you use the SnipURL, for instance, if you used any English language domain name, that could be spoofed. But if you enter in the IP address directly...

Steve: Then nothing in your system is going to your DNS server. It's directly connecting to that IP address.

Leo: The browser says I don't need an IP address. You just gave me one. Fine. In fact, that's a fast way to go to any site, if you know the address. But the problem is that's why they did this thing because nobody remembers those dotted quads.

Steve: Right. And in fact what I'm going to do is I'm going to take people back to a dotted quad when they come to GRC.com, if they're going to run the test, just to sort of - so that if they copy the link and share the link, if they write it down, if they make a shortcut, it'll automatically be giving them the IP address just as an extra level of confidence that they're able to know that they're really at GRC. And I'm going to run it over a secure connection. So again, they'll have that, as well.

Leo: So having that certificate really also gives you some reassurance. But you can't...

Steve: I can't use the certificate with the IP address, though. So it's going to have to be one or the other because the certificate is the domain name. And the domain name wouldn't be in the browser, it'd be the IP address. And who knows what random firewall, I mean, ZoneAlarm has gone so hyperreactive now, it might block you from using an IP

address. I mean, they've just really gone overboard. So but it'll be available, and it'll be a suggestion for somebody who wants to absolutely know they're actually talking to GRC, and they haven't been spoofed.

Leo: I noticed when I enter the IP address that it does resolve to a name. So maybe the certificate would work at that point.

Steve: Ah, so in their case they're, yes, so they're seeing it come in. And also is it an HTTPS? Because I think OARC is running over SSL.

Leo: It's not actually. It's just an HTTP. And then you get a very long, what looks like a hash number, followed by et.dns-oarc.net. So I don't know what they're doing there. Maybe that hash is of some security significance.

Steve: Well, I just figured that, since DNS spoofing is an issue - I delayed getting involved in doing my own for a while. I mean, I'm deep in the middle of dealing - of wrapping up this third-party cookie thing. But it's like, well, it would just be good to always have it there. And who knows, someone, an ISP might fall back and regress and stop port randomization, and no one would know it. So one of the things that GRC is doing, I'm becoming a little proactive about this. I'll be testing DNS spoofability all the time for everyone who comes and notifying anybody if their DNS server...

Leo: Oh, that's nice.

Steve: Yeah. So it'll just be happening in the background and transparent. And I'll be doing the same thing with third-party cookies, just to let people know, yup, they're still turned off. So...

Leo: It's funny, it tests - apparently because I'm using OpenDNS I have, you know, my DNS goes through OpenDNS. But it could still see that I'm on Comcast. So it tests my Comcast DNS servers as well as my OpenDNS servers. OpenDNS, great. Comcast still poor in the source port randomness. But the transaction ID randomness is great. What does that mean?

Steve: Well, so with source port randomness, it says "poor," I'm really - I'm a little annoyed with that test because you can't get a worse rating than poor, even if all the queries come from a static port. It ought to say "horrible" if you've got it all coming from one port. So how many different ports did it come from in that test?

Leo: Unique ports 24.

Steve: Okay.

Leo: And the range, let's see, number of samples, 25; unique ports, 24. They're not sequential. The scatter plot looks pretty random. So I'm not sure exactly what they're seeing here.

Steve: Right. And so it'll also show you how many bits of entropy is available.

Leo: Bits of randomness only 10, and maybe that's why it's saying "poor."

Steve: Yeah, that's definitely why. And so it sounds like something is going on. And this may be - this is a perfect example of what a lot of ISPs are still putting out is they're not super random ports. They're within a restricted range. And that's generally indicative of some sort of post-DNS server processing that's limiting the randomness of the outgoing port. And who knows how...

Leo: And they're doing some sort of weird stuff in there in addition to the DNS?

Steve: Probably, yes.

Leo: Yeah, okay.

Steve: Yeah, because if they - I mean, if they had applied the full patch, they would be generating ports over the entire 65536 or 65535 port range.

Leo: Oh, I see. It's definitely not. It's 16916 through 17815.

Steve: Right. So it's within a restricted range. And of course what that means is an attacker can see what range you're currently generating. And while it's not as easy as if you had a static port, it certainly restricts the guessing and hugely improves their opportunity for penetration.

Leo: Yeah, well, that's too bad. Nice try, Comcast.

Steve: Yeah. Well, again, we need their customers to know what's going on in order to put pressure on them to get this fixed. I also mentioned last week that I believed that the DD-WRT version of firmware was vulnerable, and it's confirmed it is, and there is a patch. So I wanted to let anybody who has been, like, flashing their routers and is running DD-WRT, I'm sure if that someone, you know who you are, that there is an update to solve this problem for individual end-user routers. Again, I don't think it's a huge issue because I would be surprised if end users would be targets. It makes much more sense to attack an ISP and thereby spoof everybody who uses that ISP's DNS server. But there are certainly - you could imagine situations where this kind of tool becomes readily available, where individuals could get targeted when they upset somebody in a blog or in an online forum or something.

Leo: Yeah, yeah.

Steve: We've seen lots of little, in the past, DoS attacks on individuals. So you could certainly imagine individualized spoofing attacks aimed at just a single person for one particular reason.

Leo: You know what's a real problem is IRC chat because it's pretty easy to figure out what somebody's IP address is in IRC.

Steve: Right.

Leo: That's usually published. And of course that's where people get in flame wars all the time. And it's where all the script kiddies hang out. So it's really kind of a perfect storm of evilness.

Hey, I want to read a poem that you sent me that is just really cute. Well, I don't know if you can hear it, Steve. The lawn blower brigade has decided to camp outside my window. I hope that's not bugging you.

Steve: No, it's quiet at this end.

Leo: They show up at this hour of the morning every morning. Or not every morning, every week. And they stand outside my window. And I think they do a little kind of precision routine. They march in and out. Oh, it's just amazing. However, a little noisy. So I just want to warn you. But let me read this. This is from a blog called Rational Survivability, a guy named Hoff.

Steve: He did a really good job with this.

Leo: Christofer Hoff wrote this. It's called "The DNS Debacle in Poetic Review." I'm going to put on my Orson Welles voice for this one:

"A few months ago

Kaminsky discovered a flaw.

It was with DNS,

It was nasty and raw"

Actually maybe I should have used the Dr. Seuss voice here. Now can you hear them? Here they come.

Steve: Now I - there they come.

Leo: I apologize.

Steve: We'll just cover it up with the poem.

Leo: I'll talk really loudly.

"He decided than rather

to disclose all at once

he'd instead only tell people

who'd fix it in months

So some meetings were had

and work soon began

vendors wrote patches

coordinated by Dan

Fast forward some time

out the closet it came

some researcher types

got into the game

Dan's rules were quite simple,

that in 30 days

he'd present during Blackhat

and we'll all be amazed

A bunch of big egos

called Dan on a bluff

said his vuln was a copy

of 10 year old stuff

So Dan swore them on handshakes

and details were provided

and those same cocky claims

soon all but subsided

It seems that Dan's warnings

weren't baseless at all

Said the same skeptical hackers

'the risk isn't that small!'

So Blackhat was nearing

the web didn't break

then out came a theory

from our friend Halvar Flake

No sooner had he posted

and described the vuln's guts

than Matasano's blog surfaced,

kicked the web in the nuts

It said 'Halvar's right!'

we'll no longer keep quiet.

The post's ripple effect

caused a nasty 'net riot

The blog quickly was pulled

but the cat's out of the bag

the arms race began

since there's no longer a gag

Meanwhile the issues

of honor and trust

rehashed the debate

of when disclosure goes bust

So Dan's days of thirty

we never did see

thirteen is OK

but I issue this plea

When researchers consider

how to disclose and thus when

will you think of the users?

How it might affect them?

This ego-fueled rush

to put your name on a vuln

has a much bigger impact

than you might have known

If the point here is really

to secure and protect

then consider what image

you really project

In this case the vuln.

is now in the wild

an exploit is coming

DNS soon defiled

The arms race has started

and the clock now is ticking

If you haven't yet patched

you'll soon take a licking

I'm not taking sides really

on the disclosure debate

but rather the topic

of patch early or late

What good is disclosure

if the world couldn't cope

with the resultant attacks

if we've all got just hope?

There's two sides to this issue

both deserve merit

but Dan's rep has been smeared

I say let's just clear it"

That's Christofer Hoff. What a great poem.

Steve: Isn't that perfect? This is wonderful.

Leo: And so is vuln, v-u-l-n, obviously short for vulnerability, I guess that must be what researchers use. Don't want to waste a syllable. Not if you can help it. Wow, that's great. Well, we'll put a link to that. That's from rationalsecurity.typepad.com. That's his blog, Rational Security, or Rational Survivability, he calls it. Actually he says it used to be called Rational Security, but security's dead, don't you know.

Steve: Right, right.

Leo: That's great.

Steve: So one other little issue, a twitch has arisen during all these patches. It turns out that the first round

of updates to DNS is causing an undisclosed performance problem on DNS machines. Paul Vixie, who's still very involved in the 'Net and DNS, has written formally acknowledging that there is a known problem with the first change. But his recommendation was, look, do not back out to the vulnerable DNS. We're going to fix the

performance problem next. But we had to get the main problem fixed first.

So that makes me think that a little something more is going on than we know so far because just outbound port randomization, unless their algorithm for doing that is somehow funky, I mean, I guess I could imagine if you were on a single port, lots of things are easier than continually allocating new outbound, setting up new outbound ports with sockets and sending packets out and getting them back and coordinating it all. So they might just have a rather first-pass implementation of DNS query source port randomization, and they're going to work on improving the performance hit. And this is only in really, really, really busy servers. I mean, those servers that are doing, like, on the order of 10,000 queries per second are, like, they're having more trouble than they were before this change. And so a lot of admins are saying, wait a minute, this is really hurting our DNS performance. And so - and Paul says, look, he implores them, keep the new patch in place, we'll get you another one soon that fixes this performance overhead.

Leo: Is it just the overhead of calculating the random numbers, or generating the random numbers?

Steve: It's - without looking...

Leo: That shouldn't take much time.

Steve: No, no. It wouldn't be random number generator. That's instantaneous these days. But it may be just, who knows what the algorithms are, what kind of data structures they had and what they now have. Certainly over a long period of time the performance of DNS has been tuned. If it had been highly tuned and optimized for one particular strategy, like a fixed port, then you could imagine that suddenly changing that to random ports will require a bunch new code. Well, that bunch new code hasn't had a great deal of time to be hand-tuned and optimized to bring its performance back up to where years of performance tuning had honed the prior approach.

Leo: That makes sense, yeah. It's just new code. It's not been optimized well.

Steve: I would guess that's what's going on.

Leo: Yeah, that makes a lot of sense.

Steve: In something completely off topic, except it's a topic near and dear to our hearts, I watched the new, recently released, like two days ago, "Stargate" direct-to-DVD movie "Continuum" last night.

Leo: And?

Steve: I loved it.

Leo: Oh, I'll have to get it.

Steve: I have to say I'm a "Stargate" fan, boy. I loved "Stargate." I watched all 10 seasons of "SG-1." I'm now in the middle of, what are we, fourth season or fifth season of "Atlantis." I mean, I'm craving sci-fi. And so "Stargate" is, you know, it's generally a fun source. But this was a - it was a time travel theme movie. I love time travel sci-fi. And this was really well done. We didn't get to see as much of Jack O'Neil as I was hoping we were going to. But he did show up for a couple little cameos. But it was a great movie. So I just wanted to tell our sci-fi enthusiast listeners that I recommend "Stargate: Continuum," the recently released DVD, which is a two-hour "Stargate" movie. I recommend it without reservation.

Leo: I've never seen "Stargate."

Steve: Well, Leo, then you're just - it's too...

Leo: You're stunned.

Steve: Too late for you. It's too late.

Leo: No, can I go back and watch the year - this is exciting to me. I now have 10 seasons to watch.

Steve: Oh, and, I mean, it's really good. I don't really mean to get off on a whole "Stargate" rant. But it is, it's very clever because they built a complete mythology. The writers really cared about it. It's a huge story arc. There's lots of neat bad guys. The concept of the stargate is wonderful, that stargates are wormhole anchors. And so they're able to establish wormholes between paired gates. And they do all kinds of neat things. I mean, they really keep within the mythology. So it's possible, as happened for example in "Star Trek," where we end up knowing how fast the food recyclers work and all kinds of mundane trivia, I mean, it's one reason you just can't watch this movie. This movie wouldn't mean anything to you without understanding who all the people were and remembering past episodes and all that.

So for a "Stargate" person, this is a spectacular movie. But I recommend the series without reservation. It went through a little kind of a rough spot maybe halfway through. There was, like, maybe one or two, or maybe a half of a bad season. But overall, I mean, it's just spectacular. So, I mean, "Stargate" is great.

Leo: Well, as you can hear in the background, the marching brigade is marching on. But...

Steve: Well, turn off your mic, and I will tell us - I'll read a SpinRite story.

Leo: Would you do that? I'm just going to - I'm going to cut my mic because this is ridiculous. They're literally, like, they're out - I don't know why they're blowing right out my window. Apparently there's a few extra leaves there. I don't know what's going on.

Steve: Okay. So this is from Jarvis Weezy, who sent us a note on - it's dated July 30th, so just a few days ago. Now, the subject threw me off because the subject was "713 Days, 20 Hours, 25 Minutes, and 23 Seconds/SpinRite Success." And I'm thinking, oh, my goodness, is that how long it took? Was he running SpinRite for 713 days? The good news is no. I guess he was - just put that in there to get my attention. So he starts his note by saying, "8/15/2006 was the last day I actually turned on the computer with this drive in it. It was running XP MCE 2005," which is Media Center Edition 2005. And he says, parens, "(It had a disk I/O error in the system event log and was now completely dead.)"

Then in his next paragraph, "7/29/2008 was the day SpinRite allowed me to boot this 500GB SATA drive that hasn't been used in two years." He says, "Usually I listen to a TechNet session, but one day last week I clicked over to Security Now! on my iPod podcasts. I listen most during my commute to work on BART." So I guess he's in Northern California. "So I've been trying to catch up on the content that's available and keep hearing about SpinRite. Now, me being from the old school, I was very skeptical of software fixing hardware problems. So when it came to my drive I was curious and started Googling SpinRite. Originally I caused the damage by not securing the drive on those green rails Dell has because I had quite a few drives occupying them, and I happened to move the computer while it was on and heard a bang as the drive moved to the front of the case and remembered I had not yet got the rails on that drive.

"So sure enough, the drive made that horrible clicking sound, and Hitachi Diag said the drive was toast. Note that I didn't have some of my stuff backed up. Some of it was, but a lot of it wasn't. When this drive was purchased two years ago it was a little more expensive than the $99 they go for now. So I switched back to the original Dell drive and moved to Vista eventually. I intended to save my money until I had enough to send the drive off to one of those recovery places. But after hearing of the three-month recovery stories and the drive that took flight from the second story, I somewhat skeptically decided to give SpinRite a try.

"So I started SpinRite this morning, and off to work I went. I came back to find the green "complete" screen. Apparently it had finished around lunch or so, as the last partition was around 11:30. So I expected to have some access to the drive. But I did not expect every sector to be recovered. Every sector SpinRite found a problem on, it recovered. Not only was I able to recover data, but this thing now boots. I am now able to access music I forgot I had. I'm able to now access videos that I forgot I had, DVD compilations for 'Def Poetry Jam.' Now, as MCE tries to do god knows how many updates and virus programs ask for renewal, I am looking at all these programs I legally bought as a student that haven't been used since I went off to Vista. And to think I was waiting all this time to save money to send the drive off to a data recovery service, when instead I paid $89 for SpinRite. Priceless. And you know, I sent a text message to my best tech friend, and he said I should have just asked him because he would have told me about SpinRite right off the bat. I am a believer. Jarvis, MCSE, MCSA, MCP, Security+."

Leo: Holy cow. He's got the certs. That's great. Hey, we got some Q&A for you. Are

you ready?

Steve: Let's do it.

Leo: You got your beanie on, your thinking cap? These are questions from Security Now! listeners. You can just go to Security Now! - I'm sorry, GRC.com/securitynow, and you can ask your questions there. Starting with Sunnz in Canberra, Australia, with an interesting password question. He says: Hello, Steve. I read about and saw your Perfect Password Page, and think it's great for things like WPA. However, for less than important things, say my Facebook account password, do you think it would suffice simply to use a sentence? For instance, "My dog is 12 years old and he runs very fast!" Perhaps with no spaces in between? Most sites don't seem to like spaces in passwords. It does contain upper and lower case, number, and symbols. And of course it's easy to remember. I imagine this is not prone to brute force attack, thanks to its length, and whole sentences aren't available in a dictionary. The advantage, of course, is that a sentence is easier to remember than something random. One step further would be to make an intentional unique grammatical mistake that only you know of, or a spelling mistake, or both. I guess that would prevent rainbow table attacks, if an attacker were to generate sentences and use that for brute force. What do you think?

Steve: Well, I think it's an interesting question.

Leo: Actually I do the same thing. I mean, I use - in fact, for my PGP password I use a phrase.

Steve: There are two things. First of all, the fact that it's easier to remember is a bit of a warning sign. I mean, if it's easy to remember, then that means something is weaker from some angle.

Leo: It's not totally random, which is the best.

Steve: Well, and, for example, if anyone glanced at it, they could quickly acquire it. That is, if they saw it written down, if they maybe even, like, watched you typing it and caught most of the letters, they could fill in the gaps just using semantics and grammar. So it's certainly, I mean, I like the approach. I think it's very strong in general. Obviously the longer the sentence, the better. There are so many words that could be combined in so many ways, so many possible sentences, that sure, it's not as strong as something from GRC's Perfect Passwords Page, but it's certainly better than a short phrase, which just doesn't contain enough entropy. A long sentence is going to have a lot of entropy in it. Not as much as random characters at the same length, but still a lot. I would just note that other humans could acquire it if they had any exposure to it much more quickly than they could something that was random that they had no experience or no - nothing that they could quickly map it onto.

Leo: All right. Yeah, because I use that. I figure...

Steve: Yeah, it's good.

Leo: Yeah. I mean, you could, I guess, do a brute-force attack. But it would be very difficult because there's different - there are so many words. And there's punctuation.

Steve: Well, and the other thing is, who's going to know that this is what you're doing? Any useful system is going to turn whatever you put in into a hash. Hopefully it's not storing your ASCII and comparing it because that's the worst thing that a system can do. The right thing, as we know, in security is to immediately hash that into a fixed-length token, which is also easier for databases to handle because that cannot be reversed. So nobody would know that that's what your password was. They wouldn't know that it wasn't a few characters or eight. So I think it's probably a good idea.

Leo: Very good. So, good. I'm going to continue to do that. I am Sunnz in Canberra. No, no, I'm not. Aaron Feickert in North Dakota wonders how safe his private key is: Steve, you've talked several times on your netcast about PGP public key encryption. I'm wondering how secure my private key really is. I use it to encrypt all my offsite backups, and I like to carry it on a USB drive with me so it's only in one place. I'm worried about what could happen if it fell into someone's hands. The private key has a passphrase. But is there any risk of an evildoer somehow breaking my encrypted backups if they got the key? That's a great question because I don't particularly protect my private key. Should I be?

Steve: Well, I love the question. First of all, PGP has been written using state-of-the-art philosophy of security. So, for example, in the case of the PGP use of a passphrase and a public key, the passphrase is hashed and is used to encrypt the public key just using symmetric encryption so it's very fast and lightweight. So the attack on the passphrase would be guessing all possible passphrases, hashing those, and applying them to the public key, which is probably more feasible than just brute-forcing the hash. The hash is going to be long. It's going to be 160 bits. You're just not going to be able to brute force that and use that to try to decrypt the public key. So the public key is - oh, I'm sorry, I'm saying public key, and I mean private key.

Leo: Private key, right, right, right.

Steve: Yes. I was sitting here staring at the text, seeing PGP public key. Yeah. So in an asymmetric encryption system where the public key is known to everyone and is used either to encrypt something that can only be decrypted by the person with the matching private key, or is used to decrypt something which will only succeed if it was encrypted with the person's private key. In both cases the strength of the system is that it provides extremely good security and authentication because you're able to publish the public key. Everyone can see what Aaron's public key is. And they know that, if they're able to decrypt something successfully using his public key, then the only way it could have been encrypted is the use of the matching private key. Okay. What this means is that keeping

the private key secret, the unencrypted private key, the actual private key, keeping it secret is crucial.

Now, to protect the private key when it's not in use, when it's being stored, as Aaron has it on his USB drive, the private key is further encrypted using the passphrase that he was asking about. So the strength of the passphrase and the, well, keeping the private key private are both important. If you absolutely protected your private key so that it was inaccessible to anyone, then someone could argue, look, no one can get it. My key management is so good, no one can get my key. Therefore I'm not going to encrypt it. That is, I'm not going to encrypt it with a passphrase because I don't want to. And you could say, okay, fine, as long as it doesn't get loose, and you're sure your key management is that good, don't bother. On the other hand, encrypting it with a passphrase absolutely obscures it so long as the passphrase is long and is not brute-forcible. So that's the point of attack. Brute-forcing the passphrase would decrypt the private key if somebody had access to it.

So if it's on a USB drive, those are inherently moved around. We've told lots of stories about unscrupulous people saying, ooh, look, a USB drive, I wonder what he's got on it, and sucking the contents out. So if your private key is ever going to leave in any way your own really good protection, then by all means use a passphrase. And the way PGP implemented it is as good as it gets.

Leo: So I see that iTunes sells "Stargate," all the seasons. Should I just start with season one and go right through?

Steve: It's a great series, Leo. I mean, actually, I would start with the original movie.

Leo: Oh, okay.

Steve: The original movie was - did you ever see that?

Leo: No, I haven't seen - I don't even know what "Stargate" is.

Steve: Oh my god.

Leo: Is that "Stargate Atlantis"? What is that original movie? What's that?

Steve: It's just "Stargate."

Leo: "Stargate." I'll find that.

Steve: The movie was called "Stargate." It is a great, fun movie. And it was the basis for the series. They continued the mythology.

Leo: You know, they're all - I'm really pleased. They're all on iTunes, so I can put them on my iPod, yeah, make it easy. Sorry, a little digression there. Brad Pliat- let's see. Okay, let me see if I can do this. Pliatsiosis. Pliatsios. Bryan says - he's from Melbourne. He's waiting for, oh, boy, GRC VPN: G'day, Steve, I've been listening since the beginning of Security Now! and jumped on the Hamachi bandwagon with the hope to move to the OpenVPN solution you were always promising. While Hamachi was bought out and other options like Back to My Mac, GoToMyPC, GoToMeeting have come up, I'm still hoping you'll eventually get to a roll-your-own solution. Not only for the preference not to route my traffic and rely on another party, for security reasons and of course because most servers are homed in the U.S., but also to set up access to my home network through the local community wireless network where the Internet services are not suitable as it's a private network. Kind regards to both you and Leo. Eternal thanks for geeking it up.

Steve: Well, I just wanted to respond to Bryan and anybody else who feels similarly. As you'll remember, I was planning to put together an OpenVPN set of how-tos. And I've got OpenVPN working. It's certainly possible to make it work. But boy, is it a pain. And it turns out that doing it right really requires - there's so much - it's like a Swiss army knife product. It's so general and so capable that the configuration file, I mean, I remember the first time I looked at the config options. It's just like, oh my goodness, how many months is this going to take? And there were problems on earlier versions of Windows that don't allow bridging of network adapters, which you need in order to get OpenVPN working in the right way. There's problems where you get network collision ranges if your network at home is in the same range as the network where you happen to be VPNing in from. Then because it's routing table based it screws up the routing tables. I mean, as I really got down to trying to make this thing work - oh. And the other thing they don't tell you is that when you make your own SSL certificates, as you have to, using OpenSSL, all of the content of your certificates is sent in the clear. So those all want to be null fields. I mean, there's just - it got so involved that I finally said, okay, wait a minute, this is dumb. I'm just going to do one.

So I've mentioned it briefly before. It is my main project once I get finished with this DNS testing facility and once I get the cookie system launched. I'm going to be plowing into a product called CryptoLink which will be GRC's first formal commercial security product. And it's going to be sort of everything. It'll do NAT traversal, it'll be Hamachi-like, it'll be able to run in an easy-to-use mode behind NAT routers where GRC will provide the connection. Or in a Trust No One mode, I call it TNO, where you're able - you're a little bit more technical savvy, where you set up your router at home to be the server end of the link and so forth.

So anyway, I don't know when. I never know when. But it is absolutely the next thing I'm going to do, as soon as I get these other little loose ends finished up. I needed to get the menuing system online, that's done; and then get the cookie system finished, that's done. And of course we have a little pause here while I do the DNS testing system because I think that's important, too. And then CryptoLink is next.

Leo: That's exciting. I'm really glad to hear that.

Steve: And you remember that I ran through with you, Leo, confidentially, three pages of bullet points when you and I were having dinner once in Vancouver. And your mouth was hanging open.

Leo: I love the - oh, what you're - yeah. It's brilliant. It's really great.

Steve: There's a bunch of new stuff that no one's done before. So I'm excited.

Leo: And, you know, it's interesting, with all the free security stuff, you've never done a commercial security product.

Steve: No.

Leo: So I think this will be more than welcome.

Steve: I'm excited.

Leo: Yeah. Peter Chase in Columbus, Ohio has an idea to avoid using spoofable DNS: Guys, if I obtained the actual IP address for each site I visit, and incorporate them into each bookmark, wouldn't that be quicker and more secure than to go to those websites using a DNS lookup? That's what we were just talking about.

Steve: Yeah, exactly. It came up in the issue of direct IP access to the DNS testing sites. So it's interesting. I mean, he's saying, okay, what if I look up the IP addresses of these important places and put them in the bookmarks instead of the domain name? We sort of touched on this last week. First of all, that would avoid spoofing. You would be going - your browser would be connecting directly to the site. I can't say for sure that you wouldn't have some side effects. For example, there is something called multi - it's not multi-homing. I don't remember the name now, Leo, I know the technology, where a bunch of different websites all live on the same IP address?

Leo: Virtual hosting? Virtual hosting service?

Steve: Virtual hosting, yes. The idea is that when your browser makes a query it connects by IP. But one of the headers in the query is the domain name that is in the URL you're using. So some systems do not give different websites each their own IP. Instead, many websites share an IP, and they depend upon the browser including this extra information, saying, well, I know I want this IP, but this is the host that I want at that IP. Which allows multiple web domains or websites to live on a single IP. That's still rather common. It is a way of conserving IP addresses. It's generally used by hosting services who set up inexpensive websites, and you don't get your own IP. And in fact, sometimes you can pay extra from such a company if for whatever reason you really want to be on your own IP address, like for example you want to offer other services than just web because only the web has the ability to use this hosts header to disambiguate which site you're wanting to access at that IP.

So my point is it's not a universal solution, that is, to use just an IP address, because that wouldn't work at a site that had multiple domains on a single IP. On the other hand, you could try it. And if it works, it's probably going to keep working, at which point you

could build it into your bookmark. The other problem, of course, is if they change their IP, then you would not - your bookmark would break because it wouldn't automatically be using the indirection, basically an indirect pointer, that DNS also provides and that you are using something that doesn't change, meaning the name, and the IP it maps to may change. On the other hand, that's what you're wanting to avoid because it might be a malicious change in the IP that you're trying to keep from happening in your case. So I would say, if somebody's really concerned, if for some reason they don't feel comfortable or are unable to switch to a fixed DNS server like those offered by OpenDNS, then, yeah, you could use an IP address, but there are some caveats.

Leo: Very good. And very interesting, yeah. The problem of course is the trouble that you'd have to take. But I guess you'd only do it once to find all of those addresses. You could just do a ping, I guess. That's what I usually do. Is that the best way, you think, just to say "ping yahoo.com," then write down the address?

Steve: Yes, that's a very good point. I was going to say nslookup is a command that we all have in our machines.

Leo: That would work, too, yeah.

Steve: But you're right, the ping command does resolve the domain name into the IP. And then it shows you, pinging this IP, blah blah blah, and that allows you to pick up the IP address.

Leo: Somebody should write a little utility to do that because you're going to want to do it frequently because, as you point out, these things change.

Steve: Actually I have one, it's called ID Serve, and it's available on GRC.com on our freeware page.

Leo: You're kidding. That's great.

Steve: Yeah, it's a cute little, nice little GUI. You just stick the URL in. And basically the idea, it was - I originally wrote it to ID the servers so you could see what kind of server people were running back in the days when IIS, Microsoft's server, was so horribly broken and insecure. There was a threat just even using some remote system that was using IIS. So ID Serve identifies the server that some remote place is using. In the process it shows you a nice little color dialogue box says, you know, what's going on. And among that information is the IP address of the...

Leo: What we really need is something that will go through my Firefox favorites, or bookmarks, or my IE favorites, and just replace them all with the ID, with the IP addresses.

Steve: IP addresses, yeah.

Leo: Shouldn't be - that wouldn't be a hard thing to write. I'll work on that on my vacation.

Steve: Oh, god. When you're not busy catching up on 10 years of Stargate.

Leo: I'm downloading the movie right now.

Steve: Oh, it's so good.

Leo: I'm excited. Scott Griswold in New London, New Hampshire is worried that he didn't need his football: Hi, guys. Love the show. Recently while paying for a transaction on GoDaddy.com I decided to use PayPal. I had my trusty PayPal security key at the ready. I was very surprised when, after entering my password, the transaction was authorized without prompting me for the secure, six-digit code. I received a confirmation email that payment was made, and I immediately went directly to PayPal.com to verify the payment made. Yeah, it was. Is this standard practice for PayPal to not require the security key when paying through a third-party vendor? It always asks me for it when I log directly into the site. Can you enlighten me as to what's going on here? Thanks so much. Keep up the great show. Boy, I've never had that happen. I've always had to use the security key.

Steve: Ditto. So I'm mystified. I wanted to just share this with our listeners so that they know this happened to Scott, apparently. I was thinking maybe if he was actively logged onto PayPal just before, his logon session may not have expired. And then if he came in on the same browser in the same session, then, you know. But I don't know. Maybe there's a bug over at the PayPal end of things. I'll be interested to see if any other users report similar behavior. If so, I'll let our listeners know. But I just thought that was an interesting little oopsie. Yeah, because I've never had it not ask. Anyone who has the football kind of like gets ready. The first thing you do is you go find it before you're going to buy something because you know you're going to have to come up with it.

Leo: Got my football here, I'm ready.

Steve: Exactly.

Leo: Matthew Justice in Austin, Texas asks just the right question at the right time: Dear Steve, I've been looking for a solution to store my passwords online, but for some reason I don't trust any of them. Since you're such a great programmer, I'd love it if you'd write a solution. You could even charge for it. Maybe something that uses, oh, a GPG key? By the way, GPG is GNU Privacy Guard, which is the open source version of PGP. That's what I use, by the way. Any thoughts? Thank you for all your hard work over the years. You got something like that?

Steve: Well, what's interesting, and when I said he asked the right question at just the right time, just that morning, yesterday morning, I got a demo from a friend of mine of a

password management solution that he is absolutely in love with. It's called Password Safe. It's open source, multiplatform - Linux, Mac, Windows. And from what I saw, I am very impressed. I've not done all the due diligence to plow into it. But one of the things that I love about it is that it's able to connect to a shared resource, a drive share, or I'm thinking through Jungle Disk to Amazon's S3 service, as long as it's running. But it looks like it's got very comprehensive sort of enterprise scalability for managing passwords.

So I will do a full episode on it because I was very impressed. It does automatic form filling. And my guess is they probably did everything right. From what I saw, everything looked like it was done right. But I haven't looked under the covers yet. I'm going to. But I thought in the meantime we'd just let our listeners know about Password Safe. If you put those two words into Google, first link is passwordsafe.sourceforge.net, where the project lives. And again, it's very nice looking. And the guy that showed it to me is a very savvy, security-aware IT guy. And he and his company have been using it successfully for some time, and he just really loves it.

Leo: I like the idea of it being, as you know, of it being open source. That's really great. Peter Fleischman in New York wants to be less nebulous about NebuAd: Is there a way that the hosts file could be modified to block NebuAd? By the way, I love your podcast. You and Leo are providing a really valuable service. Let's refresh people. NebuAd, we spent some time taking about it, and Phorm. These are the things ISPs are using to customize ads. Based on where you surf they actually follow you around. And since your Internet service provider knows everything you do, they can really keep track of every move you make, much better than something like DoubleClick.

Steve: Yes. In the case of NebuAd, I referred to it briefly when we talked about it and the fact that what NebuAd is doing is injecting their own packet, injecting a packet containing some HTML code at the very end of pages which come up. So when the backslash HTML tag that closes the page appears, NebuAd's technology triggers and basically spoofs one packet into the stream. And, I mean, it's not hard to do, but you have to really want to do this because it means you need to - we've talked about TCP protocol and sequence numbers. You need to be tracking the connection and emit a packet that looks like it's a continuation of that same connection. So, I mean, it's certainly doable. It's not rocket science.

But what they're doing is they're injecting a packet that contains a JavaScript invocation. And the key is it's pulling JavaScript. The packet itself doesn't have the script. It's pulling it from a site called a.faireagle.com. So all you would have to do is use your hosts file to preempt your computer's lookup of that domain name. I would say use both a.faireagle.com and just faireagle.com and just use a hosts file to aim those at your own machine, 127.0.0.1, the so-called "local host" address. And then everything will work fine. That script simply will not be able to find "faireagle." It will not look up "faireagle" in DNS. And no - except that you've still got a little extra debris at the end of your pages, it will be neutered, dead debris, and you're not trackable by NebuAd.

Leo: We should mention that everybody, all the ISPs have decided not to use NebuAd, at least as far as we know. It might even be illegal in England now.

Steve: Actually the reason I mentioned it specifically was that somebody who posts in our newsgroups is under an ISP using NebuAd in the United States. So it is...

Leo: Oh, that's terrible.

Steve: It is online, and it is happening.

Leo: You don't want to say the name?

Steve: No. All anyone needs to do is just do a view source of a web page, and you'll see a reference to "faireagle" at the very end of the source view.

Leo: Now, I suppose that they could change their server, and then you'd have to find, you know, have to block something else in your hosts file.

Steve: Yes, exactly. And that's the problem with this is, I mean, the annoying thing about the hosts file is it does not allow wildcards. It'd be so nice if you could do *.faireagle.com or *faireagle.com so that anything that was left of the asterisk would match. But the hosts file only does exact matches. So we don't have the ability to do that. I'm sure there are other tools around that could do this kind of preemption, and it's looking like such things might become more popular.

Leo: I'm just looking through my source code, a view in source, just to make sure. Wow, that's really scary. Fortunately it doesn't look like Comcast is using it. Although, you know, it's possible...

Steve: Well, Comcast got slapped hard for - the next time they trickle into messing with people's packets, they're going to be thinking twice.

Leo: It might be a good reason to go to Comcast now because they got slapped by the FCC.

Steve: Right.

Leo: Darrell Duffy in Coos Bay, Oregon - beautiful part of the country - has a micro question: Steve, I'm a long-time listener to Security Now! and waiting for an opportunity to use SpinRite. Perhaps I have one. My friend has a Nikon camera, a D70 - very nice camera, I use it myself, as well - and purchased a 2GB Microdrive with it. He's noticed errors over the past few days, then went on a trip to look at some real estate. He took a few hundred pictures in a day of various properties. And when he stopped by at the end of the day the pictures didn't all come off the Microdrive. It kept tossing errors and going offline. Only one or a few pictures would come off the drive each time before an error occurred. We noticed that moving to Windows XP rather than Windows Vista allowed more pictures to be recovered since XP did not read the drive to update the file data when a list display was used.

I understand you've said that SpinRite does not work on USB thumb drives. I understand why that is. I wonder about Microdrives. The Microdrive has a CompactFlash format with a 3/4" diameter hard drive actually inside the CompactFlash. I wonder if SpinRite would help recover this drive to get pictures from the drive. I gave my buddy a 4GB CompactFlash card to replace his 2GB Microdrive, but asked him to hold onto it in case SpinRite could recover it. Love the Security Now! show. Hey, that's a great question. It is a drive in there, not a flash drive.

Steve: Yeah. And the first time I heard about this I'm thinking, oh, come on.

Leo: How could they put a drive in there?

Steve: A drive in the same form factor as a little CompactFlash? But sure enough, I mean, there's a little spinning magnetic platter. And, I mean, 2GB, 2GB.

Leo: I think it actually predates the CompactFlash in that form factor. I think that was the first thing that happened was the Microdrive, as I remember.

Steve: Phenomenal.

Leo: IBM. They're brilliant.

Steve: In fact, that would make sense, too, because the Compact Flash has an IDE interface on it. I have a - one of the crazy boxes that I'm running OpenVPN on that I was talking about before - I built a diskless FreeBSD system because I just wanted to. It's where I'm running BIND 9 locally. And it's my little - my own network's UNIX machine. And all I had to do was it boots from a CompactFlash and then doesn't use the CompactFlash at all. I turned swap files off, and my VAR directory tree in UNIX is mapped to RAM. I have two RAM disks, so I copy things over at boot time so nothing is ever writing to the CompactFlash. And I've marked the root partition and the user partition both as read-only so nothing can write to them because we know you don't want to burn out your EPROM. So it is certainly possible to do that. But what was cool was a simple little bracket just adapted the IDE connector to the CompactFlash. It emulates an IDE drive. So it makes sense, Leo, that the microdrive would have predated the CompactFlash. Otherwise why would they give it an IDE interface?

But anyway, to answer Darrell's question, absolutely. We've had a lot of customers report success using SpinRite on Microdrives. And they tend to have a problem because it is a delicate little bit of mechanics. And being so small it drops. It can easily be mistreated. So, yeah, SpinRite will probably recover it.

Leo: Very cool. I love that idea. I think that they're phasing those out. I don't think you see as many of those as you used to. Because they do top out at 2GB.

Steve: And I was just going to say, in this day and age, who would use a spinning

mechanical flaky thing when you could get a solid-state CompactFlash that are just not expensive anymore. But of course the point is it's not that he doesn't wish he'd been using a solid-state drive. He did use a Microdrive, and he wants the photos that it contains.

Leo: I think that originally it was those were larger capacity than the Flash, CompactFlash. And they were faster.

Steve: Ah, right.

Leo: They were faster. But now of course we've got CompactFlash that's bigger and faster than any drive, so - amazingly enough. Technology is so cool. I love it. I just love it. Jonathan Kemp in Leicester, England defends third-party tracking cookies: Dear Steve and Leo, I work for a company in the U.K. that provides a free service to travelers. I'm not including the name as I'm not after a shameless plug. We rely entirely on affiliate advertising, and one thing that is becoming and will continue to be an issue is cookie blocking and cookie deletion, an increasing trend. In order for a lot of services to remain free, tracking cookies have to be accepted, otherwise companies like mine will be losing out on revenue we rely on. This is the other side of the argument, of course. I'd love to hear your views on this as I feel there is a fashion in deleting cookies pushed by big Internet security companies without users considering or understanding the repercussions for affiliate publishers. After all, this will eventually have a knock on effect on users looking for free services on the Internet. Keep up the good work. And I'd add to that, really, because I have a little dog in this hunt, blocking banner ads, which you can easily do. And these are free services that are paid for by advertising.

Steve: Yeah. I included this because his viewpoint had never been entertained here. I'm very anti-tracking, anti-third-party cooking - cookie. Third-party cooking. Actually I enjoy third-party cooking.

Leo: You live on third-party cooking.

Steve: I'm Mr. Restaurant. So, but I thought his position ought to be represented. There was a discussion we had, really interesting discussion in our newsgroups many years ago, back when I was entertaining the idea of basically building a filter for browsers. And one of the options we were considering was ad blocking, blocking ads completely. And the ethical question was, is it okay? Is it okay for users to block ads? And both sides were represented, and I think both sides were represented well, the idea being, okay, wait a minute. If I go to a web page, am I implicitly agreeing to accept everything the page offers? Why can I not be selective?

And the argument you bring, Leo, is a good one. It's like, okay, wait a minute, web pages depend upon advertising in order to survive. So don't users have some obligation to see all the content? And of course then I say, well, okay, I have TiVo. Why do I love TiVo? Two reasons. It allows me to watch things asynchronously, in sort of the same way I love email and newsgroups because I don't have - I'm not live chatting. I don't have to be watching television when it's being broadcast. But also, frankly, the commercial-skipping is to die for. Okay, well, as a viewer of broadcast television, don't I have an

obligation, if I'm getting this free TV, to sit there and endure the commercials? And is it okay for me to get up and go pee in the middle of the show?

Leo: Yes, it's okay.

Steve: In a commercial break. No, no, it's not okay, I have to watch the commercial.

Leo: There are even some people who think I should click on a banner once in a while, or I should buy something just to support the show. I don't think you need to do that.

Steve: Yeah, so, I mean, I guess my point is these are interesting questions. And they're not cut-and-dry. They have two sides to them.

Leo: I think we love the free stuff we get. For instance, I looked into podcasting, there were three ways we could do this show. We could do it listener donation based, which is the way I'd prefer to do it, in fact that was my original plan, but not enough people donate. Only about 2 percent of our listeners donate. Of course we don't flog it, but I don't want to flog it. So that's one way. Another way is to charge a subscription fee. And frankly, in the states at least, we're so used to getting free content, television and radio, that nobody wants to do that. And I've noticed a lot of shows that have tried that have failed, including Ricky Gervais, who had the most popular podcast in the U.K., it was at 400,000 downloads, went paid and it was over. And he went back to the free model. So I think we have to do advertising based. That's what everybody's used to in their media from the mainstream media. And you just hope that people, you know, fortunately the ads work on our shows. But we're very careful. We choose products that we like, that we think our audience would like. We try to do the ads relatively unobtrusively, with some content in them.

Steve: And my hope is that the quality of the content, the quality of the show allows it to carry, to justify, the advertising support that we need in order to be able to put the quality into the show.

Leo: I have to tell you, though, I've in recent weeks received - because we now have three ads in the show, which is, by the way, the max we'll ever have. But I've received several emails from people saying I'm not going to listen anymore, it's too many ads. Which cracks me up because if you listen to commercial radio or watch commercial TV, there's five times more ads.

Steve: Yeah.

Leo: I don't understand. I guess people don't watch any commercial TV, either. We just have to, you know, this is how we have to support ourselves. These shows used to be very cheap to do. They're not so cheap anymore. It's a great question, you know? And but then there's also the line between third-party cookies and NebuAd.

How far are you willing to go?

Steve: Right.

Leo: Where does it become a privacy violation? Bobby Clark in Berea, Kentucky brings an important new Google Mail feature to light: Steve and Leo, Google has added a setting inside of Gmail for always use HTTPS. Yay. With that set you don't have to put https://gmail.com to be guaranteed a secure connection while on Gmail. I noticed that the other day. That's great news.

Steve: Yup, I just wanted to make sure all of our listeners knew that there is that setting, which they can turn on. And mine's on because - and just the other day I was talking about Gmail flipping back to non-secure if you came in non-secure. It would briefly make you secure and then switch you back. Now you can say absolutely always. And that makes it unspoofable. The bad guys cannot spoof Gmail, that is, the DNS spoofer guys, because your browser will check Gmail's certificate on an SSL connection. And if it's going somewhere else, all you have to do is make sure HTTPS is up and running.

Leo: Yay. I've been using a Firefox plug-in called Customize Google to do that. But now it's just a setting. It should have always been a setting. I'm not sure why they didn't do that before. All right, let's get on with our very Exciting, Fantastic, Wonderful, Extra Special News of the Week. This is from Brian Scallan in London, U.K.: Hi, Steve and Leo. I wonder if Amazon has been listening to the podcasts in which you mention how the market is ripe for a competitor to PayPal? I'm excited about this, too. They've just launched a rival, Payments.Amazon.com. Thanks for the great show. I immediately took a look at that. What do you think, Steve?

Steve: It looks very good to me, Leo. I'm an Amazon fan. There's hardly a day UPS doesn't pull up with something from Amazon. And of course I'm a happy Kindle owner. And by the way, my replacement Kindle came promptly. I moved stuff over.

Leo: Well, that's good news.

Steve: I switched my account over. I sent the one with the broken screen - that I broke - back. And it was a completely good experience. So let's hope this thing, I mean, Amazon's got enough of a name that I can imagine sites that support PayPal adding an Amazon.com purchase button, much as sites are also doing for Google.

Leo: Well, I would love to replace PayPal for our payment system. We get a lot of complaints about them. And as you know, PayPal ripped me off. So I'm anxious as can be to replace PayPal. My only concern is you have to have an Amazon account to use this; right?

Steve: Correct. You do.

Leo: Yeah. So you don't have to have a PayPal account to pay us through PayPal. You can use a credit card.

Steve: Oh, interesting.

Leo: Yeah. In effect, PayPal is really just providing us with merchant services.

Steve: So it sounds maybe a little bit like Amazon is trying to push people into this to expand their overall buyer base.

Leo: Sure. Once you're - you've already got an account, just buy something, you know? And I imagine - I can't imagine many people who listen to this show aren't Amazon members except for we have a huge global audience. And while Amazon certainly has a global presence, I think in Australia, the U.K., Sweden, they may not be the same presence. For instance, in Canada, Amazon only sells books. So they're not as popular. And they're more expensive. So I think that, I don't know, this is a tough one for me. I'm thinking maybe we just get a merchant services account and let people just use a credit card.

Steve: Well, and again, as we've said, PayPal needs competition. I'm glad that another major potential competitor has stepped up.

Leo: Yes. Yeah, it can only be good to have some competition. Finally, our last question, sad to say, our Cool Tip of the Week. Ryan Morris in Niagara Falls, the Ontario, Canada side, says: Dear Steve, last year my friend went to the University of Waterloo and could not use any routers at school. We were talking about the University of Pennsylvania, right, just like that, last show. I told him to get a Mac, though he is a pure Linux user. I then explained to him that you can use a Mac as a router. If you have a Mac computer plugged in, you can turn the WiFi radio into a hub. It's very easy and in the settings. Then it's as easy as connecting to a regular WiFi router. And yes, you can add a password. The only downfall is your Mac has first priority to bandwidth - that's okay - and whatever is left is spread out. Also it can work in reverse by connecting over WiFi and turning the Ethernet port into a hub. Love the show. Ryan. P.S.: SpinRite is the only piece of software I ever bought, and I have a ton of software. Ryan's a little pirate. But he didn't pirate your stuff, and I think that's - and you don't secure, you don't put any DRM on it or any copy protection or anything.

Steve: No.

Leo: That's a really good example of, I think, when you treat people like thieves, they act like thieves.

Steve: It works for people, and they appreciate it. And how many people have we heard say this is the best $89 I ever spent?

Leo: Yup. I should point out that, yeah, you can do that with a Mac, but you can do it with any computer. Linux does it just fine. It's called - what is that called, an "ad hoc network." Right?

Steve: Yes. Yes.

Leo: So, but you need two connections, one to bring the Ethernet in, or the Internet in, in this case he's used Ethernet; and then the second connection to distribute it, which could be Ethernet or, since many machines have both Ethernet and WiFi, this is a great way to do it. You set up an ad hoc connection.

Steve: And ad hoc as opposed to base station, where you've got two computers connecting to each other as opposed to a base station and a computer.

Leo: Right. So, yeah. And I know Windows with Internet connection sharing effectively does the same thing. It's a little harder because of all the finicky bits. But you could totally do that. So that's a great tip. Steve, we've run out of time.

Steve: Well, and you're off to the airport.

Leo: Well, not exactly the airport. I'm off to San Francisco, not to the airport. I'm going to do a radio show in San Francisco, the Ronn Owens Show at 11:00 on KGO. And then I'll be back. We're going to do some Giz Wizzes because next week I am taking four days off. We've doing a drive up with the family to the gold country and take some time in the woods.

Steve: Oh, cool. Well, I did want to mention I love getting questions. The questions get to me by people who go to GRC.com/feedback. So there is a link to that at the bottom of the Security Now! page. But you can go directly there. If you've got something to say, GRC.com/feedback. And I love to hear from people. Every time I go and pull notes, I get on the order of 450 new submissions. So I apologize to people, sometimes I see them, and they say this is the fourth time I've written and you've never - it's like, I know, I'm so sorry, I mean, I get so much mail. But that's what drives these Q&A episodes. I do respond and read everything I'm able to. So it's really sincerely appreciated. So thank you, everybody, for your feedback.

Leo: Well, and while you're at GRC.com make sure you check out SpinRite, of course, Steve's great program, the ultimate disk maintenance and recovery utility, and all of the great freebies he's put up there - ShieldsUP!, Shoot The Messenger, DCOMbobulator, and don't forget Wizmo. Love Wizmo. Really useful little doohickey for your - I think the best way to describe it actually is "doohickey for your Windows." It does so many things. Does everything but give you a hickey. It's all there at GRC.com along with transcripts of this show, 16KB versions for the bandwidth impaired. Check it out today. GRC stands for Gibson Research Corporation. Steve Gibson, always a pleasure. Thank you for...

Steve: I was just going to say, there's one other thing that I forgot to mention that your reminding me about the freeware reminded me of.

Leo: Yes?

Steve: Years ago I was doing a little work, you remember, I told you about it confidentially, for the government, a communication system, a new type of communication system for the Internet. And I wrote, in research, I wrote something I called DNSRU, DNS Research Utility. And it is, as far as I know, the only really comprehensive DNS benchmarking tool ever.

Leo: Very cool.

Steve: Well, and it's funny because it's been kept alive in the hearts of the people in our newsgroups. And when I mentioned that I was going to be doing this DNS spoofing test, someone said, uh, Steve, could we have that back? Because it's funky, I never finished it because I used it for all the information that I needed. And at the time I had an expiration in it so that you had to hold both shift keys down when you launch it in order for it to - in order to, like, bypass the, hey, this copy's too old, you probably ought to refresh yourself with a new one. Except there is no new one.

Anyway, I'm going to dust it off and change it around a little bit because it had some stuff in there that wasn't about DNS benchmarking. But it's got really a cool DNS benchmark. And since people are looking at doing things like maybe changing DNS servers, or checking to see, remember that the performance of DNS is critical because it's the first thing your browser does to look up an IP address for anything it's doing. So faster DNS does mean a faster overall experience on the Internet. And so I will be adding before long a permanent addition to our freeware, which is going to be this really cool DNS server benchmark.

Leo: Oh, that's excellent. So we'll look for that, too, at GRC.com. And we will look for you next week, Mr. Steve Gibson, every Thursday. Come rain or shine or even vacation, Steve Gibson's here with the latest security news. Thank you, Steve. We'll see you next time.

Steve: Talk to you then, Leo. Bye.