VPN Solutions

Description: After catching up with a wild week of security events, we revisit a topic from the earliest episodes of the Security Now podcast: Virtual Private Networks. This coincides with the introduction of a new sponsor on the TWIT network, proXPN, a VPN provider that truly looks like the right choice.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-400.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-400-lq.mp3

SHOW TEASE: It's time for Security Now!, our 400th episode. Let's celebrate with Steve, talk about Java - yes, there's another update - talk about security and a little intro to VPN systems. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 400, recorded April 17th, 2013: VPN Solutions.

It's time for Security Now!, the show that protects you, your loved ones, and your privacy online. And it's all thanks to this man here, the Explainer in Chief, Steve Gibson of GRC.com. Steve joins us every week. Hi, Steve.

Steve Gibson: Hey, Leo. Great to be with you again, as always, for the Big 400 episode.

Leo: What?

Steve: Yeah. 400 weeks we've been doing this.

Leo: Celebrate good times. I think I'm going to light up a cigar.

Steve: And you've been here for most of those, yeah.

Leo: But by the way, if you're listening, John, I mean Paul, Paul Mentocides [sp] or

Mintisitis [sp], who sent me this contraband, I am very happy. I'm a happy, happy man.

Steve: Cuban contraband.

Leo: Cohiba Behike from Havana. Wow. "Cohiba Behike es la mxima expresin en sabor y aromas del Habano." It smells like Havana, is what they just said. So that's good. And also did you know, Steve, that not only is this the 400th episode, but it is also the eighth anniversary of the launch of the TWiT Network.

Steve: No kidding.

Leo: April 17, 2005, our very first TWiT episode aired.

Steve: Wow.

Leo: The one that I recorded at the bar at the 21st Amendment Brew Pub.

Steve: I remember that, yes.

Leo: Yeah, with Kevin and Patrick and Prager and Patrick's wife. And that was the first TWiT, TWiT 0. We actually didn't even have a name for it at the time. We called it The Revenge of the Screen Savers, I think. So Dane Atkinson's here, who is a wonderful friend of the show. He used to be at Squarespace. He has a new company which is going to be advertising soon called SumAll. And he brought me a lovely Pauillac. Actually he brought us a couple of Bordeaux and, wow. You like - I know you're a burgundy fan, Cabernet fan.

Steve: Yup.

Leo: But you must like Bordeaux.

Steve: Yeah, yeah.

Leo: They're maybe a little lighter than the big heavy reds you like. But, boy, these are good. And then also a Malbec, which I'm sure you like Malbecs.

Steve: Yes, yes, yes. I've heard John speak of that also.

Leo: From Argentina, yeah. So thank you, Dane. Thank you, Paul, who sent me these cigars. Didn't know it was going to be our fifth anniversary. And congratulations to you for your 400th episode. Wow. Eighth anniversary. Correct me, thank you. Eighth anniversary. Oh, wow.

Steve: Yeah.

Leo: All of that. Now, today what are we going to do?

Steve: I want to talk about, sort of revisit the question of virtual private networks. VPNs was a topic that we covered extensively, speaking of nostalgia and the birth of TWiT things. Episode #14, the 14th week we were doing this, the topic was Virtual Private Network Theory. #15 was VPN Secure Tunneling Solutions. Then we had our very first listener feedback episode ever on Episode #16. And then I continued with Episode 17 was on - and we had fun with these acronyms. I remember we were tripping our tongues with PPTP and L2TP and IPSec and so forth. So that was Episode 17. And then we introduced the world to Hamachi.

Leo: Oh, yeah.

Steve: And actually, I mean, this was a huge deal. Episode 18 was called Hamachi Rocks. And I remember that Dave's wife was giving him a hard time. Dave was the creator of Hamachi. And she was like, okay, you rock. And he's like, okay, well, yeah. And then 19, Episode 19 was VPNs Three, where we talked about Hamachi, one that had surfaced called iPig, unfortunately named, and then OpenVPN.

And so I chose this week to sort of just take a snapshot of where we are. There's been some - of course, I have mentioned my interest in developing something because I felt that there was a need, yet I was put off by this continual grumbling in law enforcement about their not being sure that they feel good about not being able to decrypt things on the Internet.

But this also connects with the TWiT Network having a new sponsor, which you'll be talking about in the middle of the show, a company called proXPN. I've had a chance - I was told about a month ago that this was going to happen. I told the guys in our newsgroup, the GRC newsgroups about it. And they've all been playing and have nothing but good things to say. I've had a chance to do some reconnaissance, and I'm very pleased that we have somebody, I mean, to me I think this is a perfect marriage of the show and a sponsorship, and one that, from everything I've seen, just looks like something we can, in fully good faith, recommend to our listeners.

Leo: Good.

Steve: So I wanted to sort of, like, we haven't talked about VPNs almost at all since back then, episodes 14 through 18. So I wanted to sort of do that. There's been evolution in one important area, which is in the development of the flashable routers with DD-WRT and the Tomato firmware, both which support OpenVPN. And this new sponsor of ours,

proXPN, is an OpenVPN solution provider. So it all really fits together synergistically.

Leo: Good. Good, good, good.

Steve: And of course this also ties in with the worry that people have had that their local networks may be spying on them. Remember I introduced this notion of certificate fingerprints two weeks ago. We're more than 40,000 people have availed themselves of that, more than 2,000 a day now, this new service at GRC. And one way to thwart that kind of spying, if it's a concern, is - actually THE way to thwart it is with a VPN. So everything kind of all comes together here. So I'm really glad. And of course we had a crazy week of news.

Leo: So I noticed a Java update again. What?

Steve: Well, yeah. Now, remember the last...

Leo: Is this their regular update?

Steve: Yeah, last week we told our listeners to expect something on Tuesday. We had the standard second Tuesday of the month update from Microsoft. And by the way, that was a catastrophe because it turns out that one of the patches was causing Blue Screens of Death for users of Windows 7 and some third-party software that was...

Leo: I think Kaspersky, mostly Kaspersky; right?

Steve: Yeah, and there seemed to be some Brazilian connection, too. I don't think it has anything to do with your cigars. But it was, somehow it was reports from Brazil, for some reason. So it was Kaspersky's A/V that was for some reason colliding. But enough people had it that Microsoft removed the link and withdrew it in order to figure out what it was that was going on. And so I can't really fault Microsoft, I mean, this is something it would have been better to know about before. But interaction with a few vendors' software is, if the vendor software, like what Kaspersky's done with their A/V tool, is to be very intrusive, that is, like sink their hooks deep into the system in order to monitor things. For example, this is just sort of tangential, but related, people were complaining that their SSL certificates were not matching when they were using Kaspersky's A/V.

It turns out Kaspersky installs a certificate authority and intercepts secure communications on the client machine. So, I mean, it's doing that kind of traffic inspection on behalf of the user. But that breaks SSL validation, which is really not good. For example, you're no longer going to see any of your enhanced extended validation (EV) certificates. Those all get lost because you've got - essentially you've stuck an HTTPS proxy in your computer. So that's an example of how deeply this thing is sinking its hooks into people's computers. And so you really can't fault Microsoft for doing something deeply which in some way is conflicting with some assumptions that third-party software made. I would really blame it more on the third-party software not being compatible.

So anyway, they pulled that back and warned people to uninstall it if they hadn't - or not to install it if they hadn't installed it, but even to uninstall it if they had, just to be safe. What I heard from many people was this didn't come out for a day or two afterwards; they had already installed the patch, being responsible patchers; and everything was fine. So for those where it didn't cause a problem, it's probably not going to cause a problem. But it certainly was a surprise for some people.

But what happened with Java was big news. And last week we said expect an update from Oracle on Tuesday, which was yesterday, April 16th. My favorite headline I termed the Oxymoronic Headline of the Week. And this was the Reuters coverage of this, Reuters news service. They said, and I love this: "Oracle fixes 42 holes in Java to revive security confidence." It's like, what?

Leo: Hi, I feel better. 32?

Steve: Yeah. 42.

Leo: 42?

Steve: 42 holes, yes. And then it gets worse because...

Leo: How could it get worse?

Steve: The executive vice president, Hazan Rizvi, he was quoted in this article saying, "The patch fixes 42 vulnerabilities within Java, including 'the vast majority,'" which is to say not all, "'the vast majority' of those that have been rated as the most critical."

Leo: Why, almost all of them.

Steve: Yeah. He says the company specifically states that the 39 called-out bugs "may be exploited over a network without the need for a username and password." And then, unfortunately, he says, "Although not all known problems are being fixed with the current patch" of 42, "there are no unpatched problems that are being actively exploited."

Leo: Well.

Steve: So there are unpatched problems. There are problems we know about, but no one's gotten around to exploiting them yet. So we've fixed the 42, 39 of which were being remotely exploited and required no username and password. So all of this is a nightmare except that they finally made a change proactively.

Now, some time ago they added a checkbox in the Java security settings panel that people could uncheck to disable Java in the browser. And so that was a good move. What they've done now is they have added checking for signed Java applets, which is a really nice move forward. Now, you could argue, and I'm sure people will, that it's not difficult

to sign a Java applet. However, to have a correctly signed applet, it's very much like having a correct security certificate on a website. That is, you need a certificate authority, like a VeriSign or a DigiCert, one of those guys, or unfortunately the Hong Kong Post Office. But somebody that your browser knows and trusts signs the certificate, which is then used to digitally sign the Java applet.

So this is very much like drivers now in Windows need to be digitally signed. You just can't have a random driver that Windows will install. We've said no more, that there's too much exploitation of that going on. That's not okay anymore. So finally, Oracle has added the same technology, very much like what Microsoft calls Authenticode. The apps that I have been publishing recently are all Authenticode-signed, just because it's the right thing to do. You want people to be able to verify - essentially the operating system is able to verify the identify of the signer.

Now, there are different levels of signing. That is, you could have a self-signed certificate rather than a CA, a certificate authority-signed certificate. So you'll get a dialogue box. There's a number of different dialogue boxes that Oracle pops up, depending upon sort of the degree of trust that it's able to ascertain the applet has. So you can force it past an unsigned applet. But you get now a new dialogue, and that's the key. You actually get a pop-up presentation from Java itself saying this is what we know about the applet you are trying to run.

Now, that's huge because it used to be, I mean, it was day before yesterday, 39 different problems in Java could be exploited with no user intervention, making them critical. So no user intervention is gone because of this change that Oracle has finally made to Java. So this is really, really big. In fact, Kaspersky looked at the statistics and said that Java was the vehicle for 50 percent of all cyberattacks last year in which hackers broke into computers by exploiting software bugs. And that 50 percent was followed by Adobe Reader, which was involved in 28 percent of these incidents. And then Kaspersky says, to give us some more perspective, Microsoft Windows and IE were involved in about 3 percent. So that really shows you how this terrain has shifted. Four years ago, it was all IE. I mean, IE...

Leo: That's a huge difference. It's amazing.

Steve: It is, yes.

Leo: Four percent?

Steve: Yeah, three. Remember? And so there's been a dramatic change as the browser has really been made vastly more secure. I mean, it takes Microsoft a long time to get there, but they did. And we could argue, too, it's taken Oracle a long time to get here. But they've made a big change.

So one thing that our listeners can do, I have an unsigned Java applet. It's safe. It's benign. It's my Big Number Calculator that I put up on GRC. It's under the Other menu in GRC's main menu, Other and then Big Number Calculator. I use it because I want to know the exact number that 2^128 is for cipher stuff and crypto things. It's very handy for calculating ridiculously large numbers. It just makes my little HP calculator smoke.

Leo: But it's written in Java.

Steve: It's written in Java. So it is cross-platform, cross-browser, which is the reason anyone writes in Java is to have cross-platform compatibility. The point is that it is a perfect example of an unsigned applet. So you can go to GRC's, under the Other menu, Big Number Calculator, and see what happens after you update Java. And you can see it will invoke this dialogue saying, whoa, hold on, wait a second, this applet that you're wanting to run is not trusted. Now...

Leo: Of course I don't have Java installed. So I just get "missing plugin."

Steve: I was just going to say, I tried all of this yesterday, and I got what you really want to get, which is there's no plugin available to do anything with what it is you're trying to do. That's really...

Leo: That's even safer.

Steve: That's really what you want. So actually I had to - because Safari also updated, 6.0.4. We'll talk about that in a second. But so in order to experience that, I was forced to install Java on a MacBook and update Safari because I wanted to see what Apple had also done, which was coincident with this. And so but I started off the same way, Leo. Oh, this requires a plugin that you don't have in order to go. It's like, yes, that's really the result that you want.

So anyway, this will end up being huge. It is the fact that browsers would silently invoke Java behind users' backs that was the problem. And Oracle kept having that checkbox on for the browser plugin by default. And when you install Java, it installs the plugin. So we were just going around in circles.

Now, it is still a problem that there is a lot of old Java. Remember that we showed last week that pie chart which was really disturbing...

Leo: No kidding, yeah.

Steve: ...with how much old Java there still is. And the old Java had no auto-update facility. So the old Java is staying old, and it is staying in people's browsers who don't know any better. And so this 50 percent isn't going to go down to 3, like IE has, anytime soon. There just isn't a way to get those old ones fixed. I mean, the only thing you could do would be to have a site that used Java to fix old Java. But then people would have to go there to get fixed. And they're not going to a fix-it site.

So, I mean, there just isn't - I don't know how you do this except to, as I have said, for browsers to take responsibility. But they're also using old browsers. So these are just systems that are never being updated. They're old, and they're just going to be a problem until they collapse of their own age, I suppose.

Leo: Sigh. Hey, can I ask you a security - oh, go ahead, finish. Then I'm going to ask you, when it's appropriate, a security question.

Steve: Oh.

Leo: Yeah.

Steve: Well, this is the right podcast for that.

Leo: You're the right guy; right?

Steve: So Apple also updated Safari and did something wonderful. They gave us sort of the equivalent of NoScript's per-site blocking of Java - now, this is not JavaScript - Java natively in Safari. So Safari now has a site-by-site permission Java applet execution facility. When you do something with Java, and again you can use GRC's site as an example, as a test bed, you're able to - it brings up a dialogue, that is, Safari itself does, saying hi there. You wanted to run Java. Okay. Here's what we know about it. And do you want to run it this time only? And there's checkboxes for don't ever bother me on this site again.

So this allows corporate users, who have to have Java enabled, and assuming they're also Mac corporate users using Safari, to permit Java on their own corporate Intranets, where it's arguably safe, but not on the wider Intra- Internet, sorry, Internet, external WAN, Internet, where they then have the option, if they encounter Java, to do something.

So this, again, this is a big step forward for locking this stuff down. I think everyone has been trying to avoid involving the user and more pop-ups and more dialogues. We know it's not a perfect solution. We know that unaware users are going to go, oh, fine, click, okay, okay, I just want - I want to get the page I'm trying to get to. Okay, okay, okay, okay, whatever it takes to just push through those pop-ups. But it is a worthwhile barrier for us to erect.

So it's good that this is finally happening. Like, my hat's off to Oracle. They're under tremendous pressure to fix this because it's significant. If you're the producer of software which was responsible for half of all exploits on systems globally, that's not good. And again, unfortunately, they're never going to be able to fix a lot of those because they're never going to get updated. But it's an improvement. Now, you had a question, Leo?

Leo: Yeah. Well, just, you know, I got this new phone, I was showing you before the show began, from AT&T. And I noted they did something which I thought was kind of odd. There's a sticker on the back that has the IMEI, the serial number and the SKU and so forth. Is that in any way a security flaw, to have on the back of the phone the IMEI publicly readable? That's the identifier that goes to the phone.

Steve: I don't think so because you can always get that from inside the phone, too, poking around.

Leo: I should just take the sticker off, maybe.

Steve: Yeah, yeah, I would say.

Leo: It's because on most phones you take out the battery, and it's under the battery. But you can't do that on this HTC one. So I guess they put it right on the - but I don't - it shouldn't be in - but a bad guy having the IMEI doesn't mean anything; right?

Steve: And it's not clear - I guess the only time you need it is when you're initially setting up a subscription service, where the vendor, whoever it is, AT&T, T-Mobile, whomever, needs it in order to synchronize things.

Leo: I'm going to take it off. It's ugly.

Steve: I would remove it. And I'm sure that it's available inside by browsing through properties of...

Leo: Oh, I'm sure it is, yeah.

Steve: Of the phone properties, yeah.

Leo: All right. I'll just take it off. Thank you. It's nice to have your own personal security expert just...

Steve: Get rid of it.

Leo: ...waiting in the wings.

Steve: Well, so also in the news is an interesting new botnet which has been attacking WordPress blogs. It turns out that...

Leo: Lots of them.

Steve: Yes. Well, 90,000 websites at this point are estimated to have been taken over. And the number is as big as it is because it is wormlike. That is to say that, once a WordPress blog is compromised, it begins performing outbound scanning, looking for other WordPress blogs to compromise. Thus, a worm. That's what a worm is. So there is a 90,000-website-strong botnet which has been built simply by carrying around the thousand most common passwords. And it tries to log on, when it finds a WordPress blog on the Internet, it starts using those passwords to try to log in. And unfortunately,

enough people are using "monkey" as their password...

Leo: Hey. You just gave mine away. That's not nice.

Steve: Or "password," or "9999999" or "admin" or whatever, that it's just not difficult to get in. So, I mean, evidenced by this because to do a brute-force, across-the-Internet login, I mean, what - the first thing that I'm noting is, wait a minute, no lockout? So they can - you can log in, you can attempt to log in a thousand times to the WordPress administration panel?

Leo: Yeah, yeah.

Steve: And it doesn't ever say, uh, stop it?

Leo: No. Well, they've updated their authentication, but the older WordPress is - yeah.

Steve: Well, good. So it's good that they did. Anyone running a WordPress blog, it's funny because I was also doing some research when I was poking around seeing what had been written about this. Brian has his blog hosted by WordPress. And he said, you know, Word Press blogs just like this one. We know, however, that Brian Krebs has a bizarro password that no one is going to...

Leo: One would think he'd change, not only the password, but the login.

Steve: Yes.

Leo: I mean, you leave it as "admin," you're just making it possible for people to bang on it.

Steve: But Leo, it's nice to be able to remember it.

Leo: I changed mine. Don't bang on my blog. It's already changed.

Steve: What's my username?

Leo: Yeah.

Steve: Okay, now, when this news broke, this next item, it generated massive traffic. And it may not have been true as it was written. And of course The Register carried it, so - and they never updated their story with the, well, maybe we were wrong about this.

The story was that at the Hack in the Box security summit recently - this is like late last week in Amsterdam - a security researcher, Hugo Teso, who's with the company N.Runs, and he's also a commercial airline pilot, he spent three years buying used commercial-grade airplane equipment off of eBay and using flight management software, simulation software, on his PC, which is said to involve, to reuse the same code as the cockpit instrumentation hardware. And he ended up developing two tools. He dubbed it SIMON, S-I-M-O-N, and that may be an acronym for something, but I didn't run across that. But it runs on Android in his app called PlaneSploit. And he demonstrated taking over full control of the in-flight flight systems and pilots' displays.

Leo: That doesn't seem like a good thing.

Steve: No, no.

Leo: Holy cow.

Steve: It even said, "The hacked aircraft," I mean, we're talking about a Boeing something or other. I mean, "The hacked aircraft could even be controlled using a smartphone's accelerometer to vary its course and speed by moving the handset around" in the air. So not only can you...

Leo: That's like an RC plane.

Steve: I was just going to say, not only can you control your quadrocopter four-propeller floating platform, but you can also control the Boeing 707 that you're riding in at the time.

Leo: Wow.

Steve: So the story goes that he looked at - Teso's presentation says he looked at what's called the Automatic Dependent Surveillance-Broadcast - which is ADS-B, Automatic Dependent Surveillance-Broadcast - system that updates ground controllers on an aircraft's position over a 1Mb per second data link. This has no security at all, he found, and could be used to at least passively eavesdrop on an aircraft's communications and also actively interrupt broadcasts, or feed misinformation.

He says also vulnerable is the Aircraft Communications Addressing and Reporting System, which is the acronym we've seen before, ACARS, A-C-A-R-S, the communication relay used between pilots and ground controllers. Using a Samsung Galaxy handset, he demonstrated how to use ACARS to redirect an aircraft's navigation systems to different map coordinates. And he said, "ACARS has no security at all. The airplane has no means of knowing if the messages it receives are valid or not. So they accept them, and you can use them to upload data to the airplane that triggers these vulnerabilities. And then it's game over."

The story says that Teso was also able to use flaws in ACARS to insert code into a virtual aircraft's flight management system. By running the code between the aircraft's

computer unit and the pilot's display, he was able to take control of what the air crew would be seeing in the cockpit and change the direction, altitude, and speed of the compromised craft.

So after all of that, I mean, this came out with huge news coverage. It's like, oh, my god. So then EASA, E-A-S-A, which is the European Aviation Safety Administration, and the U.S. FAA, the Federal Aviation Administration, both said that this was done using simulation software, which is the case. And they all deny that this would work on real aircraft. And their official statements read like total butt-covering mumbo jumbo. I mean, when you read what they wrote, it's like, okay. Because they're all now actively working with Teso and his N.Runs security firm to understand what he did and whether in fact they are, or not, vulnerable. But it wouldn't be at all surprising to me, unfortunately, if what we're dealing with are pre-security-conscious protocols that were designed 20 years ago, and we're still using them, and we have never retrofitted them because nobody wants to do what they don't have to do.

And so my own take, looking at all the news, is that he found something, and that they're running around frantic. They're denying it because they have to, officially. Oh, and by the way, he deliberately did not disclose all of the details. He demonstrated what he had done and what he could. But being a responsible researcher, he didn't publish the source code for everyone to go and see if they can load PlaneSploit into their own Samsung Galaxy phones and, you know, because they're not happy about the airport they're going to be landing at.

Leo: Hey, let's go somewhere else. What do you say?

Steve: Yeah. Looks like bad traffic on the freeway outside of that airport.

Leo: Wow. Wow.

Steve: Yeah. So I wouldn't be surprised if there is crappy security on this stuff because, unless you have to do it, we've had these systems now, these avionics systems, for decades. And why would they have bothered? You have to upgrade everything, Leo, and isn't that a problem? Because, you know, it costs money.

Leo: Right.

Steve: And you won't do it unless you have to. One of the things that has arisen from my talking about SSL Labs, which is that company that I've mentioned that allows you to check the security being offered by many websites, is I've had a lot of feedback from people saying, oh, my god, I can't believe how insecure my bank is. So again, unless people are forced to fix these things, they don't fix them. And look, how many stories have we covered that have exactly that as the key, I mean, as the underlying problem, is that, oh, well, yeah, it wasn't patched. Oh, okay, well, or it used weak security, so they were able to get in. Right.

And I just wanted to give a tip of the hat to a browser we rarely talk about, and it's unfortunate, and that's Opera. Opera's been around for years. We've talked about Opera Mini a couple times in various contexts. But I had an occasion to be using it because I've

been doing a lot of work with certificate stuff recently. And in fact I have a whole new breakthrough in verifying server certificate technology, like sort of a next generation beyond the fingerprints concept, which is in response to confusion that the fingerprinting was caused by servers like Google and Amazon, where they've got their huge global networks and don't always return the same certificate.

So I've removed Amazon, for example, from my list of default servers that we generate fingerprints for and expanded a section at the bottom of the page explaining why you could get false positive mismatches. But in the meantime I have completely solved that problem. So I'll have something new soon.

But in the process I needed - we were looking at public keys that certificates used. Firefox shows theirs. But IE showed a different one. And the problem is that Chrome reuses Internet Explorer's certificate management, so it was also showing something different than Firefox. And I was trying to filter through the noise, figure out what was going on. And I thought, well, I wonder about Opera. So I fired up Opera, that had been languishing for years. And it's very nice. And in fact, I wrote the numbers down.

Leo: [Chuckling]

Steve: I don't have them in front of me. But Chrome now takes about 250MB. When I launch Chrome with, like, just www.google.com as one tab, I watch memory drop by 250MB. It has become a bloated pig. It is ridiculous. A quarter gig of RAM for a browser to show me a page with nothing on it? That's obscene. And by comparison, Opera is 50, so one fifth the RAM consumption of Chrome. Chrome, I mean, I love Chrome. I know you do, Leo. I'm still using Firefox. And because we watch Firefox so closely, we watch them fight memory consumption. I mean, it's so easy for these things just to grow and grow and grow as they add technology. And it's difficult to keep that footprint down.

Yet here's Opera, very quiet, in the background, and actually more secure than any of the others. I think I probably need to explain that in a future podcast. But as I've been learning in the last couple weeks, Opera had been taking proactive measures that nobody else has been taking. For example, we talked about the problem with the 40-bit encryption, and why we were - web servers have moved 40-bit encryption to the top of the list because the cipher block chaining has been found to be susceptible to the so-called BEAST attack, B-E-A-S-T.

But the problem with 40-bit encryption was, as we covered not long ago, that it uses a stream cipher, which is why it's not subject to the BEAST attack. But the problem is that it uses the RC4 cipher that now had been further statistically analyzed. And remember that there was a chance, if you somehow could induce your browser to, like, be doing something in the background with a tab you weren't looking at, generating a lot of traffic, it would be possible to decrypt the beginning of the browser headers, which contains the session cookie, and that would allow a hijacking attack.

Well, Opera fixed this a long time ago. They proactively generate, they deliberately don't allow their browser to produce the same content at the front of each query. So it's been immune to this forever. Nobody really knows about it. I had to go digging around. It's like, what? Wow, that's very impressive. So anyway, I'm impressed with it. And, boy, it's really nice to have it launch so quickly and not chew up a quarter gig of RAM just showing one page.

Leo: Now, one thing that's interesting. They have announced, I don't think it's happened yet, that they're moving to WebKit. They're going to use a different engine on Opera. I don't think they're doing that yet, though. It's the same engine that Chrome is based on. So all of your love may be...

Steve: Well, and that actually - yeah, we'll see what happens with that, you're right.

Leo: Doesn't mean it'll be bloated because Chrome does other stuff.

Steve: It probably demonstrates how difficult it is to maintain a completely separate, state-of-the-art web page rendering facility. I mean, this is hard. I mean, it is - look, I mean, basically we're moving the OS into our browser. We're giving, with the advent of HTML5, incredible levels of capabilities in our browser. And, for example, the need for plugins is arguably going away. JavaScript is becoming a very fast execution environment. We no longer need Flash in order to play movies. Now browsers can render video and audio files natively. And on and on and on. And really nice animation stuff, like I created early last year in JavaScript.

And this is a perfect segue into something where I just kind of winced. The news was Adobe says it will contribute to Google's Blink browser engine. And I just thought, oh, please don't.

Leo: Don't contribute. No, thank you. Thank you, Adobe. No, thank you. I'm going to bring you one of my famous squirrel pies. No, thank you. We've made these for years, they're well beloved. You know, Chrome does have Flash built in. That's one of the things which I suspect adds to the bloat that Google does.

Steve: Well, and in fairness to Adobe, they have been participating in WebKit development, and they've been a useful contributor...

Leo: I'm sure they'll be fine.

Steve: ...to the project. So, yeah.

Leo: So this Adobe Blink, the fork that Adobe's doing, I'm told by the chatroom Opera is also adopting.

Steve: You mean Google Blink.

Leo: Google.

Steve: Yes.

Leo: And so this is - so Adobe will help with Google Blink, and apparently Opera's going to use Blink.

Steve: I think it must have been Opera. I remembered that there was another browser that said we're going to follow Blink also. So that would make sense. It'll be interesting to see what happens when Opera adopts Blink, how that changes everything I just said about Opera, to make it more Chrome-like.

Leo: One of the things about Blink, and one of the reasons Google says they went to Blink, is because WebKit has support for all sorts of stuff that you don't need to support - different hardware platforms, different processors - because it's an open source project. And they can eliminate...

Steve: Ah, so they'll be able to - they'd pare it down.

Leo: They said something like 15 million lines of code. So it might actually help your bloat.

Steve: Yay. That would be really good. It's just, boy, it's gotten big. Just as we were talking last week, we were discussing the collapse that was occurring as we were talking in bitcoin value.

Leo: [Whistling] Plummet.

Steve: It was at $90 this morning when I checked in order to update my notes. I tweeted a really nice article. Gizmodo produced a terrifically accurate, which I don't often say because, I mean, it's difficult to be terrifically accurate. This was. And this is Gizmodo.com. You might want to bring the page up, Leo.

Leo: Sure.

Steve: Gizmodo.com/5994446. And to any listeners - so it's Gizmodo.com/5994446.

Leo: All right.

Steve: It's just a nice page that explains what's happened in hardware. And tons, well, not tons, but seven or eight really nice pictures of crazy mining farms. Like the top of the - the image at the top of the page, you can click on that in order to get an enlargement. And it shows, I don't know, I didn't count them, but this vast array of little things, little boards, all cabled into some bizarre KVM octopod, I mean, like a hundred or so individually little things, all cranking away, trying to solve hashes. So I wanted to recommend this article in Gizmodo, Gizmodo.com/5994446. It's a great piece.

And shortly after we were talking about this, Leo, Mt. Gox shut down bitcoin trading for 12 hours, just in order to, like, stop...

Leo: Didn't they have a security issue? Wasn't that what prompted the plummet?

Steve: No, in this, I mean, they have had some, but in this case it was following the value collapse in bitcoin. They just said, okay, wait, we're going to stop here.

Leo: Like the market does. They just put a halt.

Steve: Yes, exactly.

Leo: A halt on trading.

Steve: And Mt. Gox is - 70 percent of all trades go through them. So, I mean, they're the big guy right now.

This is my last mention of my weekly mentioning of the SmushBox, which both you and I are Smooshed or Smushed or...

Leo: They're oversubscribed. They've done very well.

Steve: By more than 50 percent, yes.

Leo: Yay.

Steve: When I looked, they had $33,000. They were looking for 20. And we've got only, what, 46 or 45 hours left, so just shy of two days left, then this shuts down. I'm almost wanting another one for home. And I definitely will have one at the GRC servers I'll have to do all kinds of fun things with. But since I know Mark, I'm sure I can get another one, so that'll work. But anyway, they are oversubscribed by more than half. And we're all going to get Smush Boxes, whether we like what they're called or not. You can call yours anything you want.

Leo: Smoesh. Smoesh Box.

Steve: This is the best thing. This is just funny. This is wonderful. The acronym is, and you might want to bring it up, the URL that you can see right there in my show notes, Leo. The acronym is Completely Ridiculous And Phony CAPTCHA that Hassles for Amusement: C-R-A-P-C-H-A. In other words, CRAPCHA. So Crapcha.com presents you with some really pretty funny CAPTCHAs. And for all of us who have been faced with these things, where we're looking at it going, okay, you know, I am definitely human, I checked recently, and I cannot type that in. I'm sorry, I don't know if that's a one or a

lowercase "L" because it's smooshed in against the...

Leo: [Laughing] These are not intended to be entered by any human.

Steve: Oh, no. You can't enter them. They're just wonderful, though. It's just somebody who said, okay, let's have some fun with this. So we will create the CRAPCHA, C-R-A-P-C-H-A dotcom. Everyone should just go take a look when you get a chance because it's, I mean, and it's very reminiscent of things we've seen, and you're looking at it, going, okay, just give me another one. I'm not even going to try that.

Leo: [Laughing]

Steve: Coincident with today's...

Leo: [Laughing]

Steve: I know. They're great.

Leo: I hate CAPTCHAs. And we already have established they do nothing.

Steve: What is that black thing? Is it like a flying saucer or...

Leo: It's a smudge. It's a smudge. Oh. Oh.

Steve: Someday we'll be looking back, on Episode 800 we'll be looking back and going, yeah, remember when we were talking about that?

Leo: I'm going to put this on my web page. Because you can. They give you embed codes.

Steve: Yes.

Leo: So you can put this in your web page.

Steve: Yeah, it's wonderful.

Leo: How do I type that? What? What is that? A fishbone? What is that?

Steve: [Laughing] So our friend, Mr. Wizard, has updated his animations, also meant to

correspond with today's topic on VPNs. He's fleshed out his coverage of our original Episode 14. Now, remember, these are animations, computer animations to go along with the podcast. So the multi-animation series he has for Episode 14 and also for Episode 17, which covers the point-to-point tunneling protocol, which I'll be talking about here in a minute, PPTP, and also IPSec, IP Security, VPNs. So I wanted to give people a pointer to that. Remember, that's AskMrWizard.com is his site.

And, okay, now, Leo, you haven't seen this, and I'm reluctant to take the time to embed this in the podcast, but I really want to. This is Ellen DeGeneres, who did something just brilliant last week. Or, no, wait, this week. It might have been Monday. It's on her own YouTube channel, on Ellen's YouTube channel. And it is extremely funny, and it's about passwords [t.co/TfrjlZcOOa].

CLIP/ELLEN: I was looking around through the channels, and I saw this. I really love infomercials. I don't know if you love them as much as I do. But I found one, it's a new product that I want to share you. And, you know, if you have a hard time remember your online passwords, a lot of people have a lot of different passwords. This is going to solve your problems.

CLIP/MALE VOICE: Online passwords. There's just too many. And who can remember all those tricky combinations? So you stick them on your monitor, or you hide them in a drawer. But not anymore. Introducing Password Minder, the personal log book that takes the hassle out of passwords. Forget about sticky notes or scraps of paper because Password Minder has been specifically designed to organize and safely store passwords. You'll find them in an instant and never lose a password again.

Leo: It's like a notebook.

Steve: All it is is an address book.

CLIP/MALE VOICE: ...Password Minder. The alphabetical listing organizes all your usernames and passwords...

Leo: My mom uses something, oh, a little less organized than this.

CLIP/FEMALE VOICE: I don't have to worry anymore about security or identity theft. I now have all my passwords in one place. It's great.

CLIP/MALE VOICE: If you have passwords, you need Password Minder. So call now and get your very own Password Minder book for just $10.

CLIP/ELLEN: That's real. That's real.

Leo: That's real? That's real?

Steve: Yeah. But wait, no, keep going, Leo.

CLIP/ELLEN: Wait. You're telling me I can keep all my passwords in one place? In this

right here? And it's only $10? For half the price you could write all your passwords on a $5 bill. This is insane. Does this seem safe, to keep all your passwords in one place? In a place that's labeled "Internet Passwords"?

[Talking simultaneously]

Steve: Keep going. Keep going.

CLIP/ELLEN: I mean, what if someone gets their hands on your Password Minder? So I came up with this. It is Ellen's Internet Password Minder Protector. And what you do - yeah. You put it in here.

Leo: And you lock it. Actually, that's not so bad.

CLIP/ELLEN: You close it. And then it has a built-in combination lock right there, you see, on the side. And I know you're thinking, Ellen, what if I forget my combination? Well, if you order now, I will include this, and you can put it in there. It's the Password Minder Protector Minder.

Leo: It's the Internet Password Minder Protector Minder. A little book to put your code in.

CLIP/ELLEN: That's one place to keep your Password Minder Protector combination. And I have one more special offer. If you don't feel like writing down your passwords, send them to me, and for $10 I'll write them down for you. Don't worry about sending me your credit card information. I'll figure it out.

Leo: Oh, that's pretty good. I love it. I love it. You know, I've been doing that with my mom, today, this morning. She has all of her passwords in a document on her desktop called Passwords.doc. On her computer.

Steve: And my oh my, your mom is so sweet, Leo. I saw her sitting in your studio last week.

Leo: She's wonderful. So what we've been doing, and it's an interesting experiment, I installed LastPass on her computer, and we're going to put it on her phone and her iPad, as well. And I said, okay, now you only have to remember one password from now on, Mom. But you do have to remember this one. She starts to write it down. I said no. You have to remember this one. And everything else will be safe. So she starts to - so I said - so we came up with a process, a mnemonic process that she can recreate her password each time. I won't go into details about...

Steve: Yeah, because your name is not long enough for her to use as her password.

Leo: Oh, you don't even want to know what she used. It's a dictionary word. Well, I

mean, that's the password to protect her computer. And then on the computer there's Passwords.doc. So it's not so secure. Anyway, we're putting them, all the passwords in there. And then one by one, slowly over time, she's going to go to her websites. We changed the bank password, changed the passwords to something generated by LastPass, something long.

Steve: Good, good.

Leo: Her bank will not - will only allow letters and numbers, less than 15. But so we did that. But everywhere else I said check, make sure you have letters, numbers, upper and lower, special characters. And let's make everything 16 because why not? Make it 16 characters because you don't have to remember it, so let's make it nice and long. So it'll be a little process. And I'll be getting a few phone calls. And of course I put her LastPass password in my LastPass so it knows.

Steve: So you can recover...

Leo: So I can be...

Steve: You can be her password recovery.

Leo: I'm her Password Minder Minder.

Steve: So any of our listeners, I really...

Leo: That was funny.

Steve: You ought to see it. I did just tweet it recently, so you can find the YouTube link [t.co/TfrjlZcOOa]. I would imagine you could just go to YouTube and put Ellen's Password Minder Password Minder.

Leo: It's on her website. If you go to Ellen's website you can see it.

Steve: Oh, okay. Yeah, it's a great piece.

Leo: It's awesome. Awesome, awesome.

Steve: And I had a nice, speaking of great pieces, a note from a listener of ours, Stephen Adams, who sent, "Steve, I just wanted to say, wow. I've been a Mac user exclusively for better than 10 years and have not had access to any Windows machines in at least that time, only Mac and Linux."

Leo: Wow.

Steve: "When I heard on the podcast that it was possible to use VirtualBox to run SpinRite, I was very excited. I've been extremely busy, but sat down this morning to make it work, and it did. Amazing. SpinRite is now running on my iMac" - and he says "(2011)," so it's a recent one - "in a virtual machine booted from an external drive. I don't expect it to find anything, but you never know. And certainly, as has been testified to so many times, running it for maintenance purposes is always worthwhile. Great job. Thanks a bunch. From a faithful listener since Episode #1. That would be 400 episodes. Signed, Stephen." So thank you, Stephen...

Leo: Very nice.

Steve: ...for sharing your VirtualBox success on a Mac. That's actually happening a lot now. People have picked up on that and are playing with it on their Mac, which is cool.

Leo: So when we talked to this new advertiser, proXPN, when we said to them, well, I love the idea, we've talked about VPNs before, Virtual Private Networks. But we've got to get Mr. Gibson to approve it. We gave it to you to take a look at it. ProXPN.com/twit is the URL for our special offer. And you said okay, yes?

Steve: Yes. They're based...

Leo: It's using OpenVPN; right?

Steve: Yes. They're based in the Netherlands.

Leo: Oh, wow, I didn't know that.

Steve: Yup. They clearly, in my opinion, have their hearts in the right place. They look like they are here for offering what VPN users want, which is someone who can terminate their VPN connections somewhere and be both global and often local and trustworthy. So they have server locations in Dallas, Los Angeles, Seattle, and New York in the U.S. So, what, the Southeast, the West, the Northwest, and the Northeast. So pretty much good coverage of the U.S. And that's important, as we'll be talking about here in a minute, because when you have a VPN connection, it needs to go somewhere. And some VPNs are used, for example, to straddle corporate offices and satellite offices in order to allow entire remote networks to participate as if they were all in the same network, even though the traffic is actually bouncing around routers on the Internet. So there is the network straddling aspect.

But the other application, the typical end-user application, the one I have been interested in, is where you're somewhere unsafe. You're in a hotel. You're in a Starbucks with famously open WiFi. And we know that the term "open" is really, it's both good news and bad news because none of your traffic is encrypted in there air there. So what you need

is you need a VPN to protect that jump where your traffic is exposed, but it needs to connect to somewhere. So the idea is that you could use something like proXPN. And I've looked around. Remember we talked a long time ago about HotSpotVPN. And there's been some coverage of this stuff.

But I looked, and I like these guys, honestly, better than anybody I've seen. Outside the U.S. they've got locations in London, Amsterdam, and Singapore. And they're deliberately about the notion that people need privacy because, I mean, as a VPN provider that's what they're going to be about, and avoid censorship, avoid filtering, avoid any kind of exposure to your connection. They offer a free service which is capped at 300Kb. So it's a bandwidth cap, but it's free for life.

Leo: Wow. That's really good. I mean, and 300Kb is enough for when you're at the coffee house, and you want to check your email, or you want to do some browsing. It's not enough for streaming, but it's enough for basic Internet access. That's great.

Steve: Yeah, well, and I like it, too, because it allows - and clearly this is meant to be a loss leader. It's to get people in...

Leo: Yeah, they want you to pay for the full version; right?

Steve: To get people into the fold. Now, if you do the free service, that's OpenVPN only, meaning that, specifically - so it's both bandwidth capped and only the OpenVPN support. When you subscribe to their service, which they show it as 6.25, I think it is, or, yeah, 6.25 a month and that's $75 a year. But apparently you can get it on, like, on a month-to-month basis. So, like, 6.25. And they support both credit card and PayPal. So they do allow you to use PayPal to keep your credit information safe. And for first-time signers, they offer a seven-day money-back guarantee. So you can sign up, you can use it - and you can sign up through PayPal and try them for a week and just say, after a week, contact them and say this isn't what I expected, or I just wanted to see what it was about. I really didn't want to go any further. Please refund my 6.25. And they'll do so.

I'll be talking a lot here in a minute about OpenVPN itself. It happens to be what I'm using. I have OpenVPN clients installed on all my laptops, and I run OpenVPN servers both in my home network and in the GRC network. I mean, it is that secure. It is that safe. I have OpenVPN servers running, protected by certificates. And so, I mean, I'm confident in it being safe.

Leo: Well, let me do the ad. And then...

Steve: Well, yes.

Leo: Thank you for checking it out. So it is, it's a global VPN, which is nice. Works with almost any Internet connection. You're getting a secure encrypted tunnel through which all of your online traffic passes back and forth. You notice that it's using a 2048-bit encryption key, and the tunnel itself is 512 bits. Which is adequate; right?

Steve: Yup. It's actually way, way more than adequate.

Leo: It's way more than adequate. Any online application, including your web browser, your email, your filesharing, basically everything, instant messaging, it's all going through that encrypted tunnel. So everything you're doing while you're using proXPN is hidden, even disguising your physical location as it passes to their servers. They do offer, for the paid version, PPTP, as well, if you need to use that. So I mean, there are lots of reasons you might want to use this. You don't have to worry about your ISP's six strikes rule. You can eliminate any concerns about filtering, blocked websites, bypass geographic restrictions.

Steve: They have Tor support also.

Leo: Tor support. Software for Windows and Mac gives you more advanced control. For instance, you can select the programs and ports you want to route through proXPN. But it also works with iOS, Android. There's no app required for that. World-class support. So here's the deal. We're going to give you 20 percent off. You get the free - you can do the free version up to 300Kb.

But if you want to do the paid version, go to ProXPN.com/twit. ProXPN/twit. As you mentioned, normally $75 for an entire year for the pro version. If you go month to month, it's 10 bucks month a month, 9.95 a month. But our special offer will save you 20 percent off the lifetime of your account forever. Not the first year, forever. It's SN20. So at that point, using the yearly plan, you're talking 5 bucks, less than 5 bucks a month. And of course you cancel within seven days, as you mentioned, for a full refund. So 20 percent off for life, ProXPN.com/twit. But you have to sign up for the premium account and use the code SN20. I'm going to sign up right now because that's half what I'm paying for my current VPN solution. And of course, again, while they are a Dutch company, they have servers all over the world, including the U.S., and you can choose that.

Steve: Okay. So a couple clarifications. In fact, we'll just start talking about VPN stuff now.

Leo: Good. I'll take down the lower third, and you may go.

Steve: The PPTP protocol is not OpenVPN. So there's two that they offer. You only have access to OpenVPN for their free service. The reason the paid service gives you both is that what you really want for mobile, unless you happen to have an OpenVPN client in your mobile phone, but people don't right now, but iOS supports PPTP VPN natively, as does Android.

Leo: Oh, so that's why they offer it.

Steve: Yes.

Leo: I get it.

Steve: Exactly. So you sign up, and you get unlimited bandwidth globally for both protocols, OpenVPN, which you would install and use on any Mac or laptop, or even on your home machine. I mean, if you wanted to do stuff that your ISP couldn't see, that nobody could see, where suddenly your location was no longer where you are, but whatever server you have chosen to use, you can install this on your regular desktop system at home and VPN all of your network use through proXPN. And at the same time, when you are at Starbucks with your iPad or your iPhone, where you're using their WiFi connection, which is not secure, you can go right into the iOS control panel. There is built-in support. There's, like, VPN, and you choose one of three types. PPTP is the middle type. Put in your username and password, and you're connected through your mobile device with no additional client needed. And so that's why that's so very cool.

Now, okay. So, let's see. As I was saying before, the whole concept is one of tunneling. And I would recommend, if any of these terms that I use are foreign to people, we really, back at the dawn of this podcast, Episodes 14 through 19, covered this technology very carefully. The idea is that you can establish a connection between endpoints, that is, between you and somewhere else, or also, as I mentioned, between two complete networks with multiple systems. You establish a connection.

And then, in the same way that our browser uses SSL to encrypt the data which is flowing through that connection, including the use of certificates, which provide strong authentication that someone connecting to you actually is who they say they are, you establish an encrypted channel, and then the regular network traffic is pushed through this tunnel so that the world can see pseudorandom noise passing through the air if it's WiFi, or out of your cable modem and through your ISP. It's exactly as if you had a secure connection to a remote website over SSL. But in this case the link is using encryption, yet all of the network traffic, whether it's encrypted or not, is encrypted. And so that's the key. Nonencrypted network traffic like email, which is often not encrypted; also your DNS use.

Remember that when you, even though you may be going to websites which are SSL, you are often making queries to DNS. And DNS is not encrypted; It uses UDP protocol. And so anyone monitoring your use of DNS is able to see which domains your computer is looking up. And that's why this notion of all of your network traffic being funneled is crucial, because that means that, when your computer looks up DNS, that query goes out through the encrypted tunnel to the other end, comes out, goes and finds a DNS server, gets the answer, and sends it back through the encrypted tunnel so that essentially you just completely go dark relative to any external network traffic that your computer may have.

So there have been many VPN technologies that have been developed over time because this concept of creating a secure tunnel is sort of - it's fundamental to the - it's like a fundamental technology of what we could do once we have a public network. And we're saying, well, it's nice that we have a public network. Look how amazing it is. But, for example, a corporation might want to have satellite offices. And rather than having their traffic insecurely go across the Internet, they might want to essentially graft their satellite offices onto the main corporate network. So a VPN connection between a VPN server in the corporate environment and a remote satellite office essentially gives everyone in that remote network IP addresses on the corporate network.

Think about that again. So it's not like you have separate IPs. You're actually grafting all

of the network traffic across the Internet as if you were plugging into a router or a hub at the corporate headquarters. And so, similarly, when you bring up a VPN link, your computer's IP address changes to an IP that is assigned to it by the other end of the link. So it may be that they are using, for example, 10-dot network IPs. So that, for example, whatever, you were 192.168.something.something, you bring up this VPN tunnel, and you will find that you have a virtual interface on your computer which allows traffic to be routed to it. And it may have an IP, 10-dot something. Or they may well be slicing off IPs from their own publicly routed IP allocation.

So the notion of an encrypted tunnel can be - that's sort of basic foundation. We've talked in the past about point-to-point tunneling protocol, which is the one which has succeeded, sort of at the corporate level. You can get - Cisco routers will support point-to-point tunneling protocol as their native one. So, for example, if you wanted to create your own VPN and could configure a Cisco router, you could set it up so that it supports incoming point-to-point tunneling protocol connections.

The problem with using PPTP is that it is possible for people who wish to block the use of VPN connections to readily do so because PPTP uses well-known ports that aren't like web traffic or email traffic. And that's also the case with another common and supported by Windows mostly, L2TP is a Layer 2 Tunneling Protocol, another one offered by Windows but not as common and popular as point-to-point tunneling protocol.

So you're out and about and in a roaming mode. You have a couple choices. One would be that you connect to a service provider, an OpenVPN service provider, using OpenVPN. But yet another possibility, or something that gives you some additional flexibility, is it's now possible to use OpenVPN servers that are built into any of the firmware that can be flashed into consumer routers. The most popular OpenVPN solution uses DD-WRT as its firmware. And the Linksys Cisco E4200 V1 router is the one that most people are really comfortable with using DD-WRT. Over on the Tomato side, the Tomato firmware, ASUS has a router. The RT-N66U uses the Tomato firmware. And people are liking that best for OpenVPN.

So the idea there would be that, if you're using DD-WRT or Tomato on one of the routers that supports it, and you've got it set up and compiled with OpenVPN, then your router itself is a server offering OpenVPN connections from the public Internet. So you have a choice of, for example, if you're out roaming around, you could use a VPN service like proXPN when you want access, anonymous access to the world. But then you also have the flexibility, with the same OpenVPN client, to connect securely to home, and then your system, wherever you are, becomes an extension of your home network. You are on your home network. You get a 192.168 home IP. And it's like your computer were plugged into your hub and with complete security.

So, for example, you could connect to there and print something on your home network printer. Or if you've got filesharing and a bunch of shared directories, or you've got your NAS, your Network Attached Storage box there at home, all of those resources become available to you using an OpenVPN client on a system that supports it, and an OpenVPN endpoint server in specific router firmware that has been flashed. There are routers you can get now that are pre-Flashed with DD-WRT and the Tomato firmware, so that you're able to use them without going through the flashing process, if you're not comfortable doing that yourself.

But what we've seen is we've seen over the last eight years that the OpenVPN technology has continued to mature and become extremely stable. I mean, it's, as I said earlier, it's the VPN solution I have chosen, and I am using. I don't roam often away from home. But, for example, all the times that I've been up doing the podcast from Leo's place I've

been able to check in. And a couple times I've had some server issues while I was out roaming, and I had to connect into my network at Level 3 and be there as an admin. And so OpenVPN was the way I did it.

So that's the whole story, Leo, about where we are these days with VPNs and all the many options which are open to people, both using OpenVPN and PPTP. We've got a Q&A episode next week.

Leo: Next week, right.

Steve: And so I would encourage our listeners who are interested, who may have been, like, waiting for the right VPN service to come along. From everything I've seen, proXPN looks like the right solution. And you know me. I would not be saying this unless I had checked them out and believed it. I see no downsides. But if anyone has questions or feedback or experiences, GRC.com/feedback, and maybe we can talk about them next week.

Leo: Excellent. When you're at GRC.com, make sure you check out, of course, all the great stuff Steve gives away, including ShieldsUP!. And don't forget, of course, to buy a copy of SpinRite, right now.

Steve: Keep the lights on.

Leo: Make a yabba-dabba do, yeah. Episode 400. Congratulations, Steve. That's fantastic. By the way, we do this show every Wednesday, 11:00 a.m. Pacific, 2:00 Eastern, 1800 UTC on TWiT.tv. Watch live. You'll see some interesting things you won't see in the edited version. And of course, if you can't watch live, you can download a copy anytime, TWiT.tv/sn, or get those 16Kb audio versions Steve makes available, plus pure text transcriptions, the smallest version of Security Now!, on his website, GRC.com. Thank you, Steve.

Steve: Thanks, Leo. Great to be with you, as always, and we'll talk to you next week.

Leo: Take care. Happy 400th.

Steve: Yeah, thanks.

Leo: I'll send you a Cohiba.