Listener Feedback #164

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-397.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-397-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. Oh, get ready for this. We've got a Q&A episode. We're going to talk about security. We're going to talk about DDoS attacks. We're going to talk about telnet exploits. But we're also going to talk about coffee and Bitcoin and science fiction. Stay tuned. Security Now! is next.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 397, recorded March 27th, 2013: Your questions, Steve's answers, #164.

It's time for Security Now!, the show that's designed, carefully cultivated, and in fact proven, four out of five doctors recommend it, for protecting you online - your privacy, your security. And we thank this guy right here, the Explainer in Chief, Steve Gibson, for making it possible for six-plus years now. Hi, Steve. Happy Birthday.

Steve Gibson: Hey, Leo. Thank you. Yesterday was the big day for me, 58.

Leo: When you started this show you were just a young man of 52.

Steve: That's right. Actually, I feel better today than I did then. I don't really know why, but...

Leo: I know why, and you know why. You just don't want to say it.

Steve: Yeah.

Leo: Because of your regimen, your Vitamin D and your...

Steve: Before I turned 50 I started, I decided I was going to get serious about looking into nutrition and supplements and physical condition. And it's like, okay, I have the time now, I'm going to do it. And I've...

Leo: You're never going to die now, Steve. Never.

Steve: I've learned a lot, yeah.

Leo: You're going to live forever.

Steve: So a bunch of nice stuff this week. We've got a Q&A episode, our 164th Q&A. At the top of the news we've got both good news and bad news regarding Apple and authentication.

Leo: Oh, what a mess that was.

Steve: Oh, my goodness. Well, the bad news is a really great case study for us and our listeners because it was such a mess.

Leo: It was a cross-site forgery exploit, as I understand it.

Steve: No, not at all, actually.

Leo: No.

Steve: It was just a mistake. So it had nothing to do with cross-site anything. It was just a very simple web app programming mistake. Okay, so this involved an "I forgot my password" problem. So this was so-called "password recovery" at Apple. And until this came to light - and to Apple's credit they shut it down quickly, that is, within a day it was fixed. But it was so easy to fix because it was such a glaring, obvious mistake. So, I mean, this is What Not to Do 101 on Internet security. You'd go to iforgot.apple.com. And you went through a series of steps. You give them your email address for your registered account, and then they want your date of birth. So you put that in. Then you answer two security questions which you had previously provided, obviously, the answers to before. Then you enter the new password you want to use for your account.

Well, the mistake they made, first of all - let's back up a little bit and remember how we've sort of forced the web, which was originally designed to deliver content, how we forced it to accept content, that is to say, like the answers to these questions, the email

address, the password and so forth. The Internet never was designed for this, really. It was designed as a read-only medium with links, hyperlinks - oh, what a concept - that you click on, that take you to other read-only pages that may have their own hyperlinks that you click on, and they take you to others. So that was the original concept.

And then someone said, what if we want to, like, log in to, like, we want to protect some of these pages so just not everybody can click on the links and get to them. And then the gurus of old said, "Hmm. Really? We hadn't really planned for that." And the people said, "Yeah, but wouldn't that be cool?"

So they said, okay, how about this? We'll take that regular URL, that's the http:// with a domain name and then the whatever it is afterwards, the tail that specifies the page. And then we'll put a question mark on the end. And then anything after the question mark, the server will ignore. That is, the question mark ends the address of the page and starts stuff the user provides. Whatever they want. And then we'll enhance the HTML definition with forms. We'll have boxes you can fill in, buttons you can press, that kind of stuff. And the form will stick its data after the question mark. So the server will not care what's after the question mark, and then an application which we've added to the server will look at the stuff after the question mark as the data from the user.

So this kludge, which is the only thing you could call it, is what happened. And then they said, well, but, you know, what if you wanted to, like, fill out - wanted to submit a letter to somebody? You can't put a whole letter after a question mark on the URL. That just goes on forever, and there's got to be a limit. So they said, yeah, okay, that's a good point. So then they created another verb. Normal verb was "get," saying I want to "get" a page. They created a new verb called "post." And there the idea was you would, after you were through specifying the page you wanted this to go to, you would use the verb "post," and then you could sort of append as much stuff as you wanted to at the end of your query, rather than off the end of the address. And so that's what we have today. In this day and age, that's what we've got.

So both approaches are used. Apple was using only the original one, the get-based approach, where everything that the user submits is after the question mark in the URL. Now, that's not a problem per se because either our - you know, our part of the query that you send to the server, even though it's not really a query anymore, it's more of a, here you go, submit.

But the mistake Apple made which is so rudimentary is that anyone - anyone. Doesn't take a genius. This is not one of these incredibly complicated, okay, how did they figure this out things. Anyone looking at the traffic to and from the user and Apple would notice that that final submission of the new password didn't really need all of the previous stuff. That is, you could go to iforgot.apple.com pretending to be somebody else. All you had to know was the email address they used, which you could probably guess because it's probably their email address, and their date of birth, which of course is public record often. I'm a little uncomfortable that my Wikipedia page has it listed. If it didn't, if it wasn't already public, I wouldn't have mentioned that yesterday was my birthday because I would rather that kind of stuff not be readily available because it can be used, exactly like this, for exploits.

With only those two pieces of information, because they did everything through these simple "get" queries, you're able to skip, entirely skip the requirement for the two security questions. You don't even need those. You're able to synthesize the final submission of your new password without needing that because an analysis of the back-and-forth transactions to iforgot.apple.com made it clear to anyone, even just looking at the HTML, looking at the View Page Source option in your browser, you can see how it's

assembling the data that it's going to send back.

And so, armed with only a person's email address and their date of birth, until this was fixed - which was, as I said, immediately after it was publicly revealed - it was possible to change anyone's Apple password to anything you wanted, and in that process take over their account. So that was Apple's revealed, publicly revealed screw-up of the week. That's the authentication bad news.

Coincidentally, they also gave the world authentication good news. And we are really hoping that the guy who implemented the good news had nothing to do with implementing the bad news because we want them to have done this right. Apple has now joined the growing group of major sites like Facebook and Google and Microsoft to offer two-factor, or at least two-step authentication. Some purists have said, well, it's really not two-factor because you may be trying to use the same device you're trying to log in as the device you're authenticating with. It's like, okay. So it's two-step. But it certainly does dramatically raise the bar on, for example, preventing like the Mat Honan attack. And they've exactly done so.

Gregg Keizer, who reported the story in Computerworld, started his nice report sort of summing things up. And I'll just read the first few lines. He said: "Apple this week followed the lead of rivals like Facebook, Google and Microsoft" - I don't know that they're such rivals, but still - "Facebook, Google, and Microsoft, offering two-step authentication to help customers secure their Apple IDs against hacking. The new feature is designed to block unauthorized changes to iCloud or iTunes accounts, and keep hackers who steal Apple IDs from purchasing digital content or hardware using the credit cards stored in customers' iTunes and Apple Store accounts. iTunes users in particular have complained for years about security so lax that hackers have easily hijacked their accounts to run up big bills. Security experts this week commended Apple, even though the company was slow in pulling the trigger."

So they did a couple good things, I mean, sort of like extra good. For example, they're not using SMS, that is, simple texting on phones because, as we've discussed with Brian Krebs's SWATing adventure or misadventure last week, cell phone is prone to spoofing, and SMS messages can be spoofed and have been spoofed. And so it's better, if you have an infrastructure you can use, not to fall back on cell phones. Most companies...

Leo: Actually, they do use SMS if you don't have Find My iPhone. They can use both.

Steve: Oh, if you don't have Find My Phone, okay.

Leo: They used SMS with me. I had both, and they used SMS.

Steve: Oh, okay. So they do allow you to use their existing infrastructure, Find My Phone, which doesn't use SMS. And so, for example, it allows you, if you didn't have a cellular-equipped device, like any of the iPads that didn't have cell built in, then you're still able to use this as an authentication loop. And then they have removed, sort of in response to the Mat Honan horrific adventure that we talked about at length, they removed from Apple Support, as I understand it, the ability from Apple Support to reset passwords. Nothing you can do in terms of social engineering any longer can convince Apple to reset your password.

The way they've made that practical is they also give you a long, 14-character, backup emergency recovery key which you're able to use if, for whatever reason, you can't use the iOS device which is assigned to receive the passcodes, or it's been lost or stolen or whatever. Which I really think - we've seen a couple people do this. I know that Google Authenticator does the same sort of thing, where you get this really big, inconvenient, you would never want to use it on a regular basis, long key. But the point is that's your emergency recovery key. You print it out and stick it in a drawer somewhere so that you have that as your ultimate fallback. And then you normally use a convenient real-time feedback loop of some sort in the regular case. So congratulations to Apple for strengthening this. That's a good thing.

Leo: Yeah, and I turned it on right away. Although, in theory, that old hack doesn't work, so you don't have to worry about that. But who knows.

Steve: Oh, yeah. They closed that immediately. But, yeah, I agree. I think that Apple users have been low-hanging fruit in the past. And so it makes sense that Apple is doing this. And I think it's great, too, because Facebook has great penetration. Apple has great penetration. Certainly Google does. We're seeing the large movers educating the public about increasing their security. And this is just all good.

In a weird and unfortunately maybe related to us event, the day after we talked about the Canadian-based TD.com, I guess they're related to TD Ameritrade, Leo?

Leo: Yeah, it's Toronto Dominion Bank that's now - I think it's considered an American bank, despite the word "Toronto" in the name, yeah.

Steve: So that was easywebsoc.td.com. They are even now off the 'Net.

Leo: What? Really?

Steve: Apparently, yes, even now. I tried before the podcast. Easywebsoc.td.com, if you try to go there, it says "Service Interruption: We are currently experiencing systems issues due to an external interruption."

Leo: Oh, that sounds like a DDoS.

Steve: That's what it has been, apparently. "Support teams are working to restore services as quickly as possible. This is a service interruption issue which we are monitoring closely."

We'll remember that last week I talked about them because somebody tweeted that this was their bank, and they went to SSLLabs.com, and they got an F. And so we went into some detail into the reasons for their F grade, which were that they're still supporting SSL 2.0. They're supporting 40 and 56-bit symmetric key ciphers among the cipher protocols that their server is willing to accept from a client, which are regarded as too weak to be secure these days. And they haven't reordered their server's preference such that they're using the cipher-based chaining with the weak SSL and the early version of

SSL and TLS, which makes them subject to the BEAST attack.

So I'm wondering if some people who listened to the podcast thought, well, we should punish them for their lack of security by holding them off the 'Net. And if that's true, it's been effective because it's been a week now that easywebsoc.td.com has been unavailable as it once was. They do have a link at the top of that page that takes you to another site which has always been there. So maybe this is not their main entry portal or I don't know what. I know that it certainly used to be online and is not.

Leo: You know that there's a massive DDoS going on right now, kind of a global DDoS. I'm sure you'll talk about that.

Steve: Yeah.

Leo: It's not related, I presume. I don't know.

Steve: I assume it's not. So we've spoken a couple times in recent years about the fundamental - well, actually we've spoken many times about the fundamental tension that exists between our feeling of our own rights to privacy, the U.S. constitutionally guaranteed rights of privacy, and the really understandable need that law enforcement, legitimate law enforcement has to pursue, through evidentiary means, criminals. And this creates tension. We spoke a couple years ago, in 201l, Valerie Caproni, I remember, was at the time FBI's general counsel. And it was her speech to the American Bar Association, the ABA, that worried me about the future of even being able to encrypt with a VPN because those encryptions are something that work against the law enforcement ability to monitor everything that they want to, which is what they want.

Slate just carried a very good article, Ryan Gallagher reporting for Slate, about the new FBI general counsel Andrew Weissmann's statements in front of the same body, the American Bar Association, in an article titled "FBI Pursuing Real-Time Gmail Spying Powers as 'Top Priority' for 2013." And so I just want to share this, it's not very long, because it perfectly characterizes where we are.

Ryan wrote: "Despite the pervasiveness of law enforcement surveillance of digital communication, the FBI still has a difficult time monitoring Gmail, Google Voice, and Dropbox in real time. But that may change soon because the Bureau says it has made gaining more powers to wiretap all forms of Internet conversation and cloud storage a 'top priority' this year." "Top priority" was their words.

"Last week, during a talk for the American Bar Association in Washington, D.C., FBI general counsel Andrew Weissmann discussed some of the pressing surveillance and national security issues facing the bureau. He gave a few updates on the FBI's efforts to address what it calls the 'going dark' problem - how the rise in popularity of email and social networks has stifled its ability to monitor communications as they are being transmitted. It's no secret that under the Electronic Communications Privacy Act, the feds can easily obtain archive copies of emails. When it comes to spying on emails or Gchat in real time, however, it's a different story.

"That's because a 1994 surveillance law called" - we've talked about CALEA in the past - "the Communications Assistance for Law Enforcement Act (CALEA) only allows the government to force Internet providers and phone companies to install surveillance

equipment within their networks. But it doesn't cover email, cloud services, or online chat providers like Skype. Weissmann said that the FBI wants the power to mandate real-time surveillance of everything from Dropbox and online games" - and he says, ("the chat feature in Scrabble") - "to Gmail and Google Voice."

Leo: Yeah, crooks plan a lot of their heists on Words with Friends. I know that. That's where we go. That's our secret spot. We meet there. Actually, that's a good idea, if you're a crook.

Steve: I was thinking the same thing. It's like, hey, we'll use Scrabble Chat.

Leo: I would like to play some Words with Friends with you, if you know what I mean.

Steve: He says: "Those communications are being used for criminal conversations," said Weissmann.

Leo: So is everything.

Steve: I know.

Leo: Stop it.

Steve: Leo, I know. I just wanted...

Leo: Did you see this? Here's one. Look, this is from Reuters. "U.S. plans to let spy agencies scour American finances." The Obama administration is drawing up plans to give all U.S. spy agencies full access to those databases, those central databases that have all of our financial records in them. Apparently, though, the FBI's had this all along. So I don't know if your email or your Words With Friends chat is more revealing than your financial records.

Steve: Well, probably all of the above, Leo.

Leo: Yeah, they have it all. Just forget it. It's too late.

Steve: Yeah. So anyway...

Leo: We should fight, I guess. But I think it's hopeless. I've given up.

Steve: Well, I think this sets a useful context for the conversations that we have on the

podcast for - the tradeoff in going the extra measure to encrypt your cloud storage on the client side, as opposed to trusting your cloud provider to do it, is a perfect example. And, again, not all information is the same. Many people want to store stuff in the cloud. They want the convenience of that. And it's just random stuff that they don't - they don't care if the FBI rifles through it. Fine.

At the same time, for just the sake of privacy, for example, I'm backing up GRC's corporate books to Amazon nightly using Jungle Disk, and it's working beautifully. And I have an encryption key that I had my own passwords page make for me, so god help anybody who tries to brute-force that. I know how Jungle Disk works. I know it's doing TNO-style encryption. So all we're sending up there every night is completely pseudorandom noise. And I love the convenience of it. I love the low cost of it.

And, yes, it's not as easy as simply having Dropbox clone everything everywhere. And there are ways to do pre-encryption technology with Dropbox, but it takes a little more. So I just - this sets the tone, I think, against which our listeners make their decisions about how much they care about this. So that's why I think it's worth discussing.

Leo: Yeah. I wish there was something we could do about it. I feel like it's just - it's, like, over.

Steve: I don't disagree with you, Leo.

Leo: They're so hard to fight. And the fact that this data's all been out there, and now it's consolidated into big databases. I just read an article, I thought it was fascinating, in Nature magazine. Data scientists took location data only, anonymized location data - did you see that?

Steve: Yup, yup.

Leo: And with four points, that's all, they had 95 percent success in identifying individuals. So let's say the fifth point, they observe you at a fifth point. If they can go back and say, okay, we see him now there. Where was this person four points ago? They've now got you.

Steve: Remember the size of that new facility the NSA is building in Nevada? I mean, that thing is unbelievably big. And it's full, I mean, it's just for data storage.

Leo: It's all big data. It's all about these machines have now gotten fast enough, data big enough, and we have enough data points now...

Steve: And hard drive storage is so incredibly inexpensive.

Leo: And it's insufficient now to say what everybody's been saying all along, which is, well, but we anonymize the data. As we now know, algorithmically, you can't

anonymize data; that enough data points, you can identify it.

Steve: Yeah, well, for example, I mean, your example in the Nature article was perfect. Location, nothing but X and Y coordinates, nothing is more anonymous than X and Y numbers. Yet they just demonstrated, four of those, and they pretty much know who you are.

Leo: Four.

Steve: Yes.

Leo: Four. Can you believe that? Even that is a measure of how effective our computer algorithms are, that they can take these four points and get 95 percent accuracy. Probably six points, and it's a hundred percent.

Steve: I'm stunned by Google, just Google search. It is amazing to me what I can find, that I can - I just put a few words in for a page that I wish existed somewhere, and there's a list of them. It's amazing, when you really think about it.

Leo: It is amazing. What a world. What a world. What a world.

Steve: So speaking of amazing, I'm really pleased that Firefox, that is to say Mozilla, and Google have a competition going on because we the users are the winners. I mean, we are clearly seeing an evolution of applications off of the traditional desktop model into the cloud. And the browser is our portal, and the browser is becoming our engine.

I got a neat text from SeanT6. And normally I check people's real names so that I can just say, okay - his Twitter handle is @SeanT6. And so when I went to look at what is his name, so I could quote that fairly, his public description for his Twitter account says "My name is Shawn" - actually it's S-h-a-w-n - "and I'm an English geek. Yep, I'm from England, where the tech news is limited. Thank God for Security Now! and TWiT Network podcasts." I thought, well, that's a nice handle to be broadcasting in TWiT. So thank you, Shawn.

Anyway, he pointed me at some news from last night, which is the most recent Firefox Nightly build, which they're continually pushing out and people who really want to be on the bleeding edge can play with. And this was 22. 22 is Firefox version slated for this summer sometime. So they're already working on something that we'll be talking about going live - I think I'm on 19. I think that's where we are now in the normal. I'm not needing to be on the bleeding edge. I want all my 88 open tabs to be stable.

So anyway, what they just rolled out in the most recent Nightly is a new technology for their JavaScript engine called OdinMonkey, O-d-i-n-M-o-n-k-e-y. And it's interesting to me because it's - I was a little distraught over the direction Chrome took with their superfast acceleration because, as I understand it, it's native code, is what they call it, where they're allowing you essentially to run, like, Intel coded apps in the browser, which, okay, for one thing it breaks compatibility because nobody else's browser

understands that.

So I'm less comfortable with what Google has done than with this which the Mozilla guys have done, which I think is very clever. What they did is they looked at JavaScript. Now, JavaScript is designed to be easy to use. So you can just sort of write some script, and things just work pretty easily. It's also powerful enough that a real programmer can do some amazing stuff. Not to toot my own horn, but we remember the animation that I wrote showing hard disk wave forms coming out in real time and pulsing and so forth. That was GRC.com/animation.htm, I think. And so JavaScript is both simple to use and powerful, which is not always an easy thing to achieve.

But JavaScript the language achieves that at some substantial cost in performance because it's having to do all types, all kinds of behind-the-scenes work: variable type conversion. It manages memory for you. There's no explicit, like I need some memory, now you can have it back. JavaScript just does that. So there's something called "garbage collection," which is memory that's been released. It needs to keep track of reference system memory so it knows, if no one else is going to reference the memory, then it can free it. All of that is expensive in terms of runtime at the benefit of the programmer not having to even know about that kind of stuff. Traditional programmers do it themselves. The newer dynamic languages do it for the programmer at some cost.

So what the Mozilla people did with this OdinMonkey project is there's something called "asm.js." And "asm.js" is a declaration, that is, just a line that you can add to existing JavaScript that declares that you are a programmer who is willing to abide by some strict rules of coding, and you're going to only use a proper subset of JavaScript - sorry, I need to make sure I don't confuse that, JavaScript - and in return for you being disciplined in your coding and the language being reduced to a subset and your making this declaration, the forthcoming Mozilla and Firefox will give you unbelievable performance. I saw the numbers, and it's orders of magnitude faster, for example, than where Chrome is today.

Now, Chrome is moving forward. I mean, it's already incredibly fast. And that's why I say I'm happy that there's this competition. And of course also there are some cross-fertilizations. Not like there are teams that don't share. All of this is open. And so they're able to take each other's good ideas and employ them.

But so essentially what they've done is, by allowing a programmer to say I'm going to restrain myself and restrict myself to things that are not expensive to do, it allows the system to compile that declared code ahead of time. They use the acronym AOT for Ahead of Time compilation. And it screams. And the benefit of this is it's still compatible. It is, if you fail the browser's verification pass over your code because you broke some rules, then it says, sorry, cannot honor your pledge because you haven't honored your pledge. So we're just going to treat this like regular JavaScript and keep you out of trouble. So it's still completely cross-platform and completely cross-browser. Yet, if you have a browser that is aware of this, and if you play by the rules, you can write applications in remotely delivered pages that just outperform anything. And so this is a neat move forward.

Leo: There are other solutions like this. I think this is kind of a general thing that everybody wants to accomplish because JavaScript itself is so irrational. They're trying to rationalize it.

Steve: Yeah, it is, yeah. I mean, it's unfortunate that it is as sloppy a language as it is. I

mean, it's not easy to corral it, as you say.

There were two things that I noted on Kickstarter in the last week. One I tweeted about, which was very cool. And I know that people who follow me picked up on it, and many of them tweeted back that they were glad for it. There's actually, everyone has heard about 3D printers, of course. This is a - get this, Leo - a 3D printing pen.

Leo: Oh, I know. Jeff Jarvis ordered one.

Steve: Yes.

Leo: It's so cool.

Steve: It is so cool.

Leo: Yeah. It's a Kickstarter project.

Steve: Yup, it's a Kickstarter. I tweeted, "No wonder this Kickstarter was seeking $30,000 but now has $2,319,739 pledged."

Leo: It's gone up since you've checked. It's now 2.344 million.

Steve: Yup, exactly. It's got 26...

Leo: 3Doodler, it's called.

Steve: Yes. Anyway, I tweeted the link [t.co/n3XFL0MvL7]. If anyone is interested and wants to see it, there's a beautiful video at Kickstarter. It is closed now. When I tweeted there were 33 hours remaining, which was enough time for people who were following my Twitter feed to see that and jump onboard if they wanted.

Leo: All it's really doing is just extruding quick-drying plastic. And so you can draw in three dimensions.

Steve: So it must heat. There must be a battery-operated heater that brings it up to melting point. But what's cool is when you see the guy, like, moving the pen around in the air, and it's leaving, like, a coil behind it.

Leo: It's really a great idea.

Steve: Oh, it is just so clever.

Leo: Yeah, yeah, yeah. They're going to - this guy, he's going to be speaking at LeWeb in London in a couple of - in about a month. Very interesting. And Jeff Jarvis did order one, so I expect TWiG will have many demonstrations of 3D art.

Steve: I'll remind people who are not Twitter followers that on the web we've got a nice friend of the podcast who is chronicling all of my tweets. And I created a bit.ly shortcut, bit.ly, and then just my Twitter handle. So it's bit.ly/sggrc. And that will bring you up, and so anyone can find the things I have recently tweeted, the most recent of which, I believe, as of the time of this podcast, is a link to this thing on Kickstarter, which I would encourage people to check out the video.

Leo: 3Doodler.

Steve: It's, oh, really cool.

Leo: Yeah.

Steve: Now, not nearly as popular, but still I think interesting for people, is something that Mark Thompson told me about. Our buddy Mark Thompson, AnalogX, designed this himself, for himself, to meet his own needs, and then thought, you know - and he and I chatted about this. He looked all over the 'Net. There were a couple bad implementations that just were not done correctly. Mark wanted an automated way of sending and receiving SMS messages for his own web-based stuff that he's doing. There wasn't anything.

So he talked to a couple friends of his. He's got one friend, Earl, who was actually the winner of Survivor one year, and a talented engineer KG, who's in Santa Monica. They've put together a Kickstarter called, unfortunately, SmushBox. I don't know what - I guess it's like it's SMS, it's supposed to be. It's supposed to be SMS Box, but it's S-M-u-S-h Box, SmushBox. I know.

Leo: It's all about the name, you know.

Steve: I know. Well, in that case they're in trouble. But I'm one of the backers. As of this moment there are 46...

Leo: Oh, you've fallen for the Kickstarter thing, haven't you.

Steve: I've done Kickstarter a couple times. And it's never been a problem for me. I think you've not had such good success.

Leo: No, nothing but flop-olas.

Steve: So I wanted to tell people that - oh, and actually the pressure-sensitive pad stylus was one of my favorite things that these guys did. They did a good job of that. But anyway, so what this is is an SMS gateway in a box. They have a deal with T-Mobile, and so it's preregistered to T-Mobile. I think it's maybe like 25 bucks a month, Mark said, in order to pay for this. You have unlimited SMS texting. The hardware is beautiful. So I would encourage people, it's SmushBox.

Leo: This is so you don't have to have a phone?

Steve: No. The idea would be, if you have any kind of a web service, where for example you'd like to do two-factor authentication, multifactor authentication...

Leo: Oh, you could use this, tied to your web server, to send SMSes. I get it.

Steve: Yes. And actually a couple of these things are USB-based.

Leo: Can I send thousands of text messages?

Steve: Yes. Yes, you can.

Leo: So what I can do is I can have a SmushBox attached to our calendar. And we can ask people, hey, if you want a text message when Security Now! is about to start, we'll send one out.

Steve: Yes.

Leo: Maybe I should order one of these.

Steve: Yes.

Leo: See, that's the thing. It's not ordering one that you're doing here. You're just giving them some money to support their development.

Steve: Well, and so I'm saying I know these people. I mean, the hardware works. KG has been producing hardware for a long time. Look at the video. It's just a gorgeous thing. I mean, you just want one when you just look at it. It's just...

Leo: That's how it starts, Steve. I'm just warning you. I'm just warning you.

Steve: But this is different. I mean, this will happen. Oh, and what I wanted to mention was that it's actually a net - it is a web server itself. So you don't hook it by USB to your

server. You put it on your network. And so it it's - you have to go into all the details. The page goes on and on and on. There's a video there. Anyone who's curious what Mark Thompson looks like, you can see Mark Thompson finally because he appears on the video. But anyway, I think it's a cool thing. I would love my server to be able to receive SMS messages from me.

Leo: It's got Cylon lights. What could be wrong?

Steve: I know. And the Cylon lights change speed. I said, okay, Mark, what does it mean when it's going slow versus when it's going fast? He says, I don't know.

Leo: That's Mark Thompson right there in the grocery store.

Steve: Yes.

Leo: So he's part of this team?

Steve: Yes.

Leo: Oh, that's different.

Steve: Yes.

Leo: So he's like the software guy.

Steve: He designed the first one. He prototyped it. He built one for himself, and then he said...

Leo: Well, that's different. If it came from AnalogX, all right.

Steve: Yeah.

Leo: Yeah. Can I show you the crap that I've purchased? "Purchased" is the wrong, perhaps, word to use for the stuff I've...

Steve: Just so that I make sure people can find it if they want, the Kickstarter, I don't know if putting SMuSh in is enough, it's Smart SMS Texting for Everyone, the SmushBox.

Leo: Yeah, I just did "smush" in Kickstarter, and I found it.

Steve: Okay, good. SMuSh in Kickstarter.

Leo: Now, 225 bucks for your SmushBox.

Steve: Well, yeah. And it's, I mean, it's a real piece of equipment. It's a network appliance. It's a web server.

Leo: Hey, I know. It should be expensive. But I'm just saying. And giving them money does not guarantee you'll get one, as I've learned. So you're funding the backing of this. There's no guarantee anything will ever happen. I just wanted to give people this disclaimer because even Kickstarter says we're not a store.

Steve: Right.

Leo: You're supporting this development, but there's no guarantee you will actually get a project - get a product.

Steve: I would be a little more worried about the 26,457 backers of the 3D printing pen.

Leo: 3Doodler? Yeah.

Steve: Yeah, I think it's very likely that anyone who wants a SmushBox is going to have one.

Leo: I'm ordering one right now. I don't even know why. Maybe I'll just have it in my house.

Steve: It's just - it's cool, Leo. Look at it. Oh, my god. It's a beautiful piece of hardware.

Leo: That's what worries me.

Steve: No, it's real.

Leo: Okay. It is Mark Thompson, AnalogX. He's the real deal.

Steve: Yeah, it's going to happen. And as I was going to say, I would love - I already receive text messages now when someone buys a copy of SpinRite. My phone goes yabba-dabba-do, famously. It's funny when we're at a restaurant, too, and the phone suddenly does that. People go, okay, this guy is...

Leo: Yabba-dabba-do. Do you get chills when they do that?

Steve: So I would like to be able to send messages back, have some, like...

Leo: Oh.

Steve: Yes.

Leo: Yeah. I have no idea how I'll use this.

Steve: And this goes bidirectional. Well, just exactly like you said, Leo, you could arrange - you could allow people to subscribe to text messaging notifications...

Leo: That would be kind of cool.

Steve: ...five minutes before the show starts.

Leo: And this needs a phone line? What does it need?

Steve: No, no. Just...

Leo: T-Mobile SIM.

Steve: No, it's built-in. It's ready to go. It comes preregistered with a T-Mobile account. So you tell them, you set up an account with them for 25 bucks a month, and you get unlimited texting, in and out, bidirectional, and then just click it onto your network.

Leo: Well, there's still time, if you want to get a SmushBox. I just bought the early SMuSh kit. Does that mean I have to assemble this? Should have read that more closely. Some assembly required. I'm not going to have to solder this sucker, am I?

Steve: No. It's just...

Leo: Like the PDP-8? When they say "kit," I hope they mean - let's see. You've selected - Kickstarter is really the first - but, yeah, full SMuSh kit, which includes activated SmushBox, installation and management software, cables, unlimited texting with unlimited keywords. We'll also throw in one of our embroidered SMuSh hats. That's what put me over the top. I want the hat.

Steve: Maybe you can get a mini hat for your little Leo in front of you.

Leo: No, because it's AnalogX I believe. I believe.

Steve: I did the $225 package.

Leo: That's the one I just did. Yeah, there's still time to get in on that, if you hurry.

Steve: Yeah, 10 of 40 are left, 10 of 40 are left.

Leo: Two people have done it since you started talking about it.

Steve: The SMuSh kit early.

Leo: Yeah, the early SMuSh kit. Which they say will be available in June.

Steve: I believe it. I mean, there's the hardware. Just scroll down. Keep scrolling down, Leo. They've got pictures of it all.

Leo: Oh, yeah. It used to be on Kickstarter you could do 3D renderings, and Kickstarter had to kind of put the kybosh on that, said you actually have to have a prototype, working prototype. You can't just do a 3D rendering. So what I could do is have people sign up, and then I would send you a text. If it were 10,000 texts, would it get mad at me?

Steve: No.

Leo: It says "unlimited texting with unlimited keywords." What could possibly go wrong?

Steve: Well, and imagine...

Leo: Until it's outlawed by the federal government.

Steve: You do a page on your site where someone creates, like, signs up. And then they've got checkboxes for all of your podcasts.

Leo: Right, all you want, right. And we'll send out a SMuSh whenever it's your turn.

Steve: Well, no. You have a checkbox for when the live recording begins and also for when the podcast is available.

Leo: Oh, I like it.

Steve: Yeah.

Leo: All right. Radford, make it so. See, I've got an engineer guy now.

Steve: And now you've empowered him with the technology for it to happen.

Leo: So you've always been able to do this through the phone companies, but it's normally quite expensive.

Steve: And that's what I'm doing now. I'm having my server send me email to my synchronized Verizon email address, and then that turns into a text message to my phone. It's like, eh, okay. It works. But this is the way to do it. And this is bidirectional. I can't send it back, and this works both ways.

Leo: We'll have several levels of SMS notification. We'll have one when Leo enters the building. We'll have one when Leo's actually sat down at the microphone. We'll have one when the preshow begins, and we'll have one when the actual show begins, and then we'll have one when the show is out as a podcast.

Steve: Perfect.

Leo: I like it.

Steve: And then you can do a survey of how quickly the checkboxes are turned on and then how quickly the checkboxes are turned off.

Leo: I don't know what happened. We had 20,000 subscribers yesterday. No, I think this actually could be quite cool. I hope they don't, like, it could be used for spam. But I guess that's up to T-Mobile to police; right? They would disconnect you if you start spamming.

Steve: Yeah, they would look at what they were doing. And if they were getting complaints from people, then they'd say, oh, okay, this seems to be a problem.

Leo: Yeah, this isn't okay. Because I'm starting to get a lot of text spam now. In fact, that's a security note. I think CERT was warning people, 60 percent of all cell

phone users now get text spam. Most commonly it contains a link that, if you click the link, of course, you go to a page that usually has malware on it. But sometimes it could be worse. Sometimes it could, if you - I get one now every day saying we'll lend you money. Great, thank you, just what I want. And it says, "Text STOP to end message." And I know that the temptation is to text them back STOP. But one of the scams could be it's a $35 text message. Right?

Steve: Oooh, yes.

Leo: You have to be very careful because there are offshore companies that will, if you send a text message, charge you. And so that's one of the things. So CERT was saying, whatever you - just delete it as quickly as possible. Do not click the link, and do not respond.

Steve: Good, I'm glad everybody heard that.

Leo: And it's illegal to do this. And JBR is saying, well, the carriers require that SMS senders actually honor the STOP requests. But these guys are pirates. They're fly-by-night. I don't think that they're, yeah, oh, yeah, we're going to honor the STOP request.

Steve: And as soon as they get blocked, they'll just move identities.

Leo: Just move to another - exactly. The guy keeps calling me Michelle. I don't know why.

Steve: That's your tipoff.

Leo: I'm not Michelle. I want to text him back. Hey, it's Leo. Would you mind fixing...

Steve: Maybe it's supposed to pique your curiosity. Like, wait a minute, why? I wonder what is the back story here.

Leo: Yeah, who is this guy?

Steve: So Ron Thomas tweeted me the news, that I wanted to share, that Mark Russinovich's two novels, "Zero Day" and "Trojan Horse," are now available on Audible. So for people who have not yet...

Leo: Two great books. Can't wait. I just got "Antares Dawn." So now you're using up

all of my Audible credits.

Steve: Yay, yay, yay. I'm so glad you're going to try "Antares," Leo. It will not disappoint you.

Leo: Awesome.

Steve: That's the next thing I'm going to re-read. I've been itching to do that. And also we seem to now have the Bad Programmer Joke of the Week. It's like, okay, they're short, I can do that. Remember we had the parity-based joke last week. So now we've got: Two bytes walk into a bar. The bartender says, "Can I get you anything?" One of them says, "Yes, make us a double."

Leo: [Groan] It's a typecasting joke.

Steve: Exactly.

Leo: Cast me a double, bartender.

Steve: You don't want to be typecast. But sometimes, if you're a byte, you need to be typecast.

Leo: You need to be cast.

Steve: That's right. Because you're just not long - okay.

Leo: Oh, lord.

Steve: And totally random, I know about this, I know this is random, but I tweeted this when I was still trying to get my breathing under control. Saturday I saw "Olympus Has Fallen."

Leo: What's that?

Steve: It is pure escapism, over-the-top action.

Leo: It's a movie?

Steve: Yes. It came out Friday. The White House is under siege by foreign bad guys.

Leo: Wow. That might actually be true.

Steve: It was wonderful.

Leo: Wow. "Olympus Has Fallen." Okay, great. It's Morgan Freeman, they're saying.

Steve: Yup, and other people who don't really matter. But they're in masks and running around. It's pure - and I'm not saying it's a great movie. Lord knows it'll never be winning any awards. What I tweeted was, "Of LSV, it has tons of L and V and doesn't need any S." I said, "Wow."

Leo: I prefer my movies all S, no L and V, but that's just me.

Steve: Well, it's funny because there's - oh, I'm watching, among other things, I love "Justified." And at the end of every commercial break, up comes their warning.

Leo: Really.

Steve: And, you know, "LSV." Which of course is language, sex, and violence. And I jokingly say to Jenny, I said, "It has everything."

Leo: This is what I'm looking for.

Steve: What more could you want?

Leo: But it's a network television show. How much LSV can it really have?

Steve: Oh, "Justified"? You don't know about "Justified"?

Leo: Well, what network is it on?

Steve: Fox.

Leo: Oh, yeah, so maybe they can do more on Fox.

Steve: And it was made for Timothy Olyphant, who we all got to know in "Deadwood," HBO's "Deadwood" series.

Leo: Oh, it's based on Elmore Leonard novels.

Steve: It's really good.

Leo: Oh, it's FX, not Fox.

Steve: Oh, sorry, right, FX, right, right, right.

Leo: FX. Oh, I love Elmore Leonard. He's very gritty. Is it gritty?

Steve: It's very, yes. And it's got lots of LSV.

Leo: Really.

Steve: Oh, yeah, it's, I mean, everybody who's into it is really into it. So maybe get the first - find the first season and check it out.

Leo: Oh, yeah. I'm sure I can watch it on...

Steve: You won't be disappointed.

Leo: ...Hulu Plus or Netflix or somewhere, yeah. It's a modern-day lawman.

Steve: Yup. And he's just - he's ber cool. He is just super cool.

Leo: Is this the one in Vegas? Is he in Vegas? No.

Steve: No.

Leo: That's a different one. He's in Miami.

Steve: No. The very first episode we have an opening scene with him in Miami that sort of sets us up.

Leo: I see. He's in Kentucky now.

Steve: Yes. And he generally gets himself in trouble, and he says, well, it's justified.

Leo: Oh, I like it.

Steve: Oh, it's good.

Leo: Huge Elmore Leonard - have you ever read any of his novels?

Steve: No.

Leo: You would like Elmore Leonard. If you like this - he wrote "Get Shorty" and a number of movies, novels that were made into movies. But, yeah, you get into Elmore Leonard, you will love - it's gritty crime stuff.

Steve: Ooh, that does sound good.

Leo: I think you'll like - pick one up. I'm sure it's on Kindle. And I'll make you a deal. I'll watch "Justified."

Steve: You'll be happy. I think you'll like it a lot. And I think we're in Season 3, so you've got three really good seasons. Lots of content.

Leo: Yeah.

Steve: So I had this email from Dario Matonicki. He clearly had fun writing this. This is actually dated Wednesday, March 27th. So, wait, is that today? Oh, yeah. It was titled "My SpinRite Magic Moment." And he said, "Hi, Steve. I've been sitting on my copy of SpinRite for some time now, waiting for the moment where I can jump up and save the day, and today was that day.

"I arrived at my office this morning to a scene where a few IT chaps were gathered around a laptop with various versions of rescue disk software, eventually proclaiming the laptop deceased. 'It's pointless. Even the BIOS is not seeing the drive,' one in the group proclaimed. 'This one is dead.' 'Sorry, bud,' others chirped in as they comforted the laptop's owner. I turned to them and asked, 'What did you try?' 'We tried everything. It's dead.'

"And there it was. My SpinRite moment was standing right in front of me. 'Everything?' I said. 'Did you run SpinRite?' The room was suddenly quiet, and I was in shock that none of these self-proclaimed IT boffins had a clue what I was talking about. 'Step aside. Let me show you the magic of real craft. Nothing is declared dead until SpinRite spins it,' I professed. SpinRite CD in. Power up. SpinRite splash screen on. Start recovery option. 'Detecting mass storage drives' message pops up on the screen and stayed there for a while. 'You see? It's dead,' someone in the crowd shouted.

"I took a deep breath and gathered my thoughts and asked myself, what would Master Steve do? Never give up, that is what Master Steve would do. So I pulled the drive out of

the laptop. 'We tried that already, too,' they proclaimed. But I ran SpinRite on it outside of the troubled laptop, put the drive back in, powered it up, and voila, drive was recognized, OS booted, and the crowd rejoiced. 'How did you do this? What is this SpinRite?' Questions flew from all sides. I handed a link to GRC.com and said, 'Here. Get your copy of SpinRite now so you can save yourself when the time comes or be a hero to someone else in need. Now go and make a few yabba-dabba-dos, for it's the best money you will ever spend.' So, Master Steve, thank you for giving the world SpinRite. May the Force be with you. Dario Matonicki, Cape Town, South America."

Leo: Wow. South Africa, probably.

Steve: I'm sorry, South Africa. I was just overwhelmed. I was overcome. Dario, thank you so much.

Leo: That's a great story.

Steve: For the fun piece, yes.

Leo: So I was just looking at Elmore Leonard's novels, trying to figure out which one I should recommend, and I realize, so many of his novels...

Steve: That they're all good?

Leo: They're all good. They've been - look it. He wrote - see if you recognize any of the movies that came from this. "Hombre," 1961, of course. "Mr. Majestyk." He wrote, let's see, "Bandits," which was made into a movie with - "Freaky Deaky," "Killshot," "Get Shorty" was made into a movie. He's - "Cuba Libre," "Be Cool," great stuff. "Mr. Paradise." If you like "Justified," I bet you'd like his stuff. He's a really great novelist, been at work since 1953.

Steve: As soon as - oh, that means that he just turned 60.

Leo: No, no. Wasn't born in 1953.

Steve: Oh, whoa, then he's a lot older.

Leo: He's been writing since 1953. Yeah, he's - I interviewed him. He's a great guy. Very much like his characters. Bruce Willis, that's right, was in "Bandits." All right. I have got questions in front of me. I bet you would like to answer some questions. Would you?

Steve: That's why we're here this week, Leo.

Leo: That's why we're here. The "Listener Driven Potpourri," as Steve is wont to call it. Question Numero Uno from Steve "The Evil Scotsman."

Steve: If that's what he calls himself...

Leo: All right. He's great. He wonders what's up or down with his shields? I won't do the whole thing as a Scotsman.

Steve: No, please, please.

Leo: No, I promise. He says - although it is tempting. Steve, I was recently using your great ShieldsUP! test. Previously, every test came back as fully stealthed. But recently it's come back as stealthed apart from ports 135139, which were shown as, not stealthed, but closed. At first I thought it was a problem on my end, so I went to my ISP's forums, and I asked if some users could do the same test, which they did. Now all of their scans now come back as closed on those ports and stealthed on all others, when previously they were fully stealthed. I have a feeling I know what's going on.

So then we got a hold of an excellent tech support person from our small Internet service provider, and they said, yes, indeed, we are blocking ports 135139, but we've been doing it for years. And as far as they're concerned, nothing else has changed, and that's how the ShieldsUP! test results should have always looked. But a lot of us from that forum run the ShieldsUP! test regularly, and the result, apart from these recent tests, have always been fully stealthed. So we're wondering, did something change in ShieldsUP!? Has it been tweaked, upgraded within the last few weeks or month? Because that's when the majority of people agree they first saw a fully stealthed "passed" test was a month ago. If the test has not been changed, then our ISP will look more deeply into it. But they're going to the source. Mr. Steve Gibson, what's the story, morning glory?

Steve: I did change ShieldsUP!.

Leo: You blew it.

Steve: Actually, no.

Leo: You know, it's funny, these ports are the - not blew it. But these ports - you did it. These ports are the original ports you started ShieldsUP! for, way back when.

Steve: Yes, those are the Windows printer and file-sharing service ports. It's actually moved to port 445 is what Windows uses now. But they used to use a combination of 135 and then 137, 138, and 139. Never 136, but just I guess it's easier to block that range, so they just throw that one in for good measure. What happened was...

Leo: Those are the old - we called them NETBIOS ports.

Steve: Yes. Well, yeah. Precisely. A couple weeks ago somebody in the GRC newsgroup reconfigured their router - they're, like, a Linux/UNIX person - reconfigured their router to respond to TCP SYN packets, that is, connection-opening packets, not by dropping the packet, but by sending back an ICMP destination unreachable. That's ICMP we've discussed, back when we were talking about the underlying plumbing of the Internet technology years ago. That's a very simple protocol in the same sense that UDP and TCP are protocols. ICMP is, for example, what ping uses, where you just, when you ping a server, it's just you're sending one little packet out saying "ping," and if the server is there, it's supposed to send it back to you.

One of the things that can happen is that, when a port is closed, it declares itself closed. Now, a normal TCP closed port will send back a reset, essentially rejecting your attempt to open it, to connect to it. But it's also possible that it would send back an ICMP. There is a message, port not available. This came up because I was doing that for the UPnP exposure test that I added a couple months ago. Remember when we had the revelation that there were all these Universal Plug & Play ports exposed. So I quickly, like the day after the podcast, I added a new service to ShieldsUP! to allow people to check. And we were north of 3,000 last time I looked. Maybe we're at, like, 3,200 people have actually found themselves exposed. So that's good.

But one of the people in the newsgroups reconfigured their firewall to send back ICMP port closed in response to TCP. That's not the normal response. But it can be done. And I wasn't looking for ICMP ports, that is, ICMP packets coming back. So there was some discussion in the newsgroup, well, shouldn't you really? And at the time I was right in the middle of working on the server, and I said, well, how hard can that be? So I spent a couple hours, and it turns out the architecture that I had, which I mentioned, for the Universal Plug & Play stuff, that was so easy to add because I've really got a very good architecture that I built when I rewrote ShieldsUP! the second time. So it's like, oh, I know how to do this.

So I added some code to show when anything comes back. I was already doing an omnibus collection of "anything." That's where this true stealth label you get, if you're true stealth, it's because during all of the outbound probes, nothing ever came back. But I didn't - I wasn't showing what was coming back, just whether anything was or not. Now I'm showing which ports we hear from.

Now, what happened, this is a side effect that Steve the Evil Scotsman was the first to bring to my attention, which is people used to be stealth, but they weren't really. But it wasn't - here's the dilemma. It's not they who are not stealth. They really are. It's their ISP that is in front of them, from the standpoint of my ShieldsUP! testing, that is intercepting that port range and not dropping the traffic. In traditional firewalls, you can have a rule, when the packet matches certain criteria, like it would be TCP port 135139, then what? Well, then you could - normally you would drop the packet. That is, you just drop it.

But there's another verb that firewalls can use which is "reject." And so this ISP, and we have since learned other ISPs, are rejecting the packets, meaning they are sending something back saying this port is closed. So they're not showing as stealth any longer on the ShieldsUP! test, that is, the end user is not, not because of them, but because of their ISP that is being noisy about its blocking of those ports.

So I'm not sure what I'm going to do about it. I mean, I've got so many things that are backlogged that I want to get to. I really don't want to do a major reengineering of ShieldsUP! right now. So I'm tempted just to remove this. On the other hand, it's providing some useful information. What I really should do, and what I'm going to look at seeing if I can do without it sending me back months, is add another state of a port. Right now we have open, closed, and stealth. It would be nice to add "filtered," maybe a different color. I'm sure it would be a different color. And what it would mean is that we got something back from an IP not yours, which would probably mean it was the ISP sending back an ICMP, which would say, okay, this is not noise from you, this is noise from somebody between you and me, almost certainly your ISP. If I can do that without needing to move heaven and earth, then I'm going to do that.

So that explains it, not only for the Evil Scotsman, but for any of our listeners who are ShieldsUP! users, now or immediately after hearing this on the podcast, I imagine. And given the traffic on the website, I see that has already happened.

Leo: Just for people's understanding, and you explain it very clearly on ShieldsUP!, why is it important that it be stealth, not closed?

Steve: I don't know that it is, really.

Leo: Especially if the ISP is closing it; right?

Steve: It's something you could have, and it's cool to have it. I mean, it's just sort of like, right now the Internet is being scanned for Universal Plug & Play ports and for telnet ports as a consequence of the last couple podcasts where we've reported on these things. I think it's just nicer to not appear to be present at all.

Leo: That was the idea of stealthing is that, some bad guy knocks, instead of saying "There's nobody home," which says in fact there's somebody here, we're just not letting you in, you just don't respond.

Steve: Yes.

Leo: But if it's an ISP doing it, it's still on your IP address. Although I presume the ISP does it for all IP addresses in their block; right? Whether there's a machine on the other end or not.

Steve: Yes, and I'm glad you've raised that point because that doesn't say anything about you. It's really talking about them, meaning their entire customer base.

Leo: Now, whether the hacker is smart enough to know the difference, I don't know.

Steve: Well, now, the one argument has been that, if this blocking is occurring at the ISP's border, maybe users within an ISP can see each other's ports. And so, if someone

scanned their own IP neighborhood, then they would be scanning inside of that perimeter which is protected by the ISP. So if somebody had ports 135139 open, ShieldsUP! previously wouldn't have been giving them any reason to worry. Now at least they would know, oh, wait a minute, somebody else is blocking, so maybe I'm not safe behind that block. So it's useful information. Anyway, I didn't want people to be freaked out and confused, starting with Steve the Evil Scotsman. Who will probably now be changing his email address.

Leo: Christopher, who is not evil in the least, Christopher A. Hunt...

Steve: No.

Leo: ...said I got this email from my credit union. Actually my bank. Well, credit union. After having listened to the episode involving SSL Labs, I submitted my bank's URL, received a "C" or a "B" rating. I forget now, but it had major frightening failures. My bank now has an A rating with 90 percent or greater subdivision. Thanks for your service to the community. It's most appreciated.

Here's the email he got from the credit union: Dear Mr. Hunt, thank you for your email regarding our rating at SSL Labs. We have analyzed the result and, as a result, we've made changes on our website to mitigate the possible BEAST attack vulnerability, to bring our website up to an "A" rating. Wow.

Steve: I know.

Leo: That's why I like credit unions. You know? They're small and responsive.

Steve: Yes.

Leo: The only item left open is the currently known and problematic RC4. At this time there is no known attack that can take advantage of this vulnerability within RC4; and, until all major browser vendors, Apple being the only major vendor left, implement the fix, RC4 will continue to be used. Again, thank you for bringing this - this is somebody smart.

Steve: Yes.

Leo: Lee Anderson, network administrator, TIC Federal Credit Union, Columbus, Georgia. That is good news. Wow.

Steve: Yeah. If you get email like that back from your financial provider, yes, you've found a good one.

Leo: Feel good. You know, everybody - I was unhappy with my bank, and I asked on Twitter, what do you recommend? Universally, people who have credit unions are much, much happier with their banks. They're nonprofit. They're responsive. That's a really good example. Now, sometimes they're so small maybe they don't have good security. This one does, anyway.

Steve: Yeah.

Leo: Eric Cook, Millwood, New York, wonders about the scheme he cooked up for encrypting his tax information. I love these homemade encryption schemes. Let's see, what's the latest? Love the show, long time listener, blah blah blah. Been using a secure email program called Protected Trust, at ProtectedTrust.com, basically to send my tax information to my accountant. It asks for a password. It is encrypted. The recipient has to plug in the password to decrypt and see the message. So after sending the email - so it's a symmetric password, in other words. After sending the email, I send a separate email a few minutes later with a password, unencrypted [chuckling]. I'm sorry. Is this secure?

My rationale is the first email can only be read if it's intercepted, and they have the password. By the time the second email is sent, the first should have arrived. And even if it has been intercepted, they would not know what the password pertains to. I do not think people are intercepting emails and saving them. Is that even possible? If so, the volumes would be so great, the likelihood of them connecting the two emails would be slim. Am I correct in this, or way off the mark? Thanks.

Steve: Well, okay. So all of our listeners are...

Leo: This is the problem with symmetric key crypto. Right? Back when you were Julius Caesar, and you wanted to send a message to the Persian king that was encoded, you had to send two separate messengers, one with the key and one with the message because you needed the same key to unlock that you needed to lock it.

Steve: Yeah. Now, what I would say, from a security standpoint, the biggest vulnerability here is that all of the information required to decrypt the email containing obviously his tax information that he cares enough about encrypting to do so...

Leo: Well, it's his Social probably in it.

Steve: It's all being send through the same channel. So a bad guy monitoring just one channel gets everything that they need. If you wanted to summarize the problem, that's it. Now, there's a whole 'nother problem, which is what is ProtectedTrust.com. Is it doing client-side, browser-based, pre-transmission encryption? Or is it receiving it in the clear and encrypting it so someone else can't get it unless, I mean, the whole thing sounds kind of hokey.

But here's the smallest, easiest - because we want to provide something practical for Eric and anybody else who wants to do something like this. I would say arrange a different

channel. Write down on a piece of paper, fold it twice, stick it in an envelope, and paper mail it, the password that you've chosen. Or anybody legitimate who's in the tax accounting business is going to have a fax machine. Write it out in big letters and fax it.

Leo: That's a good idea. It's a different channel.

Steve: Use a different channel, exactly.

Leo: Somebody would have had to commandeer both to have a chance.

Steve: Right.

Leo: Although this is the problem that public key crypto solves.

Steve: Absolutely does. So if the tax accountant had a private key, then they could provide, to anyone wishing to submit secure email tax information to them, their public key. In which case Eric would encrypt with a public key. No force on Earth that we're aware of, even the NSA as far as we know, can do anything about that because that public key, the way that this would work is Eric would have some sort of an app that does this that generates a large pseudorandom symmetric key. That gets encrypted with the public key of the recipient and then all of that sent off to the recipient. And then, because they're the only people with the matching private key, they alone are able to decrypt that encrypted symmetric key to get the plaintext, the decrypted symmetric key, which they then use for their bulk decryption to decrypt Eric's taxes information. So all of this is, like, all open source, all in the public domain, open.

Leo: PGP is a great way to do this.

Steve: PGP, yes, exactly.

Leo: That was what it was designed to do.

Steve: So there are secure ways to do it. The only problem is he's saying I counted to 10 before I emailed my password. It's like, okay, that doesn't work, even counting to a hundred, because the point is it's the same channel. Use a different channel. I realize it's too late for this tax year, apparently.

Leo: It's probably okay, too. I mean, come on. Unless somebody's actively pursuing the fellow.

Steve: I know. I know.

Leo: But the public key just solves it. It's so straightforward. Instead of having a single symmetric key that both ends have to know, and so somehow this key must be exchanged securely, you have two keys, one that you can tell everybody. That's what they use to encrypt. One you keep to yourself, the private key that only can be used to decrypt.

Steve: Yeah. It is so, so cool.

Leo: It's brilliant. It's brilliant. It's a brilliant conception. And if Julius Caesar had had that, he'd be alive today. No.

Steve: And Rome would be a different place.

Leo: Rome would be a different place. Trey - oh, boy. Trey Dismukes in Houston raised an - I'm sorry, Trey, for butchering your name. Dismukes. That can't be right. Steve, regarding the trouble with having ISPs blanket blocking all UPnP UDP port 1900 traffic - right, Michelle? Right - and how it might cause some potential issues with legitimate traffic, we've come a long way in the last 10 years of network security technology. We can block much more granularly than just by a packet's destination and port number. Oh ho. On-the-fly pattern matching on the contents of packets using UDP 1900 can allow ISPs to block UPnP without affecting legitimate responses. You talk about deep packet inspection.

Steve: Leo, you can make even something as dry as on-the-fly packet...

Leo: Oh ho ho.

Steve: ...packet matching by port destination really come alive.

Leo: Yeah. Deep packet inspection, baby, heh heh heh heh.

Steve: Anyway, so Trey is exactly right, and I wanted to give him his day and to mention that he's completely right. I wasn't assuming that on the behalf of ISPs. Routers are often incapable, simple routers are - they excel at doing what they do very fast in order to keep up with the so-called "line rate," the rate at which the packets are flying in and out over the wires. So some of them are only able to do a, is this bit pattern what I'm looking for, and if so.

But on the other hand, bit patterns exist inside packets. And so he is correct that there is a, that is, you could look into the packet at more of the contents of the packet or, as you say, deep packet inspection, which is the formal term, see if this is, for example, random web traffic that just happens to be using port 1900, I'm sorry, or DNS that would be a typical client of UDP port 1900 because DNS tends to run over UDP, whereas web is over TCP, so that would disqualify TCP immediately, see if it's a DNS query. Those are well identified. And no person's browser, I'm sorry, no person's router would respond to a

DNS packet on port 1900, probably because, from inside the network, it would just pass it right through.

So if you had the ability to do deep packet inspection, you could explicitly allow either DNS packets and block others, or better would be to see whether the packet is a UPnP probe and then drop it. In which case you would be protecting your users, not wrecking up, not messing up any other traffic that's running over that port, and it would be workable. I don't know if an ISP's going to care to do that, but Trey is right. It's absolutely possible.

Leo: And a very common feature in all big firewalls, big iron firewalls. And would it be fairly easy to recognize an UPnP probe?

Steve: Yeah. They have an absolutely definitive fixed format and - because I wrote one. The ShieldsUP! system is a UPnP probe. And I followed an absolutely rigid template that you could easily match on and say, whoops, we're not letting that one go by. There's no point, there's no reason for that to ever be out on the public Internet.

Leo: That's why a good ISP really is good. You know? Find a good one.

Steve: They're worth their weight in what you pay them every month.

Leo: They tend to be, the big ones, like the big national ISPs, tend not to do a lot of that stuff because, well, for one thing, think about it. If they turn off port 25 to block SMTP, for instance, they're going to spend a million dollars in support calls from people because they have lots of customers, and some percentage of them are going to say, what the hell? So it's, you know, what are you doing?

Steve: It's like my own operations gal, Sue. She uses a Cox cable modem. Cox blocks port 25. So she's unable to connect to GRC's server, so we had to set up an alternate port that she's able to use that Cox doesn't block. And in fact I've got a RAID, I've got an email trigger on the RAID that I installed last time she had a problem, and it was very problematic getting it to be able to send email out of her computer because Cox was saying, no, we think you may be a spammer. We're not getting spam get out.

Leo: Drew Moseley in North Carolina offers a truly clever hack: Hi, Steve and Leo. Blah blah blah. I like it. He has <praise> blah blah </praise>. I was reinstalling my mother's Windows laptop the other day, and it came time to install a PDF reader. I immediately, immediately thought about downloading Foxit. And then I had a revelation. Why, there's already a PDF reader installed. It's known as Firefox 19. Since I was going to set her up with Firefox as her default browser anyway, and in the interest of not installing anything she wouldn't use, I decided to set up the file associations so that PDF files would launch Firefox.

Steve: Isn't that interesting.

Leo: Yeah. Didn't show up in the suggested apps. Windows probably didn't know to include that. But I was able to browse through the file system to select Firefox as the preferred app for PDF files. And, voila, one less app installed that required maintenance updates, et cetera. Admittedly, the PDF viewer and functionality in Firefox is new and thus likely less secure than Foxit. But since Firefox will be installed regardless, I figured, a reasonable compromise. Thanks for all you do.

Steve: I thought that was very clever. And at least in Windows, when you right-click on a file, there's, like, "Open With" is an option in the properties that comes up. And then you're able - it gives you some things that it knows can open the type of file by extension that you're opening. But you're also able to browse for your own. So he said, let me choose my own, and then he dragged through, scrolled through a list, found Firefox and said, yeah, open PDF files with Firefox. And that's all you need to do because, when you launch Firefox and give it, at the end of the command, it treats that like a URL. And when it sees .pdf it says, ah, I know how to show these now. And so it turned Firefox, multipurposed it, essentially, turning it into his system's default PDF reader. Which is very, very cool.

Now, I'll make a comment. This gives me an opportunity just to say I'm still using Firefox's native, that is, newly native PDF reader unless I want to print. It's pretty crappy when it prints. It shows things on the screen pretty well. Printing is challenging. The nice thing is, when it comes up, there's like a "Download This" icon. You can click on that. And it doesn't download it again, it just pops up a "Save As" dialogue. So then I'm able to save that PDF to my system, and then I open my normal system's PDF viewer, which is extremely capable, and then I use it to print. It's also very slow to print. So it's like, if I want to print it, I don't even try that in Firefox, though I do like it for viewing PDFs. Sort of in Drew's approach of just one fewer thing to have in a system is always good.

Leo: From Bethesda, Maryland, Doug Zuckerman comments about Windows 2008 Server: Hi, Steve. I was just listening to the feedback show from a couple of weeks ago where you mentioned you'd finally replaced your creaky old Windows 2000 machine with 2008. I just wanted to make sure to let you know that, if you chose 2008 and not 2008 R2, I would highly recommend upgrading to R2 ASAP. I have found 2008 R2 to be a phenomenal server platform, and stability-wise it's a must-have over 2008, which has some weird bugginess, most of which was fixed in SP2, but it still falls short of R2 SP1, IMO. I'm responsible - I believe if you write "IMO," in my opinion, you're supposed to write "IMHO," in my humble opinion. I'm responsible for a few hundred machines - oh, that's why he's not so humble - nearly a thousand databases, and about 300TB of data at my job, so I've had a pretty good platform to test and develop an opinion on the matter. So it's not so humble.

Steve: And I saw this, and I thought, okay, perfect opportunity for me to say I really am happy.

Leo: You use R2, of course.

Steve: I mean, I am really - of course. And I am really happy. Actually, I first did only '08, 2008, because you know me, on the theory that, well, if it's newer, it's not better. But shortly after I got the feel for that, I realized that its crypto support was still lacking.

It did not offer TLS 1.1 and 1.2. And I thought, well, okay, it's a lot better than 2000. But I felt like I was already behind the curve. Now, what I have since learned and really appreciated is that Server 2008 is the server version of Vista. Need I say more.

Leo: And R2, is that Windows 7?

Steve: Yes.

Leo: Ah, interesting.

Steve: Yes. And in fact it is Windows 7 enough that I don't run Server 2008 R2 here at home where I do my development. I'm using Windows 7 here at home, sort of prototyping it for the future day when it becomes my main workstation OS. And again, I am so impressed and happy and pleased. And so I've got IIS 7.5, the web server, running on Windows 7 because it is the same as the web server running under Windows 2008 R2. So, Doug, I am with you a thousand percent. I just wanted to say to any listeners who are Windows users or people and so forth, that that's the one. I'm really pleased. 2008 R2.

Leo: Careful, Steve. You're only a version behind now.

Steve: I know.

Leo: Oh, boy.

Steve: This is when I start catching up.

Leo: Only one version behind.

Steve: However, I won't be moving soon. So I'll start falling, I'll start drifting back, then, again.

Leo: Question 7, Mark in Colorado, Colorful Colorado, says great coffee recommendation, Steve and Leo. Not a technical question, but thank you for giving the great coffee recommendation in Episode 391. I've been on Steve's no-starch diet for the last few months, have shed 47 pounds. By the way, Steve, almost every day somebody comes to the studio and says thank you, I did Steve's diet, and I've lost. And it's - weight loss is often in that 50-pound area. It's amazing.

Steve: I know. I hear it the same way, yeah.

Leo: He said, this morning I weighed myself and was below 200 pounds for the first time in about a decade. Still have a ways to go, but I decided to treat myself with a coffee. That's such a great treat, isn't it? Since I started dieting, I haven't had any coffee, tea, et cetera, and I wanted to make this a very special treat. I remember you guys talking over your favorite coffee, so I went to GRC.com and went through the transcripts, decided to give Steve's recipe a try. I went to the store, bought a Moka pot, M-o-k-a. It's an old-fashioned Italian stovetop espresso maker. Stopped by the local coffee shop and picked up the dark roast espresso coffee, whole bean. After getting everything set up, I ground the beans, put in the water, and about seven minutes later I had the best cup of coffee I've ever had. No need for sugar or milk or anything. Thanks for the great show and great cup of Joe.

Steve: For what it's worth, Leo, I did follow your advice. I gave the Trader Joe's Kona a shot.

Leo: What did you think?

Steve: Bitter, compared to what I'm drinking.

Leo: You know, it is a little bitter, I think, yeah.

Steve: Yeah. I'm going to grind to - the grind that I have found, and send up to you Steve's coffee.

Leo: Okay.

Steve: And do you still have the cute little five-cup Zojirushi Zutto, whatever the hell that thing is, that wacky little thing?

Leo: Yes.

Steve: Is it at home or...

Leo: Oh, I have everything at home. I have many ways of making coffee. But I'll bring it in here.

Steve: Okay. I'm going to...

Leo: Now, I have to say, bitterness in coffee is a result, not necessarily of the bean, but of how you brew it, as well, because you know, and I'm sure I'm not telling you anything you don't know, but...

Steve: Well, and, see, that's why...

Leo: The extraction process, temperature, length of time and so forth, can bring out different tonalities like bitterness and acidity, things like that.

Steve: And this is why I asked you about that machine, because I have already got - I've got the exact quarter-cup measuring scoop for you. I've got the sealed, airtight container for you. I've got the beans. I want to send you, as long as you've got that coffee pot, I have everything calibrated.

Leo: Now, which one is it that I'm supposed to make, the stovetop espresso Moka pot style?

Steve: No, no, no. It's the Zoritsu or Zor...

Leo: The drip?

Steve: Yes. You use the brown coffee paper, stick it in there, and it does a drip in about five minutes. And I was at Starbucks two weeks ago with my coffee and with my regular friends there. And they're the people who, like, one of them is very health conscious, and he puts so much sugar in it, he might as well just call it syrup. So I got a couple of the little espresso paper cups from the barista, and I poured from my thermos into these espresso cups and said, here, guys, just try this. And they couldn't believe it. They said it doesn't even taste like coffee, meaning that they really don't like coffee until...

Leo: It's good, right.

Steve: Yeah, it's that good. It's just amazing. So I just want - I want to bring you onto the team, Leo, by - I'm going to send you a whole little care package.

Leo: I will gladly...

Steve: We'll see what you think.

Leo: ...try it out. I'm looking at this roaster, Tonx. Have you ever heard of Tonx, T-o-n-x?

Steve: No. No. So roaster, you're saying. That's...

Leo: Well, this is what's interesting about this. So a number of people that I trust recommended this, Tonx. What they do is they send you, like, 12 ounces every other

week. It's a subscription thing. But they express it after they roast it, so it's exactly like three days later, which is what you're supposed to apparently do. And they do their own - I don't know. It could be just silly. You know, they pick the beans, and they carefully hand roast it, blah blah blah. But I've heard very good things about that. I don't know. So I will try your beans. I will try your beans. We'll see.

Steve: I will provide my beans.

Leo: Where do you get your beans?

Steve: Starbucks. That's what's so beautiful. It's the Starbucks espresso bean. That's all it is. Universally available, everywhere in the Galaxy.

Leo: The only thing wrong with Starbucks really is not the beans, but they over-grind them for use in the coffee making.

Steve: That's why I've even found the proper setting on the machine. It's like, okay...

Leo: Grind is very important.

Steve: Here it is, baby. Give this a shot. I'm going to...

Leo: Okay, all right, Steve. We'll see. Question 8 from Bismarck Public Library in Bismarck, North Dakota. Vern Mastel writes and shines some light on the Telnet-pocalypse population: Steve, last week, one of your final comments was "What are all of these boxes?" I'll tell you, Steve. I at the library here have a bunch of HP printers. The standard in-service procedure is to turn off all the extra protocols (telnet is one) and password the printer. But that's our procedure. The default for these HP printers, telnet on, passwords not. In the past four years I've changed all my network switches to managed HP units. These come out of the box with telnet turned on also. The network switches, again, add a password and turn off extra protocols. Otherwise.... I know a number of sysadmins don't do anything like this because it's inconvenient. Cisco switches, out of the box, telnet turned on. I have nearly a hundred backup power supplies. I install the APC network management card in all of my APC SmartUPS units. Yep, default passwords, telnet turned on. I use $30 IP print servers as pingable devices in my power monitoring system. Telnet? Of course.

Boy, this guy is - Vern, you're smart. I'm glad you paid attention to this because I doubt anybody else is doing this.

I do not doubt that many, maybe all other brands of network devices also come out of the box with things like telnet turned on. Oh, boy.

Steve: So I guess when a company, a big company, has a block of public IPs, and

they're assigning IPs to all of their equipment, public IPs...

Leo: They don't bother to NAT it.

Steve: You're right, they're not NATed. Exactly. And they're certainly not firewalling, obviously.

Leo: Out on the Internet. Hey, we've got IP addresses to spare. Why should we put a router in?

Steve: Come visit.

Leo: Come visit.

Steve: Come visit.

Leo: But of course, as you say, if they're behind a router, it doesn't matter if these are open.

Steve: Right, you won't be seen from the outside.

Leo: Of course, if your router has telnet turned on...

Steve: Or Universal Plug & Play.

Leo: Right. Or both. From the Twitter comes this from @ChivalryBean in Portland, Oregon. @SGgrc - that's Steve's Twitter handle. If I understood right, my lone computer has a better chance of making a litecoin than a bitcoin. Am I right? By the way, Steve, check Mt. Gox. Your 50 bitcoins are worth over four grand now.

Steve: Woohoo.

Leo: You're rich, my friend.

Steve: Baby, free money. I like it.

Leo: But I want to make it clear because, first of all, people say, oh, TWiT, you guys never cover Bitcoin. Yes, we do. Steve did an entire episode that was so definitive, there's nothing more to say about Bitcoin. So go back in the archives of Security

Now!, and you'll find all of that [SN-287]. The other thing, though, I think we kind of implied, since we talked so much about bitcoin generation, that to play in the bitcoin space you need to be running a bitcoin mining operation. That's not true at all. Right? I mean, it's a currency. If you accept it...

Steve: Oh, oh, absolutely. You don't need to mine bitcoin.

Leo: You don't need to create bitcoins to use them.

Steve: There's some guy in Canada wants to sell his house for bitcoin. No, I got a bunch...

Leo: That's actually probably a very good idea, unless the market crashes, and then you're screwed.

Steve: Yeah.

Leo: It's a little risky because the market is volatile. But if you believe this is the future...

Steve: And if he'd sold his house for bitcoin a year ago...

Leo: He'd be sorry.

Steve: ...when the price was $15, yeah. This stuff really is appreciating.

Leo: But you could have said that about gold. It's a little risky. Let's not recommend it as an investment.

Steve: Virtual, it's virtual.

Leo: It's virtual.

Steve: Okay. So @ChivalryBean, yes. What's happened with Bitcoin, because clever as it is, it is based on well-understood cryptographic hashing, it is possible to incredibly accelerate that. There are people who use graphics processing units, GPUs in computers, to do hashing very fast. There are people who just build boxes of how many slots do they have that they can fill with GPUs to create little sort of homegrown mining machines to try to solve the hash puzzles at a competitive rate. And that's the key, a competitive rate. And then there are people like Butterfly Labs that used to sell machines like that. Now they've got ASICs, Application-Specific Integrated Circuits, ASICs, which just takes

it to another whole level. Mark Thompson was telling me that, if you could get one of these Butterfly Labs devices, they pay for themselves in four days.

Leo: What? Really?

Steve: Yes. They cost $25,000, but you will make $25,000...

Leo: You're guaranteed to make that many bitcoins.

Steve: Because it's that fast. And the point is it's competition.

Leo: Till everybody else gets one.

Steve: Until everybody else gets one, exactly. And then all that does is that ups the ante again.

Leo: Again, we've talked so much about generating bitcoins. That's irrelevant. That's just - you no more need to do that than you need to be the U.S. Mint to use dollars.

Steve: Correct, correct.

Leo: This is just a medium of exchange.

Steve: But there is an alternative that is becoming popular called Litecoin, which is what @ChivalryBean refers to. And what's unique about it is it uses memory hard problems.

Leo: Ah.

Steve: It does not use a hash. It deliberately uses Scrypt, which we've spoken of. Scrypt is the memory hard technology that I described which absolutely requires memory, which ASICs don't have in abundance, which GPUs don't have access to at the same speed. So this sort of - this resets the bar. If you wanted to play with mining a currency, even though it's not the bitcoin currency, it's the litecoin currency, that's l-i-t-e coin, the playing field has been leveled again.

Now, Mark Thompson, he and I were talking about this. He says, well, of course, but nothing to prevent you from doing ASICs with lots of RAM. Well, that's kind of true, not so much. I mean, ASICs, I mean, RAM is a specialty, and our CPUs have it now, very inexpensively. So the answer is yes. Litecoin is starting over. It's more like the days when I just stumbled on 50 bitcoin one morning. It's like, oh, look. And that has inflated to $4,000, as you just said, Leo. So...

Leo: 4,500. I just looked at Mt. Gox. It's 80, oh, wow.

Steve: By the way, you know that it was the judgment from the U.S. Treasury Department that we shared.

Leo: Yeah, boosted it up.

Steve: That's what did it, was like, people said, ya ha.

Leo: But it's - 88 bucks. But it's highly speculative. I've got to say this. This is highly...

Steve: Yes. So, because you don't...

Leo: Worse than investing in gold. I mean, this is...

Steve: You don't want listeners to go put all their money into bitcoin and then have it crash.

Leo: Oh, it's - how could it possibly go down? Or sell your house for bitcoin. It's highly speculative at this point.

Steve: But if you've got some free computers that are sitting around, and maybe it's a little cold, so you'd like the exhaust heat from them to help warm the house...

Leo: Well, that's the other calculation you have to do.

Steve: Uh-huh.

Leo: Is the cost of generating bitcoins may in fact exceed the value of the coin generated.

Steve: Yup. When the probability is so low that you can get one yourself, you end up spending more on the power, the electrical power required to try hashing such a low probability to get a coin versus the value per coin, that it just, you know, the economics don't work. And what we're seeing is a gold rush toward high-speed hashing. They keep pushing that higher and higher. So only the people that are now going to be willing to invest in ASIC-based multi-tens of thousands of dollars hashing custom hardware are going to be the miners who push the coin all the way, the rest of the way out.

Leo: Just to explain this, it's like printing money. The difference is Bitcoin has been carefully calculated so that only a certain amount can be printed. There won't be an inflation because it reaches a cap in something like 10 years, or maybe sooner with this ASIC inflation. But at that point it's just done, and there's a certain number of bitcoins, and it's done. And if you think about it, because U.S. dollars are just purely imaginary, they're pieces of paper that are not tied to any intrinsic value...

Steve: It's just agreement. When I go to a restaurant, I'm giving him or her, the server, or the owner of the restaurant ultimately, my agreement, here's something we've agreed on, and other people agree, so you'll be able to go buy something else with that.

Leo: But it's imaginary.

Steve: The medium of exchange.

Leo: And so are bitcoins.

Steve: A medium of exchange.

Leo: But it does rely upon this agreement and this consensual hallucination, as well, that it has value.

Steve: So one of the cool things about bitcoins is that, because it's a digital currency, you can have I don't know how many decimal points, but 0.000000001 of a bitcoin. And so in some future, a single bitcoin, which is now at $88, you say, will very likely be at $100,000. But that's okay because you can trade in incredible fractions of a bitcoin to buy a candy bar. You're not stuck buying a $100,000 candy bar. You just can buy a 0.000000001 of a bitcoin. And so the value scales nicely because it is digital. It's a digital currency.

Leo: I'm reading an excellent book. After our conversation of last week, I realized I really had to read up on this.

Steve: I'm so glad. I'm so glad.

Leo: Yeah, it's called "The End of Money." And it's easy, light reading. But it's very interesting, and it really does kind of underscore, well, first of all the history of money is very recent and very fascinating. It was the Chinese - Genghis Khan, the Chinese emperor Genghis Khan, who was the first to issue paper currency. And when he first issued it, he said, well, this silk script is worth a certain number of Chinese coins, and we have them in the bank. We've got them back here. At any time you can deliver that paper currency, we'll give you the coins. Because they had coinage, but it was the first paper currency. And coinage is ancient.

Steve: It was probably just too heavy to carry around.

Leo: Right. Script made sense, right. And but then, and this always happens, he got, you know, he said, hey, nobody really ever asks for the coins. We could just print more of this stuff. And they did, and they collapsed the economy, inflationary collapse because people realized it actually has no value. And we haven't been tied to gold since Nixon.

Steve: And so in terms of what actually happened in the real world is some wise street vendor said, you know, I think, if you're going to pay with that flaky funny money, then I'm going to need twice as much of it, rather than if you pay with real money, because I'm not so sure that's worth anything. Thus inflation.

Leo: And it could happen anytime, anywhere, as we've learned in Cypress [laughing]. Oh, it's fascinating. It's probably better not to talk about this.

Steve: Brazil had a problem, too.

Leo: Oh, yeah. It's probably better not to talk about it. The consensual hallucination could be damaged. It's fine. It's real. It's money. But that's what - I think that's why Bitcoin kind of freaks people out a little bit. Freaks me out because it's just as - it's no less imaginary. But it's an extra-governmental currency, which I think is fascinating.

Steve: I do, too. That's why we discuss it here on the "what do you want to know about the Internet" podcast.

Leo: Well, because it's crypto.

Steve: Yeah. Exactly. That was the original impetus was this is - and it's cool.

Leo: Right.

Steve: It was done so well. And it leveraged, at the time, everything we already knew that we've covered in, like, crypto, fundamental crypto technology, this notion that the algorithm requires you to come up with a hashed value with some number of leading zero bits. And it is increasingly hard to get more of the left-hand bits zero moving to the right. It's just more difficult. It's just more difficult, and there's no shortcut that we know of. You have to just keep guessing about values that you apply to the existing bitcoin block in order to find the value that'll give you the hash with all these leading zeroes. And the more you require of the zeroes, the harder it is to find that one unique value. It's just, oh, it's just a brilliant concept. And so simple, too, which is what makes it so elegant.

Leo: But it has to be a mutual, consensual hallucination for it to be effective.

Steve: Well, if some guy is willing to sell, if he can, sell his house for bitcoinage...

Leo: But understand, he's doing that as a speculator.

Steve: That means there's two lunatics. No, wait a minute. Yeah, I guess only one, really.

Leo: One has to buy it.

Steve: Because some guy collected all those bitcoins in order to purchase the house. And actually he collected many fewer of them this week than two weeks ago.

Leo: Right. Somebody has to buy. Somebody has to sell. And the problem is that most of the people who are doing this right now are in fact merely speculators. They're not, in my opinion, they're not really...

Steve: Well, it's coming into currency.

Leo: People, they're greedy.

Steve: There are more and more places where you can actually exchange from bitcoinage into the real world. It's a trend.

Leo: It's very interesting. Steve Gibson, if you have questions for him, he's got answers. Every other week we do a Q&A. If you want to leave a question at his website, GRC.com/feedback. Don't email him. GRC.com/feedback. You don't accept bitcoin donations, do you?

Steve: No.

Leo: No. He's got plenty of bitcoins. He doesn't need anymore bitcoin. He's rich. You can also go to GRC.com to get SpinRite - that's the donation he wants - the world's finest hard drive maintenance and recovery utility. But he also has some other stuff there, lots of free stuff like ShieldsUP!, the UPnP tester there, the probe. It's all right. That's one of the probes that doesn't hurt. But it is good to know. He's also got a lot of free software and, for this show, 16Kb audio versions, that's the smallest version made, and full transcripts, English language, written by a human transcriptionist. GRC.com.

Now, we at TWiT.tv have the bigger audio files and the video files, as well, on demand at TWiT.tv. We do this show every Wednesday, 11:00 a.m. Pacific, 2:00 p.m. Eastern, 1800 UTC on TWiT.tv. Please join us. We love having you live, watch the chatroom, interact with the chatroom. But if you can't, as I said, on demand is always available after the fact. And you can, if you're from Wisconsin, you're allowed to visit the studio at any time. We had two different, independently different sets of Wisconsin visitors.

Steve: Amazing. What a coincidence, yeah.

Leo: Yes. Somebody sent me an email, how much does it cost for tickets? It's free. And you get what you pay for, I might add. And we will make you sign a two-page waiver of all your rights when you step in the door, just in case. Thank you, Stevie. We'll see you next week.

Steve: Thanks, Leo.