Listener Feedback #165

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-399.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-399-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson's here. He'll analyze Microsoft's monthly update. We'll take a look at the end of life of Windows XP - we're counting down - and answer 10 of your questions. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 399, recorded April 10th, 2013: Your questions, Steve's answers, #165. It's time for Security Now!. There he is, the man with a plan and a big mug of coffee. That's bigger. I don't understand. Yours seems so much bigger than my Contigo. Steve Gibson is here. He's the Explainer in Chief, our security guru, the man who keeps on top of all the security issues and flaws and tells us about it, and teaches us about computing, crypto, even obscure things like Bitcoin. You know, people ask me - hello, Steve.

Steve Gibson: Hey, Leo. Great to be with you again, as always.

Leo: People ask me a lot, because there's been a lot of Bitcoin news over the last month, why don't we talk more about Bitcoin? And I say, well, we do. You're just listening to the wrong show because Steve is an expert. And I want to thank you because you encouraged us to open Bitcoin donations on the website, and we do. It's not up yet, but any day now. I'll have to go engineer somebody.

Steve: We even have a - we have a Bitcoin section in today's Q&A podcast.

Leo: Oh, good. Yeah, we've got Q&A.

Steve: Because there's so much Bitcoin news, yeah.

Leo: Cool.

Steve: So we're at Episode 399, one shy of the big four zero zero.

Leo: Wow.

Steve: So that's neat. I'm going to be doing a little KTLA TV interview, thanks to Tom, who referred them to me, actually the day after next week's podcast. So they want to talk about passwords.

Leo: Oh, perfect guy. You're the guy.

Steve: That'll be fun. I have meant to thank Tom. I'll do so. So here we are again. This is a Q&A episode. We've got a bunch of questions, some that were quickies, so I put in 12. But if we run long...

Leo: We have time. Come on.

Steve: We'll just stop when we run out.

Leo: Take your time.

Steve: But we do have news. The standard, almost constant start of every Security Now! podcast, of course, is what has been patched and updated. This is - we're at the Wednesday after the second Tuesday of the month, so we're always talking on this Wednesday, relative to that Tuesday, about Microsoft. We have nine sets, nine bundles of patches which remove 13 vulnerabilities. It's not a big exciting one. Nothing devastating. Only two were rated critical. Interestingly, one of them fixes two critical vulnerabilities which have existed since the dawn of Internet Explorer, never found before until now. This is a rollup that goes back as far as IE6 because they figure nobody is running IE5. I mean, I don't even think you can run IE5 anymore. It takes you to a - when you launch it, it takes you to a page that Microsoft hasn't had for the last decade, so it can't even get going. So everyone who wants to keep their Windows machine up to date should do this.

There's also a fix in the remote desktop protocol. If it were a critical vulnerability in the server, that would be a cause for great concern because that could be really important. This is over on the desktop client, however, so not such a big problem. But still, you know, want to keep your machines patched, which all machines other than XP you'll be able to do for the foreseeable future. XP, it turns out, had a pre-anniversary on Monday, two days ago. We are on, as of April 8th, 2013, two days ago, there were exactly 365, well, depending upon where we are with Leap Year, I'm not sure, maybe there's a quarter in there or not, or an extra one. But April 8, 2014 is the official end of Windows

XP SP3 support. So we XP users have one year left to move. And I'll be moving to Windows 7. I'm quite happy with Windows 7. It's really perfect, too, because I get to avoid the horrors on either side, so...

Leo: You mean Vista.

Steve: Uh-huh.

Leo: And Windows 8.

Steve: Uh-huh.

Leo: You know, 7, I've said for some time, couple of years now, is the best version of Windows, I think. And I know you don't want to go to it right away because you want to make sure it gets a chance to patch and become solid. And I think it's been out, what, for five years now? How long as it been out? Long time.

Steve: I'm just not in a hurry. I have it running all around me. I've got Windows 7. I mean, Skype is running on a Windows 7 box right now, when I'm talking to you. I've got one set up to sort of echo the servers at GRC because - and I did this sort of as a "Get to Know Windows 7," make sure I can do the things I need to on it. I am a little concerned. You remember Brett Glass, I'm sure, from the old days.

Leo: Yeah, yeah.

Steve: Brett was a columnist at InfoWorld and is also a deep techie. He said the same thing that Mark Thompson said of Windows 7, which makes me uncomfortable, which is, "How am I going to run my 16-bit code, which is still perfectly workable?" I mean, like, I'm running Brief, which is 16-bit.

Leo: Isn't there a compatibility mode of some kind?

Steve: Well, you know, there is. You can look at the properties of an EXE, and there is a Windows XP compatibility mode. And there's also some sort of a virtual machine thing. But I don't know if just turning that on allows it to run 16-bit code. If it does, then my only real concern is resolved. But I've got a year to figure that out.

Leo: Yeah, I don't know, actually, because it would need - it wouldn't be just tricking it into saying it's XP. It would actually have to have a 16-bit DLL or something.

Steve: I think it has - I think it has - no. I mean, yes, there's a bunch of 16-bit compatibility which has always been in Windows, which they explicitly removed from Windows 7. And they said we've removed this. But there was something you can do. But

it may be - it may require, like, running a virtual machine, I mean, going through all that.

Leo: Well, you can do that. If you have Windows 7 Pro, they throw in, just for people like you, Windows XP in a VM. And somebody in the chatroom said the 32-bit version of Windows 7 will run 16-bit, but not the 64-bit of Windows 7. That makes sense. That's what they used the 64-bit for, right, was to say, okay, get ready, here it comes.

Steve: Yeah. And, of course, that's the one you want because who really wants that 3GB working RAM limit anymore? That's a reason. And because, I mean, 8GB is so cheap these days. And then there's - so I don't have to worry about it.

So anyway, also in updating news we have another Flash player. IE and Chrome will both update for you. Firefox is generally doing a good job about telling you when you've got an out-of-date version and will warn you. So what I'm - and I was thinking about this relative to Java. We were talking about Java. Oh, and I should mention Java will be updated again next Tuesday. So that'll be on Tuesday the 16th of next week Oracle will be rolling out their next fix for Java, which is nice because it means it's not an emergency. They're saying, okay, we've got some things to fix, but you don't have to hyperventilate.

Leo: Probably not.

Steve: It really does seem to me that what we're going to be seeing as a clear necessity while we've got these vulnerable plugins that continue to be problematic is, if they're not being proactive about taking responsibility for themselves, the hosts of the plugins, meaning the browsers, are going to have to take proactive care of their users, which means either updating automatically, which is probably the best solution...

Leo: That's what Chrome does.

Steve: Or at least warning. And IE10 now does, too.

Leo: You know, I also think that - am I wrong, but I gather that of course bad guys are looking for third-party apps now because Windows is pretty well patched, and people are running software to protect themselves and so forth. So they look for holes in third-party software. But for the most part, it's browser plugins that are the real issue. So...

Steve: Yes, we've seen a change. We really have - for a while PDFs, remember, were just being attacked with abandon. That just - it was really bad. But...

Leo: Because you could get a browser to auto-launch a PDF. And if you had Adobe Reader installed...

Steve: And even your email client. Your email client, too, so sending people phishing mail. But Adobe, to their credit, they did implement sandboxing technology which has gone a long way, I mean, it took them forever, which is - we can hold their feet to the fire because it took them so long.

Leo: It took Microsoft a long time to get Windows locked down, too.

Steve: Oh, yeah, yeah.

Leo: It may just be this is kind of a hard thing to do without breaking stuff. Right?

Steve: It is definitely - security, I mean, the subtitle of this podcast is "Security is hard," and only fun for we observers, not for those who have to worry about mistakes they may have made. So, yeah. But, yes. So we're seeing a migration. We'll be talking about some Skype malware which has now become another target, another vector through which this stuff can get in.

Leo: And of course Microsoft wants you to keep Skype running all the time in the background. That's the plan.

Steve: Well, why wouldn't you?

Leo: Yeah, why wouldn't you?

Steve: So Comcast also has a page. We talked last week about Cox having a page where they list all the ports they're blocking. I'm still working on advances to the fingerprinting, the SSL/TLS/HTTPS fingerprinting technology, which has been a big hit over at GRC. So I haven't yet been able to look at updating ShieldsUP!. But what I want to do, remember what's happened is it's confusing some people because we're detecting when some ISPs send back notification of their own preemptive blocking of traffic prior to it getting to the user. So what I want to do is to add to the "open," "closed," and "stealth" status, add a fourth kind of port which would be "intercepted."

Leo: Whoa.

Steve: I think that's the perfect word.

Leo: And you'd be able to sense that.

Steve: Well, that's the problem is not all ISPs do echo something, but some do. So for those who do, now that I know they're doing it, I really can't say you're stealth. I mean, you may be, but your ISP is not, even though it's not really you. Anyway, it's confusing. But I'm going to - yes, there'll be a fourth port state which will just provide more

information to the user, and that's the whole goal, anyway.

Leo: Cool.

Steve: So Comcast is not blocking port 1900, which we wish they were, the Universal Plug & Play port. They're blocking the standard suspects: 25, of course, which is SMTP for keeping spam relays and spammers. They're blocking UDP port 68, which is DHCP, and that makes sense. You could just get up to mischief with that. There's no reason for that to cross the border. They are, of course, blocking Microsoft's famous NetBIOS ports, 135 through 139. They're also blocking SNMP, which I thought was interesting. That's the simple network management protocol, which can be used for configuring equipment, but mostly it's used for monitoring. All kinds of routers and equipment publish their, like, counters so that you can query bites in, bites out, bite rates, and so forth. You can actually pretty much probe the configuration of a router through SNMP if it is not secured. And of course it's typically not, unfortunately. So they're blocking that.

And port 445, which is the other Microsoft, the SMB protocol through which - which is file and printer sharing. Then also RIP, which I thought was interesting. That's the routing information protocol which routers use for exchanging their routing and updating their routing tables with each other. So that makes sense, again. I mean, I'm sure they have a way of securely moving that in and out of their own network for their own routers. They would have to do that. But it doesn't make sense for clients to need that. And finally the SOCKS proxy port, 1080...

Leo: Really.

Steve: ...is being blocked. So, just because, again, more mischief that the hackers would use. Lord knows what's got 1080 open. Probably all kinds of things.

Leo: Right.

Steve: And I saw a really interesting blurb that I thought, uh-huh, well, this is not really very surprising. This is Verizon high-speed Internet, the Verizon DSL service, is beginning to roll out large-scale NAT for its users. Which means - and this is something we could have anticipated. We've talked about some ISPs doing it in the past. So this is not the first. But Verizon is switching. And so they call it "CGN." And they said in their explanation, "What is CGN, and how to opt out."

They said, "The number and types of devices using the Internet have increased dramatically in recent years and, as a result, address space for these devices is being rapidly exhausted. Today's technology for IP addresses is referred to as IPv4 (Internet Protocol version 4). The IP addresses aligned with IPv4 are expected to be depleted at some point in the near future." Notice it was supposed to be last summer, but we...

Leo: Someday.

Steve: Yeah, eventually we're sure we're going to run out. "The next generation of IP

address space is IPv6, which will enable far more addresses" - like five per grains of sand, anyway, "...to be assigned than IPv4. Unfortunately, most servers and other Internet devices will not be speaking IPv6 for a while, so IPv4 will remain standard for some time to come. During this transitional period, in select areas for high-speed Internet residential customers, Verizon will be implementing Carrier Grade Network Address Translation (CGN or Carrier Grade NAT). Verizon FiOS and Verizon Business customers are not impacted at this time by the change. This transition will enable Verizon to continue serving customers with IPv4 Internet addresses. CGN" - again, Carrier Grade NAT - "will not impact the access, reliability, speed, or security of Verizon's broadband services." In fact, and this is me editorializing, it will improve security. "However, there are some applications such as online gaming" - whoops - "VPN access" - whoops - "FTP service, surveillance cameras, et cetera, that may not work when broadband service is provided via a CGN. For our customers utilizing these types of applications, Verizon provides the ability to "opt out" of CGN.

So this is interesting. What this says is they are - Verizon is looking at their overall IPv4 pool and seeing that they're having to begin prioritizing. I would, I mean, the truth that is being said, not publicly but in internal meetings, is the techies are saying not everybody needs a public IP. And they're right. Your mother, Leo, may not need a public IP. She wouldn't know if she had one or not. And so Verizon is saying we've got to start prioritizing. We want to give business-grade customers a public IP. We want to give our FIOS customers a public IP. So those who are paying more and need for various reasons a public IP are going to be able to keep one. But a vast population of our customers simply don't need that. And so the point is they will get a 10-dot IP.

So we've seen ISPs doing this before. And the reason I mentioned it increases security is for exactly the same reason a NAT router ever increases security. And that is that unsolicited traffic hits the NAT router and has nowhere to go. So essentially that means that Verizon will have a router outside of everybody else's router, and it'll be sending 10-dot IPs to the residential customers, and their routers will then be turning those into 192.168 IPs. So we'll have two layers of nonroutable IPs before you get out to a publicly routable IP.

So this is foreseeable. This is a major ISP looking at their available pool of IPv4 space and saying, okay, we need to reclaim a bunch. And this is a reclamation because right now they've got enough that all of their customers have had a public IP at their location. So Verizon is going to reclaim massive swaths of public IP space, except for people who say, no, no, no, really, I know enough to know I need one. I'm a gamer. I need a VPN into my home network. I have surveillance cameras all over. I need to be able to get to them when I'm traveling to see what's going on and so forth.

So I think Verizon's acting in a reasonable and a foreseeable fashion. I think it's very nice that they're allowing, on the granularity of the customer level, their individual customers to say, no, please, I know enough to know I need this. And for people who don't, it's like, eh, you get a little more security because nothing unsolicited will ever hit your router again, all that noise, that IBR. That's a term I haven't used for a long time. That's the term I coined, "Internet Background Radiation," the worms that never die, still out there. Code Red and Nimda are scanning around, looking for open ports.

Leo: And they never will unless ISPs block those ports, like, everywhere; right? Wouldn't they die after some sort of critical mass of blockage?

Steve: The problem is there's random things...

Leo: Windows 95 machines that are sitting in a closet just continue to try to spread them.

Steve: Precisely, yup. And you know Windows 95 never crashes, so it just keeps going. I'm sure you heard about this. A subcontractor that Walmart uses, VUDU, had a...

Leo: Oh, unbelievable.

Steve: Yeah, a physical break-in to their facility which stole the computers containing hard drives with all of the account information of their customers. Now...

Leo: That's a physical break-in.

Steve: Yeah, exactly. This is not - and this is what makes this different than what we normally talk about. This is not the persistent threat coming from overseas anywhere. This is somebody stole their equipment, their servers, or whatever it is they were using to maintain their account information. Now, it's a little distressing that it took 16 days for VUDU to get their act together and send email. Of course they just lost all of their databases, so they may not have known their customers' email addresses.

Leo: Oh, maybe that's it. Yeah, maybe that's what took so long.

Steve: Yeah, they had to, like, go back to their backups or something in order to find their...

Leo: I got the email. What they said is that it was only the last four digits of the credit card, thank goodness.

Steve: Yeah. So what they said was we want you to know "that there was a break-in at the VUDU offices" - that's V-U-D-U, by the way, offices - "on March 24, 2013, and a number of items were stolen, including hard drives. Our investigation thus far indicates that these drives contain customer information, including names, email addresses, postal addresses, phone numbers, account activity, dates of birth, and the last four digits of some credit card numbers. It's important to note that the drives did not contain full credit card numbers, as we do not store that information. Additionally, please note that, if you have never set a password on your VUDU site and have only logged in through another site, your password was not on the hard drives. While the stolen hard drives included VUDU account passwords, those passwords were encrypted. We believe it would be difficult to break the password encryption."

Leo: By the way, they said "encrypted," but I didn't hear a word "salt" in there anywhere.

Steve: No. Correct. And we don't know, when they say that, we know they probably mean a one-way hash. And we don't know what hash, or salted and so forth. So it's good that they did something. They said, "But we cannot rule out the possibility, given the circumstances of this theft."

Leo: You know, it's so trivial to password-protect a hard drive.

Steve: Oh, I mean, this is - there's never been a better case study for TrueCrypt and whole drive encryption. All they had to do was to do that, and they could just - they would say, well, okay, zero impact from the theft of our hard drives. Zero.

Leo: Yeah, because they can't get it.

Steve: Yeah.

Leo: So stupid. I mean, I do that on my portable drives because I figure I could leave it lying around, and I don't want anybody to get into it.

Steve: Yeah. So they did something not quite right. And they're, like, saying, oh, "We think it's best to be proactive and ask that you be proactive as well. Security precautions: If you had a password set on the VUDU site, we have taken the precaution of expiring and resetting that password." But that's not true.

Leo: What? Really?

Steve: Because, well, because listen, then, to the instructions. "To create a new password, go to VUDU.com. Click the Sign-in button at the top of the page. Enter your current username and password.

Leo: Oh. Well, then, if the bad guy has my password, that's all he has to do.

Steve: Yeah, exactly. They did not expire.

Leo: Pretty stupid.

Steve: Yeah, they did not expire and reset them.

Leo: No.

Steve: They're just saying we're going to make you do that. So it's like, okay, not so smart.

Leo: What the heck?

Steve: Especially when they waited two weeks...

Leo: Unbelievable.

Steve: Yeah.

Leo: Well, I will go in and change my password and then kill my account because I don't really need VUDU. It's like iTunes or any of these...

Steve: Leo, we need you to have VUDU so that, if I don't see...

Leo: So I get the email.

Steve: Yes, so that, if I don't receive these letters, you will. This was sent to me by a listener, and I thank you very much. And they do offer - they're giving everyone a free one-year protection by something called AllClear ID. Unfortunately, it's probably a scam, too. I'm sure...

Leo: I'm sure Walmart owns it.

Steve: And it's probably to get people addicted, hooked into the service.

Leo: Yeah, automatic renewal, yeah, yeah.

Steve: Exactly, yeah. So we do have an interesting little bit of news about a forthcoming Firefox. We've already talked about 22, which is somewhere in the early summer. This is v23. I get a kick out of the fact that they know that the pre-beta will be released next month on May 17th. I don't know, how do you know that?

Leo: That's how you get developers to commit to a release date. That's how that is.

Steve: They must have a crystal ball.

Leo: Okay. We're committed now, kids. We're in.

Steve: And the final release will be occurring on August 6th, just for all of you who would rather wait.

Leo: Okay. All right.

Steve: What's different is that, in Firefox 18, which is a couple versions ago, I think we're all on 20 now, Firefox 18 introduced one of those settings that's, like, there's a bazillion of them. If you go about:config, there's so many that you can't even begin to look through them. You have to then use the search box to kind of begin to narrow them down. So, but that's cool. They had a setting they added called security.mixed_content.block_active_content. So again, security.mixed_content.block_active_content. That was - they put that in there so that people could poke around with it and experiment. With v23, which we'll all officially get who are on the release channel on August 6th, in a couple months - well, actually May, June, July, oh, no, more than a couple months. It'll be in beta, pre-beta for quite a while. It'll be for the first time turned on by default. What that makes is that insecure - so insecure scripts, style sheets, plug-in content, inline frames, web fonts and web sockets will be blocked on secure pages.

Now, okay. This is not - if you went to an insecure page, nothing happens. But there are websites that are - the page itself is delivered securely, but then they contain non-HTTPS links to insecure content. Now, browsers have long been able to and often would pop up a mixed-content warning. Mixed content just means the page is secure, but this page is asking me, the browser, to retrieve some other objects to populate the page which are not secure. What should I do about that? So Firefox has just been permissive and warning. They're going to stomp on that now. Now, this is not display content like images, videos, or audio. So that's important. This is active content that's going to be blocked.

So I think this is a nice step forward for security. They're announcing this. They're trying to make developers aware because this will break things. I mean, this has the potential to break some sites that are actually not operating as securely as they should. So breaking shells is how you get eggs. Or something.

Leo: You can't make an omelet without breaking some proxy servers or something.

Steve: That's what I was looking for. Now, there was a bunch of noise about iMessage this week.

Leo: Oh, yeah. This was a fake, I think.

Steve: Yeah. And I'm not even sure what was going on. But as...

Leo: I can tell you what - I can fill you in.

Steve: Fill me in. Fill us in.

Leo: CNET kind of misunderstood a DEA alert that was sent out to police

departments saying, if you see some holes in the data request SMS messages from carriers, you should just know that that's probably iMessage because that data is encrypted, not unencrypted. And CNET interpreted that to mean, oh, good, use iMessage because the police can't read it. But of course Apple will happily hand over the contents of your iMessage upon request by police.

Steve: And we know that they do have the messages because, if your phones are off, and you turn them on, you then receive your backlog of iMessages which Apple had been storing for you.

Leo: And maybe they even save them if you delete them. We don't know because Apple doesn't say. And we know that Apple can get into them because of course they can recover your password. So even though they may be encrypted on Apple's servers, Apple has the password.

Steve: Well, yeah. And they've never documented the protocol, which is more worry than not. Bruce Schneier in his blog, as always, succinctly cut through this. He wrote, "The U.S. Drug Enforcement Agency has complained," he said, "(in a classified report, not publicly) that Apple's iMessage end-to-end encryption scheme cannot be broken. On the one hand, I'm not surprised." This is Bruce Schneier talking. "I'm not surprised. End-to-end encryption of a messaging system is a fairly easy cryptographic problem, and it should be unbreakable. On the other hand, it's nice to have some confirmation that Apple is looking out for the users' best interests and not the governments'." And he fixes this in a second. And he says, "Still, it's impossible for us to know if iMessage encryption is actually secure. It's certainly possible that Apple messed up somewhere; and, since we have no idea how their encryption actually works, we can't verify its functionality. It would be really nice if Apple would release the specifications of iMessage security."

And then to that he added an edit on Monday. So several days later he said, "There's more to this story: The DEA memo simply observes that, because iMessages are encrypted and sent via the Internet through Apple's servers, a conventional wiretap installed at the cellular carrier's facility" - exactly as you said, Leo - "isn't going to catch those iMessages along with conventional text messages. Which shouldn't exactly be surprising. A search of your" - and I love this. Bruce says, "A search of your postal mail isn't going to capture your phone calls, either."

Leo: Exactly. It's looking in the wrong place.

Steve: "So they're just different communications channels. But the CNET article strongly implies that this means encrypted iMessages cannot be accessed by law enforcement at all."

Leo: Not so.

Steve: "That is almost certainly false."

Leo: Apple even says in their terms of service, we will turn your stuff over.

Steve: Yes. And he says, "The question is whether iMessage uses true end-to-end encryption, or whether Apple has copies of the keys."

Leo: But we know they do.

Steve: Yes.

Leo: Because they can recover your password.

Steve: Yes.

Leo: Right? Doesn't that mean that they...

Steve: They could be using ephemeral keys and giving us what's called "perfect forward secrecy." And in fact the protocol, there has been some reverse engineering done of a version of the iMessaging protocol on a Mac, where the guts were more accessible to the guy doing the reverse-engineering. And what he discovered was an amazingly complex mess.

Leo: Good. Or it might be good.

Steve: So, I mean, it has got certificates flying back and forth and all kinds of stuff. So if nothing else, if somebody really did go overboard, and of course that's not always a good thing because it's more easy to make mistakes in something complicated than in something simple. And in this day and age, as Bruce says, end-to-end encryption is trivial. You do a Diffie-Hellman handshake to exchange a key, nobody in the middle is able to intercept that as long as you've got authentication of the endpoints. And presumably that's easy to have now, too.

Leo: Yeah. So in a way that kind of - the complexity of what they've implemented kind of lends one to think it's not very good.

Steve: Yeah.

Leo: As opposed to good. Since it would be very simple to implement it well.

Steve: Yes. We now have a...

Leo: I would think a company like Apple would just prefer not to know. Like just do it right, and then you can say, I don't know. We don't know. Go away. Wouldn't that be easier for Apple than to say, all right, I got a subpoena, let me go look.

Steve: Well, and I didn't cover it this week in my notes because I forgot about it, actually. But I'm sure you saw in the news Google really fighting back.

Leo: They do.

Steve: Which is nice to see.

Leo: I'm proud of them, yeah.

Steve: Yes, I am, too. They are saying no to these warrantless requests for information.

Leo: And to their credit, they have a - this is very un-Apple-like. Google has a transparency report they publish and lets you know how many requests they get, how many they've turned down, how many they've accepted. They can't, unfortunately, because of the Patriot Act, they cannot reveal raw numbers on certain requests. But I think Google does the best of anybody, at least - and Twitter's now doing this, too, by the way - at least letting people know what's going on, what governments are asking for what information.

Steve: Yeah, because as citizens we need the information. We need the feedback in order to vote intelligently.

Leo: Exactly.

Steve: That's the way democracy works. So speaking of democracy, we have a Bitcoin section, Leo, because there's enough Bitcoin stuff going on.

Leo: I love it. Because I have bitcoin. I'm interested now. Suddenly I'm interested.

Steve: Do you know that a 42-year-old media entrepreneur named Jeff Berwick is going to be bringing bitcoin ATMs to a city near you soon?

Leo: Yeah. Well, to a couple of countries where they don't like the currency anymore.

Steve: Yup. Cyprus is getting one, as is L.A.

Leo: Oh, that's interesting.

Steve: L.A. is probably just because people are hip, I guess. The article in CNN's Money section said that Berwick expects to put the first ATMs in Los Angeles and Cyprus in the next...

Leo: So how does this work? I give him money and he gives me bitcoin? Or I give him bitcoin, he gives me money? How does this work?

Steve: The machine is connected to the 'Net. And so you're able to transact your bitcoinage with cash, cash of the local currency.

Leo: Wow.

Steve: Yeah.

Leo: Wow. So it knows. I'll have to enter my passphrase or what? How do I identify myself with bitcoin? Is it a...

Steve: You'll have to have your Wallet online and appropriate security. But the idea would be, if you have bitcoinage in an online account, then you will be able to go to one of these machines and get money.

Leo: Wow.

Steve: Isn't that cool.

Leo: So I want to thank the 19 people who have given us bitcoin, totaling now a little over one whole bitcoin. I said we'd have it on the website, and I thought we would, but Radford didn't implement it. So I will ask him where the hell it is. For those of you wanted to give us bitcoin, I apologize. But I will - I can show you the QR code again, if that helps. You know, 19 people did this. This is what's going to be on the website eventually anyway. And I'll paste into the chatroom this bitcoin address. So this long - it's not hex. It's a long number and alphabetic string is my bitcoin identifier; right?

Steve: Yes. That is a globally unique ID of you. That is, that's what makes you anonymous. You're just that to the bitcoin system.

Leo: Oh, now I'm not so anonymous anymore.

Steve: Well, yeah.

Leo: But you can make many of these.

Steve: Yes, you can have - exactly. Yes, you can have as many of those as you want. And there are people who looked at the anonymity, and I've seen things, "Bitcoin's not as anonymous as you think" and so forth. But you have the facility for doing that. Unfortunately...

Leo: A donor would be anonymous to me, though; right? I can't tell who they are unless they say so because they're donating from their Wallet, which I don't know who that is.

Steve: Right.

Leo: And that's probably more important to them.

Steve: And of course the bad guys are involved. We've seen, I'm sure people have seen, I mean, in fact the currency has fluctuated because of major break-ins that have occurred in some of the various exchanges. It never really seems to dent the coinage very much. It recovers pretty quickly. And I think, as I said, once there are many more exchanges, and ATMs on every corner, people won't care that much. And it'll also distribute any damage far more widely and broadly.

But there is now malware that is getting installed via Skype. Skype messages come up asking you to click on something, something alluring. And among other things, Kaspersky discovered last Thursday a Win32 trojan they named Jorik.IRCbot.xkt. And what's funny is it installs a bitcoin mining engine on the user's machine and, not surprisingly, pins the CPU at a hundred percent. So you're suddenly thinking, gee, why is my Internet so slow? And why is my mouse not really keeping up with my movements and so forth? Well, yes, it's because your computer is frantically and somewhat fruitlessly attempting to mine bitcoins. So it joins you to a large bitcoin mining operation and saturates your CPU.

I don't imagine it will stay hidden on anyone's machine very long because the only chance it has of mining with any chance of success, I mean, and which is diminishingly small, we'll cover in a second, is really burning up cycles. Maybe if your screensaver were on, and it came to life, that would help it stay hidden, if anyone even uses screensavers...

Leo: It goes to a hundred percent right away; right?

Steve: Yeah, just pins it. It's like, okay, whoa. Now, several people mentioned that - because you and I were talking about inflation, and we were misusing - we were using the wrong term. With bitcoin value jumping, that's deflation.

Leo: Deflation, right.

Steve: Yes. James Parsons, @PolicyEconomy, tweeted me. He said, "Bitcoin deflation, not inflation. Bitcoin is currency. 1 BTC buys less stuff is inflation. 1 BTC buys more stuff is deflation."

Leo: Right.

Steve: And at midday Monday, a bitcoin was at $194.73. This morning when I looked it was at $232.

Leo: Holy mackerel.

Steve: With the last 24-hour maximum at $266 per bitcoin. So it has been going up dramatically. But what I thought of when I saw that was this changes the mining equation dramatically.

Leo: That's right.

Steve: It really does.

Leo: It makes it more feasible.

Steve: Go look at that link before I mention it, Leo, that's right there.

Leo: Yeah. Go ahead.

Steve: Just so you can bring the page up. These guys, ButterflyLabs.com, they are the people who are - and they've got an ASIC, an Application Specific IC, a little, cute little black box, the Bitcoin Miner, which is available for preorder.

Leo: It's cute.

Steve: It is. It's got a little red button there, little red dot saying I'm cranking away here.

Leo: Mining. Mining.

Steve: Okay. This is 50 gigahashes per second.

Leo: Is that fast?

Steve: 50 billion hashes per second. It blows everything else away.

Leo: You're kidding. It's only 2,500 bucks. I could be rich. All I'd need to do was get, what, two bitcoins, no, 10 bitcoins, and I'd be...

Steve: Actually what's interesting is that I could take the 50 I made, sell them now, and buy four of those with a couple grand left over. So, now, the problem is this is not - you and I are not the first people to have this idea, Leo.

Leo: Yeah.

Steve: But my point is that, with this kind of deflation of the bitcoin, it means that these machines are incredibly cheap in bitcoinage relative to their ability to mint coins. The other thing it means is that all this will do is instantly change the landscape of how difficult it is for the rest of us to make bitcoins.

Leo: By the way, you don't have to cash in your bitcoins. You could just pay for it in bitcoins. They take bitcoins.

Steve: Of course they do.

Leo: [Laughing] But I think some of this is speculative, that people are figuring that the value of bitcoins is going to go up a lot; right?

Steve: I think that's certainly the nature of speculation.

Leo: It's speculation, a lot of this.

Steve: Yeah. I would say, if you look at the curves right now, they're just too new. I mean, this thing is just going up crazy. And as I said to you before we were recording, I think it is so fun that we and our listeners are getting to participate in this. We covered it years ago. I turned on just a regular i7, a core i7. It woke up after two days, and there was 50 bitcoins.

Leo: Stop telling people about that.

Steve: Those were the days, my friend.

Leo: Those were the days, yeah. It not going to happen now.

Steve: That's not the case anymore. That won't work.

Leo: By the way, bitcoin now is down to $140 at Mt. Gox.

Steve: Wow, that's an amazing drop.

Leo: It's extremely volatile, you should realize.

Steve: I looked this morning, it was 231.

Leo: Yeah, it's extremely volatile.

Steve: What does Mt. Gox - across the top it'll show you the low in the last 24 hours.

Leo: Yeah, the low is 111 bucks.

Steve: Okay. And the high is still...

Leo: The high is 266, yeah. You saw the high. Weighted average, 219.

Steve: Well, and remember what happens. When these kind of highs hit, people cash out. There are people who are saying, whoo, I'm leaving now. And so they sell off...

Leo: It's like the stock market. You get sell-offs.

Steve: Exactly like the stock market. And that depresses the currency for a while. And it'll come back.

Leo: So Radford just came running in. The bitcoin QR code on our website is now up. So go to TWiT.tv, the front page there, and wait till the rotator comes around. And now I think we're going to get tons of bitcoins. Tons.

Steve: I do really, really think it's cool that we covered this back when it was just nascent, when it was happening. We talked about the technology. I said this thing works. And in the fullness of time, I mean, during the podcast we're getting to see the birth of a currency, a virtual Internet currency. That is just really cool. We have a Q&A question about some consequences, which I'll wait to get to, which is sort of interesting.

Leo: Good.

Steve: Mark and his team at SmushBox achieved their goal.

Leo: Yay.

Steve: Days ago. Last time I looked, again, a few hours ago, they were at 132 backers. They were at $26,165, with a target of 20K. So they've exceeded their target. They've got nine days to go. Now, Leo, since you are a frequent and somewhat bruised Kickstarter user, click that link there in my show notes because this is very cool. If you did not know before about Kicktraq.com, K-i-c-k-t-r-a-q dotcom, it is wonderful. And look at the charts that these guys show you. So this is a site that monitors Kickstarter projects...

Leo: This is good.

Steve: ...and shows you all kinds of cool stuff, and even, like, worst case and best case projected into the future, based on where you are now, where they will probably be at time of final closure of the project.

Leo: That's neat.

Steve: So, very cool. Kicktraq, t-r-a-q, dotcom.

Leo: Cool. Yeah, I just got an email from my Pebble watch saying, well, because you ordered color, we've had some trouble. Would you like black instead? And I said, yes, just send me something, anything. Anything. Everybody's already reviewed it and decided it's junk anyway.

Steve: Oh. Speaking of junk.

Leo: Yes.

Steve: I'm sorry that I ever mentioned the remake of "The Evil Dead."

Leo: Oh, yeah. See, it got terrible reviews. I was wondering what you thought.

Steve: Oh. I walked out, Leo.

Leo: Oh, dear. Oh...

Steve: The setup was fine. Then trouble began to happen. And after about 20 minutes of just really pointless interhuman brutality, I mean, some I just closed my eyes and waited, listened to the soundtrack to wait for it to be over. I just thought, what am I doing? Why am I doing this to myself? This was - I'm not a, like, I don't like that kind of movie. I don't ever go to see those kinds of movies. This was awful. I called it - I tweeted. I said, "The 'Evil Dead' remake: I walked out. A pointless, brutal gore fest. None of the original classic movie's charm, fun, wit and humor." And I have to say, "The Evil Dead 2," which was the one that then led into "Army of Darkness," it really is funny. I mean, it doesn't take itself seriously at all. It's just wonderful. It's why it's a cult classic. But this remake, oh, wow. I mean, I know there's a market for people who want to go for some reason and see this just incredible gore. That's not me.

Leo: They said it was gory, modernly gory. Yeah, yeah, yeah.

Steve: Oh. Oh ho ho ho.

Leo: Yeah. Oh, well.

Steve: But I mean, oh, yeah, anyway, I've said enough.

Leo: I saw "Justified," by the way. I watched the pilot, and I enjoyed it. Now, is the pilot typical of the whole season?

Steve: Yes.

Leo: Often pilots are different from what happens when they get a green light.

Steve: No. This thing stays good. We're in I think our fourth season. It's got a fifth season already set up.

Leo: It was very funny. It was very funny. I enjoyed it.

Steve: No, but this is - it is, in fact, I've seen some feedback from our listeners who have gone through the first season, and they just - they can't wait to get more. So I can vouch for it. It's terrific.

Leo: Good.

Steve: In nerd humor, Simon Zerafa, who tweets often, sent me something that he

found. I asked him where he found it, and he couldn't really track back its provenance. But I kind of thought it was just clever. He said, "Password must contain a capital letter, a number, a plot, a protagonist...

Leo: I saw that [laughing].

Steve: ...with some character development, and a surprise ending." That's a good one, yeah.

Leo: I love it. It is funny.

Steve: Now, here's 90 seconds, Leo, of - if you want to just inject this video into the broadcast, our audio listeners will be able to hear it. They won't be able to see it. I did tweet this link because this is wonderful. And, you know, Shatner, I just take my hat off to him. He's a class act.

Leo: He is very funny. So it's "Shatner vs. the Gorn." Let me turn on my - is there audio?

Steve: Yeah.

Leo: Is there - oh. This is your review? Wait a minute. Wait a minute.

Steve: No. It's a...

Leo: Oh, no. I got your review of "The Host" for some reason in that link. Let me go to your Twitter.

Steve: What?

Leo: I think there's...

Steve: Oh, my goodness, you're right. It's a bad link.

Leo: Yeah. It's a bad link.

Steve: Wow, sorry about that.

Leo: So let me go to your Twitter, and I'll get it from there [t.co/4JU3LYcMeu].

Steve: Yeah. The Twitter is bit.ly/sggrc, to remind our listeners, if you want to quickly grab...

Leo: It's kind of a long way to go. You could just go to Twitter.com/sggrc.

Steve: Yes, you could. But, okay.

Leo: He makes bit.lys out of us all. All right. Let's just see here. I'm going to scroll down. "The Evil Dead." "Only one year left." "Why didn't I think of that?" "Wonderful time sink." Here you go, 90-second short, "Shatner vs. the Gorn," rated T. Oh, it's a game.

[CLIP] WILLIAM SHATNER: You keep getting me killed. I thought you had my back.

[CLIP] THE GORN: [Grunting]

Leo: You've got to see this to appreciate it. Apparently he's playing a videogame against the Gorn, but with a Gorn. He punches the Gorn. The Gorn punches back. Now they're in a very slow-motion Gorn battle. William's almost 90 now, I think.

Steve: Oh, it was just his birthday, by the way.

Leo: Would be 80-something; right? He's doing pretty good for - oh, he boxes the Gorn's ears. Now they have to take a break. So I guess this is a videogame. This is an ad for it. He's 82. There you go. Pretty good for an 82 year old. That was a recreation, Trekker John Slanina says, that was a recreation of the actual battle - wait a minute. Let's go back.

[CLIP] WILLIAM SHATNER: Now you're over-acting.

Leo: Clinch for clinch, slowly work their way through it, of the actual battle from whatever the first generation...

Steve: Yes. Any serious Trekkie will remember Kirk battling the Gorn where the Gorn is extremely butch. It's a lizard creature.

Leo: It's like Godzilla, a little bit.

Steve: Yeah, it's God- but it moves very slowly.

Leo: Right.

Steve: So, you know, Kirk runs around in circles and dances and bobs and weaves, and the Gorn picks up large foam rocks and throws them, and they sort of bounce unconvincingly as Kirk dodges them. And then finally he, like, hits him simultaneously on the sides of the head, which it turns out the Gorn has very sensitive ears. Who knew?

Leo: He boxes the Gorn's ears, and it's all over.

Steve: Anyway, so anyone, if you're a Trekkie, and you didn't see my link in my tweet to our listeners, I'm saying you really - you need to go find this because it's a treat. And Shatner at 82, I mean, he's not taking himself seriously, and it's a great little piece. So 90 seconds, worthwhile. And while I was going through the Q&A bag, I did see, not a SpinRite note, which is normally the way I sound when I'm getting into a SpinRite, but just a note from Tony Fishpool in Dartford, England, who said, "Wow. Just finished 'Wormhole.' Read all three books in less than a week. All three were page-turners. Thanks for the tip, Steve," said Tony. And I just wanted to remind our listeners, they are up on Audible. "Wormhole" is the third book in the Rho, R-h-o, Agenda trilogy. So our listeners have really been enjoying it.

Leo: Neat.

Steve: And I do have a - now, this is one that, you know, I would say I'm not making this up, but we know I'm not making this up. But you might think, okay, really? Steven C. Zimmerman sent, and we received, on the 7th of April, on Sunday, a SpinRite testimonial. He said, "What a superior program, Mr. Gibson. I work for an international communications corp., and one day a young fellow was complaining about his wife's computer. It had just failed, and all of the recent pictures of his wife's father, who had just passed away, went with the PC. I asked him if I could take a look at it. He said, 'If you can recover those pictures, I'll give you this car.' It was a 1997 Honda Civic Coupe. Well, to make a long story short, SpinRite 6 did its thing. And not only were the pics recovered, but the whole PC is renewed."

Leo: And I have a new car.

Steve: "I gave him the PC, and he signed over the title."

Leo: That's awesome.

Steve: "So, Steve, I can thank your hard work for my current mode of transportation - 31 mpg and still going strong. 241,000 miles on the 'Black Beauty.'"

Leo: Aw.

Steve: Steven Zimmerman.

Leo: He took the car.

Steve: So, Steve, thank you.

Leo: Nice job, Steve. Nice job, Steve. And now we return to Security Now!, already in progress.

Steve: In progress.

Leo: I've got questions for you, Steve. You ready?

Steve: You betcha.

Leo: You feel good? You feel smart?

Steve: Ready to go.

Leo: Let's go with question Numero Uno of our listener-driven potpourri #165, a quickie, a Twitter question from @DanLoFat, which is either a Chinese name or he's been on that low-carb diet or something, I don't know, a diet, in Chicago. Steve, is there a way to mint bitcoins using distributed computing, like through a home network?

Steve: You could certainly have more machines running the bitcoin mining process. But there is, by the nature of the way it works, there is no way to pool their computing resources.

Leo: Ah, interesting. You can't - it's not threaded. You can't thread it.

Steve: Correct. Even bitcoin mining pooling, which is a new thing that has arisen, because the chance of an individual scoring a bitcoin has continued to drop as the number of people minting them has increased, the percentage, the chance of getting one has dropped. So what people have done is they've agreed to pool their resources. And the idea is that, when anyone in the pool gets a bitcoin, they will divide them evenly based on the amount of computing power they have put into the pool.

Leo: It's like when the office buys a lottery ticket.

Steve: Yeah, exactly.

Leo: Yeah, and you share it based on how much you put in.

Steve: Which is nice. So it's suddenly not an all or nothing, but it's a, oh, look, I got - so, and the larger the pool is, the greater the chance that the collective resources of the pool will score one bitcoin, which everyone then shares proportionally.

Leo: And that's the smallest denomination you get in mining is a bitcoin? One coin?

Steve: Yes. One coin per solution to the hash. And that problem keeps increasing. But also remember that every four years the amount you are awarded is cut, is also cut.

Leo: So that's why you got 50, because you got in early.

Steve: And today you only get 25 when you solve the problem. So every four years that's cut in half. And so that will keep going down as the difficulty also keeps going up.

Leo: And as I've learned, because people are donating bitcoins to us, you can donate any fraction of a bitcoin. Bitcoins can be divided kind of infinitely.

Steve: And that's why they have a future. That's why, for example, I've got 50 bitcoins, apparently now worth, depending upon what time of day it is, either $12,000 or six.

Leo: Promise me you won't jump out of a window if there's a bitcoin crash. That's all I ask.

Steve: Nah, [mumbling].

Leo: @ChivalryBean raises a point, though, with bitcoin mining, which is it's not really the cost of the hardware, as you can see. The hardware can be expensive. But it's the cost of the energy you use to run that hardware, and also energy used to cool the server room. He says: Is there any way to measure that energy use on his computer?

Steve: And you know, that prompted me, because this is something I think our users, our listeners would be interested in, there is a surprisingly inexpensive meter, which Amazon sells for $17, called Kill A Watt.

Leo: It's a great thing.

Steve: K-i-l-l A W-a-t-t.

Leo: Love it, yeah.

Steve: And what's cool about Kill A Watt is you plug it into the wall, and then you plug something, an appliance, into it. And you're able to tell it what your electric company charges you for electricity, either across 24 hours or evening versus day if you've got the kind of billing where your power costs less at night than it does during the day and so forth. You're able to put that into it. And it will first measure the gross total electrical usage of whatever it is you have plugged into it and convert that to pennies, convert it into your currency. So you can actually see what this device - so, you know, it might be like a refrigerator. And a refrigerator doesn't draw energy constantly because it's thermostatically controlled, so its compressor switches on and off and on and off and on and off.

So this thing actually measures the instantaneous energy usage and then accumulates it over a growing period, and you're able to look at it and say, oh, this is how much this costs me per month to have this thing on. So you could certainly plug your bitcoin mining box in and figure out if it's time to unplug your bitcoin mining box based on how much it's mining for you. So Kill A Watt, 17 bucks at Amazon.

Leo: Good deal.

Steve: Yeah.

Leo: And we've talked about those, I think on the Giz Wiz, and you even used them and so forth. So, yeah. David Johnston, Sydney, Australia, asks: Do you mean to say the RC4 implementation in TLS is broken? Hey, Steve. Love the show, blah blah blah. I now feel bad for having written that [chuckling]. Regarding the recent...

Steve: That's nice.

Leo: I know, I like that. Regarding the recent news involving RC4 and TLS, does this mean that TLS fails to warm up the cipher? I regard failing to warm up the 256-bit array is failing to correctly implement the cipher. So is the situation actually one of widespread implementation failure? And, if this is true, I'm bewildered, as every textbook says the cipher needs warming. Also it should be noted that a warm-up run of 256 operations was only ever the recommended amount. I use 1024 just to be sure. I don't know if anyone had fully determined that 256 was enough before now. Do you know where that number, 256, originally came from? Thanks for the great show. Dave Johnston, Sydney, Australia. What the hell's he talking about?

Steve: So, okay. What we talked about, I think a couple weeks ago, was the cryptanalysis of the use of RC4 in SSL/TLS/HTTPS, the secure web communications, where if there was some way to cause the browser to repetitively emit exactly the same query, then because the same plaintext was being delivered over and over and over, the slight statistical variances at the beginning of RC4 would show themselves. And it turns out it was much worse than was believed.

So what happened is that RC4 was really badly implemented in the original WEP WiFi encryption. There, there was no warming being done. And so it was really bad. There were bad keys. And there was very - the keys related to the pseudorandom bitstream coming out of the cipher strongly. So they fixed that by warming it up a little, but not enough. They thought at the time it was enough, but no one really looked at it to say is 256 - is discarding the first 256 bytes from the cipher enough? I don't know why they didn't do 1024. David is doing 1024. I'm proud of him. We all wish that the world was doing 1024 because all of us are having to put RC4 at the top of our server list in order to avoid the BEAST attack, which attacks unless you don't have RC4 as the preferred cipher for the server to choose among those the client is making available. Unfortunately, it's not as strong as we wish it were.

So what we really need to do is move ourselves away from SSL 3.0, which is the same as TLS 1.0, and get up to 1.1 and 1.2 universally, which does no longer have the problem that the BEAST attack uses. Then we'll be able to pull RC4 down off the top of the list. Or we could do another version of TLS, although I don't think anyone wants to, where we just warm RC4 up further in order to get the non-sufficiently pseudorandom off the front of the key stream. So it's just they didn't look close enough. They thought 256 ought to be plenty, but they didn't really analyze it. When they did, they said, oops.

Now, again, remember, it takes, what is it, 2^40, like 2^40 identical queries from the browser. 2^32 is 4.3 billion. So 2^40 is an additional 256. That number seems high, so it may be less than that. I'm not quite remembering the number. But still, it's a disturbingly low number from crypto standpoint, meaning that it's a theoretical vulnerability. And here we are. We have to have RC4 first in order to avoid BEAST. But we're not happy with RC4 being chosen because there's a theoretical problem. So right at the moment we're in this awkward place of not really having something that - any solution that works as well as we would like, until we get clients and servers that are able to move to the newer versions of the TLS protocol. Whew.

Leo: Whew. Would it be better to pick a random number of times to warm it up between 256 and 1024, something like that? Or does it matter? There's no recycling in the warm-up, is there?

Steve: If you chose a random number, then you would need to transmit that to the other end so it knew how to...

Leo: Oh, okay. They both have to do the same.

Steve: Exactly, they have to be synchronized.

Leo: Got it. Opher Banarie, a regular in many of our shows, including the Giz Wiz, as well as apparently Security Now!, in Chatsworth, California, has some thoughts about defeating employer spying: As a longtime SpinRite owner, listening to Security Now! since No. 1, Numero Uno, I must speak up about defeating employer "spying" approaches. While we could debate the pros and cons of employers implementing systems that can track employee activity on company computers and networks, there is one obvious element: They can. Not only does the technology exist, it's legal for them to do so. Most employers now have a policy statement about limiting

employee use of computers to company business. Many of these policies include termination as a consequence of violating the policy.

Rather than defeating such systems, maybe people need to ask, hey, if I'm so worried that my employer might see what I'm doing during office hours, maybe I shouldn't be doing it. I understand how your advice is helpful in public access locations. But in the office, it's pretty obvious we should be working on company business. He does have a good point. I have to agree with him on that. Right?

Steve: Yes. And...

Leo: As a boss.

Steve: So I guess my branching-off point here is to say, I'm not suggesting that it's wrong. I've never suggested it's wrong. I'm only, as always, looking out for the end-user. And I just want the end-user to be informed. So I'm not, I mean, at no point, for example, is my SSL fingerprinting meant to say this is bad for employers to be doing this. I'm just saying I would like to empower users to know. And I've said on this podcast before, every such - all of the machines being monitored should have a half-inch-high strip permanently affixed to it that says all of your Internet communications within this company and on this machine are subject to monitoring for the protection of the company, for antimalware filtering and so forth. So act accordingly. I mean, it ought to be right there.

But the problem is you get into this situation where the management doesn't feel comfortable being that blatant. Or maybe they add the technology just to sort of test to see how it goes. And it's like, oh, well, we'll tell people later if we end up keeping it, so forth. It's like, eh, I just want to empower people. So I completely understand that, in the era of malware, as we end up with HTTPS everywhere, always having secure connections, not just during login, but all of our communications, a company needs to be able to filter what comes in and out of their network onto their machines. After all, the machine is the terminus of this. And so I get that.

All I want is for the end-user to be able to see. And in fact, I would argue that my stuff helps people know that they are being monitored so they will respect their employers' intentions for the way the computer network would be used.

Leo: Yeah, I mean, speaking as a business owner, I'm liable for stuff people do on my computers.

Steve: Yup.

Leo: And if they're surfing porn, and somebody sues us for harassment, it's our fault. So we don't monitor because I trust my employees, but I would - when I've been an employee, I've assumed that anything I'm doing is visible on the corporate network. Just assume that. If you want to check out through Steve's systems, check out whether they are monitoring it or doing a man-in-the-middle on the SSL

certificate, that's fine. But assume, you should assume you're being monitored.

Steve: Yeah. Back when I had 23 people, there were some embarrassing things that got - that came out of the printer. We had a - it was back in the days of network-shared printers. And I think on email the print button was right next to the next message button or something. And, oh, there were some interesting things coming and going.

Leo: Yeah. Just assume that, I mean, there's a legal responsibility. And of course I've always said that employers have the right to do that. You're not going to win in that case. And it'd be prudent to just assume it. Right?

Steve: Yup.

Leo: I think. Mike, anonymous for reasons that will become clear to all, received an odd UPnP result on your tester. Steve and Leo, long-time Security Now! listener, love the show. Couple of weeks ago I ran the UPnP scanner while at work. I can't figure out how to interpret these results. The test reported that we did respond to the probes. However, the IP reported was 10.1.1.1. I'm thinking we're vulnerable, but I wanted to get your opinion on the results first before telling the appropriate people. I'm sure our security team will be keenly interested if we are indeed vulnerable. We found out about six months ago we had a breach and that the bad guys had been in there for quite a long time. Whoops. So they locked the wrong door. Thanks for all you do, and all the advice and insight you've given over the years.

Steve: Okay.

Leo: What is the 10.1.1.1 result?

Steve: Well, Leo, if you bring up Google and search for "UPnP test" and look at the first link that comes up, guess who?

Leo: UPnP test. Good job, Steve Gibson. You're No. 1.

Steve: But...

Leo: And then who's No. 2?

Steve: But, no. No. 1, it's not the test, it's the sample page.

Leo: Oh, that's funny. The Google result says "UPnP rejected." So if you click that,

and you thought that you were being tested, that's - oh, it's good you put a banner up there now. This is good.

Steve: Yes. That big red banner, you cannot possibly miss the fact.

Leo: That's cool. And it even scrolls along with it. That's good. Nice job.

Steve: Thank you. I did that...

Leo: A little CSS, baby.

Steve: I did that yesterday morning. Somebody - I had a Twitter conversation. I mean, I would have been puzzled by Mike's comment even now. But a guy named Ryan and I went back and forth night before last because he was actually trying it, saying, Steve, I'm sure my IP is not 10.1.1.1, and so forth. And so finally, when there were about three or four tweets back and forth, and he said, oh, I figured out, he says, I got the link from Google, and it's the sample page. He's like, ohhh. And so, yes, I immediately...

Leo: Well, you were smart enough to use 10.1.1.1 for your sample IP address, which is good. That's kind of a hint there; right? Because that's an unroutable address. That's a reserved address.

Steve: Right, exactly. Well, actually it's my own internal network. And I forced that IP, which is not a machine, so that it would not respond to anything, in order to generate that test and capture the screen and so forth. So anyway, so, yeah, I put up - so, Mike, the answer is, and I did respond to Mike already when I saw his email, that was the sample page. I immediately put up a banner to notify all future visitors because there had been some confusion, and I just didn't realize, I wasn't worried about it until I saw that Google had indexed me in the No. 1 result when you look for UPnP test.

Leo: Good job.

Steve: Yeah.

Leo: Now, you know about robots.txt; right?

Steve: Yeah.

Leo: You could exclude that page in robots.txt so that Google wouldn't index it in the future. But you don't want to hurt your result, though, so...

Steve: Well, what I need to do, right now I'm unhappy because you've got to go, to get to that test, you have to go down in through ShieldsUP!, and you get this weird-looking URL which is uncomfortable. And I just need to make it...

Leo: But Google spiders through it; right? So I don't know why it used that as the result, however. That's odd.

Steve: Yeah, yeah.

Leo: Anyway, I'm glad we could clear that up, and good idea with the banner, that's cool. Guy in Nottingham, England, found a - I know it's "Guy" because he's in Nottingham. If it were in Paris, France, it'd be "Gi" - found a port opened by his TV box? Running ShieldsUP!, I noticed port 1024 was open, something I've never had before on my occasional checks. I looked at my router and found that port 1024 was being forwarded to 8081 on the IP for my new TV recorder box. This runs a new service, YouView, here in the U.K. which includes Internet on-demand TV. I scanned the open port 8081. It reported a service called - this is scary - blackice-icecap running. Now I'd be running for the dictionary. Should I be worried about this activity? Thanks for the great informative show. I've learned lots over the years. I wish I could say I grasped everything fully. Oh, and my router does not have the UPnP problem. Whew. So thanks for yet another great tool. By the way, that's at ShieldsUP! at GRC.com, if you want to test. Regards, Guy, Nottingham, England.

Steve: Okay. So here's what's happened. He's got a TV recorder which is using UPnP the way it was intended to be used, to open a port through his router for itself. So, and this looks like it's, I mean, it's interesting that it's 1024. That's the lowest number non-service port available. So it must have said give me whatever port you've got now, and the router said, well, we're starting off at 1024, so here you go. And then what that allows is for incoming unsolicited traffic to go through the NAT router and get to this box. 8080 is sort of the traditional alternate port from port 80 for the web. HTTP protocol runs on port 80. But that's down in the service port range, those ports from 1 to 1023. And in the UNIX world, only services running as root are able to create listening ports down in the service port region.

Leo: Below 1024.

Steve: Right. So users who want to, like, run their own server, needed to use ports above 1024. And so it just became common to use 8080. So this use of 8081 is related to that. It's obviously one more than the traditional 8080. What's significant is this notion of blackice-icecap, when he said "I scanned the open port 8081, and it reported a service called 'blackice-icecap' running. Should I be worried about this activity?" No. What is meant here is that, in the dictionary of what ports different things use, port 8081 was once used by a firewall called BlackICE.

Leo: BlackICE Defender. I remember it, yeah.

Steve: Yes. And so ICEcap was some facility that they had which it chose for itself port

8081. In the same way that FTP chooses 21 and web servers use 80. So if you had port 80 open, it would have said, oh, you have a web service running. This one had 8081, so it's, oh, you've got BlackICE ICEcap running. Well, no, you don't.

Leo: It's just a lookup. It just says this is one thing that uses that.

Steve: Traditionally that's been the port, exactly. And when somebody updates their list, they'll say, oh, you must have whatever that is running on his TV recorder box.

Leo: Yeah.

Steve: Yes. So anyway, you might try disabling UPnP, if this worries you. But this does mean that incoming traffic is always able to go to this TV recorder box. And the only concern would be if it has not been written well, somebody might be able to maliciously take it over and then use it to gain access to your network. So that's always the concern of allowing devices to map ports through to themselves, is then anybody on the outside can get to those devices. And that's a cause for some concern.

Leo: It's easy to think of why it might do that. The service might be pushing TV Guide updates down. Instead of having the machine pull, which it wouldn't have to open a port for, it's pushing it to the machine whenever it's got an update, things like that.

Steve: Right. And so the machine would be advertising to some central server, hey, whenever you've got something for me, this is where I am, at this IP and this port.

Leo: They may even register it. That may be part of the deal when you get the device. Advait in India wonders, why not cloud your servers? You've been sharing the news and adventures of setting up your new servers. But I was wondering, why do you do it yourself? Why don't you virtualize your new servers? Have them reside on some cloud service like EC2 or Rackspace, which you talk about all the time? Or something similar. In this day and age, why mess around with managing your own hardware when you can just have them be virtual machines up in some cheap, highly reliable, highly redundant cloud service? Blah blah blah, effusive praise, SpinRite owner. Advait.

Steve: Well, so the answer is, probably more than anything, control.

Leo: You're a do-it-yourself kind of guy.

Steve: Well, and in some areas I'm a control freak. And, for example, we constantly report here on this podcast of breaches of people's networks and systems that affect all their customers. And I run an eCommerce system, selling SpinRite. And I'm not willing to release responsibility, which I'm fully willing to take, by sending all this off to some virtual cloud and then have Amazon say, oh, we're really sorry. We thought that the

virtual machines were insulated from each other. And we've already seen instances of cross-virtual machine contamination in these shared hosting systems, where they weren't as isolated as we believed.

So my feeling is I could see, maybe, eventually I want to do web-based forums. That's one of the things I want to set up in the future. And there's no way I'm going to put those on GRC's main server. I'm just not comfortable with so much of somebody else's code running on the same box as my core services and my eCommerce stuff, all of which I've written myself from scratch. So I could easily see hosting that somewhere else. Except that now I've already got a rack and bandwidth and everything at Level 3. So I'll just give it a physically separate machine and isolate it on the network so that no leakage can occur between boxes. So since I'm already committed to having my own stuff, as you said, Leo, I am a do-it-myselfer. I love that aspect of working on this stuff.

Leo: Yeah, it's how you learn. It's a good way to learn.

Steve: Yeah, yeah. And I have to say, too, my experience has been it's not necessarily cheaper. They're there to make money. And I have a very nice fixed-price contract with Level 3. I buy it on the so-called - my bandwidth on 95/5, which is to say that they take the highest 5 percent of my usage through the month, and they charge me for 95 percent of what that is. And that is, if it's over my cap, which is 10Mb. And so I spike, you know, 50Mb and so forth higher all the time. But it's people downloading all the podcasts at once and so forth, and then it sort of settles down. So that our average ends up being probably about half that, around 5Mb. And so that gives me the flexibility to offer good bandwidth and good responsiveness, yet at a price that makes sense for me.

And I just, in my experience, when you start really trying to source things from Amazon, what was it, oh, I did, I put all of our audio up there. I do have all of our audio backed up, but it's not coming from there. I did have it coming from there, and it was expensive. So it's not cheap to actually be using that bandwidth in the cloud.

Leo: We should point out that Steve's kind of like half cloudy. He's not running the servers out of his house. As you can tell, he's got what's called a "colo," where you buy the hardware and put it in there, but you're in a network operations center run by another company.

Steve: Yes. They provide power, air conditioning, and security. And basically so I have a full rack over in Tustin.

Leo: So you are in the cloud, it's just that you're buying your own hardware and running and managing it. You're managing your own servers. We do the same thing. We lease servers from SoftLayer, but we manage them ourselves. There is another level above that where you can get managed servers. And then there's finally this new thing, which Rackspace, Amazon, Google and others are doing, where it's kind of all virtual.

Steve: True virtualization.

Leo: It's fully virtual. You don't know or care about the hardware. And in fact there's certain advantages to this because the hardware is distributed often geographically. So if there's a power outage in Seattle, it may not affect you because your servers are all over the place, and if there's a failover it's all distributed. But I don't think, Steve, you're telling people, oh, you should do your own eCommerce solution, either.

Steve: Oh, no, no.

Leo: Steve knows what he's doing.

Steve: No.

Leo: And this is a unique situation that is not typical by any means.

Steve: We were being pursued by Digital River.

Leo: He wrote his own software, folks.

Steve: And they finally called Sue, after we didn't return their messages or anything. And they got Sue, my operations gal, on the line. And she finally said, look, he's writing - I think this was when I was in the process - "He's writing his own eCommerce system." And the guy at the other end of the phone said, "Oh, no, no, people don't write those."

Leo: Somebody does.

Steve: Apparently.

Leo: Did she tell him he's writing it in assembly language?

Steve: He would have...

Leo: He would have said, "No. Who am I talking to here, George Morrow? What is this?" Yeah. I mean, so this is a unique situation. And in fact I think you would counsel that, unless you really, really, really are experienced in this, you should not be writing your own eCommerce solution. You should be using an eCommerce solution from a trusted provider who knows what they're doing. These things are nontrivial.

Steve: And the last piece I would mention is I don't know that I even could host GRC because GRC is very special. We've got custom-made UDP packets and TCP packets and

all kinds of low-level networking stuff coming and going out of our systems. It took Level 3 a while to get used to me. They were saying, uh, Steve, what's going on over here? And then now they all know, okay, just leave him alone. He's kind of strange, but he seems to be doing a good thing.

Leo: I remember when Kevin Rose set up Digg for the first time. They had the colo. They had a cage, just like you. And they bought hardware, and they brought it in, and they installed it. But that was how you had to do it in those days. And I'm sure with Milk and his later enterprises, nowadays when you start up an app or you start up something else, you generally do run it on a cloud. It's cheaper to start up that way. And you can scale it up as needed and so forth.

Steve: Yeah, and for most people's servers, I think that's a perfectly acceptable solution.

Leo: Oh, yeah. Oh, yeah.

Steve: You just sort of create the service, and then you upload the content, and now you've got a site.

Leo: Most people don't need dedicated servers. They certainly don't need a colo.

Steve: Right. But that's nothing like what GRC is doing, where I'm doing low-level network packet...

Leo: Well, Steve's his own sysadmin. I used to be my own sysadmin. And I have - it's been a lot of trouble. But I did it because I wanted to learn. And I did. I learned how to use cPanel and all that stuff. I did a great job. I see you looking at the clock. Don't worry about that. Let's continue on.

Brent in Illinois has a question, as long as we're talking about your servers: I thought I heard you mention sometime back you were using one of the BSDs - OpenBSD, FreeBSD, NetBSD, one of those. Recently I heard about your server upgrade. You said you went from Windows 2000 to Windows 2008 R2. So what do you use?

Steve: Both. This is an instance of the proper tool for the proper purpose. I am a FreeBSD person. I was turned on to FreeBSD by Brett Glass, who I mentioned before. Brett said this is the one you want, and I think Brett was right. I love FreeBSD. I've got a FreeBSD server running at Level 3, also one here. At Level 3 it is my OpenVPN terminus. So I run OpenVPN on that box. But also I run INN, the traditional NNTP, the Network News server which hosts GRC's newsgroups.

Leo: I didn't know you were running that on NNTP. That's hysterical.

Steve: Oh, yeah.

Leo: You are very old school.

Steve: Yeah, we've got a very active, super useful group of gurus who hang out there. It's news.grc.com is the machine. And so that's a FreeBSD box. So I use the appropriate one for the appropriate application.

Leo: It's UNIX. It's strong.

Steve: But I don't code to it as much because I'm a Windows developer. So I'm comfortable over on Windows.

Leo: Scott Elsdon in New Zealand wants more of the missing bits, he says: Steve, I really enjoy the chatter between you and Leo. And while Security Now! is essential, I heard in it that you talk to Leo before the show for half an hour about sci-fi, books, TV shows and coffee. These I miss. I'm in New Zealand. Listening in to the pre-show is hard because of the time difference. I guess it's real early in the morning when we do the show. I've missed these recently in the main show. Is there any chance that the half-hour could be distributed also, as a chat show, or Steve and Leo's missives? Missing some good sci-fi recommendations, et cetera, I'm sure. Plowing through "The Second Ship" now because of your mention and love it. You know, we...

Steve: So, Leo, you mentioned that one of your streaming carriers...

Leo: Justin.tv.

Steve: That's the one.

Leo: Yeah.

Steve: Records everything.

Leo: Yeah. So it records it in chunks. So you can go to a specific time, and you can watch - they archive it, and you can watch again, as if we were offering it. We don't - there's no reason really to offer it because it's hit or miss. Sometimes it's got great stuff in it. A lot of times, like today, it didn't have a whole lot in it.

Steve: Eh, not so much. So you go to Justin.tv and, for example, look at the 11:00 a.m. Pacific time. And there you would see about a half an hour, typically, of us adjusting ourselves and getting ready and talking about whatever. Knowing, frankly, that it's a little - we're less formal because we're not in the official podcast at that point.

Leo: Well, and it's - my goal, and I'm not making a secret of it, is I really like having all of that stuff because I want people to watch live. I want people to kind of get conditioned to watching what we do live. And so I'm not averse to having some content that isn't available for download. We make the shows proper available for download. But I think that my goal is that you watch everything, not just the shows, but the making of. You're watching the making of, really. So if you like watching Steve adjust himself, you can do that. Justin.tv/twit/videos. People make highlights, which is kind of cool.

But you can see all - you can see past broadcasts, and you can see highlights. I'll get emails all the time, people say I highlighted this portion of it or that portion of it. In fact, if that's something you would like to do, you could make a highlight, Scott, that says this is the pre-show, the Security Now! pre-show, and make that be a highlight. It's easy to do. It's just basically doing the time codes. And then others could see it, as well. Somebody may already be doing that. So that's the best way to do that. I can't make a show out of everything. And I do appreciate the time difference. I understand that. We're kind of set up to be in the afternoon in the U.S., for the most part, and early evening.

Steve: So Leo, this next question is our last one because I also have a rock underneath my right contact lens.

Leo: Oh. I, oh, heavens. Heaven forfend. Well, let's quickly get Rob Altenburg - is that the one you'd like me to do, about bitcoin taxation?

Steve: Yes, yes.

Leo: He's an attorney in Pennsylvania. Now that the Treasury Department has given bitcoin a stamp of approval, the next big think is, well, what's the IRS think? In the U.S., "any accession to wealth," that's the term of art, is considered in calculating income tax unless it falls under an exception. Wealth earned from bitcoin mining or speculation should be taxed. The big question is how, and when. The rules depend on what bitcoins are considered. If the IRS thinks it's a foreign currency, one set of rules might prevail. If it's more like gold, commodities, or stock certificates, other rules might apply. Also, it's not just bitcoins. These questions apply to in-game currency on MMOs, too. Why should we say money from real world work is taxable but money from in-game work isn't? He says: I'm a lawyer, but not a tax lawyer. By the way, that's why people like Bitcoin, because it's anonymous.

Steve: Well, at the moment it's off the radar. And, like, for example, purchasing on the Internet used to be nontaxable. Amazon famously began taxing. And it wasn't that it was always tax-free. It was that consumers were responsible for reporting their purchases and taxing themselves. And of course few people were doing that. So Amazon said, okay, well, we're going to take responsibility for that. I mean, and this brings up an interesting point, I thought. I got famously those 50 bitcoin which, depending upon when you check, are worth maybe $12,000. Well, where did that come from? I mean, is it free money?

Leo: It's taxable, I can promise you.

Steve: [Laughing]

Leo: When in doubt. They want their cut.

Steve: There is no doubt. Now, I have held it for more than a year, so maybe that means it's a long-term capital gain.

Leo: I don't think it's taxable probably until you turn it into greenbacks.

Steve: Oh, I hope not because otherwise - Leo, I formatted my hard drive. It was the saddest event, you know.

Leo: Gone. Yeah, you might have made a mistake talking a lot about your Wallet. But otherwise they'd have no way of knowing; right? I mean, it's just a number. You're a number, not a man.

Steve: Men, men, men. So maybe they'll just do a hands-off. But I don't think so. I think, ultimately, I think we're going to see legislation. Mark my words, my friend, it's going to be legislated. That's the way our government is going to get around to dealing with this because...

Leo: It's such, you know what, it's such a tiny amount at this point that I don't think there's going to be...

Steve: I hope not.

Leo: You've got years before this gets on everybody's radar.

Steve: Don't wreck our fun. Don't wreck our fun, government.

Leo: Steve, they just figured out the Internet exists. It's going to be a while.

Steve: Yeah.

Leo: And you can pay them in bitcoin, see how they take that. Wouldn't that be interesting. Pay your tax in bitcoin.

Steve: Oh, good point.

Leo: Right?

Steve: I made it in bitcoin. You can have it in bitcoin. Here's a code. Here's my QR code, IRS annoying person.

Leo: Right.

Steve: There you go.

Leo: Well, so somebody's saying when it's converted to greenbacks. But remember, if bitcoin is considered just like a foreign currency, there are tax rules. If you make - when I make Canadian dollars, I don't have to convert them to U.S. dollars before they're taxable. Oh, no, my friend. They want their share. They want their share.

Steve: And it's not really work product, either, because I know, for example, from my experience with community property, having been married, that the work product of each person in the marriage inures to the benefit of that communal entity.

Leo: Well, but so does money made from investments and so forth. So I think that that counts.

Steve: But not inheritance. Inheritance you didn't work to get, so that's actually sole and separate.

Leo: Ah, interesting. That's yours. Hey, I want to thank Mark Class for sending us more...

Steve: Or it's at least less hers.

Leo: These are our - yeah, right [chuckling]. These are our...

Steve: Oh, now I'm in trouble.

Leo: We've got our new 8-bit TWiT pens. They come in four colors. And...

Steve: What? What?

Leo: He sent this.

Steve: Oh, you're not kidding.

Leo: No. This is Mark Class makes these. He's a - what is the name of his company? I have it here somewhere. Worldwide Pens. Three colors. Oh, and a stylus. One of them's not a color at all but just a stylus for your tablet.

Steve: Leo, you have binary combination. Three colors gives you eight.

Leo: Uh-huh. There you go, because I can color over. And these little TWiT Wipes. If you come to the TWiT Brick House, we don't send them out. You have to come here and visit. But visitors, thanks to Mark Class of Worldwide Pens...

Steve: You have TWiT Wipes? I don't think I want to know about that.

Leo: No, these are good. They're microfiber lens cloths.

Steve: Goes with the Man Pack.

Leo: Yes. I'll put one in a pocket right here. Steve Gibson joins us each and every week, Wednesdays, 11:00 a.m. Pacific, 2:00 p.m. Eastern time, 1800 UTC. I'm sorry, 1900 UTC now, thanks to the time change, at TWiT.tv. Do watch live. We'd love it if you watch live. And that's how you catch the before and after. But if you can't, we do make on-demand versions of the show available, of all our shows, audio and video. In this case, TWiT.tv/sn. And Steve has the special edition Security Now!, the 16Kb audio for the bandwidth-impaired and the beautifully handwritten transcriptions by Elaine Farris that are so perfectly spelled and annotated.

Steve: And speaking of Elaine, it is her birthday today.

Leo: Happy birthday, Elaine.

Steve: Happy birthday. And the transcript, she warned me, since she's got family descending on her, may be a day late. But they will never be a dollar short. So not a problem. Happy birthday, Elaine. Enjoy your birthday. [Thanks, guys. Elaine] You're probably exhausted now that you've gotten to the end of this podcast.

Leo: She didn't hear our greetings till she was finished typing. You can stop now, Elaine. You can all stop watching, ladies and gentlemen. Although This Week in Google's next. And you know who's going to be on Triangulation this afternoon?

Brewster Kahle, I know you know that name, of the Internet Archive. He created a company called WAIS, a database company which he sold for some money to AOL some years ago and decided to devote his life to philanthropy. He created the Internet Archive to archive all of the Internet some years ago. They save terabytes every - I think every month. Maybe even every day.

Steve: That's amazing.

Leo: Isn't it incredible? And it's such a great idea.

Steve: Oh, and I'll tell you, it's very embarrassing, Leo.

Leo: Wayback.org if you want to see how Steve's site used to look.

Steve: Oh, my god, don't go.

Leo: The Wayback Machine is a...

Steve: Do not. Do not look.

Leo: ...feature of the Internet Archive. Everything lives forever, Steve. Just remember that.

Steve: Oh, I'm so sorry.

Leo: Yeah, yeah. Hey, yeah, Archives.org, not Wayback.org. Thank you so much, Steve Gibson. We will see you next time on Security Now!.

Steve: Thanks, Leo.