Listener Feedback #161

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-391.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-391-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here, and we've got questions from our audience. Steve's got answers, too. Our Q&A episode, next on Security Now!.

Leo Laporte: It's time for Security Now! with Steve Gibson, Episode 391, recorded February 13th, 2013: Your questions, Steve's answers, #161.

It's time for Security Now!, the show that protects you and your loved ones, your privacy and more online, more and more important. Here he is, the guy who does it all for us, our Explainer in Chief, Mr. Steve Gibson of GRC.com. Hello, Steve.

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

Leo: You were on the radio show talking about this problem, this...

Steve: And where are we? I've not looked recently.

Leo: UPnP. But I'll tell you, when you went on the radio show, more than a hundred people...

Steve: 200 on the first day you mentioned it. You mentioned it on Saturday around 1:30. And it jumped by about 200 then.

Leo: That means people who had the vulnerability. You have millions probably of tests. But people who showed positive on the vulnerability.

Steve: Yes. I'm not counting everyone because lots of people do multiple tests. And it just didn't make sense to try to disambiguate their IPs. I mean, you know, IPs drift and so forth. So I am never double-counting anyone who tests positive. But I am not trying to say, okay, here's the actual percentage that we're finding.

Leo: Right.

Steve: And let me go to the test right now, and we'll see what an updated count gives us. It was higher than 1,700 when I looked, I think earlier today or very early this morning, I think it was.

Leo: 1,700 people. Now, the good news is those 1,700 people now know that you...

Steve: 1,790. 1,790 as of this moment.

Leo: Wow. That's 530 more than before you went on the radio show.

Steve: And I think we were at 800 something last week when we talked about it.

Leo: Jiminy Christmas. It's not surprising. I mean, you figure the people who are listening to the radio show are probably a little less sophisticated than the people who listen to this show.

Steve: Good point. And so...

Leo: Although that's not necessarily a factor. But many of them may have UPnP turned on still in their router. Wow. And of course not word one from any router manufacturer.

Steve: Unh-unh. Well, and again, as we said, they're scared to death of admitting any culpability and liability. They don't want to, like, say anything because, if someone got hurt this way, you could make an argument that this was foreseeable, and this was defective.

Leo: You blew it.

Steve: And it allowed their network to get penetrated.

Leo: Yeah, you blew it. Well. All right. We're going to talk about other matters today. We have Q&A; right?

Steve: Yes, we do. And next week we're going to have a special guest whom we've never had.

Leo: You're not taking Presidents Week off?

Steve: No, Leo, we can't take any time off or we just get pummeled to death by our listeners...

Leo: Thank you. Thank you, Steve.

Steve: ...who have incorporated this into their lives.

Leo: It is Presidents Month. I think the entire month of February we're closed.

Steve: No, no, no, no, no. Brian Krebs is going to join us.

Leo: Oh, I'm such a fan. Now, Brian we got to know because he worked at the Washington Post writing a security column. Left the Post a couple years ago, still does Krebs on Security on his own and is really one of the best people to follow if you want to keep up on what's going on.

Steve: Well, and his particular shtick that I, I mean, the reason I mention him so often in the podcast is he tracks the underworld. He has got probably, I mean, he doesn't talk about it, but he probably has multiple identities, and he's infiltrated that aspect, the dark black hacker forums where this stuff is bought and sold and so forth. Anyway, he did a really interesting blog post about a week ago that talked about Microsoft and Symantec taking down and taking over a big botnet and then using their control of it to inform the infected victims that they had this problem. And I thought, oh, you know, I mean, he is so much in the middle of this. I thought he'd just make a really fun special guest.

Leo: Can't wait to meet him. I've been reading him for years. That's exciting. Next week.

Steve: Yup, next week. So this week we've got the questions which we didn't get to two weeks ago because...

Leo: [Laughing]

Steve: We did four two weeks ago. But, hey, we gave everybody 90 minutes of, you know...

Leo: Yeah, it wasn't a short show by any means. It was just we had other stuff to talk about.

Steve: Well, and that was the Universal Plug & Play revelation. That was the whole Rapid7 and HD Moore in there, and that had to get covered on that week.

Leo: And my guess, we'll have a few questions about that this week.

Steve: Yeah, actually. And actually some good stuff about memory hard problems. People have asked some questions. But the showstopper is this is, or yesterday was, the second largest Patch Tuesday in Microsoft history, their Mega Super Tuesday Patch Jubilee.

Leo: [Laughing] Well, it was Mardi Gras. Maybe they're celebrating early.

Steve: The biggest one ever, they hit us with 64 vulnerabilities.

Leo: Holy cow.

Steve: This one came in at 57. And across the board, both OS and Server OS platforms, I mean, both desktop and server OS platforms...

Leo: This puts a little bit of a lie to what we had been saying, which was that, oh, things are getting a little stabler now. They're settling down. People are attacking other platforms because Microsoft does such a good job...

Steve: Well, actually, 32 of the 64 came from one guy at Google.

Leo: Well, thank you, Google, I guess.

Steve: Yes.

Leo: You know, it's ironic because Microsoft's been taking potshots at Google with their Scroogled ads. Meanwhile, Google's very kindly...

Steve: Bing, everyone says Bing, but I don't - I just - I get Bing off of my browsers every time it shows up. It's like, eh, I don't want Bing, I want - it just sort of seems lame. But anyway, so IE, Office, .NET Frameworks across the board. I'm not going to go

and enumerate them for an hour because it's just more of the same. They're all really bad, and they're remote code execution, and so patch.

Leo: Wow.

Steve: And this one is a big one, so...

Leo: You said 57?

Steve: 57 vulnerabilities.

Leo: Really.

Steve: Yeah. And when you scroll through the list of affected systems, I mean, you know you're in trouble with the scrollbar scrunches down to about half an inch. It's like, oh, I'll be scrolling for a while then. And so that was the case.

Meanwhile, we have a new zero-day PDF exploit in the wild. This just came to light yesterday. An outfit called FireEye Malware Intelligence Lab - I thought, well, I wonder if they tried to work an acronym out of that. FEMIL? I don't think so.

Leo: FEMIL. Sounds like a menstrual...

Steve: Or an artery, maybe.

Leo: The femoral artery.

Steve: Yes.

Leo: Sounds like a pill for cramps.

Steve: What they found was they found this being exploited, effectively exploited in Adobe Reader 9.5.3, 10.1.5, and 11.0.1.

Leo: Oh, crap. Just when we thought it was safe to use Adobe products.

Steve: Eh, so. And quoting from them, they said, "Upon successful exploitation, it will drop two DLLs. The first DLL shows a fake error message and opens a decoy PDF document, which is usually common in targeted attacks. The second DLL in turn drops the callback component, which talks to a remote domain." And since this release, Adobe has confirmed they've got a problem. So, and that's - it just happened. We don't really

know much more about it than that at this point. But the takeaway is, if you can, don't open any PDFs.

What we're seeing is that this is being used in spearphishing. So it would be, unfortunately, somebody who is spoofing their identity, sending you something that you're expecting or you would expect to receive or that sort of thing, like something relative to your industry, and this thing would get you. So the thing to do actually would just be to stay away from Reader, I think. It's specifically Adobe's Reader that has the problem. So if you could switch to a third-party, a non-Adobe...

Leo: I think most of our viewers have already done so with things like CuteFTP or Foxit Pro, I mean, there's so many good and free readers that I - it's just that most non-technical people just Adobe Reader either comes with it, or it's kind of automatic.

Steve: Or there's a link that says, "If you can't open this, click here" to get...

Leo: Yeah, and so they're all using it, yeah.

Steve: To get infected.

Leo: You know what's nice is most, well, I think Windows 8 now has a PDF reader built in. So I don't think it's going to be an issue anymore.

Steve: Really. Well, and the browsers of course are heading in that direction.

Leo: All the browsers will do it, yeah.

Steve: Google's got it, and FoxPro, or, yeah...

Leo: Firefox?

Steve: Firefox is on the way. So there was something that initially looks very scary, and it was worrisome until we learned more about it. And that has been called the "Packet of Death."

Leo: Well, that's a good name.

Steve: Yeah. It turned out what - the first report was that Intel's extremely popular 82574L - now, that seems like Stardate, but it's not. But the 82574L is, like, everywhere. That's the very high-performance, beautifully designed gigabit Ethernet controller. I actually went under NDA with Intel. It took a long time, too, to convince them that I wasn't going to steal their chip, I just needed to program it, and I couldn't use their

drivers. This was back when I was being DDoSed all the time, and I needed to come up with an ultra high-performance wire speed DoS prevention. And to do that I had to talk to the hardware. Anyway, so this chip is ubiquitous on any kind of Intel platforms. And many other, like Supermicro and other people who like Intel will use that chip, too.

So what happened was customers' hardware was locking up tight at the hardware level and crashing in the microcode running in the chip, requiring a full power-down cycle. You couldn't reboot the OS. You had to pull the plug, wait for things to drain, and then plug in again. And this was happening, it first came to light with one company whose customers were having this happen to them on their equipment. And so it got their attention. It turned out it was one VoIP vendor's packets that were doing it. And then, quoting from their page, they said, "Problem packets had just the right Call-ID, tags, and branches to cause the '2' in the ptime to line up with 0x47f." So there you go.

And they said - so basically they found out, like, exactly what it was that was the bad spot, and they said, "With a modified HTTP server configured to generate the data at byte value (based on headers, host, etc.) you could easily configure an HTTP 200 response," which is the standard response to an HTTP query, "to contain the packet of death and kill client machines behind firewalls." So the idea would be you could create an evil server, and anybody who asked for a page from that server would die. It would just kill their, I mean, just completely crash their Internet connection so that they just go off the 'Net. They'd have to completely power down, wait a second, and then power back up again.

And the guy even created a test page where you do not want to go, so I just thought I'd mention that. But then Intel of course got involved. And the good news is this is not that bad. An Intel spokesperson says that this is, quote, "one case scenario isolated to one specific motherboard maker and incorrect implementation of the controller on their motherboard (incorrect EEPROM image was programmed during manufacturing)." So it was like a weird glitch.

Leo: They burned a buggy ROM onto it.

Steve: Yes, yes, yeah.

Leo: Okay. It is ironic, after all, that the Intel reference code for Universal Plug & Play is the code that is causing this Universal Plug & Play issue. Seems like Intel maybe should hire some better coders.

Steve: Well, but remember, I hold them harmless.

Leo: I agree because they didn't intend for it to be put into production. It's obvious.

Steve: It was Romper Room code. I mean, it was so ridiculous.

Leo: It was demonstration, yeah.

Steve: Yeah. I mean, it was - it would - you were scanning for something and waiting until you got to the CRLF, to the slash...

Leo: Now you're at the end of the line. Go ahead.

Steve: Just right off into oblivion. I mean, no one could think that was good. So, I mean, and as we said two weeks ago, clearly this was demonstration. This was to illustrate how someone serious would write code that would actually check for boundaries and buffer conditions and so forth. So, yeah.

I did get a tweet from someone I thought I would pass on. I have often talked about having coffee with Stina Ehrensvrd of Yubico, of course famously the YubiKey. She did an interview on Hak5 at Rev 3. It's on YouTube. And so I imagine you could go to YouTube and search for, like, Hak - it's Hak5, and then I guess they have an episode number, it's 1226.1.

Leo: YouTube.com/techfeed, I think.

Steve: Okay. And she looks...

Leo: Or /Hak5.

Steve: She seemed really nervous. I mean, I know her pretty well. We get together all the time. She's completely relaxed with me. But I think she was camera shy.

Leo: Darren Kitchen scared the hell out of her.

Steve: But anyway, so people can get a sense for - I think it's short. It's 12 minutes, and some girl with bunny ears is on for the first...

Leo: That's not "some girl," my friend, that is Shannon Morse.

Steve: Okay.

Leo: Of our - she works for us, too.

Steve: She does? She was kind of petting her ears there on...

Leo: Yeah, those ears, believe it or not, sense brain waves.

Steve: Having seen her, I'm believing it.

Leo: And I guess that's not Darren Kitchen, it's Paul Tobias who's doing the interview.

Steve: Well, actually the interviewer comes on later, unless you've already gotten there.

Leo: Darren is a hardcore hacker, so he's on TNT all the time, as well. So, neat. Good. So it's worth watching? There's Stina.

Steve: I don't know. I saw - I was in a hurry. I didn't sleep last night. I was preparing the podcast. I saw this. I looked enough to sort of see her, and kind of she looked a little, whoo, okay. Her hair's a little different than I remembered it, so I think she's changed it. She's, you know, she's European.

Leo: Well, she's on Hak5 now. That's the big-time.

Steve: Exactly. So anyway, I thought people who have heard us speak of her so often and know of YubiKey might get a kick out of seeing her. And not a day went by, Leo, after I went off last week about the underpaid PR firm for Silent Circle, that I saw another article, this time in ExtremeTech.com. The headline, once again, "Cryptography Super-Group Creates Unbreakable Encryption Designed for Mass Market." And they have a team of ex-Navy Seals, Leo.

Leo: Oh. Seal Team Six is doing your encryption.

Steve: Yeah, not just the CEO. It's not just the CEO who's an ex-commando. He's got his buddies there, too, just to make - if anyone does crack the crypto, they're going to come and visit you. So don't try. Anyway, yeah, this is the underpaid PR firm's story. It's amazing.

I did get a nice acronym, another one, for UPnP: Un-Plug Now Please.

Leo: Yes. I think that was the name of the Rapid7 article; wasn't it?

Steve: No, theirs was UnPlug & Don't Play.

Leo: That's it. That's right.

Steve: Yeah, or do not play, Unplug & Do Not Play. So Un-Plug Now Please, I like that. I think that's crisp, short...

Leo: Says it all.

Steve: To our listeners who may be trying to download Security Now! from my site, I just wanted to make a note that I know all of the audio is gone. Last night I put the new server online. I'm so tickled with it. I mentioned the architecture a couple times on the podcast. I have four highly overprovisioned, single level cell SSDs. "Highly overprovisioned" means they're actually 64GB SSDs, but they only give me 46. They keep the entire balance for sparing. So that's what we mean by "highly overprovisioned." If anything goes wrong, there's a ton of essentially spare sectors to swap in. So I take those four, run it in a RAID 6 configuration, which is a notch above RAID 5. RAID 5 allows one drive, any one drive to die. RAID 6 allows any two drives to die. So with a four-drive RAID 6 configuration, any two can completely go belly-up, and I'm fine.

Then the RAID controller has half a gig of battery backed-up cache which has a write-back policy, not a write-through. So the cache stays dirty on purpose, which lowers the write fatiguing on the SSDs. So the cache never writes to the RAID array unless that region of the cache is needed by somebody else. So, for example, anything that's, like, frequently changing a certain location in a file is not even written to the file. It just is changed in the battery backed-up cache. And it's safe to do that because the RAID controller knows exactly what it has written so far. And if, you know, you pulled the plug right in the middle, it would keep what it's - I think I've got 48 hours of battery backup at this point.

Leo: That's awesome. That's a great solution to...

Steve: And it's got double redundant power supplies, double redundant blowers. I mean, already the processors, it's got a Xeon X3450, which is the high-end server. It's got eight threads that it runs. And anyway, so I didn't sleep last night. I brought the system online.

Leo: With excitement? Oh, oh, you were working.

Steve: Well, it was both. It was excitement, too. I was running Windows 2000 Server. That's what I had been running all of, you know, for 13 years. And so it was getting a little long in the tooth. And what I believe happened is that there was a subtle date bug in Windows 2000 IIS 5, which was the web server for that platform, that nobody ever found because nobody ever ran it for 13 years. But I did. And it used to be...

Leo: [Laughing]

Steve: It used to go years without having a problem, and then it began crashing. I mean, I've been, like, I missed the crash a few nights ago, I think it was like the middle of last weekend. We were off the 'Net for, like, six hours while I was asleep, and I didn't know it. I have alarms and everything, but it died in a different way that didn't - so the alarms were pacified, yet nobody on the 'Net was. So anyway, I'm hugely relieved to replace this. And I have to say, everyone knows I'm no Microsoft fanboy. But what they have done with their server platform I'm very impressed with. It is - they've modularized it so that you - and at first it was, like, different. So I was like, oh, I don't like different. You know, because you and I are getting a little old, Leo.

Leo: Ah, see? I told you.

Steve: Oh, yeah. But then I kind of - I thought, whoa, you know? The modularization means that the attack surface is lower. And we've often talked from a security standpoint about you don't want to have things there that you need to prevent people from doing. It's better not to have them at all. So here you're like, you only put in that you - Microsoft lets you only load the modules you want. So it's smaller and lighter weight, a lower attack surface, and that's the case for the server platform and IIS.

Anyway, I am so tickled with my choice. I mean, I bought all this stuff two years ago because I actually had problems once when I was up in Petaluma with you. And something went a little wonky down here in the datacenter, and I thought, okay, I've got to fix this. And so that's when I went to solid state because I thought, okay, I'm king of SpinRite. I know that drives have problems. And several of the drives, I'm back on - I think these were Ultra SCSIs. That was the era when I built this was the - I think the Ultra SCSI 320s was the technology back then. And you can't get those anymore. So the drives are dying slowly. I have a full redundant server. Oh, and I even have one of these, a second of one of these that will just sit there, powered off, if, like, the motherboard catches fire or something completely bizarre, in which case I still won't be off the 'Net for long.

So, but, oh, my point was I forgot to transfer the media. I got the whole website up, all the active content. I've been working on it for a week. Microsoft did change things that caught me out in a number of places where I had to work around stuff. So I was - I had to change my code to make it work under Windows 2008 versus Windows 2000. And then I forgot to transfer all of the Security Now! files. So people started this morning complaining, saying, hey, you know, I'm getting a 404 error on the small versions of the content. Because of course the large versions bounce through Podtrac and to you, Leo, and I only serve the small ones. So it's like, oh, what? And it's like, oh, that's right, I didn't move those over. So anyway, I'll do that after the podcast today, and then I'm going to go to sleep.

Okay. So this is the last chance that there will ever be for people to get one of those [indicating blinky lights]. The PDP-8 kit did go live on Kickstarter [bit.ly/pdp-8]. And Leo, there are now only seven left. They started with 30. Let's see if there's still seven.

Leo: I still haven't bought mine.

Steve: Well, if you want, I will build it.

Leo: No, it's too expensive. I'm not gonna...

Steve: Okay, okay.

Leo: I can't - it's for blinking lights you're paying 800, 900 bucks? That's crazy talk.

Steve: Well, if that's who you are, then that's true. But remember also, all the

documentation on this mini computer is online. I have it all on my site. The operating system OS/8 is there, the assemblers and editors and so forth. But if anyone was interested, I mean, it makes a great demo, hang it on the wall with the lights blinking. But it is a perfect instruction set for someone to learn.

Leo: You want to - I know you've mentioned this before, that your retirement plan is to write a new OS for the PDP-8 instruction set.

Steve: Actually I decided that was a bad idea.

Leo: Good, thank you.

Steve: After writing those programs, I had enough.

Leo: Yeah. You don't want to stay up all night again.

Steve: Well, it's just there are too many things that, for coming from a big CISC processor side, as I am...

Leo: This is a RISC processor?

Steve: Well, no, no. But it's certainly not a complex instruction set. The opcode is three bits.

Leo: It's primitive, is what it is.

Steve: It's three bits. So you can have eight different things. There's, you know, jump, and there's...

Leo: Really, that's it, eight instructions.

Steve: Eight instructions, yes. And so - and then the rest are - the rest is address. So it's, I mean, it is a perfect instruction set if someone wanted to learn...

Leo: For learning, yeah.

Steve: Yes. If someone wanted to learn...

Leo: It's probably got, what, a jump, a compare, an add, rotate probably...

Steve: If you go to GRC.com/pdp-8/pdp-8, that first page shows a beautiful front panel that, scroll down, and there I lay out the instruction set and show people what the instructions are. But so if somebody wanted to, like, start, maybe with their kids...

Leo: Perfect, yeah.

Steve: ...and build this, and then write some programs, you can really write programs. I did. And there's also a beautiful emulator on the Mac that's - actually I dusted off one of my Macs.

Leo: See, I'll just do that. It'd be cheaper to buy a Mac Mini and put lights on it.

Steve: Yeah, well, okay. So anyone who's interested, bit.ly/pdp-8. I made a shortcut for it.

Leo: And you know who you are.

Steve: Bit.ly, bit.ly/pdp-8.

Leo: And look over Steve's left shoulder, and you'll see what you're going to get.

Steve: Yup. There were 30 because that's all Bob had. There were only 30 of these Harris HD-6120 chips left in the world, as far as we know. And 23 of them are spoken for now. There are seven left, and we have 10 days to go. So I'll remind everyone next week, and then you'll never have to hear about this again because, one way or the other, the Kickstarter will have closed.

Leo: Actually, it's a little deceptive because they have a - I'm looking at this - a multipurpose operate instruction which can do one instruction, complement-rotate-increment.

Steve: Yes. It is. And, oh, and it's beautiful, too, because you can do really fun things with it.

Leo: So that one instruction really does quite a bit.

Steve: Yes. It is amazing how you can combine the bits in there to - and so that's the one non-memory reference instruction. Everything else is a memory reference instruction, meaning that the fourth bit says either the other eight are addressing page zero, or in the current page. It was an inspired little machine at the time. It's my first computer. It's what I learned. The first computer I ever saw was a real PDP-8. And I learned how to program in machine language on it, assembly language. So anyway, it's there. It's an opportunity. It is true that you could do this, if someone wrote an emulator

for the iPad, for example...

Leo: Wouldn't that be cool.

Steve: ...you could, you know, touch the buttons and flip things and make it go...

Leo: Oh, I like that. That's a good project. Maybe somebody should do that.

Steve: And I have thought about that. The deal here, though, is it's an actual front panel. For some people, actually 23 people so far, that's been appealing. And of course I have three, so...

Leo: So those switches, you could flip those switches, they all work, and they all do what the early PDP-8 did.

Steve: Yeah.

Leo: It's a fully functional replica.

Steve: Yeah. If anyone's wondering, I did have three videos on the site until last night. They'll come back this afternoon because I demo the one that I built and show the actual unit that I assembled in one.

Leo: That's really cool.

Steve: Then I also demo the two programs, one that is the blinking lights program called Deep Thought, and the other one is a puzzle program called Lights Out. Oh, and Bob is going to burn both of those...

Leo: Oh, neat.

Steve: ...into the ROM of these. So they will be built in and come along with it.

Leo: They come with their own built-in game.

Steve: A puzzle and blinking lights, yeah. Okay. So I've tweeted this. And Leo, oh, my god. Bit.ly/coolmodems, all lowercase, c-o-o-l-m-o-d-e-m-s. Bit.ly/coolmodems. If you zoom in on that, that is a timeline diagram showing exactly, step by step, what modems are doing when they're going through their mating ritual.

Leo: [Mimicking modem] That thing.

Steve: Yup. I mean, you can see at the beginning the touchtone, which is a two-tone matrix, and so you can see it dialing touchtone.

Leo: This is the handshake is what they call this.

Steve: Yes. It is the entire modem handshake sequence, stretched out. But it's showing you the acoustic spectrum where the various modems are, like, sending test things to each other in order to see what, like, gauge the nature of the channel which is interconnecting them. Anyway, I just thought it was very cool, bit.ly/coolmodems.

And I did want to mention, I think maybe we mentioned it after we stopped recording, but a number of people mentioned it, that I misspoke last week and used the word "Java" in a context where I clearly meant "JavaScript."

Leo: I said, that can't be possible. Mr. Gibson would never do that.

Steve: I just got carried away in my enthusiasm.

Leo: He knows the difference, though, folks.

Steve: Yeah, I certainly do.

Leo: So wherever he said Java, just put JavaScript in.

Steve: That's what I meant. And I apologize for - I hope I didn't confuse anyone.

Leo: I think people probably understood. Certainly...

Steve: I got a nice note from Donn Edwards in Johannesburg, South Africa, written to both of us. Both of us got a note, Leo. But it was addressed to me. But, "Dear Steve and Leo," he says. "I'm a long-time Security Now! listener and SpinRite user." Oh, I should say the subject was "SpinRite made a pensioner cry."

Leo: Aw.

Steve: "...[A]nd SpinRite user. On Thursday a family friend phoned me near to tears because her computer wouldn't boot properly, even after trying the last known good configuration option."

Leo: Which almost never works, by the way.

Steve: No, I don't think I've ever had that work.

Leo: Yeah. It's not magic.

Steve: It's like, I think it was Microsoft trying to pretend to care. That's what I think. So he said, "She was starting to panic because there is financial information on the PC that will ensure she gets her pension this year. I brought the computer home, booted up with SpinRite, and it soon found an unrecoverable sector which it repaired and did its magic. After checking that everything is fine now that the sector has been fixed, I called her with the good news. She just burst into tears. What can I say? Thank you for a wonderfully helpful utility. Best wishes. Donn." And, Donn, thank you for sharing that with me and our listeners.

Leo: Yeah. All right. Now it is time for Q&A.

Steve: Ah, okay.

Leo: I wonder if I should install Flash before I do that. Geez, Louise. It always makes me nervous when I see a Flash update. It's like, oh, I'd better do that, huh?

Steve: I wonder, that's got to be an ASCII code because he put something, an "it" on the end.

Leo: Oh, are you talking about the first question?

Steve: Yeah, I don't know what that is. That's a...

Leo: Let me look at it.

Steve: It's an ASCII - 23 in hex. 23 hex.

Leo: That's his - you're talking about his Twitter handle.

Steve: Yeah.

Leo: 00100011it.

Steve: Yeah. So that's 23 in hex.

Leo: 23. What is the ASCII for 23?

Steve: That's going to be a control code because it's less than 32.

Leo: Huh. Interesting. Well, we leave this as an exercise for the listener.

Steve: Yes, we do. We might as well actually...

Leo: Who will absolutely give you the answer. @00100011it says: In Episode 387 you said you had four solid-state drives in RAID 6. RAID 10 would give you the same size volume with much better performance, and the mirror is safer. Why don't you use RAID 10?

Steve: Because he's wrong. RAID 10 is a combination of striping and mirroring. RAID 0 is striping, where the idea is you split the data across two drives, where you can sort of think of like all of the...

Leo: We figured it out, by the way. 23 hex is ASCII for the pound sign. We believe his handle is "Pound It."

Steve: Ah, very nice. That makes sense.

Leo: And it's just vaguely filthy, which, yeah, makes it seem appropriate. Go ahead, please.

Steve: And only someone who's sufficiently geeky is going to get that, so everyone's going, what the heck is that 001? Anyway, so RAID 0 is striping, meaning that you take the size of the drive, if you have two drives that are identical size, and double it, and then you sort of spread the data across both drives. That gives you performance because, for example, if the drives are, well, you're able to read and write to both at once, you get twice the read and twice the write performance. The problem is it's lower reliability because, if either drive dies, you lose everything.

Leo: Right. You don't want that.

Steve: No. So then RAID...

Leo: That's what we call "Scary RAID."

Steve: So, well, but back in the day when drives were small and people wanted more storage, they would - and they had faith, or...

Leo: Is it the case, and I've been saying this, so I hope it is, that if you have two drives striped, you have twice the chance of failure? You're multiplying the chance of failure of each drive? Actually adding.

Steve: Correct.

Leo: So it's twice as likely to fail. Three drives would be three times as likely to fail?

Steve: Oh, yeah, three drives...

Leo: If any one drive dies, the whole RAID dies.

Steve: You lose it all.

Leo: So that's why I call it, and Alex Lindsay gave me the name, "Scary RAID."

Steve: Scary RAID. So that was RAID 0. RAID 1 is also called "mirroring," where this gives you complete safety against either drive dying. So you write to both, and you read from one. And if for some reason you can't read from that one, you read from the other one. So you get - you'd have redundancy. So RAID 10, think of it as a one and a zero, meaning that both striping and mirroring are going on. RAID 10 is four drives which are mirrored, or I should say are striped and mirrored. So you get the performance benefit of the striping and the redundancy benefit of the mirroring using four drives. But it's not safer because, think about it. The way I have mine set up with RAID 6, any two drives can fail, and I'm fine.

But in a RAID 10, there are several combinations of two that take you out. That is, if two that were striped and mirrored die, it's as if, well, you're hosed. So there are, what is that, one, two, three, four, five, six, there are six combinations of two drives which, well, there are six combinations of two drives in a set of four. And two of those six possible pairs of failures would take you out. So much less safe than RAID 6. However, it is higher performance. He's right about that. RAID 6 incurs some performance hit because it's doing some math on the data that writes to the drives in order to create that redundancy. I don't see that because the RAID controller has half a gig of battery-backed-up cache. So the RAID controller buffers and only writes if - and it's a write-back policy rather than a write-through policy.

So anyway, it's very good performance. And I just don't want to mess with - well, and the other thing that I should mention is, when I'm looking at the drives, they just kind of flicker every so often. I'm in a huge datacenter, and I've looked at other people's servers. And I'm thinking, what are they doing? I mean, the drives are just going crazy. I mean, just nonstop. Mine, I have to sit there and wait to see them flicker to sort of make sure that everything's still working right. So anyway, that's why RAID 6 is superior from a reliability standpoint than RAID 10. But, agreed, at a cost of performance.

Leo: Question 2 comes to us from John in Arizona. He's wondering about whole disk encryption on solid-state drives. Actually, we've talked a little bit about this before. It is a question I have, as well: I've stayed in the mechanical hard drive world using whole disk encryption with TrueCrypt on laptops. I'd like to enter the SSD world on Windows XP or 7. Could you explain how you can have the same level of Trust No One using whole disk encryption on a solid state drive using something like TrueCrypt? Owner of SpinRite since November 2010. Thanks for your response.

Steve: So this was an interesting question. And I wondered if other people might be similarly confused because you can use TrueCrypt on an SSD.

Leo: Doesn't matter. Okay.

Steve: Yeah. The software, the whole disk encryption technology doesn't care what the underlying technology is, whether it's magnetic or electrostatic, essentially, is what an SSD is. It just doesn't matter. So...

Leo: He might be confusing, now, there is an issue with secure wiping in SSD; right? Maybe he's confused...

Steve: Actually, there is not.

Leo: Oh, there's not.

Steve: Because, remember, because there was a similar concern with wiping a hard drive because hard drives spare sectors in the same way that SSDs spare chunks. Remember that the secret is run TrueCrypt before you ever put any data on the drive.

Leo: Ah. So it will always be scrambled, never in the clear.

Steve: Yes. You never have any, I mean, any spares that got spared out will be encrypted, and it's just full of random noise. So that's the key is don't add TrueCrypt to an already setup system. Make an image of your current drive, set TrueCrypt on this, and then restore that image to the TrueCrypted drive so that that drive never is unencrypted. But, yes, you can absolutely use TrueCrypt on an SSD. In fact, I do.

Leo: Question 4 is from "g33kp0w3r," spelled in leet, in Stanton, California, wants to know about private email: Dear Elders of the Internet, I love your show, own SpinRite, blah blah blah.

Steve: But I got a kick out of it. I guess you and I, Leo...

Leo: I told you.

Steve: ...are the elders of the Internet.

Leo: I said it before the show began. I have crossed the Rubicon into old age. I am now an elder. And you know how I know that? Because every Thursday when I go over to the supermarket over there I get a senior discount, 10 percent off.

Steve: Yeah, I get the discount at the movies now. At first I was sort of balking at that. But it's like, hey, wait a minute.

Leo: I'll take it.

Steve: I'll take a couple bucks, what the heck.

Leo: Yeah. We are the elders of the Internet. At least according to the movie and grocery...

Steve: And I've got switches, I've got switches and blinking lights behind me to prove it, Leo.

Leo: You're a PDP-8 programmer. That makes you an elder.

Steve: I actually used those in the old days, yes.

Leo: Since the Mat Hogan - he says "Hogan," but it's "Honan" - incident, I've been wondering what the best host would be for an anonymous email account so I could use it to register all my other accounts. I've tried S-Mail - I don't know that - S-Mail.com, but they deactivate any free account after 30 days. I'm looking for something that I don't have to pay for because it's very complicated to pay anonymously. That's a good point.

Steve: Yeah.

Leo: I don't mind ads as long as they're anonymous, like on TV and radio. They don't know anything about me except they're probably reaching people. He's talking - maybe he's thinking about this Scroogled campaign from Microsoft in which Microsoft says "Google reads your email." Of course they do, as does Microsoft. Google and Microsoft both have to read your email to provide antispam filtering.

Steve: Well, and to target advertising.

Leo: Well, Microsoft - and this is what Microsoft should be saying: We both read your email. But Google uses it to target ads. We just use it for spam fighting.

Steve: Google understands it, and we don't.

Leo: Right. Maybe they understand. I think it's a little bit of FUD because it really comes from this notion that reading your email is a human reading it and with a human understanding. It's not - it's not that.

Steve: And we can't even agree on whether you're reading books, Leo, so...

Leo: [Laughing] What is reading email? In my opinion, indexing keywords in an email is not the same thing as some human reading it and making sense out of it. And you can tell that because the contextual ads on Google's Gmail suck. They don't - they have nothing to do with anything. And Microsoft even makes this point in the ad. Look, see, you've used the word "mortgage," so you're getting mortgage ads. The ads don't work. I think that to me that's an evidence that, yes, they're scanning email for keywords, but it's not reading your email in any sense that we understand, anyway. He's worried about people reading his email.

Steve: And my question to you is, do you know of any free anonymous email systems?

Leo: Yeah.

Steve: And I guess he doesn't like Google. Or...

Leo: Well, if you don't want to use Google, use Yahoo! or Microsoft's Outlook, both of which are free and anonymous.

Steve: Well, I think following from Mat's experience, he wants to use Google, for example, for his main, everyday use account, but he wants his registered email, key recovery and password recovery to be somewhere completely different and to be anonymous, to also be free.

Leo: So the first thing I would say is that any email system that offers antispam protection is reading your email just the same as Google is. You can decide whether that bothers you more than - if what you're saying is I don't want targeted ads, Outlook or Hotmail/Outlook or Yahoo! Mail - I think Yahoo! Mail...

Steve: I think all he's saying here is he just wants to be anonymous.

Leo: Well, that's - and Gmail's anonymous. I mean, your IP address is visible to any website you visit.

Steve: Well, but remember, the idea is he wants to use Gmail for his main account, so he needs an off-the-beaten path sort of...

Leo: Well, like I said, Outlook.com and Yahoo! Mail. But all web-based email sees your IP address unless you're using TOR.

Steve: I think I'd stay away from Yahoo!. Yahoo! seems to be having a real problem lately holding onto their accounts.

Leo: This is one I've used in the past. And, you know, Phil Zimmermann set this one up, it's called HushMail.

Steve: Oh, yeah, sure.

Leo: It's HIPAA-compliant private business email. They provide PGP. Encryption is built in. You have to pay for it, which means it's not fully anonymous. See, this is why I don't like this Scroogled campaign because I think it conflates a lot of different concepts. When you say "anonymous," is it not the case, Steve, that your IP address is visible to anybody you visit?

Steve: Yup.

Leo: And if a federal law official...

Steve: And ISPs are being required now to log.

Leo: Oh, yeah. Well, okay. So let's just talk about the email first. They're all subpoenable. So they can get your IP address and then go to the ISP and say who was using this IP address at this time, and the ISP says, oh, whatever you want. But absolutely, you make a very good point, which is that ISPs are in many cases, they're not yet required to, although they will be soon, I'm sure, recording everything you do anyway. So really all they have to do is figure out what ISP you're using, and then they go to the ISP and say, "Tell us everything about Leo." And the ISP in most cases, unless you have a very good ISP, but if you have Comcast or a standard ISP, will say, yeah, whatever you want to know, sure, sure, sure, here you go. So I think if you really, if you really want private email, it's a little more complicated than you might think.

Steve: Maybe lick a stamp, Leo.

Leo: I don't know how private that is, either.

Steve: Ah, that's true.

Leo: I mean, the truth is, if you're using encryption and TOR, you're pretty good; right? Because TOR would give you some anonymity about your IP address.

Steve: Yeah, that's a very good point. Running through TOR solves the problem. So you could use TOR and Outlook.com. I think Outlook seems like a reasonable free alternative to use as your repository for password account...

Leo: TOR's not perfect either because the ends have been in the past subpoenaed. But it's better than - it's probably pretty good; right? Nothing's perfect.

Steve: Yeah. And it's the people who are running mega downloads of really noxious content that draw attention to themselves through TOR, not somebody who's connecting to an SMTP server somewhere.

Leo: And, further, we should point out, if you use an Internet service provider, you're probably busted no matter what you do. And so really anonymity on the Internet, I don't know. I don't think that's really...

Steve: It's being lost.

Leo: Yeah. So anonymity means getting off the grid, using only cash, not using the Internet, not living anywhere where there are cameras of any kind. You pretty much have to move to the woods and be a survivalist, if you really want to be anonymous. I don't - I agree we all deserve privacy, but I doubt we're going to get it. So the problem with things like Scroogled is there's some sort of implication that Microsoft is doing a better job of privacy, and I don't think it's the case.

Steve: Where does - what is Scroogled? Is that the name of the campaign?

Leo: Oh. You don't know about this. Yeah, there's a whole Microsoft campaign called "Scroogled." It's Scroogled.com, but I just saw a TV ad for it, so they're actually advertising now, as well.

Steve: God, and they have a domain?

Leo: Yeah. And what they're telling people, Scroogled started with something not completely wrong, which was that Google Shopper, which used to be a search result,

is now all paid ads. That's legitimate. That's something people probably should know. But now they're saying, "And by the way, Google reads your email." They've been saying this for a while, Gmail Man reads your email. And it's really FUD, and I think it's kind of unfortunate because - for two reasons. One is it plays upon people's fear of technology and the anthropomorphizing of technology.

Steve: Yeah, and so Microsoft is being hurt to some degree by that, too.

Leo: It's a dumb thing, yeah, exactly, it's dumb. And it has the implication that somehow you're more private with Outlook Mail, which is not the case. The only difference is Outlook Mail doesn't use keywords to target ads. But it's still reading your mail. Has to. That's the only way you can do spam fighting. If "reading," quote, is what you're worried about.

Paul Vines, Seattle, Washington: Thanks for the job. He says: Steve and Leo, I started listening to the show about a year ago, and I have you to thank for a computer security internship I just got. Right on, Paul. The phone interview questions were all about SSL and SSH, what their vulnerable points were, and different types of attacks that could be performed on them. Halfway through the interview I realized just about all of my answers were coming from what I'd learned on Security Now!. Hah. So thanks for a great show, and keep up the good work. Isn't that nice.

Steve: It was very nice. I just sort of tossed that in because I thought that was cool.

Leo: Here's another kind of thank you from Joseph in Los Angeles. He says: Thanks for recommending DigiCert. I switched from Comodo to DigiCert. Comodo wanted $1,616 for my three certs; DigiCert wanted, like, half that. You saved me $837. The EV validation process was pain-free, and the installation instructions were easy to follow. Start to finish was less than four hours, including going to lunch. I like anything that involves lunch. I even had to call their tech support because of a mistake I'd made when ordering. They walked me through how to correct my mistake. Thanks so much for letting your listeners know about your experience. Joseph.

Steve: And I wanted - I saw this, and I thought, good, that gives me a segue because I had yet another amazingly positive experience. This new server that I was talking about having set up is running - is on Windows 2008 and IIS 7, whereas the creaky old one that finally died was IIS 5. Well, the certificates are incompatible. And so here I was, I think it was maybe Thursday night, maybe Friday night. It was after 5:00 Pacific time. So even if - I don't know where DigiCert is. Maybe they're in the Pacific Northwest. I don't remember. But, I mean, it was after hours, and I sent email to Todd, the guy that I'd worked with before, and I said, hey, I see how I can reissue things, but I absolutely want to make sure that that doesn't revoke the existing certificates because we're using those right now.

Leo: Good point, yeah.

Steve: And so I don't want to press the wrong button. And then I kind of poked around their website, and I saw where they had made it very explicit that they would always warn before anything would happen that would revoke existing ones. And one of their cool policies is, you buy one certificate, and you can use them on as many servers as you want. Now, that may not help many people who only have one server. But in my case I needed to straddle - I needed to set up the new server with different certificates for the same domains.

Anyway, the whole thing was, like, 10 minutes for three different - two EV and one standard certificate. I used their web interface. I recreated certificate signing requests on IIS 7. I dropped them into the website, pressed a button, and it emailed me my results. It was like [chuckling], it's just amazing. And it's like, this is the way - it's like a little certificate factory. This is the way it ought to be. And I've never understood why no one else can get it right. These guys really do. Oh, and my point was that, after I was about halfway through that, I got email back at, like, 5:45 from this guy. He said, "Hey, Steve. I'm no longer doing customer service. I'm over in something or other. But I saw your note and wanted to respond."

Leo: Isn't that great.

Steve: And I thought, wow, this is - DigiCert, D-i-g-i-C-e-r-t. They're the guys.

Leo: These are expensive. Are these the extended certificates, extended SSL?

Steve: Yes, the EV.

Leo: That's why they're so expensive, yeah.

Steve: Yes. And the EV, you get your root domain and your "www" for free.

Leo: Oh, that's nice.

Steve: And two other wildcards. So you can - so, like, I have...

Leo: Like images.grc.com or something.

Steve: Exactly. And in my case media.grc.com. They're all - they all live in one. And then I have my lower quality one is grctech.com, which is only used as a third-party for cookie checking, in order to try to get cookies set by third parties. So it had to be in a non-similar domain.

Leo: Well, I hope you've enjoyed this nontechnical respite because now we go to Question 7, and things get hard. Specifically, hard memory. Christiaan Basson in

Cape Town, South Africa asks of memory hard problems: Does it scale? Longtime listener, love the show, really appreciate the easily digestible chunks and resources you produce. That's a little disgusting. After listening...

Steve: Hopefully they're not chunky when they come back.

Leo: Eww. After listening to the recent episode covering memory hard problems, I couldn't help but think: Does it scale? How practical is the solution for a web farm churning through many authentication requests a minute? Could you perhaps explore this practical aspect of trying to implement this at scale? Thanks again for a great show. Christiaan.

Steve: So it's a great question. And I've got two memory hard questions here because it generated a lot of interest. I just couldn't even put them all in one podcast or we'd just have had the memory hard question podcast. Consider the lifecycle of your involvement with a web server, that is, how much real time is used in it validating your password versus how much time you're spending there? So you enter your username and password, and if it has to do this memory hard function that takes a second, I mean, that's all we're talking about, a second.

Now, understand that hashes, we see the Bitcoin guys talking about gigahashes per second, billions of hashes per second. And they're, like, at 50 gigahashes per second, 50 billion hashes per second. I imagine, though, that a memory hard system can only do one a second. It takes a whole second. So this is 50 billion times slower, and there's no way to speed it up. So that means that any hacker is going to run 50 billion times slower. So it's achieved its goal. And my point is that, yes, a second is a long time on the server end to spend. But that's the cost of offering this security. But in terms of the user's life with their login session, it's nothing. I mean, we only log in somewhere, we're poking around for a minute or two, maybe. And so my point is that, despite the fact that that's much more than a 50 billionth of a second, it's a whole second, it still works because the total population of people visiting that server farm will all be spending one second, yet hanging out there for minutes. And so it does scale. And sort of like in just the right way.

Leo: Beautiful. A lovely thing. Question 8 from Jason Crow, Rochester, Minnesota. He's wondering also about memory hard problems. Obviously a coder.

Steve: You have a problem with that whole...

Leo: He's a coder. Well, he's got a block here, a <Begin-Obligatory-Compliment> block.

Steve: Oh, yeah.

Leo: Yeah. Since the beginning (blah blah blah), a bright spot in my life (blah blah blah), please never stop (blah blah blah), SpinRite user (blah blah blah)... <End-

Obligatory-Compliment> block. I think you need a for while loop here, actually. While still smiling, I really enjoyed your explanation of memory hard problems in Episode 388, and I have a question: Would it be possible for the pipelined FPGAs to access some kind of shared mapped memory or shared page file, which already had the required memory hard problem contents mapped into it? In other words, work on the same pool of data.

Steve: Right.

Leo: If so, couldn't the first FPGA be, for lack of a better term, the super FPGA, the only one with the needed memory, which as part of its dedicated function is the only FPGA which creates and then stores the contents of the memory to a location which the following FPGAs then access? It's sure to be still much slower than each FPGA having its own memory, but I would think it would be much faster than each FPGA recalculating the needed contents of the memory space every time it's required. In an extension to this, couldn't each memory address space retrieval then also be pipelined? This isn't something we'd put in our living rooms, but perhaps not out of the realm of possibility for a nation state. Nowadays, with cheap hardware, probably anybody could do this. Your thoughts? This is clustering. Jason Crow, Rochester, Minnesota.

Steve: And the answer is no.

Leo: No.

Steve: What's so cool about this, I just - I love how simple and elegant this is. Remember that you take a region of memory, and you use the password to - you just hash it, for example, in a standard hashing hash, to get the first value. And you stick that in the first location of memory. Then you hash that using, again, the password as the key, and you stick it in the second slot of memory. And you do it again for the third and again for the fourth and again for the fifth. So what you end up with is pseudorandom noise in this array.

But then, okay, so what he's saying is couldn't you do like a super FPGA to just sort of blast that out? Now, then, he somehow wants to do the next step in parallel. And the beauty of this is you can't because you then take the result from the final memory cell that you filled, you hash that, and that you treat as an address into the array. And the contents of that address you hash, and that gives you the next address. So there's nothing to do in parallel. You have to follow a path. It's a little bit like my Off The Grid approach using the Latin squares. You have to follow a path. And the contents of each memory cell, mixed with the key that is the master key, only that gives you the next location in memory. And then only when you know that do you have the next one. So it's provable and incredibly elegant that you - there's nothing you can do in parallel. You don't know anything until you have the next - the data in the cell you jump to, and then its contents, not its location, its contents tells you where to go. It's just - it's beautiful. And no one has figured out any way to speed it up. It's great.

Leo: That's the point.

Steve: Yeah. Exactly.

Leo: A reminder about something we talked about many moons ago, which is I'm curious about what the status is. Chris Rhodus in Madison, Mississippi - MS is Mississippi; right? - reminds us about the spray-on nanocapacitor antennas. Remember those? I was cleaning up my bookmarks this morning and came across a bookmark for Chamtech, which was chamtechops.com. They had a spray-on antenna kit you could buy. No longer on their website, but I started to do a little research. I came across an article. They partnered with an investment banking firm, Hickey Freihofner Capital, so maybe things are starting to happen. Did you ever hear from anyone who actually used the product? Was it a TED Talk or something like that? Oh, no, it was a Solve for X Intel talk or something like that. Chris Rhodus. Thanks for all the hard work.

Steve: And what I remember, to refresh our memories, remember they, like, sprayed it on a rock, and it turned the rock into an antenna? And they sprayed it on a tree, and it turned the tree into an antenna.

Leo: Yeah, nano antennas onto something, yeah.

Steve: Yeah. And it was nanocapacitors, some sort of a wacky nanocapacitor emulsion which they claim radiates in an amazing way. And so I did follow the link, and it was SFGate.com on their PR website, about their partnering with an investment banking firm. Apparently there's huge interest being shown by everyone who listened to our podcast who want to spray rocks. And so they need to raise some capital.

Leo: Well, why did they take it off their website? I am still [muttering].

Steve: Yeah, no, I agree. And we have a friend of ours who listens, who's a big antenna guy. I'm blanking on his name right now. But I remember he waved his arms around and shouted and said, no, no, no, no, no. I design antennas. You can't spray rocks.

Leo: [Laughing] So was it, I mean...

Steve: Wait, could it be Spencer Webb? Is that somebody - no, no. That's somebody from PC Week, I think [Spencer Webb is at AntennaSys].

Leo: I have to say, when I go to their website, it is not inspiring.

Steve: No, it's little scary, isn't it.

Leo: What do they have on there? Looks like an 1890s mechanical...

Steve: Yeah, a [chyrasopterus ph] or something.

Leo: Yeah. I...

Steve: Maybe they let the domain go.

Leo: Yeah. Well, the other possibility is, since they say we proudly serve a variety of government and military agencies, is that maybe - no, this is the same company. Maybe they just - maybe somebody bought it. Maybe the feds said, you know, you might not want to talk about this anymore.

Steve: Okay. Yeah, I mean, it's hard to guess. They said, "'Our decision to engage Hickey Freihofner Capital is a significant step in helping us realize our vision of improving the range, energy efficiency, and quality of the devices we all use to stay connected,' said Anthony J. Sutera, co-founder, CEO, and president." Oh, I wonder if he's also a Navy Seal.

Leo: [Laughing]

Steve: "The antenna application of nCap" - oh, they've got an acronym now - "nCap technology are virtually limitless." Hey, if you've got rocks and trees covered, pardon the pun, then I suppose you pretty much can...

Leo: That's pretty good.

Steve: ...anything you want.

Leo: That's unlimited.

Steve: "From improving cell phone reception to enabling consumers to access wireless services from almost anywhere." Didn't they spray it on a wall?

Leo: Yeah, a brick wall.

Steve: I mean, I remember it was kind of - it was wacky. It was fun. Anyway, so they've patented it, but that doesn't mean anything because people patent windup steamrollers and things, so...

Leo: Patent things like, well, don't get me started on patent law.

Steve: [Laughing] No.

Leo: That could be a long conversation. William Parsley - I love your name, William - in Ohio had a random question: About a year ago, your podcast was brought up by a student in one of my classes. He was recommending the podcast to someone else, but I overheard it. I was intrigued. I decided to check it out next time I had some free time. Well, I've been listening to Security Now! from the beginning for a little less than a year now, I think, and I'm up to Episode 167. Oh, you've got a way to go there, Mr. Parsley. You're not even halfway there.

I feel like I've learned a ton from your podcast I wasn't getting from school or books. I'm not sure if that's because of the approach you use to present things or the fact that the content is consistently relevant to today's world. And this is taking into account I'm not even into the year 2009. It's almost like ...

Steve: And now all the content is gone off the website, and he's unable to listen to anything.

Leo: Well, now, we still have all the content.

Steve: I know.

Leo: It's just your versions are gone.

Steve: And it'll be back later today because I'm obviously not going to go to sleep anytime soon.

Leo: Yeah, Steve does - oh, dear. Steve, you should get some sleep. It's okay. Steve has 16Kb and transcripts and so forth. But we still have the high-quality audio and video. So he can still get it.

It's almost like a soap opera, where I can't wait till the next week to see if the problem that's brought up in the show has been addressed by Microsoft, by Google, by Wells Fargo, whoever it is that had the problem in the earlier episode. One random off-topic thing you said that caught my attention has been haunting me. You mention in one of the recent episodes, well, recent for me, that is, you carry around an iPod with background music on it [SN-165]. This is kind of an odd request, but I'd really be curious to know what you have as your background music. I've been looking for something like that, but the music always distracts me. I like listening to it, I guess, instead of working. Not a question, just wanted to say thanks to you and Leo for putting out a wonderful podcast. I travel a decent amount for work, and this podcast makes it easy. What do you listen to? Oh, lookit, he's holding up CDs, folks.

Steve: Yes. I really, really like this. It's a series of 10 called "Liquid Mind." And the artist is Chuck Wild. And it's not for everybody. It is, I mean, if you tend to doze, this will knock you right off. I mean, I could listen to it right now, and I wouldn't be able to finish the sentence.

Leo: He's a daytime Emmy nominee.

Steve: Some of it is just beautiful. I think it's synthetic. It's sort of chords merging and blending, and there's clear composition involved. Many of the pieces I've actually really come, like, I'll stop and listen to it. But don't worry, William, that's not normally what I do. But it is, it's perfect for when you want to fill the background to blank out noise, yet you don't want to - you just want to relax, and you want to read. Or, well, no, I guess when Leo's reading he's listening. So you want to do something where you want an audio background. And I think I have 40 hours of it.

[Music]

Leo: This is it. Listen. Go to sleep. I'll play it from the beginning.

Steve: Boy, that almost - that really did almost put me out.

Leo: Can I make a suggestion?

Steve: Yeah.

Leo: Because I have seen studies that say the best music to listen to if you want to keep thinking, but not - obviously, anything with lyrics is out because we're going to start listening to lyrics, and then you're not being able to program or whatever. So it's got to be instrumental.

Steve: Oh, I can't, absolutely can't. And so I have...

Leo: Gotta be instrumental.

Steve: But my employees used to tease me because I had, you know, my music was filling the company. And they said, yeah, Steve's music with no lyrics.

Leo: I'm going to make a suggestion. I have seen research that says baroque classical music - Bach...

Steve: For me it's Vivaldi. I love...

Leo: Vivaldi, Purcell. It's very bright, very upbeat, no lyrics. And I have seen many studies that say that actually you can listen to that, and it will actually improve your productivity.

Steve: The only problem I have with it is it sometimes can be a little too engaging. They'll have crescendos and, like, things happening. And you're like, whoa. Very little happens in Chuck Wild's Liquid Mind.

Leo: No [humming]. It's the kind of music that they play when I get a massage. And, frankly, it just puts me right out.

Steve: Yeah, that's exactly it. And so anyway, that's the answer to William's question. I love it. So if anyone else is interested, check it - wherever you found it, Leo, I guess other people can, like, go...

Leo: Oh, yeah, yeah. LiquidMindMusic.com.

Steve: Oh, perfect.

Leo: And it's on iTunes, as well. You can buy it from iTunes. I, um, yeah, give me baroque.

Steve: Hey, it doesn't have to be for you. It's for me.

Leo: Give me baroque. I like the baroque, yeah. Little Brandenburg Concerto, I don't...

Steve: Oh, No. 3 in G major.

Leo: Yeah, it's beautiful.

Steve: That is the best thing ever written.

Leo: [Indiscernible].

Steve: I can't do - oh, are you kidding me? My world comes to a halt if Brandenburg Concerto No. 3 in G major is playing. It's like, okay.

Leo: No, you're right. That's pretty good.

Steve: It's just it's, oh, my god, it's so well done.

Leo: Yeah. No, you're right. Brandenburg may be too good.

Steve: Yeah.

Leo: But a lot of Vivaldi. I listen to Water Music. There's some good stuff out there that just will - it's bright, but won't get you going. And I, see, I don't - I'm not big into the new age sound, which is what this is. This is kind of...

Steve: So [Cruz Cova ph] just tweeted, and he says, "Hey, Steve. I have those CDs, too." He says, "I can't focus without them."

Leo: I mean, they certainly don't distract. You're not going to stop and go, ooh, what's that?

Steve: Actually there is one that I do stop on, one particular composition out of about 40 of them. Oh, that might be the one, actually.

Leo: This is relaxing. I'm afraid it'd be too relaxing for me. You, I bet you, because you work at Starbucks and stuff, I bet you part of the reason you do this is not so much for the music but to seal out the outside world.

Steve: Yes, as I was saying, it is a beaut- if you were, like, trying to read print on a train or on a bus or on a plane...

Leo: You can't hear anything, yeah, you don't hear anything else. And that's really more the point than the music itself. It just is - it's just something, you know, you could almost listen to white noise except that's not quite as attractive.

Steve: Yeah, I just think that's lovely.

Leo: Yeah [humming].

Steve: Because I've got enough going on. I'm twitchy enough.

Leo: Yeah, you could use a little - all that coffee you drink. How much is that? Now, I know people want to know this. You were up all night. You haven't slept in 24 hours.

Steve: Correct.

Leo: What coffee brews are you using? What are you using to stay awake?

Steve: Actually, I have something I like so much, I'm fantasizing about somehow arranging to have you taste it because it's just - it's so good. But this is the end of my third pot.

Leo: Holy cow.

Steve: And around 11:00 I thought, well, I'm going to stay up all night, so let's start having some coffee. I really had a ball last night.

Leo: So, what - is it a bean that you like here? What is going on? What is this?

Steve: It's not exotic at all. That's the thing. But, for example, at Starbucks the other day I had my crew - I got the little espresso paper cups, and I poured some from my canteen into my little cup, and I said, just try this.

Leo: This is real coffee.

Steve: And they're all, like - yeah. And they're all, like, they've got froufrou, and they've got cream and sugar and everything to, like, manage what Starbucks gives them. And they, like, they couldn't believe how good it was. Jenny...

Leo: Is it the bean? What is it? What is - you've got to give us a hint here.

Steve: So here it is. It's just Starbucks' espresso bean. And I grind it for drip, and then I drip it through my little brown paper Melitta filter.

Leo: That's fabulous.

Steve: Using my little whatever that wacky - you knew the name of that silver pot that is like a five-cup sort of thing.

Leo: Yeah, yeah, moka pot, yeah.

Steve: Whatever. Anyway, it is - so you get - it's the dark roast. It's actually lighter in caffeine because, as we know, espresso has less caffeine than lighter grind, or lighter roast because roasting roasts the caffeine out of the bean. And it's - but I don't do decaf because decaf is scary processing. And, oh, my god, Leo, it's just - and I just, you know, black, no cream, no sugar. And it's just - it's a smooth, amazing cup of coffee, just the espresso bean ground for drip and dripped.

Leo: You have Trader Joe's down there; right?

Steve: Oh, we do.

Leo: Next time you're at Trader Joe's, get a can of the Kona. The good Kona. It's expensive.

Steve: Okay. I don't care. I'll try it.

Leo: I think you might even like it better.

Steve: I'll try it.

Leo: It is the most smooth delicious coffee I've ever had. So good.

Steve: No kidding.

Leo: Oh, yeah.

Steve: Oh, neat. I'm...

Leo: If you can get a good Kona pea bean, you're getting the best, in my opinion.

Steve: Okay.

Leo: It's also among the most expensive coffees in the world. But it's very good.

Steve: Well, I mean, and Trader Joe's generally is pretty affordable. So I'll...

Leo: Yeah, it's not bad. It's not bad.

Steve: They've brought it at the best price you could get.

Leo: Right, and they have a good Kona. It's really good. Now, I actually don't use it because I'm using - making espresso. It's a waste of good Kona. When I do the press, I do the Kona. But for the espresso I just - we have a local coffee roaster here who does something called Godfather's Roar which is just right for me. It's a coffee I

can't refuse.

Steve: You have a roaster. Wow, Leo, I'm so jealous. And a personal trainer. And...

Leo: Oh, I get the whole...

Steve: And a masseuse, apparently, who, okay, so you don't want that music playing during your massage.

Leo: I, you know, I used to get massages every week, and I stopped doing that because I was too relaxed [laughing].

Steve: Yeah.

Leo: Now I just get them as needed.

Steve: We've all noticed that's a problem with the people on the TWiT network.

Leo: I get them on demand.

Steve: They're all too relaxed.

Leo: Yeah. I guess for President's Day maybe I'll get a massage. You know, actually we have a...

Steve: When is - is that Monday?

Leo: It's Monday. We have an all-day - this is funny. Lisa and I have - normally Friday's a day off. We're going to take all day. We're meeting with patent attorneys all day. It's an all-day affair.

Steve: What?

Leo: I'll tell you offline. But as a reward, at 5:00 p.m. she booked us a massage. It's like, if you're going to spend your day off, 10 hours with attorneys, you deserve something, a reward at the end of that.

Steve: That'll be cool.

Leo: Don't think even Kona's going to help me on this one. Steve Gibson does this show every Wednesday, 11:00 a.m. Pacific, 2:00 p.m. Eastern time.

Steve: Come hell or high rise.

Leo: He does not stop.

Steve: And I may not have slept, so I'll still be rising.

Leo: Holy - you'd better get some sleep. I want you to - you're going to start hallucinating.

Steve: Nah. I think my - the most I went was three days.

Leo: Augh.

Steve: I rewrote the entire I/O system of an Interdata operating system, changed it, at Bob's Big Boy on a pad of engineering paper.

Leo: Jiminy.

Steve: In a three-day, no-sleep - because Bob's Big Boy was 24 hours back then.

Leo: Sure. Oh, yeah. Oh, yeah.

Steve: And I liked their chowder.

Leo: That's where finer programmers go to - all the best.

Steve: Just sat there and ate French fries and drank coffee and rewrote the whole I/O system. And it worked. So it was - and I did that a couple times. But three days is about my limit.

Leo: Wow, you know, I think I am getting old because the idea of going without any sleep of any kind is just painful.

Steve: And you should know I'm a big sleeper. I mean, this is...

Leo: Good, I'm glad to hear that.

Steve: This is not something I do often. But I was watching "Morning Joe" a couple weeks ago, and I was really surprised. They were sort of talking around about how little sleep they get.

Leo: Well, they do a morning show.

Steve: And that's what Jenny said, she said, oh, you know - well, exactly. That's part of the problem. And then she said, oh, you know, it's sort of macho not to get - not to need that much sleep. And I said, well, you know, I mean, I'm really an eight-hours-a-night person.

Leo: Me, too.

Steve: Because I know it's so important. It is anti-inflammatory. Your body needs it to recover. And, no, it's...

Leo: It's important for health, I agree. You're putting your - you're taking life in your hands here, Steve.

Steve: Yeah, well, we've got to get the videos and the audio back online.

Leo: All right, okay.

Steve: So I'm headed to Level 3 right now.

Leo: Steve Gibson, GRC.com, that's the website you must go to. Later today the 16Kb versions of all the shows will be back online, as well the transcriptions that Elaine does, the actual English-language, written by a human transcriptions of each and every episode. We have the 64Kb MP3s and the video in a variety of formats on our site, TWiT.tv/sn, and wherever better Internet programming is made available. That would include iTunes, the Zune Marketplace. On your phone there's a variety of things like Stitcher, for instance, you can listen to Security Now!, and I encourage you to do so.

Steve: And YouTube has it now, YouTube dot...

Leo: YouTube.com/securitynow, yeah. Yeah, that's another spot for it. Thank you, Steverino.

Steve: Thanks, Leo.

Leo: See you next time on Security Now!.