CacheBleed

Description: Leo and I discuss an event-filled week of security news (with some comic relief courtesy of John McAfee on the Apple conflict), after which we examine the latest side-channel attack, which is effective even against carefully written crypto code designed to thwart side-channel attacks.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-550.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-550-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. Lots to talk about. He's finally going to break his silence about John McAfee. And then we'll look at an academic security flaw called CacheBleed. It's probably not something you need to worry about too much, but it is fascinating. Also quantum computing, how soon? It's all next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 550, recorded Tuesday, March 8th, 2016: CacheBleed.

It's time for Security Now!, the show where we talk about all the latest security news. We help protect you. We help you understand what's going on. And really that's almost the most important role that this guy plays, the Explainer in Chief, Steve Gibson. Hi, Steve.

Steve Gibson: Hey, Leo. Great to be with you again for Episode 550.

Leo: Wow.

Steve: Like those round numbers. Now, 555, that'll be another good one. And then there'll be 567. And, okay, I'm done. Then probably nothing really of interest until a thousand.

Leo: I think we should - we missed a bet. We should have numbered the show, well, you always wanted to start at zero. But I think we should have done it in hexadecimal.

Steve: Ooh, that would have been good.

Leo: Wouldn't it have been fun?

Steve: That would have scrambled up some people.

Leo: Nobody would - what, FF?

Steve: Wait a minute. ADAB2? What? What?

Leo: Chatroom, what is 550 in hex? Somebody's got a hex calculator there sitting around. It would be kind of fun.

Steve: Yeah. So it'll be a one, eight...

Leo: He's doing hex in his head, folks.

Steve: I can, but of course I've got a hex calculator within reaching distance. I didn't want to cheat, though. Decimal 550 is hex, oh, 226.

Leo: 226. Chickenhead got it, 226. Yeah, that would confuse the hell out of people.

Steve: Yeah. Especially when - then it goes to 22B, and they're like, wait.

Leo: What?

Steve: Where's A? Well, A was in front of B, but then C and D and F.

Leo: Yeah, we can't really do that.

Steve: 22E. What?

Leo: Yeah, it wouldn't work.

Steve: I don't think.

Leo: So I see that the show's title is CacheBleed.

Steve: Yes.

Leo: I guess that's an appropriate topic for today.

Steve: Well, I had intended, as I said last week, to do DROWN and CacheBleed. But the week provided so much entertainment, up to and not including McAfee, who admitted that he was lying before. I didn't even cover him, deliberately didn't talk about him the last couple weeks.

Leo: He said he could - first he was going to have his crack team of hackers social-engineer their way into the San Bernardino iPhone. That was blatantly bizarre since the owner was dead. There's not much you could do there. And then he said, oh, everybody knows how to crack an iPhone.

Steve: Just give it to me and let, you know...

Leo: "I'll eat my shoe," he said, and I'm hoping he's going to do it, "I'll eat my shoe if I can't crack that iPhone."

Steve: Yeah, I don't know if you noticed he walking around in chocolate shoes now. So that's not such a big deal. But anyway, so there has been, finally, that has sort of come full circle. So that and a whole bunch of other stuff. Of course RSA's going on, so there's some RSA stuff. So anyway, the DROWN attack is so cool that I didn't want to shortchange it.

The CacheBleed attack is also cool. It's a new form of side-channel attack that is effective against even the latest OpenSSL, which is deliberately engineered to thwart side-channel attacks so that, as we've talked about before, the way you do that is you don't allow your keying material to change the order of execution of the instructions because that can be sensed by power drop or power consumption or radio emissions or whatever. So even on code where the keying material doesn't change the code execution, some very clever researchers have figured out still how to suck keying out of OpenSSL.

So that's the big topic for this week, after we catch up with a whole week of really great news. So a great podcast. And I completely - it's really annoying now that Microsoft's Second Tuesday collides with our Tuesday. And I'm wondering, maybe I could call somebody and say, hey, look, move that release of your patches.

Leo: Yeah, terrible timing.

Steve: On the other hand, they laughed at me when I told them to take raw sockets out of XP, so I doubt that there's much chance that we're going to get them to change when they release their patches. But there was - this is Patch Tuesday, being the 8th of the month, last Tuesday being the first. And I haven't even looked at it except that, when I turned my Win7 box on, it said - and I had just finished updating it a couple days ago. It said, oh, 13 important or, yeah, 13 important updates. So I just said fine, go do it, and I'll check and see if there's any emergencies.

But I don't think so. I certainly haven't seen any in the news. So it's not like there was everyone going oh my god, oh my god, oh my god, and through all the other inputs that I have, and this is the Tuesday that fixes that. So there is nothing that we know of that is pending and is a catastrophe for Windows at the moment. So great podcast, and here we go.

So I don't know why I am not yet in the habit of putting the topic that corresponds with the Picture of the Week as the first topic of the week because I want to, like, note the Picture of the week, and then I'm thinking, okay, we're going to talk about this later. Well, let's talk about it now.

Leo: All right.

Steve: Because the Picture of the Week is wonderful, and the news just occurred. The EFF put out a press release that the Let's Encrypt initiative has issued its millionth free HTTPS cert.

Leo: Wow. Isn't that great.

Steve: And it began, that Picture of the Week shows that it was a little ways into December of 2015 that this went online. It got out of beta, and they began issuing certs in earnest. And so we have December, January, February, and we are the same little bit into March. And they have crossed the one million mark. What's also interesting is that some of the certs are multidomain. So they are actually covering 2.5 million fully qualified domain names.

They said: "Three months from the first beta version of the service becoming available, Let's Encrypt has passed this significant landmark and is helping to ensure websites are more secure with encryption. Moreover, since a single certificate can cover more than one domain, the million certs Let's Encrypt CA has issued are actually valid for 2.5 million domain names."

They also said, and I thought this was interesting: "Much more work remains to be done before the Internet is free from insecure protocols, but this is substantial and rapid progress. It is clear that the cost and bureaucracy of obtaining certificates was forcing many websites to continue with the insecure HTTP protocol, long after we've known that HTTPS needs to be the default. We're very proud to be seeing that change and helping to create a future in which newly provisioned websites are automatically secure and encrypted."

Now, I guess I'll buffer that a little bit, to suggest that, when encryption is made this easy, then, yes, there's absolutely no reason not to use it. But certainly, even among this initial million certificates and 2.5 million domains, there's sort of opportunistic encryption. There's like, well, yeah, I mean, it's a blog, and nobody needs security there. But, hey, it's better to have it be encrypted. And we know that Google is, if they haven't yet, they've been talking about biasing search results pro encrypted sites. So that's another reason to encrypt is for higher Google search rankings.

And I'll remind people, again, that this is still - it's a very minimal level of true security. For example, I'm continuing to buy certificates from DigiCert, my absolute favorite

certificate provider, and I just did that two weeks ago. I refreshed all of GRC's certificates. I'd had older ones that I had co-issued, both in SHA-1 and SHA-256. I switched over on New Year's Eve so that Google's Chrome browser wouldn't be upset. And yet I was still able to use SHA-1 through 2015 without raising any alarms so that people could get to GRC who had older browsers or, for example, had the corporate appliances that were signing the certs with their SHA-1 private key or, yeah, exactly.

But again, the reason I'm buying DigiCert certificates is that I want to have the extended validation where they go much further than just saying, yes, you have demonstrated control over this domain name. It's, yes, you have proven you are Gibson Research Corporation, a corporation in good standing. You're known through other real world means and so forth. So, which is not, again, everybody knows what a fan I have been of Let's Encrypt. What this does, though, it expands the ecosystem, essentially to automate the process of getting a certificate for a domain name which represents nothing more than that. Yet that does provide encryption, I mean, potentially for everything. There's no reason not to use it to encrypt your website. It's just, it's free, and it's easy.

And the graph is just wonderful. I mean, it is an exponential-looking graph. It has got some kinks in it. It's not a smooth exponential curve. So there were some events at various points, who knows what, like maybe a major hosting provider incorporated automated Let's Encrypt certificates so that suddenly all of their hosted domains were able to be HTTPS. That's the kind of thing that helps this to happen.

And I'm sure that what we'll see in the future is, if it isn't already, and I haven't looked, is that later distributions of Nginx and Apache, and maybe someday even IIS, will just incorporate the Let's Encrypt protocol in their base, so you don't even have to go get it, just it's on by default, and you have to say, no, I'm going to install - I would rather use my own higher level of assertion certificate. But then, if you don't override it, it just gets one from Let's Encrypt. Why wouldn't it? So anyway, really, really, really great progress.

I wanted to just mention, just a tiny mention of the smartphone encryption update, and that is we talked last week about how Judge Orenstein, I think it was, had agreed with Apple and stated that the FBI or the Department of Justice was overreaching with their request that Apple unlock an iPhone 5c that had iOS7, which means Apple could unlock that phone, if they chose to. They were resisting, as they will. And the judge argued that the All Writs Act was insufficient, I mean, it was like just way the wrong approach. And so the news since then is that the Justice Department is appealing that decision.

And so the battle goes on; and hopefully, as we all know, this ends up in front of Congress's committees. And in fact, while we were doing the podcast last week, one was underway. And this is looking very good for the people that are encouraging encryption. I mean, I'm really hopeful now that this may turn out okay because we've got the NSA agreeing that strong encryption is important. So, I mean, the NSA, and all other commercial entities, all the academic, all the cryptographers, I mean, everybody. So essentially it's everyone saying what law enforcement wants is wrong. And it'll be difficult to see how Congress can just ignore all of that, this overwhelming support for what Apple is waging.

I didn't hear you talk about it on MacBreak Weekly, but I imagine you had to, Leo, the first Mac ransomware...

Leo: Yeah.

Steve: ...to appear. What happened is that, on March 4th, Palo Alto Networks was quick to detect that the installer for a nice, fast, easy, free, BitTorrent client was bringing along a little more than the fast, easy, and free BitTorrent client. It had a fully mature and operational ransomware, technically the first for the Mac. They have a very nice short brief on this that I'll just share because it's hard to say it any cleaner than they said.

They said: "On March 4th we detected that the Transmission BitTorrent client installer for OS X was infected with ransomware, just a few hours after installers were initially posted. We have named the Ransomware 'KeRanger,' K-E-R-A-N-G-E-R. The only previous ransomware for OS X we're aware of is FileCoder" - and I remember us talking about it two years ago - "which was discovered by Kaspersky Lab in 2014. As FileCoder was incomplete at the time of its discovery, we believe KeRanger is the first fully functional ransomware seen on the OS X platform.

"Attackers infected two installers of Transmission v2.90 with KeRanger on the morning of March 4th. When we identified the issue, the infected DMG files were still available for downloading from the Transmission site. Transmission is an open source project. It's possible that Transmission's official website was compromised" - and that certainly seems likely - "and the files were replaced by recompiled malicious versions, but we cannot confirm how this infection occurred.

"The KeRanger application was signed with a valid Mac app development certificate; therefore, it was able to bypass Apple's Gatekeeper protection. If a user installs the infected apps, an embedded executable file is run on the system. KeRanger then waits for three days before connecting with command-and-control servers over the Tor anonymizer network. The malware then begins encrypting certain types of document and data files on the system. After completing the encryption process, KeRanger demands that victims pay one bitcoin, about $400 at this time, to a specific address to receive their files. Additionally, KeRanger appears to still be under active development, and it seems the malware is also attempting to encrypt Time Machine backup files to prevent victims from recovering their backup data.

"Palo Alto Networks reported the ransomware issue to the Transmission Project and to Apple on March 4th. Apple has since revoked the abused certificate and updated XProtect antivirus signature, and Transmission Project has removed the malicious installers from its website. Palo Alto Networks has also updated URL filtering and Threat Prevention" - those are its products - "to stop KeRanger from impacting systems."

And so a couple interesting details. KeRanger infected the Transmission installers that, as I mentioned, were signed with a legitimate certificate. It was a developer whose certificate was owned by a Turkish company, and a different developer ID was used to sign previous versions of the Transmission installer. So that indeed suggests that the way this happened was that either the Turkish company's certificate got loose, or an employee there, or who knows what. But it was signed...

Leo: No, they think the bad guys actually were the Turkish company.

Steve: Oh, interesting, okay, okay.

Leo: Yeah. You can get arrested, I guess, I don't know.

Steve: And so probably then the site was broken into somehow, defaced, and those files were replaced.

Leo: Same thing, you know, just happened recently with another open source project where - I'm trying - oh, Mint Linux, same exact thing. Remember that?

Steve: Yes.

Leo: So, you know, just because it's open source it makes it a little easier because you can recompile the whole thing and just put in the installer, put a little extra little something something.

Steve: Yup, and in fact I remember that, we talked about that, and that's one of the reasons I don't provide open source. Not only is it all assembly language with a whole ton of custom include files, and people would just say, uh, what is he doing over here? But also I don't want my stuff, the GRC apps, to be cloned and offered in other file downloading sites.

So anyway, after connecting to the command-and-control server and retrieving the encryption key from the user's computer, thus exporting it so that the C&C server has it, then the executable will traverse the /users and /volumes directories, encrypting all files under /users and encrypt all files under /volumes which have specific extensions. And the Palo Alto Networks document specifies, it enumerates some of them. And basically it's 300 different file extensions, which to me looks like everything it can possibly encrypt, but your system still runs. So it's not encrypting the kernel itself, but all your documents, all your images, audio files, archives, source code, database files, email, and certificates. So everything that you've added to the system that you value and care about is scrambled.

So anyway, so if anyone worries that they may be, I mean, if they're hearing about this for the first time, it's people who would have downloaded the Transmission BitTorrent client from 11:00 a.m. Pacific Time on March 4th through 7:00 p.m. on March 5th. That's when it finally got taken down. They could have been, you know, those people could be running right now this ransomware.

Leo: Yeah, you'd know pretty quickly.

Steve: Yeah. I was just looking at the date. Today's the 8th. So unfortunately...

Leo: It started yesterday. It didn't start doing anything till Monday.

Steve: Correct. And I'm thinking, so if you downloaded it late in the day on the 5th, and you hear this now, unplug your computer. Take it off the 'Net because you do not want to let it get in touch with the command-and-control server. It will not do anything until it's established that relationship. So keeping it from connecting is your emergency, pull-the-cord-out-of-the-wall maneuver. And then there are remediation steps. I've got the link to the announcement. I'm sure there are other things since. I didn't go digging deep for

other references, but there must be other things telling you what to do if you think you've got this. But the Palo Alto Networks link that I have in the show notes does have steps you can take to get this thing out of your system before it activates.

Leo: And they've shipped an update that actually removes the malware.

Steve: Apple has?

Leo: No, Transmission has.

Steve: Oh, good. Oh, good. So...

Leo: So in fact, Apple immediately pulled their cert, which means Gatekeeper, if you tried to run the installer at this point, would say no, you can't install that.

Steve: Right.

Leo: And they added, they have a kind of hidden malware detection and removal tool that gets updated. They've added the signature for it to that.

Steve: Nice.

Leo: So I think it's - 6,500 people downloaded it, according to Transmission. We haven't heard of anybody who actually got their files encrypted.

Steve: Nice.

Leo: And of course the best thing is, if you have a good backup, you're also okay. You just delete the encrypted files and start over.

Steve: Well, and so this demonstrates the need for fast response. And it is very cool that it was signed by a cert that could be instantly revoked and that revocation pushed out so that immediately the ecosystem responded.

Leo: That's a good system. That's the Gatekeeper system. It really works, yeah.

Steve: Yes, yes.

Leo: It's really good.

Steve: Yeah. And of course this is why I spent some time last year being upset with Google over Chrome's absolutely nonfunctional revocation system. They say that it works, but we proved that it doesn't. You go to revoked.grc.com with Chrome, and it says, oh, yeah, that's fine. Except that that's a revoked certificate, so...

Leo: But it complains if you go to - somebody sent me a note saying you're using an old SSL - you're using whatever it was, Hash128, on our Tech Guy Labs site, which doesn't have SSL. But I guess if you enter https://techguylabs.com, you'll get an error message. But that's because there's no cert on there. So I don't know what...

Steve: I know.

Leo: Thank you, Google.

Steve: I know. So the RSA conference happened, and a bit of news came out.

Leo: I'm thinking next year we should cover this, and you should be there. You think?

Steve: I probably should.

Leo: And we'll cover it with you.

Steve: You know, the one time that I went was Stina.

Leo: You met Stina, I know.

Steve: I mean, look what happened with Yubico as a consequence of that. So, yeah, it's just a matter of time. But, yeah, it would be fascinating. And in fact I - why do I think I have a link? Oh, I do, it's later in the show notes I have a link to the posted, the official posted by RSA cryptographer's forum, which is fascinating. It is the, literally in the case of Whitfield Diffie, the white-bearded cryptographer, I mean, it's the whole RSA team and a few other guys who are very active, the fathers of crypto, for 47 minutes having a really great conversation about cryptography. Anyway, we'll get there in a second. And I also created a bit.ly link, I think it's just rsacrypto, all lowercase, rsacrypto. And that will bounce you over to the YouTube video that's really, really worthwhile.

Anyway, everybody's wondering and worrying that quantum computing spells the end of cryptography. And so I just sort of want to assuage people's concerns. What was just released in the IEEE Spectrum magazine and site was some news from a breakthrough at MIT and the University of Innsbruck, who made a breakthrough in quantum crypto factoring of a number. Now, the number was 15.

Leo: They factored 15?

Steve: They did.

Leo: Wow. Let's see, five, three, and one. Wow.

Steve: An unbelievable amount of technology. They had cryo compressors cranking away. They brought the temperature down. They stabilized the platform so that it wouldn't shake the atoms out of alignment, and anyway. And they managed to factor the number 15.

Leo: It's pretty impressive.

Steve: Now, it did it very fast. It did it atomically, you know. So I have in my show notes, I wrote there was a recent breakthrough MIT and the University of Innsbruck researchers made who successfully used a device known as an "ion trap" containing five atoms to successfully compute the factors of the number 15. Now, okay. What is cool is that five atoms can somehow do that. And I have no idea how. Just I haven't gotten around to looking into it. I do, however, I thought, as I was writing this down, I thought, you know, I think I had a book I was getting ready to read.

And so I'm holding it in front of the screen, a book titled "Post-Quantum Cryptography." And the lead author, right up at the top, is our friend Daniel Bernstein, who is already involved. So for what it's worth I wanted to mention that there's already lots of academic research going into, uh-oh, what if factoring huge numbers suddenly becomes not hard anymore? And you'll need more, a bunch more atoms. And again, we know that these sorts of things never get worse. They only get better. And so they'll get six atoms, then they'll get seven, then they'll get eight, then they'll get nine. Now, they're going to need a whole lot more atoms in order to factor numbers with as many bits as current large RSA keys have. And then apparently you start having other problems which five atoms don't have, like keeping 2,000 of them all, like, disciplined in your ion trap.

Anyway, so I just wanted to assure people that we're at the point today where breakthroughs are factoring the number 15. And what's cool is that somehow five atoms do that, and that, you know, someday, I think it's - we can see the path. And that is that factoring a really huge number into the two primes that were multiplied to originally get it, which is that that's the hard thing about the hardness in RSA crypto is that it's trivial to multiply two primes to get a big number. We don't know how to, in any reasonable amount of time, break that apart again, to take that big number and figure out the two primes that were used to create it. And somehow, apparently someday, some atoms will do that instantly. I hope I am alive to see that happen because that would just then - then it's time to figure out, okay, how are atoms doing this? I have no idea how five atoms can factor a number. But, you know, that's what...

Leo: It's very cool.

Steve: It is. Just the idea of that happening is very cool.

Leo: But that's the point, it's kind of a distant, you know, I hope I'm alive when they can do it kind of thing.

Steve: Yeah, yeah, exactly. And I should also mention that the NSA is already getting ready to propose the standard for the next - oh, and in fact that's mentioned in this 47-minute YouTube piece that I hope everybody will listen to or watch. It's just, it's heads, it's talking heads, although they're cool-looking heads. So I would watch it if you can. Otherwise...

Leo: Famous heads.

Steve: They're, yeah, they're - and there's one guy on the end who's like, what, are these hair extensions here? And I don't know what's going on. But, you know, they're - oh, my god. Next week's T-shirt is the best thing I've ever seen. It shows an employed programmer standing next to an unemployed programmer. And then someone sent me another picture of two headshots. And that is these guys. These guys' employment with a university, I mean, their tenure is so deep that they can look like anything they want to, and really they're kind of supposed to.

Leo: Right. You would trust them, yeah.

Steve: Rivest looks normal. And it's like, well, what do you know?

Leo: Yeah, how could you be a wizard?

Steve: Come on, you know? You don't look like a wizard. Exactly. Or like you have hair extensions. So anyway, they mention in there toward the end that the NSA is already proposing the post-quantum algorithm. So they exist. The book, this book is, you know, that's what it's got is discussing post-quantum crypto. And on of these days I'm just going to figure it out. If I ever take a vacation, or maybe when I'm on the plane vibrating my way up to Petaluma...

Leo: There you go. Come visit.

Steve: ...I'll use the time to get in...

Leo: And read the book.

Steve: ...and be able to describe how five atoms are able to factor something because I want to - I'm getting to the point where I need to know, and I know our users want me to explain it. So - our users. Our listeners. Our followers.

Okay. So Verizon is fined $1.35 million. And I look at that, and I don't think I was sipping

coffee, or I might have, like, had to wipe off the screen. Because that's nothing for Verizon. That's like, I mean, they don't even feel it. It's a slap on the wrist. This was a fine that the FCC imposed for their use of supercookies, that we've talked about, which is a completely pernicious privacy-violating technology that they implemented in a way that they were unblockable - thus the superness - unless you used HTTPS.

And this was that, as a Verizon Wireless customer, you are using their gateway, essentially. They're your wireless ISP. So by definition all of your traffic goes through their portal. And any that wasn't encrypted, any browser queries or HTTP queries had a Verizon supercookie added, which was tied to your account, and which we now know they were sharing with others. That is, they were remarketing their tracking of their customers to other parties.

So what annoyed me about the 1.3 million is they made vastly more than that much money doing this. So from their boardroom standpoint, this was a highly profitable venture. You know, 1.35 million is the toll for doing this? Fine, we'll pay it. Can we keep doing it? We'd be happy to pay this every year. Anyway, so they've agreed in their consent agreement to obtain consumer consent before sending data about supercookies under the settlement. And I'm still, it's like, okay, let's wait to see how this comes out because the idea is there's language in there that says users can opt out. Well, does that mean you can change your mind after agreeing? And how do you do that?

And what we really want, and unfortunately it's probably not there, I'm sure it's not there, is a timeout where you have to opt in, and it expires after six months, and then you have to opt in again. I mean, that's the fair way to do it. And who knows? And we've discussed this before. Would Verizon maybe give you a discount on your costs if you opt in? Then a lot of people are going to say yeah, I'd rather have cheaper service, and I don't care about that tracking business. And remember, it's still, until they start forcing a certificate on their users, which is frighteningly likely, they could only do this for nonencrypted traffic.

But anyway, this made the news. A lot of our listeners sent it to me. So I wanted to just comment. It's like, yeah, okay, big deal. You know, again, if this was the cost of doing it, they'd happily do it. They'd happily pay the fine annually because it was no doubt making, you know, they were generating so much revenue from this. And we have yet to see how they're going to implement this. It seems unlikely that there'll be a timeout. And I just hope they make it clear what's going on so people can choose. Again, if they give somebody a $5 discount a month on their service, then certainly a lot of people are going to say yes. And a lot of people are going to say, uh, no thanks.

Leo: The bigger punishment would be if people read this article and go, oh, well, I guess I don't want Verizon to be my cell phone company, and switch.

Steve: Exactly.

Leo: But, you know what, nobody cares. That's my sad realization.

Steve: Exactly. Exactly. Facebook had a little bit of an oops. Really, and this was an interesting hack. And in the details I found myself realizing that Facebook still hadn't gotten it right, which makes it a perfect subject for the podcast, too.

So what happened was that a researcher poking around discovered that he was able to hack anyone's Facebook account for whom he had their phone number or email address. And so the way it works is as follows. There is a page you go to when you forget your password. And it's like "find your account" or something is the title. I went there this morning and looked at it. And it's like, enter your email address or a phone number, which are registered to your account. And it sends you the now-becoming-commonplace six-digit code. I don't know why six. Because Apple's decided to put six digits on its lock screen. All the one-time tokens are all six digits. It's basically, that's enough that somebody can't guess it. And the technology verifying is able to say, you've got it wrong, sorry.

Okay. So what he found was that you were - oh, and so what happens is you enter that. Then it sends the code to your phone through a text message or to email and changes the page waiting for you to enter that six-digit code. So he puts the wrong one in, and it says, "Wrong, try again." He puts the wrong one in, and it says, "Wrong, try again." Puts the wrong one in. It says, "Wrong, try again." Now, at this point I'm thinking, okay.

Leo: It's going to take a while.

Steve: What part of this process do Facebook's users, I mean, do Facebook's engineers not understand? Because this is not supposed to be try a lot...

Leo: Until you find one.

Steve: Until you find one.

Leo: This is not something you forgot. This is something they just gave you.

Steve: Precisely. So I could say, oops, maybe you've made a typo. We'll give you one more try. Then you're going to have to ask for another one. That's the way these work.

Leo: Yeah.

Steve: But Facebook said...

Leo: Keep trying.

Steve: For some bizarre reason their main Facebook site lets you go - and he said 10 to 12. Maybe he wasn't counting because he got bored guessing. But 10 to 12 before it says, sorry, you apparently have a real problem with your code.

Leo: But there's still a million codes; right? I mean, it's not like...

Steve: Correct. And they are blocking you after somewhere between 10 to 12.

Leo: Well, that seems all right. I mean, it's...

Steve: No, Leo, it's wrong. It is a fundamental flaw in their cryptography. You may think I'm being Gibsonian about this.

Leo: Well, tell me why because, to brute-force it, you'd need many, many guesses; right?

Steve: Yes, but this is not...

Leo: Many more than 10.

Steve: This is not the way the code works. The code is sent to you. You enter it. And I could acknowledge being given one if you typed it in carelessly. They would say, sorry, try it again. And if you mistake, then they say, okay, you seem to have a problem with this particular code. Go back, reenter your information. We'll send you another one. That, I mean, my point is the security model is clean, and it's clear. There is no reason you should possibly need 10. You might have a redo, so you get one other try. And then you just ask for another code. That kills that one, and they present - so what I'm saying is this demonstrates - that would demonstrate a proper understanding of the way this is supposed to work.

What Facebook has done, 10? I mean, how can - there's no - it's inexplicable. But, okay. Even so, Facebook.com was blocking after 10 to 12. However, beta.facebook.com and mbasic.beta.facebook.com are two other full copies of Facebook that are the developmental, not-yet-primetime, that had the whole content and no protection. They just...

Leo: You could enter any code, you mean?

Steve: Any code forever, Leo. And since it's an automated submission, in the disclosure this guy showed that it is an HTTP query that is lsd - and I thought that was interesting, I don't know what that stands for - equals AVoywo13&n= and then the six digits [lsd=AVoywo13&n=XXXXXX]. And you can issue those as fast as you want. And there's no limit...

Leo: Hmm.

Steve: ...if you issue them to the beta - yeah, yeah, bad - to the beta.facebook.com. And what that does is, since there's no limit, he at machine speed runs through - and there are a million six-digit codes. So 000000 to 999999.

Leo: So he still has to get the right one. It just doesn't limit you.

Steve: Correct. No limit. And with a - but a million. I mean, so it's going to take a while. But the system is just sitting there [humming]...

Leo: No, try again. No, that's not it.

Steve: Try again.

Leo: Try that, try again.

Steve: Right. And it's automatable.

Leo: It doesn't say "warmer," "colder," does it?

Steve: And since the - he didn't want to - okay, you got...

Leo: You're getting warm. Do it like Mastermind. Two are right, and one is in the right position.

Steve: And this clown who set it to 10 attempts I'm surprised didn't say, okay, you missed one of those digits, but we're going to give you some more tries. Anyway, so he responsibly cracked his own account so that he wasn't cracking anybody else's.

Leo: So he went through - now, the average would be half a million tries; right? I don't know how that works. Is that right? It's one half of the total?

Steve: Yeah, correct, yes. So...

Leo: And getting no clues.

Steve: Right.

Leo: That's a lot of tries.

Steve: He cracked his own account. He told Facebook. They said, "Whoops," and they turned on the limiter, the 10 to 12 invalid attempt limiter from main Facebook. They added it to the beta.facebook.com, and then he disclosed. So nobody, as far as we know, nobody was hacked. But it had, again, if anybody else had found this and knew any

user's email address or phone number - now, that user would have received a notice of a password reset attempt. So they would have received the proper six-digit code, either on their phone or by email. So, but, you know, we get those. Everybody sometimes gets, like, okay, somebody tried to log into your...

Leo: Yeah, I get them all time, yeah. People are always...

Steve: Yeah, exactly. So it's like, okay, fine. And so you just sort of blow it off. But that would have started the hackers' attempt then to brute-force that six-digit code to successfully get your account, at which point he can change your password, has access to your credit card numbers in your payment section of Facebook. And, well, basically full authentication of your identity, able to do everything you could do as a freshly authenticated and reauthenticatable on demand user/owner of that account. So anyway, a little bit of an oops. But also it's like, okay, if they can't get it in two tries, don't keep giving them more chances. Why? Why 10? Just tell them to get another one. That's the way the algorithm should work.

Spoofing. I didn't ask you how many sponsors we have today.

Leo: Just one more.

Steve: Okay. Because I was going to say this would have been a good time to break, but we'll...

Leo: We've got time, yeah, yeah. I'll break after SpinRite; yeah?

Steve: Perfect.

Leo: All right.

Steve: So spoofing a fingerprint got easier. Some researchers at Michigan State University, they're in the department of computer science and engineering, used a very cool hack. You might want to go to this link, Leo. It's Agic.cc/en, Agic.cc/en. This is the Japanese company which sells - and if you click on the hobbyist side, up at the top, those two blocks. They sell the ability to print a circuit board.

Leo: Oh, that's neat.

Steve: Isn't that cool?

Leo: That's neat.

Steve: So they have - and this is something that people are doing. So they have a

special paper which receives a silver, a high silver content ink. So there are a number of ink jet printers which are compatible, and they list those further down that page. You replace its three cartridges with their three cartridges and use their paper. And you can then print working circuits.

Leo: Wow. That is really cool.

Steve: Yeah.

Leo: I love that.

Steve: It is really neat.

Leo: I've got to tell Father Robert. We'll do a Know How with that one. That's awesome.

Steve: Totally makes sense, yeah. Poke some holes through and then run some components through, and you're good to go.

Leo: Wow.

Steve: Unfortunately, it's conductive. Which means it's going to have a variable capacitance just like a fingerprint's ridges do.

Leo: Oh. Oh, dear. Oh, dear.

Steve: So now this is the new way of spoofing fingerprint readers.

Leo: You can inkjet print them.

Steve: Yes. Yes.

Leo: What the what? Wow.

Steve: So you take a picture of somebody's fingerprint, maybe from their own phone, or maybe from the wineglass that you handed them because you wanted to get a clean thumbprint from them.

Leo: Right, right.

Steve: And then you horizontally invert it, clean it up, and then print it at one-to-one size using this inkjet printer with their paper and their ink. This makes a conductive raised-ridges copy of the fingerprint. And it does work. They may not have had an iPhone, but they said they opened a Samsung Galaxy S6 and a Huawei Honor 7 that were both biometrically locked. And it's just easy. The previous hack or spoof that we described back when the fingerprint reader was new came from Germany's Chaos Computer Club. And we'll remember that they did this using a gummi finger which they had 2.5D printed. They had a 2.5D printer and some sort of a gummi stuff. So they created - because they understood they needed 3D-ness. And they may have sprayed it with something to make it conductive afterwards. I don't remember. But now we have an advance of the technology where, yup, you just print a fingerprint. Or you could keep a spare fingerprint in your wallet, if you needed to, like, you know...

Leo: Oh, that's handy. If you lose your hand, you can always just, yeah.

Steve: Yeah. Exactly. Or you need to give it to a relative or something.

Leo: Yeah, here's my fingerprint, yeah, yeah. You can use this.

Steve: Here's my fingerprint.

Leo: Yeah. I've got it in my phone if, yeah, wow.

Steve: Yeah, very cool. Very cool. Okay. McAfee. Oh, boy. You know? And I did, I had to say, I have to say that I was put in mind of Donald Trump because he acknowledged that he lied specifically to generate YouTube traffic, and then boasted 700,000 views of him saying, basically, yeah, I could, you know, they should just give the phone to me. I can unlock it in no time. It's just not going to be a problem. And it's like, okay, John. I mean, as I said, I didn't cover this for the last couple weeks because I was just rolling my eyes. But this is just a wonderful interview that the Daily Dot did.

So McAfee says, or originally he said: "I speak through the press, to the press, and to the general public. For example, last night I was on RT, and I gave a vastly oversimplified" - now, this is John - "a vastly oversimplified explanation of how you would hack into the iPhone. I can't possibly go in and talk about the secure spaces on the A7 chip. I mean, who's going to understand that crap? Nobody. But you've got to believe me: I understand it."

Leo: Oh, yeah, sure.

Steve: "And I do know what I'm doing, else I would not be where I am." And I think...

Leo: Where are you?

Steve: With dogs being shot by neighbors in Bolivia? You know?

Leo: Where are you, yes.

Steve: Yeah, exactly.

Leo: It made me the man I am today.

Steve: Where did we leave off with your escape from South America? Anyway, so he says: "But you've got to believe me. I understand it. And I do know what I'm doing, else I would not be where I am. This is a fact. Someone who does not understand software cannot start a multibillion dollar company." I'm just gagging. And he says: "This is just a fact of life. So if I look like an idiot, it's because I am speaking to idiots."

Leo: Oh, that'll go over well.

Steve: Oh, yeah. "But I promise you this: You get me on a coding table" - and I think...

Leo: Coding table? They make those now?

Steve: What is a coding table? "Get me on a coding table..."

Leo: I want a coding table.

Steve: "...against somebody, I will kick your ass," says John.

Leo: Oh, god. Oh, please.

Steve: Okay. So the interviewer says: "Anything else you'd like to talk about?" And of course McAfee, never one who's shy or short for words, says: "Yeah. If you're on Reddit, tell those guys, cut me a little slack. I am not quite as stupid as they think. I mean, I may be pretty damn stupid, but nowhere near what they think. And if somebody wants to test me, please. Bring a laptop, a coding pencil..."

Leo: Oh, to go with his coding table.

Steve: What is that, one with a big eraser? What is a coding pencil?

Leo: I'm thinking he's never written any code.

Steve: I know he hasn't. "Bring a laptop, a coding pencil, or ask them how to - here's

one. If you have a computer with no memory and only two registers, how do you exchange register A" - and he actually means the contents of register A - "with the contents of register B. And all you have are Boolean operators. Now, you ask them that. How many people can do that within one minute?"

Leo: One minute? It's a timer?

Steve: That's the question - no, no, the coding...

Leo: In their head. Answer your question.

Steve: The coding pencil is going to expire after a minute.

Leo: Yes. After a minute you have - your time is up.

Steve: "That's the question I used to ask everybody who came to work for me at McAfee." Right, because his multibillion dollar company he was still doing the hiring.

Leo: The hiring, yeah, yeah, yeah.

Steve: "If you can't solve that in a minute, you're an idiot. You shouldn't be programming. And I guarantee you that 99% cannot do it. All right?"

Leo: Oh, come on.

Steve: He says: "Two registers, only Boolean operators, no memory, and you must exchange the contents of those two registers. So you don't have adds and subtracts. No, only Boolean - AND, OR, XOR. You got it?"

Leo: Oh, you have XOR, good, all right.

Steve: And so the interviewer says: "I will pass that challenge along." McAfee says, again....

Leo: You're an idiot.

Steve: "And just tell them, the first time somebody asked me that question, I popped out the answer instantly."

Leo: Oh, because he's a genius, with his coding pencil and his coding table.

Steve: Oh, my lord. Yeah.

Leo: But we now know who Mr. Trump will be nominating for vice president, I think.

Steve: And you understand now why I was put in mind of the Donald is it's like, okay, this, you know...

Leo: I'm a genius. They're all idiots.

Steve: In a different venue. Anyway, so of course we discussed this years ago. It even has its own Wikipedia page, this clever, but inefficient, technique. I mean, it's rare that you don't have a swap instruction, or Intel calls it the XCHG, X-C-H-G. But three XOR operations between those two registers can swap their contents.

Leo: Wait a minute, Steve, you didn't use your whole minute.

Steve: I know, sorry.

Leo: But you probably had a faster coding pencil.

Steve: And I would argue that any programmer learns this in 101.

Leo: Oh, yeah. Oh, yeah.

Steve: I mean, in like Boolean math it's like it's a cool thing that you can do this. Anyway, so I just - this was, again, this was typical John. This is why I didn't bother us for the last couple weeks with his shoe challenge because it was just nonsense. But I just love this.

Leo: I hope he eats his shoe now. I really do.

Steve: It's like, wow, yeah.

Leo: That's great.

Steve: Okay. So RSA. I just had a short note to make sure people knew that there was a 47-minute panel conversation. The YouTube link, bit.ly/rsacrypto. I mean, it's riveting.

Absolutely, as I said, first of all, you've got to see these guys. They're just, they're classic crypto people except Rivest, who really needs to be weird somehow. If we could just give him maybe rose-colored glasses or something. But anyway, definitely fun.

Leo: I'm pulling it up right now. I'll show - I'll just let people who are watching the video just...

Steve: Oh, good. Yeah, yeah, yeah, do.

Leo: You talk because, I mean, obviously people, most people are listening. They're not going to see the video. They're going to have to do this for themselves. But let's - I'm just curious what these guys look like now. Now you've got me, you've got me going. Oh, yeah. They look like, oh, whoa, the guy on the right. Whoa.

Steve: That's my guy. That's my guy with the hair.

Leo: Okay.

Steve: Wait till we get a close-up of him. He is really - he's a character.

Leo: Now, who is the elder gentleman who looks like Gandalf?

Steve: That's Whitfield Diffie.

Leo: Whit Diffie, by the way, won the Turing Prize, million dollar Turing Prize. He deserves it. And who is this guy?

Steve: That's Mr. Hair.

Leo: I love it. And he's wearing a pink shirt. It's really interesting. And it looks like a puka shell.

Steve: Classic groove. And we have - that in the middle there is Shamir of RSA.

Leo: Now, Shamir, by the way, just recently said, at RSA no doubt, that Apple should give the FBI anything it wants, which surprised me, since he invented public key crypto.

Steve: He did. And in fact, Whit Diffie was at the AI Lab at Stanford when I was there in college.

Leo: Oh, really. Oh, yeah.

Steve: He had a number of neat...

Leo: I've interviewed Whit, actually.

Steve: He was big on Spacewar. We used to play Spacewar.

Leo: Oh, what fun, huh?

Steve: At 4:00 in the morning, yeah.

Leo: Put that on your MAME. I'm sure this was fascinating. We shouldn't mock people's appearance because of course they're geniuses.

Steve: No, no, they're wonderful.

Leo: We love them.

Steve: I mean, as I said, they're, yeah, they're wonderful.

Leo: Yeah.

Steve: Okay. So Toby tweets me, and actually...

Leo: Oh, that was Moxie Marlinspike.

Steve: Is that Moxie?

Leo: That's Moxie Marlinspike.

Steve: Okay.

Leo: Of course it is. I should have recognized him.

Steve: Yup, yup.

Leo: With a name like Moxie Marlinspike, it's got to be good.

Steve: Once again, yes.

Leo: No hair shaming. Moxie, we love you. Keep up the good work.

Steve: Nice. Okay. So Toby tweeted both of us. He said: "Updated Windows 10 and hating it. What operating system would you recommend? FreeBSD or Linux Mint?"

Leo: Yeah, yeah. I ignored that because it's a complicated answer. Not doable in 140 characters, frankly.

Steve: Precisely not. But for me, anybody can DM me and vice versa came to my rescue, and Toby was following me. So I just thought it was an opportunity. I've been - I'm going to try to figure out what it is about upgrading. And I think the best analogy I have, well, what I think it is, it's not really learned helplessness, it's a domain where we have no expertise. That is, where we cannot form, we don't have an informed opinion.

And the best, I came up with an extreme example to highlight it. And that is, somebody hands you an axe and says, okay, chop down this tree. And so you grab it and swing back, and the person says, oh, whoa, whoa, no no no no no no no. You're holding it wrong. You're supposed to hold the blade and whack the trunk of the tree with the handle. And you'd say, what? And they'd say, yeah, that's how I want you to chop the tree down. And you'd say, well, you're a moron. That's not how an axe is used. And they say, yeah, but I'm telling you, I'm an expert in tree chopping.

Leo: I'm an expert. That's where you've got to watch out.

Steve: This is how you - so, and the key is, you know better. And, see, I run into this now in the medical area all the time because I'm studying research, reading studies, actively, proactively educating myself on tightly focused specific topics. And I end up becoming a small topic expert. And those are the things I've shared with people, like the Vitamin D podcast and the Sugar Hill stuff, digging into the science, understanding it, putting it all together so that it makes sense. And so the problem that most people have is that it's not an axe. It's way more complicated than that. And so they don't know. And so here we come to Windows 10. Same thing.

Leo: It's not an axe.

Steve: It's not an axe. We know what I think it is. I've been [crosstalk] it.

Leo: It's a flying something. Yes.

Steve: So Toby says he hates Windows 10, what should he do? So I tweeted back: "Toby, for the time being I'm staying with Win7. I think it's perfect. It predates Microsoft's switch to OS as an overcommunicating social media service; it will be kept updated until 2020; it runs a recent model IE for talking to Microsoft; it supports all of the latest communications security standards (forward secrecy, TLSv1.2, SHA-256, et cetera). It's available in mature 32- and 64-bit versions, so plenty of RAM expansion space. It's supported by current laptop and desktop hardware. It runs the user with reduced rights, which can be easily and transiently elevated when needed. And, of course, it also manages all peripheral I/O devices, storage, and networking; launches all 32- and 64-bit Windows apps; includes a free built-in VM for running XP and much older 16-bit apps, if needed. It can be easily tweaked to never upgrade to Windows 10. What's not to love, and what more could anyone want or need?"

Leo: Right.

Steve: And so that's my point is there is this sense of need to upgrade because there is something newer. And I remember the love fest that Paul and Mary Jo had over Windows 8, and then 8.1. Now it also is a flying we-know-what, and a horrible mistake that Microsoft should have never made, and they love Windows 10. To me it's like, okay. I'm staying with 7, which absolutely does what I need.

Leo: There you go. And we'll cross the bridge of what the hell to do when it...

Steve: In four years.

Leo: In four years.

Steve: Yeah. And I'm happy to have four years. And you know me. I mean, I'm still using XP. So, and there'll probably be an embedded version that still gets updates until you're on your boat. So...

Leo: And I wouldn't, just to - I should have answered his question. I wouldn't go with Linux Mint at this point, although I have to say it's a shame because it is the most Windows-like version of Linux, and very easy for people to use. But unfortunately they've made some decisions about upgrading that I think are problematic. So I'd go with Ubuntu, I think, is a fine version of Linux to use.

Steve: There's a also a desktop version of FreeBSD which I've looked at a little bit. I don't know how it compares at all, but...

Leo: It's fine. It's good. And of course, as you know, as we know, that's the most secure of all operating systems. I mean, it really, both through obscurity and through design. So that's another good choice, I think.

Steve: Yeah.

Leo: But harder to use, I think, for an end-user, especially somebody coming from Windows.

Steve: Yeah. Again, it's certainly a function of your techno level.

Leo: Yes, exactly.

Steve: I'm with you a thousand percent, Leo, in recommending the Chromebook to people who just need to surf the web and do email.

Leo: That's a great choice, yeah, yeah.

Steve: I downloaded, just because I was curious, another email client which can do IMAP and was able to do GRC's email on the Chromebook. So you certainly aren't constrained to just...

Leo: Is it a plugin? It must be a Chrome plugin; right? What's it called?

Steve: It's like Cloud something.

Leo: Okay. That's good to know.

Steve: But it runs on the Chromebook, and now I have all my email, I mean, I'm not using it seriously because I really do want a strong machine. But I just wanted to verify that, like if somebody got it, and they were a Cox subscriber, that they could set it up to still get their mail through Cox and not have to, for example, do webmail, which Cox does offer. And so, yeah, that works.

Leo: Good.

Steve: Last week we talked briefly about my evolving Healthy Sleep Formula, and you mentioned your success with it. Naturally, a great number of our listeners also cannot sleep well through the night. And the statistics show that about a third of the population, as we get older especially, has a recurring significant problem, enough so that they say, yes, I can't sleep. So it wasn't a deluge because people were waiting. But I got a lot of DMs and just regular public tweets saying, you know, "Pssst, I really need it. Can you just, I know it's not done, but can you share it?"

So there is a page that I threw together, but you no longer even need a URL because it's gotten loose. And I wanted somebody other than me to google this to see if it's the first link for non-me because we know that Google tends to bias itself. So if you google "healthy sleep formula," Leo, what's the first thing that comes up?

Leo: No word of Gibson in it, just "healthy sleep formula."

Steve: Mm-hmm.

Leo: GRC Healthy Sleep Formula, number one.

Steve: Okay.

Leo: Number one on the hit parade. So it's easy to find.

Steve: Easy to find.

Leo: And now you have to add Taurine to this, though.

Steve: It's on the page. I didn't put it up in the top six, but you'll see that second box there says, "And get yourself some Taurine."

Leo: Now, it would behoove me at this point to say Steve is not a doctor, and you should always, before taking a supplement, consult your physician to make sure it doesn't interact with your own medications dangerously because that's always a possibility.

Steve: Yes.

Leo: So don't just blithely go out there. However, I have taken it, and it has made a big difference. Now, I'm hoping it's not addictive, and I'm not going to get cancer in six months. But I trust Steve. If you don't know Steve as well as I do, you might want to consider that this is just one guy's thing. Okay. Now I've said the disclaimer.

Steve: Yes, thank you.

Leo: It works for me. Yeah.

Steve: Thank you. And I've already had reports of it working...

Leo: It's amazing.

Steve: Yes. I've never had a report yet of it not working.

Leo: Well, when we all get cancer in a year, maybe. But, you know, right now it's good.

Steve: Well, none of this stuff is weird. It's all either in us, or it's the main amino acid in green tea. The L-theanine is the predominant amino acid in green tea.

Leo: And you're recommending around 200 milligrams. Is that kind of comparable to a few cups of tea, or a million cups of tea, or...

Steve: You have to drink, oh...

Leo: Not an unreasonable amount, I would guess.

Steve: No, no, it's not. And this is a standard offered supplement level.

Leo: Yeah, you're getting these from Now for three of them, which is a well-known...

Steve: And they're a great company. So GABA is the existing neurotransmitter that we already have in us. Glycine, same thing, is a neurotransmitter and the smallest amino acid. So it's in our diet, and it's all in us already. Melatonin is the hormone which our pineal gland secretes at night and when there's a lack of blue light.

Leo: By the way, you're number two in Germany, according to Martin.

Steve: Cool. And the first ingredient, Seriphos, is a version of phosphatidylserine, which is...

Leo: Oh, you had me taking that before.

Steve: Yes, exactly. What it does is it sensitizes and actually recovers the sensitivity of the cortisol sensors that the hypothalamus and the pituitary both use to determine whether their request for cortisol to be released has been met by our adrenal glands. And so there's a negative feedback loop such that, when cortisol is released, the hypothalamus stops releasing, well, it's an adrenocorticotropic hormone. And that goes to the adrenal gland, which releases corticotropic releasing hormone, which then goes to the adrenal glands and causes them to release cortisol. When they sense that cortisol is available, then they down-regulate their request for more. So it's a negative feedback loop.

The problem is, as we age, that cortisol sensing becomes less sensitive. So the hypothalamus and the pituitary sense less cortisol, therefore asking for more than we really need. So what phosphatidylserine does is, among other things, it brings the sensitivity of those receptors back up. It improves their sensitivity, thus cortisol is

reduced. That's why I had you taking it, because cortisol is a problem for a big chunk of the population because of just chronic stress. It's in the Healthy Sleep Formula because it's also a problem at night for people not being able to get to sleep or waking up too early.

So all of these have a specific reason. And in fact it turns out that phosphatidylserine and GABA are synergistic, and it helps GABA to cross the blood-brain barrier, which is one of the reasons people don't think that supplementing with GABA actually works. Anyway, I do, at the bottom of that page, explain the first of those five. I haven't had time to get to Taurine yet. But it's going to get added. So anyway...

Leo: And this is how much? Because I didn't pay for any of this, I just got it in the box. It came to me, magically.

Steve: Yeah, and in fact that's a very good point. I show the prices of Amazon's. But I also note, someone told me that in the U.K., I think it was, or no, it was in Canada, he said that the Seriphos was, like, 50-some dollars.

Leo: Whoa.

Steve: And I said, whoa. So I checked ca.iherb.com, and it's the normal price there.

Leo: Of course, as soon as people find out about this, it's all going to double because, if it really does what you say it does, it's worth whatever that is, five bucks - how much a night is it, roughly?

Steve: I haven't done the math. I will.

Leo: Get a spreadsheet out to do that.

Steve: Well, and again, people need to understand, at the top of the page I say this is a beta at this point. I reserve the right, I need to still play with it a little bit. And it's slow going because, like, I'll take something out, and I'll wake up at 4:00 a.m. And it's like, gosh darn it.

Leo: It takes a whole night to try each one.

Steve: Well, worse than that, the next night you can't count on because you had a bad night the night before so there's sleep pressure. So it basically takes several nights, like three nights to recover from taking one out, and then it destroys the whole - the way the thing fits together. But I've been, as I said, I've been putting it together. It is all, every single thing is innate to us in reasonable concentrations. And in fact, again, what I'll end up doing when I get time is each one of those will get its own page because, for example, Taurine - and I should just mention that Taurine can lower your blood pressure. So if you're on high blood pressure medication, you want to make sure you don't

undershoot.

Leo: Yes. This is why you want to consult your physician.

Steve: Precisely.

Leo: Because there's interactions with all this stuff.

Steve: Precisely. And so I will spell those things out so that people can know. Also, this particular melatonin is time-release, which is crucial for this.

Leo: Because it's a lower dose than, I mean, it was only one milligram.

Steve: It is, yes. And, see, that's the point. People make the mistake of blasting themselves with 20 milligrams of melatonin, which is vastly more than ever occurs biologically. And so the secret is trickling it out over the course of the night. The problem is this adds B6, and some people have a B6 sensitivity. So one of the things I'm doing now is I want to experiment. There are a couple other time-release melatonins without B6. In fact, Life Extension brand is a 300 microgram time-release that I'm going to switch to. It wasn't working for me before the Taurine; but with the Taurine, this has really strengthened the whole thing.

So I want to see if I can adjust the melatonin down and still have it work, and thus get rid of the B6. B6 is an important factor in neurotransmitter synthesis. You have to have it for some of the enzyme actions, for example, the one that - actually it's called Decarboxylase - that converts the 5-HTP to serotonin. We want that to happen. And so the reason they put B6 in is it generally helps generating the calming neurotransmitters.

But anyway, I have all the science behind this. I've got tons of research. I just haven't had a chance to make it public. But, you know, you're playing with it. A bunch of people are playing with it. I've already had positive results. Someone was sensitive to the melatonin, dropped it, and didn't need it. So it may also be the case that you can go without melatonin. I'll get all this documented. But I just want to let people know it is there, if you want to get it and start experimenting, understanding that it's an experiment.

Leo: Both Lisa and I were a little groggy the next morning, and have been a little bit, but not badly so.

Steve: When you took two of each; right?

Leo: Yeah, well, even last night I took one. But as you point out, it takes a couple of tries to really know what the effect is. But nothing that a cup of coffee and a good bike ride didn't fix. But it just, you know...

Steve: Well, and the other thing, too, is one of the things that I experienced at the beginning of this was sort of that same sense of feeling. And I began to wonder whether it's that I was just...

Leo: Finally getting a good night's sleep.

Steve: Yes. I was really relaxed.

Leo: Kind of euphoric.

Steve: Exactly. I felt a little - in fact, I said to the gal that serves me for lunch, I said, "I think I'm kind of high right now," because I was also doing Taurine and glycine in the morning. And those, after a good night's sleep, it'll give you kind of a nice little buzz.

Leo: Well, and there are lots of reasons to think that a good night's sleep is healthful.

Steve: Oh, that's the other thing.

Leo: Very necessary to health, yeah.

Steve: That's the other thing we haven't talked about. But, oh, my lord, it is unbelievably important. I mean, one of the things that's happened since the '50s is, since the 1950s, the amount of self-reported sleep has dropped by between one and a half and two hours per night. People are staying up later, and they're getting up earlier. And I've heard people, like on television, bragging about how little they need.

Leo: I only need two hours' sleep, yeah.

Steve: It's like, this is not a bragging point.

Leo: Not a good thing.

Steve: You know, it's really - our bodies...

Leo: John McAfee sleeps 20 minutes a day.

Steve: And boy, does it show.

Leo: Look how smart he is.

Steve: Yeah, boy.

Leo: Well, again, I just, you know, it always makes me a little uncomfortable to recommend anything. But all the standard disclaimers apply. But I think, if you find something, I think this is great. I mean, at this point I actually don't not take it because the times I have, I haven't slept well. And it's like...

Steve: And I look forward, I look forward to going to sleep.

Leo: Yeah. I sleep very well, yeah.

Steve: Now, there'll be one more addition, or an optional. And that is, if you like dreaming, there's an herb called Rhodiola rosea. And it's not in there because that was like...

Leo: It makes you dream.

Steve: Oh, my lord. And in fact, this kind of vivid dreaming, you never get into as deep a sleep as I think people should. But I know there are people who, like, occasionally would just want to - it's like eight hours of entertainment. It's like the craziest - it's just the craziest stuff that has ever happened. It's just wonderful.

Leo: I'll try that.

Steve: So anyway, we'll have some fun.

Leo: You know, that first sleep suggestion you made for me, way back when, when I think I was worried about jetlag on a long trip, did cause me to dream a lot.

Steve: Yes. In fact, what I did, that was all - that was the - you had to go to sleep super early for New Year's Eve...

Leo: Right. Oh, that was New Year's Eve, that's right, yeah.

Steve: ...before last. So we had to knock you out so that you'd be able to go to sleep at, like...

Leo: Right. And it worked, yeah.

Steve: ...6:00 or something, yeah. And it was 5-HTP and melatonin. And those two things, and you were able to get them from the local drugstore.

Leo: Yeah, still have them.

Steve: Yes, and 5-HTP is a potent serotonin generator. It's the immediate precursor to serotonin. Tryptophan has a hard time crossing the blood-brain barrier, but 5-HTP doesn't. It's able to get through, through passive diffusion. And so, if you've got enough B6, it just gets converted to serotonin. And, oh, boy, will you dream.

Leo: But you don't dream much with this current formulation.

Steve: No.

Leo: Not till you're kind of starting to wake up.

Steve: For example, yes, exactly. And for example, you don't see L-tryptophan there that you would expect to see, or 5-HTP, specifically because I don't want to encourage too much serotonin. It's just it's a little distracting. I mean, in fact, I'm wearing my little Zeo headband, and it's saying I'm asleep, and I'm thinking, I don't feel asleep. I feel like I'm...

Leo: I'm wide awake, yeah, oh, yeah.

Steve: I mean, and I'm not a big dreamer, and I'm not one who remembers his dreams. But I've got some, like, storylines that would freak Jenny out if I ever told them to her.

Leo: See, I'm kind of, yeah, I had some very good dreams, too. So I want to, I definitely want to try that once in a while. All right. So what is that for the dreaming?

Steve: Rhodiola.

Leo: Rhodiola.

Steve: Rosea. Also from Now foods, R-H-O-D-I-O-L-A. Rhodiola rosea, R-O-S-E-A.

Leo: All right. Sweet dreams, everyone. Good luck.

Steve: And, yeah. What it acts, the way that - its mechanism of action - and one of the things we're going to do when we have some time to do a special is I'm going to just do a podcast on the neurobiology of our brain because I've had to learn it in order to understand how all of this stuff works. And it is so fascinating, and I know it would produce a podcast that even people who didn't care would just find really interesting.

But one of the ways that the neural signaling system works, neurotransmitters work is, after emitting this chemical, the neurotransmitter chemical, it's necessary to end the stimulation. It's meant to be an event, not a haze. And so the stimulating neuron has an "active transport," it's called, which is like little vacuum cleaners which try to suck those back in so that it recycles them because it's metabolically more efficient to recycle than to have to...

Leo: Reuptake.

Steve: ...reuptake, exactly, rather than rebuilding an all new neurotransmitter. But because it's goo, I mean, it's sort of an aqueous environment, some of them may wander off. And you don't want sort of a cloud gathering over time because that would be bad. So our biochemistry also has enzymes which actively break down the neurotransmitters that have gotten away, that have sort of become lost. And those are called monoamine oxidase enzymes because they oxidize the monoamine, which is what the neurotransmitter is. Thus a monoamine oxidase inhibitor, an MAOI, that was the original form of antidepressant medication.

Leo: Right, right.

Steve: And so it worked by inhibiting the destruction of those neurotransmitters that had sort of wandered off and allowed them to sort of increase their effect over time. Rhodiola rosea is a mild MAOI. And so it tends to inhibit, I think it's MAOI A and B, which are the monoamine oxidase inhibitors for both serotonin, and I think it's glycine. And I think acetylcholine, also. So anyway, this will all get written down, and we'll have a fun podcast sometime talking about it.

Leo: All right.

Steve: In the meantime, Jeff in Ontario, Canada wrote with a subject "Not a Security Question." And I happened to find this in the mailbag, thought I would share it, just because there is a little bit of a takeaway from this for our listeners. He said: "Hi, Steve. I have a WD My Passport 1TB portable USB hard drive. I had bought a copy of SpinRite some time ago to support you and your podcast, which I thoroughly enjoy every week. I partitioned the aforementioned portable hard disk drive with three primary partitions and a bunch of logical partitions. I made the drive bootable and installed a bootloader. The drive held a number of useful PC diagnostic, maintenance, and repair tools, including SpinRite, some live Linux distros, Memtest, et cetera.

"A few weeks ago I clumsily dropped my portable HDD. It fell from about waist height. A few days later I noticed I was unable to save some files to the drive from a Linux machine. The OS was showing me I/O errors. I was also unable to copy some large (over 2GB) files from the drive to my Windows 7 laptop. The Windows copy dialog was getting

stuck and claiming an ETA of a couple of decades. I plugged the hard drive..."

Leo: Never seen that. That's good.

Steve: Yeah. "I plugged the hard drive into a spare workstation at work and booted SpinRite from the drive's first partition. I then sent SpinRite to work on all the partitions of the same drive. I'm not sure if it's a good idea to have SpinRite test the same media it booted from? It is plugged in by USB, not SATA. Do you think SpinRite can breathe new life into a hard drive that has suffered physical trauma, i.e., has been dropped? It did not hold any data that wasn't backed up, so I'm not concerned with data recovery. But I'd love to have the drive working again. Maybe I'll just get one of those shockproof portable HDDs, those with the rubber bumpers."

Leo: I use SSDs, which I think are more...

Steve: That's a very good point. They're shockproof; and, as we have found, they are subject to SpinRite's machinations in recovering when they need recovery. So that would make a lot of sense. For what it's worth, the good news is it sounds like the drive wasn't running at the time, so that's better, although it does sound like the physical drop hurt it. SpinRite has a long history, from the laptop fell off the back of the couch to my dog ran by and knocked the computer over and such stories of machines where the drives were running, the heads were flying, and they got bounced on the media, SpinRite came along and recovered the data and fixed them, and things were good to go again.

So, first, it absolutely can help with physically damaged drives because that's really what sector errors are. That's physical defects that are causing the magnetic flux reversals not to be recoverable on the drive. And secondly, it's absolutely fine to run it on itself. Since it boots, it comes in, it runs, it no longer has any connection or open files or ties back to that drive. So absolutely. In fact, back when it was running from a floppy, boy, I put in a bunch of logic so that it could write its log file of what it did back to the media that it was operating on, even if at the same time it needed to be relocating the sectors and the clusters that the log file was being written to. I made it all work somehow. So absolutely it is safe to run it from the media it was booted from.

And once we get back from the break, I'm going to talk about a, like, okay, you've got to be kidding me, there's still some way to eke out a private key from a system whose code plays by all the rules. Yes, one more bleed. We had Heartbleed; now we have CacheBleed.

Leo: No relation to Cachefly, our fine content distribution network. All right, let's talk CacheBleed with Steve Gibson.

Steve: Yeah, and I'm seeing them advertising on major networks now, too.

Leo: They're everywhere. They're everywhere now. It's a huge success story. It's really great. And we're really happy to be part of that, I think.

Steve: Okay. CacheBleed. The well-understood rules for avoiding or preventing side-channel attacks of any kind depend upon, well, where the attacks depend upon a secret-based alteration to the code path. We've talked about this before, the idea being that any encryption or decryption is, by its nature, is using an algorithm which is typically a standard. And it is a keyed algorithm where the key provides the secret that specifies the details of how the algorithm scrambles the bits, or unscrambles the bits, going in and coming out. And the idea is that, by looking at the bits on both sides, you gain no useful information about the key. And the key itself has enough bits that it's impractical to try all the combinations of bits. So you've got a strong system.

What we don't want is the use, the dynamic use of this algorithm to leak any information about the key's bits. That would be bad. And so the example we've discussed, where this is done wrongly, is if you ever have a branch which branches the code based on bits of the key, then the act of branching changes the timing and the power consumption enough that somebody on the outside can detect it. And whereas once upon a time people would have said, "Yeah, so what, I mean, you can't use that," boy, you give these academicians a challenge, and they will wrestle it to the floor. And so now all kinds of attacks have been demonstrated, and we discussed one just last week or the week before, like through a wall, magnetic emanations of something decrypting PGP was able to obtain the private key from just listening to the magnetic output from a standard laptop sitting on the other side of the wall. So it's like, yes, this stuff has been reduced to nearly practical level.

So the OpenSSL guys are aware of this. And they have used only fixed-time instructions where the instructions' arguments depend upon secret key data so that there's no variation. And no conditional branching is done that depends upon secret data. But there's a third rule which has been - people have been aware of it, but it hasn't ever - it's one of those things where, again, there just wasn't any, didn't seem to be a practical way of taking advantage of it. The third rule is do not use memory access patterns that depend upon secret key data. Now, this is interesting and becomes a little tougher, maybe, not to have the memory access patterns, not even memory access depend upon secret key data.

So it turns out that crypto algorithms, which exist today, which are side-channel attack proof, explicitly made so, even though in some cases they're slowed down because they can't use, like if they could use the secret key they could have that, direct branches, they could make it so much faster. But no, can't do that. So they've had to slow the algorithms down, deoptimize them in terms of speed in order to optimize a different characteristic, which is absolutely no variation based on the secret, that is, variation in the instructions which are executed. Turns out that people have worried about variations in the data which is fetched. And thus it's been, they have found a way to do this.

And the way, the good news is it is much more invasive than any kind of a receiver nearby sniffing something because, again, this has been understood to be a problem, but no one has been able to see, like, how to actually leverage it. For example, the data that is being fetched is probably not something you can detect at a distance. So, yes, we've seen that the instructions you execute can, variations in those can be detected. But, eh, you know, you've got three levels of caching that's going to blur things.

The architecture of today's systems are, for example, in an Intel multicore processor you have some number of cores. We'll just say four for the sake of argument because that's kind of middle of the road now. They go up to eight, I think, or maybe two. So you'll have a core. The cores are hyperthreaded, meaning that they have essentially two program counters, which means that that core, that processor can have two threads of execution actually running through it at the same time. And in the old days you just had

one. You had a program counter, and it specified the address from which the next instruction would be fetched. And a jump instruction changed the value of the program counter, thus causing the next instruction which would be fetched to be something else, not just moving linearly forward, which is what the program counter, thus the name "counter," does by default.

So these new cores have two threads because that's found to be - it's inexpensive for Intel to put a second program counter in, in terms of chip real estate. Doesn't make the chip much bigger. And although it's not nearly as good as a second whole core, it's enough better than only one program counter for the cost that it's now what all the Intel processors do. They're all hyperthreaded because it just makes sense.

So the Level 1 cache is the cache nearest to those cores. And they're small. And there's a separate instruction cache and data cache, meaning that fetches for data are asked of the data cache, the L1 data cache, and fetches for instructions are asked for from the small instruction cache. So there are separate instruction and data caches. And so, for example, if you were executing in a tight loop, then the instructions you had just recently executed would still be in the instruction cache, and so you wouldn't have to go any further outside the core, or even to the Level 2 cache in the core in order to get those instructions. But instruction and data is separate.

So also part of the core is the next stage, the Level 2 cache, which is significantly larger and is a shared cache. Instructions and data both share the same cache. And then outside of all the cores is the L3, the Level 3 cache, which is still bigger again, maybe a couple megabytes on the newer, larger processors. So all of that is on one Intel chip, is the Level 3 cache, which is the main buffer for all of the external RAM on the system's motherboard. And then that big Level 3 cache feeds all of the individual core's Level 2 caches, which then in turn feed each core's split Level 1 instruction and data caches.

Okay. So what these guys figured out was that they could target software which does violate this third law, this third rule of not allowing memory access patterns to be a function of the secret key. I don't know if we're going to be able to harden our crypto code against that because that's a high bar. But I imagine some people will start trying.

What they found, what they were able to leverage is known as a cache bank conflict. So to facilitate access to the cache, that is, the Level 1 cache, and to allow concurrent access to the Level 1 cache, remember we've got two threads running in a single core, and those two threads share the Level 1 cache. So to allow concurrent access to that Level 1 cache, the cache is divided into multiple banks. And in the processor that these researchers tested, there were 16 banks of, I think they were four bytes wide.

So 16 banks of - although I don't know how many lines in the cache, so they may be larger. But 16 banks. And the idea being that one thread - what dividing the L1 cache into 16 banks does is, as you would imagine, it reduces the conflicts. That is, if they were one bank, then essentially the threads would have to alternate for access to the Level 1 cache because they would always be wanting instructions and data from the Level 1 cache. It's the closest one to them. If they break them up into 16, then the probability of a collision, that is, both of the hyperthreads simultaneously asking for something in the same cache is 1/16 of the time. Most of the time, 15/16 of the time, assuming random fetching patterns, they will not be colliding.

Okay. But if they collide with that 1/16 probability, one of the threads stalls. And that can be detected. And it turns out it can be detected by the thread that got stalled. So this is why this is not a huge, run around screaming, hair-on-fire problem. Essentially you are running this malware or probeware, whatever you want to call it. This is not a passive

attack by any means. You're not sniffing anything. In one of the hyperthreads you are running something that is timing itself like crazy.

And a long time ago, when I talked about harvesting entropy [SN-456], I talked about the exquisite granularity of detail that the Intel processors provide to the code running in them. This is an amazing amount of sort of management housekeeping counters that just count everything, you know, branches taken, branches not taken, roads less traveled, predictions that were correct and mispredictions, just an amazing amount of stuff. And I suck all that in, for example, in SQRL's client because it's completely unpredictable and just crazy full of entropy.

So the one thread running in one side of a core is able to time itself and to detect when its accesses have been stalled by the other hyperthread running in the same core. And it turns out that, because the data fetches, even though instruction fetches are not altered, data fetches are altered based on the key data. That thread sharing that core is actually able to, and they have done it, determine the secret key, which is when it is used by the other hyperthread in the shared core based on minute stalls of the attacking hyperthread, when it can't get to its instruction or data cache with the same speed it would expect to. And so it's like, oh, wow.

Again, not a problem at a distance. Not a passive attack. We have seen problems where systems of multicores hosting virtualized OSes, where you can breach the virtualization barrier because they are running on the same processor, even if they're in virtualized, separate, and completely independent address spaces, it is possible to actively breach that, if you have a hostile agent in one, you know, like anywhere in the server that is able to sense tiny changes because they are sharing processors. Here we are running an exquisitely sensitive, purpose-designed code on one hyperthread and detecting its little fluctuations and determining what the key was that was being used at the time it was being used by the other thread on the same core. So it's like, okay. We don't have to worry about this. Maybe the OpenSSL guys are going to worry about it. I don't know if they're going to worry about it or not.

But it'll be interesting to see if mitigations are developed for this, or if people just think, okay, at some point we've got to stop worrying about how close the attacker can be before they're just in here with us in the same process, reading this stuff directly. I mean, this is almost that level of difficult to perpetrate. And, I mean, they have to thread lock, they have to hyperthread lock their process. They have to set thread affinity and processor and hyperthread affinity in order to always be executing on the same core and the same hyperthread on the same core, and then account for other interruptions and things. I mean, they did pull it off. But they pulled it off by deliberately running on the same hyperthread. And I'm not sure whether a processor will run, will share hyperthreads cross-OS.

Leo: Kind of seems unlikely; right?

Steve: It does seem unlikely. So you might not ever be in a situation. It might be that you could have threads in the same process sharing a core. But maybe not even cross-process, let alone cross-VM. So probably hard to make work. But, wow, again...

Leo: It's great, a pretty neat thing to do.

Steve: ...a neat, neat, tech-y, academic example of, yes, we can still get your key, no matter. Even though you played by all the rules everyone does now, we broke the last one. It's like, oh.

Leo: It seems similar to factoring 15 using four atoms.

Steve: Yeah.

Leo: Seems in that vein.

Steve: It's down there. It's like where...

Leo: It's good work, you know. Nice. Wow.

Steve: Yeah. Yeah. And it got a really nice paper written. And we'll keep our eye out for...

Leo: Well, I'm glad you talked about it because I saw that, and I was very curious, well, how practical is this? Is this, you know, and obviously it's highly impractical.

Steve: Yeah. This is not - unlike Heartbleed, where the whole world came to a screeching halt. And remember all the certificate revocation. In fact, it was that, it was Heartbleed and the revocation storm which Chrome didn't honor that caused me to do the revoked.grc.com site because it was like, hey, you know, there's all these now likely revoked or likely hacked sites that Chrome still is happy to honor. So there's our podcast.

Leo: Well, we've all learned something here today, I'll tell you. And this was better than GABA and Seriphos combined.

Steve: I was going to say, if that didn't put you to sleep...

Leo: No, no.

Steve: Then we do have...

Leo: See, I find that stuff fascinating. It's awesome. Steve Gibson is at GRC.com. That's where you'll go to find all of his fine works. Of course, start with SpinRite, the world's best hard drive maintenance and recovery utility. But go from there to, oh, so many things, including now the sleep formula, Gibson's Healthy Sleep Formula, patent pending. By the way, did you notice I have an Echo sitting right here? See that? I'm ready to ask it any questions that come up.

Steve: Nice.

Leo: You can also, while you're there, get a copy of, well, let's see, SQRL, getting close, getting close.

Steve: Close.

Leo: There's forums there.

Steve: In fact, I worked on it so much yesterday that I stole all the time I normally spend prepping for the podcast. So I did wake - I woke myself up with an alarm, which I don't normally do, because I just - I needed to get this done. And we did put together a nice podcast.

Leo: Thank you.

Steve: So I'm happy for that.

Leo: And people sometimes say, "Leo, if you'd just get out of Steve's way, we could get SpinRite 6 going, or 6.1, and we could" - I feel bad. I feel guilty.

Steve: No, it's not your fault. For example, someone said, "Steve, I heard you and Leo talking about your sleep formula. And I know I desperately want SQRL, and I desperately need SpinRite 6.1, but I absolutely cannot sleep. So even though I need everything else you're working on, I know how busy you are, please, please, please can't you tell me what the formula is."

Leo: That's the beauty of Steve Gibson.

Steve: And it's like, well, okay, yeah.

Leo: Everything he does is useful.

Steve: And now I'm getting back to, well, I'll have SpinRite - I'll have SpinRite. I'll have SQRL - I'm back to SQRL fulltime.

Leo: Good.

Steve: And we'll push that out, and then back to 6.1.

Leo: Nice. You can also get the podcast there, of course, GRC.com. And he has 16Kb versions, 64Kb versions of the audio; transcripts that are excellent and very useful. If you like to read along while Steve talks, it's a great way to kind of enhance your understanding of it. GRC.com. We have 64Kb audio, and we even have video at our site, TWiT.tv/sn. And let's see, what else? Oh, we do the show on Tuesdays, 1:30 Pacific, 4:30 Eastern time. I guess next week will probably be a Q&A, so you might want to go to GRC.com/feedback, if you have a question.

Steve: Actually, no, I think I'm going to push it off by one.

Leo: Okay. Okay. Well, you can still ask a question, it just may not get answered right away.

Steve: Maybe. Yeah, my plan was to do DROWN next week.

Leo: Oh, yeah.

Steve: But I may, I think we'll see. And I should mention also the bottom of the Healthy Sleep Formula has a feedback link specifically for the Healthy Sleep Formula. So I wanted just to put that out to people if they've got, I mean, to tell me how they're doing, what they find, what they discover.

Leo: So you'd like reports on how people are doing with this.

Steve: Oh, yeah, yeah, yeah. It is definitely a community endeavor because at this point it works for me, it works for you.

Leo: Yeah.

Steve: I guess for Lisa, and a bunch of people who have responded and reported. But it needs to mature over time.

Leo: Yeah, absolutely. So GRC.com. And we'll be back here next Tuesday for another episode. By the way, Steve's on Twitter: @SGgrc. He accepts DMs from anybody, but you can also tweet at him if you want to have a public conversation: @SGgrc.

Steve: And as you said, GRC.com/feedback for next week's Q&A.

Leo: If we do one.

Steve: If we do one.

Leo: For Q&A at some point.

Steve: Hey, it'll go in the mailbag, and I will see it, if not next week, then the week after.

Leo: Absolutely. Hey, thanks, Steve, always a pleasure. See you next time.

Steve: Thanks, Leo.