SECURITY NOW!

Transcript of Episode #277

Listener Feedback #106

Description: Before plowing into this week's Q&A content, Steve and Leo catch up with the industry's security and privacy related news. Steve shares a vitamin D researcher's reaction to a troubling new report about vitamin D, and shares his recent science fiction reading discoveries and opinions.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-277.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-277-lq.mp3

Leo Laporte: It's time for Security Now!, a wide-ranging episode, this 277th. Steve's going to talk about his favorite sci-fi novels; a little response to a New York Times article about Vitamin D; and, of course, your questions and answers, including the Firefox Add-on Tip of the Day. It's all coming up with Security Now!.

It's time for Security Now!, the show that protects you and your loved ones on the Interwebs. Here he is, the star of Security Now!, the man, the myth, the legend - I love saying that.

Steve Gibson: You're now making me self-conscious about the myth part.

Leo: Steve Gibson.

Steve: Ah, yes.

Leo: There are myths about you.

Steve: We'll do a little mythology over the Christmas break. We'll have a mythological episode.

Leo: Yeah, we should tell everybody that. For the first time ever, I've convinced Steve to take a week off. First, it'll be - you don't have to, if you really don't want to. But everybody else is going to be gone the week after Christmas. But, no, we can get somebody in here.

Steve: Hello, hello.

Leo: We'll just turn on a camera and let you do the show. But since you have this great episode that's so appropriate, I think it's going to end up being kind of our Christmas goose, you know, where...

Steve: Does make sense. And there is some churn in our listeners, so there are certainly people hearing this podcast that are going, "The portable dog killer? What the hell are they talking about?"

Leo: Although the notion of a rerun in podcasts is a trifle ridiculous.

Steve: Leo, you are a pioneer. If anything can be said of you, it's that you are a pioneer.

Leo: I am a pioneer.

Steve: Pioneered the podcast rerun.

Leo: Yes, my wagon wheel hath broken. Let us - what are we doing today? We're doing a Q&A; are we not?

Steve: We have a Q&A. This is a broad-spectrum Q&A. I remember saying yesterday - it just feels like yesterday - last week that I imagined that our Q&A would be focusing on DNS. I don't think one of them was about DNS.

Leo: Oh, isn't that funny.

Steve: Because we had done the prior two podcasts about, first, the GRC DNS Benchmark, and then the Spoofability Test. And I thought, oh, well, we'll do a bunch of Q&A about that. But I just started, I found so many interesting questions and so much to talk about this week that I didn't get around to that. So no DNS. Well, actually there was one question, but it only tangentially rates DNS. It's more about the nightmare of routing on the Internet.

So, but I got a ton of people, listeners, and twits and tweets and everything happened because there was a report on Vitamin D that was on the front page of The New York Times, The Wall Street Journal. NPR covered it. Local radio. People at Starbucks this morning were asking me. And so I wanted to talk about that a little bit because it was a very bad, bad report that came out. And we've got some news. And a number of people have asked for a sci-fi update, like what I've been reading lately. So I thought I'd...

Leo: Oh, good. Always like that.

Steve: ...update people on that. So we've got tons of fun stuff to talk about. I think a great podcast for everybody.

Leo: And just a word of warning. I just saw a twitter that Denise Howell, who hosts our This Week in Law program, is listening. She says, "I must be the first Security Now! listener to ever listen in a kindergarten classroom." I don't think that's true, but I'm glad you're listening, Denise. So, Steve, let's start with our security updates. Are there any?

Steve: Well, we don't actually have any security updates.

Leo: Really? What?

Steve: We had another slow week. However, I did note that Adobe has updated their v10 of Flash, not patching security problems, but reportedly working to essentially lower its power consumption. It's interesting. So they're at 10.2 now. And it was maybe like last week I was at a Starbucks, operating on batteries, I think with a PC, and I don't remember now what it was. Something Flash was going on, and I have my battery meter set so that it's showing me how much remaining time it estimates I have. And that's something where it's looking at the history of the battery use. It's dynamically measuring the current that the whole system is pulling from the battery and extrapolating based on the current current draw, if things stayed the way they are now, how long would that last? Sort of the same way SpinRite estimates how long it's going to take to get done. Which, you know, it's the best you can do, even though it can be fooled.

So, for example, if I turn the screen brightness way up, and I wait a few seconds, I'll see that it's like, oh, that seems to be big, you know, it's drawing a lot of power. And suddenly my battery is projected to last a lot less long as opposed to turning the screen brightness down. Well, what I noticed was when Flash was doing whatever it was doing - I don't think I was watching a video. I think it was some other application was jumping around. It seriously dropped the performance, the battery life of my system.

So this is what we've heard. It's what Jobs was complaining about. His justification for not putting Flash on the iPad was that it was just a hog in terms of performance. And, I mean, the fact that just video movement is drawing so much power tells us, well, tells me as an engineer the degree to which there has been a huge effort already in minimizing power consumption. That is, if changing stuff on the screen makes that big a difference as opposed to having your screen static - in fact, I then played around with just, like, scrolling. And sure enough, if I was scrolling all the time, I could see an impact on my battery life compared to not.

So our systems have become so sensitive to anything going on, in order to get the battery life that we want and that they claim - in fact, that's one of the reasons that, when people were benchmarking the iPad after its release, the iPad was claimed to have a battery of 12-plus hours. People played videos on them for that long to see, if you kept it alive and kept it busy, how long the battery lasted.

So anyway, it's good news that Adobe is sensitive to this. Our listeners may remember that with v10 they were beginning to not do all of their video rendering in software, but they were going to be tied more directly to the hardware. Which of course makes it bigger still. But given that you've got some hardware that Flash can sink its teeth into and hook into, the potential is that you would be able to see less power consumption hit with Flash doing what it's doing. So it's a good thing that they're moving forward. I think I might still be on 9 and haven't moved to 10. So it's probably worth doing that and see if I see an improvement. So that's changed.

We do have some news. Not surprisingly, Windows is in trouble once again. Just a few days ago news came out of a privilege escalation zero-day vulnerability, meaning that malware was found in the wild that was using a hitherto - hitherto? Is that right?

Leo: Yeah, hitherto.

Steve: Hitherto.

Leo: I don't know if "unhitherto" is a word, but "hitherto" is a word.

Steve: A hitherto...

Leo: A not hitherto.

Steve: Not previously known [laughter], but henceforth known.

Leo: There you go. I'm sure Denise Howell would know how to say that.

Steve: Yes. Notwithstanding, never did quite get my hands around that one. But anyway, problem with the kernel in both 32 and 64-bit XP, Vista, Win7, and Win2008/SP2, which allows software which has already made it onto your machine, allows software to increase its privilege, so a privilege escalation vulnerability. There's a stack overflow error that was found in the NtGdiEnableEUDC function, which allows an attacker who calls that function to inject their return address as a return address into their own code so that, when that function, which is a privileged function, returns, it returns to their code, maintaining full system privileges.

And this is significant because proof-of-concept code is in the wild. And it then would allow full system privileges to be obtained by code which would normally be running with restricted privileges, which much more code does these days, for example, especially under Vista in Win7. And this is, like, exactly what code wants in order to install rootkits because it is, by running with limited privileges, that the kinds of things you want to do, like writing to sector zero of the hard drive or installing hooks into the operating system, those things you cannot do under limited privileges, but you have much more ability to do that if you've got system privileges.

So the bad news is that we're recording this on December 1st, which is Wednesday, meaning that we missed by one day having Tuesday be the first day of the month, which would have meant that the second Tuesday, if yesterday were December 1st, would have been the earliest possible second Tuesday. Instead, it's the worst possible second Tuesday, meaning that the second Tuesday doesn't occur until December 14th, which is as late as it's ever possible to have it occur, which is this month. Meaning that, even if Microsoft - of course they could go crazy and respond to this in an out-of-band patch. But I don't think they're going to.

Leo: Well, it also takes a while to do a patch. I mean, you can't just whip it out.

Steve: True, because it's all of their operating system platforms. It's both the 32 and 64-bit version. They want to make sure they don't break something else when they fix this. I mean, a stack overflow mistake on a parameter of a function call like this, that's just about as easy to fix as anything I could imagine. I mean, there's going to be one compare instruction which is responsible, which is missing, which they need to stick in to prevent this. So this is about as simple and clean a fix as I can imagine.

I just don't think they're going to see that this is crucial unless something horrible happens between now and two weeks from yesterday, which would really make them jump faster. So I expect to see this thing fixed in two weeks, probably not before. There's nothing really actionable that our listeners can do. There's no workarounds. There's no patches or anything. It's not crucial, but it has happened. So I wanted people to know. And as a little bit of additional explanation of why these things are bad, this is exactly what rootkit installers live for is this kind of thing.

And just in other news, relative to topics we've covered several times, you may have seen that Ahmadinejad has acknowledged publicly that the Stuxnet worm did in fact infiltrate the nuclear fuel enrichment processes in Iran and took some of their centrifuges offline. He of course downplayed the significance and vulnerability. It'll never happen again, he said. Well, that one probably won't. But it's very hard, as we know, to keep these things from creeping around in people's computer systems. But so essentially, very early on, before there was much evidence, people were suggesting that this was the case. I didn't talk about it then because there just didn't seem to be nearly enough evidence to make that claim, though it was certainly feasible.

hen, thanks to Symantec's great reverse engineering, they demonstrated convincingly, which is when I finally said, okay, this really does look like there's enough to believe it, they convincingly demonstrated how narrowly targeted and focused the actual exploit end of this worm was. And then, a week later, it was acknowledged that, yes, in fact, it had been effective to some degree in slowing them down. So for those people who've been worried about Iran's nuclear enrichment, I guess - the problem is, millions of systems got infected with Stuxnet in order to just target one, essentially.

Leo: Oh, you think all of the Stuxnet worms are from the same source.

Steve: Yeah.

Leo: And probably, let's face it, Israel.

Steve: Yeah. Well, yeah.

Leo: It's funny because I was at dinner last night with smart, but not particularly technical people. And that was a topic of conversation. It was so interesting to hear people talking about Stuxnet, whether Israel had anything to do with it, what its impact was. I thought, wow. This has gone mainstream.

Steve: And in fact, I don't know what it was, it was on one of the programs I watch, regular broadcast TV. And they were, like, saying "Stuxnet" like they were trying to pronounce it correctly. And it's like, wow. This, as you say, Leo, really has gone mainstream. But for good reason.

Speaking of mainstream, also in the news was WikiLeaks and this massive leak of more than a quarter million previously secret cables between countries. And I thought - my angle on it was to see what I could find and share about the Siprnet, which is the acronym for Secret IP Routed Network, which is the government's global non-Internet Internet, essentially. That is, it uses IP protocols. It has TCP/IP. It uses existing router technology. But it's a network that exists physically disconnected from the regular Internet. And unfortunately, one of the consequences of the U.S.'s post-9/11 attempt to get agencies to communicate much better - "stovepiping" was the term that we heard in Congress, the idea being that individual stovepipes were sort of, if you can imagine it visually, dropped around different departments that were containing their information and not communicating.

Well, here's, I mean, this is a classic example of what happens when you do create much greater degrees of communication. Apparently they believe that it was some Private First Class in Baghdad, a security analyst, a junior security analyst who, as a consequence of this much-enhanced interdepartmental communication, had on his own machine access to all this. And he had some gripes against things that he saw going on, and so he took it upon himself to send all this stuff off to WikiLeaks. What's interesting is that there was some immediate reaction, saying, oh, well, we're going to disable writing to removable thumb drives on these Siprnet-equipped, high-security systems. And it's like, oh, you're going to do that now?

Leo: Surprising that they didn't do it...

Steve: Oh, my goodness. I mean, and on all removable devices. It's like, well, why do these computers have removable devices? It's just nutty that it's like, oh, well. And then they're going to require that two people be present in order to transfer any information from a classified machine to a non-classified machine. And so now they're going to take a bunch of measures to deal with really what should have been done before. But that's the nature of the government's involvement with technology largely is it just sort of doesn't get it right the first time. So this was certainly a huge diplomatic catastrophe. People are saying that not that much was learned that wasn't known before. Certainly some embarrassment and problems. And it does hurt the U.S. from a diplomatic standpoint. So not a good thing. And we'll talk about this a little bit later on, relative to some concerns about the U.S.'s clamping down on domains they don't like because...

Leo: Now, that bothers me, this ICE thing, yeah.

Steve: Yes, it does bother me. And you can imagine that they could say, oh, well, we don't want WikiLeaks to be available either because we think they're bad. And so that suddenly disappears from the Earth. Which I agree with you, Leo, it's really a double-edged sword.

In errata, I noted that the Supreme Court had declined to hear the Whitney Harper case, which I was distraught about, but not surprised, unfortunately. The Whitney Harper case is a 10-year-old RIAA/MPAA lawsuit against a girl, a student, who at the time was 12 years old, when she was using...

Leo: Oh, please.

Steve: Yeah, when she was using Kazaa to download music and share it with friends, which she didn't understand she could not do 10 years ago. She thought it was like Internet radio. And under the law there's something known as the "inadvertent innocent infringer," which carries a fine of $200 maximum; as opposed to the non-innocent infringer, which carries a fine, which is what the RIAA is seeking, of $150,000 per song. So they're saying that she and her family are liable for $150,000 per song, for I think it was 40-some songs that they identified at the time, making this a huge problem.

Now, the first trial judge agreed with her defense attorneys, saying that she was innocent, first of all, because she really didn't understand this was illegal, and no copyright notice of any kind was present in or on what she downloaded. So here she was saying, and her defense attorneys were saying, wait a minute, the RIAA...

Leo: How was she supposed to know?

Steve: Exactly. The RIAA is saying that these are copyrighted. But the beginning of the songs didn't state that. And it didn't say so anywhere during her experience. So this went to appeal, and the federal appeals court judges concluded that a copyright notice anywhere trumps the innocent infringer defense, meaning...

Leo: Oh, my goodness.

Steve: I know. The RIAA was saying that the labels on the original CD cases, which had to have been opened in order to take the CD out of the case to upload it to the Internet, where she found it, those cases contained a copyright notice. And that's enough.

Leo: Well, I can understand that. If they're being pirated, the pirate's not going to reproduce the copyright notice in any event.

Steve: Right. But, now...

Leo: But this is a 12-year-old girl. I mean, if this is not the definition of an innocent offender, I don't know what is.

Steve: And so the problem was that the federal appeals court judges agreed with the RIAA's plaintiff attorneys that she was guilty under the non-innocent infringer case and could be fined as much as $150,000 per song. So everyone was holding their breath, hoping that, now that this had gone to the appellate court, that this would be heard by the Supreme Court. And they declined. So...

Leo: I can understand that. I mean, you don't want to set a precedent that, if a pirate strips out the copyright, then you don't know anything about it. Because you could strip a copyright out of everything. And certainly music, we don't want it to say at the beginning of every song, copyright 2010 by Madonna, all rights reserved, at the beginning of every song. So I can understand that.

Steve: Well, and of course, if they did that, then the people uploading it would just trim that off the front.

Leo: Exactly, exactly.

Steve: This is out of control, unfortunately.

Leo: You've got to wonder, though, if you're a recording artist, how you would feel, how you feel about the fact that your label - your label - is going after a 12-year-old girl, asking for $155,000 fine for the download of your song - your song.

Steve: Per song.

Leo: How would you feel? How do you feel, artists? Why do you put up with this? Why do you allow this? Because to me all it would do is encourage, frankly, people to steal. I don't think this is a good way to win goodwill in any way.

Steve: Over the holidays, well, the first holiday, Thanksgiving, I encountered the notice on Wikipedia about donations.

Leo: Yes. You couldn't miss it.

Steve: Yeah, you could not miss it. It was very much in your face. And I gave the guy a hundred bucks. I gave Wikipedia a hundred bucks.

Leo: Me, too. That's funny, that's exactly what I gave them, too. Yeah. I've done that before, too.

Steve: Yeah. And so I just wanted to make a mention of the fact that, I mean, you and I can afford a hundred bucks. I don't expect all of our listeners to do that.

Leo: No. But a dollar is fine. Anything.

Steve: Yes. But only if you use Wikipedia. My point was that I encountered it because I use Wikipedia. I mean, I don't know if there's a day, frankly, now...

Leo: Exactly.

Steve: ...that goes by. It's the first link that you see in Google when you put anything in, virtually. And I find it highly useful. And I know there are skeptics who say, oh, well, anybody can go in there and modify. It's like, whoa, whoa, whoa, wait a minute. I mean, yes, there's a bunch of nonsense on the Internet. There's also a bunch of high-quality material. And I would say, it's free, but it sure beats anything else that I know of, if nothing else as a starting point for research. And in fact it contains so much valuable information that I'm thinking that maybe the way I will spend my retirement is in dumping everything I've learned in my life of technical and useful nature into Wikipedia.

Leo: That would be an even bigger contribution than a hundred bucks. That would be of great value.

Steve: But still, I just sort of wanted to mention to our listeners...

Leo: I agree, I agree.

Steve: ...just say, hey, if you find yourself using it, if you rely on it, if you value it, give it a few bucks because, I mean, we don't want it to have to become advertising supported.

Leo: No. That's one of the neat things. I mean, Jimmy Wales has said, I've been told he says, we could make hundreds of millions of dollars a year by putting ads on Wikipedia. We don't want to. But in order to avoid that, we need to ask for support because these servers aren't free. And I think it's one of the great resources of the 21st Century. Absolutely everybody who uses it should contribute a little bit, as much as you can. I agree with you a hundred percent.

Steve: So yesterday, as I mentioned at the top of the show, I got flooded - actually I encountered it in the morning on the front page of The New York Times. And I thought, oh, goodness. I mean, the headline was essentially, I don't have it in front of me, but it was "No Need to Supplement With Extra Vitamin D and Calcium."

Leo: Really.

Steve: Yes. And New York Times, Wall Street Journal, NPR, it was on ABC Good Morning something or other, I got email from friends, I got - you can imagine my Twitter feed went nuts with our listeners. And then a ton of email, which I knew was going to happen. Anyway, so I wanted to share with our listeners the reaction that I knew would be coming from the founder of the Vitamin D Council, John Cannell, who's an MD, whose video I have on the Vitamin D page, because he nicely summarizes this.

I'll say first of all that this was a sort of a quasi-governmental - in fact that's his term - agency, the Food and Nutrition Board. And they only addressed the bone strength aspects of Vitamin D. So to the degree that they addressed this, they were correct. I noted that two weeks ago there was a news blurb where it was found that one in five children in the world had symptoms of rickets. So it's certainly not the case that everybody is getting even that incredibly low-level minimum amount of Vitamin D required to prevent that.

But this spring, as I've mentioned before, I received an awful lot of email feedback from our listeners saying that last winter, because I talked about Vitamin D last August, and many people started supplementing, that they were reporting in the winter that it was the first - or in the spring following the winter. It was the first time they'd cruised through the holiday season without catching cold and the 'flu. Mark Thompson, my good...

Leo: Me, too.

Steve: Yes. Mark Thompson, my good buddy who does the AnalogX website, who's in Phoenix, of all places, well, he actually does live like a bat. I visited his home the other day for the first time, and he has box shutters, all of which are closed. So no light comes in the house at all. He is actually running wacky programmer hours at the moment. He gets up in the middle of the afternoon, and he works all night long. And sleeps during the day, so he has to do that in order to get some sleep. But he was, a couple years ago, he was sick every single time I talked to him on the phone. He'd be coughing and sneezing and wheezing. I mean, so that I was really actively getting concerned about him. It's like, Mark, you're sick all the time, every time I talk to you. And he's like, oh, yeah, well, I just got back from a trip somewhere, blah blah blah.

He started taking Vitamin D after I learned about it last summer. He hasn't been sick once since. I mean, it completely changed his life. And of course we know that that's immune system boosting. But remember that - and so not getting colds and 'flu is the short-term consequence. But the long-term consequence is not getting cancer. Because it's our immune system that is protecting us all the time from little cancers that are trying to start, and are getting zapped before they ever have a chance to get going. So anyway, this - and I'm not going to do a SpinRite testimonial because I want to read this instead. John writes:

"After 13 years of silence, the quasi-governmental agency, the Institute of Medicine's Food and Nutrition Board today recommended that a three-pound premature infant take virtually the same amount of vitamin D as a 300-pound pregnant woman. While that 400 IU/day dose is close to adequate for infants, 600 IU/day in pregnant women will do nothing to help the three childhood epidemics most closely associated with gestational and early childhood vitamin D deficiencies: asthma, auto-immune disorders, and as recently reported in the largest pediatric journal in the world, autism. Professor Bruce Hollis of the Medical University of South Carolina has shown pregnant and lactating women need at least 5,000 IU/day, not 600.

"The FNB also reported that vitamin D toxicity might occur at an intake of 10,000 IU per day" - which is 250 micrograms per day - "although they could produce no reproducible evidence that 10,000 IU/day has ever caused toxicity in humans and only one poorly conducted study indicating 20,000 IU/day that may cause mild elevations in serum calcium, but not clinical toxicity.

"Viewed with different measure, this FNB report recommends that an infant should take 10 micrograms/day" - that is to say 400 IU - "and a pregnant woman 15 micrograms/day (600 IU). As a single 30-minute dose of summer sunshine gives adults more than 10,000 IU, the FNB is apparently also warning that natural vitamin D input as occurred from the sun before the widespread use of sunscreen is dangerous. That is, the FNB is implying that God does not know what she is doing."

Leo: I like that.

Steve: "Disturbingly, this FNB committee focused on bone health, just like they did 14 years ago. They ignored the thousands of studies from the last 10 years that showed higher doses of vitamin D helps: heart health, brain health, breast health, prostate health, pancreatic health, muscle health, nerve health, eye health, immune health, colon health, liver health, mood health, skin health, and especially fetal health."

Leo: And health health.

Steve: And health health. "Tens of millions of pregnant women and their breastfeeding infants are severely vitamin D deficient, resulting in a great increase in the medieval disease, rickets. The FNB report seems to reason that, if so many pregnant women have low vitamin D blood levels, then it must be okay because such low levels are so common. However, such circular logic simply represents the cave man existence (never exposed to the light of the sun) of most modern-day pregnant women." Which of course is what has happened, is we've all gone indoors.

Leo: The sun is bad for you, don't you...

Steve: And when we're outdoors we're wearing clothes and/or sunscreen. He says, "Hence, if you want to optimize your vitamin D levels, not just optimize the bone effect, supplementing is crucial. But it is almost impossible to significantly raise your vitamin D levels when supplementing at only 600 IU/day. Pregnant women taking 400 IU/day have the same blood levels as pregnant women not taking vitamin D; that is, 400 IU is a meaninglessly small dose for pregnant women. Even taking 2,000 IU/day of vitamin D will only increase the vitamin D levels of most pregnant women by about 10 points, depending mainly on their weight. Professor Bruce Hollis has shown that 2,000 IU/day does not raise vitamin D to healthy or natural levels in either pregnant or lactating women. Therefore, supplementing with higher amounts like 5,000 IU/day is crucial for those women who want their fetus to enjoy optimal vitamin D levels, and the future health benefits that go along with it.

"For example, taking only two of the hundreds of recently published studies: Professor Urashima and colleagues in Japan gave 1,200 IU/day of vitamin D3 for six months to Japanese 10 year olds in a randomized controlled trial. They found vitamin D dramatically reduced the incidence of influenza A as well as the episodes of asthma attacks in the treated kids, while the placebo group was not so fortunate. If Dr. Urashima had followed the newest FNB recommendations, it is unlikely that 400 IU/day treatment arm would have done much of anything, and some of the treated young teenagers may have come to serious harm without the vitamin D.

"Likewise, a randomized controlled prevention trial of adults by Professor Joan Lappe and colleagues at Creighton University, which showed dramatic improvements in the health of internal organs, used more than twice the FNB's new adult recommendations.

"Finally, the FNB committee consulted with 14 vitamin D experts and - after reading these 14 different reports - the FNB decided to suppress their reports. Many of these 14 consultants are either famous vitamin D researchers, like Professor Robert Heaney at Creighton; or, as in the case of Professor Walter Willett at Harvard, the single best-known nutritionist in the world. So the FNB will not tell us what Professors Heaney and Willett thought of their new report? Why not?

"Today, the Vitamin D Council directed our attorney to file a federal Freedom of Information (FOI) request to the IOM's FNB for the release of these 14 reports.

"Most of my friends, hundreds of patients, and thousands of readers of the Vitamin D Council newsletter (not to mention myself), have been taking 5,000 IU/day for up to eight years. Not only have they reported no significant side-effects, indeed, they have reported greatly improved health in multiple organ systems.

"My advice, especially for pregnant women: continue taking 5,000 IU/day until your 25 (OH)D is between 50-80 ng/mL (the vitamin D blood levels obtained by humans who live and work in the sun and the mid-point of the current reference ranges at all American laboratories).

"Gestational vitamin D deficiency is not only associated with rickets, but a significantly increased risk of neonatal pneumonia, a doubled risk for preeclampsia, a tripled risk for gestational diabetes, and a quadrupled risk for primary cesarean section.

"Today, the FNB has failed millions of pregnant women whose as yet unborn babies will pay the price. Let us hope the FNB will comply with the spirit of "transparency" by quickly responding to our Freedom of Information requests."

And I should just mention that the story in The New York Times produced a phenomenal response in people posting to the story. When I looked in the morning, there were already 255-some responses, and many had been redacted by the people at The New York Times, I mean, saying that they had protocols, they couldn't allow the level of fury that was being expressed, no doubt expletives and obscenities. So they were deleting these things. But there were a number of very knowledgeable responses from people who were saying, okay, this is just really irresponsible to be in the news.

Leo: It's so odd. And I noticed, since you raised my awareness on this, that my own doctor started testing for Vitamin D when he does blood tests. It's just kind of part of the routine blood tests now. My wife got hers back, and she was low. And she recommended supplementation.

Steve: Anyway, I know that it's been a big interest of our listeners ever since I did the podcast, August before last. And this generated so much feedback that I wanted to cover it today and just say they looked only at bone health. It is the case that much less D is necessary for bone health, much more necessary - essentially the level you would have if you were spending your days out in the sun, and you were a young person near the equator - to keep you healthy.

Leo: I'm taking my supplements. At least I know they're not harmful. But you should, obviously, folks, we're not doctors, you should consult your physician.

Steve: Yes.

Leo: And if you're worried, ask for a Vitamin D test. All right. So a little sci-fi.

Steve: A little sci-fi. So I read science fiction when I'm on my stair climber, which I do most days for about 66 minutes a day. It works up a good sweat, gets my heart rate up and so forth.

Leo: Why 66 minutes?

Steve: It just sort of evolved that way.

Leo: That's interesting.

Steve: I think I was at an hour. And I looked at the calories I was burning, and I was, like, 643...

Leo: You wanted to get to 700?

Steve: And I thought, yeah, I'll go to 700. And I think I hit 700 by about 64.5 minutes. And then I thought, well, 66 is a prettier number than 64.5. So I just kept rounding up, one parameter or the next, until I ended up at 66. And that takes me on the high side of 700 calories.

Leo: That's awesome. That's great.

Steve: So I just sort of stay there. So consequently I'm needing a source of something to read. And so I went looking for some more stuff. And I'm constantly getting feedback from listeners, saying, hey, Steve, what's happening in the world of sci-fi? So as it happens, still the very best things that I have found are what we've talked about before. If listeners are not familiar with Peter Hamilton, he's at the top of my list.

Leo: Me, too. And you introduced me to him, and I love him.

Steve: Oh. "Fallen Dragon." You get an introduction. It's a standalone volume. He's very wordy. But so these books are long.

Leo: But they're all good words.

Steve: Yes, they are. And he paints such a rich environment that, I mean, I still see all of these worlds that he has created for me. So "Fallen Dragon" is a perfect introduction. Then my second favorite series, it's just a two-volume series, is "Pandora's Star," followed by "Judas Unchained," which is the sequel to "Pandora's Star," which is just - I've read "Fallen Dragon" I think three times. I've read both "Pandora's Star" and "Judas Unchained" twice. Because these are things you can reread, or I can. They're just spectacular pieces of work.

Then my second favorite we've also spoken of before, and that's Michael McCollum's books. He has a website, Scifi-AZ.com, Michael McCollum. He also writes multi-volume series which I very much enjoy. Because, again, if I read one book, it's like, okay, well, that's gone. It's annoying if the series isn't finished, and then you're, like, stuck waiting, which happens to me from time to time. But his Antares Trilogy - "Antares Dawn," "Antares Passage," and "Antares Victory" - is just fantastic. I read them all twice. And I'm just sort of waiting now for it to be long enough for me to reread them.

And then the Gibraltar Trilogy I've mentioned: "Gibraltar Earth," "... Sun," and "... Stars" is fantastic. And in the case of "Stars," I read it before it was published because just to be his proofreader. So that came out. And I reread the prior two in order to get ready for the third one to be done. So that's great. And he also has many individual novels.

But new stuff that I haven't talked about before, I made a posting to the sci-fi newsgroup at GRC, and I said, "Hey, guys, I'm looking for more to read. I need, like, kind of space opera stuff. What have you got?" And someone mentioned what was called "The Lost Fleet" series that's written by a guy named John G. Hemry. But he writes under the pen name Jack Campbell. And this is a series of six books called "The Lost Fleet" series: Dauntless, Fearless, Courageous, Valiant, Relentless, and Victorious. And I had never read anything like them before. And they were really effective in filling time. I can't say that they were fantastic science fiction. But I needed something to do on the stair climber. But I could also recommend them.

Leo: There are audio books of this as well.

Steve: No kidding.

Leo: Tomaho (sp) says it's on Audible.

Steve: Great. And this gives nothing away. I won't do any spoilers here. Because in the first few pages we're reviving a survivor of the beginning of a war from a hundred years before. So we're bringing him out of cryo sleep. And what's happened is there's been this war that's been going on for a hundred years between two chunks of human civilization that are really upset with each other. Because so many casualties and people have been promoted so quickly, the people in the current fleet, whose side we're on, have sort of lost the art of space combat.

And so we revive this guy from a hundred years before who says, wait a minute. This is the way you're fighting? And he organizes space combat in a really compelling and convincing fashion. So we don't have warp drive. We have worm holes you can jump between star systems with. But the laws of physics and the speed of light play into this intimately. And the author sets up some really interesting problems and solutions that involve configurations of fleets of ships that basically have conventional weapons and some beams and missiles and interesting weapons. But things are constrained enough that you're working within a domain, a fictional domain with real limitations, which makes it really interesting. And I found myself being sucked along in this. So if you've run out of stuff to read, or to listen to, give the first one a try. And I'll be surprised if you don't get hooked and end up with all six of them because...

Leo: Sounds like Horatio Hornblower in the 25th Century or something like that.

Steve: I think actually I've heard exactly that analogy being made.

Leo: I love those kinds of seafaring novels, so...

Steve: Yeah. And there's interesting - there's a lot of politics because he ends up being, because he's a hundred years ago, he ends up being the most senior officer. So he ends up commanding the fleet. But then there's lots of people who of course don't like that. And then there's some political interplay, and we've got a little romance stuff going on. But mostly really, I mean, obviously contrived because it's fiction, but satisfying space battles. And I've never seen, I've never read anything of this scope where you've got really interesting space battle scenarios with interesting puzzles and limitations. So I wouldn't be surprised if you read the first one and then didn't get hooked.

Leo: Sounds cool.

Steve: So I did all of those. Then I said, okay, what next? Then I ran across something called "Helfort's War."

Leo: You like these big long series, don't you. You don't want just one book. You don't want just two books.

Steve: Well, and here was one where I ran out before the fourth book. This is a series of four. And it's sort of the classic newly minted graduate from Star Fleet, I mean, it's not set in the Star Trek environment, but we do have like the academy. He's graduated from the academy, and we follow his career through four books. And I ran out at the end of the book three, and book four just was published on the 23rd of November. So it's available for Kindle, which is where I'm reading this stuff. And I haven't yet started because I'm just finishing the fourth book in another series of six, which is Gregory Benford's Galactic Center Series.

So the Helfort's War books I really liked also. Again, I recommend them. I mean, top of the list is Peter Hamilton and Michael McCollum. I don't think I would read these other ones a second time, where I have read the earlier ones a second time. Of course not that much time has gone by. But still I feel like I'm sort of done with those. But really, I mean, they were diverting and interesting and I think stand very well. And then Gregory Benford actually is a UCI physics professor.

Leo: I like that. I like hard science.

Steve: This is. His is the so-called Galactic Center Series. I've just finished "Tides of Light," which is the fourth in the series of six. And here we sort of - we've got the humans versus the machines is like sort of the overall scenario there. And I loved, back in the day, Fred Saberhagen's Berserker series.

Leo: I haven't read those, either.

Steve: Oh, those are really good, Leo. Berserkers being machines left over from some unknown alien race in the past that are out to kill off all biological life. And really interesting sci-fi that's old. It's been around forever. But now we've got the so-called "mechs," the mechs versus the humans. And this is a huge scope, like tens of thousands of years of history, but really interesting new ideas that I've never read before. And also substantial works. So I'm liking those, as well. So "The Lost Fleet," "Helfort's War," and Gregory Benford's Galactic Center series.

Leo: I'm amazed you have time to read all this stuff.

Steve: I spend a lot of time on the stair climber.

Leo: I guess so. Well, that's one of the advantages of being fit. You have more time to read.

Steve: Exactly.

Leo: Now, are you ready, Steve? Questions for you.

Steve: Yes, indeed. And I just will mention that you're right about the book series. I look for the series because I'm wanting to get engaged and have a lot to read. So it is a reason that I'm choosing those deliberately. When I see it's, like, book six, I go, okay, good, I'll go find number one and move through them.

Leo: No, I know what you mean because I like to get immersed. And instead of, you know, once you get immersed, sometimes if you get immersed in a world, and it's over, it's like, well, golly.

Steve: Yeah, exactly. If Peter Hamilton kept writing, I just wish he would keep going with his various universes.

Leo: Well, what was it, was it "Judas Unchained" went on a little long. I thought.

Steve: Yeah, and I never got into "The Dreaming Void," I think that's his next one. Because I was just sort of - it sounded a little, I mean, I really do like hard sci-fi.

Leo: Yeah, yeah.

Steve: I don't want fantasy stuff and people dreaming about something. I sort of read the synopsis, I thought, eh, don't think so.

Leo: Yeah, no, I like the hardcore stuff. All right.

Steve: When he had, who was it, Al Capone coming back to life?

Leo: Yeah.

Steve: It's like, uh, no, no, no.

Leo: Yeah. That really - yeah.

Steve: Yeah.

Leo: "Fallen Dragon," that's the one.

Steve: Oh, it's a great first book, yeah.

Leo: Question 1, an anonymous listener raises a good and disturbing point: Steve and Leo, regarding the Chinese redirection of traffic, you forgot to mention that SSL would not have prevented snooping in the latest traffic redirection incident. China controls root certificates that are installed on our systems - we've mentioned that before, including the Hong Kong Post Office - which enables them to do transparent SSL man in the middle. Is that right?

Steve: That's exactly right. So it is the case that - I do not think this was deliberate because many mistakes have been made with BGP, the Border Gateway Protocol, in the past.

Leo: Yes, yes.

Steve: So it's much more likely that it was a misconfiguration in the router tables that inherently propagate themselves to the routers that they're connected to, which then propagate those to the routers they're connected to and so forth. So this kind of thing can ripple through the Internet, and has many times before.

Leo: Yes, yes, yes.

Steve: Yet it is also the case that this protocol is not secure. And had this been deliberate, then traffic would have been routed, and there's absolutely nothing preventing them from doing on-the-fly certificate synthesis, signing the certificates with the private keys of the certificate authorities that are installed in all of our browsers. So this anonymous listener is exactly right, that it is the case that SSL would not protect us. And in fact, what that means is we would be saying www.amazon.com, be looking at what appeared to be a valid certificate, and not knowing that the traffic had been redirected through someone who had control of a certificate authority that had signed the certificate that was synthesized on the fly because they knew we were connected to Amazon. So, yeah. Not good.

Leo: Not good.

Steve: Not good.

Leo: Question 2, another anonymous listener had a thought about defeating Phorm-style man-in-the-middle eavesdropping: Steve and Leo, would it be possible to derive a simple protocol using certain parameters known by both the browser and the server - but I guess no one else. That would deter some systems like Phorm, but not unduly impede security services. I was thinking perhaps the server would know, say, the connection IP address or some header, and the browser would know both the IP address of the server and the requested URL. XOR them, should be fast and transient enough? John Doe. What do you think?

Steve: Well, no.

Leo: Maybe you'd better explain it to me.

Steve: Yeah.

Leo: I don't know what he's proposing here.

Steve: Well, so what he's saying is, isn't there something, some simple way of preventing Phorm, which is essentially an ISP-sanctioned man-in-the-middle and eavesdropping entity. Phorm is the thing which was installing its own cookies on other people's domains so that it can track us and profile us, essentially. So he's saying, if we established a secure connection between browser and server, then the man-in-the-middle aspect and the eavesdropping aspect could be thwarted.

The problem with doing that is, and exactly as you said, Leo, is that the man in the middle would have to be excluded from information that only the browser and the server knew. The man in the middle could see the IPs at each end, could see the headers that were being exchanged. So...

Leo: So now you're talking encryption.

Steve: Well...

Leo: Public key encryption or something like that.

Steve: Yeah. You couldn't - you'd need both encryption, and you'd need authentication. And we've talked about how, if you don't have authentication, if you can't authenticate, for example, the server at the server end, then anybody, by definition, anybody could impersonate the server and become a man in the middle. And the only way to get authentication is for there to be some sort of secret which the authenticating party is able to prove they have. And the only way to do that in an open public system is to use a public key, where the authenticating party is able to prove they own the matching private key to the public key which you and everybody else have.

So unfortunately our listener is trying to come up with, like, a simpler solution, something less heavyweight, easier, faster, lighter weight, XOR - well, of course XOR is extremely weak. Well, it's not even crypto, I can't call it crypto because it would be trivial to, even without doing anything but looking at the traffic that has been XOR'd, you could easily crack that, if you were XORing against a fixed pattern. If you were XORing against a pseudorandom stream, like the RC4 crypto does, then, all other things being secure, this could potentially be secure, too. But the problem is there just, there isn't a way to make it simpler. If you make it simpler, you lose authentication. And if you lose that, you've got nothing. So just unfortunately we have made it exactly as simple as possible, which is unfortunately not very.

Leo: Question 3, Rick Shepherd, Reno, Nevada, wonders about the ".p2p" TLD, Top Level Domain: Steve, I'd like to hear your thoughts on the proposed .p2p TLD. It's supposed to be ICANN-independent. And this is relevant to what's going on right now with ICANN being used by the Department of Homeland Security to take down torrent servers. It would allow we-the-people, he says, to bypass traditional DNS and thereby remove the power from ICE or whomever may wish to take down domain names. He refers to a website, dot-p2p.org, it's a wiki, for more information on that one.

Steve: So this is interesting. What is being proposed is a sort of a secondary or alternative DNS which would be decentralized. And whereas our existing DNS is based on a hierarchy, starting at the top with root servers, the famous 13 root servers that then point to the .com and the .org and the .net and all of the second-level domain and so forth. There's this proposal to create a .p2p, sort of like .com, .net, .org, .edu and so forth.

The problem is it's being led by the Pirate Bay guy, Peter Sunde, who was just convicted recently of, along with the two other Pirate Bay people, of being complicit in the theft of copyrighted material. And they're appealing this judgment that did just recently come down against them. The prison term was reduced to eight months, yet the fine was increased to, I think it was $8.8 million U.S., although it was denominated in their currency.

So in principle I'm troubled, as you are, Leo, by the idea that our government, the U.S. government, and presumably other governments, could get it into their head that removing domains from the Internet is, wow, gee, that was easy. In the same way that we've got this problem with earmarks in our legislation, where some legislator tags something into legislation that's going by, and it gets through, you can imagine someone saying, yeah, could you remove this domain for me as a favor because they're our competition. And it gets sort of slid into some other package of domains being removed.

I mean, to me it feels like a slippery slope. The problem I have is that I hate the idea of this being used only for piracy and theft of copyrighted material, which is really the way this seems like it's being set up. I'm troubled by the idea that domains can get removed. So what this is, the idea is it would be like BitTorrent. And in fact they're proposing that it would actually use the decentralized BitTorrent hashing protocol.

Leo: Oh, that's interesting. Because you have a problem, if you're not in the main directory servers, how do you get visible?

Steve: Right. And so the idea is that people who wanted access to this, it's probably going to end up being a hierarchy of pirate domains, which if nothing else would live sort of off the grid, or off the hierarchy. You would run a client on your computer, which would link up in BitTorrent style to a mesh of other clients and share all of this .p2p top level domain, essentially share the hierarchy of DNS. The client living on your computer would filter your outgoing DNS queries. If the domains going out were not .p2p, that is, didn't have that on the far right side, it would let it go through. And the regular public DNS hierarchy would resolve the IP address.

If, however, anything you put into your web browser, piratesrus.p2p, then the client running on your machine would see that, intercept it, and then use this sort of decentralized, floating in the cloud, interlinked, peer-to-peer DNS alternative for its IP resolution. And you'd get the IP of that domain. And it would be, from a user standpoint, rather transparent. So it's clever. It can work. And it is going to happen.

It's pretty much, I mean, there's enough inertia behind this already that I think - and it's an interesting enough idea that people who are interested think, hey, that's kind of cool. I mean, I would think it was kind of cool except that I'm afraid it's only going to be used by the dark forces and not by people who are sort of more honestly wishing to avoid government control. But I'm sure it'll be used for that, too. So...

Leo: I think at some point we may need a darknet.

Steve: You know, the way things are going, it does seem like it. I mean, I'm finding myself, as I was talking about, I mean, innocently exchanging some email about what's going on in airports with body scanning, and even talking about nuclear and Iran and Stuxnet, I'm finding myself a little self-conscious about the fact that I'm probably now being, I mean, I'm using words that are tripping filters somewhere, and my email is being observed by our government. And it's a little creepy to think that that's going on. I mean, I hope they understand I'm one of the good guys. But it is unfortunate that this is changing. And you know, Leo, you can almost sort of feel unfortunately this happening.

Leo: You really can.

Steve: As the Internet matures, it's like, well, they're not happy about the taxes they're losing for Internet sales. They're not happy about what happened with WikiLeaks and these cables getting out. The government wants control. And of course now we have the FBI not happy about encryption. And it's poked me right in my own backyard.

Leo: I think the forces of reaction, the reactionaries are actually gaining power. And the good news is the people who know how to use technology can be the freedom fighters. I think it's the 21st-century freedom fighters are the hackers of the world, and I say that in the best sense of the word, who know how to use technology. And I think ultimately we might have to create a darknet. But the good news is, we can. We know how.

Steve: Yes, that's true. It is true. And the bad news is, I mean, when I look at, for example, my own intention of doing CryptoLink, I want to empower people to have secure private communications. I'm not going to do it if the law requires that I put a backdoor into the product such that I'm not able to offer them secure private communications. And what's so sad about this is math is what this is based on. Math exists already. I mean, the technology to do this exists. OpenVPN is a perfectly fine, functional VPN system. It's way clunky, and I could make something far better. But the bad guys will use that if they want something that cannot be eavesdropped on. I mean, it already exists. The horses have left the barn. So I don't know what my position is on something like a distributed, control-free network. It is certainly possible to do, just like secure crypto is possible to do.

Leo: I would say now is the time for all good men to learn a little programming and network configuration because - I actually said this about eight years ago. I did an interview for a movie about Adrian Lamo about hacking. And I said, I think hackers are the freedom fighters of the 21st Century. I think instead of the right to bear arms, we need a new Second Amendment that includes the right to bear technology. Mark Jones - go ahead.

Steve: I was just going to say, and I hate the idea, I hate the idea that CryptoLink might be used for a purpose that was really foul, I mean, really evil. But that's the nature of, I mean, that's the nature of technology, in the same way that a nuclear bomb can be used for something that is really wrong, really evil. It's not the atom's fault that it contains a lot of energy.

Leo: I think you have to consider what the alternative is. Yes, it's bad. But the alternative is worse. Or yes, it's potentially bad, but the alternative is far worse. It's basically a world controlled by those who would assert their power.

Steve: And unfortunately we see that they choose to.

Leo: And they're glad to.

Steve: Yes.

Leo: Mark Jones in Midland, Michigan wonders about web fingerprinting and fonts. You're turning me into a libertarian. We're both, you know, it's funny. Steve and I are both staunch liberals. But I have a feeling we're becoming more libertarian as the government becomes more reactionary. Mark Jones in Midland, Michigan wonders about web fingerprinting and fonts: Steve, let me thank you for the wonderful podcast. It's been my favorite and a must-listen for several years now. You and Leo are the best.

Today's Wall Street Journal's front page contains another article in their on-going series on web privacy. This one addresses - which we have decried, I might add. This one addresses the technology of BlueCava for web fingerprinting. The technology is clearly not unique to

BlueCava. It is the web fingerprinting technology you described some time ago that polls many different attributes of a particular system. A unique

pattern that identifies the system emerges when these attributes are viewed as a set. I don't remember what episode we talked about that in, but it's just a few episodes ago and worth listening to. It wasn't the evercookie, it was...

Steve: Unlike the other episodes.

Leo: They're all great. Well, you know, it's really interesting because this show is, in many says, on the cutting edge of what's going on here. It's not just security and privacy, it's everything. As a loyal Security Now listener, I was surprised to actually learn something from the mass media about security. He's talking about the Journal article, not us.

Steve: Right.

Leo: The article called to my attention that one of the means the fingerprinting uses is to interrogate fonts on the system. I think you mentioned this, actually.

Steve: Yes, font enumeration, yup.

Leo: Right. Several years ago I converted my handwriting into a font. I gave the resulting font the fairly obvious name of my name. My name is fairly generic, but I'm betting I might be the only person to have a font with my name. I bet you're right. I never thought this might be a beacon for tracking me on the web. And by itself, even if your name is John Smith, by itself it might not be. But then if there's a universe of 12 John Smiths who have fonts named John Smith, you're the only one with this version of Flash, this version of a browser, this particular screen resolution. By the time they add them all up, we're all one of a kind.

This prompts a couple of questions: How many ways can the fonts on your system be interrogated by a website you visit? Can all of the BlueCava methods be blocked by the use of NoScript? Are there other means to block the font list from prying eyes? I think that's it.

Steve: How many ways can the fonts on your system be interrogated by a website you visit?

Leo: Is it JavaScript that does that? JavaScript is activated by the visited site, and it says - because sites can typically query your computer about its capabilities.

Steve: Yes. Now, some of the information is just in the browser headers. But, for example - well, okay. So the reason I chose this question was not so that I could tell him that there were three ways that fonts can be queried. Because, I mean, who knows how many? It's just I thought this was a great question. Unfortunately, BlueCava is somewhere, I mean, I'm looking over my shoulder now because they're in Irvine.

Leo: Is it a company?

Steve: Yeah, it's a company. The Wall Street Journal's article is just horrifying. I mean, it is chilling. This guy, I mean...

Leo: This is legal, by the way. It's completely legal.

Steve: Yes, exactly. I mean, but it's one of those things where you read the article, and it just sends shivers up the spine of anyone who's concerned about, like, their privacy. Because he's boasting how many different fingerprints he's accumulated, and how unique they are. And just in the news, I didn't pull this out for the podcast, but a Department of Transportation in, I think it was in Florida, was just found guilty of selling tens of millions of drivers' personal information to an Internet-based marketing company. So it's a government agency.

Leo: How dare they? How dare they?

Steve: I know. Including Social Security numbers, which they have.

Leo: What?

Steve: Yes.

Leo: What state was that? Arkansas?

Steve: It was in Orlando.

Leo: Orlando, Florida. Geez.

Steve: Yeah. I think if you put in Orlando, Florida - boy, I can't - I pulled it up by putting the name of the marketing company.

Leo: That's terrible.

Steve: But I just - it's like, oh, goodness. So now we have the government profiting from selling our personal information to Internet-based marketing companies. So, I mean, they'll get their hands slapped hard, and it's wrong that they did it. But the information is loose now. It's gone. You can't get it back.

Leo: I'd be incensed.

Steve: So I wanted to reiterate that, yes, the number one thing that's protecting you is blocking scripting, that is, NoScript. Because all of this stuff, font enumeration, I should say the deeper lock-onto-you technology involves scripting. So remember that scripting, I mean, it's a mixed blessing. Yes, more and more sites need it. I know that a huge percentage of our listeners are running NoScript. And, yes, it's annoying. It gets in your way to be blocking scripting by default. I'll go to sites that I haven't visited before, and something kind of doesn't seem right. It happened this morning when I was going to some sites, looking around at things. It's like, okay, this page doesn't seem correct. Or, like, I'll fill in the state that I'm in, and then the fields on a form below didn't populate, and I go, ugh. And so I turn on scripting, and now the site comes alive, and the form works the way it's supposed to.

Well, so it isn't transparent. But given that there's so much power in scripting, you want it to be only used on your behalf, for your benefit, and not against you. And unfortunately, companies like this, that are founding themselves on what scripting can do, are taking advantage of that. So scripting is necessary for enumerating fonts. You can't do it without it. But even without scripting, browsers give away a lot in their headers, as we've seen. I think it was the EFF that did their - the name's not coming to me now - Panopticlick that we talked about, again, several months ago. Panopticlick, as I remember, was just doing passive examination of what the browser was relinquishing without scripting. And it was comprehensive.

So even just looking at, like, the version numbers of all the things that we've got installed on our computer tend to make it unique. And the resolution of our screens, and the obvious information that is getting away. So somebody who really is concerned about this does need to do something like we've talked about, which is boot a browser-enabled OS from a CD, or use a virtual machine, use a VM, and to use a generic browser that you haven't customized much, and do your surfing that way, and maybe change it from time to time so that you don't have a static fingerprint.

I mean, I don't mean to overhype the issue of tracking and fingerprinting. I know that some people just, eh, they don't care. But increasingly, when people realize that this is going on behind their back, if nothing else, they ought to understand what they can do to prevent it if they do care. And, sadly, scripting is the means for this happening, and disabling it conditionally is the way to get around it.

Leo: I don't like it...

Steve: No.

Leo: ...when smart techies are the wrong side of the equation.

Steve: Yeah, it's interesting, this guy who founded BlueCava, he apparently years ago started off because he wanted to protect downloadable music software. And so he came up with a way of locking music software to a machine by looking for, like, the fingerprint of the machine so that it would only run in the machine with that fingerprint, and people could use it freely, try it out in a demo before purchasing it, and then he wouldn't have to worry about it getting loose. And then he realized, hey, there's a lot here that I can lock onto that makes this unique. And it's like now, of course, he's switched over to the dark side, going to make money by tracking and profiling and building up his big database of fingerprints.

Leo: Oh, he's so proud of it, too, if you visit the website. It's like, I've got a patent, and look what I can do, and blah blah blah blah blah. Boo, hiss. Question 5, Edward "Ted" Doyle in Columbia, Missouri wonders about the allocation of IP addresses for efficient routing: Steve, I have been listening since Episode 1, my favorite podcast. I've been reading a wonderful free book about TCP/IP, and neither your past podcasts introducing basic Internet concepts, nor the first 500 pages of the book, have addressed so far the notion of IP address allocation for efficient routing.

There are about 64 times 256, or something like 16,000 Class B addresses, that is, IPv4 with the first number of the IP address starting 128 through 191. If these addresses are assigned to organizations in a disorganized fashion, the following situation could occur. I don't know if I want to read all this. Basically, 140.65.* goes to a company in Australia. Then 66 to Poland, 67 to Edmonton, you get the idea. They're all just geographically random. There must be some order to the way addresses are assigned. He's thinking, like, zip codes, where it narrows it down geographically.

Steve: And zip codes is a great example, as a matter of fact, Leo.

Leo: Yeah. For instance, if the IP block with 140 through 147 in the first byte were assigned to Europe, and then Europe could, say, take 140 and assign it to England, 141 to France and so on - I don't think it was anywhere near this organized, of course. Thus the router in St. Louis, using one router table entry, could examine the first number in the IP address, see something between 140 and 147 and know the packet needs to be routed eastward toward Europe.

Is this how IP addresses are assigned and routed? If not, could you describe how IP addresses are allocated to make routing feasible? We need Jon Postel on. He was the guy who made this all up way back in the - way back when, the late Jon Postel at USC. Yeah, I know that most routers use Classless Inter Domain Routing, or CIDR, obsoleting the old class A, B, and C systems. The book I'm reading, by the way, is "The TCP/IP Guide" by Charles Kozierok. The full 1,600-page text is available - I love this - at tcpipguide.com. So far I'm only about a third of the way in. The next 100 to 200 pages I'll reach the chapters on routing protocols. I will continue reading the book and listening to your podcast for the answer to this question. Best regards, Ted Doyle, Columbia, Missouri.

Steve: Okay. So there's a cool URL you need to put into a browser, and our listeners should if they're listening: bgp.potaroo.net.

Leo: Bgp.potaroo.net. Oh, look at this. This is interesting. I don't know what it is, but it's...

Steve: Well, that's the growth of the BGP router table over time.

Leo: So this is the table that all border gateway routers use to figure out where goes what.

Steve: It's the size of the table. Currently 336,807 entries.

Leo: How big is it?

Steve: Well...

Leo: Is it 100K? A megabyte? A gigabyte?

Steve: No.

Leo: Can't be very big.

Steve: These routers, well, the good news is, an IPv4 address is four bytes. And a mask is four bytes. So all of these, they do compress, and they are very dense, but there are a lot of them. So to wind back a little bit and answer Edward "Ted" Doyle's question, is unfortunately, had we to do it again, we would do it differently. But when has that not been the case?

Leo: Nobody thought it would be this way.

Steve: No one thought it was going to even work, Leo.

Leo: This, I don't know who is "potaroo," but this is a really interesting site.

Steve: Yeah, it's a great site.

Leo: Wow.

Steve: There's a lot of interesting statistics. So to some degree this does work. For example, Level 3 has the whole four-dot network. So to the degree that Level 3 controls the routing within their network, there doesn't have to be individual entries in the global BGP tables for every network within Level 3. For example, my little 16 IPs at Level 3, they certainly aren't represented uniquely in some router table entry in Bulgaria. Instead, anything that begins with four goes in the direction of Level 3, and that's the last of it. So it absolutely is the case that, as we know, there is a hierarchical allocation of IP space where four-dot is Level 3. And I think HP has 15 and 16, or they have two consecutive ones that are Class A networks. And so everything beginning with 15 and 16 goes towards HP.

Now, the problem is HP is widely distributed geographically. So their IPs are probably global, and there will be many more entries for things beginning with 15 and 16 than, for example, Level 3 that might be more regional. But it's certainly the case that there is some regionality to routing. And so when a large ISP is regional and giving their various customers chunks of address space, well, everything first goes to the ISP and is routed monotonically to the ISP. Then the ISP's routers break it up and send it to the appropriate customers within those networks. So if we could renumber the Internet, oh, we could radically simplify things.

Leo: Interesting. Interesting.

Steve: But we can't renumber the Internet. I mean, no one wants to have chunks of their IPs just ripped away and changed. So we're sort of stuck with this. It's not clear that it's going to get any better, either. I mean, we can see the growth is - it's not exponential, but it's certainly a little more than linear over time. And here we're saying we need - that 4.3 billion IPs is no longer enough. So we've outgrown 32 bits of IP space. Unfortunately, routing is going to keep being a challenge. So, yes, it would be nice if it were done somewhat more sanely. But at this point the cat's out of the bag.

Leo: Too late.

Steve: Yup.

Leo: Dennis Keefe, Panama City, wonders about securely using LastPass on a work PC. Steve, the following is a post from my blog. What do you think? If you love LastPass but are not exactly comfortable about having it installed on your work PC, you might like this solution. Today I tried this approach. First I used TrueCrypt to create an encrypted volume on the hard drive. Most offices won't let you do that, by the way. Many offices won't. Mine will. Next - maybe he works for me. Next I went to PortableApps.com, and instead of downloading the software to a USB drive as usual, I installed it into the encrypted volume. Now the only way to access Firefox and my LastPass vault is by mounting that TrueCrypt volume. Of course I need the pass to do it. If you still need Firefox installed for others in your office, just install a stripped-down version for others to use that doesn't include any personal info, and you're safe. Keep up the great work. Dennis Keefe, TheCommonGeek.com, Panama City, Florida. That's actually a very clever idea.

Steve: It is clever. There's one thing I would add to it. First of all, what PortableApps does is kind of neat. They've got portable-ized versions of existing apps, like Firefox, for example, that are specifically well-behaved in not using things like the registry. So, for example, Firefox will create a traditional INI, an initialization-style file, where all of the things that it would normally be storing in the registry, all of its configuration information, it will store locally instead. So these are deliberately portable-ized versions of otherwise non-portable, or maybe you say "unclean" from a standpoint of leaving fingerprints or footprints behind, applications.

So the one thing I would add is that the LastPass people themselves have done a portable LastPass. So instead of using the normal LastPass, use LastPass Portable, which is freely available and downloadable, and then you've really got the best of both worlds. You've got Firefox, which is itself not going to dirty up the computer leaving anything behind; and LastPass, which you can be absolutely sure isn't going to do that, either. The problem with running non-portable LastPass and Firefox is that, although Firefox may be behaving itself, you don't know that the plug-ins you're running are going to behave themselves. And they certainly could reach out and go put stuff in the registry, which you're saying you explicitly don't want to have happen. So use the portable version of LastPass, and then you're good to go.

Leo: Perfect. Question 7, Ralph in California. He wonders about alternatives for Macintosh for reading PDFs. In Episode 276, "Testing DNS Spoofability," you encouraged listeners to find an alternative to Adobe Reader. And I think we mentioned Foxit. I use Foxit Phantom, which I love, on Windows. What are the best-of-breed PDF readers for the Mac?

Steve: And Leo, this is a question for you.

Leo: You don't need one.

Steve: That's what I thought you were going to say.

Leo: Because in fact that's really what's kind of killed the whole market for PDF readers for the Mac. Apple distributes Preview with Macintosh, which reads PDFs. If you want to annotate PDFs, there's a free open source program called Formulate Pro. It's what I use. Lets you take a PDF and annotate it. Whenever I get documents that I need to sign, I just open them in Formulate, paste my signature on them - it's probably illegal - save them out, and I've got a PDF with a signature on it. So you don't need it. Preview works great.

Steve: And, you know, Apple must have had a deal with Adobe a long time ago because of course the original Apple LaserWriter that was the first laser printer was using PostScript as its language. And we know that that's the basis for all of this PDF technology and so forth that Adobe has. So I would imagine some sort of license agreement was created back in the dim early days of personal computing which Apple has been able to cruise on ever since.

Leo: The NeXT Corporation used something called Display PostScript for its display layer.

Steve: Right, the entire system was PostScript-based.

Leo: It's my understanding, you know, I've asked this question because I'm not clear, did they license this? PostScript is open. And so I think...

Steve: So the specification is formally open.

Leo: Exactly. So I don't believe that Apple actually licenses the ability to read and write PDFs.

Steve: They don't need to.

Leo: Or to use Display PostScript. I think they wrote their own clean code based on an open standard.

Steve: That would explain why Adobe's not running around suing everybody, because they can't.

Leo: Whoops. I'm sure they would love to. Rick in Canada gives us our last question, which happens to be the Firefox Add-on Tip of the Week. Put echo in there later, okay? Steve and Leo, I found a great Firefox add-on. It's SSLPersonas. All one word, SSLPersonas. What it does is change the Firefox persona on the fly - I guess that's kind of like its profile; right?

Steve: Well, it's the way the whole UI looks, like coloration and so on.

Leo: Oh, everything, okay. So that you know you're on an SSL site, when you're on an SSL site it rewrites the look of the whole browser. Instead of needing to look for a little lock or the "s" on the "http" on the address bar or the green address bar, it changes everything. Check it out. Listener since No. 1, and a happy owner of SpinRite. Rick in Canada. Did you try it?

Steve: I did not try it, but I'm going to. I didn't because I've got so many tabs open that restarting Firefox is a major event.

Leo: I don't even want to restart Firefox, says Steve.

Steve: But I looked at the reviews. It looks really neat. So I wanted to recommend it. I mean, you might call this "in your face," SSLPersonas, because in the examples it turns the whole thing green, or the whole thing blue. It's able to essentially verify the validity of the certificate. So it's not just are you using SSL, but are you using SSL with a completely valid certificate, in which case it just, I mean, it really makes it obvious, which I think is nice. I like the idea that the UI is going to be really showing me the security of the page that I'm on. So I can't wait to restart Firefox after the podcast and give it a shot. But I wanted to share with our listeners because I think that's a great add-on.

Leo: Yeah. And you could always do - it doesn't have to be green. I mean, you could do something really silly.

Steve: Yeah.

Leo: You could say "safe." I like he's put locks and certificates and all sorts of stuff on it. That would be a great thing to do for less sophisticated family members.

Steve: Sophisticated, yes.

Leo: Say, "Mom, unless you see this, you ain't got it."

Steve: Right.

Leo: I think that's good, yeah. He has a bunch of different, I guess, templates that you can use. No Chrome version that I know of, but that would be a nice little Chrome extension, if anybody wants to write one.

Steve: Oh, and speaking of Chrome, there is a portable Chrome to go with, I mean, I'm sorry, portable Chrome and portable LastPass for Chrome.

Leo: Right.

Steve: So people who are Chrome users, as I know you are, Leo, can do the same portability trick with LastPass using the portable LastPass for Chrome, in addition to the portable LastPass for Firefox.

Leo: LastPass did everything right.

Steve: Oh, they really - and I will take this opportunity again to say I'm loving it.

Leo: I use it everywhere.

Steve: I mean, I really am. It's just I can't imagine now life without it.

Leo: Yeah, no kidding. Just done right.

Steve: And it's free.

Leo: Steve Gibson is at GRC.com. That's free, also. Lots of freebies. Lots of great free utilities, that DNS spoofability thing that we talked about, the DNS Benchmark thing that we talked about, there's all sorts of stuff. ShieldsUP! - why are you laughing? What do you call it?

Steve: The spoofability thing. The Spoofability Test.

Leo: Tester, yeah. Oh, there's so much free stuff there. I like Wizmo. That still works on Windows 7. It's great. It's like 12K of assembly code. It's tiny. And of course don't forget the bread and butter, which is SpinRite, the world's best hard drive maintenance and recovery utility, a must-have if you've got a hard drive.

Steve: I did run across three really fun testimonials just this morning when I was reading the email bag. So I'm saving those. I'm saving one of those for next week and for weeks to come. So...

Leo: Must make you feel good to get all those.

Steve: ...thank you for sending them. Yes, it does.

Leo: You're saving hard drives right and left. You can also find this podcast there, including 16KB versions, which are only available from Steve because he actually makes them. And he also gets the transcripts done by Elaine, so that's what you'll find there, all the show notes. We also have it, of course, it's on iTunes and the Zune Marketplace and at TWiT.tv/sn. We record the show every Wednesday at 11:00 a.m. Pacific, 2:00 p.m. Eastern time, at live.twit.tv. We invite you to tune in and join us in the chatroom, irc.twit.tv. It's fun, but you can always listen after the fact.

We have audio as well, and video, too, by the way, so you can watch Steve. And Steve sometimes does this show with his eyes closed and his hands like this, and it's really fun. Steve, always a pleasure. I am not going to be here next week. I'm in France. Tom Merritt will fill in, I'm sure quite capably. Have a great time next week, and we'll see you in two weeks.

Steve: Will do. Thanks, Leo. Talk to you in two weeks. And thanks so much.

Leo: All right. Take care.