SECURITY NOW!

Transcript of Episode #210

Listener Feedback #73

Description: Steve and Leo discuss the week's major security events and discuss questions and comments from listeners of previous episodes. They tie up loose ends, explore a wide range of topics that are too small to fill their own episode, clarify any confusion from previous installments, and present real world 'application notes' for any of the security technologies and issues we have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-210.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-210-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Music and Spinner.com, where you can get free MP3s, exclusive interviews, and more.

This is Security Now! with Steve Gibson, Episode 210 for August 20, 2009: Listener Feedback #73. This show is brought to you by listeners like you and your contributions. We couldn't do it without you. Thanks so much.

It's time for Security Now!, the show that covers your security - very important - your privacy and all that stuff. Steve Gibson is here, the man who discovered spyware, coined the term, created the first antispyware tool. He's a security researcher and expert engineer, the creator of SpinRite, the world's best hard drive maintenance utility, and the owner of GRC.com, which is a great website full of wonderful tools. And it's so great to see him in our fifth year now of Security Now!.

Steve Gibson: Yay.

Leo: At some point I will stop - I won't have to introduce you anymore. I'll just - no.

Steve: Wonder when that will be.

Leo: You know, Steve.

Steve: I don't think that's going to happen.

Leo: It's good to say it, in case there's people, new people coming along.

Steve: Well, and we do know, yes, I know from the feedback that there are people who are discovering the podcast. And they say, oh, yeah, this is the first one I listened to, or I just heard - I discovered you last month because my boss turned me onto it or something, and I owe him big-time kind of thing. So there are people who, as you say, have not been here for all prior 209 times you've said that.

Leo: Well, and that's really good because, if we weren't growing, we would be shrinking because, you know, there is some attrition.

Steve: There's attrition, yeah.

Leo: So it's important that we get new listeners.

Steve: New blood. New blood.

Leo: In fact, if you like the show, tell your boss, tell your employees, spread the word. Let people know they can hear the show. They can watch it live. We do it live every Wednesday at 2:00 p.m. Eastern, 11:00 a.m. Pacific on live.twit.tv.

Steve: Actually that's right now, Leo.

Leo: Oh, my gosh, we'd better get going.

Steve: That's what we're doing.

Leo: We release the show on Thursdays.

Steve: Hello.

Leo: And we have a Q&A today; right?

Steve: We do.

Leo: Yeah. Some great questions from our audience, and Steve's answers. But before we get to our questions and answers, do you have any updates?

Steve: Oh, we've got a bunch of security news and some errata, you betcha. The big news probably, I think this - because it's been a relatively quiet week. However, it was recently revealed that all Linux kernels based on the 2.4 and 2.6 series, since 2001, so over the last eight years, are vulnerable to a really bad privilege escalation attack. Basically it allows anyone with restricted rights to get root on a Linux machine. It turns out that it was discovered there were null pointer references in some rarely used protocol initialization structures in the kernel. And an exploit is available, and it is being used, that is, I mean, it's...

Leo: Oh, it's out there?

Steve: It's out there. Debian has updated immediately. Ubuntu has done the same. There's nothing yet for Red Hat Enterprise, but they have published a workaround. So I just wanted to let all of our Linux users know that it's definitely time to, based on what flavor of Linux you're using, check in with headquarters and see if they've got yet a fix for this. I guess there's a whole bunch of different Ubuntu flavors, also - Xubuntu and all kinds of crazy prefixes on the front of that. And they've responded. So everyone is scrambling. I mean, this is just like today and yesterday this is happening, when we're recording this on August 18th.

Leo: This is huge.

Steve: Yes, or the 19th. Yeah, it is big. So it's - from what I can tell it's not a remote exploit. That is, it's not like a protocol port. It's a local...

Leo: You have to have physical access.

Steve: Yes.

Leo: Oh, that's a relief.

Steve: Yes, yes, yes. So it's a way of writing code which uses not common protocols. For example, AppleTalk, IPX, the old...

Leo: That's the NetWare protocol.

Steve: ...NetWare protocol, exactly. IrDA, the IR protocol, X.25, Bluetooth, a version of INET6, the IPv6 protocol, and ISDN. So it turns out that, when you create a socket in UNIX or Linux, you specify the protocol the socket will have. The protocol that you're going to use - for example, you would typically use IP protocol, IPv4 for standard IP communications - that protocol then defines which operations can be performed on the socket. And if the operation is not defined for the protocol, you should have it pointing to a not-implemented procedure, basically. So that if you try to execute that procedure, it just returns an error saying this particular operation is not implemented on this protocol. It turns out that those not-implemented pointers are sometimes not filled in. And this has been the case for eight years. And somebody...

Leo: Really. For eight years.

Steve: For eight years. And so somebody - so there is now an exploit that allows elevation to root. That is, anybody can get root on any Linux that is - and they're all, I guess, based on the series 2.4 and 2.6.

Leo: They all use the same kernels, yeah.

Steve: Exactly. So for eight years it's been possible to do this.

Leo: Holy mackerel.

Steve: It was just discovered and published. So there's no need to have a fancy password to log in as root. Anyone can get root on your Linux machine. So it's something I imagine lots of Linux people will want to fix.

Leo: But that's always less of a risk if you need physical access. It's not like they can hack in from outside.

Steve: Yes, absolutely. It's not...

Leo: So, for instance, I'd be worried about my servers, which are all running Ubuntu. But you'd have to be at the network center, and you'd have to get in there.

Steve: Yeah, exactly. So the idea is, it's possible to write code which says - it creates a socket. It says, okay, I want to use Bluetooth. And then to execute a deliberately non-supported function against that Bluetooth protocol-defined socket, which will then, you know, causes problems because, instead of being returned - oh, this is not implemented on this socket - the return you get is something that allows you then to leverage this into a privileged escalation, and you're able to get root privileges.

Leo: Right. Of course we will update this. But the fact is that it's less of an issue.

Steve: Yes. Oh, I mean, if this were a remote exploit it'd be...

Leo: Oh...

Steve: It would be the end of the world.

Leo: Yeah, no kidding. I mean...

Steve: That would be really bad.

Leo: Anybody could take over any server. I mean, it'd be awful. Thank goodness, okay.

Steve: Yeah, yeah, yeah. Also we spoke last week about the UC Berkeley researchers who got a lot of attention for their discovery, their research which indicated that more than half of the Internet's top websites were no longer relying on browser cookies to maintain state, but were using Flash cookies, which are a lot less well known than browser cookies, for which there's no easy button to push, there's no UI built into the Flash player, it's just sort of an embedded thing. Whereas browsers, the user interface on the browser allows us to say, oh, I don't want to allow - I want to disallow third-party cookies, or I want to treat them as session cookies and so forth.

It turns out that a major provider of web analytics, a company called Quantcast, had been, for who knows how long, one of the services they were offering to their clients, Hulu being one that was mentioned, was to reinstate browser cookies that the user deliberately deleted by using the Flash cookies.

Leo: Oh. Cookie flash thing, yeah.

Steve: And we've talked about this a couple times. The idea being that the user says, I want this to be a session cookie; I don't want you to remember me. Well, Quantcast said, oh, guess what. As a service, since we've got code running on the website, we'll use Flash cookies, which are stickier, to basically respawn any browser cookies that are deleted. So the problem with that, of course, is that, as we know, and I'm annoyed by this because this is one of those things that unfortunately is opt-out that should be opt-in, the whole cookie deal, but all browsers still have third-party cookies enabled by default, which enables tracking, as we've described. But for users to deliberately disable them, that would imply user intent. That is, they didn't disable them by mistake. They weren't disabled by default. Someone had to say, I know what I'm doing; I don't want to be tracked. And so for a company to come back and reinstate those where, you know, basically overriding the wishes of the owner who's visiting the website, seems really bad.

Leo: Oh, yeah. Oh, yeah.

Steve: Well, the good news is, the day after this report came out, they stopped it.

Leo: Good.

Steve: So I think they recognized preemptively that they were about to be in a world of hurt because people like us would be saying this company is doing this and it's really bad. So they formally said, hey, we're not going to do that anymore. People who delete their cookies are expressing their intent, so we're going to honor that intent. It's like, well, good.

I don't know if you saw the story about Palm getting some heat about the Pre tracking?

Leo: Oh, yeah. It's phoning home.

Steve: Yeah. And this is what surprised people. Arguably, down in the fine print, it may say that that's okay. But for our listeners who haven't heard, the Palm Pre turns out to be providing geolocation information about all Pre phones, even when you're not using location-based services. Which was really the gotcha. It's not that, you know, you can imagine that the phone is providing benefits based on GPS and standard state-of-the-art geolocation services. The problem is, the Pre is sending back your location to the mothership continuously, whether you're using geolocation or not.

And it did bring up, though, a secondary aspect, which is - and I guess this is maybe not such a big deal. But, for example, even the Apple iPhone, third-party apps are able to query the iPhone for its location. And nothing prevents them from leaking that information back out to wherever they want to.

Leo: The iPhone does say, "This third-party app wants to know your location. Okay or not?" So you're queried every single time. Even if you say yes, the next time you launch the app it will ask you again.

Steve: Okay. So at the OS, where the app is trying to say where is the phone, that brings up a dialogue that the app is unable to interfere with or suppress.

Leo: Apparently. I mean, it may be some bug.

Steve: So you're giving the app permission.

Leo: Yes, exactly. You have to give it explicit permission each and every time.

Steve: Right.

Leo: Now, it is an interesting point, and somebody made this point when I talked about this on the radio show, that the phone company knows where you are. It has all that information. It may not have it as granularly because it's by cell site.

Steve: By cell tower, yes.

Leo: As opposed to, you know, the longitude and latitude, which is accurate to a few meters. But we kind of know that, and we accept that with the phone company. For

Palm to know that is a little much. And Palm, by the way, while acknowledging it and apologizing, didn't say they were going to stop.

Steve: No. They said that's part of what the phone does.

Leo: It's what we do. It makes it easier for you.

Steve: Yeah, in fact, it's funny. You were talking about the comment raised about how cell companies know where you are, I mean, that's now - that's in the common culture enough so that when we see - we're watching TV or a movie or something, and somebody's on the cell phone, it's like, okay, hang up, hang up, take the battery out. Don't you know they're going to track you?

Leo: Right.

Steve: I mean, it's just - we all know that now.

Leo: We know that, yeah. But we don't assume that the handset manufacturer's keeping track of that.

Steve: Yeah.

Leo: Wow.

Steve: And you have to wonder why. I mean, and they say, oh, it's part of all the value-add. We're going to provide you services that are enhanced because, if we know where you are, we can tell you where the nearest pizza is or something. I mean, okay.

Leo: Hmm. Hmm.

Steve: Yeah. Real Networks, we talked about this about a year ago, has been fighting and continually losing their battle for their product called RealDVD. RealDVD is a technology which allows people to copy DVDs to their computers. It's supposed to make it easier for them to watch DVDs. They're not able to duplicate them. And they are still encrypted. But Real Networks has contended that, hey, this is not a breach of anyone's copyright because it's still only viewable on the machine to which it's been copied, and how is that different that putting the disk into the machine's own DVD player and running a built-in DVD movie player app? Unfortunately, Paramount, Sony, Universal, and Disney all disagree. A temporary injunction has just been turned into a preliminary injunction, strengthening it, and essentially preventing Real from continuing to sell; well, they have been already prevented. But, I mean, this strengthens it to the point where the next step now is to go to trial.

So I just wanted to move us forward in this saga. Apparently Real, in order to do this, did sign licensing agreements in order to access the DVD decrypto technology. So they're a licensee, a formal licensee of that, as you'd expect. And the argument is, well, you're breaching your license by doing this. You are decrypting the DVD in a way that we're not happy with. And so Real is having to defend themselves.

Leo: Yeah. Motion picture industry, as usual, not too happy with this kind of thing.

Steve: With any kind of use that they don't have complete control over.

Leo: They essentially say you don't have the right to back it up.

Steve: Right.

Leo: You can't even back it up.

Steve: And in another little bit of weird randomness, Twitter was found to be used controlling a botnet, not surprisingly. A botnet was following a Twitter account. And somebody was using Twitter, literally, sending tweets to Twitter. And all of his bots were following him, and it's how he was - that was his command-and-control channel for the botnet. This was discovered after the denial of service attack problems that we talked about last week. A researcher looking closely realized there was some strange traffic on one channel, and they closed the account. And apparently the same person was using Jaiku prior to that.

And it turns out that, increasingly, botnets are finding new and sort of unique ways of phoning home and staying in touch with their owners. One that I thought was particularly interesting is that the botnet clients, the bots themselves, will issue strange search queries which would normally not turn up anything. But the owner of the botnet fleet knows what search queries his bots are going to issue. And so he can then create a website which the search engines will find and index, and then the weird queries result in hits against that site that allow the bots to find code to update themselves.

Leo: It seems odd that you would do that in a public place like Twitter. I mean, it's so much easier just to have an IRC server secretly running. Twitter, it's so obvious, you know?

Steve: Yeah, exactly.

Leo: He was discovered right away.

Steve: Exactly, because it's exactly the sort of little messages that are being broadcast by Twitter is that.

Leo: Yeah.

Steve: So, I mean, it wasn't very inspired, and it didn't last very long. They saw it, they closed it down, sorry.

Leo: I like dumb hackers like that. Give me more of them.

Steve: We wish everyone was a little slow.

Leo: Yeah, those are the ones I want.

Steve: And next week's topic is going to be a nice, deep, serious, techie, you know, back to Security Now! style, a detailed look at hacking a voting machine, how it's done. Because at the USENIX '09 eVoting Workshop, some researchers from a handful of universities revealed their research into how what was believed to be one of the least hackable eVoting machines, which is widely used in the U.S., how they managed to take it over. And it's really interesting because it's not based on Linux or Windows or any of these, like, big OSes that would immediately make me just sort of sigh and wonder why this approach was taken. The machine runs on a Z80 chip, and with a very small amount of code. And what's really interesting is that it's a so-called "Harvard" architecture as opposed to the traditional architecture where instructions and data are all mixed together. And we understand the danger of that because everything that we're hearing is how data is being misunderstood as instructions, and so data is being executed.

Well, the developers of this said, oh, not a problem. We're going to create a really tight, small, beautiful little eVoting machine - and they did - where the hardware itself will prevent data from being executed. That is, ROM, the code will be in ROM, and of course data will be in RAM. And it will be impossible for the chip to execute commands out of RAM. It can only execute the ROM that we provide. And these guys found a way around that such that it is possible to change the outcome of voting.

Leo: Wow.

Steve: So we're going to have fun next week with looking at exactly how that works.

In errata, I referred to, incorrectly and improperly, DynDNS as something that, I mean, I was wrong in thinking that it was sort of a hobbyist, not to take seriously DNS service. I've run across it because it's possible, for example, to set up a DynDNS account and have your residential router stay synchronized so that you're able to create a domain name, a DynDNS domain name that will always point to the IP of your router to allow you to find it if your ISP, using DHCP, should assign your router a different IP. Because as we know, while DHCP-assigned IPs are relatively static, they're not absolutely fixed. So it's necessary to have some sort of a system that will be able to track the IP if it changes. And I was - we were talking about Twitter and the fact that they use DynDNS. And I said, oh, my goodness, I mean, get a real DNS service.

Leo: Well, to your credit you said, "I read this"; "I'd heard this." You didn't say "I know this for a fact." I mean...

Steve: Right. Well, it turns out that DynDNS has grown up a lot since I last saw them, and they have an enterprise-class service which is robust and strong and serious and solid. And so the fact that Twitter is using that in no way weakens Twitter. And in fact this was not an attack on DNS. The reason - what I read was that there was an increase in traffic to DynDNS due to the attack. But, I mean, that also follows because remember that the first thing that happens when you do a lookup of anything on the 'Net is you've got to get the IP address. So if a whole bunch of clients were, as we now believe, essentially clicking on links on Twitter blogs, then all those clients would be referred, would have their DNS lookups performed by their DNS server that would query DynDNS to get the current IP of Twitter. But it's not, literally, dynamic DNS because there is a whole other enterprise class service, you know, big iron DNS, which the same folks offer who offer the home router version with a very different targeted audience.

Leo: Excellent. Well, so our apologies. And we've corrected that, yeah.

Steve: I keep hearing people in our feedback telling us they love our minor divergences from security. One, of course, is our favorite, is sci-fi. And so I have to just say that I loved Peter Jackson's "District 9."

Leo: Yeah. Now, don't - no spoilers because...

Steve: Oh, I'm not spoiling anything. Oh, my...

Leo: Yeah. Because apparently it's best to know as little as possible before going in to see this movie.

Steve: It is a spectacular piece of work.

Leo: I can't wait to see it, yeah.

Steve: So I wanted to - any of our listeners who are sci-fi people, I just wanted to say "District 9" is really good. I mean, in a very different way. I mean, I would say it blows the most recent "Star Trek" movie away.

Leo: Wow.

Steve: Which I also loved.

Leo: And that was an excellent movie.

Steve: Yeah, but it was - oh, okay, yes. It was an excellent movie. I loved it. I'm glad we're going to have more "Star Trek" movies. But "District 9" is in a class by itself. I mean, it is fantastic science fiction. So...

Leo: I heard people say their reaction to this was the same as when they saw "The Matrix" the first time. It was just like [small exclamation].

Steve: Yeah.

Leo: I can't wait to see it.

Steve: It was, I mean, I went with a couple friends. And we were just, like, turning and looking at each other with our mouths hanging open during the movie. It was like, my god, this is good. It was just - it was spectacular.

Leo: I can't wait.

Steve: I also picked up a comment, I don't remember now why, but I was watching you, Leo, on the weekend, on your Tech Guy show. And a caller was talking about their drive clicking.

Leo: Yes.

Steve: And the drive was no longer working, and it was clicking. And I hear that enough that I just wanted to address that briefly. And this is not a pro-SpinRite story. This is unfortunately something that's not SpinRite nor anything else except serious, serious drive repair can fix. That clicking is what the drive does when it is arguably at or past life, unfortunately.

Leo: Oh.

Steve: It is the - the drive will put the heads out on the surface and try to obtain a servo lock. Which means it's looking for the special non-data servoing information which is now stored periodically around the track. If you imagine two different signals which are out of phase, like a sine wave signal where from left to right that sine wave diminishes in strength. And then there's another sine wave that's 180 degrees out of phase, meaning that its peaks and valleys are the reverse of the first one. And its strength increases from left to right. So that sort of creates almost sort of a "V" shape. And imagine that the head running down the middle is now receiving both sine waves, the in-phase and the out-of-phase one. Well, as it drifts off track, the signal it gets, which is the composite of both, will start to change. And it can tell by which way the phase changes which direction it's off. And so by moving back to the center and, like, nulling out these two competing sine waves, it's able to stay on track.

Well, that's a good visualization of how servoing works on contemporary drives. And so those little servo bursts, as they're called, occur periodically, and they give the drive-servoing technology, the head-positioning technology, periodic updates on where it is as it moves along the track. Well, the drive's ability to lock onto this servo information is, like, it's the first thing it does when it puts the heads out. If it's unable to acquire that servo information, it'll wait a bit, and trying, moving the heads around, looking for it. And if it can't, it retracts the heads in what's called a "recalibrate operation," and puts them out again. That's the click you hear.

So that clicking is the drive's inability, essentially, to get itself going. So what happens is, when you power the drive up, the platters spin up to speed, which causes the heads to begin flying over the surface. And once the system sees that the platters are up to speed, it then sends the heads out in order to go to the first cylinder and obtain their servo lock. If they can't, it retracts the heads, waits a little bit, and just tries again. There's nothing else it can do. And so what you hear is a clickitic, clickitic, clickitic, clickitic.

Leo: Uh-huh, uh-huh.

Steve: And it's not until the drive achieves that servo lock that it then lights up the API, that is, it lights up the interface and says, "I'm online." So essentially the drive is offline. It's not - it isn't paying attention to its interface. There's nothing any software can do. There's nothing anything, anyone can do. Sometimes this is where you put the drive in the refrigerator because that's an old-school approach. But, I mean, you're literally - you don't have many boots left of this - on a drive that's doing that.

Leo: Well, now, let's distinguish that between a drive that's having trouble reading a sector and trying over and over again. That sounds a little bit like a clickety, too. That's like an eh-eh, eh-eh, eh-eh.

Steve: Yes. There can be that. And in fact SpinRite will generate that because one of the things that SpinRite does is it moves off in either direction to random distances and then comes back at the sector, hoping to get a slightly different head positioning to allow it to obtain a good read on the sector because all of this, there's like - there's a little bit of slop in all of this. There's the drive, for example, in that servoing example, the drive doesn't recorrect its head position until the error signal is enough in one direction or the other to tell it that it's got to move the head back into the center. So it's got to be a little bit off center before it knows to recenter. So retrying, which is one of SpinRite's success strategies, often works. But I guess there's a - it's a louder, sort of distinctive sound which you will hear shortly after you power up the system where the drive is just kind of going geklunkit, geklankit, geklankit, geklankit, geklankit.

Leo: Hmm, that sound, yeah, yeah, I know that sound. Yeah, yeah, yeah. It's distinctive. If you've not heard it before...

Steve: Yeah, and you don't ever want to hear it.

Leo: Yeah.

Steve: But your caller did hear it. And the problem is that drive has not declared itself online. So the BIOS won't see it. SpinRite won't see it. Nothing will see it. It's literally - it's not - it's ignoring the cable connections to the outside world. It's just trying to get itself going. And then it would turn around and say, okay, what do you want me to do? It's just not even there. And so if you had - if you can't get it not to do that, that is, if that's all it will do, even putting it in the refrigerator for a few hours and trying again, and you absolutely have to have the data, that's beyond SpinRite. It's, like I said, it's not even - it's not online. That's where you have to say, okay, and take it to a professional data recovery service that takes the drive apart, literally. I mean, you're at that stage. And that's typically lots of money.

Leo: Very good. Thanks for that clarification.

Steve: And that's all I have.

Leo: [Laughing] And, I'm done.

Steve: We have a bunch of great reactions to last week's...

Leo: I'll tell you, I've been taking Vitamin D every day since then.

Steve: Well, great. There's something funny around in the middle of them that you're going to get a kick out of. But it's true. But so today I wanted to let people know we will, trust me, we'll be back to security big-time next week. But reactions were phenomenal from last week. And so I wanted to share those with our listeners today.

Leo: And we do have a lot of security questions, too, so don't fear that. Steve, you ready for some questions?

Steve: Absolutely, questions and feedback and comments.

Leo: So, question number one, Anthony DiSante listening in Pennsylvania wrote to say the occasional off-topic shows are great, for example, Vitamin D: Hi, Steve. I'm a long-time listener of Security Now! and a couple of Leo's other shows, too. This week I actually listened to my podcasts out of order, skipping MacBreak Weekly - what? - because I couldn't wait to hear about your Vitamin D research. Thanks for sharing these kinds of non-security topics. I'm sure I speak for many other listeners when I say that, after coming to know and love you as "the security guy" for so long, it's nice to see another side of you, while learning something interesting at the same time. Speaking of off-topic stuff, is there anything exciting to report on the super-capacitor front? Oh, yes. That was an interesting subject we talked about some months ago. Maybe it's time you started a second podcast: "Vitamin D and Supercapacitors Now!" Doesn't that roll off the tongue. So, yeah, thank you. I'm glad - and I've been taking my Vitamin D. I've got my D3.

Steve: Yup.

Leo: Poppin' that every day.

Steve: And I just wanted to say, I mean, I was - well, basically all the feedback that we received was about last week's episode, not surprisingly. There were a couple grumpy people who said, hey, if I wanted to have a health podcast, I'd go subscribe to one. I listen to Security Now! for security information, so stay on topic. And it's like, okay. I mean, I really do understand that. And I want to reaffirm to everyone that this is a security podcast and that next week we'll be back to where we've always been for the last four years with more full-strength security stuff than ever. At the same time, my hope was that this would be interesting and useful. And from all the feedback that I got, I think we really scored there big-time.

To the degree that anything else like this happens again, I think I've sort of established my interest as a health hobbyist among our listeners. I'll just make a reference in the errata time at the beginning of a podcast to go check out a certain page at GRC and leave it at that, trusting people to be able to do that if they choose to. So I wanted to acknowledge the couple people who said, hey, they wished that we'd stayed on security topic. At the same time, the response was phenomenal from everyone who said, wow, I didn't know what you told us about, and that's really why I listen is to learn things. So I just wanted to acknowledge that. And relative to supercapacitors, we'll certainly keep our eye on those and let our listeners know.

Leo: But nothing to report so far.

Steve: Not at this point.

Leo: There's still a few months left in the year. They can still do it. Eliezer Martinez in sunny and Vitamin D supercharged Puerto Rico says: Great Vitamin D episode! As a medical technologist - we are now called clinical laboratory scientists - I rate your Vitamin D episode A+. Aside from a couple of small errors (technically, fungi does not equal plant) - yeah, of course not - you handled your dissertation on the subject like a science major. It proves once again you really do your homework. I'm impressed!

I don't think you are going to get any backlash for a non-security episode. Not everyone who listens to Security Now! is a computer whiz, but everyone who listens is smart. I would agree with that. Funny how I am a lab professional with a computer hobby while you are a computer pro with a medical hobby. Yeah, there you go. Keep up the good work. Don't hesitate to bring to our attention anything that's really important. P.S.: Is Vitamin D intake via HTTPS a feature of CryptoLink? Just kidding.

Steve: So again, just I wanted to share some of the feedback with our listeners sort of generically and to thank everyone for having responded.

Leo: Robert Wicks in Atlanta notes that Vitamin D is especially important for black people: Steve, I wanted to let you know that your information on Vitamin D was very valuable, even for non-Caucasians. I'm African American and was unaware of the incredible importance of this hormone, although because of the skin pigment I'm at a greater risk of having an insufficient level of it than you are. I am a UNIX sysadmin. Sun is in short supply in the server room. I would expect that. Additionally, my wife recently had her thyroid removed and has had to take vitamin D and calcium supplements following her surgery. We are going to have our blood checked and speak to our family doctor about all of us taking Vitamin D going forward. That's great, Robert. Thank you for what was, as you said, the most important podcast you've produced. It is if, you know, if people are healthier because of it, that is pretty important.

Steve: Yes. Again, we've never missed an episode. And so I wanted to, to the degree necessary to explain to people why I went off topic, it's because I really - I ended up as a result of studying this for several months thinking, wow, this is just something, some information that I think everyone should have. And from the feedback that we received that was all like this in various ways, I think the factual basis for what we were able to explain surprised a lot of people.

Leo: Yeah, I think it's just fascinating. Jim from Newfoundland, Canada has a comment about Vitamin D and rickets: Hi, Steve. Right now I'm listening to your latest Security Now! podcast. Had to pause to send you this message when you mentioned the resurgence of rickets as a result of Vitamin D deficiency. A few weeks ago I was watching a YouTube video by Pat Condell wherein he mentioned that more children were being born with rickets to Muslim women who don't get enough sun on their skin due to wearing the full body covering called the "burka," which only leaves the eyes and hands uncovered. I have included links to the video and the article he references in support of that claim.

I appreciate that you have deviated to a certain degree from the standard security format. I think it's good you've done so. Geeks can oftentimes have much more exposure to light from a computer monitor than from the sun. So your advice should be taken as a word to the wise. In order for us to keep the body's security defenses in good protective order to guard against infection or breakdown and help extend the mean time between failure of the bodily system, your advice on Vitamin D should really not be considered a deviation from format at all, but merely sage advice on patching a known system vulnerability. I like that. May I suggest you tack on a 15-second reminder to the end of each podcast just to remind us to get out in the sunlight for 15 to 30 minutes of exposure to natural light that we need to keep fit? Thanks to both you and Leo for valuing listeners enough to pass on this health concern.

Steve: Well, I'm not going to be bothering our listeners all the time about it. You know, Leo, you do well at tossing in reminders like that. So I'll let you do that when you think it might be important. I did run across a lot of comment in the research specifically about Saudi Arabian women and the extra problem that they have because of the burkas, that they're literally, even when they're outside, not getting any incidental sunlight. And not surprisingly, I mean, we learned that age decreases our skin's ability to make D; that sun is, you know, exposure to UVB from sunlight is essentially the only natural source, aside from some food sources, but that's only really fatty fish; and that lacking the sun and sufficient youthful skin, there's no source for D. Yet it's, as we know, not a vitamin. It's an important hormone for our body. And so the more, for example, computer guys are inside, as some of our comments have written, receiving radiation from a monitor and not from the sun, the less opportunity we have to make that. And it can get really critical.

Leo: All right. We have time for one more. Normally we would do 12 questions, but these are all Vitamin D questions, so we'll hold them for another time, another day.

Steve: Or not. I think we're done with Vitamin D at this point. I don't want to...

Leo: You got a lot of mail about this. It's obviously an interesting - a topic that's interesting to you.

Steve: It was a phenomenal response. I mean, hundreds of responses. And so, yes. But I think we've done it. People know where to find some more about it.

Leo: You get the idea, folks. Yeah, yeah. Well, actually that's a question from Phill, Phill Moore in Sydney. He's wondering about a book called "The Vitamin D Cure." I was reading a blog post by a personal trainer named Tony Gentilcore - good name for a personal trainer - and he recommended everyone should read "The Vitamin D Cure" by James E. Dowd, M.D. After last week's podcast, I figure this is right up your alley. Thanks for all the great work. Do you know that book?

Steve: I do know it. I own the book. And it was the first book I stumbled on. And what happened was I was reading the book. There were lots of references in the literature to studies. And it was - but for me, I really wanted to go to the source material, which is what our listeners heard from me last week. So I began digging into the actual research. I ended up finding a book that I like a lot more than "The Vitamin D Cure." It's called "The Vitamin D Prescription." I have a picture of it and a link to it on the GRC.com/health Vitamin D page. And that's the book I would recommend, for example if our listeners have family members or relatives or something who might be interested in reading something. It is very well written. And basically it exactly follows the literature. So it's sort of a gentle, nice introduction to the topic, which is a real-world reflection of what all the research is. And I think that's my favorite book of all to recommend to people who would want to turn on to this.

Leo: Say it again, say the name?

Steve: It's called "The Vitamin D Prescription."

Leo: Okay. I'm sure that's in bookstores. There's been a lot of talk about this all around, in general. People are very interested in this.

Steve: I think we're probably at the tip of a so-called tipping point, where a lot of - it's beginning to get buzz. It's in the news. It's just it's so annoying that a blood test is really the only way to know where you stand, I mean, because people tend to shy away from medical procedures. No one wants, I mean, I'm doing it every week, forcing myself to because I'm really wanting to experiment with sun production in my skin. And it's not fun to be stuck with a needle.

Leo: No.

Steve: And it's just it's too bad there isn't a better way to know. But it's funny, many people prefer not to know. And I completely understand that, too, because you can sort of say, oh, well, I'm probably getting enough. But I was hit with this low number, it's like, whoa, okay. I am a computer geek who goes from one cave to another and never gets much exposure to the sun.

Leo: Yeah. Me, too.

Steve: So, yeah. Anyway, I'm glad that we've sort of alerted our listeners to it. We will be back to security, full speed ahead, next week with a really neat episode about the inner workings of what looked like a bulletproof eVoting machine and how it turned out not to be.

Leo: Yeah, there's another one where I'm just - eVoting. Boy, the more I...

Steve: It just makes you nervous.

Leo: Yeah, yeah. It's funny because you expect people like you and me who just love technology would be jumping on this bandwagon. And every technologist I talk to, the more you know about technology, the more you realize what a bad idea this is.

Steve: Yeah. On the other hand, you've got hanging chad and dimpled cards. So it's like, that doesn't seem to be a good solution. Although, arguably, the eVoting problem can be much more sweeping because - in the same way that anything in the physical world is pretty much restricted to just that one instance. If a particular machine had wide, really widespread adoption, and it turned out to be vulnerable and exploitable, as so far many of these have, that's a huge problem.

Leo: Yeah. Well, Steve, great stuff, as always. I look forward to next week. We'll be talking about voting machines. If you want to know more, you know where to find him, GRC.com. And the Vitamin D stuff is at GRC.com/health. All the links are there.

And we'll - that'll be it on that. Except I do want you to report back when you get the final results.

Steve: Absolutely. Will do.

Leo: I'd like to know how that's going. But next week voting machines. GRC.com for SpinRite, the world's best hard drive maintenance and recovery utility for all those great freebies that Steve gives you, like Wizmo and DCOMbobulator, ShieldsUP!, we can't forget that. It's all there: 16KB versions of the show; transcriptions, too. GRC, that's short for Gibson Research Corporation, dot com. Steve, we'll see you again next week.

Steve: And as always, GRC.com/feedback...

Leo: Oh, yes.

Steve: ...for all of your ideas, questions, comments, suggestions for future shows and so forth.

Leo: Very good.

Steve: Talk to you then, Leo.

Leo: Bye bye.