SECURITY NOW!

Transcript of Episode #558

Listener Feedback #233

Description: Leo and I discuss another interesting week of security news including the U.S. Congress's passage of the Email Privacy Act, the Snowden/Zakaria encryption debate, the still unresolved question of compelling fingerprint unlocking, more Android trouble with Stagefright, WhatsApp going dark in Brazil again, the return of Who Is Satoshi, Steve's fabulous new puzzle discovery, and more. Plus some more questions from Security Now! listeners if we have any time left.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-558.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-558-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson's here. He's got a wrap-up on all the big security news, including his take on the Satoshi Nakamoto drama playing out right now with Dr. Craig Wright. He also talks a little bit about new problems with Android. Yeah, there's another Stagefright bug. And we'll answer five more questions from our great audience. Security Now! is next.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 558, recorded Tuesday, May 3rd, 2016: BitCon.

It's time for Security Now!, the show where we cover your security and safety online. Makes it sound scary. It's actually a great show, a fun show, where you learn a lot about technology with this guy, Steve Gibson. Hey, Steve.

Steve Gibson: Hey, Leo. Great to be with you again. We only got four of our nominally 10 questions in last week because we had so much to talk about. And I have a similar concern this week because there's lots of fun stuff has happened. Congress has passed an Email Privacy Act. Edward Snowden and Fareed Zakaria debated for an hour on the issue of encryption. We still have this question of can you be compelled to have your finger pressed against the iPhone unlock button up in the air. Android has continuing problems with the Mediaserver module which of course we're introduced to with the exploits known as Stagefright. And Google has in fact renamed their monthly security now from "Nexus Security Update" to "Android Security Update," acknowledging that Android ecosystem is bigger than just Nexus. WhatsApp was ordered shut down again by the same moron judge. And we found out what WTF is in Portuguese. Then of course everyone wants to know...

Leo: But it's back, you know. The higher court overturned it once again.

Steve: Yeah. One hour.

Leo: One hour.

Steve: I mean one day. It was supposed to be out for 72 hours; and it's like, okay, it's back up the next day. And it was the same judge.

Leo: Was it? I thought it was a different - it's a different case though; right?

Steve: Different case, same judge.

Leo: Oh, how funny.

Steve: He just is annoyed.

Leo: He doesn't like it.

Steve: Yeah. And then the question is do we finally know who Satoshi Nakamoto is. And it's funny, too, because in my show notes I put, "Will the real Satoshi Nakamoto please stand up." And I thought, I wonder if our audience is too young to understand that reference?

Leo: No. Oh, you don't see - okay. So here's the thing, Steve. You're too old to understand that reference. You're thinking about "To Tell the Truth."

Steve: Correct.

Leo: And our young audience is thinking about Slim Shady.

Steve: Who?

Leo: Yeah, see, okay. It's an Eminem song: "Will the real Slim Shady please stand up."

Steve: Yeah.

Leo: So it works. But this is one of those rare multigenerational references.

Steve: Nice. Nice. Well, then I'll keep that in my repertoire. And I have discovered a new puzzle. And so far I'm batting, what is it, a thousand is good. A thousand is perfect, as I understand it.

Leo: Well, I brought back Blek for iPad Today yesterday because it was such a great game. And I'm ready. I'm ready for a new one. Let's do it.

Steve: Well, good. Because that's the best-named one I've come up with, or that I've seen.

Leo: Blek?

Steve: Yeah, I'm not a fan. I'll explain why.

Leo: Oh, okay.

Steve: It's just it's not my kind of thing. I like more of a sort of a strategy...

Leo: Something cerebral.

Steve: Yeah, thank you.

Leo: That was more of a kinetic puzzle, yeah.

Steve: Lots to - and Blek is, if nothing else, it's kinetic. So we have lots to talk about this week. And maybe, if we have time, we will continue with some questions because we were on a great roll there with those first four that everyone liked last week.

Leo: They were awesome, yeah.

Steve: We ran out of time. So we'll see. We'll play it by ear. Maybe we'll do some more Q&A if we have time.

Leo: Another great Security Now! all queued up.

Steve: Lots of stuff. So we did have a nice little bit of legislation coming out of the Congress.

Leo: I thought it was kind of telling. Congress hasn't passed a bill unanimously in years.

Steve: No. And the fact that this was unanimous in the House, given how partisan the House is, this just says - what it means is it will just cruise through the Senate because now this thing goes from the House to the Senate. The Senate will say fine. They'll bless it. And then it'll be sent to the President for his signature. So this is the Email Privacy Act which updates what was a 30-year-old law, the Electronic Communications Privacy Act, called the ECPA, of 1986. So, yeah, maybe needed a little bit of updating.

What this does is requires the government to obtain a probable cause warrant from a judge before obtaining private communications and documents stored online with companies such as Google, Facebook, and Dropbox. The EFF supports this and was jumping up and down, and they were happy this passed. They did note, though, that one thing it did not do is require any notification by the government that this was being done to the user accounts where it was. So this still allows for secrecy. And the EFF considers that notification is important because it would then allow users to obtain some legal counsel to lobby for their rights. So the EFF wasn't totally happy. But this was a nice big step forward.

And this also upheld, or it codified, rather, a previous appellate court, the Sixth Circuit Court's ruling that the Fourth Amendment demands that the government first obtain a warrant before accessing email stored in cloud service providers. So there had been some case law, but it hadn't been - but that was just decided by a court and attorneys arguing. Now it's been codified as formal doctrine. So this is nice. And great to see this, as you said, Leo, unanimous is like, whoa. Nobody said no? So that's...

Leo: I think what it tells you, what it tells me, is they're a little nervous about - because the whole thing was, you know, up to this point, actually it's still the law, anything older than 180 days is abandoned and doesn't need a warrant.

Steve: Right.

Leo: And I think that...

Steve: So half a year.

Leo: ...they realized, oh, crap, they're going to be able to read our email. There goes Dennis Hastert on his perp walk from old stuff. Maybe we'd better get some better protections for us. That's about, I bet, I mean, that's cynical of me, but I think that's maybe got something to do with it.

Steve: No, it's a very good point, Leo. Very good point.

Leo: I mean, it's unanimous. It's got to be something like that; right?

Steve: Yeah. It was surprising.

Leo: Yes.

Steve: And what it does mean is, unlike many of these things, I don't expect this to die. It's not going to die in the Senate. If it's unanimous in the House...

Leo: Oh, no, it'll go through, yeah.

Steve: It'll just cruise right through.

Leo: They all have skeletons in their email. Every one of them.

Steve: Yeah. And I see no reason why the President would not sign this into law. It's like, seems like a good thing, so. And, I mean, it keeps with this notion that the Constitution provides against overreach, where you have to convince a judge that there's probable cause for search. And so this follows that model.

Speaking of which, this was the argument that Fareed Zakaria had in his debate with Edward Snowden. There's something called the Debates of the Century series. And I perked up when I heard that some notable billionaires were funding this. And so they're a series of sort of high-end debates being held about significant questions. And they were debating - oh, I'm sorry, Fareed and Edward Snowden, who was there of course by telepresence. He was in Moscow. And Fareed is arguably my favorite CNN guy on Sundays. He has a Sunday show, "GPS," Global Public Square. And I just - I like his approach. It's sort of no-nonsense. It's clean. Maybe a little academic, but also grounded.

So he debated with Edward Snowden the motion, quote: "Government should have lawful access to any encrypted message or device." That is, you know, they're debating the question of, as we call it on this podcast, DOD, Decryption On Demand. Should that be the way the law is? It's an interesting debate, although - and I watched it this morning. And I didn't feel that we learned anything new. I was a little distraught by Snowden being a little cute. I think, I mean, he's been the focus of this question for so long, he's developed some anecdotes. And from my standpoint, when I see somebody saying something that's important, which is arguably wrong, but is being stated as a fact, that's a problem. I mean, opinions are fine, but facts are facts.

Now, they did an online poll of the audience and their online viewers because this was being streamed. I don't know how many, how large the sample was. We didn't see a viewership number. But before the debate began, the moderator gave everybody a text message number where they could text how they feel, that is, government should have lawful access to any encrypted message or device: no, yes, or undecided. Before the debate, no was a little over three quarters, 77%; yes was 13; and undecided was 10. After this hour-long discussion, no dropped to 69, and yes went up from 13 to 22, and undecided dropped a little bit, well, by 1%, to 9%.

So for what it's worth, Fareed made some good points. And Fareed's position, frankly, was my position, which is that he's had smart people tell him that this could be done if we wanted to do it. Edward Snowden's position was there's no possible way of - it's just not possible. He kept using things like outlawing encryption, and we know this is not about outlawing encryption. "Governments should have lawful access to any encrypted message or device" is not about outlawing encryption. It's about putting in the law a means for providing access, which is different from outlawing encryption.

So anyway, I made it the bit.ly link of the week, for anyone who's interested. It was a good discussion. But there was nothing dramatically new brought forward. So at bit.ly/sn-558, if anyone wants - that just bounces you to the YouTube video. I think, with the introductions, it's a little over a hour. And, you know, I enjoyed it. And these are the arguments that we've seen before. And the question of our era at the moment is where will the law come down? And there were some interesting points made. So, but, again, nothing earth-shattering.

And we still have this fingerprint compulsion question, like, in the wind. Actually, all of these things are still up in the air, even can you be compelled to give testimony against yourself in the form of your passcode if you're not using biometrics. This was brought back into the news because an L.A. judge or court ruled that the girlfriend of an alleged Armenian gang member had to press her finger against an iPhone which had been seized from a home in Glendale, where it was believed that this iPhone would contain important evidence in a case.

So as we know, we've talked about this before, this whole question of is a biometric, because it's something you are, not something you know, the argument has been that it doesn't qualify as testimony. And so what the Constitution protects is self-incriminating testimony. And so there have been arguments that compelling someone to release a passcode is requiring them to testify against their interests.

Well, there are scholars that believe that this can be, that argument can be extended to unlocking a phone; that if a phone contains incriminating evidence, then even though it's sort of one step removed, the same law applies. So the Supreme Court has ruled, at the Supreme Court level, that police can search your phone if they have a warrant; and, separately, that they can order you to produce fingerprints without a court order. However, it's not clear that the two could be combined.

So what we're still doing here is we're sort of rummaging around in the lower courts, very much like Apple and the FBI were, needing the highest court to formalize law that works for 2016 and going forward. We talked about two years ago, in 2014, that case in Virginia that set some precedent, which determined that fingerprints were okay to compel, but passcodes were not. At the same time, it's not decided.

At the moment there is a 17-year veteran and former sergeant of the Philadelphia Police Department who is suspected of, but not formally charged with, possession of child abuse images on encrypted hard drives. He is in contempt of court because he has refused to provide the passphrase that would unlock those drives. So although he's not even formally charged, because he refuses to provide those passphrases, he's been in jail for seven months, and the judge says he will remain locked up indefinitely until he decrypts the drive, saying that, quote, "he carries the keys to his prison in his own pocket."

So here again we have the same sort of problem, is we've got competing interests and attorneys arguing their sides of these cases. And every court decides what it wants to, based on some precedent or ignoring precedent. And meanwhile, we need the Supreme Court to decide these issues. But at this point it's not clear.

There's a woman, Mary Fan, who's a law professor at the University of Washington, who was asked by Ars Technica on this issue, and she said, "This is why I tell my criminal procedure students that they have more protections today if they use a passcode rather than a fingerprint to guard entry to their phones. While I don't," she said, "conduct crimes on my cell phone, I still decline to use my fingerprint out of an abundance of caution." And of course I also don't conduct crimes on my iPhone, and I use my fingerprint out of an abundance of convenience.

Leo: I think what's interesting, I mean, we've always said this, that they can collect a fingerprint; they can collect hair. But I understand why this is now, and it should be, going to court, and ultimately should be decided by Congress, as with all of these things, because a fingerprint is like giving a piece of evidence, or hair is a piece of evidence. It's not testifying against yourself. But unlocking your phone is more than a piece of evidence. It's giving...

Steve: It's an action.

Leo: It's an action that gives a much larger pool of information to law enforcement. So I understand why this is actually being contested.

Steve: Yeah.

Leo: And I do hope that they will see this as more than simply giving up a fingerprint or giving a DNA sample.

Steve: Right, a fingerprint traditionally has been limited to identifying you.

Leo: Right.

Steve: That is, you know, is that your fingerprint on a murder weapon.

Leo: It's a piece of evidence, but not self-testimony, right.

Steve: Right.

Leo: It's, you know, again, as the President said, we are fetishizing our phones. But there's a good reason for it. They have everything. They've got it all.

Steve: Well, and I would argue that privacy needs to be pried from our cold, dead hands. That is, let's fight for all of it that we can get, and we'll see how much we can hold onto. My guess is we're not going to - it's not going to be something that we can have absolutely. And of course we know on this podcast that there's no such thing. The phrase "electronic Internet privacy" is an oxymoron because one portion of the ecosystem is unlocked, but all of the conduits in and out can be spied on. So, okay, there is an aspect of this that isn't as absolute as we would like to imagine that it actually is.

Leo: It'll be very interesting to see this whole thing play out. I think we're going to see it play out. And it may end up being a small footnote to the presidential election which is actually playing out right now. It may be moot, in other words.

Steve: I meant to talk to you about this before...

Leo: Well, we don't want to get political on this show. Yet many of the subjects that come up in covering technology are political. This is a perfect example. It affects us.

Steve: Yeah, although it's never been clear to me how this really divides down party lines. And we might argue that the unanimous vote for email privacy hasn't. Things like Hillary's email. That's clearly political realm stuff. I went on record months ago saying, if there was actually an operating server in a closet in some random office building, then if you don't have physical security, you have no security. So that was unconscionable. I have, you know, just to get to my servers, where there's not that much of great import, I've got to go through three different hoops, you know, and guarded camera scanning, dogs are sniffing around, I mean, it's intimidating. And then we hear that the server was in operation in a closet off of the bathroom. It's like, what?

Leo: Well, but I think that that's a larger story because I think that that's more a reaction to the fact that the government didn't have secure servers and so...

Steve: And wasn't really enforcing policy.

Leo: Yeah, I mean...

Steve: They say they had policy, but...

Leo: It's because email's so new, frankly. And so I'm sure by now, I would hope, that they have. But these governmental email servers were not any more secure than one in your closet.

Steve: No.

Leo: In fact perhaps less so because they were a target. So, I mean, I can't impute her intention, but you could make the case that she felt it was more secure to run her own server than it would be to trust the government servers.

Steve: Well, and we've talked about this before. But the fact that her email address wasn't dot gov, it was dot bill or something.

Leo: It was clintonemail, clintonemail.com, yeah. She was using, basically, she was using her personal email for government business. But again, that's because this was all new, and still is somewhat new. Government moves slowly. Remember, we've had email for a long time. They're just now figuring out that, if you don't use your email for six months, it's not abandoned, you know.

Steve: Right. And Colin Powell did the same thing.

Leo: He did the same thing, exactly, because it was new.

Steve: So this hadn't been addressed.

Leo: Right.

Steve: And certainly has been over-addressed now.

Leo: Yeah.

Steve: But anyway, my point was that clearly that is a political issue...

Leo: Yes, it's partisan; right.

Steve: ...that I have a feeling we're going to be living with until November. But this, to me, seems apolitical. It seems, I mean, I don't see where this is partisan. But this is policy, and incredibly intriguing. I've got a bunch of projects on hold pending the outcome of this.

Leo: Yeah, no, I've got watch and see what happens, yeah, yeah, yeah.

Steve: So Android is back in the news, but in the same way that all of our deeply inspected platforms now are. What we're seeing is, if there's a takeaway with a broad brush, it would have to be, if you look really, really, really hard at anything that's really complicated, you will find holes. We see it over and over and over. I just read, and I didn't have a chance to dig it up because I just - it just came by an hour ago that OpenSSL just had two longstanding critical patches made. There it is. It's everywhere. It's longstanding. There are, like, really big problems with it. And it's like, okay, yeah, and we just fixed two real big problems that presumably everybody needs to fix OpenSSL now. And so we have a history of problems with Windows.

Now Android is the new kid on the block. As I mentioned at the top of the show, what Google was calling the "Nexus Security Bulletin" has been renamed the "Android Security Bulletin" yesterday. And nothing huge to mention. They did push out an over-the-air update containing 32 vulnerabilities. The carriers received this package a month ago, on

April 4th. So with any luck they've been pushing those out, too. There were two privately disclosed - so these are not zero-day. They are not known to be currently exploited. But once again in the Mediaserver module, two critical remote code execution vulnerabilities which affect versions 4.4.4, 5.0.2, 5.1.1, 6.0, and 6.0.1. And those are all in the show notes for anyone who's interested.

The problem is that Mediaserver is very exposed. In one podcast some months ago we really took a close look [SN-518]. We were looking at the C code and looking at the pointer math where it was so easy, they hadn't casted the same variable the same way. So this is the problem with C is that it's very literal, as programming languages are. And because there was a slight mix-up in the interpretation of the variable, the inequality was treated as signed or unsigned or a different length. I don't remember the exact detail, but we covered it at the time.

So what's happening is now people are looking carefully at this and finding more problems. But the crux of it is that it's this shared media processing library that needs to handle a wide range of different input file types and formats. And the so-called Stagefright vulnerability or this Mediaserver module is accessible in a number of different ways. And what we've also seen is that media parsers have historically been problematical. You know, parsers in general tend to be kind of an inflection point. We see them, for example, with font rendering. That's a font format parser where it's essentially taking sort of a meta language and interpreting it to understand the exact handling of the media that it's bringing along, whether it's a font or it's a graphics file or, in the case of Mediaserver, MMS or MPEG movies or whatever.

So it's a difficult type of code to get right. And as we know, it's necessary to be perfect because, if it's not perfect, and it's possible for an exploit to find its way to the flaw, then that can be leveraged. And the problem is that many different components within the Android OS invoke this Mediaserver module, sort of by implication. It's just there to handle their media needs. And so there are all kinds of - so what that means is it has a large attack surface. And there's just all kinds of ways to get externally supplied sort of pseudo media at this module. And if it's not perfect, that can cause problems.

So anyway, I'm hoping that Google will get this out to everyone with Nexus devices. If you have an option, you certainly want to update. I know that Amazon is - I've got a Fire device, and every time I turn it on it's been doing things. So I'm assuming that these updates are getting out in a timely fashion. And again, not super critical. It's not like it was before, where this was a zero-day, and it was already being exploited in the wild, and people's phones were getting taken over. But this is just something you want to get taken care of. And probably we haven't seen the last of it.

Oh, and I forgot to mention that this server is operating with extensive rights on the platform. It needs to have access to the camera and the microphone and lots of the platform's hardware. So it's in a privileged position. And unfortunately it's prone to being poked at.

I tweeted earlier today that we now know that the Portuguese abbreviation PQP is our equivalent of WTF because there were a lot of people tweeting...

Leo: I want to hear you say it in Portuguese.

Steve: Oh, and speaking of which, from now on I am spelling Australian city names. Talking about batting a thousand with puzzles, I'm at zero for...

Leo: They're impossible, I know.

Steve: Just I'm not doing it anymore. I'm going to spell them because I just have no idea how to pronounce them. I can't do it. So once again a judge yesterday ordered a three-day blackout of WhatsApp in Brazil because WhatsApp, of course now owned by Facebook, and now sporting the Signal messaging protocol which is designed so that it cannot be decrypted, and given the way it's structured - we've covered it extensively - it's just it's a beautiful protocol. Hats off to Moxie and group for producing Signal and for WhatsApp and Facebook for incorporating it in.

So this judge is the same guy who a few months ago not only ordered WhatsApp to be blacked out, but put a WhatsApp executive in jail briefly. And so he's just on the warpath. He just doesn't get this, that this has been designed so that it's not possible. And they say it's not possible. And so then the fine would be the equivalent of $142,000 to a carrier, a cell phone carrier, who did not comply with the judge's order.

So throughout Brazil WhatsApp was blocked, and it went dark. Then the order was once again overturned. The executive a couple months ago, he was let out of prison. People were just scratching their heads saying, "We don't know what's wrong with this judge; but, you know, sorry about that, sir." So again, we're seeing the consequence of this weird place we're in where we are currently designing encryption that no one is able to decrypt, and the courts haven't caught up with that. And I don't know what'll happen. I mean, we're having a big enough problem in the U.S. where we're watching this all happen. But there's Brazil, and then there was - what was the country, do you remember, that was going to outlaw completely, ban all encryption?

Leo: Oh, yeah. I don't remember. It was a former Soviet Bloc country.

Steve: Yeah. I don't remember now.

Leo: Oh, it was Hungary. Hungary.

Steve: Yes, you're right, Hungarian, yes, [crosstalk].

Leo: But obviously this is going to be a battle that's going to be held all over the world.

Steve: Yup.

Leo: And, see, my answer to the Fareed Zakaria/Snowden debate is that that's not - that's posing kind of the wrong question. I would agree that lawful interception of encryption would be nice. However, it's just not available because any time you do that, you undermine encryption. And so people want to - and good encryption exists. It'd be very, I mean, if countries try to really outlaw strong encryption, which is the only...

Steve: Well, the argument, the best argument is that, as we know, strong encryption apps exist.

Leo: There's nothing we can do about them.

Steve: Even if Apple was compelled to redesign their system so that iPhones could be unlocked on demand without any weakening, well, doesn't matter because ISIS already has their own [crosstalk].

Leo: Well, I do, too, and so do you. Everybody does. And WhatsApp has kind of jumped the game by building it into their app, as well, so everybody has access to that. So then what do you do? The only next logical step is to ban use of strong encryption. Which, by the way, would also, somebody pointed out, Burr-Feinstein would also ban the use of a browser since it has built-in strong encryption, and the guy who makes the browser cannot break it. Or we'll stop using browsers because they'll do a man in the middle; right? And at that point then the only thing you could do is ban strong encryption. And when that happens, well, I fear for the world because, what, are you going to put everybody in jail who uses PGP? Leo Laporte, Steve Gibson talking security and moving on.

Steve: So we're back again to who is the...

Leo: Oh, man.

Steve: ...creator of the Bitcoin. And back in December, so, what, like five months ago, five and a half months ago, this other person came to the fore, Craig Wright, W-R-I-G-H-T. And two publications were claiming that he was the guy. We talked about it a little bit at the time. I didn't give it much time on the podcast.

Leo: It had broken during the show.

Steve: Ah.

Leo: Which is why. So you didn't have time to really think about it. And by the time we were back next week it was like, yeah, that's bogus.

Steve: Well, and his location was raided.

Leo: The day that it was broken, and it was broken in Gizmodo and Wired magazine.

Steve: Yup.

Leo: And it was suspect from the beginning. And that day he was raided by Australian tax authorities.

Steve: Right, right. And so we just let it drop. Okay, then suddenly there's this big flurry a couple days ago. And, I mean, every - because bitcoin is a big thing, it's an opportunity for everyone on the Internet to say something about who is this. Anyway, my tweet from this morning - Craig Wright put up a second tweet this morning.

Leo: Well, we should say that this started up again because the BBC and the Economist...

Steve: Yes.

Leo: BBC said, oh, we found him. This is for sure true. The Economist hedged it a little bit. But in both cases they were partially convinced by the former director of the Bitcoin Foundation, a man I've interviewed on Triangulation, Gavin Andresen, who is a smart, and one thinks, one trusts, guy with integrity, and one of the few people who's personally corresponded with Nakamoto. He took over the Bitcoin Foundation when Nakamoto withdrew from the Internet in 2011. He said to Andresen, "Okay, you're in charge. I'll see you." So if anybody, you'd think Gavin would be the guy to ask. And he met with Wright, flew to meet with Wright to see the proofs, the demonstrations of the proofs, and wrote on his blog, "This is it. I thought before I met with him it would be true, and it is." And of course immediately his commit keys were withdrawn on GitHub from the Bitcoin repository because people thought either he was hacked or he's delusional. We still don't know. I don't think Gavin's said anything much since then.

Steve: So, okay. So thank you for the background.

Leo: Yeah. So people know where we stand.

Steve: Yeah. So there was a first post a couple days ago which it just - it sort of felt like a shell game. I mean, very much like Craig, who is - so this Craig Wright guy, who is claiming to be Satoshi, he says in his first post, you know, "I really sort of reluctantly have decided that I need to assert proof that I'm Satoshi because I was hoping this would all blow over back in December, and it kind of did, but then again it kind of didn't, and my friends and family and acquaintances are being harassed." And it's like, okay, you know, either you are or you're not.

Leo: And meanwhile, he's benefited significantly from the perception that he is Satoshi.

Steve: Right. And the problem is that, as we know from our podcast on Bitcoin years ago, that what there is ultimately is a private key. And that private key is used to sign things. And we talk about this sort of concept in crypto on the podcast all the time. And that if he purchased - if he spent a bitcoin that he mined - and what we believe is that he's got a million bitcoins that are now worth 449...

Leo: Satoshi does. The real Satoshi does.

Steve: Satoshi, correct, Satoshi, yeah, right. We believe that the originator of the blockchain has, I mean, no. We know that there are a million bitcoins presumably created by and owned by and being held by the real Satoshi. And all that's necessary is that, if Satoshi wants to prove his identity, he spend a fraction of a bitcoin.

Leo: If he can move a bitcoin from the known Satoshi blocks...

Steve: Yes.

Leo: But preannounce it. Say "I, Dr. Craig Wright, am now going to move a coin from the Satoshi block." That would be sufficient; right?

Steve: Correct, because...

Leo: Unless he's stolen his keys or something.

Steve: The only way to do that is with the private key in the bitcoin wallet. So this "evidence" that was shown wasn't that. It was some sort of obscure use of scripts and kind of, again, I liken it to a shell game.

Leo: It was a magic trick. It was B.S.

Steve: Yeah, where sort of some things were shown, and some hashes were made, and don't look behind the curtain. And, oh, look, these hashes are identical. Now, a number of people have torn that apart. Then this morning Craig posted again. And so I read as I was preparing for the podcast this latest blog posting of his that I'm going to share because what I tweeted was, "I sure hope this clown is not Satoshi. Get a load of this latest spew of nonsense." So, okay. So, and, I mean, I'll let people draw their own conclusions. But so he says - the posting was titled "Extraordinary claims require extraordinary proof." And people have had a lot of fun with that already because it's like, no. Just proof.

Leo: Any proof. The real proof.

Steve: Just real, exactly, real proof. Not extraordinary, just actual. So he says: "Yesterday, Andreas Antonopoulos posted a fantastic piece on Reddit." And this is Craig speaking in his blog post this morning. "Andreas said something critically important, and it bears repeating: 'I think the identity of Satoshi Nakamoto does not matter.'" And then

Craig continues: "He is absolutely right. It doesn't, and shouldn't, matter to the bitcoin community.

"I cannot deny," writes Craig, "that my interest in bringing the origins of Bitcoin into the light" - into the light - "is ultimately and undeniably a selfish one. The only person to whom this should matter is me. In the wake of the articles last December in which I was outed, I still believed that I could remain silent. I still believed that I could retreat into anonymity, sever contact, go quiet, and that the storm would eventually pass, and life would return to normal.

"I was right and wrong. The story did eventually retreat, but not before it turned. And the allegations of fraud and hoax, not to mention personal threats and slurs against me and my family, clung to me. I now know that I can never go back. So I must go through and go forward. Mr. Antonopoulos's post also notes that, if Satoshi wants to prove identity, 'they don't need an authority to do so. They can do it in a public open manner.' This," again writes Craig, "is absolutely true, but not necessarily complete. I can prove access to the early keys, and I can and will do so by moving bitcoin. But this should be a necessary but not sufficient condition for such an extraordinary claim." What?

Anyway, "And this is why I wanted to speak with Gavin weeks ago. Gavin was in a unique position as we dealt with each other directly while we nurtured Bitcoin to life in 2010. I knew that Gavin would remember the content of those messages and discussions and would recall our arguments and early interactions. I wanted to speak with Gavin first, not to appeal to his authority, but because I wanted him to know I owed him that. It was important to me that we could reestablish our relationship. Simply signing messages or moving bitcoin would never be enough for Gavin." Okay, I don't know what any of that means. He says: "And it should not be enough for anyone else." No, sorry, just spend some bitcoin. Anyway, so he says, he finally says: "So over the coming days I will be posting a series of pieces that will lay the foundations for this extraordinary claim."

Leo: This really sounds like a con artist.

Steve: Doesn't it? It does.

Leo: Stroking Gavin because Gavin, you know, is the mark. And it just really feels like that kind of a con.

Steve: "I'll be posting a series of pieces..."

Leo: A grandiose, narcissistic - yeah.

Steve: "...to lay the foundations for this extraordinary claim, which will include posting independently verifiable documents and evidence."

Leo: No, just stop talking and do it; right?

Steve: Exactly.

Leo: Just do it.

Steve: "And addressing some of the false allegations that have been leveled, and transferring bitcoin from an early block. For some, there is no burden of proof high enough." Swooning. "No, no evidence that cannot be dismissed as fabrication or manipulation. This is the nature of belief. And swimming against this current would be futile. You should be skeptical. You should question. I would. I will present what I believe to be extraordinary proof and ask only that it be independently validated. Ultimately, I can do no more than that." And it's like, oh, my lord.

Leo: It's B.S. It's just blatant B.S. It's obvious.

Steve: It is. And so now you understand why my tweet was, "I sure hope this clown is not Satoshi. Get a load of this latest spew of nonsense."

Leo: Yeah.

Steve: Robert Graham followed up with a very nice cryptographic deconstruction titled "How Craig Wright's deception worked," where he basically takes apart what was done a few days ago. And no one understood a few days ago why he just didn't do it. And we're still waiting. I mean, we don't know until - we don't know what's going to come next. But he said he's...

Leo: I love it that he put screenshots of the proof.

Steve: Yes.

Leo: With typos, by the way. The bash commands that he uses wouldn't actually run, if you typed them in. So this is very common kind of con artist behavior. And it's sad because I feel that Gavin's been taken in by it, but...

Steve: Well, the guy, Craig, should just dig a hole and crawl in it and stop doing anything because I don't...

Leo: If you wonder what's in it for him, he has left Australia. He's in flight there because he owes a lot of money to the tax authorities because what he was doing was using bitcoin to generate tax refunds and collecting actual cash for bitcoin transactions. And so, by the way, if you're Satoshi, you don't really need to do this because you've got $100 million in bitcoin. Yeah, so he would do these - he did the $30 million bitcoin transaction and asked for a tax refund. The tax refund's in real Australian dollars, so he'd get the check. That's why he was under investigation. They want his money back. So he left the country.

Steve: Is that why he's in London?

Leo: Yeah. It's just obvious what's going on. It's sad. And, you know, Gavin Andresen has not published anything since his original confirmation. There's some question in my mind. Maybe he was compromised. Where is he? What is his response? Maybe he's just embarrassed because, you know, if you've been conned, what you want to do is, oh, no no no, really. You want to - you double down on it.

Steve: You want exoneration.

Leo: Yeah. You don't want to admit that you were fooled.

Steve: Yeah.

Leo: So it's sad.

Steve: So for our listeners, we still don't know. But John McAfee's been a little quiet lately, so we have some more entertainment. Wow. I did want to follow up on something that we talked about last week. David Roots sent me a DM. And he said, "In the latest Security Now! episode you and Leo agreed that turning off the computer adds no real security." He says, "That's not the case when we're not talking of a home computer which is in a 'safe' environment, like your house.

"However, I work in a bank. My workstation stays in the office after I leave for the day. I always turn it off each day, even though it adds a minute of boot time for tomorrow. The reasons are as follows: I do now know who has physical access to the PC when I'm gone. I've set BIOS passwords for boot and admin which should at least make it more difficult to boot the OS or from USB. I've encrypted my hard drive, which has to be unlocked before boot. I have no real faith in the Ubuntu 'lock screen.'" That's nice that he's using Ubuntu. "There are ways to bypass it. When shut off, there is nothing in the RAM - no loaded SSH keys, no login passwords, et cetera."

So I just wanted to tack that on to the end of our discussion because I thought that was a good point. We leave our machines on because it's better for them to stay on. They're not thermally cycling, going hot and cold and hot and cold. Once upon a time ICs used to creep out of their sockets, when integrated circuits were in sockets. They're not in sockets anymore, and lord knows the CPU cannot possibly get loose from where it's contained because it's screwed down tight against its sockets. But still, it's just not good if you don't need to, I would argue, to power cycle a machine that doesn't need to be.

But David makes a great point. If you don't have oversight over the machine for the two thirds of its life that you're not sitting in front of it, definitely better to turn it off. And if it's the bank's computer, presumably they're keeping it current and backed up. And if it does have a problem, they'll get you another one. So no biggie.

Leo: It also saves power.

Steve: Yes. Very good point. Okay. Now, errata. I stepped in it last week.

Leo: Oh, I'm sorry. I usually try to protect you from those things. What happened? I feel bad. I feel like it's my fault.

Steve: Well, on this podcast, I endorsed something that I myself could not physically bring myself to do. And I did it without thinking, so I apologize. I endorsed the idea of piping the output from curl into bash in order to set up an OpenVPN server on the Raspberry Pi. What I loved, the first of a tweet storm that I received from our very security-conscious, absolutely correct listeners, was from a Paddy Kerley. He tweeted: "Really, Steve? Pipe this random script from a guy called Inphektion to install something? What happened to TNO?"

And so everybody who sent this is of course correct. I mean, if I were sitting there, I wouldn't be physically capable of entering that command because I would run - I would pull the contents of the URL into a file and look at it. I would, out of curiosity and because I would implicitly understand that I'm pulling a script off of the Internet, and it's running, you know, it's essentially providing a stream of commands to the bash command prompt, doing who knows what. Now, at the same time, it is sort of time for a reality check because I did find out, by the way, that Inphektion is 40 years old and has kids. So we were sort of...

Leo: It's his old handle. He's not Inphektion anymore. Now he's Dad.

Steve: Yeah. So at the same time, let's all remember the degree of implicit trust that we have in everything we do. Unless you design the chip and bring the sand in from the beach and make it and program it and build it up from its roots, at every single stage we're trusting the goodwill of the people that provided this to us. And there have been lots of accusations of, like, secret things, even in some of the early Intel chips, things that were undocumented and that we weren't sure about. And of course there's that famous NSA key in Windows. That thing, that rumor never goes away because it happens there's some coincidental string that happens to be NSA that people keep finding inside of Windows. It's like, no, no, no, no, the NSA does not have master keys to Windows. I mean, so I wanted to acknowledge and thank everybody.

Leo: The point kind of is that Trust No One is an impossible goal. It's a good motto, and it's a good thing to aim for. But you can't compute without trusting a lot of people. Right?

Steve: Well, and, yeah, even in the Trust No One model, which is, for example, you encrypt something locally and then you stick it on the cloud, the point being you pre-encrypt it. And we were calling it "PIE" for a while, Pre-Internet Encryption. Even there, unless you wrote the crypto yourself, you are trusting the authors of the crypto. So all of these things have a security perimeter.

Leo: What was it that we were piping?

Steve: It's very cool.

Leo: I forgot, to be honest with you.

Steve: Yeah. You connect a Raspberry Pi to your router. You bring up the command shell on the Raspberry Pi, and you type in one line, which is a curl - curl retrieves a URL from the Internet - and then the vertical pipe character, and bash. So basically you're piping a script into bash.

Leo: A script into bash. Which is no different than downloading the script and then invoking it. It just saves a step.

Steve: Well, and that's exactly right. You could, what, you could download an executable that performed all the same configuration stuff. So what I liked was the elegance, the minimalism of that. But with it comes some responsibility, that we are trusting the integrity and the intentions of the person who did this. Now, I will say that something that, for example, did this hourly or daily, that would raise my alarms higher because then at any time in the future, if there was a compromise, like imagine the world is full of these Raspberry Pis that are doing this every day. Well, then that's a huge target of opportunity. Somebody compromises that script once, and suddenly all these devices download something nefarious. To me, it's different if you get it once. And by all means, look over the script.

Leo: Well, is it a bash script that you're downloading? Because if it is, you can just look. It's open source. The code's open.

Steve: Yeah, it's a text file.

Leo: Look at it, and but then probably download it once, look at it, and run it in a cron job instead of running the curl command each time in the cron job. But by the way...

Steve: No, it doesn't have to be run each time. It only is run once. And so what I was...

Leo: Once. But by the way, we all do this all the time. Have you ever downloaded some code from Git and compiled it and run it? That's essentially the same thing. And so it behooves you to trust the person you got it from. And the nice thing is, if it's a script, you can read it.

Steve: Right.

Leo: So you can - by the way, this brings up a point because over the past week a number of people have sent me scripts for downloading every Security Now!

episode. And I've posted those scripts on my blog, LeoLaporte.com. And I said in the post, I haven't run them. And a cursory glance looks like they're not malicious. But if you want to use these, it's on your head. So there's a bash script from @sethleedy. There's a Python script from @thepunkgeek. And Gary Nevills sent me a PowerShell script for you Windows 10 users that will either download individual episodes of Security Now!, or all the episodes if you want, or other episodes of other shows, as well. So those are at LeoLaporte.com. And you know what, it's the same thing. Just as risky.

Steve: Yeah. I did, however, want to acknowledge the...

Leo: They're not named Inphektion.

Steve: ...the people who said, wait a minute. And I should have said something. I didn't say anything last week. So that's why this is in errata. I should have said "I wouldn't type that." I mean, I would obtain the script.

Leo: And read it.

Steve: And I would, out of curiosity if nothing else, just peruse it to see what it's doing and decide, okay. And then send it into bash to set up the VPN. And by the way, it works. I've had several tweets from people who said, oh, my god, my Raspberry Pi is now an OpenVPN server running plugged into my router, and I can VPN to my home network. Works beautifully. So congratulations to Inphektion, a proud father, not a teen.

Leo: He wrote a script that does everything you would do manually.

Steve: Yes.

Leo: Automatedly. You can review it. And you know what, that's a hell of a lot safer than a binary blob that you have no idea what it's doing.

Steve: Good point.

Leo: So I don't have a problem with that. Read it before you curl it. I mean, curl it, read it, then bash it.

Steve: Right. Okay. So, Leo, if you scroll down you'll find a JIF or YIF or GIF.

Leo: We're going to call it YIFs from now on. I love the YIF.

Steve: No, please, not a YIF. It's blogspot.com. Click that so you can show that. That's an animated GIF. I've always called them JIF, so I'm going with JIF.

Leo: Yeah, me, too.

Steve: Or was it GIF? Now I've even forgotten what I used to call it.

Leo: I do both to drive people crazy.

Steve: Yeah. Actually what - okay. So I have a new puzzle. I tweeted it when I discovered it. And I owe someone of our listeners a thanks because this is one that I had already obtained, and it was sitting on my device, and I just hadn't gotten around to it yet.

Leo: Ooh, I like this. This looks good.

Steve: Oh, Leo, it is wonderful. Now, we had Rails in the past, which was the...

Leo: Choo-choo trains.

Steve: The choo-choo train track thing that was fun. Blockwick a lot of people loved. That was a really nice sort of satisfying sliding block puzzle. Hook, of course, was very popular. The only problem with it, there was only like 25 levels. And I contacted the author, and I said, "Everybody wants more." And he said, "No, I'm going to do something different." Well, okay. I said, "If you ever need more money, just do more levels, and we'll all - we want more." Then of course there was Osmos and Auralux.

Leo: Oh, yeah.

Steve: Which are sort of similar, and both wonderful. And then Infinite Loop. Infinite Loop probably is the most favorite of the puzzles I have recommended because it's more of sort of a doodle. It doesn't take much thought. You just tap it, and it rotates pieces in order to, like, knit this thing into a finished little puzzle. And it's infinite. So after the disappointment of discovering that Hook only had 25 levels, we really wanted something that we wouldn't run out of.

Okay. This one is a win. It's called The Sequence. And I created some jump links. The first 13 levels are available free on the Android platform. So...

Leo: It's only 99 cents. I'm buying it for the whole thing; right?

Steve: Yes, Leo. You absolutely must.

Leo: Yeah. I trust you, Steve. It's worth a buck.

Steve: I tweeted it maybe like five days ago. And people already know that they're in trouble when I recommend a puzzle.

Leo: By the way, it's also not only available on Android, but also iOS and Steam.

Steve: Correct.

Leo: And Windows.

Steve: Correct.

Leo: So you've got your - you'll have a platform you can play this on.

Steve: Yes. It is the grand prize winner of the Unity Game Developer Contest. Unity is a cross-platform development environment, and these guys took first grand prize. This is different than the other things. The person who recommended it to me said, "Steve, you like programming, you'll probably like this." First of all, the developer is gifted. There's sort of a whimsicalness to it. Not only is it a great concept, but it is beautifully done. So after I tweeted, I got a reply back from Pete Shanahan, who said: "@SGgrc, you are the only person whose game recommendations get immediately purchased/downloaded. You have stellar taste, sir."

And so I wrote back, I DM'd him back, I said: "Thank you, Pete. Because people have figured out that I love puzzles, I get lots of recommendations, but only a few make it through my own filter. So I'm always excited to share those that do. My criteria are clear: No hurry. No timers. No reflexes being tested. No unnecessary punishment. Under-designed, not over-designed. No hidden stuff that you need to poke at to find. Just the kind of thing where everything you need to know is in front of you so that you can stare at the screen, running possibilities through your mind. This one goes a bit further and is actually charming and humorous in its execution. I think people who have enjoyed my previous discoveries will find this one equally wonderful. Thanks again."

So The Sequence. And as you said, Leo, it's available on all platforms, and the first 13 levels free on Android. I just love it. So to give people who are just listening to this some idea, you have a grid that is, like, seven by nine, something like that. It's an odd by odd so that you have a center column and center row. Not that that's important, but I've just noticed that. And there's one cell where there is a binary object. It's a little white circle. And that's sort of the source. And then there's another sync where you need to transfer this binary circle over from the source to the sync.

And you have little modules. For example, there's a module which is a pusher. And so anything that is in front of it, it pushes to the next square. But it can't push it further than that because then it's not in front of it any longer. Then there's something else that grabs it and rotates it 90 degrees into a square off to the side. And then there's another thing which spins whatever is in front of it. And then there's another thing that reverses the polarity of the thing that it's connected to. So like it would cause the next spin to be in the other direction, or it turns the pusher into a puller.

Anyway, the point is for just - I've only - I'm at, like, level 25 or something. And I've found - there's five objects that have been. And this is sort of selectively revealed to you. A little tutorial in the beginning, kind of gets you to get the hang of it. And then you're off. And so this is more - this is something not to be upset about that some of these are difficult. This is not so much a doodler as it is a real problem solver. But, boy, I just think people who are hooked by this are going to enjoy being hooked because it is fun. The soundtrack is nice, but a little repetitive in the background. But the actual sounds of the actions are fun.

And then just after you think you get it arranged, you start it. And then this whole thing sort of runs in a stepwise fashion because you assign a sequence to each of these little blocks. And so they execute one at a time. And their actions then all link together in order to move this little binary bit thing from the source to the sync. And it has to do it four times in order for you to succeed on the level. And you'll sort of get the hang of it when you see it.

But anyway, I have no reservations except that I will say it's a little tougher. Some of these things, I have no problem putting them down and then coming back to them a few hours later or the next day and going, okay. And oftentimes I have an inspiration. So some of them are tricky. But I really think people who enjoy the podcast...

Leo: Yeah, it's programming, it really is.

Steve: Yeah, it is. It is. It's a little graphical programming language. I should mention, too, just so that I haven't omitted it, that the same author has a previous game called Hard Logic. And that's in the offing. I've poked at it a little bit, and it's like, oh, it was well named. It is even more minimal, but it does look like it's a - but I'm just loving this. Oh, and after you get the 32nd level - I think it's 32. Maybe it's 35. Anyway, then it unlocks a playground. And I think what that means is you can just build your own machines.

Leo: Oh, neat.

Steve: Which, yeah, I think would really be fun. They're just - I don't know what it is about it. But the execution is just beautiful. The graphics, the little noises they make, I just get a kick out of watching the thing go, and you feel a real sense of accomplishment when you've built one of these because, as I said, they do get challenging.

Leo: Cool.

Steve: Yeah. I wanted to mention that KB3035583 resurfaced when I turned my machine on this morning, my Windows 7 machine.

Leo: Oh.

Steve: And of course 3035583, you've got to be a real geek to know what that number means. That's the infamous WGX...

Leo: GWX, yeah, although...

Steve: The Get Windows 10 - yeah, sorry, GWX.

Leo: Although you might be tempted to call it WTF, yeah.

Steve: Yeah, exactly. So it's like, why are they changing it? I don't know why. I bit the bullet because, you know, I have to. I have to make sure they haven't, like, done something really stupid. Maybe they're backing off. Oh, Leo, we forgot to talk about the weather lady.

Leo: Well, we did it on Windows Weekly last week, so, yeah.

Steve: I don't believe that we forgot to talk about the weather lady.

Leo: But that is proof positive that Microsoft has gone too far.

Steve: Oh, boy. For anyone who's been living under a rock, you probably already know. But during a morning - and was it, like, was it last Wednesday? It's been since the last podcast. But she - yup, there it is.

[Clip]

Leo: The best is the last line, though, here.

Steve: Yes, I know.

WEATHER LADY: What's going on? Where's my clicker now? Okay, winds have been very gusty overnight, as well. It's the Windows 10; right? That's what people are going to say. Don't do it.

Leo: Don't do it.

Steve: Don't do it. Oh. So she's doing, you know, she's a meteorologist standing in front of the green screen. And up comes the big, well, we all know what it looks like, the big white and blue, you know, Microsoft recommends updating to Windows 10. Oh. And it's like, oh, boy. Wow.

Leo: Oh, lord.

Steve: Enough said.

Leo: Oh, lord. Oh.

Steve: So and of course I got a lot of people tweeting, saying, oh, you ought to tell them about Never10. It's like, yeah, well, I'm sure they know now. Oh, boy.

Leo: Yeah. She's famous now, though. It was a good thing for her. She got her viral video.

Steve: And I just need to go off the reservation completely to share one of my discoveries that I am very excited about. And that is, I've been using this for a few months. And this is a beautiful six-port 60W USB charger.

Leo: I have several of those. The Anker?

Steve: Of the Ankers?

Leo: Yeah.

Steve: Yup, yup.

Leo: Love them. I keep buying more. I have them everywhere in the house.

Steve: Yes, exactly. It was on the occasion of me buying two more that I thought, okay, the first one proved itself. I need to share this with our audience. So it's A-N-K-E-R.

Leo: They make great stuff. They're a really good company.

Steve: Amazon carries it, 60W. And what's special about this is people may know that a USB charger is not just a five-volt supply. You need to support some minimal USB protocol in order to get devices to understand the capabilities of the charger that they're being plugged into. So this thing is universal. Again, and it's not easy to find one with six outputs because that's a lot of juice. And the other side is not a wall wart, but an actual AC cord. So inside is a little switch, a very high-efficiency switching power supply that drives six ports. And so I just, again, as I said, it's completely a non sequitur, but I love this. And you can get it in black or white. It's about $32 on Amazon. And the black one, I don't know about the white one, has 2,057 five-star reviews on Amazon. So, yeah, just my recommendation.

Leo: It's a good thing. I have, as I said, I have three or four, like you. It's so funny. And then just I have them everywhere in the house. I have it on my bedside table. I have one in...

Steve: It's the right one.

Leo: Yeah, yeah.

Steve: I mean, it beats - because we all have so many USB charging things now. And the normal USB adapters are big blobs that often block the adjacent port, or you have to have an octopus coming off in order to work with them. So, yeah. I waited a few months.

Leo: By the way, they now have, for a hundred bucks, a 10-port, if you really want to go crazy.

Steve: Wow.

Leo: How many watts is the 10-port? Yeah, still 60W. So, see, maybe you'd be better off with fewer ports because you'd get more watts per port.

Steve: Yeah, and your dollars per watt has dropped a lot, too.

Leo: Yeah, that's a little expensive. Amazon makes, and this is kind of interesting, an AmazonBasics that looks exactly the same, and it's 25 bucks. And I'm wondering if that's, you know, all of these companies just source these from Chinese companies and label them.

Steve: Yeah. It's just private labeled.

Leo: So it's 60W, six-port, USB charger. I don't know. Anker's so good. You could trust Anker. I only use Anker stuff.

Steve: I do. And I've been very impressed with it, so I wanted to share it.

Leo: Good.

Steve: And one more recommendation I have is for something called SpinRite.

Leo: Oh, yeah, I heard of that.

Steve: Not surprisingly, yeah.

Leo: Yeah.

Steve: Simon Willcock in Manchester in the U.K., he asked a quick question. And in the spirit of this nominally being a Q&A, and we've got time for some questions here in a second, he said: "Steve, a quick question. I have a friend whose introduction to her laptop was 'The disk is dead; can you get me a new one?' she said. I asked if I could run SpinRite on it. She agreed, and I ran it at both Level 2 and 4, and no errors were found. She is convinced that she needs a new disk." Then he says, "PCWorld tech guy told her so. From what I can see, there's no problem with the disk. How confident can I be?" And so, okay. What's not clear is where the original idea of the disk being dead came from. Disks can declare themselves in trouble through the so-called SMART, the Self-Monitoring - what's the A? Self-Monitoring - S-M-A-R-T. Self-Monitoring something and Reporting Tool, or Technology.

Leo: Yeah. As I remember, it's not an intuitive acronym.

Steve: S-M-A-R-T. Self-monitoring...

Leo: I'll look it up for you.

Steve: And reporting? Yeah, and.

Leo: Is it really? Oh, all right.

Steve: I think it's Self-Monitoring and Reporting Technology. Anyway, so disks can provide a warning, and BIOSes can read that and put up a notice when you boot the machine that the disk is in trouble. SpinRite monitors...

Leo: It stands for Self-Monitoring Analysis and Reporting Technology.

Steve: Analysis and reporting. Okay, thank you.

Leo: But whatever it is, it's not very smart.

Steve: No, it's not. However, and this is my point, if the drive is freaked out enough to say that it's dying, I would believe it. On the other hand, SpinRite checks for that. It explicitly looks for that. And I've had people running SpinRite tell me that SpinRite suddenly put up a note saying this drive is reporting it's near death. You may want to stop running SpinRite and back up what you can.

So the fact that SpinRite ran twice on it with no such report to me says this entire thing was specious. And wherever this idea came from that it was dead was clearly wrong. So Simon, if you run SpinRite on it, and SpinRite is happy, we know two things: first, that SpinRite is happy, and also that the drive is not unhappy with its own condition because, if it were, SpinRite would let you know. And since...

Leo: SpinRite is smarter than SMART. Seriously.

Steve: Oh, it's way smarter than SMART.

Leo: Yeah. SMART was - the hard drive companies didn't really want SMART, so they dumbed it down.

Steve: Correct. Kicking and screaming. Compaq said we're not going to buy from you unless you give us some means of knowing what's going on inside the black box. That was as drives became - the IDE drives were the first, where the controller moved into the drive. And Compaq said, look, how do we test these? Drives fail. And so, actually, and Compaq was using SpinRite to prequalify the drives...

Leo: Really. Good for them.

Steve: ...before they put them in users' machines, yeah.

Leo: Wow, that's nice. That must have felt pretty good.

Steve: Yeah. And next week we're going to talk about Samsung and the SmartThings hack.

Leo: Ooh, yes.

Steve: So lots of interesting information there. And in general, about IoT stuff because that's going to end up being, unfortunately, a big topic for the podcast moving forward.

Leo: Yeah. Yeah, yeah, yeah. All right. We are going to pick up where we left off. Right, Steve?

Steve: Yes. Yeah. Perfect. I think we're going to get the rest of these other remaining six questions. We've got half an hour.

Leo: Should be no problem.

Steve: Be perfect, yeah.

Leo: Let's go to - is it Oscar Morales who's next?

Steve: It's Neil, number five.

Leo: Oh, Neil Baldridge of Lubbock, Texas. Question 5 was where we left off last time. He's wondering about LTE safety in the light of this kind of bogus, but still scary, "60 Minutes" piece, and particularly on SS7: You mentioned last week it was unclear if SS7 eavesdropping would apply to LTE data. I've always made the assumption that LTE data would be reasonably secure, especially when compared to open WiFi. But it's my assumption. It's not based on any evidence. Have you learned any more about whether SS7 vulnerabilities would allow eavesdropping on LTE data that is not specifically or otherwise encrypted, say on an HTTPS link?

Steve: So what we know is that the cellular network itself, I mean, what "60 Minutes" was right about, although this wasn't newsy because we talked about it a couple years before...

Leo: It's been a lot longer than that, apparently.

Steve: Yeah, it was at the Chaos Computer meeting in 2014 in the summer that this was first shown is that the entire, the glue that knits the global cellular system together has never been secure because what it lacks is authentication. And, you know, that's always the bugaboo. You can bring up security. You can have negotiated keys between endpoints. But if you don't know who you're negotiating with, then even if you, on the fly, negotiate a key, there could be someone in the middle, and you're negotiating your key with him, and he's negotiating separately with the other end, and knitting the conversation together, being in the middle. So, and the problem is, in an electronic environment, where you don't see who you're talking to, you don't know.

So what we have to understand is that the cellular system lacks authentication. That being the case, we know what it means, that it isn't secure. So HTTPS, for example, and he mentions between a smartphone and an HTTPS banking site, HTTPS does provide authentication. That's what the certificate is. It is an assertion. That's why we talk about them so much, because they're so important. The certificate is a statement of identity of the certificate issuer. And it's the reason certificates must be protected and kept safe, because you don't want your identity stolen. You don't want anybody else to be able to pretend that you're Bank of America or whomever.

So the HTTPS, that is, the TLS protocol, with certificates, provides authentication. And so it doesn't matter if the channel it's transiting is insecure, is not secured, or itself provides no authentication, because the endpoints do, and the protocol protects us. So what's not secure would be standard voice conversations or standard SMS and MMS that are not using any kind of a third-party wrapper or protocol.

If you were to use Signal or WhatsApp or anything else, that is, some other technology which provides its own encryption and some means of authentication, then it doesn't matter. If it's between two tin cans with a string, it's going to be that essentially you're using the carrier just to get the data across, and then the layer on top is providing safety. So if this whole SS7 thing worries you, and you want to, for example, have a truly private voice conversation, then you need to use a third-party voice app of some kind that will then provide the security.

Leo: All right. Oscar Morales in Paris, France and Bogota, Colombia with a question: Steve, why haven't we seen any attacks to Android phones in real life? I've been a consultant on Information Security for the past 10 years, and as a big fan I've been listening for six years. Talking to a fellow IT security consultant about Android phone security, he argued he's going to still use his little Motorola Android phone, even if it took him months to get the latest OS updates. Now, he says Motorola. I don't know what generation we're talking about here. But, he says, I was speechless when he said, if it was so bad or dangerous, why, despite having more than a quarter of a billion vulnerable phones, we never hear about people being attacked or compromised due to these vulnerabilities? And that question's been bothering Oscar.

ARS Technica announced that 950 million Android phones were at risk, that was back July 27th, 2015. On March 18th, 2016, we got news of 275 million Android phones at risk with a new vulnerability. Steve, you just mentioned another Stagefright vulnerability. That seems like a good bounty, says Oscar, 275 million personal devices compromised. However, have there been even a million complaints? Has anyone noticed anything funny running in their pockets? Why is no one taking advantage of this? What is protecting us? Why it isn't yet the end of the civilization as we know it? Thanks for your show and for the answers. Actually, I ask the same question, Steve. Why?

Steve: Yeah. If we look at history, we can see what the pattern is, which is it took us a long time to get things like Code Red and Nimda and MSBlast. We had insecure platforms for a long time until someone decided to do those things. And frankly, look how long it took before we ended up with crypto malware. You might argue that, well, they needed some sort of an anonymous payment system, which unfortunately Bitcoin now provides them. But there is, without question, a decoupling between what could be done and what is done. We often mused about how viruses were, like, rampant, but they didn't destroy things. They just sort of seemed to be viruses for the sake of being viruses. They used vulnerabilities just for the sake of propagating. People were just sort of screwing around, seeing if they could make something propagate. Until, of course, it became profitable, and now we have crypto malware.

So the fact that these phones and the Android platform is vulnerable doesn't immediately beget worms and big, high-profile attacks. There were reports of people receiving MMS messages when Stagefright was new. People were getting, like, hit all the time, and we covered it. And the advice was turn off MMS. Don't open those messages. The known phone numbers of blocks of phones were being scanned, just because they were there. So they weren't weaponized because people didn't bother to do that. They were just sort of screwing around, crashing people's phones because they could.

So I guess my point is that the fact that there are vulnerabilities doesn't mean that there will be automatically attacks against them. History shows us there's, for some reason, there's a disconnect between that. And I'm thankful for it. Well, on one hand I'm thankful for it. It would be nice if there was more pressure to fix these things because it's a little annoying that attacks are allowed to remain outstanding until they actually are being exploited in the wild. Then it's a big panic to get them patched. That sort of is just the nature of this industry.

Leo: I also think that it's a little bit harder to exploit these platforms than merely having the exploit, that mobile platforms are really kind of significantly different than desktop platforms. And so I think it's going to be a little bit more difficult for people even knowing the vulnerabilities exist.

Steve: I agree. I also think it's a bit of a higher end hack.

Leo: Yes.

Steve: When you have a Windows machine with all of the debugging and developer tools and sort of everything here in front of you, even though you don't have the source, I think it's easier to build a virus for that than it is for a very complex mobile platform where you do have access to the source in some cases.

Leo: Right.

Steve: I think you have to have some motivation. I would guess...

Leo: I think these mobile platforms also were designed in a post-virus world. So there are things done on these mobile platforms, Android and iOS, that weren't done on desktop operating systems.

Steve: For example, they all have Address Space Layout Randomization.

Leo: But even they have stores. I mean, there's a whole, you know, you can download any arbitrary code you want on a Windows system. Have fun; right? It's not so trivial or easy on a mobile device.

Steve: The apps are curated, yup.

Leo: So, and both iOS and Android have kill switches. They both have scanners built in that check everything you download before you run it. Windows finally has something like that, and Apple does. But this was kind of - I think security was kind of built in a little bit more on these mobile...

Steve: Well, and they had the advantage of coming in later and understanding.

Leo: They knew.

Steve: I mean, like no one today would build a browser that didn't have strong security as the first thing, like as a fundamental of what they were doing because we now understand how important it was. But the early browsers had no concept.

Leo: However, I think that your point's well taken. Give it time.

Steve: Yeah.

Leo: It probably is just a matter of time.

Steve: And if an individual is worried about if they're like a high-profile target, then this is the kind of thing that the spooks, as they say in the U.K., they could do targeted attacks if they wanted to get somebody, rather than just 275 million people all getting a dancing bear.

Leo: Yeah. John in Montreal isn't at all sold on Signal's security. Uh-oh. Just because your copy of Signal can be verified bit-for-bit to be identical between your phone and some other build, it doesn't mean that WhatsApp uses THAT version of Signal. If Signal is a demand-loaded module, WhatsApp could even load it but not use it. Sorry to rain on your parade. Niener niener niener.

Steve: So, yeah. And again, this comes back to, well, yes. Doing any of this requires that we extend some trust. There is absolutely no way around that. If you want absolute security, arrange to be in the physical presence of the other person and whisper in their ear. Otherwise, if you stick it on a wire, and you didn't design every aspect of what happens to it, you have no great security.

Leo: Yeah.

Steve: I mean, so, yeah, I take John's point. But it's like, okay, what's the takeaway? What can we do? Mine is there's nothing I'm doing on these platforms that is really important.

Leo: And it's my argument that you really don't have security unless you have open source security. And you can, I mean, truthfully, it'd be better if you could read all the code and understand it and vet it. And we've learned...

Steve: And of course Signal is. Signal is.

Leo: Right.

Steve: And so if you wanted to download this Signal app or [crosstalk] build it...

Leo: You'd be better off building it from source.

Steve: Yes.

Leo: Then you know what you got; right?

Steve: Yes.

Leo: And so that's, I mean, truthfully, I think it's probably good for us to spread the word because, if encryption does become outlawed or somehow modified, it'd be good for everybody to know, and it's not hard, how to download code, look at it, compile it, build it yourself. That's better, much better than a binary blob, you don't know where it came from. Especially if, as he points out, it loads on demand. Who knows what that is?

Gregg in North Hollywood, California wants an episode on Tor appliances. Like a refrigerator?

Steve: A refrigerator, and you don't know where it is.

Leo: Anonymous refrigerator. Hi, Steve. Watching TekThing 68 - that's Patrick Norton's show he does with Shannon Morse - and they have a Tor appliance. I have a Tor appliance in my pocket right now. Could you do a show, multi-part if needed, on these offerings? You could make your own Tor network appliance thingy using a Raspberry Pi, Banana Pi, Intel NUC, cheap small motherboard, et cetera; or make your own private Tor using DigitalOcean - which is a sponsor, we should mention - Droplets, data centers in San Francisco, New York, Amsterdam. Yeah, you could totally do that. You could use the Tor browser. I have in my pocket here a Tor appliance. So let me let you answer, and then I will show you mine.

Steve: Actually, you'd better show me yours because I have no idea why this question is here. Last week there must have been something I had to say about this.

Leo: Netcat just wants to know.

Steve: And I have no idea.

Leo: Inquiring minds. So one of the things that would be nice is to make VPN and Tor just automatic, right, so that...

Steve: Easy.

Leo: Easy. So that it would just be built in. And of course, if you built it yourself from a Raspberry Pi, you could vet the code. But I'm going to show you something that just breaks all the rules I just mentioned. This is a binary blob from a source I don't know except I trust him. I'm talked before about my Tiny Hardware Firewall, TinyHardwareFirewall.com. This is the latest.

Steve: Look at that little cute thing.

Leo: Isn't that cute?

Steve: Oh, my goodness.

Leo: So you plug this into your laptop. It's a WiFi-to-WiFi device. So it's both a WiFi receiver and a WiFi transmitter. You plug it into your laptop. It takes about three or four minutes to boot because, as you might imagine, it's a very slow processor. But there is - it's a little computer. And what happens is, once it boots up, you will see it as an access point on your computer, with a randomly generated name and WPA2 key.

Steve: No kidding.

Leo: Yes.

Steve: So it's only getting power from the USB port.

Leo: That's all it needs. I'll show you right now. I'll plug it in. And then of course you know ahead of time what the key and everything is. So it is going to take a while to boot, so I won't be able to show you how it works in any reasonable amount of time.

Steve: Oh, look. It lit up a little green light.

Leo: Yeah, it's booting up. So then you'll join it. And once you join it, you surf in your browser to the address of this device, and you can configure it. First thing you're going to do is you're going to configure its WiFi access to the open access point at the coffee shop that you're at. So you log into that. And that's how it handles captive portals and all of that.

Steve: Yup.

Leo: Once you've logged into that, now there's a button on the website that says "Engage VPN." You could choose your server and start up the VPN. There's another button that says "Engage Tor." And at that point all of the traffic coming and going from this device will be both through a VPN and through Tor.

Steve: Okay, now, everybody wants to know what this is, so we have to tell them.

Leo: So this little device, and by the way, not very expensive, I've recommended these before, this is the latest from TinyHardwareFirewall.com.

Steve: Oh, those guys. Yeah, yeah, yeah.

Leo: We've mentioned them before. The thing about this is...

Steve: And it's cute.

Leo: ...it's cute.

Steve: For people who don't, who can't see the video...

Leo: Well, I keep this in my pocket. It's the size of a...

Steve: That's the cutest thing I've ever seen.

Leo: It's only as big as a USB key.

Steve: Wow.

Leo: That's all you need. Now, they make a bigger one that does Ethernet, which would be more secure, obviously. But this one is - let me look at the price. The way they sell these is a little weird. And I should just say this is one of many. You could buy this device without this deal. But the way they sell these is with a year's worth of VPN from HotSpotVPN.

Steve: Ah.

Leo: So this is essentially a HotSpotVPN product. But they make - I've had the bigger one before. But these little USB ones are so tiny and easy to use. I mean, and it's got Tor built in; right?

Steve: It's just adorable.

Leo: Yeah. So this is a Tor appliance. Now, you would be more secure, I admit, if you built your own out of a Raspberry Pi. So 30 bucks, I think, for this. If you want a year's worth of firewall plus the hardware, 91 bucks. You basically pay for the firewall, and you get the hardware for free. But if you just wanted the hardware, 35 bucks. These are cheap. This USB thing, it's called a Napoleon, is $30.

Steve: And it's just cool.

Leo: And so I love this idea; right?

Steve: Yup, yup. So...

Leo: So that, I think, is what they're talking about.

Steve: Yup. So the VPN gets you out of your local insecure environment.

Leo: Right.

Steve: Through a VPN tunnel. And then if additionally you want Tor's "promise of anonymity," and I'm calling it that rather than "anonymity" because, as we know, lots of attention has gone to deanonymizing Tor users.

Leo: Not fully anonymous; yeah.

Steve: Right. Location obscuring.

Leo: Governmental, yeah.

Steve: Then you turn that on, and you get way worse performance, but way more secrecy, essentially.

Leo: Yeah, yeah. And it's not, you know, this one is not...

Steve: Very, very cool.

Leo: It's not horribly slow, I have to say.

Steve: Good.

Leo: So it's slower.

Steve: Right, because you're...

Leo: But you [crosstalk] your megabits...

Steve: ...bouncing typically through three Tor nodes.

Leo: Right. Still in my speed test, you know, it's maybe 3Mb down, something like that, you know, 550K up. Enough to get email and surf the web safely.

Steve: Yeah. Very nice.

Leo: So I really love this idea. And just, the thing is, this makes it so easy. You just carry it around. You don't even have to put it in a laptop. In fact, you might not want to. I just have a little battery, right, one of those little portable batteries, plug it into that, and that'll run all day. So you keep it in your backpack, and you have in your backpack, that you just log into, a server. Couldn't be easier.

Steve: Very cool.

Leo: Yeah, yeah.

Steve: Very cool.

Leo: Yeah. Well, I'm glad I was here for that one.

Steve: Yeah, because I was useless on that one.

Leo: Like, what is a Tor appliance? Well, that's the idea.

Steve: Why did I choose that one?

Leo: That's the idea. And there's, you know, you could create, as I guess Patrick and Shannon showed, you can create your own, which would be, for a Trust No One person like you, probably a good idea.

Ramsey's wondering about implementing key hierarchies: Love the show, blah blah blah. Can you explain how encryption systems can have master keys? The scenario

I'm thinking of is when an employee quits and leaves behind an encrypted hard drive on a company laptop, can the company decrypt the drive? I think yes, but I can't quite figure out how the crypto would work in that case.

Steve: So, yeah. This was sort of a quick one to answer. Well, could be. The idea is, and we'll take Ramsey's use case, you have a drive which is encrypted under some key which was arrived at randomly. So, and we'll take the TrueCrypt model, that is, when you're setting up TrueCrypt, there's some source of entropy that may or may not involve the user. TrueCrypt, for some reason, liked telling you to move the mouse randomly around and, you know, crazy for a while, until you decide you're done, and then press a button. And that always bothered me because the question was, wait a minute. People are not random. And so how much are we supposed to move the mouse? What if we don't move the mouse enough? That was just always nonsense. But it's like, okay, fine.

The point is that generates the key that encrypts the drive. Now we encrypt that key. That is, so that's the master drive encryption key. So now the user provides a passphrase, hopefully long and high-entropy, and so that master drive encryption key is encrypted using the user's long passphrase. But nothing, and here's where the key hierarchy essentially comes from, although this is a flat hierarchy, nothing prevents that same master hard drive key from being encrypted also under, like, an administrative super master password. So now you have two encrypted things, one which is decryptable to the hard drive master key with the user's password, and the other one which, if the administrator applies their super master key, decrypts to the same master hard drive password. So two people can have their own keys to the same device.

And the crypto is, I mean, so, and this has always been my argument, for example. This is in fact a variation of the argument on the whole decryption on demand. That is, phones could be the same way. You could have two separate keys, one stored by the entity responsible for being able to respond to a court order, the administrator; and the other one is the user's. And either one can be used, and neither lowers the security of the other except in the obvious way. But from a technology standpoint there is no difference between them, and the encryption is not outlawed or weakened or broken or anything. So that's what's so cool about these little modules, these little crypto components that we have now, is they can be put together in all kinds of ways to create any kind of interlock that we ask. And so this simple little flat one is an example of a key hierarchy. Just taking the master key and then reencrypting it under two different keys that are known by different people.

Leo: Well, here's another kind of related question. This is about interlocking. Hendrik in Germany has a question about WhatsApp and interlock protocol: Wondering if the code comparison in WhatsApp encryption could be verified via the interlock protocol, by sending alternating digits. You have to explain what this all means.

Steve: So I thought that this was sort of fun. This was - we talked about how, with Signal, and I want to be careful with my wording because when we say WhatsApp, what we're talking about is the Signal protocol in WhatsApp. I'm comfortable talking about the Signal protocol because that's what's published, and it's what we know Moxie and his group have worked on in order to just nail. And, boy, they got it right. So when we were talking about this a couple weeks ago, the whole - we come back to authentication.

And so what Hendrik is asking about is could we verify the identity of the other person by sending alternating digits back and forth. And the problem is that you have to have an association between the endpoints in order to send alternating digits back and forth. Remember that you could ask the WhatsApp version of Signal to show you that key for the conversation. And that was both a QR code and, what was it, 80-some digits? It was a lot of characters. But the idea was you could then read those to the other person and have them verify them.

The problem is that, if you sent them back and forth - well, okay. I should explain. If you did it by voice, then you would know you were talking to the other person. But if you do it in-band rather than out-of-band, that is, if you use the protocol itself to prove the identity of the other end, well, there could still be a man in the middle. And so they would be verifying the fraudulent connection to them with each of the endpoints, and the endpoints would think that they had verified with the far end when in fact they were verifying with the man in the middle. So that's why the key is an out-of-band verification.

And Leo, you did this when, on the show, your two phones, you showed one of your phones the QR code. That was out of band. That was the optical channel directly between phones, not going through the connection. And that's what you have to do. You have to have some sort of independent verification, just once, and then you absolutely want to turn on the "Notify me if this contacts verification ever changes" because it's not that it absolutely can't ever. But it should absolutely raise a red flag. And I don't know why that's turned off by default. That's just nuts that it's off by default because the contact changing is a serious man-in-the-middle warning, and it just ought to be part, it ought to be on by default.

Leo: Yeah.

Steve: So that's the one thing that I think they got wrong. Clearly, for convenience and usability and because most people wouldn't know what it meant if it popped up. Unfortunately, the only reason it's really going to pop up is if there is somebody who's stuck themselves in between. And the system was designed with that authentication to prevent that. So anyway...

Leo: Nice. Very cool.

Steve: You can't do it in-band. You have to do it out of band.

Leo: And that, ladies and gentlemen, concludes our edition of Security Now! for this third day of May. Thank you, Steve. I'm just connecting up to the Tor on here so that I will be able to surf completely, like, well, mostly anonymously.

Steve: I'll bet this is going to be - this'll be a hit with our listeners, Leo. This is the cutest little thing.

Leo: Yeah, I just love the idea. And the thing is, I just carry it around so that it's an easy thing to use if I'm at an open access point or a hotel. I got it before - I was trying to get it before the cruise because I knew I was going to be a whole week on an open access point on the cruise ship, you know, their WiFi. And I thought, that's disaster. [Crosstalk] a whole week. And there are 5,000 other people using it. I probably should have some sort of protection. Unfortunately, it didn't come in time. But there you go. I don't think I got hacked.

Steve, it's always a thrill, always a slice. I'm so glad...

Steve: A thrill.

Leo: It's a thrill and a chill. And we didn't mention "Silicon Valley" or "Veep" or "Game of Thrones" or "Expansion" or...

Steve: Or "The Night Manager."

Leo: "The Night Manager," episode two was even better.

Steve: Yes.

Leo: They kind of started a little slow, as you said it would. Episode 2, "slow" wouldn't be the word I'd use. Wow.

Steve: Yeah, I can't wait till tonight.

Leo: I love John le Carr. I just think he is the greatest, the best spy writer because he was a spy. He was in MI6. All right, Steve. We do the show...

Steve: Okay, my friend.

Leo: ...every Wednesday, Tuesday, I'm sorry, Tuesday, 1:30 Pacific, 4:30 Eastern, 20:30 UTC. You must tune in and watch, be in the chatroom. If you can't, though, don't worry. On demand audio and video is available. Steve's site has it, GRC.com. He's even got written transcripts. He's got audio at his site. He also has great stuff including SpinRite, the world's best hard drive maintenance and recovery utility at his site, and lots of freebies. He's very generous with the freebies. You'll also find versions of the show at TWiT.tv/sn, or subscribe in your favorite podcatcher so you won't miss an episode. And as I mentioned, LeoLaporte.com, my blog, LeoLaporte.com has a script, several, one in Python, one in bash, and one in PowerShell, that you can modify to your heart's content to download every single episode, if you wish, of Security Now!.

Steve: Wow.

Leo: The PowerShell downloads from your site. I think the Python and the bash scripts - they're very simple, by the way. You can look at them and assure yourself that there's nothing going on.

Steve: Nothing nefarious.

Leo: As I say, nothing nefarious. Thank you, Steve.

Steve: And next week, IoT, I believe. We'll talk about Samsung's SmartThings and other nightmares with your refrigerator.

Leo: And, you know, one of the things I really enjoy doing when I use Tor is just seeing where I am. Let me just see if I can find out what my IP address is. You know, if you just type "IP" into Google it'll tell you?

Steve: Yeah, yeah.

Leo: Where you are? Although, because it sees me coming from a Tor, it's asking me for a CAPTCHA.

Steve: Ah.

Leo: "Our systems have detected unusual traffic." I am at 128.153.145.125. And I'll have to do a WHOIS to figure out where in the world I am. I really enjoy that.

Steve: Where in the world is Leo?

Leo: So my traffic, you know, it bit me because I signed into Facebook, and Facebook blocked me, saying you're signing in from Cairo.

Steve: Ah. Nice.

Leo: I'm at Clarkson University right now. So there. Isn't that fun?

Steve: Who knew.

Leo: Who knew? And I'm sitting here in the Brick House.

Steve: That's very nice.

Leo: Thank you, Steve. We'll see you next time on Security Now!.

Steve: Okay, buddy.