SECURITY NOW!

Transcript of Episode #474

Listener Feedback #197

Description: Leo and I discuss the week's major security events and discuss questions and comments from listeners of previous episodes. We 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-474.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-474-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. The iPhone 6 is here. We'll talk a little bit about iPhone security. And then we've got lots of questions about all sorts of things coming up next with Steve Gibson and Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 474, recorded September 23rd, 2014: Your questions, Steve's answers, #197.

It's time for Security Now!, the show that protects you and your loved ones, your online presence, your privacy. It's really expanded, hasn't it, to privacy as much as security. Steve Gibson is here.

Steve Gibson: Oh, boy.

Leo: Go ahead.

Steve: Yeah, I was just going to say that I heard the questions you were receiving during your Tech Guy show on the weekend. And oh, boy, are people, like, wound up and worried about this.

Leo: That's an interesting issue. And we're going to...

Steve: Yeah, it really is.

Leo: We have a Q&A episode. But I think your take on this is very valuable. You and Jeff Jarvis might be on opposite ends of the continuum. I don't think you're in completely disagreement. But, and I think I'm more on the Jeff Jarvis end. But the issue comes up a lot of trust and privacy. And my feeling is, if you get too crazy about this stuff, then we're not going to get the technologies that we have. I mean, if you're going to use the Internet and technology, if you want it to be safe, completely private and safe, you're going to break it.

Steve: Yeah. I think we're going through a rough patch as a consequence, I mean, in the entirely predictable reaction to the Edward Snowden revelations and the NSA. Arguably, nothing has really changed.

Leo: Yeah.

Steve: One of the things, one of my followers broke down the CA Trust Root Store in iOS 8, which Apple published. They said, "Here are the trusted roots that we trust in iOS 8." And we'll talk about that here in a minute. But it's very interesting. It absolutely supports my contention that us running around in circles like something's on fire is just an expenditure of energy for no purpose. The idea, I mean, and my point is that I'm sure deep in the bowels of the intelligence agencies all of us, all of our handwringing over maybe there's a flaw in the pseudorandom number generator that got slipped into this, and oh my god, you know, while the DOD, the U.S. Department of Defense has - and I'm scrolling down to look for it here - five trusted root certificates in the Apple trust. So they can make any certificate they want. They don't need to crack any crypto. They have keys to the front door. They don't need any freaky backdoor, like oh, my god, maybe the bits have a slight skew from pure entropy.

Leo: Well, that's interesting because we didn't know this for sure last week. We were saying it's likely. And so that is the fact.

Steve: Yeah. And the Hong Kong Post Office is listed in Apple's list.

Leo: But is that the Chinese government, the Hong Kong Post Office? Is that...

Steve: Who imagines that, if the Chinese government says "We'd like a certificate," that Hong Kong Post Office is going to say no.

Leo: Right, right.

Steve: I mean, it's probably an operating branch. So anyway, so what I started to say was I don't think there's been any massive change at all. I mean, one of the questions in the Q&A, which we'll get to, is a great discussion starting point for the work that Google is doing to move things forward. And I completely agree with its assertion and the idea that in general it's just useful to, I mean, these are useful things to study, useful things to look at, and the Internet ought to move to encryption, if only because we've gone from AOL email as pretty much all anyone was doing to real dependence. I mean, in the same way you sort of, you know, my advice about people using PCs, they would say, "Oh, yeah, I don't really back it up because there's nothing on there. We just surf the 'Net and answer email from Aunt Edna." Or, and this also came up back in the days of firewalls. It's like, "Oh, we're really not worried about the security of our computer."

And I said, well, you know, what's going to happen is your usage is going to creep over time. It's going to expand. Your bank will say, hey, you know, we'll give you a lower rate if you won't ever show up in our facilities, if you'll just do this online. I was planning a trip for a nephew's wedding over the weekend, and I had to change plans at the last minute. And I was at the gate, and this gate attendant said, "Well, do you have a smartphone?" And I said yeah. And she said, "Well, it's cheaper if you just go over and do it on that, if I don't have to talk to you." It's like, oh, okay.

Leo: That's a good tip. Thank you.

Steve: So, yes, thank you. So what happens is our usage expands, but our security lags. And it's that window that exists between our expanded usage and security. Security lags, I mean, and this is really what Google was working to directly address in last week's topic of forcing end-user sites to fix their certificates preemptively, is they were looking at the lag they saw last time and saying, oh, we have the power to force a change, so let's use it. And so what I'm seeing is a continual increase in people's use of the global network for things that are increasingly private. So whereas it might have just been fan mail from Aunt Edna, now it's things that they realize they really do want to imagine they're keeping private.

And even though I would argue ultimately they can't because governmental power can crack our crypto unless, I mean, sort of the generic operating crypto. If I encrypt something with a key that only you and I share, Leo, I'm absolutely certain that I can send that blob to you, and it cannot be cracked. But things like website communications, which are now encrypted increasingly by default, yeah, that can be opened if somebody with sufficient resources like a government chooses to do that.

But still in general I think the movement toward everything being encrypted, I mean, that's where we're headed. And everything being encrypted is better than it not being. If nothing else, it prevents the casual sniffing which we've seen in open WiFi situations that just discloses an amazing amount of information. And so we're just sort of moving in the right direction and having a lot of fun in the meantime.

Leo: Yay. Well, we've got a Q&A today. You've got tech news.

Steve: We do. I do have the note - I've not gone through this whitepaper. I'm probably just after because there's not a huge...

Leo: The Apple, the Apple whitepaper, yeah.

Steve: Yeah, sorry, thank you. I'm looking here at the words "Apple iOS Security," and I realize our listening audience can't see where my eyes are focused. It's been such a short time since we did an exhaustive coverage of iOS 7, and there are apparently some things that have changed. But the bulk of iOS 8 security was reflected in that iOS 7 security. So I plan to read through it and probably come back with, okay, here's the things that I see that have changed in 8 from 7. And, I mean, and there has been news of improved security.

Leo: Well, the big, the TLDR, the big one is that Tim Cook has said, and of course we trust him, that they now encrypt the data on the iPhone in such a way that they cannot hand it over to the feds.

Steve: Yes, I think that's really interesting, that they're saying that no longer can they even accept phones in this escrowing queue where ultimately they get to it, and then they perform some sort of brute-force attack. They're saying no. And I think he's clearly keyed in on exactly the angst that some of your callers over the weekend were expressing. They're saying we're about privacy because these little slabs of beauty are our product, you are not. Whereas - and of course he's clearly aiming at Google, saying their harvesting of everything they can learn is the way they generate more revenue. So he's using that as a differentiating point.

Leo: Absolutely, yeah.

Steve: Also CloudFlare announced what they call "Keyless SSL" that I want to just take note of. Google and Dropbox have teamed up with a new venture. Google, a bunch of a people tweeted me about a "malvertiser" that was operating under Google's nose, which they stomped on. And I have a huge thanks to offer Android users everywhere.

Leo: Uh-oh.

Steve: And 10 really interesting questions and talking points from our listeners.

Leo: Coming up on Security Now!. All right. All right, Steve. Let's get into it.

Steve: I will do a deep dive into the iOS updated whitepaper, which as Rene expected, I'm well aware of, and see what I can find that they've changed. But it's hard for me to imagine what that might be because as far as I could tell they pretty much have it nailed. But what I thought was interesting, there's a blog posting, as I mentioned, of an analysis that was done. His name is Karl Kornel, K-A-R-L dot K-O-R-N-E-L dot U-S. And so if our listeners are interested, there's more details that I'm going to cover here. I'm just going to touch on some of his brief, sort of the bullet points here.

So, for example, there are, in iOS 8, 222 trusted root certificates, meaning that any certificate signed by any of those 222 roots, is trusted because we are trusting all of those roots. The bulk of the certificates, those root certificates, are signed using 2048-bit RSA signatures, and that's 138 of the 222. So 2048-bit, which is sort of the - that's the existing but fading out standard being replaced rather quickly by 4096-bit signatures. Forty-four of the certificates, the root certs are signed using 4K-bit RSA signatures. And this is all kind of confusing because these are, I mean, 4096 bits is an incredibly long signature, but that's because RSA itself isn't as strong as some of our newer technologies.

So, for example, also the next-generation ECC, the elliptic curve signatures, 12 of the CAs have 384-bit. And so that's 384 bits of ECC signature is roughly equivalent to the strength of 4096-bit RSA. That is, you just need a lot more bits to make the problem under RSA sufficiently difficult to solve, to the same similar difficulty as you can get using only 384 bits of elliptic curve. And since bits take time to process, that's also why ECC is seeing much more popularity. It achieves equivalent strength with a much shorter key, and that equates to much faster processing time because you just have to deal with fewer bits.

So those are the various keys. The predominant signature algorithm is still SHA-1; 149 of the CAs are hashing their certificate using SHA-1. So it's 149 SHA-1. Next down is what we were talking about last week, SHA-256, 42 certificate authorities use SHA-256; 17 SHA-384; and one of them SHA-512. And oddly enough, there are three certificate authorities that have signed their cert with MD2 that's, like, I'm curious actually to know which three they are because that's just - that's crazy, MD2. I mean, that's worse than MD5. And 10 CAs have their certs signed by MD5.

The problem is that the root doesn't expire. These root certs, they, like, have expirations in 2038. And I'm not sure if they go any further. 2038 is a weird year because I think that's the year that the UNIX time wraps around. And we're going to be, if the podcast is still going in 2038, we may actually have a Y2K experience then because, when the UNIX time wraps, we may be in for some fun because - although it's been understood that that's happening for a long time, and extensions have long since existed for that. But I do, for some reason, I'm remembering certificates expiring in 2038.

The point is that the roots don't expire because they're built into our infrastructure. It's the certificates that they sign which expire every two or three years and need to be continuously renewed. So some interesting demographics there. However, I'll just wrap by saying that Karl scanned, just visually scanned the list and noted a number of governments that have trusted root certs in Apple's iOS 8 store. And I don't mean to be singling Apple out at all. I mean, I'm sure this is the same certificate store that is in the Macs. And if anything, Microsoft trusts twice as many. As I remember, they're in the 400s of root certs. So Microsoft is probably a superset of these.

But, for example, we've got a certificate not only from the Hong Kong Post Office, but China itself. The China Internet Network Information Center is a trusted certificate signer. Japan has three CAs, certificate authorities. The Netherlands has three. Taiwan has one. Turkey has one. And the United States has five, as I mentioned, via the Department of Defense. So these are all equally trusted, meaning that, in the same way that Google, well, Google may be an exception, at least under Chrome, because they do so much certificate pinning. Like they're able to spot certificates, forged Google certificates if you're using Chrome because they look at the exact signature, not just to see if the signature is valid. But what I was going to say was that all these roots being trusted is, I mean, what that implies is that they can sign a certificate for any website they choose, and no alarm gets raised.

Now, anyone scrutinizing the certificate chain would see that this terminates in an odd place if it wasn't signed by VeriSign or DigiCert or GoDaddy or one of the biggies. It was signed by China, or it was signed by the U.S. DOD. But for selective decryption, that is, for selective interception of specific traffic, it's difficult to imagine that, because they risk exposure, because they can't do this and have it completely unseen, but they certainly can do it on demand, I'd be very surprised if this wasn't something that was being done on a limited basis, that is, if this wide body of trust isn't doing things we wouldn't expect.

And everyone will, actually people who have either started recently listening to the podcast from the beginning or have really good memories will remember the podcast when, after years of being away from looking at the trusted root, I had an occasion to look at it, and I came back on the podcast, and I said, oh, my god, Leo. I mean, I remember when there were 12.

Leo: I do, yeah, yeah, yeah.

Steve: Remember? And I remember saying...

Leo: And the Hong Kong Post Office has been the butt of a joke ever since.

Steve: Yeah. I remember saying, "This is bad." I mean, and then I explained why my mind was blown, that, like, without me paying attention or anyone particularly paying attention, it had gone from, like, 12 companies who were in the business of selling certificates to, like, the Hong Kong Post Office and everybody else who we were trusting equally. And so just like, well, that's the way it works. But again, I think the point here is to understand what's going on. And that's what the podcast is for, to explain that what we're getting now is a useful next level of encryption. But it is still not TNO. TNO is different. TNO means you're not even trusting the root certs. You're not trusting anybody. TNO, Trust No One, means you have arranged to have a key, you've encrypted your data yourself, and you've given it to somebody else to whom you have somehow managed to communicate that key. That technology I believe cannot be cracked. I mean, period. I mean, really, truly.

But that's not the security most people use. Most people use a security which is good. It's like iMessage. It's like, if Apple is handing you the keys - people say, "Oh, Apple doesn't have the keys." Well, yes, they do, because they've given me the key which I've used to sign a message to someone else. So they could also give me a key to sign a message to them, and I wouldn't know it. So the point is we are getting encryption. It's better than not having it. But it isn't TNO. TNO has the beauty of being absolute. We can say this is absolute security. And it isn't what most people use. But most people really don't need that level of crazy absolute security.

CloudFlare is a service that we've talked about. One of our favorite techies, John Graham-Cumming, is one of the technologists there, over in the U.K. And he did the book, what was it, it was the really tech...

Leo: A couple of things. One was the travel, like the top 30 spots geeks should see in the world.

Steve: Yeah, yeah, yeah, really neat things. Yeah.

Leo: He's a neat guy. We've known him for years.

Steve: Yes. Anyway...

Leo: He also got Alan Turing's name, he got the apology from the British government.

Steve: Oh, did he.

Leo: Yes.

Steve: Nice. That's right, I forgot, yes. And we did talk about that. And in fact somebody sent me or tweeted something, I don't remember what it was, but it was just recently, they had gone to the museum and were really moved by the strength of the apology that was now there and made...

Leo: Was it Tony Blair? I think it was - I don't think it was Cameron. I think it was Tony Blair. Anyway, yes. So he's a great guy.

Steve: So the question is, their business is protecting websites from attack. And they've had a problem, which is, if they are what the web browser connects to when it wants a secure session, they have to have the keys for the website that they're standing in for, and they need to stand in for the website in order to filter the traffic. In their blog posting announcing - and this is just in the last week - announcing what they call "keyless SSL," they explain how two years ago, in 2012, they got a call from one of the world's largest banks, in New York, at a time when they were just a small startup.

And this banker, the, like, CEO or CIO, said, "We're suffering denial of service attacks of a strength we can't handle. We need to talk. Can you guys come?" And the author of the blog posting for CloudFlare said, "We were a small team," and he took a little tangent and talked about who wore shorts too often and the Hawaiian shirts and so forth, and said please don't wear your khakis to the meeting of the president of the largest bank in the world.

So they flew to the states. They flew to New York, met with the banker or the CIO. And the problem was that the bank wanted the protection, needed the protection of a massive pipe and denial of service filtering technology in front of the bank's network; yet, being the bank, they could not release the keys. They said, in fact, any discovery that we have lost control of our private server keys requires an immediate disclosure to the U.S. federal government.

Leo: Wow.

Steve: I mean, it is critical. So these guys flew home. And it's funny because he said that they spent some time on the chalkboard, and the engineers' minds got engaged. And they named someone, I don't remember his name, and they said he's the kind of guy who cannot sleep when he's working on a problem. And he says, "That is a hiring criteria at CloudFlare." So...

Leo: I love it.

Steve: Yeah, it was great.

Leo: I want to work there.

Steve: Yes.

Leo: I love that.

Steve: So they've just announced a solution to the problem. It's not hard to do it in a way that doesn't scale. It's very difficult to do it in a way that scales. And I've not looked at the whitepaper. There's a technical nitty-gritty details whitepaper. I will check it out and figure out and see if there's enough meat there because it's interesting. It's an intriguing problem in security. Basically you need to farm out, you need to subcontract the SSL, the TLS, HTTPS negotiation to a third party while never giving them your security certificate. So somehow they've arranged to proxy the connection. And again, immediately you can see how it's possible. We've talked about the SSL handshake, how there's a communication process.

So one could imagine that there was probably a way for them to send a query to New York to get some of the crypto stuff, which then comes back, and then they send it to the client and so forth, where they're sort of being a privileged man in the middle, but they need to do it in a way that doesn't disclose any of the sensitive crypto material that the party that they're standing in for has. And they've solved it. So anyway, I got - a bunch of people wanted to make sure that I knew about that. I do. And I will dig into it and see if I've said all that really needs to be said, or if it's an interesting topic for the podcast.

Meanwhile, Google and Dropbox have - this just sort of is a news bullet, not a lot of technical news here, in fact none. But I thought it was interesting that they had formed a team. They've created a new entity called Simply Secure at SimplySecure.org. And pretty much nothing is there right now. I guess they've just sort of - they created an organization called Simply Secure. Their charter is to search for ways to bring the security in the lab to the real world, recognizing that - and one of the team leaders has spent time at Google. She, too, was involved in the second-factor work and just sort of in general in security-focused, customer-facing, user-facing security.

And we all recognize that there is cryptographic technology that isn't yet being used. I mean, my own SQRL system, which is not a breakthrough, it's just the application of standard crypto. It's like, look, that's why I was tempted to call it HIPS, Hiding In Plain Sight, because it's like, okay, why hasn't anybody done this? So that's an example of something really simple, really secure, that just isn't being used. So anyway, we don't know what's going to come out of them, but I wanted to just sort of note the spawning of this organization, SimplySecure.org, by Google and Dropbox. And we'll kind of keep an eye on it and see if they come up with something interesting.

And Google did have a problem this last week, they shut them down on Friday, with what's called a "malvertiser." They were serving ads through their DoubleClick subsidiary - remember they bought DoubleClick a few years back - from another ad network called

Zedo, Z-E-D-O, dot com. And one thinks that this was one of those domain-name-driven companies, where it's like, okay, what names are left? Zedo is left.

Leo: Yeah.

Steve: Okay, fine. Well, that's only four letters. That's good, we'll go with Zedo.

Leo: You did check SQRL.com, I hope.

Steve: Oh, yeah, that was gone a long time ago, unfortunately. Although I got it in a few random, off-brand domains, just to have it.

Leo: Hey, at this point parents ought to check the web to make sure they can get their kids' names for the URL. Don't name a kid John Smith. I mean, forget it, you'll never find him.

Steve: Yeah, and, boy, will he get spam.

Leo: Right. Right. So I think parents - watch, because kids names are going to get wild soon.

Steve: Yeah. I think it hasn't - it's been a while since I've mentioned, but Jenny told me that she had her friend, Diana, who was just being buried under spam. And unfortunately Diana has her own domain name for her yoga dojo or whatever it's called. And so it's diana at yogadojo.com. And when Jenny said what can she do, I said she can change her email address. And I've looked at the packet traffic at GRC's SMTP servers. And it is random, it's not even lists.

Leo: They try all common first names.

Steve: Yes, yes. Something connects, and it just sits there and goes through Bob and Bill and Benny and Bert and Bernadine and so forth. And for a long time I was steve@grc.com. And of course I was being killed, not because I was, I mean, I had an email address for a long time, but because my email address was just Steve. And what I realized was all - in fact, it's one of the nice things we have now is if - I'm using hMailServer. And it will see that behavior and put in a temporary blacklist of any web server that connects. And it had, like, three misfires of name that just don't exist in our domain at all, it just says, okay, this guy's just guessing. We're just going to block from now on, you know...

Leo: Smart, smart. That's good.

Steve: Yeah, blacklist them.

Leo: Yeah.

Steve: So anyway, this Zedo.com was probably, I mean, I looked at their website. They look legitimate, too. So I think what happened was they were inadvertently hosting a malicious ad that somebody sent through their network, which they then sent through DoubleClick, which then Google sent out to Last.fm was one of the big sites hosting this malvertising, The Times of Israel, and The Jerusalem Post. So draw your own conclusions. But those were the three that were mentioned as being the heavy carriers of this malicious ad which was hosting JavaScript, of course, which would then download the Zermot downloader, Z-E-R-M-O-T, which is well known. Microsoft knows about it, Windows Defender and Security Essentials both know about it.

So pretty much anybody who had good, active, up-to-date antimalware would probably not have had a problem. But anybody who wasn't running antimalware and visited those sites, and I don't think you needed to click, I think it was a no user action required, the script just ran and somehow leveraged some behavior in the browser to get outside of the browser sandbox, and people were being infected. So the moment Google found out, which was last Friday, they foreclosed, they lowered the boom on Zedo.

Leo: Yeah. And this isn't the first time this has happened. We've seen it happen with any kind of - Yahoo! has had it happen to them - automated advertising platform. They're set up so that you don't have to get anybody's approval. You just buy an ad, and you put it in there. They've got to fix that. That's not a good, you know, unattended HTML and CSS and who knows what else is not a good thing.

Steve: Yeah. It is really, I mean, it's an inherent problem with the way the advertising model has developed. I mean, and I've talked about this. I see, because I'm using NoScript, I'll like click on the little logo in the toolbar. And I look at the number of domains which are enumerated there by NoScript which are referred to by the page I am visiting and trying to provide their own content to this page. I mean, so the truth is that servers are trusting a vast network of other content. And it's just sort of - it sort of accrued over time like barnacles. It's like, oh, well, we want to be able to use the features of jQuery. So jQuery is now one of the blobs that each web page we serve, I don't mean "we" GRC because I don't use them. But that's the way these things are done is browsers are pulling from an incredible number of third parties.

And one type of third party that just tends to be a little more in the gray zone is ad servers. They're just serving lots of ads. And so, and the fact that they have the ability to change the content at will, and in some cases to make them sensitive to the context of the user or where they're visiting, it's like, well, ads on this site will tend to have this kind of content. That means that you're not able to lock them down and check the script and then ask it to qualify through some checksum. The ads are just changing all the time.

So it's a disturbing aspect of the way we're using the web. And we'd like to be able to turn off JavaScript, but I'm running into more and more sites that, over time, we would expect this, over time sites are becoming increasingly dependent upon scripting. They're wanting to run code in your browser to offer you the more, the web, whatever version we're on now - I think I heard Andy say it's 49.2, you know, web version whatever - in order to give us the features that we want. So less and less, running with no scripting enabled at all is becoming infeasible. Okay. My huge heartfelt...

Leo: I'm waiting for what this is. This is good. This is - something's going on here deep.

Steve: Thank you, thank you to all Android users everywhere.

Leo: Okay, you mentioned this. Now I'm worried.

Steve: Because when I posted over the weekend that my life had been changed by the ability to install third-party keyboards, I got tweets back saying, "Welcome to 2010."

Leo: Yeah. This is the new meme from Android folks, yeah, yeah.

Steve: Gibson, it's like where have you been, where have they...

Leo: Ooh, predictive text. Are you excited? Are you excited?

Steve: Okay, so Leo.

Leo: We had that on the BlackBerry, I think.

Steve: I've ended up settling for Swype.

Leo: Oh, really. Okay.

Steve: Yeah.

Leo: You know you can swipe on SwiftKey.

Steve: Oh, I know. But Swype does a few things that I like better. If I Swype a word, and it's wrong, backspace removes the entire word.

Leo: That's nice, yeah.

Steve: That doesn't happen on SwiftKey.

Leo: Okay, okay. That's good, yeah.

Steve: So normally that's a better thing. Also, although there's more a bit of a learning curve associated with this, when iOS first came out, you and I were talking about how you could hold a key, and then you'd get a little submenu that would pop up. Or you could just, like, stroke upwards from the comma or something, and you would get a double quote. I like those power features. Under Swype, the entire shifted keyboard is always there without shift, if you just hold. So, for example, I now know that G is open parens and H is closed parens. And so to me that's valuable. I did have to learn it, but now I can - because I like to parenthesize things, that's nice.

Leo: You iPhoners, you're just so cute.

Steve: And, okay, okay.

Leo: By the way, no, that's a huge - SwiftKey does that, as well. But that's a huge feature, I agree. I agree. I use it all the time. For numbers and all punctuation.

Steve: And swiping Z down to the spacebar gives you a quick exclamation point. Swiping M, I think it is, or L down gives you a question mark. Anyway, the point is, oh, my goodness. And I have given it some words. I was just chuckling because I'm having to go, like, back and forth across the keyboard, blah blah blah blah, like Busterfreedonical or something like that.

Leo: Oh, yeah. Oh, yeah.

Steve: Some crazy word. And it says, yeah, there you go. And it's like, oh, my god. Anyway, I'm having dinner with Jen, and I'm going to change her life, too, because she did upgrade to 8, but I haven't had a chance to sit down with her and show her this. And my best friend Mark's going to join us. And this, I mean, oh, my god. Well, you know, I cannot stand that old keyboard on iOS pre-8.

Leo: I've hated it for years, yeah.

Steve: It was the worst thing.

Leo: It kind of bugs me because it still pops up whenever you enter a password. So you have to kind of go back and start using that keyboard, which is...

Steve: Yeah, and there's a couple problems.

Leo: I understand why.

Steve: Tweetbot has a problem, I guess, with third-party keyboards. I don't think it's the keyboard. It's Tweetbot. So I can't use them yet. But these things will get fixed.

Leo: A couple of points, though.

Steve: But I just wanted to say thank you, thank you, thank you. Wow.

Leo: A couple of points. First of all, press and hold backspace will delete a full word back on SwiftKey, so it does have that capability.

Steve: Ah, okay, good.

Leo: You just have to hold it for a little longer.

Steve: And we should mention SwiftKey is free, but Swype is either one or two...

Leo: Right, 99 cents.

Steve: Okay, 99 cents.

Leo: Yeah. The other point, well, it's a question because of course the first thing that happens when you install a third-party keyboard is Apple puts a very long, very scary warning, "That keyboard is capturing all your keystrokes and sending it back. We don't know what they're doing with it." Android, to Google's credit, does the same kind of warning. But it seems to scare people. So you're not worried about that?

Steve: Okay. So SwiftKey does that. Swype doesn't. Now, okay. Also I should mention that Swype runs on the iPads. SwiftKey doesn't. So...

Leo: Well, SwiftKey runs in an iPad, but it doesn't do Flow. Doesn't do...

Steve: Yes, sorry, correct. It doesn't do Flow. They claim that they don't have sufficient memory, that is, that the memory allocation...

Leo: Oh, that's interesting.

Steve: ...that the pads give them isn't enough to allow them to do Flow.

Leo: Right.

Steve: And Flow is the only thing I want. Oh, my god.

Leo: Oh, I agree. It's much faster than typing.

Steve: Yes. And I saw you mention, Leo, that you, like, swipe - you Flow down to the spacebar as if you're doing multiple words in a single swipe, which I'm not. I'm lifting my finger at the end of a word.

Leo: No, I am, too. I don't know...

Steve: Oh, okay. Okay.

Leo: Yeah, yeah. No, I am, too.

Steve: Yeah. Then I just misunderstood. So, okay. So I really like the idea of networking because I'm a multi-device person. I've got a pad next to me. There's one that lives in the car. I've got my new big megaphone. And so the idea that SwiftKey would be cloud-syncing the things it's learning about me on these different devices, that's a convenience.

However, I received a ton of tweets over the weekend from people say, well, yeah, but SwiftKey - because I first tweeted about SwiftKey, saying, oh, my god. And then the more I looked at it, I thought, you know, I think I just sort of do like Swype better. Well, for one thing, I really like being able to do the Flow over on the pads, and I'm still a pad user. Although Flow on a big keyboard isn't really, you know, it's a lot of movement. Although I guess your fingers are still moving when you're tapping on a big keyboard. But anyway, I just wanted to say thank you to Android users. If you're the reason these apps...

Leo: You can also thank Android users for these big phones, too. I mean, I don't think Apple would have done a 5.5" phone if it weren't for all the...

Steve: Oh, in fact I wanted to mention the funniest reaction that I was noting of myself is when - because I got the white bezel gold tone, champagne, whatever the hell they call that, iPhone. It's the first one I have ever got that isn't black. But I thought, eh, what the hell, it looks pretty. And every time my eye fell on it, I thought Samsung. I mean, it just...

Leo: The white one looks a Samsung? Yeah.

Steve: It does.

Leo: It really does.

Steve: It's, I mean, and I'm so - after years of these big white Samsung phones, that's what I think I own. I look at it, and my brain says, "Okay, that's a Samsung."

Leo: Guess I went Samsung, and I didn't even know it. Yeah, I think those were the two issues I had with iPhone were the screen size and the keyboard.

Steve: Oh, yes. And I now look at my 5s, and I think...

Leo: It's dinky.

Steve: ...how did I ever - no wonder I never actually used it. I had, to give you a sense, lifetime talk on my iPhone 5, which I happened to see as I was decommissioning it was three minutes.

Leo: What?

Steve: I've never had a...

Leo: Three minutes?

Steve: I've never spoken on my iPhone 5 except, like...

Leo: You have no one to call. Who you going to call?

Steve: I don't use it.

Leo: Have you started using - we're not going to turn this into the iPhone show. But have you started using in messages the audio?

Steve: I see that. I haven't yet...

Leo: Jenny uses an iPhone. It needs to be to other iPhone users.

Steve: Yes, she does. Oh, and that's the other thing. In the whole iPhone versus Android, because I've been listening to you for the last week, I wanted to mention that it is also a function of ecosystem. I don't know a single Android phone user.

Leo: Well, you know me.

Steve: My entire family, all my friends. But, I mean, like the people I'm in total constant texting mode with. And we have, like, iMessage groups.

Leo: And in that case, that's a very compelling reason to use the iPhone because, for instance, iPhoning to my daughter, half the time I don't text her, I just give her an audio thing. Same thing to Lisa, she's an iPhone user. And that really is compelling. You can send pictures very easily the same way: Hold the picture thing down. It'll snap a picture and then slide up. It'll send it.

Steve: Yeah. And I do agree with you, that double-touch nonsense about sliding the screen down? I just think that's, like, somebody said, hey, you know, we can sense when you tap the Touch ID without pressing the button. So...

Leo: Let's do something with that.

Steve: ...what can we do? Exactly. Let's make that something. It's like, oh, okay.

Leo: Some people love that. And you know why I don't care about it is because Android phones have these menu keys at the bottom. And so most of the stuff that I want to do is within reach of my thumb at all times on an Android phone. I realized - so maybe I'm not being fair to the people who use iPhones who are really thrown by this mega screen. You call it your megaphone. I like it.

Steve: It's the megaphone. I also feel like they're halfway there on the screen rotation. Boy, is it buggy in some places. And it just doesn't work. And it's like, okay. Either do it or don't, but don't choose not to do it when maybe you ought to. So it's like - or I just think - I think it's a little - it's showing - oh, and in general I should just say that the feeling I've had in listening to you talking about this is, or in some cases ranting, as you were at various points over the weekend...

Leo: I've been in rant mode for a whole week.

Steve: And I was in agreement in some cases. It feels to me like Apple is struggling with the phone's identity. It began as a beautiful closed system of very simple, like duh, use it, apps, where there was nothing hidden. I mean, there was like, they were all of them beautifully crafted, very simple. But they are trying to power this thing up into a pocket computer. And now we're getting interapp communication. And we've had, thank goodness, copy-and-paste functionality to transport information back and forth. But, I mean, the problem I think we're having now is that their interface is beginning to collapse. The super simple UI is struggling under the demands of a much more sophisticated device that really wants, like, multiple-choice dropdown menus and a more classic desktop UI, yet we're not getting them. Instead we're just kind of getting funky operation.

Leo: Yeah. I haven't decided, but I think I'm going to stick with Android. I'm waiting to get my cognac leather-backed X. And we'll see.

Steve: And I'll just say again I agree with you that I think the watch is a fiasco. I think it's...

Leo: I'll be interested to see what happens there, yeah.

Steve: Yeah. Especially at the price that I've heard people guessing.

Leo: $6,000 [laughing].

Steve: And I wanted to mention, when Dvorak talked about melting it down, that the gold is not worth nearly what the watch retail price will be.

Leo: Well, I don't know how many ounces of gold you think it is. Four? That would be, what, 12, 2,400 bucks. I don't know.

Steve: I guess the price of gold has gone up.

Leo: Oh, it's a lot, yeah.

Steve: I bought a bunch when it was $400 an ounce, so...

Leo: Well, hold that gold. Is it in your backyard in a hole? I can't remember what it is an ounce now, but it's quite expensive.

Steve: Yeah, it sort of crept up. I got a great little note I just wanted to share, that actually follows up on a question I guess we answered. It was Martin who wrote from Frankfurt, Germany. I ran across this on - he sent it on September - where are we?

Leo: $1,200 an ounce.

Steve: Okay, cool.

Leo: So, yeah. If there's four ounces in there, you're going to have to charge $6,000.

Steve: Boy, yeah.

Leo: But it's not 24-karat gold, it's 18-karat gold.

Steve: Is that harder or softer? That's harder, yes.

Leo: The lower the karats, the harder the gold.

Steve: Right, right. So anyway, Martin says Level 2 "look but don't touch" actually does save the day. And he said: "Hello Steve. Thanks for answering my question about how SpinRite on Level 2 actually fixes things on one of the last shows. Only a few days later I was witness to it actually fixing a huge problem using Level 2. A friend's work PC refused to boot, and his company's IT department gave up on it without being able to recover ANY," Martin has in all caps, "of his valuable data. Of course the backup had silently failed without him or anyone else noticing, and his data was gone.

"So we gave SpinRite a try on Level 2, and it slowed down and started working a lot harder about a quarter of the way in, seemingly not moving any further. So my friend lost patience and turned the machine off. I told him not to give up and just let SpinRite run for however long it takes. Well, after about eight hours of chewing on the drive, it was finished. The PC booted again with complete data recovery. Hooray for SpinRite. Now I am his hero, but actually you are. Thank you very much on behalf of my friend who got all of his data back thanks to SpinRite. Martin."

And I'll just say I don't have a problem, although this is technically not how we license SpinRite, our listeners know that if someone is in trouble like this, I don't have a problem with a friend helping a friend. And this friend now knows about SpinRite, so he may spread the word or grab a copy for himself. So thanks for sharing, Martin.

Leo: You're very generous and genial.

Steve: We've got some great talking points and questions and feedback from our listeners. So I'm glad we do this, 197 times.

Leo: I am, too, actually. It's become kind of an important part of the show overall is to give people a chance to get clarification and get ideas from you.

Steve: And there's some pithy stuff every so often. We have one great note. As you say, we're never going to be finished talking about the stringing Ethernet across a great distance.

Leo: Oh, no, no, more?

Steve: All of us have just been put in our place.

Leo: Oh. Probably by somebody smarter than Nietzsche.

Steve: An interesting gal.

Leo: Matthew Urch kicks us off, though, Matthew, pronounced like "church," Toronto, Ontario, Canada. He found us four weeks ago: Hey, Steve. I found the podcast a month or so ago, and I've been working to get caught up on all the years of great content I've missed between new episodes airing. He says he's listened to the first 93 so far. You've got quite a way to go. What is it, nine years of shows? However, whenever I hear a suggestion of yours and/or Leo's, since the suggestion took place in some cases the better part of a decade ago, I always wonder what the current state of those suggestions are.

Kerio Firewall, remember that? The Astaro Gateway. Blink from eEye, remember that? Really just an update on items that you've thoroughly discussed or suggested numerous times in the past. Reason I ask, I recently listened to the Blink from eEye episode. When I looked it up, the company has been acquired, the product has been re-branded, and the only option is requesting a quote. I don't even know if it's still the same product. Anyway, thanks for the great content. I look forward to getting stuck in traffic so I can listen to more Security Now!. And by the way, I'm planning on buying SpinRite very soon. That is one of the flaws of being such a long-time successful show.

Steve: Yeah, I guess. I wouldn't call it a flaw. I would say that it's a consequence of the fact that the show really is two things. Clearly we care about the news of the day. I mean, it's just interesting, talking about Google's decision to force the change in certificate signature technology, that's really interesting. How can we not talk about that? Now, a decade from now that'll be of historical interest, but clearly not as useful. On the other hand, the fundamentals of the way the Internet works, which we've done a series on, or the fundamentals of computing technology, which Matthew will be getting to here pretty soon. Those are almost timeless. So we have a mix of things.

Now, if we didn't archive them, then we'd purely be broadcasting into the ether. You'd get the ones you could and have no access to the past. I think it's really super useful. But I'm sorry, Matthew and anybody else, it doesn't make sense for us to add to the burden we're already carrying of, like, oh, and here's where we stand with the Kerio Firewall and Blink from eEye. I mean, we can't, you know, we're making archive episodes available because certainly for some purposes they're valuable. But not for here's our favorite twitch from 10 years ago. It's just that there is information that is going to age and decay and no longer be useful mixed in with the stuff that's timeless.

Leo: Look. Somebody in the chatroom pointed out National Geographic continues to publish magazines, and you may have a stack of them, but the fact that you've gone back to 1963 to read that article doesn't put a burden on National Geographic to correct it.

Steve: Ah.

Leo: It's frozen in amber.

Steve: Been published.

Leo: Been published, done with that. So what I encourage you to do, and I'm sure you're doing this, is listen to the current episodes. If you want to listen to the past ones that's great. But recommendations for current products from old episodes, they're meaningless. They don't...

Steve: It is true, though, that we're building on knowledge. And so I was...

Leo: Oh, yeah, no, it's good to listen to the old ones. Yes.

Steve: Yeah, I don't want to discourage anybody from filling up their new multi-gig pocket device with this stuff because there is plenty there.

Leo: It is called "Security Now!."

Steve: Yeah.

Leo: Now. Robert Osorio in Lady Lake, Florida brings back the bouncing battery mystery: Steve and Leo, the answer to why a dead battery bounces is from cannotunsee.net, why a dead battery will bounce and a new one does not.

Steve: So there's a video link in the show notes. I don't know if it's worth going through it. It's actually pretty long, Leo. But I'll summarize it as follows, and remember that I think we talked about this on the podcast. This sort of hit the meme of the day a few months ago where bizarrely enough it was found that a dead battery bounces actively, and a live battery with still juice in it to give just thuds. And, I mean, it was just a great Internet meme that occurred. And so these guys do a series of experiments.

Leo: They actually built a device so that they would have the same trajectory each time.

Steve: Yeah, yeah. So, I mean, and...

Leo: Oh, look it, it does. It's true. You really see it.

Steve: Boing oing oing oing oing. Yeah.

Leo: This is like a ping pong ball.

Steve: And now charged up, blunk.

Leo: Yeah. No, that's true. Well, there we go. That's proof positive it does it. So why does it do it?

Steve: So it turns out that a used-up battery is - oh, and then they have theories of outgassing, or I don't remember what they called the other one. Apparently there's something called a "recoilless hammer"? Never knew about that.

Leo: Oh, yeah, yeah, yeah.

Steve: You can get a hammer that's got, like, BBs in it.

Leo: Right.

Steve: And when you hit something with it...

Leo: It thuds, yeah.

Steve: Anyway, so the point is that - and this is the way - I would normally never be able to remember which bounced and which didn't. Is it the charged battery that bounces, or the discharged battery that bounces? Now I have a way of never knowing because what happens is the electrolyte is completely dried out in a used-up battery. It is not gooey at all. It is dry. And so it acts as a solid. Oh, and so here they're doing outgassing. They're dropping something on the battery to see if it's springy or not. So they're dropping a slug...

Leo: Oh, lord. They really did this seriously. That's amazing. They care a lot about it.

Steve: The point is that a battery filled with wet goo doesn't bounce. It thuds because the properties of the goo essentially absorb the battery's kinetic energy.

Leo: That makes sense, yeah.

Steve: Whereas the dry battery bounces like a bunny rabbit. So now we know. Thank you, Robert. And in this video that I link to, they get around to sawing the batteries open and, like, sticking stuff in and stirring it around. And you see that the one that just thuds, that's got charge left in it, is just a gooey mess inside; whereas the dead one, oh, my goodness, it looks like a dry creek bed. So complete difference.

Leo: Cannotunsee.net. And that's actually a great site. They've got a lot of interesting stuff on there. It's a tumblog.

Steve: It's like something like old guys, retired engineers or something, having dinner or something.

Leo: They have some sort of ad for ROMEO: Retired Old Men Eating Out.

Steve: That's it.

Leo: I don't know what it is. Is it a group? I don't know what it is. But maybe you and I should join. Melissa Good in Miami, Florida teaches old engineers something about Ethernet. Steve, one reason why fiber should be used between two houses 400 feet apart is because Ethernet over twisted pair's limit is 328 feet, or 100 meters. I'll leave the whole issue of power imbalance alone. Love the podcast. Never miss it. Melissa. Okay, okay, okay, okay.

Steve: I just loved it. It just sort of - just ended the debate.

Leo: We stand corrected, yes, yes.

Steve: Should two houses 400 feet away be connected by Ethernet? Uh, probably not because it's a 100-meter limit, which is 328 feet, and that's less than 400. So there's the answer to our question. Doesn't matter about balanced loads and current loops and shielded wires and all this mumbo-jumbo. Nope, it's just too far away.

Leo: You may also remember we talked a little bit about two-factor authentication at gas pumps using zip codes. And of course we said that's not going to work in Canada. Well, Faiz Imam in Montreal, Canada solves the mystery of the Canadian gas pump zip code authentication: MasterCard is aware of the issue of gas pump authentication, he writes, and has an ingenious workaround that maintains the spirit of the zip code. It's really quite simple. You take your Canadian postal code, for example, J3N 4N5. Just keep the numbers, 345, then add two zeroes at the end: 34500. Enter that into the gas pump, and it will be accepted. This is not a trick. It's official MasterCard policy. And he quotes MasterCard.ca. This way you still need info only you know, and apparently MasterCard, but it fits within the U.S. standard. Users of Visa and other cards will be out of luck. Just an FYI for Canadian MasterCard users. I don't know how they publicize that.

Steve: Yeah, it's interesting. But we have.

Leo: It's cool. Now you know.

Steve: Yeah, now we know. And just for the record, there was a ton of feedback from our very correct and security-conscious listeners who were noting that, well, you know, you probably could guess a zip code because after all it's not a random five numbers, it's tied to your geography, and they probably have some idea, blah blah blah. So it's like, okay. Or you can certainly guess the first several digits because, as we know, the zip code is actually sequential based on physical location. And I'm in a 926 area, and so...

Leo: I think it's better than nothing.

Steve: It's absolutely better than nothing. I'm happy I'm being asked.

Leo: It's a pretty low standard, but it is our standard.

Steve: Yeah. It does not meet our crypto high entropy standard. But then anything that did, nobody could remember. And the beauty is pretty much you know what your zip code is.

Leo: Right.

Steve: Just it's just not a random five digits. And that means that other people could have an idea, too. So I wanted to just acknowledge all the people who said, eh, it's really not that good. It's like, eh, it's better than nothing.

Leo: Eric follows up with a final thought about his new installation of Windows XP on a Virtual Machine. Steve, thanks for answering my question about the need to install updates into a new, VM-isolated Windows XP instance. You said you should.

Steve: Yup.

Leo: One additional note: I realized I did need to go online anyway, at least briefly, to authenticate Windows. Oh, that's a good point.

Steve: Ah, yes.

Leo: So even if I have to just do it once, I'll be doing the Windows Update. Thanks. Eric.

Steve: Yeah, it was a good point. I thought that was a good point because I was saying, oh, my god, the one thing you do know about a virgin installation of XP is that every worm written in the last decade or even more is targeting that OS. And so absolutely bring it current. And so then it was like, yeah, but if there's absolutely really no Internet connection, then you really don't have to; right? I mean, it's not going to just decay by itself. No. But as he noted, I mean, like, I'm sure he did this, and then Windows was saying, "I haven't been authenticated." He's like, oh, crap. I do have to give it an Internet connection in order to get Microsoft to bless it. So if I'm doing that, I might as well update it. So, yeah.

Leo: Question 6.

Steve: Oh, and...

Leo: Go ahead.

Steve: During one of your away missions, with Father Robert, I noted that my little postage weigh scale system didn't seem to be receiving XP updates, even though I did the cute little "I'm XP Embedded" hack to the registry. I did want to follow up and say it definitely is. I turned it on the other day and, oh, look, it's got a bunch of updates to receive. So it might have just taken a while to get synchronized and caught up or who knows what.

Leo: Oh, good.

Steve: But so that hack is keeping XP updated and has not been shut down yet. So it's not like XP actually died, for anybody who cares.

Leo: I think it makes sense that Microsoft, who surely knows about it by now, just says, well, you know, if somebody's going to do that, we won't get in their way.

Steve: Yeah.

Leo: Kirill in State College, PA notes that having nothing to hide is not the point: As a regular Security Now! listener since 2008, I thank you for what you're doing to enlighten your listeners and viewers. But lately I cringe every time I hear you or Leo say that it's fine for lots of stuff to be unencrypted because the information in question is not sensitive. Certainly one purpose of encrypting information is to protect the information from unwanted disclosure, but the other is to maintain privacy as a general principle. By taking that approach, if it's not sensitive it doesn't need to be hidden, well, then you miss the latter aspect.

If 99% of your communications are in the clear, and suddenly you use Tor or PGP for something, you might as well be waving a big red flag that says "Pay attention to what I'm doing, this is important, and I want to keep it secret." The point of routinely encrypting everything is to make it impossible for our NSA overlords to distinguish between someone actively trying to preserve his or her privacy, thus potentially singling that person out for closer surveillance, and everyone just going about their routine business.

Steve: So this really is the question that I was referring to earlier, where I agree that in general it makes sense for us to be increasing our use of security. We clearly see that we're moving in that direction with more and more sites implementing HTTPS. I think that he was responding, though, when he said "Every time I hear you and Leo saying sensitive stuff doesn't have to be encrypted," for example, probably he was referring to our conversation about email. And that's sort of a special case, only because it is really difficult, unfortunately, to encrypt email. That's been one of the things we've been talking about here over the last few months with PGP and Gmail and Yahoo's announcements that they're going to start focusing on this more.

It's just that our clients and email itself, unlike web serving, or web surfing and web browsing, there the protocol that Netscape introduced with SSL 1.0, the messiness is completely encapsulated in the connection. And we do have that with email to some degree. Unfortunately, it's only the connection that is optionally encrypted, not the envelope that we're mailing in. So part of our conversation about this that we just had a week or two ago was that, you know, with email, eh, we're probably just going to have to kind of give up on that one and use messaging, or any of the forthcoming communications systems which will have been designed cryptographically strong from the start, and just sort of let email be like, eh, well, fine. As everyone knows it's in the open, so don't send anything important there.

But I certainly also agree with his notion that every Internet - all the packets on the Internet should look like random nonsense. You should not be able to put a packet sniffer on the 'Net, which we know PRISM was. PRISM was the NSA's suck-it-all-in and, you know, do keyword searches and so forth on all this wealth of unencrypted data. It's easy enough for us to wrap that in encryption that we probably should, not to thwart the NSA because I don't really think we can, but just because, once the technology has been put in place, then we get encryption for free, the way we have it now with using HTTPS. It's essentially for free.

Leo: Yeah, I mean, I used to say the same thing, that everybody should use PGP because then no one will stand out when they do use PGP. A couple of points to make, though. First, that implies that somehow, if you use PGP, the feds will be able to crack it. And if it's strong encryption, it doesn't matter whether it stands out or not. If you trust the encryption, you trust the encryption.

Steve: Good point.

Leo: Certainly enough traffic is encrypted that the feds are still going to have a challenge. They're not going to have a super quantum computer and have to only focus on one email. The second issue, well, you raised the issue that the difficulty involved, on everything, even HTTPS server, means that it's not necessarily practicable to encrypt everything.

Steve: Right.

Leo: And we do know, by the way, that the feds decide that anything that uses Tor or PGP is by default suspect and included in their databases. So, I mean, he has a point there. But it's not like being in their databases means that suddenly they can read it. They still have to crack it.

Steve: Right, right.

Leo: So I think it's sufficient to occasionally use it, would be my point. You don't have to use it a hundred percent of the time. But if everybody used it a third of the time, see, it's hard for - as you point out, I have to get your key to send you an encrypted thing. Every email I send out is not going to be encrypted. It never will be.

Steve: Right.

Leo: Because I'd have to get everybody's keys ahead of time. But if you encrypt a third of it, I think that's sufficient to bug the feds and to mean that they cannot focus on any particular thing.

Steve: Yeah. For me, for example, my use of encryption is with Jungle Disk to encrypt everything that goes out of here for archival. So I have offsite archiving. I will absolutely, I wouldn't consider not encrypting it myself before it goes. So there's nothing there. I mean, it's our corporate information. It's all of the work I do, all my source code and everything. There's trade secret stuff in there. It's like SpinRite and everything. So I absolutely don't want that to fall into someone else's, basically into any one bad guy's hands. I really wouldn't mind the government having it. I assume that they wouldn't do anything wrong with it. It's for pure business-related intellectual property privacy. That's my use of encryption.

Leo: I think it's, you're right, it's a flag. But is it...

Steve: And, you know, and our story we talked about last week about the crazy - the guy's name was Jeremy, the agent at Comcast who was basically trying to hold people out as being exceptions for using Tor. This sort of plays into that, too. At the moment, someone using Tor does seem more suspicious.

Leo: Right.

Steve: It's like, well, what are they trying to hide?

Leo: Right.

Steve: Sort of it begs the question.

Leo: Yeah. And Faiz's point, well taken, is that if everybody used Tor, then nobody would - but it's just not practicable.

Steve: No.

Leo: So use it as much as you can. Encrypt as much as you can.

Steve: It's really slow.

Leo: And I have many correspondents who routinely use encryption with me. And I encrypt back. And we do that because there's nothing in there, but it's just, well, yeah, it just adds to the noise.

Steve: Yeah. Fill your drives with this, you feds.

Leo: I think that's sufficient.

Steve: Yeah.

Leo: Everybody should have some sort of S/MIME or PGP encryption installed and use it when you've got somebody's keys, and that's enough.

Steve: Yeah. Well, and right now you and I have encrypted packets moving over the Internet, streaming back and forth with audio and video. Do we think it is impossible to crack? No. But it's certainly not in plaintext, and I assume somewhere there's a hard drive sucking it in in case it's ever useful for something. It's like, well, knock yourself out. You can also get it unencrypted on YouTube and on GRC.com and on TWiT.tv.

Leo: Won't you be surprised when you find that out.

Steve: Yeah. And it has the benefit of having been edited a little bit, too.

Leo: Yes, it's a little cleaner, yes, absolutely. Spyros in Upstate New York shares his theory on this HTTPS up-ranking Google's doing: Over the last few weeks I've listened to your discussion as to why Google might be up-ranking sites that offer secure HTTP, and whether this is a good idea. The theory I have is Google's attempting to increase the amount of encrypted traffic flowing over the 'Net. To what end? Well, with all the fear of being watched, it would seem an abundance of encrypted data would make the snoopers' job harder. Same point as Faiz.

Steve: Yup.

Leo: It's just a theory, but I hadn't heard it brought up, so I thought I'd mention it. Keep up the great work.

Steve: Yup. And this plays into the same thing. I think I actually would argue that, to the degree that Google's ranking algorithm, and I watched you and Jeff and Gina have an interesting talk about this last week, just like, wow, what do you think that algorithm looks like?

Leo: Yeah.

Steve: Probably won't fit on the back of a napkin anymore.

Leo: No.

Steve: So it's a multi - certainly their ranking architecture is very sophisticated. It's been - the complexity's been increased both to improve the quality and also to thwart abuse because we know that the SEO, there was a big flurry for a while back in the early days where it became, you know, the idea of spoofing the search engine's ranking was a big deal, and people would do things like fill pages that the user couldn't see with keywords that the search engine would see. And if the search engine wasn't differentiating between what the user could see and not see, that opened them up to abuse.

So my point is that I think as one's additional signal, not heavily weighted, but just an additional signal, sites - and understand we're talking about a mathematical algorithm that is not sentient. It is a spider sucking in web pages, I mean, an unbelievable number of web pages. And its goal is to offer users the absolute best links it can. So it needs to use any signals that it can find from the noise.

I think a useful signal, again, not one or zero, but some fraction of a percent of merit, is whether the site supports HTTPS. Because, again, in general, although I don't like the notion of noncommercial sites being dinged as a consequence, but sites that use HTTPS, again, when you're a blind spider, that's probably a useful signal. I do think Google is encouraging the use of security. We know they are. We talk about it all the time. Google is pushing for a secure Internet. Yay. But I also think it's useful for search ranking as one of many signals going into the algorithm.

Leo: That's a good point. That's a site then that's not a fly-by-night site. It's not...

Steve: Correct.

Leo: It's a serious site that paid money to get a cert.

Steve: Yes.

Leo: Actually, that's a very good point. It's more than just security. It is a good signal.

Steve: Yes.

Leo: By itself.

Steve: I think it demonstrates an investment has been made by the people. They care...

Leo: We know for instance they use as a signal how long your domain registration is. If it's a one-year or shorter registration, you're ranked lower than if it's three years. If it's three years, you're here. You mean to be here. You spent more money on it. It's less likely a spam site. A certificate would be very similar to that. So maybe it's - they couched it in security terms, but I think there is actual value in it over and above that.

Steve: Yeah.

Leo: Yeah, you make a good point. Here, so does Mike in Florida. He asks a question Steve has never heard before, ha-ha: When you do a full, not a quick, but a full format of a hard drive, Steve, does it repair the disk? In other words, if I'm getting disk errors, can I just format it, full format?

Steve: And oddly enough, I don't think anyone has ever asked me that.

Leo: No, you're not being sarcastic.

Steve: No, I'm not.

Leo: Oh. I thought that would be the first thing people would ask you.

Steve: I talked recently about how nobody anymore actually does a format of a drive.

Leo: No, because drives are too big. It takes forever.

Steve: Yeah. It just is not practical. And what it's doing is, when you do a so-called "long format," and that word is now an understatement to the extreme, is in the old days it was going out, I mean, there was no such thing as a quick or a short format. Format was format. That's the first thing you would do on your 30MB ST-238 RLL drive that had 23 sectors per track. I should remember how many cylinders...

Leo: You know all of this, don't you.

Steve: Yeah. So...

Leo: 1024, right? No.

Steve: I think it was. No, actually you could push it to a little further. I think it was a 1050, actually. You could go a little further. There was some unused space at the end that they just sort of left, and you could actually put data out there. So what it was doing is it was looking at the sector headers. So it was looking for so-called "bad sectors" that had been factory marked as this sector contains a defect, do not use it. It would then look - typically sectors that were half a K, they were 512-byte sectors, it would use 4K sectors, so it would use eight of those half a K sectors, those 512-byte sectors, to create a cluster. So any cluster in the directory, in the file system, that contained even one bad marked sector, the whole cluster would be marked as unallocatable or bad in the file allocation table in the directory.

So that's what that all was. That process doesn't fix anything unless the sector is repairable, has like an ECC soft error, and reading the sector might cause the drive to say, oh, I didn't realize there was a defect that I need to get sort of thinking about here. I'm going to spare that out and swap in a good sector. So it certainly doesn't do data recovery. It's not a bad thing to do unless you value the length of time you have left to be alive because it's going to take forever to format that thing. It's really slow.

Leo: How long does it take for like a 2TB drive?

Steve: Oh, days.

Leo: Days. What, days?

Steve: Days, days.

Leo: Oh, well then nobody's going to do it.

Steve: No. And...

Leo: Then the answer is moot because who's got, you know, that's crazy.

Steve: And what we've done is we've just gone to an "assume the drive is good," and we'll deal with problems if/as we encounter them.

Leo: Right.

Steve: And nobody was marking those bad, the sectors bad, anyway. And when we switched to the new IDE drives, which have intelligence in the drive, they're supposed to handle that. So the drive never has any bad sectors. If it did, it would have swapped them out for spares. So that's really the theory under which there are no more bad sectors, is drives are smart now.

Leo: More questions for you, Steve. Question 9 from Jeffrey, Allentown, Pennsylvania. He wants to share his experience with POS, which can mean two things.

Steve: Yes.

Leo: Yeah, and maybe it's the same thing...

Steve: And in this context it really means both.

Leo: It's the same thing, both. But I have personal experience working for a point-of-sale merchant services company - that's what POS stands for normally. I can explain why these point-of-sale computers are running unpatched Windows XP Embedded, point-of-sale ready. My company had issues where our software would break after applying a critical Windows update. This bug hugely annoyed the merchant because, of course, when the system's down, they can't make any sales. So for a period the company enforced a policy of not letting any of our POS systems ever run Windows Update. I think this is true in many businesses for a lot of reasons.

Steve: Yup.

Leo: Windows Update can break things. And in a mission-critical environment, that's not what you want. And this is a distressingly common policy, he adds. I strongly suspect that both Target and Home Depot had set up their OS images not to run updates. The common belief has been that simply disabling access to IE would be sufficient to keep them safe.

Steve: Yeah, I thought that was neat feedback from the field. Nothing surprising, but of course the Home Depot recent escapade is being regarded as the largest, most critical breach in history.

Leo: What a mess.

Steve: Yeah, it is a huge mess. And apparently there are ex-employees now, and we have to consider that they're ex, so they're no longer part of the faithful. But they've been providing information that Home Depot was fully aware of the security problems that their systems had and essentially did nothing. I would say chose to do nothing, but they didn't chose to do anything. They didn't choose to do anything, which is passively choosing to do nothing. But, yeah. And as you say, Leo, well, this is the reason Microsoft went to the Second Tuesday of the Month.

Remember that once upon a time before this, patches would just come out randomly at just arbitrary times and be like, oh, here's an update, which drove the IT people crazy because they had to do some planning. What we found is, because patches would occasionally interact with specific software on corporate machines, that these patches were killing things. And so IT said please, please, please, please, A, give us a schedule and so that we know when things are happening. We will set time and people, personnel, whatever's required, aside to vet these changes on our specific systems with our vertical applications, whatever it is we're doing to make sure they don't break anything. And then let us redeploy those within our Intranet. And of course that's now the model that's being used.

But the problem is these embedded systems, they don't feel like they have a computer in them. They don't feel like they have Windows XP Embedded. They feel like, it's like, oh, so it's a keypad and a mag stripe reader. Well, how can that get in trouble? Well, we know how.

Leo: Our last, our very last question comes to us from Kevin in New York. He wonders about the long-term reliability of solid-state drives based on their error correction, ECC rate: I have an older model Sandisk, 128GB SSD. While I've not been too hard on it - 55TB of writes over the course of a little over two years - how would he know that? Is something keeping track of that?

Steve: Boy, I bet. He has something that's doing that.

Leo: Yeah. once in a while I run SpinRite on Level 2, largely to look at the error rate, and I have noticed some issues. It seems that over the past year the ECC corrected rate has steadily increased from around 7,000 - that's per minute?

Steve: It's not clear. SpinRite has a total, and it also reports a ECC rate in per megabytes.

Leo: Per megabytes, okay. Yeah, I've seen that. This looks like that.

Steve: Yeah.

Leo: Around 7,000 to close to 15,000 and a full erase before restoring data has no impact on the error rate. The SSD rates itself as having 95% life remaining, so it seems like that may be a bit inaccurate. Furthermore, with the increasing error rate as the drive is used, it makes me wonder how long this drive will last before data begins to become corrupted. So what are your thoughts, Steve, on the reliability of solid-state drives where over time, as you use them, the ECC has to work harder? We should say that ECC means you're not losing data. But it does mean that there are failures; right?

Steve: Yes. And, okay, so two things. Or a couple things. The neatest thing - well, okay. One of the many neat things that SpinRite does is this note, this idea of capturing the SMART data on the fly, which SpinRite processes to show you the rates at which errors are happening. Nothing else does this. And it is such - it's really, it's like it's underused intelligence which happily Kevin is taking advantage of. The point is that the SMART system doesn't really tell you anything unless it's under load. But nothing that puts it under load reads the SMART system except SpinRite. So he's able to say, and he has here, that he has seen an increase in the rate of corrections being required by this SSD. Now, the fact that he has done a full erase and restore, and the rate didn't drop, that's - and he understands that, and he's right. I doubt 95% life remaining is right. I would worry or wonder if it even had 40 or 50%.

Leo: Huh.

Steve: I think this is a very - I think this is a danger sign. Now, the better thing to do would be to have been monitoring this over time, where it would have been 7,000, 7,000, 7,000, 7,000, 7,000, 15,000. That is, if you saw - or probably seven, eight, nine, 10, 11, 15. The point is, if you saw a need in a curve of how much ECC is being required, that would be an indication that, like, something bad has happened. Or it's now aging at an accelerated pace because it's getting into trouble. But what the rate means is that, if he hadn't erased it and restored it, that is, hadn't just recently rewritten all of these capacitors - remember that these are little floating capacitors. They're little tiny bits of conductive silicon which have a crowd of electrons sitting on them. And they're going to be bleeding out, bleeding off. That charge is going to bleed at some rate, very low, so that typically you have retention times in a hundred years, or like of a hundred years. But if there are defects, the leakage can be higher.

And the reason writing is fatiguing is that it's poking holes in the insulation, and the process is called "tunneling," in order to, like, force those electrons through this insulative barrier to strand them out on this little island. And that process fatigues the insulation and increases the leakage. Now, if he had only been doing retests and saw the error rate increase, that could indicate that we're seeing bits are leaking that are requiring correction. Except this is freshly rewritten, and he's seeing a greater error rate. And that's what scares me. That's a great test he performed. And frankly, I don't know in terms of writes, I mean, what is it, it's 120GB SSD upon which he's written 155TB. So that's not, that's, what, 60 writes of the whole drive?

Leo: Yeah.

Steve: It's something like that. So it doesn't seem like many writes. I agree with him. But, boy, do keep it backed up.

Leo: I have to say that, first of all, it's an older drive, as he says. And I think that the drives are probably getting better. But also...

Steve: Nice hat.

Leo: Do you notice what it says? I'll show you the hat in a second. But also that I just anecdotally do not hear of a more, of a higher failure rate on SSDs. And I use SSDs all the time.

Steve: I agree. I agree.

Leo: So that's one drive. Maybe he's got a bad one. We don't know. The question is should we be concerned about longevity in SSDs in general. And I haven't seen any evidence to suggest that. But maybe you have.

Steve: No, there was - there was a meme that ran through the Internet in the last week, and I didn't pick up on it. I was busy working, and it kind of got past me. But it was something about the amount, it was like data being written to SSDs that was fatiguing them. I'm sure somebody knows about it, probably Simon Zerafa, our buddy who's an amazing fount of tweets. I'm sure he knows what it was. And in fact it may have been from him. He's probably going to put it in my stream after the podcast, and I'll pick up on it and check it out. And I'll add it to the notes for next week. Because there was something that went by that was - I thought it was interesting, but I just - I was overloaded at the moment, so I didn't add that to my pile.

Leo: Right. Yeah, I mean, I'll just, from my own experience and talking to people, I have not heard about any problems with SSDs.

Steve: Yeah. I agree. Although...

Leo: In fact, it may well be they're more reliable than spinning drives in the long run.

Steve: The good news is SpinRite recovers them. So for what it's worth, that's why there's plenty of life left in SpinRite.

Leo: And he didn't leave one for you, but I thought this was an appropriate hat to wear during the show. That eagle you might recognize is the emblem of the National Security Agency.

Steve: Nice.

Leo: United States of America, established 1952. And apparently one of our listeners works for the NSA and dropped it off. So I'll be wearing this around as I travel around London. I don't think I'll have too much trouble, you think?

Steve: No. No, I have a hat that I was given by some FBI agents. And one time I was out riding on the bike paths in Irvine, and some really rude people just, like, almost forced me off the path when I was wearing my regular, actually I think might have been a SpinRite hat or something else. And I was really - it was really just disrespectful. They could have easily moved over. And so I just had this inspiration. It's like, oh, I'll wear my FBI hat. And what a change it made. It's fantastic. I mean, I look like an agent, all dressed in black.

Leo: People are - you look like an FBI agent anyway.

Steve: I do. And so this hat, it cinches the deal. People, I mean, they, like, avert their gaze and move off into - and they're now, they're in the weeds, and I'm in the middle of the...

Leo: Yeah, they're not going to mess with you.

Steve: ...sidewalk. So it's, yeah, it's very nice. Solved the problem.

Leo: Thanks, Mark, for leaving this hat for us. He's off to run in the Big Sur Marathon, but he thought it'd be fun to leave this behind. By the way, the eagle is holding a key, a big key. I wonder what that key unlocks.

Steve: So we don't have you next week, and the podcast is Wednesday; right?

Leo: Yeah. So here's, yeah, this is the time to talk about all of this. I'm going to London on Sunday. I'll be back pretty quickly, the following Sunday, so I'm not going to miss any TWiTs. But I will miss one Security Now!, and Father Robert's...

Steve: And you're wishing that you had made a longer reservation in London.

Leo: I do. I absolutely do. But duty calls.

Steve: So it's vacation; right?

Leo: Yeah, it's a six-day vacation, basically.

Steve: Very nice, very nice.

Leo: Robert will be here. He does a great job. So I appreciate that. And, yes, you're going to be at a different time because Microsoft - I can't, it's hard to - time is rushing by. When we started this show, the current version of Windows was Windows XP. It is Windows 9, the next version of Windows.

Steve: And I of course, I think I was no longer using NT, but I was probably using Windows 2000.

Leo: 2000, you were using Windows 2000, yeah. So the next version of Windows.

Microsoft is going to reveal technical information on September 30th. That's normally our day. So what's going to happen is Paul and Mary Jo are going to be at that briefing, a small private briefing. But they're going to come right up afterwards and do a special Windows Weekly at this time.

Steve: In this time slot.

Leo: In this time slot, 1:00 p.m. Pacific, 4:00 p.m. Eastern time on Tuesday. And so that will be Windows Weekly. So we're going to put you in Windows Weekly's time slot the following Wednesday, 11:00 a.m. Pacific, 2:00 p.m. Eastern time, 1800 UTC.

Steve: Ah, okay. So it's not - I was told it was my old time slot. Oh, yeah, no, it is.

Leo: Yeah.

Steve: At 11:00 o'clock on Wednesday. So we move me up to 11:00, but we drop me back to Wednesday. Okay.

Leo: Wednesday at 11:00. That's all you have to remember, Steve.

Steve: Okay.

Leo: Robert will be here; right? Yeah, Robert will be here. And then we'll be back to our normal schedule, and I will be back with many tales to tell of my adventures as a National Security Agency representative in Jolly Olde England. That'll be interesting.

Steve Gibson is at GRC.com. That's where you'll find, not only 16Kb podcast versions of this show, but also fully human transcribed, thank you Elaine Farris, transcriptions of the show. You'll also find SpinRite, the world's best hard drive maintenance and recovery utility, and all the great freebies that Steve gives away all the time. It's also a place to go for questions: GRC.com/feedback, specifically. That's where you should leave your questions for future feedback episodes.

We have full-bandwidth audio and video versions of the show at our website, TWiT.tv/sn for Security Now!. It's also on YouTube.com/securitynow. It's also wherever you get podcasts. In fact, subscribe. You're going to want the complete set. We have not yet put out the leather-bound edition, so you'll have to make your own. But you do that by getting every episode every week of Security Now!. Thanks, Steve. We'll see you next time.

Steve: Thanks, my friend.