A Newsy Week!

Description: So much happened during the past week that today's podcast will consist of a series of rather deep dives into the many interesting things we have to discuss.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-427.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-427-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here, and it's just a potpourri of security news. There's so much to talk about, including a new, amazingly well-coded malware that's bad news. Stay tuned. Security Now! is next.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 427, recorded October 23rd, 2013: A Newsy Week.

It's time for Security Now!, the show that protects you and your loved ones, your privacy, your security online. I mean, this is the show that continues to grow because there's never been more interest in all of this. Steve Gibson is our Explainer in Chief, the king of Security Now! for the last 427 episodes.

Steve Gibson: Wow.

Leo: And he's back again. Yeah, wow. And we thought when we started there wouldn't be enough to talk about.

Steve: Oh, yes. And that was my concern when you proposed a weekly - it was going to be a weekly half-hour rather than what it's become, is often 100+ minutes per week.

Leo: Yeah. Well, you're in a - you have the luck of being in a booming business.

Steve: Well, and as we have seen, I mean, looking back over the history of the podcast, since I love technology, security is sort of the hub. But then we've gone off and, like, covered exactly how the Internet works, what is packets and routing and all of that.

Leo: But all stuff you need to know, really, I think, to understand these topics.

Steve: Exactly. So it's all of that rich background that creates a good knowledge base. Today there's just been - there was so much that happened this past week. And so we're technically a Q&A, but I decided not to do the Q&A format because instead the content is by popular request of our listeners. I want to chat with you a little bit about yesterday's Apple announcements. John McAfee is back in the news, believe it or not. Google has something called...

Leo: His 15 minutes aren't up? God.

Steve: He almost got a lot more, but then the government shutdown preempted him. Google has something called Project Shield, offering DDoS protection. Another casualty of the NSA. Everyone's been asking for me to look into CryptoLocker malware. I've already warned Jenny about it because this would be really bad. Although she's using Carbonite, and I did check recently that it was, like, all lit up and working for her. So that would be good. There's a Flash virtual machine in JavaScript. Some news, a lot of news, actually, in the instant messenger category: Hemlis, BlackBerry, and Threema. Some U.S. Patent Office news about the so-called "Steve Jobs Patent." And, believe it or not, even a bunch of miscellaneous stuff. So tons of stuff to talk about this week. And so we've just got - that's what we're going to do for the next however long.

Leo: All right. Do you want to talk about Apple's thing?

Steve: Well, just briefly.

Leo: I'm curious what your take is. You're an iPad owner and user.

Steve: Oh, Leo, I use my Pad more than any other electronic device I own. I mean, it's...

Leo: Yeah. You're not alone. I think that's very common.

Steve: It is my device. It is - I just - I take it with me every morning. I do reading and research. And I'm, I mean, I love it. And so for me the question is, I mean, yes, I will get the new device. The question is which is it? I was interested yesterday to hear you talking about that you really like your mini.

Leo: Yes.

Steve: And I think I do, too, because maybe then it's a little more easy to always have it with you. On the other hand, the phone - remember that I've traditionally been a BlackBerry user. And I am, I do, I got my 5s last week. And I'm in the process of migrating myself. I need to convert all of my custom sounds over to M4R ringtones so

that I can get them into the phone and associate them because I really love having per-contact sounds for instant messaging and email. And then I'm going to just swap the numbers. I will exchange the phone numbers between the iPhone and the BlackBerry, which is me being committed, and then see how it goes.

Leo: I think you might - it might be painful initially because of the keyboard. But I think you might find you like it, especially since you like the iPad so much.

Steve: What I'm finding is that I can't hold it and do the double-thumb typing, which I do on the BlackBerry. It doesn't set itself up for that kind of double-thumb typing. But I hold it in one hand and then type with the other, with my first finger of my left hand, and that seems to work.

Leo: Unfortunately, I've never been able to type effectively on an iPhone. It's just too small. And once I got to the bigger Android devices, I found much more comfort there. Plus you can change, they have a variety of different keyboard styles which I find more comfortable. But you may never really love the keyboard on the iPhone, I guess is my point.

Steve: Yeah. And I, yeah, I may just not type as much.

Leo: Just don't type as much, yeah.

Steve: But to have, like, a...

Leo: Dictation is quite good on it, you know. And that's kind of a nice feature. I don't know if you use the dictation Siri on the iPad.

Steve: No.

Leo: I dictate a lot of stuff now.

Steve: Hmm.

Leo: That saves me that typing.

Steve: Hmm. Interesting. So...

Leo: So the new iPad - Apple has a problem, in my opinion, which is that the iPad, going back probably almost to the iPad 2, is pretty much perfect.

Steve: Yes.

Leo: It doesn't - it's hard to do much to improve it.

Steve: Yes.

Leo: So they've done what they can: thinner, lighter, smaller bezel, faster processor.

Steve: Well, and are they obsoleting them? I mean, like I'm going to replace my existing one and find somebody who needs it. But are they broadening the market? I mean, like what's their...

Leo: Well, the only way...

Steve: It's not like Microsoft, that's always trying to sell us a new OS in order to kill off the old one and generate revenue from upgrades.

Leo: They've updated the OS for all but the oldest iPads to iOS 7.

Steve: Oh, and by the way, Leo, going to 7.03 and turning off all that ridiculous animation is so much nicer. You just get...

Leo: People thought I was nuts when I said all this swoopy-doopy's making me sick.

Steve: You just get cross-fade between...

Leo: Too much.

Steve: Yeah, it's much nicer. Faster and nicer.

Leo: They had this accessibility switch before to turn off motion, but it only turned it off a little bit. Now, with iOS 7.0.3, it turns it off entirely and replaces it with a dissolve.

Steve: Yup.

Leo: I find that much more appealing. It wasn't a deal breaker, but it's - thank you, Apple. Obviously we're not alone.

Steve: Yeah, it was just nonsense. It was eyewash. It was unnecessary.

Leo: Waste of cycles, yeah.

Steve: Yup, exactly.

Leo: I turn that off on Android, too. I turn all those visual effects like that off. So I would say that you should try a mini. Now that it has the retina, it's the same resolution as its big brother.

Steve: Yes, and that's what I've been waiting for. That's more, well, same pixel resolution, but higher pixel density.

Leo: Higher PPI, yeah.

Steve: Even than the latest iPad. So...

Leo: Buy a couple, yeah.

Steve: I'll get one of each, and then I'll see which one...

Leo: That's one way to do it.

Steve: I'm still grandfathered into my original AT&T unlimited bandwidth account.

Leo: Oh, that's nice. Be careful with that. You know they're going to try to take that away from you.

Steve: Yes. So far they haven't. And it's moved between Pads very nicely. So...

Leo: There's an interesting argument. A lot of people say, well, look at the Nexus 7, $229, really nice device. And I agree, I have one, love it. But there's an interesting and kind of unexpected dichotomy between the aspect ratios. 16:9 is a little strange compared to 4:3.

Steve: Yeah.

Leo: And it seems like a small thing. But I actually think I prefer 4:3.

Steve: I know what you mean.

Leo: The widescreen's just a little too wide.

Steve: Yup. And in fact, that's what I felt when I got one was, for example, when you're reading a page, it was too tall.

Leo: Yeah. It's weird, it's a little weird.

Steve: Yeah.

Leo: But for reading and for a lot of the things, music scores, things like that, 4:3 is actually a more optimal aspect ratio, unexpectedly. It's not more optimal for watching movies and TV.

Steve: Right.

Leo: So, yeah, you should have all of them [laughing]. Oh, my goodness. That's why I'm in this business, so I can have everything.

Steve: Well, and I do love the idea that they may have fixed, like tweaked the full-size Pad, which we're not going to call the Maxi Pad.

Leo: No, the Air.

Steve: By pulling down the borders, making it lighter and a little thinner. And it's like, wow, that might be just the ticket for, like, so you still get the larger screen, but it does feel physically smaller, and it is definitely lighter.

Leo: I think I said that yesterday, which is, while I am a fan of the mini, they may have made the Air small enough that it accomplishes the same thing. So I'm not going to buy both, but Sarah's going to get the new Air for iPad Today. And I'll get the mini because I like that. And then I can decide which I want to use all the time. But this is iPad 3, third generation, not even the fourth generation, not even the current one. It's fine. I don't feel - and this is where Apple has a problem. I don't feel any urgency to upgrade.

Steve: Yes. If it wasn't the device I use all the time - for example, I have three others. And I'm not going to bother upgrading them because they're just fine. They're retinas, and they're all I need.

Leo: That's kind of a problem for Apple.

Steve: And I do really like the ecosystem, the iCloud Sync now and cross-syncing the devices. I'm beginning to play with that. And it's nice that you buy an app once, and you've got it on all of your various form factors.

Leo: I agree. I agree, yeah.

Steve: Okay. So get a load of this. CNBC was the first person or the first outlet that I saw pick up on this. Actually, Rachel Maddow did a hilarious segment on this. Her opening segment last night was 15 minutes of this, where she did, as Rachel does when she does a deep dive, really went into John McAfee's background and said, "You're not going to believe how this ties into Washington." And she kind of held that to the end because prior to the October 1st shutdown and debt ceiling mess, John McAfee had been selected and chosen by the Affordable Care Act Oversight Committee to provide them with advice on the HealthCare.gov website.

Leo: Some moron senator said, you know, I have that McAfee antivirus. Let's get him. And what's Peter Norton doing today? I think we should ask him, too. Holy cow.

Steve: Oh. And, I mean, Rachel even reminded us, she went as far as to remind people how, when they buy a new computer, it's got this really annoying McAfee antivirus stuff, like preinstalled, and it's difficult to get rid of, and it wants you to upgrade it after it expires, blah blah blah. I mean, and she talked about, as we have, we've covered it, how he was in Belize, and he had 11 dogs, Rottweilers or something, I think, and they were barking, and his neighbor was complaining, and his neighbor ended up being shot in the head, and then the escape to wherever it was he went to. I mean, it's just...

Leo: All they have to do is show that crazy video. Well, is he still on the panel?

Steve: No. Apparently it got dropped, somehow it got dropped during the shutdown. And maybe people who were a little more clued in said, You might want to watch this video and decide..."

Leo: A staffer wandered over and said, "Congressman, take a look."

Steve: Right.

Leo: Is this what you want? That, by the way, I don't know if - we haven't really talked about the health exchange snafus.

Steve: Oh, Leo.

Leo: I have to say that I think what happens is people go, well, look, Facebook handles this fine. Google handles this fine. How come the government can't make a website? But what they're trying to do, and once I dug deep into it, and actually...

Steve: Yes. The integration...

Leo: Harper Reed, who worked on the Obama campaign and is a superb computer scientist, said this is nontrivial. They're integrating 50 different databases, or more than that. I mean, it is not a simple thing to do. I don't know many hundreds of millions of lines of code it is. It could - it's not surprising it doesn't work, frankly.

Steve: Yeah. I'm unsurprised. It does sound like it was a catastrophe of design. The subcontractor that did it is a wholly owned subsidiary of a Canadian firm. Among other things, it loads 65 different JavaScript files in order to operate. So there's a concern.

Leo: That's a problem.

Steve: Yeah.

Leo: They say, well, we didn't - we wrote the front end. But the back end, the connections to all the databases, that's not our thing. And that's really where all the problems are occurring is the connectivity that's required for this thing.

Steve: Yeah. And of course the problem is that all anybody wants is for it to work. And so everyone is, you could argue rightfully, blaming what they see, is HealthCare.gov doesn't work. And no one is going to be able, I mean, can you imagine this going to some congressional committee?

Leo: They don't understand it.

Steve: Again, they chose John McAfee. They chose John McAfee to, like, oh, you must know what's going on. So...

Leo: Well, and the other issue is that it's government. And I think it's an impedance mismatch between technology and government. Government's designed to move slowly, to move by consensus, by committee. Everybody gets their two cents in. This is the worst way...

Steve: And to fight. I mean, that's...

Leo: Right. And they were making changes till one week before the launch. I mean,

of course it didn't work because - and I think that this is a structural - I remember talking to Harper, we interviewed him on Triangulation, about how was it the Obama campaign was so technically literate, but then once you got to the White House, this transparent White House just never materialized.

Steve: Apples and oranges.

Leo: He says, well, the technology in government is ancient. I mean, they're using Windows XP and stuff. And we were stymied by security regulations, politics. You can't do it. And I think it's a fundamental mismatch between the way this government was designed by our founding fathers intentionally to be inefficient. They don't want an efficient government.

Steve: Jon Stewart had a hysterical piece also, Monday's Comedy Central "Daily Show," where one of his guys, after he got through really lambasting the administration, one of his roving reporters had been trying to get in and was somehow transported into the server, where Pacman was chasing him around going [making sounds]. And Jon said, "How old is this software?" So it also had sort of a look like "The Matrix" with numbers changing, and Jon said, "What are those fours and fives?" And the other guy said, "I know, they're supposed to be ones and zeroes, but this one has fours and fives." So anyway, it was pretty good. If you can see Monday's "Daily Show"...

Leo: John Oliver, he is so funny. I love him.

Steve: Yeah, exactly, John Oliver.

Leo: Yeah, so, I mean, there's not much for us to say about HealthCare.gov except that...

Steve: I'll just end by saying that what I believe is that, whatever happens during the 2014 midterm elections, that it will be decided based on the Affordable Care Act. I mean, if they get this fixed, and it comes up and runs and is doing a good thing, then that'll be one outcome. I mean, it's very possible that this really just could collapse, that, I mean, that it's going to take months. And what I'm worried about is I'm hearing the pundits say, "We have three weeks." They're saying, like, this has to be working in three weeks, and otherwise it's just too long. And it's like, well, maybe three months. As you said, it is big and complex.

Leo: I don't know if three months is enough. I mean, I don't know.

Steve: I know. It could be easily - it could take a year for it to all get running correctly. It's big. It's bad.

Leo: Yeah.

Steve: So Google has something interesting, and I wanted to fix some of the misconceptions about this because the news, the little snippets that I saw were saying, oh, Google is going to be offering DDoS protection. Well, kinda. Forbes carried the story and carefully explained what Project Shield was and was not. And so they said: "Over its years as an Internet behemoth, Google has learned a lot about fighting hackers who would knock its services off the web. Now it's offering its muscle to a far more vulnerable set of targets." And that's the point. Well, I'll go on.

"On Monday of this week, the company announced that it will offer free - free - protection for websites against so-called 'distributed denial of service' cyberattacks that flood them with junk traffic from hundreds or thousands of computers, taking them offline. The project, which is part of the company's Google Ideas initiative to take on global problems, has already been working for months with at-risk sites around the world in countries like Iran, Syria, Burma, and other places where sites with political content are often subject to attack, and will expand in its initial phase to hundreds of sites.

"CJ Adams, an associate with Google who announced the Shield project at a company summit in New York, said, 'We're able to take the people who face the greatest threats to distributed denial of service attacks and get them behind our protection. If they face an attack, it has to get through us first, and after years of working on this we're pretty good at stopping these attacks.' Among the beta users of Project Shield are the Persian-language political blog Balatarin, a Syrian website called Aymta that provides early warnings of SCUD missile launches, and an election monitoring website in Kenya called the Independent Electoral and Boundary Commission. Adams said in his talk at the summit that Project Shield had enabled the Kenyan site to stay online through a Kenyan election for the first time in its attack-ridden history. Adams said, 'Things that can take many of these sites offline are so small to us, we can easily absorb them. That's made this something we can provide fairly easily. It has a huge impact for them, and we can take the hit.'"

So I just think that's neat. It's pro bono. It's sort of selectively helping organizations that Google deems worthy of having sort of the right to be on the Internet. And not available commercially. You can't buy this from Google. And it's those sorts of politically and socially sensitive sites and Google sort of promoting free peace or free speech, rather, is just saying, yeah, we're just going to do this for you.

Leo: Good.

Steve: So that's neat.

Leo: Yeah. It's not a full - there are companies that provide this kind of DDoS protection.

Steve: Yes. Oh, that you buy for extreme...

Leo: And this wouldn't replace that.

Steve: Correct. So, for example, gambling sites that absolutely have to be on during the big fight, where they have been subject to extortion, saying either you pay us this much money or you're going to be down during this period of time that you absolutely have to be online. And it is often the case that those sites will go down. Then they'll learn their lesson, and then they'll start paying for very expensive bandwidth that is, you know, you have to essentially share a really big pipe with a lot of people like this in order to manage the costs because really big pipes are really expensive.

Leo: Right.

Steve: We have another victim of the NSA's, essentially the NSA's and actually our government's approach to dealing with the Patriot Act consequences. A VPN, a commercial VPN service known as CryptoSeal said, they posted a couple days ago: "With immediate effect as of this notice, CryptoSeal Privacy, our consumer VPN service, is terminated. All cryptographic keys used in the operation of the service have been zero-filled (purged). And while no logs were produced (by design) during operation of the service, all records created incidental to the operation of the service have been deleted to the best of our ability. Essentially, the service was created and operated under a certain understanding of current U.S. law, and that understanding may not currently be valid. As we are a U.S. company and comply fully with U.S. law, but wish to protect the privacy of our users, it is impossible for us to continue offering the CryptoSeal Privacy consumer VPN product."

The statement continued, saying: "The government takes the position that, if a pen register order is made on a provider, and the provider's systems do not readily facilitate full monitoring of pen register information and delivery to the government in real-time, the Government can compel production of cryptographic keys via a warrant to support a government-provided pen trap device."

So this is a sort of somewhat more formal statement of what we saw play out with Lavabit. We saw the drama of Lavabit. And so here is their understanding of why, as a U.S. company, they can no longer honor their obligation to provide the security that they believed they could. And so they're just saying, okay, we're wiping our keys and shutting down.

Leo: Wow.

Steve: Yeah.

Leo: If you were using this service, what's the impact to you?

Steve: I don't know in detail what technology they had. That is, whether, for example, the connections had perfect forward secrecy as an option, that is, were they negotiating keys for the connections that were not dependent upon the master keys. But what this does say is they've wiped the keys and deleted them so even if traffic had been captured,

by preemptively wiping the keys, they can no longer be compelled to turn them over. So they're gone. So in this case, even if the connections were not using perfect forward secrecy, they have kept those keys out of the hands of the U.S. government. And so the prior possibly recorded encrypted traffic of their customers is safe.

Leo: Good.

Steve: And so that was their goal. And that's what you have to do if you really want to - if you're serious about this.

Leo: People probably are wondering about our sponsor, proXPN. And they are based out of Holland and Singapore. I don't know - they're multi-homed, and I think one of the reasons is they don't want to - they're worried about U.S. requirements. But I don't know what they require. I don't know what the status is. Are all VPN services now that operate in the United States subject to this problem?

Steve: I don't know. I mean, they have stated, proXPN has stated that they do comply with the laws of the countries in which they operate. So...

Leo: Well, as everybody does. You have to, or you don't operate in the country anymore.

Steve: So maybe that means you connect to non-U.S. endpoints which proXPN offers, and then that way you're out of U.S. clutches.

Leo: I think you have to.

Steve: That's what I would do, yes. That's what I would do.

Leo: Geez, Louise. I mean, now, and we talked, and I think I sent you a link to this very interesting article by a long-time security guy, security researcher Dan Greer. Or Geer, I should say. And I think maybe in a future episode we should talk about it. But I want to - I put it in the chatroom, and I'm hoping people will take a look at it because he makes an interesting point, which is you don't have much choice. As soon as the political will of the people and of the governing bodies, the government, is we want total security, never again will we have an attack on our shores, as soon as that mandate is issued, the only way to ensure it is for total information awareness. You need to, you cannot with a hundred percent certainty protect the country unless you know everything that's happening. Otherwise you can't say with certainty that something hasn't happened. And so he says we've made a deal with the devil, in effect.

Steve: People have probably seen the news about IBM's Watson computer, which won the, what was the game show that Watson...

Leo: "Jeopardy." "Jeopardy," yeah.

Steve: "Jeopardy." And now it's apparently, I just saw a blurb that it's better at diagnosing cancer than cancer specialists, than oncologists are, given the same data. And you can well imagine the NSA ordering up some Watson machines.

Leo: Well, they did. We already know they did. We know Watson is now helping - oh, no, we - they - IBM has said it, that Watson's new task is no longer playing television game shows or curing cancer, but analyzing security threats. Oh, no, they've already said that.

Steve: Oh, boy.

Leo: But, and so he raises the really, I mean, important point, I think, that the NSA is really - you can't really blame these security agencies. They have been tasked with doing something that is virtually impossible and which requires gathering of all information. And so they're just doing their job.

Steve: So we're going to talk about instant message clients here in a minute. But we know that the good news is TNO technology, Trust No One technology, is readily available. So we have cloud backup that cannot be compromised. We have instant messaging that cannot be compromised. Not everyone uses it. And you have to be careful how you operate. But the problem is, if you want to connect to a remote server over the public Internet, there you don't have the same one-to-one encryption guarantee that you can create when you're backing up your own data. And so only you need to be able to get it. Or you have a - you've established cryptographic keys a la PGP with somebody else. Then it's absolutely the case that the fact of your communication cannot be hidden, but the content of your communication can. So...

Leo: Right. Although ironically, and Dan Geer talks about this, as well, the metadata is often more valuable than the content. So the fact that they can in fact see all the transactions is probably all they really need.

Steve: As you and I talked about when the whole PRISM thing first broke, and people were saying, oh, but it's only the metadata, it's like, oh, my god, that's the social network that is of vital importance. And that's why, as we talked about last week, they're sucking in everybody's buddy lists in order to, again, to build networks.

Leo: Right. Incredible.

Steve: Okay. So we have - okay. So the headline here is I don't know why this didn't happen sooner. And we've been on borrowed time, really, with malware that hasn't been really evil. Years ago there was a piece of really evil malware called the Chernobyl virus. CIH was the acronym for it. And it wiped out the first megabyte of your hard drive. That's what it did. If you got infected with this thing, it zeroed, wrote zeroes over the first

megabyte of your drive. And because of my position in the industry with SpinRite, I got all this influx of, like, oh, my god, will SpinRite help me? And of course no. I mean, the first megabyte of your drive is gone. But then I thought about it, and I ended up writing FIX-CIH and gave it away for free. In the same way, remember Trouble in Paradise, TIP, which was a thing that fixed...

Leo: That's how we met.

Steve: ...the Iomega Zip drives. Yes, it was. So this thing, what I realized was, even though it wiped out your partition table, it wiped out the root directory and, like, most of the FAT - with drives at that time, the second copy of the FAT had not been touched. That is, the first copy of the file allocation table was it pushed things far enough away that I was able basically to perform a full drive reconstruction. And to a huge number of people's relief, because this thing spread like wildfire, they were able to run FIX-CIH, and then everything was back. They were, like, a little surprised. But so what we have today - I mean, so there was just pure malice. And it didn't make anybody any money, which is why probably it died off quickly. Also it tended to kill its victims. And when something kills its own, like, kills its host, then it's unable to propagate from there.

So now what we have is something that surfaced about three weeks ago called CryptoLocker. And the most recent incarnation of it accepts anonymous payments through Bitcoin. Okay. So let's back up a bit because our listeners have been asking me to tell them about CryptoLocker for a while. The headline that Dan Goodin at Ars Technica wrote said: "You're infected. If you want to see your data again, pay us $300 in Bitcoins." And the subhead was: "Ransomware comes of age with unbreakable crypto and anonymous payments." So, and if you want to, Leo, just put "CryptoLocker" into Google, and you will see, I mean, it is bad.

Okay. So what does it do? It is typically installed through phishing attacks in email. So people will get an email that looks reasonable to them, and they will click on a link, and it'll be an executable, and they will now be infected. It installs itself into the Documents & Settings folder under a randomly generated name and adds itself to - and this is Windows only - to the Windows autorun list so that it executes every time you run Windows or start up Windows. It produces a lengthy list of random-looking server names in the domains of .biz, .co.uk, .com, .info, .net, .org, and .ru.

And we know from talking about this before that these are cryptographically generated domain names where the code knows, based on date, what set of domains out of a huge array may be online at that time. So this is the way they avoid anyone getting involved in shutting them down is this - it's like it's a spray of long, random-looking domain names, one or two of which will be valid among a huge population. And it's continually changing. So the bad guys know what the domain name-generating algorithm is, and they selectively register valid random-looking domain names out into the future. And so it's really difficult for authorities to get in there and stop this.

So after generating this large collection of random-looking server names, it then tries to make web connections to each of these servers in turn, trying one every second until it finds the valid one hidden among this debris which responds. When it does, it uploads a file which essentially we can think of as the CryptoLocker ID for the user. Then that remote server generates an asymmetric key pair, 2048-bit RSA asymmetric encryption, public key encryption, based on the user's unique ID, and sends only the public key back to the user's computer.

I mean, so what I'm going to describe here is perfect cryptography. Evil, but perfectly executed. I mean, these guys made no mistake. So then the malware uses the public key. It generates a random 256-bit AES key. So it uses AES 256-bit encryption, generates a random symmetric key which it encrypts with the user's public key and sends that back to the server. So now you have an encrypted with the public key symmetric key for performing bulk encryption that can only be decrypted with the never sent to the computer, never present on the victim computer, private key.

The program then goes through and enumerates and encrypts under the Rijndael AES cipher every single document that it can find on your machine - images, videos, spreadsheets, there's a large list of filename extensions that it - wildcard, *.doc, *.txt, *. spreadsheet, everything. Everything, all the kinds of files that are typically user-created content, it runs through. It also searches for files on all drives and in all folders it can access from your computer, including workgroup files shared by colleagues, resources on company servers, and more. Anything within its reach.

Leo: Backups, by the way, including backups.

Steve: Yes, exactly. Including - so if you have hot online backups, they're victims of this. So essentially, the more privileged your account is, the worse the overall damage will be. So it does that to you, and then it pops up the pay page, giving the victim a limited time, typically 72 hours, to buy back - oh, and so once done with all this encryption, it overwrites and erases, zeroes the symmetric key. So it is gone now from your computer. That no longer exists. Nothing on your computer has the information to decrypt what was just encrypted. And in this little message, well, in fact, I'll read what it says. This pops up on your screen and says, not in good English, says "Your important files encryption produced on this computer: photos, videos documents, etc. Here" - with a link - "is a complete list of encrypted files, and you can personally verify this." So it shows you the list of everything that it just ruined for you.

Then it goes on, saying, "Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt file you need to obtain the private key. The single copy of the private key, which would allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files. To obtain the private key for the computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR, similar amount in another currency. Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server." And then it shows you a countdown timer of hours, minutes, and seconds remaining until you no longer will ever have access to your data. And I've heard from several people who were stricken by this who tried to get a MoneyPak, and wherever they went the person said, well, it's weird, there's been a run on those recently.

Leo: Oh, yeah.

Steve: We're out of MoneyPaks. And it's because of this thing, and people are - and what's sad is that, when law enforcement has found and taken down the servers...

Leo: Doesn't matter. All they do is hurt people.

Steve: Well, precisely.

Leo: They're killing the keys.

Steve: Precisely. They are killing the keys, and then it's impossible for you to get your files back. Not good.

Leo: Wow. Now, in this, Dan Goodin, who's so good, writes that you should have a cold online backup. What is the difference between a hot and a cold online backup?

Steve: Well, that's...

Leo: I guess Dropbox would be hot, right, because it's active.

Steve: Yes. Anything that your computer can see through Windows Explorer, where you're able to browse through the normal file system, would be considered a hot backup.

Leo: So Dropbox, any kind of built-in sharing kind of, yeah.

Steve: Yeah, anything that creates, yeah, essentially, if it has a drive letter, and you can see it in Windows Explorer, then this thing is able to find the drive letter, go out and look for files and encrypt them.

Leo: Presumably then Carbonite would be immune.

Steve: Yeah. Yes.

Leo: Because it's just running - it's running as a program. It's not - you don't have - you can't see the...

Steve: You don't have a file mapping to Carbonite.

Leo: Right, right.

Steve: Exactly, yes.

Leo: Well, then, let me do a Carbonite ad.

Steve: Now would be a good time, Leo.

Leo: Yeah, and I would bet, knowing Carbonite, because they're very sharp about this kind of stuff, that they also provide further protections against this program accessing your data in any way.

Steve: I mean, it's horrifying.

Leo: It is.

Steve: As I said at the beginning, I mean, there is no mistake they made. This is cryptography being perfectly deployed for malicious end. And the hook is it's not like it wiped out your files, ha ha ha. It has taken them from you, and you actually can get them back if you pay $300. And apparently they're making a ton of money.

Leo: Oh, yeah. The FBI said, with other ransomware things, as much as $5 million a year.

Steve: Yes.

Leo: Presumably this is even more. You could see the incentive to do this. Almost impossible to catch you.

Steve: Yeah, and I would just say to our listeners, warn your friends. I know people who listen to this...

Leo: Well, I'll talk about it on the radio show, for sure.

Steve: Yes. People who listen to the podcast are among the savviest users. We do not click on links in email. But our friends and family aren't so careful. And that's who's getting bit by this, and it's a bad bite. So, yeah.

Leo: Wow. It's just amazing. We've seen this before, but this is really a particularly nasty variant.

Steve: Well, and the problem is all of the technology is in place now. As I said when I started this, I don't know why it didn't happen sooner. The technology has been available. We've really been on borrowed time that malware has just sort of oddly existed for the sake of existing. I mean, yeah, I guess there's some weird, like installing search bars and cruft in browsers, where there's some way to monetize that so that you - it changes your search to something where there's - some sort of, like, social networking search stuff where people install this junk and make money. But this is a problem. This is generating, I mean, the problem is this is going to succeed, and we're going to see more of this. My sense is this is going to change the landscape a little bit. I'm not sure how.

But, I mean, this is really bad. And so this is not a nuisance. Jenny got her laptop infected with one of these search bar things. It was popping up a whole bunch of tabs a couple weeks ago. And so I fixed it for her. And it was like, okay, it's fixed now. But this is a different category. This is not "Remove it and then you're okay." This is "Your data is gone." So, yeah, I'm glad she's using Carbonite, as she is.

Leo: Tell your friends.

Steve: So I got a neat tweet a couple days ago from a friend of ours who we've heard from before, Christian Alexandrov, tweeting from @Diabolikkant. I'm not sure what that is, but that's his Twitter handle. And first he sent me a tweet, he said "SpinRite saved me twice today. I wanted to share with Security Now! listeners." And so I just - I glanced up and saw that in my TweetDeck. And so I wrote back, I said, well, okay, you could do a video, or you could write it up and post it to GRC.com/feedback. I said, if you do, tweet me, and I'll go get it, so that I see it.

And so not long after that I got another tweet, he said, "I sent the story to you in text on GRC.com/feedback, titled "Twice the time, twice the good." So, and it was kind of fun, so I wanted to share it. So this is - he's in Sofia City, Bulgaria. And he said, "Hello, Steve and Leo. I want to share a SpinRite story with all Security Now! friends. I called my dentist to schedule a session for a tooth that hurts me. My dentist tells me his computer went down again." And we may remember this is where we heard from Christian before was that he had dental problems and got some free work done.

He says, "So he told me I have few hours before he can do anything," meaning that I guess the office was closed because he has no computer. So Christian says, "I decided to go to the nearest restaurant to have a breakfast. Guess what? Restaurant was out of business for the day. Guess why? Computer failure. You see where this is going; right, Steve and Leo?" he writes. So I offered my help to both restaurant and dentist. Then it just struck the dentist like bolt of lightning, we had an arrangement. I fix his computer, he heals my teeth in return."

Then Christian writes, "Dentist is done." Whatever that means. "So dentist told me to come to my clinic at 1600 hours to take care of the PC, and I will take care for you. Good. I had six hours free," writes Christian. "The restaurant owner was desperate and accepted my offer. I let SpinRite loose on restaurant's computer on Level 2. It took SpinRite four hours to process the drive. After that, some Windows and Office updates, disk cleaning, registry cleanup, defragment the drive, and the computer was every bit as good as new. The restaurant owner was happy and promised me a dinner for me and my beloved. Later, I went to my dentist with my tools." And teeth, apparently. "Same operations like the restaurant were in order for the PC. But SpinRite..."

Leo: So funny. So funny.

Steve: Things must be rough in Bulgaria. "But SpinRite brought me a headache," he wrote. And I thought, what? Anyway, he says, "While SpinRite was loose on Level 2, the dentist healed me. When we finished, I interrupted SpinRite and rebooted the PC. Turns SpinRite fixed the problem while the dentist was healing me. Well, SpinRite brought the disk back from the realm of the dead to realm of the living to find that the computer was infected. I used Sysinternals tools to remove the malware. Thanks, Mark Russinovich, for such great tools.

"Well, the PC was up and running. Then the dentist's phone rang. It was IT support, telling the dentist they can take his case in 48 hours from now, apologizing for inconvenience. The dentist told them not to bother, he hired someone else to fix the problem, and the PC is up and running. After I removed the malware, I updated Windows, Office, and ran disk cleanup, registry cleanup, disk defragment, and after all finished I asked my dentist to check my work. The dentist loved it. Then out of nowhere his IT support came to ask what is going on. The dentist just fired him without much explanations. Now I'm his IT support. So he was so happy that he asked, what else can I do for you? I asked him to check my girlfriend's teeth." [Laughter] "He not only checked her, but started full and complete healing sessions for her FOR FREE" - in all caps.

Leo: Wow, he's a happy dentist.

Steve: "Later this evening we got back to the restaurant, where we had our romantic dinner with nice music, fine meals, and fine wine, as promised by the restaurant owner, for free. Thank you, Steve, for this great software. Thank you, Leo, for your great Security Now! podcast. And last but not least, thank you, Mark Russinovich, for your great Sysinternals tool and your great books, 'Zero Day' and 'Trojan Horse.' I look forward for the third one, 'Raw Code.' Christian Alexandrov."

Leo: Awesome. Awesome. Next time I want you to read that in a Bulgarian accent.

Steve: Oh, I can't, no. We would never get through it.

Leo: [With accent] SpinRite fixes teeth and makes dinner. Makes happy girlfriend.

Steve: Oh, that's wonderful, yes. Makes girlfriend happy. And happy teeth. So...

Leo: Continue on. I have one more ad to do, so you tell me when it's an appropriate time to break.

Steve: Okay.

Leo: All right.

Steve: We have a - this is really interesting to me. Written entirely in JavaScript by the Mozilla Project, a Flash Virtual Machine.

Leo: Oh, wow.

Steve: Yeah. It's called Shumway. And I ran out of time. I meant to look up, what does Shumway mean?

Leo: That's a very familiar name; isn't it.

Steve: Isn't it? It's like somebody in some movie or series or something. It just seems familiar to me. Shumway must have been someway. I'm sure the chatroom will probably instantly identify it.

Leo: Norman Shumway pioneered heart surgery at Stanford. I don't think it's him. Sounds like something from, like, "I Dream of Jeannie" or something; doesn't it?

Steve: Or something maybe more pop and recent, I don't know.

Leo: Oh, Gordon Shumway is Alf. Or Norman Shumway. Alf.

Steve: Was the actor who played Alf?

Leo: I don't know.

Steve: No, Alf was a puppet.

Leo: Alf had a real name. Gordon Shumway.

Steve: Oh, really? Okay. So the website...

Leo: I don't know what that has to do with Flash.

Steve: The website is AreWeFlashYet.com. So you can just go to AreWeFlashYet.com, and that will - you'll be in the Shumway project. And this is a group. Their official statement - it is over on GitHub. Their official statement is "Shumway is an HTML5 technology experiment that explores building a faithful and efficient renderer for the SWF file format without native code assistance."

Leo: That's amazing.

Steve: I know. I just can't, it's like, thank god that's not my project.

Leo: Do you need to have Flash? Or you don't need Flash at all.

Steve: No. No, this will run...

Leo: It replaces it.

Steve: Yes, it replaces it with native - in the same way that Firefox is now natively rendering PDFs, they are working towards native rendering Flash.

Leo: Wow.

Steve: So they say, "Our goal is to create a general purpose, web standards-based platform for parsing and rendering SWFs. Integration with Firefox is a possibility if the experiment proves successful."

Leo: You know, the name may come from the old joke. Ask me what's a Shumway. Ask me what's a Shumway.

Steve: Okay. Leo?

Leo: Yeah?

Steve: What's a Shumway?

Leo: About five pounds. No?

Steve: Oh, my god.

Leo: No, that's pretty bad.

Steve: Unfortunately, that's the humor I grew up with.

Leo: And it may be the humor the Mozilla folks grew up with, too.

Steve: My grandfather would say, "I opened the window, and influenza."

Leo: Yes, exactly. All right. The chatroom may have it. So what is Alf backwards? FLA. The filename extension for a Flash file, one of them, is Alf backwards. And Alf's real name was Gordon Shumway.

Steve: Got it.

Leo: That's a long way to go.

Steve: Wow. That's a really...

Leo: But you know geeks.

Steve: Yeah.

Leo: Yeah.

Steve: Okay. So the first of three instant messaging topics: BlackBerry Messenger now available for iOS and Android.

Leo: Now, you're one of those people still using a BlackBerry. So I'm curious what you think of this. By the way, it's so popular, when you download it and install it, it says "Wait in line."

Steve: Yes. So 10 million downloads in the first 24 hours, says BlackBerry. It became the No. 1 download on both iOS and Android platforms after announcement. And they were overwhelmed with response. And so as you said, Leo, I think it was maybe Monday, maybe Monday evening, I got it, and then it said, sorry, you're going to have to wait in line. And then this was on my new iPhone 5s that I wanted to install it because, you're right, I'm still - haven't yet made the conversion over. I'm still using a BlackBerry. So I thought, oh, cool. And I gave them an email address for me, and they said, "We'll email you when you are first in line." And then I saw a link to a way to get around needing to wait. CNET has a story, "How to Avoid Waiting for BBM on Android and iOS." It turns out their blockage isn't very high tech, and so it's easy to get yourself first in line.

And what PC Mag said was: "BBM was the originator of the modern read receipt, and while that's been replicated in both iMessage and Hangouts, BBM still does it pretty well. You can also do group chats, share pictures, and send files. It basically does all the stuff the first-party messaging clients do, but it's running through BlackBerry's servers. If you're worried about security, this should be on your radar." Now the problem is, I take issue with that. I mean, we know that BlackBerry was big on security. The problem is, even BlackBerry themselves say that you should consider your messages scrambled and not encrypted. And my message to our listeners is BlackBerry Messenger is not TNO. BlackBerry uses a PIN technology, and you're assigned a PIN when you register your BBM on - you get one on a BlackBerry, and it assigns you one when you register it on an iOS or Android device. And unfortunately the encryption uses a global key that everybody has.

Leo: Everybody has, great.

Steve: I know. So thank you very much.

Leo: It stops nothing, no one.

Steve: Yes, exactly. In BlackBerry's own documents they said PIN-to-PIN messages are encrypted under a common global key, and they pass through BlackBerry's infrastructure. They are definitely subject to selective decryption. PIN-to-PIN is not suitable" - that's okay, Leo, keep sighing, because we're going to talk about one that is here in a minute. But "not suitable for exchanging sensitive messages, although..."

Leo: It's also lame because you have to find out somebody's PIN.

Steve: Yes. Although PIN-to-PIN messages are encrypted using Triple-DES, which...

Leo: Oh. That's strong. Of course, everybody knows the key.

Steve: Yes. That's the problem. "The key used is a global cryptographic key that is common to every BlackBerry device in the world. This means any BlackBerry device can potentially decrypt all PIN-to-PIN messages sent by any other BlackBerry device, if the messages can be intercepted and the destination PIN spoofed. Further, unfriendly third parties who know the key could potentially use it to decrypt messages captured over the air. Note that the 'BlackBerry Solution Security Technical Overview' document published by RIM specifically advises users to 'consider PIN messages as scrambled, not encrypted.'"

So they're obfuscated. Now, so where would this be useful? I don't know why 10 million people downloaded it. And I'm not sure now why I'm one of those. But I did. However, after doing additional research, that is, this research, it's like, that's not what I wanted. What I was looking for was something to lift a dialogue with my best friend out of texting because, first of all, it's annoying that you have 140-character limit in texts, or I guess is it - I guess it's 160?

Leo: It's 160, technically, yeah.

Steve: Yeah, exactly, because Twitter is 140.

Leo: Yeah. And that's because of UNICODE or something, I can't remember. There's a reason.

Steve: So that's annoying. Well, it's because you want to encrypt your handle back and forth in order for that, for public stuff. But so that's annoying. But mostly he's using a corporate iPhone, and he's a little anxious, like when we're talking about playing hooky and rendezvousing to go see some wonderful sci-fi on a Friday afternoon, that, well, I wouldn't like my boss to know that that's what I'm doing. So it's nothing mission critical. We don't care if the NSA knows. But we would just like to not have it, because it's a company phone, for his employer to have access to it. So it's like, okay, this looks like it would be nice. I mean, it's very nicely executed. I did play with it for a while. BBM is a

nice piece of work. Not TNO.

So, next up, I just got email from Hemlis. Remember that Hemlis means "secret" in Swedish. And we have so far been unimpressed. Their site is Heml.is, so they found their name by finding a top-level domain that's .is and then doing an H-e-m-l in front of it in order to get their name as their domain. And what they sent me was news of a new video showing it in operation, where they have three phones, and they're, like, sending text messages between these three phones. And it's like, okay. So now it works.

The problem is, in their Q&A, their own question is: What technology will Hemlis use? And then the answer is: We are building Hemlis on top of proven technologies such as XMPP with PGP." Then the next question is: Why not use OTR? That's of course Off The Record, which we did a podcast on, which is what Cryptocat uses for its secure messaging, and it's really good. But they respond to that question: Even though we love OTR, it's not really feasible to use in a mobile environment. The problem is that OTR needs both parties to be online for a session to start, which is true. But a normal phone would not always be online. It would not work at all for offline messages, neither, they say.

And then the kicker is the last question that I highlighted: Will you provide an API and/or allow third-party clients? Their response is: At this point we don't see how that would be possible without compromising the security. So for now the answer is no. And that ends it. Because what we know, I mean, there's no lesson our listeners should know better than a system that relies on the secrecy of its architecture is not secure. Just look, for example, at SQRL, SQRL that I've talked about. Completely open. Here's how it works. This is what it does. No secrets. Because the architecture is secure, and anyone who wants to make a client is able to do so. So, I mean, that's the way you do security now. It's like GNU Privacy Guard, where it's completely open. It's like TrueCrypt.

Leo: You have to, yeah, yeah.

Steve: Open source. Here's TrueCrypt, open source, and the point is that you can - anyone could do, could write a TrueCrypt-compatible interpreter to interpret a TrueCrypt volume with the documentation that's there. That's the way you do it. So the idea that they're saying, no, we won't let you look inside, it's like, that's wrong. And it's the other reason that I felt so good about LastPass was that, when they - when Joe showed me how it worked, explained every detail of it, he even had sample code JavaScript right there, demonstrating it functioning. So it's like, yeah, prove it to yourself. Encrypt something, and go to the web page here, and we'll decrypt it for you, and you can look at the code. It's like, yep, that's the way you want to do it.

So I tweeted about BlackBerry Messenger this morning, and I got a bunch of people who responded, saying, well, then, what is TNO? What should we use? And so I wanted to remind everyone about Threema, which I really like and which really looks good. And when I remind you, Leo, that it's the one with the three dots, then you go, oh, yeah, I like that one. It's not free. It's $1.99 U.S. So, and the good news is, you pay two bucks, and you're supporting them. You're not wondering what their economic model is for existence. They say: "Threema is a mobile messaging app that puts security first. With true end-to-end encryption, you can rest assured that only you and the intended recipient can read your messages. Unlike other popular messaging apps (including those claiming to use encryption), even we as the server operator have absolutely no way to read your messages."

And so these three levels, Level 1, one dot which is red, is the ID and public key have been obtained from the server because you received a message from this contact for the first time. No matching contact was found in your address book, by phone number or email, and therefore you cannot be sure that the person who they claim to be is - I'm sorry. That the person is who they claim to be in their messages. So they're saying, okay. That's the red level of trust. Then Level 2, the orange level, which is two dots, the ID has been matched with a contact in your address book by phone number or email. Since the server verifies phone numbers and email addresses, you can be reasonably sure that the person is who they claim to be. And then, third, the full-strength, three-dot green level, is you have personally verified the ID and public key of the person by scanning their QR code. Assuming their device has not been hijacked, you can be very sure that messages from this contact were really written by the person they indicate.

And so what I'm doing is I'm going to have my buddy Mark buy Threema, and we will meet and swap QR codes, swap public keys face to face, and that way...

Leo: That's a great idea.

Steve: Isn't that neat? And then...

Leo: I'm going to do that, too. I'm buying it, downloading it right now.

Steve: Yup. I really - this is my choice. These guys make...

Leo: iOS and Android, which is great.

Steve: Correct. And they said the verification levels don't change anything in the encryption strength. It is always the same high-grade elliptic curve cryptography-based encryption. But they are a measure of the trust that the public keys saved for your contacts really belong to them. Having the wrong public keys leaves you open to man-in-the-middle attacks. Therefore it is important to verify the keys. And then they also said: Why the name Threema? And I was curious, so I looked. It says it started life as an abbreviation, EEEMA, for End-to-End Encrypted Messaging Application. The three E's were a bit unwieldy, so it became Threema.

Anyway, the other thing I love about this, Leo, you can, on that FAQ page, they're saying: I don't know anybody yet who has Threema. How do I make sure it's working? And they give you a QR code right there for their ECHOECHO person. And so I scanned it. It created a contact in my contact list, and I sent it a message which instantaneously was returned. And that's the other thing that is so cool, is why I like being in an Internet-based service rather than texting, is that sometimes Mark and I, he'll be swinging by to pick me up, and I'll say, "Send me a text, and I'll run out." And the other day he said, hey, you know, he finally called me. He said, well, hey, I texted you, and you didn't come out. It's like, well, okay. And it wasn't until we were at dinner that I finally got his text message. So just not having any texting delay is really nice. This thing, you could easily have instantaneous real-time conversations using Threema with absolute standard, public key-swapping, end-to-end encryption.

Leo: So I got it on - I set up a key. Now it gave me a string, an easy-to-remember-and-say string of, I don't know, seven or eight letters. So I could give you that.

Steve: Yes. What I'll do is...

Leo: But the QR code would be more secure.

Steve: Yeah. I will put you in my address book, and I will send you something so that you can get it, so you and I can exchange and achieve orange level. And then when I see you over New Year's, we'll aim our phones at each other and go to green level.

Leo: [Chuckling] I love this.

Steve: It's very cool.

Leo: I have no idea if it's good or not. But I trust you, so.

Steve: Okay, so...

Leo: It's not open source so there could be a backdoor in it; right?

Steve: I just don't see any, I mean, it's like, okay, yeah, but I'm trusting these guys. They seem 100% to have done it right and to be doing the right thing. And wherever they are, they're not in the U.S., either.

Leo: Switzerland. They're Swiss.

Steve: Yes. Yes.

Leo: Cool. All right. Now, Steve Gibson, and something weird in the Patent & Trademark Office. Doesn't seem unlikely, frankly.

Steve: Well, okay. After last week's podcast, on Thursday, October 17th, came the news that the U.S. Patent & Trademark Office had reversed a prior decision...

Leo: By the way, I said proXPN, not OpenVPN.com. ProXPN, proXPN.com. Let's get that right. Go ahead. They've reversed their decision.

Steve: They have reversed their decision on what is being called the "Steve Jobs

Patent." This is a patent that Apple has which is amazingly broad and essentially forecloses any other use of touch for managing a device. There are 20 claims in this patent. And there was a - it was secretly contested, meaning that someone, and it is speculated Samsung or Google, said to the U.S. Patent & Trademark Office, we need - we're challenging this patent secretly, so we think it needs to be overturned. Initially, that was granted. Last Thursday, on further analysis, all 20 claims were upheld.

And, for example, among them is you put your finger on a touch-sensitive surface, and moving it vertically scrolls the page. That's Claim No. 1. You put your finger on the touch-sensitive surface and moving it side to side changes items. That's Claim No. 2. And it goes on like that. I mean, I don't know what this means, but it seems like it's really bad news for anybody else who wants to do a touch-enabled device, like Samsung and Microsoft and Google, because this has been really looked at, and the claims are being upheld. Maybe what now has to happen is that this goes to court, and those with interests other than Apple, maybe they'd get together or individually they find a prior art, or they demonstrate that this fails the obviousness test because that's of course one of the tests that a patent has to pass is that it would not be obvious to someone trained in the art.

I remember I had a crazy program, it's the Windows program that I wrote to teach myself Windows programming called ChromaZone. It was a commercial product that GRC did that used palette animation. And one of the things that ChromaZone did was you could scroll the help by putting the mouse on the surface and dragging the surface, which is exactly what you do with your finger dragging the surface. So it's like, well, okay, is that not the same? I don't know. But it stuns me, first of all, that this patent, it seemed reasonable that it would be overturned. Now it's been - all 20 claims have been upheld.

Leo: Wow.

Steve: So, wow.

Leo: Yeah. Patent Office loves that Steve Jobs.

Steve: Well, and Steve's name is No. 1 in the list of inventors. There's about 50 in the list. It's like everybody at Apple.

Leo: I doubt Steve actually invented it.

Steve: One wonders what his role was, yeah.

Leo: Wow, that's kind of surprising.

Steve: But really, Leo, how would you scroll something on a touch surface without doing that? It's like, uh, duh. So, yow.

Leo: Well, and this is the risk of inter partes appeal of patents. You can get a reexamination, but it doesn't guarantee they're going to do the right thing.

Steve: Yeah, and I think it's going to have to get litigated, and it's going to have to be - it's difficult to understand that Apple would be getting...

Leo: [Indiscernible] is doing the same thing with the podcast patent. And it's a debatable strategy because, if you win, it ends all litigation. If you lose, it makes it that much harder to...

Steve: I think I just saw really good news, Leo, about that. I was thinking of you. Didn't I send...

Leo: No, no. They began the inter partes.

Steve: Oh, okay.

Leo: That's - it's 18 months before we'll have a result.

Steve: Wow.

Leo: Takes a long time.

Steve: Yeah.

Leo: So beginning it is not concluding it. And there's - you don't - I presume the lawyers at EFF looked at it and said, hmm, this prior art is strong, and we think we have a case. But it's a very risky thing to do. And we don't know if it was Samsung that pursued this. It's an anonymous request. And the problem is that now makes it very difficult for Samsung. And I'm not saying this is a bad thing because I'm a Samsung fan or anti-Apple. It's a bad thing because it means innovation now has a tax in touch. You have to pay Apple if you want to use their patent.

Steve: Yes. Yes. Yes.

Leo: And it does seem like a pretty trivial and obvious solution.

Steve: So our comment last week about there not having been any great sci-fi on TV...

Leo: I was so wrong. I take it back.

Steve: It drew a lot of ire from our listeners, who said, what? Did you not see "Fringe," you moron? It's like, oh, yeah, of course. I loved "Fringe." And, I mean, everyone did.

Leo: I didn't like "Fringe" all that much, but...

Steve: Okay, I did.

Leo: "Battlestar Galactica." You had mentioned "Firefly," which is true.

Steve: Right. And I've talked about "Stargate SG-1." Anybody who wants to just fall into a beautifully produced sci-fi series, "Stargate SG-1" was really good. What I loved about it was the premise that these - an ancient civilization completely covered the universe with stargates that allowed you to hop from place to place. And so "Star Trek" solved the problem by getting in a bus and going somewhere. And we need warp drive so we can get there in a lifetime. "Stargate" solved the problem by creating wormhole between portals. And it just - it's a perfect substrate for building a science fiction series. And I loved it. It had Richard Dean Anderson, who from "MacGyver" on I thought he was whimsical and fun. So I loved it.

And I will confess that I'm enjoying "Agents of S.H.I.E.L.D." Which is about - I think we're about four episodes in. And, I mean, it is a little bubblegum. But it's fun. I'm liking it. So, yeah, there is some sci-fi. And, yeah, "Galactica" was also great for the first couple of seasons.

Leo: It was I who said that. Not Steve. I said that. Steve defended television sci-fi.

Steve: Steve may be on jury duty.

Leo: Good luck. It's actually fun. I enjoyed it.

Steve: Well, I've never been impaneled, and I got the notice, like, six weeks ago. I start phoning in Friday. So there's a chance it could impact next week's recording, which is why I'm mentioning it now. I've never been impaneled. A litigator who's a friend of mine from Starbucks said the end of the month tends to be, like, no one's starting a new case then. So they're not needing lots of new jurors because they're winding things down. For some reason, she said, there's no real reason that anything would be month aligned. But people don't like to start them at the end of the month, for some reason. So anyway, we'll see. Maybe you and I can find a time to do it when I'm, like...

Leo: Oh, yes, we'll work it out.

Steve: That works for both of us if I'm unable to do it on Wednesday.

Leo: We'll do it at night.

Steve: Because we know there would be an uprising if we...

Leo: No, we have to do it. And we will do it.

Steve: If we didn't have it.

Leo: And don't try to get off the - you wouldn't do this, I know. But sometimes people say, oh, there's good strategies for getting off the jury. No, because that means all the smart people get off the jury, and the only people left are people who are too stupid to be able to get off juries.

Steve: Actually, the same person - I tried to last time. I would love to. I've never done it.

Leo: Yeah, serve. It's part of your civic duty.

Steve: This litigator said, "Steve, you are the last person they want on a jury because..."

Leo: You're analytic.

Steve: ..."it's clear, well, and you cannot be controlled. They want people that they can control." And she said, "And frankly, knowing you, you would probably end up being the foreman, and so you'd run the show, and so, well..."

Leo: They don't want you. I thought the same, and I was impaneled, and I was very surprised because I said, you know, the judge, or maybe it was one of the attorneys, I think it was the judge said, "Would you talk about this on the air?" And I said, yeah, after the trial's over. They said, you know, it was very obvious that I - I thought, oh, there's no way you're going to put a journalist who will then write about the story after the fact on the panel. No, they did impanel me. So it's unpredictable. But you know what, you want to get on there. That's your job. We will support you. I will give you the required $20 a day.

Steve: It's only - I think I get 15.

Leo: Fifteen.

Steve: It's only the collision with the podcast which would give me pause. And so if we can work around that, that would be great. There is an amazing illustrated guide to SQRL. Go to SQRL.pl.

Leo: You didn't do this.

Steve: No, not by me.

Leo: Somebody in Poland. Somebody in Poland did it.

Steve: Well, .pl, wherever that is.

Leo: That's Poland, yeah.

Steve: They may have just gotten it. SQRL.pl is beautiful. It was, yeah, they really did a neat job of visually explaining it.

Leo: Wow. Holy cow. Holy cow. Very nice. This is great.

Steve: Yeah, it's just beautiful. My mention last week of an addition, an expansion of the protocol to allow people to change their identities, like remember I said, like, okay, you broke up with a spouse who had your phone, or maybe not a spouse, just a boyfriend or girlfriend who had your phone, and they took their phone with them, but your identity was in their phone. Or you were crossing a border, and bad guys confiscated your phone for weeks or days, or for whatever reason you felt uncomfortable about your SQRL identity maybe being compromised. And we know it's deeply encrypted, so it would take anyone forever to, I mean, like impractically to brute-force it. But for whatever reason you just want a change.

And so what I talked about last week was that a simple extension to the existing protocol, where you'd offer the old key and a new key, and that was signed by both, allowed the server to very smoothly change identities. Well, that created a firestorm of concern in the GRC newsgroup. We're approaching 3,000 postings, unfortunately. I'm again 1,100 behind. I briefly got caught up. And so it's been tough to stay current because there's just so much interest and dialogue going on about this. But the feeling was that allowing what I'll call "in-band identity changing" as opposed to out-of-band changing, where you would go to a website, and you would prove your identity with email or by using old-school username and password, and then it would say, okay, you've authenticated by some other means than SQRL.

The argument that the really security-concerned people had was that you're using a credential that you fear may be compromised in order to authorize the change to the new one. They said, okay, that's just brain dead. It's like, well, okay. I mean, I could see their point. And so the argument was that, if a bad guy got your credentials, that is, somehow you used a really bad password, really, like, "abc" or something, or like "monkey" or "password," something like the first thing a bad guy would guess, or it was somebody who might know your password. For whatever reason, if they were able to acquire your

identity before you, then allowing in-band identity changing would let them change your identity and lock you out of your use of SQRL. And I thought, okay, I, yeah, I can, I mean, if we allow all those things lined up in a row to be true, then, yeah, I could see that in-band identity changing should have a higher bar.

So yesterday morning I spent a couple hours at Starbucks. And I designed the protocol - I designed a protocol that does that. It is again perfect. It's a technology where your identities will be locked after you assert them and associate your SQRL identity with a website. Nothing can change it. That is, even you can't change it because, again, a bad guy could be you. A bad guy could be impersonating you. And the way this works is there's a separate key which is not your normal master key, which you can freely move around among devices. But this is your identity unlock key, which you would only use in the event of wanting to change your identity associations, change your master identity key.

And so the point is it does not live in your device. It is never written to nonvolatile memory. It will not be stored. It is just for this purpose. And it turns out it's a pretty simple protocol. It uses all the existing primitives we already have, very low requirement over on the web server side. It just has to make available a little more storage. But the client does the work. I haven't published it yet. I've got diagrams and text written, but I just need a little more time with it. But so that's where we are with the project. We're moving forward. More people are supporting it. And we're ticking off issues and solving problems as we get this thing nailed down.

Leo: Any sentence that begins "I spent a couple of hours in Starbucks and created a protocol" is my kind of sentence. You're my kind of guy. Steve Gibson. You'll find more about SQRL, not only at SQRL.pl, but also at GRC.com. That's Steve's site, and it's a great place to go, I mean, there's all sorts of stuff there. Of course SpinRite, the world's best hard drive maintenance utility. You've got to get that. But everything else there is free, including his security forums. The discussion of SQRL lives there. If you want a question answered by Steve, the best way to do it, he doesn't do email, is to go to the website, GRC.com/feedback, pose the question there. I guess we'll do questions next week.

Steve: Yeah.

Leo: So this would be a good time to leave those questions there, barring some emergency security topic, and get all the free stuff, read about passwords, it's becoming more and more just a great place to go for everything that you're interested in. Because you're listening to the show, I figure that's a safe bet. Steve, let me know about the jury duty. We'll let people know, we'll put it on our calendar at TWiT.tv. There's a calendar there of our broadcast and production schedule, and we'll update that as soon as - if there is a change, thanks to jury duty. What else? You could find 16Kb versions of this show, the audio for bandwidth-impaired, or transcripts, too, that Steve pays to have done by the great Elaine Farris on his site, GRC.com.

On our site, full-bandwidth audio and video, each and every week on demand, TWiT.tv/sn for Security Now!. But you can also get it anywhere you get podcasts. If you subscribe, you'll get it every week automatically. And that's a nice thing to do. Everybody should have the complete set, in my opinion. Looks nice on the wall.

Somebody maybe we'll do DVDs, the Steve Gibson Collection. No. I don't think that's going to happen. I don't think that's going to happen. Who's on Triangulation tonight? Is it Ladar Levison? It is.

Steve: No kidding.

Leo: So you might be interested in tuning in...

Steve: Cool.

Leo: Yeah. You might be interested in tuning in for Triangulation, about 4:00 p.m. Pacific, 7:00 p.m. Eastern tonight.

Steve: Yay. Just to remind our listeners, he is the founder of Lavabit who deliberately decided he had to pull his service down.

Leo: You know, I would love it, Steve, if you wanted to join us for that. You would be more than welcome.

Steve: I would, if I didn't have plans this evening, but I do.

Leo: [Singing] Jenny.

Steve: Yup, it is Jenny.

Leo: I would never want to get between you and your loved ones. Well, anyway, if you can't watch the show live, you can always get a copy of Triangulation, as well, at TWiT.tv. All of our shows are available that way.

Steve: You're going to do a great job.

Leo: Well, thanks to you I'm kind of up on this subject a little bit.

Steve: Yes, cool.

Leo: I can't wait. I think it's a great score to get him on.

Steve: Yay.

Leo: And I'm sure there's a lot he can't say, so it's going to be a little bit of a dodging and ducking and weaving kind of a...

Steve: Yeah. He may have his attorney sitting next to him.

Leo: I hope he does, for his own sake. I don't want to entrap him by any means. And I certainly don't want the government to use what we talk about on their behalf. So thank you, thank you, thank you, Steve Gibson. And thank you all for being here. We'll see you next week sometime. Maybe our regularly scheduled time, which is 11:00 a.m. Pacific, 2:00 p.m. Eastern time, 18:00 UTC on Wednesdays.

Steve: Almost certainly.

Leo: Almost, yeah, you're not going to be [inaudible].

Steve: Thanks, Leo.