SECURITY NOW!

Transcript of Episode #437

New Year's News Catch-Up

Description: This first podcast of 2014 catches us up on all of the news that transpired over the Christmas and New Year's holidays - and there was a LOT of it! (Like it or not, the NSA news just keeps on coming!)

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-437.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-437-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve is back. Our first show of the new year, what are we talking about: the NSA and the ANT protocols. Lots of security news. We'll catch up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 437, recorded January 7th, 2014: New Year's News Catch-Up.

It's time for Security Now!, the show that covers your security and privacy online, your safety online, with the guy in charge, the "Explainer in Chief" we call him, Steve Gibson. Oh, my goodness, Happy New Year, Steve.

Steve Gibson: Yes, indeed. And I was wearing my Explainer in Chief T-shirt for the day up there with you for...

Leo: I loved that.

Steve: I didn't make it 24 hours. Actually I had a lot of people asking me, "Where did you get that TNO T-shirt?" And it was from one of our listeners. I'm so sorry that I've, like, it was so long ago, it was a couple years ago, and I just kept the T-shirt for the right occasion. I thought this was the right occasion.

Leo: It was the right occasion.

Steve: It was someone who prints T-shirts professionally, and he just sort of sent me that as a gift to thank me for the podcast. And many people were saying, "Oh, where did you get that?" as if maybe they want one. So if you're still listening to us, Mr. T-Shirt Maker, tweet me or drop me a note or something.

Leo: We should make them.

Steve: Certainly, yeah, it was very nice.

Leo: It said "TNO" in big letters.

Steve: Big letters. And then down along the bottom, "Except the Explainer in Chief."

Leo: So, Steve, so we've got a lot of - it's been, like, it's only been two weeks, but it feels like a year.

Steve: It does.

Leo: We've got a lot to talk about. But first I'd say, Steve, thank you for coming up to our New Year's Party. We did 20 - it was going to be 24 hours of 2014. It was, like, 23 hours and 48 minutes of 2014.

Steve: Okay. Yeah, I bailed at about 1:30 a.m.

Leo: Did you?

Steve: Well, because it was beginning to feel like it was petering out. And I thought, okay, don't think...

Leo: Yeah, it was a perfect time to leave.

Steve: ...much more is going to happen.

Leo: What was going on there, I think it was me, Brian Brushwood, Justin Robert Young, and Will Harris.

Steve: Filling time, basically.

Leo: No, it was like standing around at the bar. It was great.

Steve: Oh, okay.

Leo: If you think of it as filling time, then that's fine.

Steve: Well, I didn't see it. I didn't see it, so...

Leo: You know what we did see, and I have footage, I don't know if I - I don't know. I don't want to embarrass you or anything.

Steve: Of me with Chad's hair, navigating?

Leo: That was fun.

Steve: Oh, my goodness.

Leo: And then of course at midnight, at midnight we played in the new year. And Steve apparently danced with Captain Kirk.

Steve: Well, yeah, you know...

Leo: And you're quite the dancer. Kirk was not very responsive.

Steve: No, no.

Leo: But you? You know how to dance.

Steve: And I was sober, believe it or not. That was - actually, I couldn't have done all of that jumping around and spinning and twirling.

Leo: You were fired on coffee. If you didn't - now, we're taking a lot of that New Year's Eve broadcast. There was so much. I went to bed that night, and you know how sometimes you kind of go over the day's events and think about them. I couldn't. There was so much stuff from that 24 hours. We did so many things, including...

Steve: Plus, in fact, toward the end we were talking about things that had happened that morning as if they were yesterday. I mean, it felt like it was a long time ago...

Leo: Well, it was.

Steve: ...that that happened. And it was four hours, or 12 hours, yeah.

Leo: So, but, Steve, thank you for coming. You showed up almost at the very beginning. We made coffee. So what I was about to say is there were so many things, we didn't want to just put out a 24-hour video. So our editors, once they recover, are working on chopping it into bits. And one of the bits will be Steve making coffee.

Steve: Yup, we did that, as I had promised our listeners a long time ago when I came.

Leo: Awesome.

Steve: Thank you. Yes, you did like it.

Leo: And then you were very good as the navigation officer aboard the Starship Artemis.

Steve: Yes, twice. I got the hang of it the first time, and then - or, yeah, by the end of the first time. And then we were much better navigating the second time. So...

Leo: First time I was the captain. I wasn't so good. Then we let Justin Robert Young and Brian Brushwood captain the starship. They were different. A lot of shouting.

Steve: But that was, you know, also toward the end of the night. And, yeah, lot of fun.

Leo: Anyway, we decided that the event was so much fun that we're going to do it again. In fact, I think we'll be doing it every New Year.

Steve: Well, and the beer tasting that you and I did, I think, was another one of...

Leo: Wasn't that fun.

Steve: ...the highlights that were sort of unexpected.

Leo: Yeah. With Mary Jo Foley.

Steve: Yup. And a number of people, that very first beer, I've seen tweets thanking us for introducing them to that sweet pink one.

Leo: The Kriek Lambic, yeah, Lambic. It was a cherry-flavored lambic beer that, you're right, you loved.

Steve: Well, it was the first one. And I agree, after we went into the tar beers, then...

Leo: You're not a beer drinker.

Steve: ...going back to the cherry was like, whoa, okay. Wait a minute, that's a little fruity.

Leo: It's from a Belgian brewer. It's Lindemans Kriek, and it had cherries in it. It was almost like a fruit punch. So, yeah, that will be another segment we'll chop up.

Steve: So where will our listeners find these pieces of history, which will be preserved for all time? Will you guys be hosting them? Will they be on TWiT.tv? Because Simon Zerafa, our friend of the show, commented that he was seeing them appearing on the Inside TWiT YouTube account.

Leo: That's where they'll be appearing. So if you go to YouTube.com/insidetwit, so far we've got three segments up. You know what, I am not fully in control of this. What I would like eventually is to have this chopped up even more. But we do have, from the very beginning...

Steve: The first Game of Geeks...

Leo: Yeah. But, I mean, we have - this is an hour from the - there's three segments; okay? So there's three chopped-up segments. Anyway, YouTube.com/insidetwit. I can't make the editors work too hard. So I think what they're doing, it looks like, is an hour at a time.

Steve: Well, and I would - I have to tip my hat to your whole crew. I mean, you were standing there asking them, okay, now where should I stand? Now what's next? I mean, because this whole day was mapped out and planned and designed by them. And it was just fabulous. It was an absolute success.

Leo: I think if nothing else we've demonstrated that the studio is an amazing place; that with our very, very talented and motivated staff, we can do amazing things. And I just look forward to doing this every - in fact...

Steve: And none of the champagne corks broke anything. I was amazed. I mean, I kept waiting. I mean, they were violent; and, you know, there were 24 of them because we kept blowing champagne every hour. And nothing broke.

Leo: I think you're in Hour 3. Yeah, here's the coffee-making. So Hour 3 stream.

[Crosstalk]

Leo: Because when I was out wine tasting - here we are, Steve and I, making coffee, wearing his TNO shirt. So that's in the Hour 3 of 24, just went up on Inside Twit.

Steve: And you can see there that I had my six-shot venti latte in front of me.

Leo: Oh, yeah.

Steve: That got me going in order to get there.

Leo: Lesson No. 1, never try to make coffee without being caffeinated, apparently. Heavily caffeinated. Steve's...

Steve: That's called "booting," booting your coffee process.

Leo: So what you're saying is this is your firmware, and...

Steve: That's my BIOS. That's my BIOS, baby.

Leo: The other thing I wanted to mention is last week's episode, which, if you didn't see, do go see. It's a video episode.

Steve: Oh. You're talking about the holiday episode.

Leo: Yeah, yeah.

Steve: Yes. Again, fabulous feedback. Every - I've never - I hear nothing negative. Everyone who did say something absolutely loved our blast from the past, the so-called "time capsule episode" that was for you and me meeting the first time in the flesh, 15 years ago. And the shows from ZDTV, the commercials, a lot of them I left in just to sort of set the tenor...

Leo: That's kind of fun, isn't it?

Steve: ...of the time. Yeah. And talking about backing up hard drives to VHS tapes. It's like, okay.

Leo: Yeah. That was a good idea - then.

Steve: Yeah. So...

Leo: I don't know, if you had those VHS tapes today, I don't think they'd be worth anything, but...

Steve: I do have the one - I used to drive your production crew in those days crazy. I would, you know, I'd fly up on my own dime and be there and do the shows with you. All I asked for in return was the video.

Leo: Fair enough.

Steve: I didn't know why, but that's what I asked for. Even when, years later, we were doing it in Toronto and then in Vancouver, I just said, you know - and I'd sort of just politely remind them with email, uh, can you send those tapes? And I'd get four a month. And so I've got all of them. So...

Leo: That's awesome.

Steve: ...we'll have plenty of time capsule episodes in the future.

Leo: That's great. But we do have some catching up to do because...

Steve: Oh, my lord, yes.

Leo: What's surprising is normally in tech news nothing happens during the holiday break. But bad guys never rest.

Steve: Oh, well, and it's funny, too, because - okay, so as I have been doing, "Today on Security Now!": New Year's Eve at the Brick House, which we've already covered. 2013 was certainly not the end of annoying NSA news, not by a long shot. In fact, we have truly unsettling NSA news.

Leo: Oh, boy.

Steve: It turns out that routers, many routers, are quietly listening on port 32764. We'll discuss that. We've got a note about Mozilla's screaming native code operation progress; Snapchat's massive 4.6 million username and phone number disclosure, involuntary disclosure; and even my long-awaited sci-fi reading guide and much more. So a ton of fun stuff to talk about.

Leo: We will begin the New Year, Security Now!, our 437th episode, in just a moment. By the way, our new time, too. So if you tuned in Wednesday to watch, and we weren't there, that's because we're on Tuesdays now, and not at 11:00 a.m. anymore, but 1:00 p.m. Pacific, 4:00 p.m. Eastern time, 21:00 UTC. We do love you to watch live. That's my preferred thing because you can interact. I can watch the chatroom and so forth. But if you cannot, fear not, because of course on-demand's always available after the fact.

Steve: And you know, I'm glad you mentioned the chatroom because they were so neat during the New Year's Eve event. And I wanted to make sure that people who are in the chatroom understand the degree to which everybody there is dependent...

Leo: Oh, yeah.

Steve: ...on the chatroom. And you know that because, as I was, someone standing basically anywhere you are in the TWiT Brick House, there is a screen monitoring real-time chat somewhere.

Leo: Oh, yes.

Steve: All you have to do, you can just look anywhere you are, and there is a scroll happening with what people are saying. I mean, so it really does, like, connect us in and make it an interactive process.

Leo: Yeah, you probably don't realize that if you're not in the studio.

Steve: Exactly. That's why I want to make it really clear to people.

Leo: You don't watch the chatroom while you're doing your show because you're focused on what you're talking about.

Steve: Oh, I just couldn't get it. Yeah, no, it would distract me like crazy.

Leo: Well, it's a skill I've learned. In fact, so much so that I can't do it without the chatroom. I don't know if people know this. We don't usually talk about when we're DDoSed, but we did get DDoSed during the show, during - I can't remember what it was. But during one of the shows, maybe it was TNT. And Sarah Lane and I, both who live on the chatroom all the time, the chatroom was down, and we were both thrown. And Sarah said, "Where's the chatroom?" And I said, "It's down, just ignore it." And it's funny, it's like if you've been doing a Broadway show in front of a sold-out crowd for years, and then suddenly there's no one in the theater. It's weird. So, yeah, that's why the chatroom kept dropping connections. Occasionally this does happen, we get DDoSed. But we have DDoS protection. We flipped the switch, and it was fine. I'm not sure what was going on.

Steve: I just wanted everyone to know that, I mean, it's a crucial part of the operation there.

Leo: Absolutely. We adore it. We adore it. Let's get to the security news. There's quite a bit of it. Leo Laporte, Steve Gibson, Security Now! on the air. Let's catch up. What did we miss last week?

Steve: Okay. So, many of our listeners were concerned when I said at the end of 2013 that we would not turn this into the NSA Now! podcast. And so I got a lot of this through Twitter. And so I was tweeting back, no, don't worry. If stuff continues to happen, we'll absolutely cover it. Well, boy. So first of all, don't anyone worry. In fact, next week is just going to be a deep dive into one of the stories I'm going to discuss this week, but kind of cover the surface of it because there is so much there, I just haven't had time, I haven't set aside the amount of time I'm going to need to give it the kind of coverage I want.

But first, what has to be the most disturbing news of both the old and the new year was something that came to light through a Reuters story and surprised everyone, that RSA, the famous cryptographic research and cryptography commercializing company, founded by serious academic cryptographers who developed a lot of these technologies, accepted $10 million from the NSA in order to set that weak pseudorandom number generator as the default, we believe. That's what this Reuters story alleges. Which is to say - now, okay. To remind people a little bit, there was a set of four pseudorandom number generators that the National Institutes of Standards and Technology (NIST) was establishing as standards. People could use them, and they were saying they generated really good random numbers.

So when we've covered this, as we did in 2013, and in fact even before that, when the first concerns about this so-called "dual elliptic curve deterministic random bit generator" came out, I was the one who said, "Don't worry about this. Nobody in their right mind would use this one." There were four, and this was the weirdest and slowest of them. Even if we didn't know that it had been potentially and apparently compromised by the NSA, you don't want a slow random number generator that's no better than the faster ones.

And so I was thinking no one would use it. So it's like, okay, so it's there, and maybe it's been corrupted by dark forces, but who cares. Well, it turns out we then learned it was the default, which, like, okay, that's - you know. And then on the podcast before, last year, I was saying, well, these are smart cryptographers. Why is it the default? How do you explain that that's the default?

And then the other shoe dropped. And while $10 million may not seem like a lot of money, the year that it was paid, that was one third of RSA's annual revenue. And there's a lot of expenses that go against revenue. This was expense-free. They had to set a bit somewhere in order to have that be the default random number generator that you get when you use their BSAFE library. And I haven't mentioned this or shown this before, Leo. But I own the BSAFE library.

Leo: Oh. Oh.

Steve: I mean, this is it. I mean, this was the standard of cryptography at the time. I purchased it years ago. And in fact the copyright on this copy is 1992. I looked this morning, yep, copyright 1992.

Leo: So that predates this arrangement.

Steve: Exactly. And here on the page of random number generators, they only have two, and they are hash-based pseudorandom number generators. So that's before all of this happened, and it was pure then. Subsequently, here is a page from release notes of RSA BSAFE. This particular version of BSAFE is called Share for C/C++ 1.1. And in the release notes, the very first item under Content says New Features, and the second item is Changes. And on Page 2, which is where we get Changes and New Features, the very first item under Changes says: "The changes in this release of Share for C include" - the first one - "all random numbers generated for use in Share for C are generated by the dual elliptic curve (EC) deterministic random bit generator (DRBG) using the P-256 prime curve." And it says, "(128-bit security strength by default)." So that is exactly, I mean, this is, and this is dated 15th of September, 2009.

Leo: Oh, man.

Steve: So that's, I mean, that was the page from the release notes showing the change when this happened about five years ago. So the wording of this in the article I thought was really perfect. So I'm just going to share this. This is exactly as Reuters wrote it. They said: "An algorithm called Dual Elliptic Curve, developed inside the NSA, was on the road to approval by the National Institutes of Standards and Technology (NIST) as one of four acceptable methods for generating random numbers. NIST's blessing is required for many products sold to the government and often sets a broader de facto standard," meaning within the entire computer industry, which certainly is the case.

"RSA adopted the Dual_EC_DRBG algorithm even before NIST approved it. According to an official familiar with the proceedings, the NSA then cited the early use of Dual Elliptic Curve [PRNG] inside the government to argue successfully for NIST approval. RSA's contract" - that is, this one for which they received $10 million - "made Dual Elliptic Curve the default option for producing random numbers in the RSA toolkit. No alarms were raised, former employees said, because the deal was handled by business leaders rather than the technologists. 'The labs group had played a very intricate role at BSAFE, and they were basically gone,' said labs veteran Michael Wenocur, who left in 1999. Within a year, major questions were raised about Dual Elliptic Curve. Cryptography authority Bruce Schneier wrote that the weaknesses in the formula 'can only be described as a back door.'"

So what we have is sort of a classic bureaucratic bureaucracy management where the technologists weren't involved, whereby paying RSA to make it the default in their package. After BSAFE was then in use, and it wasn't yet approved, the NSA got it approved, got the NIST to approve it because it was in use. And it was in use only because RSA had been paid $10 million to put it in use. So, I mean, it's stomach-turning.

Leo: Wow, yeah.

Steve: Yeah. And I want to draw some contrasts here because we're going to be talking about the Der Spiegel article here in a minute, and the amazing revelations there. This is of concern because what we believe is that this then widely used package became the core random number generator, like throughout the industry, and that the NSA had unique knowledge of RSA's documentation, and they believed I'm sure that it gave 128 bits of strength. It is probably not 128 bits strong if you know the way in which it's biased. And it's probably been biased deliberately.

I mean, there was really no evidence, even as suspicious as we were of it, there was no concrete evidence. But the fact that it's the slower of the four - and the other three are based on sound technology. They're based on hashing, or they're based on a good cipher. Running a cipher, using a cipher with a key to generate pseudorandom data is absolutely an acceptable, bulletproof way of generating that data. If the cipher is good, the pseudorandom data will be good, too. Similarly, running a hash in a cycle where the output goes back into the input, if the hash is a good hash, you're going to get out really good pseudorandom numbers. Or if you want to key it, you use an HMAC, which is basically a means of mixing a key in with the hash and, again, putting in data that will come out pseudorandomly. Those are all recognized strong techniques.

And then out of right field comes this thing that the NSA designed and wants added, and then arranges to make the default, even though it's unproven and improvably secure, where the other ones are, and the slowest of all of them. So, I mean, if we didn't have enough reason already to be suspicious, the fact is that now we get this report from a very reputable source. And people have since been interviewed, and they've said, yeah, uh, yeah.

Leo: Yeah? Yeah? Yeah?

Steve: And RSA's conference is coming up at the end of February, the annual 2014 RSA Security Conference.

Leo: Oh, that's going to be interesting.

Steve: Well, several major speakers have dropped out in protest.

Leo: This is so damaging.

Steve: I know.

Leo: True or not. And I think it probably is true. But true or not, this is so damaging to U.S. interests.

Steve: Yeah. Yeah, well, wait till we get to damaging to U.S. interests. That's our next story. I will note, however, for anyone who's attending, don't leave the conference early because he'll probably be pretty funny. Stephen Colbert has been confirmed as the closing keynote of the conference. And so lord knows what he's going to do.

Leo: It's all showbiz now.

Steve: I hope the RSA knows what he's going to do. Yikes. Sorry for a little noise here in the background. We have a garbage truck is going to empty some cans. Okay. So, next up. And this is what I want - I need to look at this more closely than I have been able to, and I will do it for next week because it fascinates me, and we can't do it justice along with everything else we have to talk about this week. So this is the tease, the setup, essentially, for next week's episode. And this is the so-called ANT division of NSA, whose catalog of exploits for nearly every major software and hardware and network came to light from an article in Der Spiegel.

And I tweeted this. I guess I just tweeted the link to the catalog this morning. As we have been doing now, this is the fifth episode where I have been posting the same show notes that you and I are reading right now, Leo, as part of the material over at GRC for the episode. And I tweeted the link to the show notes before we began so that people who are watching in the chatroom can also read along. I created a bit.ly shortcut for this catalog, so it's bit.ly/, all lowercase, nsa-ant [bit.ly/nsa-ant]. And this is a WordPress blog that's leaksource.wordpress.com is where that bit.ly expands to. And it truly makes your head spin, to the extent that Bruce Schneier, who has also not been happy as a consequence of the Snowden links and everything that has come from it, Bruce is now doing a blog post a day to take each of these on in turn.

So to give our listeners a sense for it now, what this page describes, what it contains is a series of image slides from this catalog which lists dates when the exploits are becoming available, what versions they're in, how much they cost. Some of these are $30. If you just want a cable that allows you to spy on the video information going by, that's 30 bucks. If you want your own GSM cell tower, that'll be $40,000. But you can order one if you're an NSA division that needs that, and they've got one. So these all go by two-word concatenated code names like DeityBounce, or IronChef, or FeedThrough, GourmetTrough, HalluxWater, JetPlow, SouffleTrough, HeadWater, SchoolMontana, SierraMontana, StuccoMontana. They were happy with these Montanas there for a while.

Leo: They like Montana.

Steve: Yeah, the CTX4000 is a model number of - I think that might be the cell tower or something. It's data collection.

Leo: As Schneier points out in this, though, these are all retail attacks. They're targeted attacks; right?

Steve: Yes. And so that's - so let me get through this really quickly. So LoadAuto, NightStand, NightWatch, PhotoAnglo, Sparrow II, TawdryYard, Ginsu, HowlerMonkey, IrateMonk, JuniorMint, I mean, some of these are going to go down in history. Maestro-II, SoberKnave, Swap, Trinity, WistfulToll, SurlySpawn, DropoutJeep - and we're going to cover that specifically in a second because that's about iPhones and generated a lot of news over the holidays. GopherSet, MonkeyCalendar, Picasso, ToteChaser, ToteGhostly 2.0, CandyGram, CrossBeam, Cyclone Hx9, EBSR, Entourage, Genesis, Nebula, Typhon HX, WaterWitch, CottonMouth I, II, and III...

Leo: I can't keep up.

Steve: ...FireWalk and RageMaster. I mean, and this is, I mean, it sounds like a joke, but it appears absolutely authentic. And we skimmed over that. But the reason I need to give it a podcast, our listeners will understand next week when I do because there is a disturbing level of detail specified about each of these, what they do and how they work. And what I want to get from studying this, and what I want to share, is sort of the overall gestalt, the mindset; and, stepping back a bit from it, what lessons does this teach us. But what's worth mentioning, Leo, you started into, which is I consider this very different from a deliberate attempt to weaken a random number generator that the entire industry and world uses. And as you said, this is targeted.

This is the NSA wants to penetrate a BigIron Juniper router, and one of these projects allows a division to purchase that technology, or sometimes it doesn't cost anything, to acquire that from this division of the NSA that designs penetration technology. And again, remember that these are exploits for nearly every major hardware and software package. All the router technologies, all, I mean, like the stuff we use all the time. There are fake cell towers, cell tower technologies in a package that the NSA can set up when they want a bad guy's phone to connect to them rather than a real tower.

There's no evidence of collusion on the part of the companies whose material has been hacked. And more and more, I mean, with the exception of the government letters which go to companies which prohibit them from mentioning that they've received one, but which specifically requests data in a certain case, it really, I mean, it is looking like these companies are really taking the brunt of the damage because, even though no one now thinks that they were complicit in this, it's looking like the NSA has really strong hackers who are able to dig right through secure firewalls.

So, I mean, one of the things we see often is BIOS-level attack. And so many of these, as I was scrolling through, generating that list, I was seeing essentially the same graphic, with small variations, recurring. And it looks like - and I'll have an absolute grip on this and grasp of it next week - that one of the things the NSA likes to do is get in and modify firmware. That seems to be one of their approaches is they will launch a targeted attack at a person, and that person will execute code which gets under the OS, down to the motherboard, makes some changes in the firmware, and then that enables a persistent - gives the NSA persistent access to that platform.

But the point I didn't finish making was that modifying a random number generator that everybody uses is really wrong in every way. I mean, it just - that's upsetting. The idea that the NSA probably had this was something we all probably thought. I was never imagining that the NSA was paying RSA $10 million to give the entire world crappy random numbers in a way that they could leverage.

But the idea that there was a division like ANT, the ANT division, that was cooking these other really cool penetration technologies up, that's what we hoped, that's how we hoped our dollars were being spent because they are targeted. They're not blanket monitoring everyone's telephone metadata in the world. It's we think this guy is bad; we need to get in and monitor him.

So next week I'm going to break all of those acronyms down, not individually because there's too many of them, but it's not really necessary. I want to be able to explain to our audience what the NSA wishes we didn't know, which is exactly what this means. What does this mean, essentially, that they're able to do this? And what are they able to do, based on the catalog that is now in public view? But one of those stood out over the holidays, and that was called DropoutJeep. And the question arose, does the NSA have total iPhone access? And it looks like at one point they did. We don't know where they are today.

Leo: That's one thing to mention on all these slides, is they're old. And DropoutJeep is 2008, the second iPhone.

Steve: Yes. It came out a year after the initial introduction of the iPhone. And remember that another thing we talked about is we know that there are baseband processor vulnerabilities. That's not the ARM7 that Apple is using. That's some component which is actually probably a Snapdragon or some Qualcomm chip because Qualcomm was big into cellular technology. And so it's, like, in charge of all the cellular communications. The ARM7 processor is, like, making icons look pretty. It's all eyewash and GUI stuff, and it's what all of the iOS apps run on. Whereas this Qualcomm or Snapdragon processor, that's the so-called "baseband" processor, and we talked about that a few episodes back, which no one really pays attention to, and the NSA is probably glad because that's very likely their way in is through this aspect that we're just not looking at where everyone's worrying about, oh, is my 16GB encrypted when I type my four-digit passcode, and the NSA's going, uh-huh, good luck with that. We're not worried about that.

So what we know is the NSA had worked on software that would allow it to remotely retrieve, and this is from the reporting over the holidays, virtually all the information on an iPhone, including text messages, photos, contacts, location, voicemail, and live calls. So the slide, of these many for DropoutJeep, says - and here you get a sense for the jargonism of the NSA. It's a StraitBizarre, that's another concatenated pair of words, S-t-r-a-i-t, StraitBizarre - that's a noun, apparently, in this jargon - based software implant - and that's a word we see, the NSA uses the term "implant" for this kind of exploit - for the Apple iPhone - and I'm reading from the slide - operating system, and uses the ChimneyPool framework. DropoutJeep is compliant with the FreeFlow project. Isn't that nice. Therefore, it is supported in the Turbulence architecture.

And so we have a block diagram, six blocks connected in a circle so that they're chasing their tail. It starts with the NSA ROC Operator. Then that has an arrow pointing to the Load Specified Module, which then goes to Send Data Request, which then links to iPhone Accepts the Request, and then Retrieves Requested SIGINT Data, and that points to Encrypt and Send Exfil Data. We know that that's exfiltration, meaning out. And then that returns, the final arrow returns us back to NSA ROC Operator.

So what that is saying is that, once an iPhone has had this implanted in it, the DropoutJeep StraitBizarre implanted in it, then in real-time the NSA ROC operator can query that iPhone over its communications protocol for whatever they want. And so below this diagram it says "DropoutJeep is a software implant for the Apple iPhone that uses modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device. SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, et cetera. Command, control, and data exfiltration can occur over SMS messaging" - okay, slowly - "or a GPRS data connection. All communications with the implant will be covert and encrypted." Don't we wish our own communications with an iPhone were.

"The initial release of DropoutJeep will focus on installing the implant via close access methods. A remote installation capability will be pursued for a future release." So that's what we know. I mean, that gives you a sample, a feeling of one of those incredible number of exploits that are available in the catalog.

Leo: But because it's old, that's a snapshot of what they could do in 2008. I mean, presumably they're keeping this stuff up to date and can do more, and work with more modern operating systems, et cetera.

Steve: Yeah. Yeah. And, I mean, if we've learned anything over the years that we've been looking closely at security on the podcast, it's that very complex software, and unfortunately all of our software today is very complex, has bugs. I mean, it's not yet the second Tuesday of the month. That'll be - or is it? No, it's not. That'll be next Tuesday. And Microsoft will roll out their bugs du month for us at that point. And, I mean, there's never been a month without them.

And all the other software products that are really complex have problems. So if you have enough money, and you are sufficiently motivated, really it's hard to argue that there isn't a way in. And so basically this is the quiver of arrows that the NSA has created for themselves and, as you said, Leo, even though these are old, has doubtless been creating even more frantically recently as the ante has been upped on this and as they've been able to obtain more money and budgets and more technology. And look at the center that they're building down there in Utah for this. So, yeah. Wow.

Another little bit of news came up, and that was - it sort of put me in mind of the question, when is a power light not a power light? And the answer is when it is separately controlled by firmware.

Leo: I know where you're going with this one.

Steve: Yeah.

Leo: Didn't we have this discussion when we first talked about the idea of taking over webcams?

Steve: Yes.

Leo: Could you do that without tripping the red light?

Steve: Exactly. And of course my advice, which has stood the test of time, is put a sticker over it.

Leo: It think it will continue to stand the test of time.

Steve: Yeah. I mean, it's still not the case, from what I've seen, that laptops have a mechanical shutter. But they absolutely should.

Leo: Some do. They're starting to do that, yeah.

Steve: Oh, good. Good, good, good, good. They absolutely should. I was going to mention the laser that I own, the very high-power laser, which has triple interlock, as law requires. And one of them is a delay. When you press the button to turn it on, there's a legally enforced delay before it engages. It also requires a key, separately from the button, a key switch that must be engaged. And law requires a physical shutter over the front. And this is why. I mean, obviously, if that shutter is closed, doesn't matter what happens electrically, you've blocked it. You've blocked the photons. And what you want is a reliable photon blocker, folks. You do not want to trust, unfortunately, the technology.

So here's what came to light. It turns out that it is possible, sadly, but hardly surprisingly, to turn on webcams and the cameras on devices. And again, we presume that any device with a light, maybe it can be controlled separately. Wired.co.uk had an interesting article, actually it was late last year, but I liked their description so I want to share it. It's perfect, and we'll discuss it a little bit more. It says: "One signal wire line" - and this is the actual design, and I think this was an early MacBook. Yeah, I'm sure it was a MacBook. "One signal wire line joins the USB interface chip to an input on the imaging sensor" - and that line is called "standby," or that input is called "standby." "When the line is held high by the interface chip, the sensor is put into standby mode and thus stops producing data. When [that line is] held low, the sensor is taken out of standby mode and starts [streaming] data. The same line is also wired to the negative side of an LED."

And actually that's just what you want. So the positive side of the LED is connected probably through a resistor to 5 volts. The negative side is connected to this wire. So when that line is high, it'll be the same. The negative side to the LED is at the same voltage as the positive side. Thus the light is off, and the imaging chip is off because it's getting the high, standby-enabled signal. When that line is pulled low, then the imaging sensor is taken out of standby. And now the LED has voltage across it, probably 5 volts, because the bottom of it is being held at ground, held low, so the LED is on. And now, okay, that sounds great; right? So that whenever the sensor is taken out of standby, the LED is going to be turned on. So in principle this should serve as a hardware interlock.

Unfortunately, the whole system is controlled by a layer of software. When the device driver for the camera is loaded, the host PC uploads a small program into the USB controller. It doesn't have any permanent firmware storage of its own. So it needs to be loaded every time the camera driver is loaded, whenever the machine is turned on. This small program, in turn, configures the imaging chip. The imaging chip doesn't have too many configurable properties. But one thing it does have is whether or not it pays any attention at all to the standby input.

Leo: Why would it pay any attention?

Steve: So you can disable, in software, the standby input, then not bother bringing it down to take it out of standby; and thus, turning the light on, leave it up as if it's in standby mode, thus suppressing the LED. Yet, if you've changed the firmware associated with the driver, you're streaming data anyway.

So the Wired.co.uk article continues, saying: "Apple's own drivers set a configuration where standby is respected. But other configurations are possible, such as one where the chip ignores standby entirely and always produces image data. With this knowledge in hand, the researchers" - the researchers this article is citing - "wrote a new piece of software to upload to the webcam. This piece of software was much like the normal webcam software, but with two differences: First, it told the imaging sensor to ignore the standby input; second, it ensured that the standby line was always held high to prevent the LED from ever illuminating. Result: a webcam with a hardwired LED indicator that nonetheless allowed image capture without the indicator LED ever illuminating."

Leo: So I have to tape everything over now.

Steve: We really do. I mean, that is, again, as I said, the original advice stands. You just, I mean, and why not? I mean, unless you're really using your camera all the time, just put a Post-it note over it. Jenny got freaked out because she got some junk, some malware on her laptop, and it was that one that - it was extortionware that said, oh, it alleged to be from the FBI. And because this was your first offense, you could send them money, and then they would let you off the hook.

Leo: Yeah. She's not running a Mac?

Steve: No, she's still - she's a Windows person. I have asked her about that because I think a Mac would make a lot of sense for her, too. But this also - so it showed some really distasteful images of child pornography which it said it found on...

Leo: What?

Steve: Oh, yeah.

Leo: That's a new thing. That's disgusting.

Steve: Yes, it alleged that it had found on her computer, and of course it didn't. But it also showed a picture of her, sitting in front of her laptop. So this thing had used her camera in order to snap a picture of her, to increase the credibility and horror factor of this. And so anyway, just putting a Post-it note, a little piece, just a little one-quarter by one-quarter, just snip off the sticky end of a Post-it note and just stick it over the hole. And it peels off easily, if you ever want to use the camera. But just leave it there, and every time you see it you can just sort of smile to yourself and say, yup, nobody's looking at me. Have to do it.

Leo: Wow.

Steve: So 32764, Leo.

Leo: 32764.

Steve: Yes. Now, I know that you are thinking, ah, that's the zip code of Deltona and Osteen, Florida.

Leo: Oh, of course.

Steve: And you would be correct. But it's not what we're talking...

Leo: There's more to it than that?

Steve: It turns out it can also be a port number because it's in the range between 0 and 65536, as actually are many zip codes. 32764 is interesting to me because, being Mr. Binary, we all know 32768 is an even power of 2. It is 2^15 is 32768. So this is four less than exactly midway in the port range. So it's like it's four below the exact centerline of ports 0 through 65535. A well-known hacker named Eloi Vanderbeken posted a note on GitHub when he discovered that his Linksys WAG200G wireless DSL gateway was, for no reason he knew, listening and accepting TCP connections on that port. There's no purpose for it, no reason for it. He then discovered that this was also true of Linksys, Netgear, Cisco, and other routers.

Now, this is important, listeners. When I first saw this, it looked like it was LAN only. It turns out it is not LAN only. There are at least five known routers who have this port exposed on the WAN interface of the router, meaning the public Internet: the Cisco WAP4410N-E, with a bunch of firmware models, 2 point something something somethings; the Linksys WAG120N; the Netgear DG834B; and the Netgear DGN2000, with a bunch of firmware models; and, finally, the OpenWAG200. There are many more routers that are exposing this mysterious port on the LAN side. I mean, like 30 or 40, a huge list. All you have to do to get more information is put in the zip code of Deltona and Osteen, Florida, into Google. You put in 32764. Just google "32764." The first link up currently is the link to the GitHub page. The second and third links are, not surprisingly, relating to real estate in Florida at that zip code.

So what you should do is simply use ShieldsUP! immediately, unless you know you don't have a problem. That's what ShieldsUP! was designed for. And I have a custom port probe as one of the many tests there. So just go to GRC.com, navigate through ShieldsUP!. You'll come to a dialogue with a bunch of buttons. Put "32764," and then click "probe my port." And actually you could do it with a URL. I've got a direct probe port URL. I think you just go GRC.com/portprobe=32764.

Leo: Oh, that's nice.

Steve: So you can just do it that way. And why don't you - can you try that, Leo? I mean...

Leo: Yeah, that's a good question.

Steve: I should have been a little more prepared here.

Leo: GRC.com/portprobe=...

Steve: 32764.

Leo: Yes, it does.

Steve: Yay, it does. There it is. And then...

Leo: Well, it gives you the database; right? I mean, does it do the probe?

Steve: And so then click "Probe THIS Port."

Leo: Ah.

Steve: And, [sound].

Leo: [Sound] Got it.

Steve: That's the sound.

Leo: That's the probe porting sound.

Steve: Oh, you do a /x/ and then portprobe=32764, and it'll do it.

Leo: All right.

Steve: And I got a stealth on my network. And hopefully that's what everyone gets. Stealth or at least closed is what you want. So GRC.com/x/portprobe=32764, and you can instantly check to make sure your router doesn't have that exposed publicly. That's the big concern. Now, so here's the strange thing. Oh, and you're stealth, too, Leo.

Leo: I am indeed, yeah.

Steve: So we don't know what this is for. There's been a conjecture that it relates to a manufacturer. And I forgot to write it down here. I don't see it written. There is some, like, manufacturer, like Simcom or something. Because what happens when you connect to this port, if you have that port, with, like, telnet or just your web browser even, you can, for example, put into your web browser http:// your gateway IP, which is often your private network, typically 192.168.0.1, or maybe it's .1.1. Anyway, so that IP, colon, 32764. That tells your browser to connect to port 32764 of your own router. And it'll spit out S-c-M-M, or that backwards, which is interestingly byte-swapped. It may put out M-M-c-S.

So we will be finding out soon because I'm sure many gifted, you know, hacking router firmware is now become an art. And so there's lots of guys who've put together router hacking toolkits where they can download the firmware; they can unzip it, unpack it, analyze it. I'm sure soon we will find out what's going on. This may be nothing but a benign listener that is an undocumented service that this company put in, I have no idea why. It's not exposed to the WAN, so it's not like they could scan the Internet and find all of their own routers.

I mean, the point is we don't know if you can do more with it than this yet. We hope it's not some evil server, and we of course hope that the NSA had nothing to do with causing this company to allocate this high, high port up in the boonies and have it listen. If it were really going to be stealth, it wouldn't spit out this string. So it really seems more like just sort of a wacky ID for the firmware that someone just happened to mention, or rather notice. I'm sure we'll see disassemblies of the firmware before long, and you know that we'll cover it here. And if any of our listeners finds a note of that, tweet it to me so that I'm sure I don't miss it, and we'll talk about that.

So in the meantime, if you do have that port open, exposed, and in ShieldsUP! the port probe will say open if it is, what you can - the suggested workaround is to manually put in a firewall rule to block that port for the WAN side. Having it on the LAN side, that's kind of creepy, too. We don't know what it does. We don't know what power it may have. It may accept commands and other things, and if you don't give it one, that's when it spits out the little ID string. We just don't know yet.

But putting firewall rules in and then of course retesting will allow you to immediately shut that down so that whatever it is, you don't want it. I would not call it a beneficial feature of the router that it does this. But it is, if you, again, google 32764, check out that GitHub posting because there is a growing list of known compromised routers. And, I mean, it's a big list. So whatever this company is that may have been the original progenitor of the firmware, they put a little cookie in there that we're not all happy about now. It certainly raises some questions.

Okay. We knew this was going to happen, and it's right on cue. We have three CryptoLocker follow-ons that have been identified. Initially there was something that was actually calling itself CryptoLocker 2. So the question raised was, well, is this an improvement of CryptoLocker, or is this actually something different? So it has now been analyzed. It's been a few weeks now. It's been analyzed in detail. Whereas CryptoLocker v1 uses 2048-bit RSA public key encryption for its unbreakable work, v2 claims to use 4096, but oddly actually uses only 1024. So that's strange.

Also, v1 was written in C++, whereas v2 is written in C#. Very different languages, even though they both start with C. Version 1 accepts payment in Bitcoin, MoneyPal, Ukash, and CashU; whereas v2, Bitcoin only. Version 1 doesn't encrypt images, videos, and music files; whereas v2 does. So that seems a little more personal attack. Version 1 uses AES, the Rijndael cipher; whereas v2 uses 3DES.

We talked about the file header a couple weeks ago where, after the file is encrypted, the pseudorandom key which was obtained from the OS and then encrypted using the private key or public key - no, I guess it would be the private key obtained from the remote server. That's appended to the front of the file to create a new header. That's v1. Version 2 does something different. It creates, for every file it encrypts, it creates that same filename.k key file. So it makes a whole bunch of more files containing the decryption keys required, but those keys are encrypted so that you still need to pay somebody. And then also v2 contains a bunch of weird, fake, like, software activators and cracks for commercial software, e.g., an activator for Windows 7 and 8; an activator for Office 2013; one for Team Viewer; something for Adobe's Photoshop; and even ESET's Smart Security software. And ESET performed this analysis.

So that sort of says, okay, that they intend to, like, salt the Internet with fake Windows 7 activators - cracks, essentially, for Windows - and get people to download them and run them in order to get themselves infected with this. Which was nowhere in v1. So the conclusion is we have a completely independently authored, but lookalike, because, I mean, that was what caused the confusion is that the dialogue boxes are very much the same. So the v2 people, the CryptoLocker 2, completely implemented their own from scratch, yet emulated the look of the original CryptoLocker. So that's one of the first, that's one of the three new ones.

There's also been found in some discussion forums discussion of something called in some places PrisonLocker, and elsewhere PowerLocker. And it apparently is not out yet. The concern is that the author whose forum postings have been quoted says he's intending to sell this as, like, a ready-to-go kit for $100, which is a little confusing because we've seen the numbers that CryptoLocker's evil people produced using this. And, I mean, it was in the hundreds of thousands of dollars. So there's also a comment where the guy says, because I read all of this forum stuff to get some sense for who he was, that this is his first C code.

Leo: Wow.

Steve: And there is a lot of, like, okay, in Windows, how do I make a window stay on top, and how do I prevent them from switching away from the window? So there's also mention of MASM elsewhere. So it sounds like he's a lower-level coder.

Leo: Assembly language programmer.

Steve: Assembly language coder, yeah, I mean, this is - and to do most of this you certainly, well, we know I would use assembler, but I wouldn't ever write a program like this. But it sounds like that's what he's doing. And now he's, like, learning the GUI stuff. Oh, in fact, he said this is his first C program, and he farmed out the production of the graphical user interface to someone else, and he's going to give him a piece of the action that this thing generates. So that's apparently really happening.

Now, what's really weird is that - and this may never get off the ground. As far as we know, it hasn't yet. But if we're to take the research that's been done from his postings on face value, his ICQ handle, his long string, has leaked. And he appears to be a 23-year-old Pisces named David Klukinski. So, David...

Leo: What's your sign, David?

Steve: Yeah, you're a Pisces. Good luck to you. Yeah, he was born on March 3rd. So if we've already figured out who you are, maybe you ought to abort this whole effort before you really get yourself into deep trouble.

And then, completely independently, No. 3 was reported by TheRegister.co.uk. And this is something called Locker, just Locker. It has been found already in the wild, so it exists, written in Delphi, which we remember is Borland's sort of Pascal outgrowth language. And I think that went - did it go open source and public? I think maybe it did.

Leo: Turbo Pascal?

Steve: Well, Delphi.

Leo: Delphi, oh. I don't know. You know who would know? Paul Thurrott.

Steve: Yeah, he would. Anyway, so...

Leo: Yeah. I think it's ColdFusion now, is what I think.

Steve: Okay. The Register reported that it was written in Delphi using the TurboPower LockBox crypto library to encrypt files in AES-CTR mode. But apparently it wasn't done very well, and it is possible, without payment, for smart engineers to decrypt the files. So I imagine that'll get fixed, now that The Register's reported it.

So unfortunately, this was inevitable. Essentially we've entered a new era. And I don't know why we're going to go back because this could have been done 10 years ago. And it's been nice that we had 10 years without it being done. But with the money that CryptoLocker made, and we already said this on the podcast months ago, you know, get ready, folks, this is coming. Because why wouldn't other malware authors decide, hey. Oh, look, here's a crypto library. Oh, look, here's crypto open source. I mean, crypto is done. Unbreakable crypto is freely available in every language now. And so it was just a matter of time before it would get leveraged in this fashion. And that time has arrived, unfortunately.

Leo: Yeah, wow.

Steve: Now, also in the news was a massive leak, and embarrassing for Snapchat, of 4.6 million users' usernames and phone numbers of their mobile devices. Snapchat has not performed admirably, unfortunately, in this. They were warned back last June or July, so about five months, at least, ago about this, and they did nothing. They didn't respond to the guys who found it. And I have to mention, the guys who found it, unfortunately, have decided to call themselves Gibson Security.

Leo: Now, yeah. Well, I mean, I don't know. They're not naming themselves that for you.

Steve: No. And I know in fact now for sure that it's after "hacking the Gibson," that phrase from the classic cult movie "Hackers" with Angelina Jolie.

Leo: But it is confusing.

Steve: Well, not only that, Leo. I was bombarded by the press on Monday, all wanting to know more. And so I...

Leo: They googled "security" and "Gibson," and they found you, yeah.

Steve: Yes, yes, yes. And, I mean, so these guys, it's GibsonSec.org, G-i-b-s-o-n-S-e-c dot org. And many Twitter followers of mine were similarly confused because they were saying, "Bravo, posting the API." And it's like...

Leo: Oh, geez.

Steve: ...whoa, whoa, whoa, whoa. That wasn't me, folks. So no relationship whatsoever. They're in Australia. But I have to say, having now studied their postings, they seem like neat guys. They are asking for donations, calling themselves, like, starving students or something. But I just - I like their style. I like the way they write, the way they think. So they're not part of GRC in any way, but they seem like good folks.

So, okay. Snapchat. What Snapchat has done [exasperated sound], I mean, it is just - it is so - whoever did this should just be embarrassed because they were entirely relying on obfuscation, on no one looking closely. And we know how well that works. So these guys, the Gibson Security folks in Australia, completely reverse-engineered the Snapchat API and laid it all out. Now, and this is only after they waited five months after telling Snapchat, you know, this is really bad. This is really dumb. And there's all kinds of things, bad things about this. I mean, it's hard to even enumerate them. And Snapchat blew them off, didn't respond, changed nothing.

And so then these guys just said, okay, here's the API. And a different party, not the Gibson Security guys, a different party leveraged the information that the Gibson Security folks published to produce this 4.6 million user database. And it's trivial to do. I mean, with the information that's now publicly available, not a problem. So to give you a sense, our listeners are savvy enough, and anyone who's followed the podcast for long will be able to follow this. This gives you a sense for how poorly implemented their security is. There are some magic numbers that cannot be well hidden. There's a secret, a so-called secret that never changes: iEk21fuwZ blah blah blah. It's a pseudorandom string that looks like it's probably base64 converted. And it's just there. And then there's a so-called "pattern" of zeroes and ones: 0001110111101111000 and so forth, just sounds like gibberish. And all it is, is just a random string of zeroes and ones.

So to authenticate, what they call "authentication," is you first log into the Snapchat server, which returns a session token. So you just - you say, hey, give me a token, and the server gives you a token. Now, any API request you made needs to be authenticated using that token. Except that authentication means that you take the time of day, and you hash it with the token, and you convert that to hex. Okay? That's hash 1. Then you take that secret that never changes, and you hash that with the token, and you convert that to hex. And now that's hash 2. Then you use that pattern of ones and zeroes. That directs you from whether you select the character from hash 1 or hash 2 in building a new string. And that's how you authenticate. I mean, it's like, what?

Leo: Well, somebody said that just the whole notion of Find Friends is inherently problematic. Right?

Steve: True. Yes. And I wanted to mention that I haven't looked closely at whether it's possible to make this secure. Because exactly as you said and has been said, the idea that, I mean, the reason there is an API in there, presumably you allow Snapchat to have access to your phone book, your contacts. And so it runs through your contacts, looking. And essentially, through this API, it submits every phone number in your contacts list and learns from the server whether that is a Snapchat user and, if so, returns their username or allows you to connect to them and find them.

So the problem is there is no authentication, no effective authentication, no rate limiting at all. And this is what the attackers used in order to launch this attach, is essentially they said, we'd like to log in, please, and the Snapchat server said, yeah, here you go. And then they said, okay, now what about 0000000000? No. Nobody by that phone number. How about 001? How about 002? How about 00 - turns out you can do easily 5,000 a minute, and that's without running parallel threads or high bandwidth or anything. I mean, so basically Snapchat's entire, I mean, critical aspects of their database is completely wide open.

Leo: Yeah. By API, which is great.

Steve: Yes. By an API that's now fully documented. And, I mean, for example, I just - there's so many things that they could have done in order to make this stronger. I mean, maybe it's, as you said, Leo, not possible to really make it stronger. But you could certainly detect this kind of behavior and then disavow that token, and maybe remember that IP asked for that token, I mean, there are all kinds of things that...

Leo: And they are going to rate limit going forward.

Steve: I hope they do.

Leo: No, they said they would.

Steve: Oh, good.

Leo: But what they're not doing is changing the API or attempting to make it more secure. Their response to this is, well, you could turn the Find My Friends feature off, and then you won't be revealed; and we're going to rate limit. So even if they do get some, they won't get...

Steve: So maybe you could turn the feature that allows you to be found...

Leo: Yeah, that's probably it. Yeah, yeah.

Steve: Okay. That would make sense.

Leo: In other words, take your number out of their database.

Steve: Right, right. Or just...

Leo: By default it will be in there.

Steve: Yeah.

Leo: Hmm. It's an interesting conundrum. Their position, they didn't apologize, which is what most people got upset - I don't think that that's - that's neither here nor there.

Steve: Well, I did like the comment that said they were too busy turning down offers of acquisition from Google and Facebook.

Leo: I think that what happens - this happens a lot with programmers. They go - the same thing happened with Path - "Well, gosh, it's obvious, if you have a Find My Friends feature, that information will be revealed. So you should have known that. What do you want us to do?" So, I mean, I guess allowing yourself to opt out, allowing opt-outs, although not on by default. And then the real problem is the teenagers - I should have asked my son. He was just here. The teenagers who use Snapchat have no idea.

Steve: No. And the point was raised also that what you obtain in return for passing it a candidate phone number is a username, and that many people reuse the same username, even if they're not using the same password. Maybe we're beyond that, but not so much. But they use the same username all over the place. So this allows you to tie a phone number obtained through Snapchat to any other reuse of that username on the Internet, if it's not a common username. And of course often it's not because you get told, oh, that username is already in use. So it's like, oh, okay, thanks for filtering that for us.

Leo: Yup, yup.

Steve: Yeah. So I wanted to give our listeners a heads-up that the name McAfee Security will be falling into disuse...

Leo: Really.

Steve: ...over the course of the next year.

Leo: They don't like being associated with that guy.

Steve: Yeah, Big John finally took it too far. And, yeah. So it's going to be relabeled Intel Security. So when you begin seeing Intel Security, you can think, uh-huh, McAfee. Although they're keeping the red shield M. They're not going to change that because I guess they feel that's too recognizable. I'm wondering whether Intel Security is going to try to download when I update my Adobe Flash or my Adobe Reader and so forth. It's like, whoa, here, wouldn't you like a free McAfee security scan? No, thank you, I wouldn't.

Leo: McAfee. A name that will live in infamy.

Steve: Goodbye, John, yeah.

Leo: Intel owns them. So I was surprised that they kept the name for as long as they did, frankly.

Steve: Yeah, well, I mean, once upon a time it was a major brand, and they were certainly - they bought it for more than $7 billion.

Leo: What?

Steve: 7.68 or something billion dollars they paid.

Leo: What?

Steve: Yeah.

Leo: Man. Do you ever feel like we should have, we could have - if we'd just been more prescient, you could have written an antivirus.

Steve: No. Believe me, 23 people was more than I could handle. And you're about at your limit, too, Leo, so...

Leo: Oh, you'd better believe it, yeah. That's why we're firing people left and right.

We just - we can't handle it.

Steve: I've never been happier than when I just have Greg and Sue. It's like, okay, that's about the right number.

Leo: And anybody who is on the, as we are, court side during all of this stuff going back to the '90s, watching the Internet explode, feels like sometimes, I think at some point, golly, maybe I should have done an app.

Steve: Although I have to say, Jenny and I saw "The Wolf of Wall Street" last night.

Leo: Ooh. I haven't seen it yet. I'm not sure I want to see it.

Steve: Well, I came away, I mean, it was fun and funny and well written. It was long. Scorsese and Leo, apparently, Leonardo DiCaprio...

Leo: Yeah, don't call him Leo.

Steve: No, [Scorsese and] Leonardo have a great relationship because, I mean, basically this was the DiCaprio onscreen movie. It was really all about Leo and his acting. But - I'm sorry, Leonardo. The point is that apparently some people are thinking, wow, that would have been kind of nice.

Leo: No.

Steve: And I have to say, I was looking at it thinking, oh, what a mess.

Leo: No. And the guy was a con man and, I mean, I don't know. Yeah. I might go see it. I don't know.

Steve: I don't want to have a life like that.

Leo: His daughter, the real-life guy's daughter, wrote a scathing editorial saying, you know, don't downplay the harm this fellow did, including to his family and me.

Steve: Yeah. So I just thought I would - we talked about the wrongheaded porn blocking decision that was made in the U.K. many months ago. And Boy Genius Report (BGR) had a neat story that wrote: "As was predicted by just about everyone, the United Kingdom's initiative to get U.K. ISPs to add default pornography filters has been a complete and utter disaster so far."

Leo: Of course.

Steve: Yeah. I mean - okay. I'll save that for a second. "Not only have the filters been blocking access to pornographic content, but they've also been blocking access to health information websites and charity websites, among other unintended targets." Again, of course. But, "There is some justice to come out of all this, however: The Independent reports that the filters have also blocked access to the website of Conservative MP Claire Perry, who has been one of the leading crusaders for implementing porn filters in the U.K."

Leo: That's ironic.

Steve: Uh-huh. "It seems that Perry's website contained information on her assorted anti-pornography campaigns, which was apparently enough to get her site caught in the porn filter dragnet."

Leo: Wow. Wow.

Steve: And it's like, we know this can't work. People keep trying it, and it keeps failing. Computers have enough trouble figuring out whether someone is human or not. I mean, that seems to be, you know, the CAPTCHA problem is an insurmountable problem. And even the Supreme Court famously, in 1964, Supreme Court Justice Potter Stewart failed to define what pornography was, saying famously, "Well, I can't define it, but I know it when I see it." And unfortunately, that's not a rule you can put into the firewall.

Leo: Right. If you see porn, let us know.

Steve: Yeah. If some comes by, well, we'll apologize and turn it off.

Leo: My sense is this was all politics. What a surprise.

Steve: Yeah. I just saw a nice note. There's a battle waging, and I don't know how it's going to turn out, maybe it'll be all of the above, between Mozilla's asm.js - which actually is the solution I favor, even favoring it over native code, which is Google's approach.

Google has this thing called Native Client, which is an open source technology to allow web applications to be built to seamlessly execute native compiled code inside the browser. It's like, uh, okay. If you contain it well enough, if you VM it so that it can't misbehave, then that's a way to get essentially your browser to, like a website - the point was you could go to a website, and it would download an app, I mean a full-on native compiled app, into your browser, and run it. And so this is Google's future.

Mozilla did the other thing, which I really think is so cool, and we've discussed it before, asm.js. They defined a strict subset of Java, I'm sorry, of JavaScript, I will be careful, JavaScript, which is otherwise very hostile to high-speed execution. The nature of JavaScript is that it's a dynamic language. Which means, for example, you don't have to declare when you've stopped using memory. You just define arrays, and it's up to the language itself, the guts, to figure out, oh, look, he's not referencing that array anywhere, so you decrement the reference count. And when it goes to zero, then the garbage collector comes along and collects the garbage. So that's difficult to speed up.

What asm.js does is define a strict subset of JavaScript which doesn't have any of those tricks in it, which means it can be compiled to run very fast. And what they did over the holidays was took it from running 2x slower than native code - which already is very fast. They've got the Unreal Engine running in it, and running Unreal 3 in their browser. So, I mean, it is screaming. So they took it from going two times slower to only 1.5 times slower than native code. And of course when it gets down to one, then it's the same speed as native code, yet cross-platform, cross-chip, essentially, because this is a subset of JavaScript. If you don't have it running on Mozilla, it'll still run because it's just JavaScript. If you do have it running under Firefox, it goes like a bat out of hell. So anyway, I like that approach. Maybe we'll end up with both of them. But I just think - I commend Mozilla for what they're doing. I just really like that approach.

Leo: Yeah.

Steve: I have a bunch of miscellaneous things I want to talk about. But I did want to share a one-day-after-Christmas really nice note from a listener of ours named Jonathan Bailey, who's in New Orleans. And the subject was, not surprisingly, "SpinRite Testimonial." But a neat story, and it's not too long. He said: "I was at a friend's house on Christmas Day when she told us the hard drive on her laptop wasn't working. It wouldn't boot, and even booting it off of a Live CD didn't give access to the data on it." And I'm sort of impressed. Either this person whose house he was at knew about Live CD, or maybe he tried that first. But it doesn't sound like it. Sounds like they'd already tried that, or someone did. But that wouldn't work.

So he said: "While the laptop was old, and she didn't care that much about it, it did have a lot of important stuff, most notable the photos of her son's wedding a few years ago, and there were no known complete backups. I took the laptop home and, using my receipt, downloaded a fresh copy of SpinRite. Immediately, on the first sector, it seemed to freeze" - that is, SpinRite seemed to freeze - "and it spent so long at 0% that I considered aborting it. However, being a listener of Security Now!, I knew to be patient and put my faith in the SpinRite gods, so I went to bed with it running. I awoke to the green 'SpinRite Complete' screen. I took out the CD, rebooted, and, huzzah! The laptop booted right into Windows. It was a true day-after-Christmas miracle. Thank you so much for your great product. After four years of ownership, I finally get to share my 'SpinRite saved me' story." And Jonathan, thanks for sharing that. That I appreciate.

Leo: Yay.

Steve: So, miscellaneous loose ends. Just we're right up here at 3:00 o'clock, so I think it's just about right. I just had to mention, BlackBerry has sued the Typo Keyboard people over their BlackBerry-like keyboard. We mentioned it on the show...

Leo: Oh, yeah, what's his name's keyboard.

Steve: Yes.

Leo: You were all excited about it.

Steve: I am. In fact, even more so because NBC News this morning had it on. A buddy of mine texted me because we both have been complaining about typos on our touchscreen iPhones. And apparently NBC News said that it was an excellent keyboard, but they could not say any more about it due to the BlackBerry lawsuit, which is the biggest bunch of nonsense I've ever heard. But maybe they don't know any better. I mean, there's no injunction that has been filed.

Leo: I don't watch mainstream coverage of technology anymore. It's just painful.

Steve: No, no. But the good news is somebody who used it apparently loves it. And I can't wait. It was mailed on the 31st, I think.

Leo: Oh, you actually are getting one.

Steve: Oh, are you kidding me? Oh, Leo.

Leo: So you ordered it before the lawsuit, so you'll at least get to keep it.

Steve: Yes. Absolutely. And I'm...

Leo: We did note that it looked very much like the domed key caps of a BlackBerry.

Steve: Well, and BlackBerry has a raft of patents on the keyboard.

Leo: But it doesn't seem like they should be able to prevent physical keyboards attached to a phone.

Steve: I agree. I agree. And I imagine, now, there are design patents. And this looks like a true rip-off. I mean, I have to say that, now that mine's already in the mail. It looks like a true rip-off, and I couldn't be more happy.

Leo: [Laughing] Yeah, the closer it is to the BlackBerry keyboard, the happier you are.

Steve: The better I'm going to like it, exactly. Certainly they could change that back into something that isn't really a clone of a BlackBerry. And one wonders about patenting a design. It's like not - who knows. That's another whole issue. I don't want to get into it. But I am excited. I may have a report. I imagine by this time next week I will have been using it for a few days. So, I mean, it just - oh, there it is, yeah.

Leo: Yeah. This is USA Today. It does look like a BlackBerry keyboard, doesn't it.

Steve: Oh, my god. Oh, yes. Ooh, baby.

Leo: Wow. Now I wish I'd ordered one. It's called the Typo Keyboard. I wonder if Ryan Seacrest was there to show it off.

Steve: You can still order it, Leo. They're accepting orders, and I think they're shipping and just, I mean, there's no injunction. So as long as they get them out the door - that's TypoKeyboard.com. And it looks great. The other thing I'll remind you of is that oftentimes when the keyboard comes out onto the screen, you lose half your screen real estate. And so while you lose any...

Leo: I agree. I don't like that part.

Steve: No.

Leo: But he does say - this is Jefferson Graham writing for USA Today - that if you've gotten used to typing on the screen of the Apple, it's kind of difficult to go back.

Steve: Yeah, baby, bring it on. I will be giving up my fingerprint. You lose that because there is a Home button in the lower right.

Leo: Oh, right, yeah.

Steve: The thumbprint ability disappears. But, oh, I'll have a report next week.

Leo: Good. Good, look forward to it.

Steve: Also, for all people who listen to this in time, the new CBS show "Intelligence" premieres tonight. Tonight is the night, January 7th on CBS at 9:00 p.m. Don't know anything about it. I'm not recommending it. I'm just letting people know who think they may like it. This is the guy that gets a chip implanted in his brain that ties him into the global information networks, and we'll go from there. So who knows. And if you missed it on Tuesday, and you can't find it on any of your get-them-back deals, it re-airs this Friday. So they are airing it twice for those - after a buzz is created, hopefully tonight if it's any good, then people will go, oh, shoot, I missed it. But you can watch it on Friday.

Also I mentioned a sci-fi reading guide. I prepared this initially for - actually for Bob up in Canada, whom you have met, because I sent him one of my old Kindles where I had all of my books that I have read since Bob departed for parts north. And I built a beautiful PDF where I laid everything out. And I realized, oh, this is the "Steve's Sci-Fi Reading Guide" that everybody has been wanting for so long. So there's a bit.ly link to it: bit.ly/sgscifi, all lowercase, because bit.ly is case sensitive, bit.ly/sgscifi. That link expands to a PDF.

And I got a lot of Twitter followers, because I tweeted this a couple weeks ago, saying that they were chuckling because they were getting a PDF from me, as if that was unsafe. And it's like, okay, folks, wait a minute. PDFs from me are not malicious. PDFs themselves are not malicious. It's not like PDF is a problem. It's that, like an executable, you download GRC's EXEs night and day because you know they're not malicious. But you're very careful when you download some random foreign executable on a download site because it might very well be malicious. Similarly, PDFs can be dangerous. But, sure, I love PDFs. They're fabulous. Leo, you're looking at one that I just made for you. So...

Leo: I do accept them from you. But I think part of the issue is I always say don't accept attachments, even from people you know, because it could be posing as you. But if you expect a PDF from Steve, and it doesn't have the appearance of an automatically generated email, I think it's probably all right.

Steve: Right. As I mentioned to you when we were up, well, earlier, was it this week? No. I don't know what week it is.

Leo: I don't know where we are or what we're doing. It was a week ago, last Tuesday.

Steve: I had started to reread the Honor Harrington series. I finished Book 2, so I've just finished rereading, just they're fresh now, books 1 and 2. So I wanted to mention to everybody, something is happening. We're going to get a movie or a series of movies or maybe a TV series. I'm now seeing different reports. It might have evolved into a TV series, or that might be older news than the movies. We're going to be getting movies. You absolutely must, if you ever plan on watching the movie, unless you really, really hate reading, you have to read these first.

I mean, I reread, rerode, reread - slow down, Steve - reread "Ender's Game" the book before the movie came out because I knew the book was going to be so much better. And oh, my god, it was fabulously better than the movie, which really was not that good. That goes squared for Honor Harrington. These books are so rich, there's no way - now we've got a really loud thing going on. These books are so rich, there's no way the movie could do them justice. And so the reason I'm mentioning this is that Amazon now has them both free. iBooks from Apple has books 1 and 2 both free. And the Baen, B-a-e-n, website has both books 1 and 2 free. So no excuse for not grabbing them. And in fact I may be switching over to iBooks, Leo, because I just discovered, to my...

Leo: What?

Steve: Yes. I discovered to my infinite joy that the version, the new version of iBooks, 3.0, that came out late last year, allows continuous scrolling for the first time. No more of this ridiculous page turning. You can just put your thumb there and smoothly scroll up. And especially for reading iBooks on a screen as small as the phone. That just seems so much better than that page-turn, pretend-to-be-a-book baloney. You can't, you'll never be able to do this - well, not never, never is a long time - on eInk. Right now the technology of eInk is hostile to a page scroll. But actually I got a second mini because I want to experiment with switching over to reading on the mini because of this update to iBooks which would allow me to scroll, like, continuously.

Leo: And why do you want that?

Steve: Want what?

Leo: Continuous scroll? I mean, because, okay, so I'm imagining you. You're on your Stairmaster or treadmill, whatever it is.

Steve: Oh, no, no, I mean, I only do a little bit of reading there. So that would still be page at a time.

Leo: You don't care about it there. Just like in real life when you're reading.

Steve: Yeah. I just love the idea of being able to smoothly scroll through the book. I just think that's going to be the right way.

Leo: Okay. I'll be curious. Because it feels like I would lose my place easily doing that.

Steve: I know what you mean, when you're not on a discrete page.

Leo: Yeah.

Steve: I know what you mean. And of course Apple and iCloud are really good about doing cross-device synchronization now.

Leo: Is somebody disassembling some hardware in your office?

Steve: No.

Leo: What's that sound?

Steve: It's the dumpsters.

Leo: It's outside? Sounds like it's right next to you.

Steve: Unfortunately, this may be a side effect of us...

Leo: Oh, 1:00 in the afternoon.

Steve: Yes, exactly, because this goes on every afternoon around this time.

Leo: Every, well, hey, at least they empty the trash daily.

Steve: They're uniform, yes. And I posted and got some interesting feedback about my assembly language. We know that I program in assembler. I'm now writing SQRL in assembler. And I thought it would be interesting for people to see what that looks like. And so there is an image for which I have a bit.ly link, bit.ly/, and for some reason I did mixed case. I'm sorry about that. I don't know why. Capital S, lowercase q-r-l, capital S, lowercase i-g-n. So it's SqrlSign with the two S's capitalized, S-q-r-l-S-i-g-n. If anyone's curious, that will give you - your browser will show you what my assembly language actually does look like for the code that I'm writing for SQRL.

And speaking of that, all the crypto libraries are up and running and linked into my assembly library. We're currently settling on an export and storage, an encrypted export and host storage format, the details of that, and also nailing down the details of the way we use the Scrypt Password-Based Key Derivation Function (PBKDF). But we're down to the ending details, and I'm writing code, so I'm excited. I hope to have something here before long, get that out to the world, and I'm right back to working on SpinRite 6.1.

Leo: You are. Awesome.

Steve: Yup.

Leo: All right. Steve, we're going to move on to the rest of the lineup on our new day, Tuesdays.

Steve: Yes. And so next week I'm going to have...

Leo: Garbage day.

Steve: ...an in-depth analysis of what exactly it is the NSA has up their sleeves. I'm going to study every one of those slides and pull them together into a comprehensive take on what the NSA ANT project is, and fundamentally what they can do.

Leo: Okay, look forward to that, the in-depth look at ANT next week on the show. Steve Gibson is at GRC.com. That's where his website is. That's where you'll find SpinRite, the world's best hard drive maintenance and recovery utility; all the freebies Steve gives to the world, like ShieldsUP!; lots of software information about passwords; information about health and dieting. It's not his business, it's just a sideline. You can tweet him at @SGgrc. That's his Twitter handle, @SGgrc. If you have a question - I guess we're not doing feedback next week. But if you do have a question for a future feedback episode, that would be GRC.com/feedback. Do not email him.

Steve: Yeah. We did a bunch of Q&As in a row, and we caught up a little bit. So we'll go back to Q&A in two weeks, but I really want to do an in-depth look at the NSA ANT.

Leo: Good. Thank you, Steve. Remember Tuesdays, 1:00 p.m. Pacific, 4:00 p.m. Eastern time, 21:00 UTC. That's the new time for Security Now!. We'll see you back here next week live. If you can't watch live, on-demand audio and video available at our site, TWiT.tv/SN for Security Now!. Steve has 16Kb versions, plus Elaine Farris - and Elaine was in the chatroom saying, "Thank god you're back, I was getting bored." Elaine Farris's transcripts, so you can read along as you listen, are at his website, GRC.com. Have a great - yes.

Steve: Yes, and for those of you who have any additional time in your week, track down those New Year's Eve hours that Leo's group are posting. There's a lot of fun there. I mean, it was a blast.

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

Steve: Thanks, Leo.