"Monkey" Was 26th!

Description: The past week was so jam-packed with so much fun and interesting security news that we had a hard time just fitting it all in. So this week's podcast is news, news, news!

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-429.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-429-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. Such a big security week, he's just going to talk about security news, everything from the big Adobe breach to the idea that viruses could leap through the air. And a couple of engineers at Google respond to NSA spying allegations with a profanity-laced post. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now!, with Steve Gibson, Episode 429, recorded November 6th, 2013: "Monkey" was 26th.

It's time for Security Now!, the show that protects you, your privacy, and your loved ones online. And it does all that thanks to this man right here, the Explainer in Chief, Mr. Steven "Tiberius" Gibson. He is the guy...

Steve Gibson: If you keep saying that, it's going to work its way into the Wikipedia page. That's what's going to...

Leo: It's my goal. Hey, if Moxie Marlinspike can be named Moxie Marlinspike, you can be Steve "Tiberius" Gibson.

Steve: Yup, and we take him very seriously...

Leo: Heck, yes.

Steve: ...because he knows what he's talking about.

Leo: He is in fact going to be the subject of one of your screeds today. We have a lot of tech news, so much so that we maybe won't get to questions. Is that right?

Steve: Yeah. So much happened this week. And really fun, interesting stuff. Lots, I mean, I was busy tweeting things. So my Twitter feed is full of links that people may want to check. And I was actually tweeting a bunch this morning as I was finding things that I wanted to talk about. And just I was sort of - my plan was originally that this would be another Q&A because we'd been skipping so many Q&As, just because there was too much happening. We weren't able to get to them. So I thought, let's do a little makeup Q&A. But too much happened again. So it got pushed off.

Leo: That's all right. We'll get to questions, you know, someday.

Steve: I couldn't decide whether to call this "Monkey Was 26th" or "256 Bits Is the New Black." So we've got...

Leo: Boy, those are both intriguing.

Steve: Yeah. We've got a new zero-day Windows Office vulnerability. We've got an update on the TrueCrypt auditing project. Ladar Levison wants to raise money. Viruses are leaving the network and leaping across the room.

Leo: [Laughing] I really want to know your take on that one, by the way.

Steve: An escalation of the CryptoLocker battle. A major new update to LastPass. Sync news from BitTorrent. Google versus the NSA. My reactions to the iPad Air, "Ender's Game," and my discovery of the best iPhone case after trying 50 of them.

Leo: Wow. Wow.

Steve: Yeah. And maybe we'll have time for a sponsorship or two. I'm not really sure, though. You'd better get one in right now, Leo, otherwise it's just - there's not going to be any hope.

Leo: By the way, it has made it to your Wikipedia page. You are now Steve Tiberius Maury Gibson. That's not how you spell "Tiberius," kids. But other than that...

Steve: Boy, those editors are fast.

Leo: [Laughing] It's i-u-s.

Steve: SQRL has a Wikipedia page, by the way.

Leo: SQRL? Well, of course it does. I would expect that, yeah. I absolutely expect it. Our show today, we'll get to all of that and more in just a bit, but our show today brought to you by our friends...

Steve: That was a summary, by the way.

Leo: I know. You did a nice job. I thought that was - this is a new feature of the show. There's so much in it, it's like a Victorian novel. In the old days of Victorian novels they loved lists. Remember? You would have, at the beginning of a Victorian novel, a chapter. It would say - a chapter heading would say something like "In which our hero discusses...," you know, or "takes on the champion boxer of...," and it goes on and on and on. The Victorians loved that stuff.

Steve: I worry about sometimes science fiction books where you open up the book, back when you could open up a book - actually, eBooks do it, too - and they show you a fabulously detailed map of the universe with all kinds of little points noted. And you're thinking, okay, wait. Will there be a test on this? Do I have to memorize this? What am I supposed to do with this map?

Leo: Memorize the universe.

Steve: Shows random places that the author made up.

Leo: Steven Tiberius - I didn't know your middle name was Maury.

Steve: Yeah. My dad was Maurice, and he never liked that. He just - and in fact I remember him telling me once that he, when he was choosing this name for me when I was in the process of being born, he wanted to deliberately choose a name that I would be proud of, that I would like. And I like Steve. I think it's, you know, it's like Mark or Paul or...

Leo: Steve's a great - is it Steven?

Steve: S-t-e-v-e-n, yes.

Leo: Not p-h.

Steve: Not p-h.

Leo: Yeah. So I could call you Steven Maury Gibson, and you'd feel like you were in deep trouble.

Steve: At the AI Lab at Stanford, where I spent a couple years, we used our initials as our logins. And so they were calling me "Smog."

Leo: Oh, I love it.

Steve: I don't really want to be Smog.

Leo: I hope they spelled it, not S-m-o-g, but in the true geek fashion, S-m-a-u-g.

Steve: No, no, this, well, no.

Leo: You know why. Smaug is the dragon that hoards all that gold in "The Hobbit" that they go out and steal from.

Steve: Yeah, that's a real pissed-off dragon at the moment.

Leo: Yes.

Steve: Where we left him, he was not happy.

Leo: Not happy. And I've seen the trailers for this Christmas. I'm very excited.

Steve: I have, too, and he looks like he's getting more annoyed.

Leo: So I'm going to call you S-m-a-u-g, Smaug. I love it.

Steve: Okay. I'm getting myself in more trouble here.

Leo: All right. Let's get to the matter at hand. There's lots to talk about.

Steve: Tons. So first off, standard business. Microsoft issued a report a couple days ago that they had this sort of an emergency out-of-band report. They don't have a patch for this yet. But they were alerting people who subscribe to their various security lists that they have found targeted attacks using a deliberately malformed TIFF image file. You remember TIFF, Tagged Image File Format.

Leo: Still quite widely used by Photoshop users and others.

Steve: Yup. It was an early format and...

Leo: It has the value of being lossless, if it's got compression at all, lossless compression.

Steve: Yup. So, okay. The good news is the latest version of Office - this affects Windows Office users. The latest version of Office, Office 2013, is not affected anywhere. But Office 2003 and 2007, which is not the next most recent because that would be Office 2010, but '03 and '07 are affected across all platforms. All versions of Windows have this TIFF image file format problem. Office 2010 only has the problem on XP and Server 2003. So specifically not Windows 7 or 8 or Server 2008. I don't know who would be using Office on a server platform, but you never know.

So the exploit bypasses Microsoft's exploitation mitigations, specifically DEP that we've talked about, Data Execution Prevention, which is where you mark regions of memory as being executable or not. So, for example, the stack would typically not have execution prevention. Well, this avoids that problem. And also Address Space Layout Randomization, ASLR, where code jumps to known locations to pick up little bits of existing code and is able to knit together its devious needs that way. And this bypasses those protections, too. So it's a problem.

Microsoft has a quick fix. I created one of my little bit.ly shortcuts called "notiff." So bit.ly/notiff, all lowercase. That'll quickly take you to Microsoft's page, where all they've done essentially is they've - turns out they've added a line in the registry to disable the TIFF codec, so it kills rendering of TIFF files.

Leo: It also kills your ability to look at TIFFs.

Steve: Well, but I don't know that that's going to really annoy anybody because, as you said, it's been around for a long time.

Leo: No, it's still widely used, absolutely.

Steve: Oh. Okay.

Leo: Oh, no, no, no. That's not insignificant.

Steve: Yes. So it will kill your ability to see TIFF files. So right now these are targeted attacks, mostly in Europe and Asia, not even in the U.S. But Microsoft knows how these things go, and now the word is out. So if you don't have Office, you have nothing to worry about. If you've got Office 2013 you have nothing to worry about. If you've got Office 2010, but not XP or 2003, again, nothing to worry about. But you may, if you fall within that class where you - and people are receiving email or browsing to websites that

display a TIFF file. Just receiving the email with a TIFF embedded in it will display it and take over your computer. Don't even have to click on it or anything. So if you fit that profile, it may be worth disabling TIFF format file images, unless you know you need them. And this little bit.ly shortcut will do that for you. All it does is add a line to the registry saying turn off that codec, please.

Leo: Hmm. That's a pretty weak fix. I'm sure they'll have a patch next Tuesday.

Steve: Oh, yeah, yeah. Absolutely. Okay. I labeled this "Adobe Face Plant" because, boy, did they...

Leo: They scared the hell out of me. I got the email, like last week maybe. And they offer you a year's free security check. I have a credit card on file with them. And they forced me to reset.

Steve: Well, in fact your email is in the list.

Leo: Oh, it is? You checked?

Steve: Actually, people tweeted the fact to me because I sent them news, because I got a note from Joe Siegrist at LastPass that he had just added a new LastPass service. So anyone who wants to check and go to LastPass.com/adobe, which - and they've done this before. We've covered it before. He's taken the entire database and made it instantly email address searchable because one of the things that was leaked was the password database, which contains everybody's email address in the clear.

Now, what's really bad about this is, I mean, this is every best practice ignored. So when Adobe first announced the problem, they said, well, don't worry because the passwords were "encrypted." And people who knew, like, best practices, thought, well, that's just probably some PR flack who didn't understand that what they really meant was "hashed." No, what they really meant was encrypted. We're guessing based on the evidence because the block length of the encryption is 64 bits. And so we're thinking, okay, well, maybe that's a DES, that is the encryption that DES uses with a key length of 56 bits. But it's probably 3DES because that's readily available. And so they're...

Leo: Secure, and the other is not.

Steve: Yeah. And you use DES three times, so you process - to take 64 bits in and process it, get 64 bits out. Then you send it in again to another round of DES, but with the next 56 bits' worth of the key. And then you do it a third time with the final 56 bits' worth of key. So you end up with a long enough key length and pretty good encryption. And so the problem is that this is not the way you store passwords because what an analysis of the database also showed, and this was posted on the Internet, the initial release was we believed it was about 3 million customer records. Then, as additional information came out, it looked like, well, maybe it was more like 38 million. Well, now we know that it's 130,324,429.

Leo: Somebody said in the Guinness Book of World Records for the largest compromise in history. Likely, anyway.

Steve: Yes. It's also been...

Leo: The year's not over yet.

Steve: ...the dumbest one because the database that's out has all these records, everybody's email address, their account ID, but apparently very few people had one in the database. But also the password hint, which was in plaintext.

Leo: And very revealing. I've read some of these password hints.

Steve: Yes. For example, "rhymes with assword."

Leo: That was my favorite.

Steve: What could that be? Yes. The title of this podcast is "Monkey Is 26th," because of course we've often talked about "monkey" and what a sort of a random-seeming word that is, which is always near the top.

Leo: Isn't that funny. I used to use it, too. I don't understand what part of our brain...

Steve: Yes. Yeah. I like "letmein." That was No. 25. That's just one above. We have "sunshine," which is a positive.

Leo: Sophos has a really great, on their Naked Security page, analysis.

Steve: Yes. And I have - I tweeted a link to the Sophos page saying it was absolutely the best write-up that I have seen [bit.ly/nodobe]. Now, No. 1 on the Adobe hit parade, used by 1,911,938 individual people creating a password for themselves on Adobe's website, and the password is, "123456."

Leo: People clearly didn't take it seriously. But they, in many cases, I mean, I had credit card information in there.

Steve: Well, no, that's the other problem, is their credit card information was also encrypted, and the worry is it was encrypted the same way.

Leo: Right.

Steve: Now, see, here's the problem, is if they had used a salted hash, where the salt is a so-called "initialization vector," you can show the salt. You just want to, in fact you need to, you need to have the salt available because you add that to the user's password, then you hash it. Then you get out something that's a fixed length, that is, the length of the hash. And if the salt - the salt doesn't have to be secret. It just has to be a nonce, a so-called, you know, a number used once. It just has to be a pseudorandom value that you mix in because what that does is it makes everybody's hash different. Which is what you want because, if that's not done, then everybody who has the same password gets the same hash. And as we know, there are rainbow tables that are basically big lookup tables where they've put in all these passwords once, done the hash, found the output, which makes it very easy to essentially reverse the hash.

Well, Adobe didn't do that. Adobe used a block encryption in the worst possible way. They used what's called - it's ECB mode. We've talked about encryption modes where, if you have a really good cipher, like Rijndael, which was chosen as the AES, the encryption standard which everyone is encouraged to unify around because we know it's really good. The idea is that every time you put the same thing in, under the same key, you get the same thing out. So that's good, except that's like the simplest, dumbest way to do encryption because, if different people's passwords, for example, just began with the same stuff, then you're going to get the same thing out. So - and that's called Electronic Code Book, ECB, because it's like a codebook. Same pattern in, same data out. Same pattern in, same data out. That's why we know exactly how many people used "123456," because there are 1.9 million instances of EQ7FIPT7I/Q. That's what happens when you put "123456" through this symmetric cipher. You get that out.

Now, we don't know what the key is yet which does that. And that's what probably people are working on right now because that will then reveal everyone's credit card number. And they would probably like to have that.

So the problem is there is a key which you put this in, and you get the same thing out. All Adobe had to do was once again use an initialization vector so that they would mix that in and then every single instance would be different. But they didn't. They simply, from what we've seen, they simply put the first eight bytes of the password into DES and encrypted it, and out came a different eight bytes. Then, without any dependence, that's the other thing you want to do with a symmetric cipher is you chain. That's why CBC, Cipher Block Chaining, is what you want to do. You want to take the output and then XOR it with the next one's input. That way you end up with a reversible sequence, that is, it's possible to decrypt that.

But that means that every successive block is dependent upon the one that came before. And the first block is dependent upon the initialization vector. So that's the proper way of doing encryption with a symmetric cipher. And Adobe didn't. They just used probably 3DES and said, oh, this is good enough. I mean, and of course our listeners are always freaked out when they say, "I forgot my password," and Adobe says, "Oh, here it is." The fact that they can give it back to you, and they ought to be really embarrassed if they say, oh, here, it's 123456.

Leo: Yeah, no kidding.

[Talking simultaneously]

Steve: ...very good that it is. So anyway, this was just - now is anyone worried or, like, confused about the problems we've had with Flash and PDF documents over the years? I mean, this is the security that the company that produced Acrobat Reader and Flash, which has caused so much grief for us all, this is their security practices.

Leo: It would be prudent for everybody to change their Adobe password. But if you had a long, strong password, is there cause for concern?

Steve: If it were something that came out of LastPass, for example, or picked up...

Leo: Yes, that's what mine is, yeah.

Steve: Yes, or something like, you know, I have a password generator at GRC.com that lots of people use which is just absolutely high-quality pseudorandom noise. Then no one else will have used it, and you're okay. See, here's the problem. If you use a password that any of the other 130 million people might have used, and their plaintext hint says "Password is..." blank, and many of them do that, by the way, many of the password hints on the list...

Leo: Don't, don't do that.

Steve: Password is...

Leo: Of course they shouldn't - unencrypted. But still...

Steve: That's quite a hint. Anyway, so the point is, if you used a password that anyone else used, and your hint was very good, but their hint was very bad, then because of the way Adobe did this, your encryption matches their encryption, and so the bad guy knows your password because the bad guy knows their password. I mean, this is so wrong in every way you can imagine.

Leo: Wow.

Steve: Yeah. So Adobe face plant.

Leo: Yeah.

Steve: And some. Oh, and Sophos finishes up, saying: "After all this, there's more to concern yourself with. Adobe also described the customer credit card data and other

personally identifiable information that was stolen in the same attack as 'encrypted.' And, as fellow" - this is the Naked Security blog on Sophos - "as fellow Naked Security writer Mark Stockley asked, 'Was that data encrypted with similar care and expertise, do you think?' If you were on Adobe's breach list - and the silver lining is that all passwords have now been reset, forcing you to pick a new one - why not get in touch and ask for clarification?"

So, and I did mention that LastPass.com has now a /adobe page where you can check to see if your password was among those. And the wonderful, the ever-wonderful xkcd.com...

Leo: Oh, I love their cartoon on this. Yes, yeah, really good.

Steve: Oh, not to be outdone. It's No. 1286, so xkcd.com/1286 describes this as the best crossword puzzle ever.

Leo: It is. It's kind of - that's kind of a good - because if you have the - so the idea is you have the hint, and you have the, I guess, do you have the length of the password? Can you deduce that from the - no.

Steve: What happens is, apparently there's a null termination character as C store strings as seven characters plus a zero. So if the password is seven or fewer, it fits within one block of encryption. And so it's the first length. If it's eight characters of actual password, the null zero on the end forces it out of the first block, so it requires two blocks in order to encrypt it. So that's where you see the two things, the first one and the second one. And if you thought you were doing a good job by using a really long password, Leo, I'm tempted to wonder, I mean, there's a password here, No. 14. 61,453 chose "1234." So there was no minimum length, apparently. Or, if there was, it was four. I'm wondering if a password of one would have been accepted. Nobody chose one that I could see, or at least not many, because I'm only looking at the list of the top 100. I wouldn't be surprised if it's there somewhere because Adobe certainly wasn't enforcing any minimum because "1234" was completely acceptable. Unbelievable.

Leo: Unbelievable.

Steve: Unbelievable. "Fdsa," where is that, fd - oh, that's the first - that's asdf backwards.

Leo: Oh, clever. Oh.

Steve: We have, of course, "fy," the expansion of that, ever present. You wouldn't want to miss the opportunity...

Leo: "Fu," yeah, yeah. I wonder if they take two letters. I can just do "fu." That'd save me some typing.

Steve: 27,415 people chose "Michael" as their password, which is not up there with "monkey," but it's close. Oh, we have "princess."

Leo: You know why it's a good password? Because it's not my name, it's my kid's name. No one would guess that.

Steve: Oh, good, yeah. "Soccer," yeah.

Leo: My sport. No one would guess that.

Steve: There's "Jennifer" and "Jordan" right next to each other. Oh, and a number of our listeners did point out that No. 70 on the list - want to get there first, Leo?

Leo: Monkey123?

Steve: No, No. 70.

Leo: Okay.

Steve: "Trustnoone" [laughter]. Certainly not Adobe.

Leo: They listen to the show, but they don't quite understand it. Oh. "Peacock," I love it.

Steve: Speaking of not understanding something, there is some reason to wonder whether a security researcher by the name of Dragos - boy, I was pronouncing his...

Leo: Oh, I love his last name, yeah.

Steve: Ruiu?

Leo: Yeah, I don't know.

Steve: R-u-i-u, Ruiu. Dragos Ruiu has made some claims. Now, he's apparently a researcher of some repute. So what he wrote was not just ignored.

Leo: No.

Steve: But because of the outrageousness, it was the single most tweeted thing that I

received all week.

Leo: Oh, yeah. Oh, yeah.

Steve: Because what he was claiming was that for three years he's been battling some insidious BIOS-based malware virus thing which has been jumping from one system to the other. And he even - it was even jumping onto laptops with no network connection, no wire, no WiFi, yet it was leaping across the room. And so it wasn't until he disconnected the microphone and speaker on his laptop that he believed that finally the computer was cut off, which led him to the conclusion, which is what upset everyone this last week, that this was an airborne audible networking virus using ultrasound. So our friend Dan Goodin at Ars Technica did a nice job. He said: "As Ars reported last week, Dragos Ruiu said the malware first took hold of a MacBook Air of his three years ago..." - boy, I have one. I'm glad I don't live near him.

Leo: Or within earshot, anyway.

Steve: Within earshot, yes, "...and has since infected his laboratory computers running Windows, Linux, and BSD." So it's a multipurpose piece of malware.

Leo: We should mention that Dragos is the creator of CanSecWest. He does the Pwn2Own hacking competition. This guy's well known in the community.

Steve: Yeah.

Leo: He's not just some guy.

Steve: He's not a crank. Which is why people took him seriously. And then Dan says: "Even more intriguing are his claims the malware targets his computers' low-level BIOS, Unified Extensible Firmware Interface," that's the UEFI, "or Extensible Firmware Interface," which apparently was before it got unified, "and allows infected machines to communicate even when they're not connected over a network."

Now, finally, after a week of turmoil that this caused, our other good friend, Tavis Ormandy - we've spoken of Tavis often, a Google security researcher - posted a note to Dragos. He said, "Dragos..."

Leo: What you smokin'?

Steve: "I've looked at your" - yeah, that's the short version. Tavis is very polite. "I've looked at your BIOS dump, your procmon" - procedure monitor - "your procmon logs, font files" - because there was also a claim that the fonts were infected - "and your disk images. I see nothing" - just like, it wasn't Colonel Klink, it was...

Leo: "I know nothing" was...

Steve: I know nothing.

Leo: I know nothing.

Steve: I know nothing. Sergeant somebody.

Leo: Sergeant Schultz.

Steve: Sergeant Schultz, yes. "I see nothing," says Tavis, "to suggest there is anything suspicious here. These are either all entirely consistent" - and, by the way, this was the evidence that Dragos made available to other security researchers to prove his claim. "These are either all entirely consistent with what I would expect to see, or have very simple explanations that do not require a sophisticated attacker. My guess is it's just a combination of stress and healthy paranoia" - this is the ever-polite Tavis - "causing you to connect unrelated events."

Then a little bit later in his note he said: "Regarding the procmon logs" - this is still Tavis. "Regarding the procmon logs, one is noisy, and the other is much quieter; but the noise is mostly consistent with just general usage. I can see you were working on some documents, browsing Facebook, installing some Sysinternals tools and so on. Nothing suspicious there. Hopefully you trust my opinion on font exploitation. I've published on the topic multiple times, was nominated for a Pwnie award for some of my research, and have been credited in lots of Microsoft advisories on the topic. The behavior you described is not consistent with font exploitation, and the font files you published all look well formed to me. If they're connected to any malware, it's just the regular kind, and not an exploitation attempt. I get the impression you're not going to believe me, but please at least think about taking a break from this."

Leo: Wow.

Steve: And then he did a little smiley face.

Leo: Smiley face, wow.

Steve: And then Dan Goodin finishes, saying: "As every student in an Intro to Logic course learns, the absence of proof is not proof of absence. I continue to agree with other security researchers when they say it's perfectly feasible for a determined attacker to develop malware as advanced as 'badBIOS'" - which is what this thing became known as - "and unleash it wittingly or otherwise on Ruiu's machines. At the same time, extraordinary claims require extraordinary proof."

And then in the midst of all this, because, I mean, I just, I let this sort of wash over me, and I'm thinking, okay. I mean, and Leo, I know you and I have both received really

over-the-top email over the years, where well-meaning end-users are convinced that for five years they have had a specific attacker who's been after them. I get email like that. And so it's like, okay, I've seen this kind of concern. But I posted on Saturday a tweet that said - or I tweeted: "badBIOS reality check." And I said: "This somewhat cranky analysis makes a LOT of sense."

And this is a guy with a lot of experience with BIOSes. And so, just quoting a small piece of this, he said: "Look, I'm not known for pulling punches, and I'm not about to start now. The fact is that everything I have read about badBIOS is completely and utterly wrong, from the supposed 'escaping air gap' to, well, everything. And I should know. I've dealt with malicious BIOS and firmware loads in the past. I've also dealt with BIOS development and modification for two decades. It's a very important skill to have when you regularly build systems that are well outside manufacturer-recommended areas. The whole of the analysis would be laughable if people weren't actually taking it seriously and believing it because they've seen edge cases or very specific examples. And the result is that they're looking in the wrong place.

"First and foremost, the very idea that there is some malicious BIOS load that can escape air-gapping and is portable is beyond laughable. I don't care what you think you know, BIOS code is not portable, period. Oh, sure, you can have a common source for multiple motherboards. But every single model, revision, and minor revision requires you to recompile UEFI elements in the best case. That's before you get into changes to UEFI libraries and shells.

"Secondly, the concept that BIOS malware could somehow escape detection is, again, beyond laughable. Look, I've been doing BIOS work for ages and then some. I can and would spot any malicious load pretty much instantly even before flashing a board. Certainly I would have no trouble finding it from a ROM dump. Period." So...

Leo: There's not a lot of code in BIOS. And of course it's always written specifically to the machine. The point of BIOS is its low-level - it's assembly language, I presume, right, code?

Steve: Yeah. Well, some of it's actually been written in...

Leo: I guess it could be C.

Steve: It's been in Forth. Forth is often used for BIOS because it's so compact, and it allows them to quickly port it. It gives them some processor independence because they can write a little Forth interpreter, if it doesn't already exist. It probably exists for every chip made. And then you have all this. But it is not - inherently, it never needs to move. So it's not position-independent code. It is position-locked. And that more than anything else means it just can't jump into a different motherboard. I mean, it can't.

Leo: Right, because of where it loads.

Steve: So maybe Dragos is misinterpreting what he's seeing. Again, as you say, he's not a loon. So how, you know - and this thing's been bothering him for three years. So...

Leo: That's the thing that bothers me. It took three years, yeah.

Steve: Yeah.

Leo: Okay.

Steve: Okay. And our hit parade continues. We have new customer service options offered by CryptoLocker.

Leo: [Laughing] This is the malware we spent a lot of time last couple of weeks mentioning and talking about.

Steve: We covered it extensively last week. I saw a lot of people appreciating the fact that we explained how it works; why they did crypto right, unfortunately; and why somebody who has been gotten by this is in trouble. Well, now the AV companies are catching up, and that's sort of the bad news because, for example, Microsoft will happily remove it from your machine. Unfortunately, that may not be what you want, if you're willing to pay $300. Now, I am seeing everyone's advice out there saying, oh, no, no, don't pay the ransom because that encourages them. Well, okay. But if you don't have a backup, I mean, it's very easy for those advice-givers to give that advice. But in the real world, if you don't have a backup, and you desperately need all the things that it just encrypted, $300 doesn't sound like such a problem.

Leo: Yeah.

Steve: So now we've got some evidence that it may be, in later incantations, or incarnations, deleting volume shadow copies, because it wasn't initially. And so if you had so-called - a volume shadow copy is the technical term for Microsoft's rollback technology in Windows. It allows you to go back to a previous version if something you've done has hurt your machine. So that was the advice. Of course, any advice that appears on the Internet, these guys are also seeing. And so that's why long-term I'm very concerned that this is going to be difficult for us to deal with.

However, if the worst happens, and you eradicate the registry key, which apparently is the key for your being able to decrypt your stuff and/or remove - if you remove the whole virus, you have been able to download it again. It's something called, it's ridiculous, it's 0883.exe or something, that has been available. So you could reinfect your machine in order to then go through the decryption process to get your files back. So the problem is three days might pass; and then, as we know, you have a 72-hour window, in which case, after that, you're hosed.

Ah, but we now have the new high-priced service being offered through the Tor hidden services system. So this is a service hidden by the Tor network, and we've talked about how Tor hidden services work, where for 10 bitcoins at the current going price, whatever that happens to be - currently a bitcoin is about $210. So 10 of these...

Leo: 260. Just went up.

Steve: Ooh, boy.

Leo: It's at a record high. Or not record, but it's very high.

Steve: I'm liking it. I'm liking my 50 bitcoin...

Leo: Yeah, baby.

Steve: So, yes, now we're at $2,600 you would have to pay them to get your files back. The good news is there's no time limit on this. So if you are in a position where this is your only recourse, you have no backup, the stuff you need is worth whatever the current price is for 10 bitcoins, and as Leo said, currently $2,600, you can go to this Tor hidden service, and you give it one of your encrypted files. Apparently the encrypter puts a header on the encrypted file that allows it to perform a search for your public key. So it puts like a - it's a 1024-bit header is what I saw. So that would allow it to find your public key. Then it says, ah, found it. So we can decrypt your files. Download the handy-dandy decrypter from this link and pay us 10 bitcoins. They then wait for the bitcoin network to verify the transaction. They wait, they stated, from 10 to 15 confirmations out on the network. And then they will provide you with the matching private key in order to perform your decryption.

Oh, and if the three days have not expired, that is, if you want to use the service within the 72 hours because you did - something came along and removed this before you were able to pay them, then in an update on Monday they made a change such that, within the first 72 hours you only have to pay the two bitcoin price. Which now would be, what, 512 or, no...

Leo: Yeah, 520.

Steve: There was 260, yeah, 520.

Leo: Kind of amazing, yeah.

Steve: So that's certainly better. So you can use the service within three days and pay the reduced price. Or, if you wait past 72 hours, then you're going to have to pay $2,600 at the current going price.

Leo: At least they save it. Because sometimes you're out of town, and you don't get to see it, and I think that's just fabulous, yeah.

Steve: Yeah. Yeah. So for frequent travelers we have a service.

Leo: Geez, Louise.

Steve: Now, in an interesting sort of related post, it turns out that users of the OpenDNS Umbrella service are safe from this. Because, when you think about it, this is all based on DNS. It turns out - and I'll just quote from their blog. They said, the Umbrella service said: "First, a quick recap of how OpenDNS provides protection against CryptoLocker. In a previous post, we introduced a predictive algorithmic method called 'The Ripple Effect' for detecting CryptoLocker command-and-control domains."

And remember we've talked about how they're just a bunch of gibberish. It's a long crypto-looking thing dot something - .ru, .nz, dot whatever. It's in a bunch of top-level domains, but then it's just gibberish-looking. And the bad guys only need to register one of the many that are generated. And the CryptoLocker infection on the user's machine uses the current date in order to generate a large list of candidate domains. And it doesn't know which one is valid, but the bad guys know. But what we do know is that one among them will be valid. So the virus starts doing DNS lookups in very short order of this random gibberish. Oh, and these are 1215 characters long. So when you think about it, a smart DNS server could see your computer beginning to do this and say, whoa, hold on.

Leo: Awesome.

Steve: And it does.

Leo: Now, that's their Umbrella service. What is their - it's business security. So you have to...

Steve: Yes. It's only corporate.

Leo: That's a paid service. It's not for...

Steve: Yes.

Leo: Because I use OpenDNS, of course, but...

Steve: Yeah, and unfortunately it's not available to OpenDNS users, and it's not cheap.

Leo: But Umbrella is designed to protect you against malware and botnets, so this is good.

Steve: Yeah. So, "The method uses the fact that the malware contacts a set of randomly generated domains to fetch an asymmetric crypto key before it starts encrypting the data files on the victim's system." So this blocks it after infection, but prior to encryption,

which is perfect. And it says: "The Ripple Effect method relies on the co-occurring pattern of the domain requests made consecutively by the malware within a short time window."

And then they said: "A number of users of our free DNS service were infected with the malware." Meaning that OpenDNS itself doesn't provide this protection. "But OpenDNS customers using Umbrella are protected against losing their valuable data to CryptoLocker because we successfully cut off the outbound communication initiated by the malware for retrieving the encryption key." That is, if the client can't reach the command-and-control server, it can't get the key.

"OpenDNS customers are spared the data loss and gain time to remove the malware before it can cause damage. If you're an Umbrella user, you can check for evidence of CryptoLocker in the Dashboard," which is their UI to the client, the user side of this. "On the Security Activity Report, filter by security category 'botnet.' There is a very good chance, if you were infected by CryptoLocker, you will see a long list of botnet domains displaying the following patterns: 12, 13, 14, or 15 random characters, top-level domains rotating among .info, .com, .ru, .biz, and .co.uk." And then: "Frequent requests made in very short intervals to about 1,000 unique domains following the above string patterns." So a thousand.

Leo: Now, I wouldn't, if I were them, crow too much because it would be easy to modify CryptoLocker slightly to bypass this. Right? Somebody in the chatroom said, yeah, just encrypt with a weak encryption and then send the key out, or, I mean...

Steve: Ah, good point. You could do a - good point. You could easily generate locally your own symmetric key, so use local entropy on the machine to generate a very strong symmetric key, hold that while you're waiting to share it with command central, and encrypt all the files using that. So, yes, you could absolutely do that.

Leo: So don't get - don't make too big a deal, OpenDNS, about this. You're just attracting attention. You started saying it was expensive. How much is the service?

Steve: It's like 29 per something per user. So I don't know...

Leo: $30 a user per month, probably. That makes sense.

Steve: Wow, that's pricey. I mean, ouch.

Leo: Maybe it's per year.

Steve: Oh, it's per year or per month?

Leo: Maybe, I don't know.

Steve: Anyway, if you put "Umbrella" into Google, or "OpenDNS Umbrella," it'll take you

there, and you can see that they have a big button you click to get pricing. And it shows you, like, four different types of plans they have. But, boy, they're not cheap.

Leo: Seems like it's something we probably should do here.

Steve: Oh, yes.

Leo: $33 per user per year. That's...

Steve: Okay, that's not that bad.

Leo: No, it's nothing, in fact. And then, yeah, $39 for the top-of-the-line protection. Okay.

I was going to say real quickly, one thing that, if LastPass is listening, you might want to change in that nice, that kind of nice idea that you go into LastPass.com/adobe to see if you've been hacked, and you enter your email, unfortunately LastPass then sends out an email to that address. And I've received many, many emails from LastPass as people test my address in the Adobe cracked database. So LastPass probably might want to change that.

Steve: I wonder why they're doing that.

Leo: That's really annoying. Well, because they want to - you are receiving this email because you have - because hi. You're receiving this email because you used LastPass - not me, but somebody used LastPass - to confirm your Adobe account credentials were leaked and requested that your Adobe password hint be mailed to you. Actually, maybe that's a checkmark in that page? Let's just go quickly and see.

Steve: Oh, but, yeah, they can't...

Leo: It's really annoying.

Steve: Oh, email the hint. Yeah, that's a good point. The hint is there with every email address.

Leo: But it doesn't say, it just says put your email in and test my email. It doesn't say - I didn't - nobody [growling]. Stop it, LastPass. I liked you up to now. I've gotten a lot of these. I don't need more spam.

Steve: You probably do have - Leo, with your email address being leo@leoville.com?

Leo: Oh, thanks for telling everybody that [laughing].

Steve: Yeah, I know, that's a secret. I guess the problem is you're receiving it from LastPass, and they're whitelisted on your spam...

Leo: Well, not anymore. I've just told Google this is spam, LastPass. Little hint. Might not want to do that anymore.

Steve: So to wrap up our CryptoLocker update, CryptoPrevent, which is a very nice free or paid - you can pay for the auto-updating version if you would like auto updates. And that would have paid off, by the way, because they've updated it now to - we were at 3.0, I think, last week. Now we're at 4.0. So additional features. The guy is continuing to hone it. My concern is that this is - it's not strong protection. It's certainly better than nothing. So it uses Windows' group policy system in order to block some of the behavior which CryptoLocker exhibits in terms of where it puts things to execute. But all it has to do is put them somewhere else. And that's why it's like, eh, okay, it's better than nothing. But it also kind of messes things up in your system. And there has been a problem with it blocking, doing a false-positive block because other things are able to behave in the same way that CryptoLocker does. So it's like, eh. Okay.

However, Sandboxie, our old friend Sandboxie, is effective in containing CryptoLocker. It's been verified that, if you were to put your email client and your web browser in Sandboxie, if you were to Sandboxie those two things, and we've talked about - we did a podcast on Sandboxie [SN-172]. Anybody could, like, google "Sandboxie Security Now!," I'm sure you'll find it, or go to GRC.com/sn, and I've got a search field that I pay Google handsomely for, and put Sandboxie in, and you'll find the podcast where we explain it. What happens is, if you get a CryptoLocker infection through email or web browsing, and you have employed Sandboxie, then an encrypted copy of your files are created in the sandbox, but nothing gets out of the sandbox. So your original files are all fine. And all you do is empty the sandbox, and CryptoLocker and all of its damage it tried to do is gone. So...

Leo: Nice. Nice, nice, nice.

Steve: Yes. So that's a solution that makes sense. I like Sandboxie because it is lightweight. The heavyweight, the industrial-strength solution is a virtual machine. I've always owned VMware, so I still have that. But the free VM, the one that Oracle offers, I can't think of what it's called. It's the one everybody uses because it's good, and it's free.

Leo: Oracle?

Steve: Isn't it Oracle? Sun?

Leo: Oh, yeah, yeah, Onebox. Or VirtualBox. VirtualBox.

Steve: VirtualBox. VirtualBox, yes. VirtualBox is industrial strength. Many people have asked, well, would that work? Absolutely. So you set up VirtualBox and do email and surfing there. And there you have total control over what drives are visible. And drive letters is what CryptoLocker ties to. Thus network shares that are mapped to drive letters are what CryptoLocker is able to follow in order to, like, encrypt people's shared network storage, which will ruin your day. So the problem is that using a full VM takes up a chunk of memory out of your system. I mean, it's stronger protection, but just using Sandboxie is a very nice lightweight solution, and we know now that it is effective in blocking CryptoLocker. So yay to that.

Now, I'm sorry you're not happy with LastPass, Leo, because...

Leo: I'm mad at you, LastPass.

Steve: ...the world is happy with LastPass. They came out with a big v3.0 upgrade.

Leo: Yeah, I like v3, yeah.

Steve: Yes. And many people do. In fact, I just googled, I wanted to kind of get a sense for it. So I just googled LastPass v3.0. The first link that came up said - it was a forum posting, and it read: "Hi. I'm a recent LastPass user. After trying several alternatives (1Password, Locko, Dashlane, and KeepassX), I chose LastPass mostly because it offers the best feature set for a competitive price, a good tradeoff of security versus flexibility, and Steve Gibson can be mighty persuasive."

Leo: That must make you happy. That's great.

Steve: Then he said: "But the one thing that really put me off was the poor user interface." And we're talking about the old version. "LastPass hasn't been designed, it has been programmed." Now, frankly...

Leo: Never bothered me.

Steve: ...that's what turned me on to it.

Leo: Yeah, yeah. Never bothered me at all.

Steve: Serious, serious technology. Joe has been completely open about how it works. That's why I've been able to talk about it. I still can't talk about BitTorrent Sync because they won't tell me how it works. So it's like, well, okay. They're bragging about having a million users. It's like, okay. I mean, it's probably safe. But we can't know.

Leo: We don't know.

Steve: Until they'll share it with us. So anyway, this guy just goes on to say, basically, he loves the change that's been made to the aesthetics, all kinds of things. The flow is better; the design is better. So this is a very nice, substantial usability and UI upgrade to LastPass, taking it to 3.0. And also there's a thing called Family Folders, which is a new feature that allows members of a close-knit family group to share in some fashion. I haven't looked at it closely because it's just me using LastPass. But bravo.

Leo: Yeah, no, I just think they've done a really nice job. It's cleaned up; it's beautiful. They probably hired a designer.

Steve: Yeah, which is good. But I'm glad they did that first. The problem, for example, with - there was that messaging client. It wasn't Threema, although Threema just apparently added group messaging, which I haven't had a chance to look at it yet. I just saw that this morning.

Leo: You know, I had to delete Threema from my - so if people sent - first of all, I made a mistake giving out my QR code because I was getting, like, 30 or 40 messages an hour. But then, and maybe it's because I was getting so many messages, Threema just crashed my Moto, that's my Android phone, badly, forcing a reboot. And so I've removed it because I can't...

Steve: There was one, it wasn't Threema, but apparently they were, like, UI designers. And I've talked about them several times. The name will come to me.

Leo: Not Hemlis. Not the Hemlis guys.

Steve: Hemlis, yes, Heml.is, Hemlis. Gorgeous-looking. Very pretty. Rainbow colors. Oh, and it's got just such a nice balanced-looking UI. However, their crypto, they're saying, well, we can't tell you how it works because them maybe it could be hacked. It's like, what?

Leo: That's a bad sign.

Steve: What?

Leo: Always a bad sign.

Steve: Yeah. So LastPass just came out of the gate saying, look, this is what we do. And that's the reason I fell in love with it is that it's like, okay, that's correct.

Leo: And that's the right way to do it.

Steve: You did everything right.

Leo: Yeah, that's correct, yeah.

Steve: Yes. It's the only way to - and it's like the way the SQRL project is going. I have an update on that, by the way, because I scrapped the Identity Unlock that I had last week with one that I came up with Monday that made it much better. But we'll get to that in a second. So bravo, LastPass.

BitTorrent Sync, as I mentioned, just had a big ballyhoo news that they have a million users. They have also opened the developer API. But apparently you still use a closed, nondocumented engine. So the developer API lets third parties now create apps on top of the BitTorrent Sync protocol, which is closed, and which we know nothing about. And I'm sure lots of people will. And I don't understand why they're not telling us how the protocol works because that's reason for concern. But they're not. So it's still closed protocol. No security analysis is possible of it. We just assume that it's a good thing. So, and a million people are apparently doing that now. It's free, and it's out of alpha, and download it and go.

Leo: Leo Laporte with Steve Gibson. Yes?

Steve: I was going to say password lists are just fascinating.

Leo: Oh, you're reading that Sophos list? Yeah.

Steve: It's just wonderful. I did tweet, for anyone who's interested, a link to the nice list of passwords [bit.ly/1bYTopN]. It's just wonderful. I don't know what it is about it. It's sort of like you get to sort of reverse-engineer what people are thinking. Like there's "1q2w3e4r," which of course comes right off the keyboard. And you had to think, whoa, nobody is going to come up with that one. And 22,000 people did the same thing.

Leo: "1q2w3e4r." That's a good one.

Steve: Yeah. It's just sort of - we've got "Hannah" and "Ginger" and...

Leo: Yeah. Again, I'm sure that's not their name because that would be too easy. It's their kids' names or their dogs' names. In fact, some of the clues are "My dog's name." I love the hints. The hints are as much fun, frankly, as the passwords.

Steve: Oh, god, yeah. Oh, it's wonderful. Okay. So the good news is, a piece of software that we here on the podcast love...

Leo: Yes?

Steve: TrueCrypt.

Leo: Uh-huh.

Steve: ...has easily made its audit money goal.

Leo: Oh, that's such good news.

Steve: And I'm annoyed that they're over on Indiegogo because I don't have an account there. But I'm going to have to set one up just so I can pay them the money and get the T-shirt because I need the TrueCrypt T-shirt. And you get stickers and all kinds of other stuff. They wanted to raise $25,000, which I think is a very reasonable number - unlike what Ladar wants, but we'll get to that in a minute - $25,000 to do the audit. And they're at $35,264 last I looked, a few hours ago.

Leo: Yay, yay, yay.

Steve: So an additional $10,000 over their goal. And of course this is Matthew Green, a world-renowned cryptographer, who said, you know...

Leo: He doesn't work for TrueCrypt, we should mention. Right?

Steve: Say what? What?

Leo: He does not work for TrueCrypt. This is an independent audit. Or does Matthew...

Steve: Oh, absolutely. No, no, completely, no. He's with university of something, living in Chicago maybe [Johns Hopkins, Baltimore]. I don't remember exactly where. But, yeah, this is absolutely independent. The goal is that they're going to take the source, and they're going to verify that they get binary identical builds by having lots of separate people create it. So the idea will be we can get a reproducible binary image from the source, and then they're going to do a complete careful read, really crypto-smart people reading this line by line, was everything done right. Is there anything wrong in here, anything hinky, anything that doesn't look like we understand why it's there? And, I mean, it'll just give us all a neat warm fuzzy. And then we'll lock that down, and that will be the source for TrueCrypt.

And, I mean, I think it'll tremendously increase its value. I mean, I use it now because it's, like, sure better than NoCrypt. But it'll be nice to know that there is nothing that crept in. I mean, one of the things we've learned, unfortunately, from Snowden is there has been an infinite budget and infinite will to get everywhere possible in security. It certainly is not beyond the pale to imagine that the NSA may have had some influence. So we just need to know that that isn't there.

Speaking of the NSA, yesterday Google engineer Mike Hearn weighed in on Google and the NSA. He in his Google+ posting quoted another colleague in the security team,

Brandon Downey. And he said, "Recently Brandon Downey, a colleague of mine on the Google security team, said, after the usual disclaimers about being personal opinions and not speaking for the firm," he said, "which I repeat here," and I can't say what Brandon said, but eff these guys, meaning the NSA. I mean, this gives us...

Leo: They were pissed.

Steve: Yes. The reason this is interesting to me is this really gives us a window into Google's feelings about this. And so then Mike says, this is yesterday: "Now I join him in issuing a giant FY to the people who made these slides," referring to the NSA slides. "I am not American, I am a Brit, but it's no different - GCHQ turns out to be even worse than the NSA.

"We designed this system to keep criminals out. There's no ambiguity here. The warrant system, with skeptical judges, paths for appeal, and rules of evidence, was built from centuries of hard-won experience. When it works, it represents as good a balance as we've got between the need to restrain the state and the need to keep crime in check. Bypassing that system is illegal for a good reason. Unfortunately, we live in a world where, all too often, laws are for the little people. Nobody at GCHQ or the NSA will ever stand before a judge and answer for this industrial-scale subversion of the judicial process.

"In the absence of working law enforcement, we therefore do what Internet engineers have always done - build more secure software. The traffic shown in the slides below is now all encrypted, and the work the NSA/GCHQ staff did on understanding it ruined. Thank you, Edward Snowden. For me personally, this is the most interesting revelation all summer."

Leo: We said that, when we talked about that slide with the smiley face on the Post-it note, here's where we get all this stuff, we said - they had shown it to somebody at Google who, like, was - that's outrageous. Was it Eric Schmidt? I think it might have been Eric Schmidt. So I'm really starting, between these two posts and Eric Schmidt, I'm starting to think Google really doesn't know anything about this, and they're miffed.

Steve: Well, and then in response to Mike's posting, we learned something else, I did, which I thought was very interesting. Jeff Weiss was the first person to respond, saying: "Until this article, no one had mentioned that the intercepted traffic was on leased fiber, not on the public Internet. That makes the cleartext transmission seem like a less glaring error. I suppose I can see how it wouldn't seem necessary. In fact, anyone claiming it was necessary probably would have been seen as paranoid until now. Still," Jeff writes, "encrypting data sent over the wire is not difficult. Considering the value of the data in question, and the number of parties who could access it - at least two, the fiber owners and the government - it seems like a worthwhile investment. Lesson learned, I suppose."

And then Mike replied, the original poster who I first quoted, Mike replied: "I think the fact that Google uses private fiber has been well known for quite a while, actually. Just search for," and he says, "'google dark fiber,' and you'll find many news stories discussing that, and it was mentioned offhand in previous stories as well, I think. Yes, that's pretty much it. Encryption was being worked on prior to Snowden, but it didn't seem like a high priority because there was no evidence it would achieve anything useful,

and it cost a lot of resources. Once it became clear how badly compromised the fiber paths were, there was a crash effort to encrypt everything."

And then he finally says: "Re: 'not difficult,' I disagree. Doing end-to-end," meaning encryption, end-to-end encryption, which is, as we know, the gold standard, that's all that matters, doing end-to-end, which is why, for example, PGP works for email, but nothing else does, "doing end-to-end on the scale of Google is a lot harder than it looks. Ignoring CPU capacity constraints, the entire thing requires a large and complex key distribution and management infrastructure," he says, "(fortunately already present). Also, lots of different protocols flow over our wires, each one of which has to be handled."

So there was a lot here that I thought was interesting. As you said, Leo, we get a look, finally, into Google's authentic feelings about this. And the fact that this - they were buying, essentially, leasing their own fiber. So this was not going out on routers across the Internet. This was, you know, we've talked about how the Internet is packet-switched. And the brilliance of it was that you could just send little packets off into sort of nowhere, and they would, with an address, just carrying a destination address, and they would get there, sort of like writing an address on an envelope and dropping it into any mailbox, and it finds its way to its destination. That's how the Internet works. Whereas before that, we used to have dialup lines where you and your modem called CompuServe and their modem, and your phone was tied up, and no one could call you. You got a busy signal if you tried while you were using CompuServe or the Source or AOL in the old days.

So these are like that. This is Google purchasing dedicated, their own, they have all of the bandwidth of this optical connection where they blink lights in one end, and it blinks out the other, essentially, between their data centers. So they had every reason to believe this was absolutely private. The government tapped that.

Leo: And that's why they tapped it, of course, because it was likely unencrypted. It isn't now, by the way.

Steve: Well, Leo, because it was there. They tapped it because it was there. And I wanted to wrap this segment up by just saying, in the NSA's defense, we got what we asked for. That is, it really was the case that, in the U.S., at least, Congress said, "Protect us from anything like 9/11 again at any cost. Get full information. Do whatever you need to do." So now the good news is, as a consequence of Snowden's revelation and all of the backlash, we understand what we unleashed. And so now it looks like there will be some dialing back of that. It's like, oh, now we know what happens if we say "Do anything you want," and you have as much money as you need. Well, I mean, that's what the people in the crypto palace want is carte blanche. And we gave it to them, and they tapped everything. So now it's like, whoa. Okay. Except maybe not Angela's phone anymore because that really annoyed her.

Leo: Angela Merkel, Chancellor of Germany?

Steve: Yes [laughing].

Leo: Yeah, I don't know, maybe they stopped, or maybe they just made it a little bit more secretive. I don't know.

Steve: I know. So anyway, this has been good. Again...

Leo: Oh, yes. This is - anybody who thinks that what Edward Snowden did is somehow unpatriotic doesn't - I think is missing the point.

Steve: And that was our first reaction upon hearing it. The first moment this came out, I watched that video that was made of him in the hotel room, and I thought, okay, this guy knows what he's talking about.

Leo: Yeah. Boy, the more we see, the more - my only complaint is that it seems that they're dribbling it out with an aim to maximizing profit as opposed to...

Steve: I think it maximizes that because...

Leo: But also attention. It maximizes attention.

Steve: Yes, yes. I think this is brilliant because, if it was just a big blob...

Leo: Be too much.

Steve: ...if they dropped - it would be overwhelming. Yes. This is like, it's like, oh, god, you wake up on a Monday morning, and the NSA has to be thinking, what now? What? What? Because they know what hasn't been revealed yet. And they have to be thinking now, he got it all. So it's just a matter of time.

Leo: Hey, speaking of spam, can I apologize? And did you get an email from me asking you to join Twitter? I apologize.

Steve: Oh, I did, actually. I got two. And I...

Leo: Okay, yeah. If I have - just ignore it. If I have several addresses on file in my contact list for anybody, you got one for each address. Dr. Mom got six invitations from me. And let me just show you. I think it's Twitter's fault. Well, it's my fault. But let me just show you because I was signing up for - I was signing up with my Twitter on my new Nexus 5. And this is how it happened. You're now on Twitter. Follow your friends. Now, I should have just said skip it. I said, oh, no, no, that's good, I'd like to follow. Yeah, you can have access to my contact list. And this is where my troubles began. Follow your friends. I'll follow them all. Yeah, actually I think I did follow

them all. Okay. Now, invite friends.

The default on the phone is a little different. This is on iPhone. On Android it's defaulted to "select all." If I press this right arrow - this is the default. Tell me how you get out of this. Because, if I press this right arrow, all of the contacts in my address book, each address in my address book will get an invitation from Twitter. Every one of them. And it was just, I mean, admittedly I should have paid more attention when I was signing up. But there was no are you sure you want to email everybody in your address book or anything like that. It just did it. And so I apologize. My mom sent me a text today saying, "Well, I joined Twitter like you asked me." It was like, no, Mom, don't, don't join Twitter. We will securely upload all - I'm glad it's secure that they've uploaded my contact list to Twitter. Follow friends. Okay, done on that one. Invite...

Steve: And Twitter's never made a mistake with their security, so...

Leo: Yeah. So here's the one, this is the one that happens on the Android phone. It's by default all are selected. If I tap "done," an invitation will go out.

Steve: Ooh. Wow. Yup. Little too easy.

Leo: Yeah. And I accidentally typed "done," like I'm done. I don't want you to invite everybody. Instead it said, oh, you're done, we're going to invite everybody. So I apologize to all the people who received emails.

Steve: And the headline of my next topic is...

Leo: I don't really want you to join Twitter, by the way. Stop.

Steve: The headline of my next topic is "It's not a bug, it's a feature."

Leo: Yeah. Exactly right. So go ahead. Take her away.

Steve: That was Google's response last August when the blogger - remember we talked about this on the podcast - declared that Chrome was flawed because it wasn't masking the passwords that Chrome was saving, your website passwords that Chrome was saving for you. And I defended Google, saying, "It's not a flaw. Look at it. It's the way they designed it." Now, we could complain about the design, but calling it a flaw, the way this was phrased made it sound like it was a defect. No, it was by design. So Google said it's not a bug, it's a feature. And then they said, okay, well, maybe we can do better.

So what they're doing is they're giving us what users, security-conscious users have apparently asked for. For example, Safari on the Mac re-prompts for the machine's standard login password if you want to display your web browser passwords, which seems reasonable. Firefox, as we know, by default allows you to set a master password,

sort of a master password password, to protect the viewing of and access to your passwords. And so Google said - their original position was, well, we just feel that that gives users a false sense of security. We don't want to do that because, if anyone has physical access to their machine, well, that means there's no security. And many people responded, saying, wait a minute. And actually someone said, well, what about my crackhead brother? It's like, okay, well, that's a little disturbing. But, yes, we can understand that maybe you'd want to keep him from logging into your websites.

So in what's called the "Canary" version of Chrome for OS X on the Mac, which is not yet released into the mainstream, it's been noticed that Chrome has added the feature which, as with Safari, will re-prompt you for your Mac platform, your Mac OS X master password, if you want to view your passwords in Chrome. So congratulations. I think that's a good thing. We haven't seen it across platform on...

Leo: Well, you will. Canary is the - so Canary is basically alpha. There's a beta channel. There's Chrome, Chrome Beta, and then there's Chrome Canary, which is an alpha channel. But that means it will be migrating up, I'm sure, unless there's some problem with it.

Steve: And it ought to, yeah, it ought to. It's like, that's a good thing. Many people asked about a new app that appeared in the iTunes store just yesterday called Knock.

Leo: Yeah, I thought this was interesting.

Steve: Yeah. And so I spent enough time with it to familiarize myself with it, look at the security model, and then I tweeted, yup, they did everything right. So here's what the deal is. It's from some guys from Square, so they understand security and UI and things. And so they said, okay, how can we improve the user login experience? Their first version had an automatic login to your Mac OS when you approached your machine with your phone in your pocket. And that was a little unnerving to users. They said, you know, it just sort of has a mind of its own, and what if I'm just sitting down at Starbucks with a fresh cup of coffee, I don't want to unlock my laptop right now, well, it just unlocked for me. So back off. And they've been playing with this with about a hundred testers, I guess, for, like, six months.

And so they said, okay, how about if you have to go knock-knock on your phone? They take advantage of the inertial sensor in the phone and make knocking twice on the phone in your pocket be the key to unlocking your laptop. So be very careful, because it's not free, that you have the required compatible equipment. You need - basically what this is is it takes advantage of the Bluetooth 4.0 or the so-called LE, the low-energy version of Bluetooth. That has a reduced range, which is fine for unlocking your Mac; also a reduced bandwidth and data rate. It also, though, has a reduced latency. Whereas regular Bluetooth takes about half, or I'm sorry, about a tenth of a second to negotiate, this negotiates in six milliseconds. So it's very suitable for quick little bursts of information, like here is the - and a privately encrypted key.

And when I said they did this right, what they did is they used 2048-bit standard RSA public key asymmetric encryption. They encrypt the password using your private key on the phone. So there's no way for an attacker who gets your phone or tries to take it apart or do anything to get anything useful. They send that when you have a connection to your laptop and when you have tapped twice on your phone. They send it over this

Bluetooth low-energy connection to the companion app, which is free. I should mention the iTunes app is four bucks, 3.99. And it has, your Mac has your public key. Does not have the password there, just the public key. So again, it can't do anything because it doesn't have anything that it can use, until it receives the private key encrypted password. Then it's able to decrypt it, use it, and unlock your machine.

So you do need an iPhone 4s and later, an iPad 3 or later, an iPod Touch 5 or later. The mini has always had Bluetooth low-energy and iOS 5 as the operating platform, and later. And Macs are a little confusing: 2011 MacBook Air or newer, a 2012 MacBook Pro or newer, a 2012 iMac or newer, a 2011 Mac mini or newer, or a 2013 Mac Pro. They spell this out over on iTunes under "Compatibility." Make sure you don't waste $4. A couple people apparently have. They've been unhappy, as they commented in the iTunes store.

Leo: No refunds on the App Store. That's...

Steve: Right.

Leo: You bought it, you pay for it.

Steve: Yeah. So anyway, so for people who are wondering, yes, it looks like they got the security right. And they say they're going to do more things. They're not Apple-only. They're going to address Android when they can. But the Android market is more fragmented. There isn't the same uniformity of API, so it's a bigger challenge for them. But kind of a cool idea.

Leo: Well, the cool idea is Bluetooth LE. That's really the cool idea. And there are so many things we're going to see with that. I'm just really excited about it.

Steve: Yeah, the energy is so low that a single-cell coin battery can run more than a year. So...

Leo: So people are putting beacons in - we could put a beacon in the Brick House, for instance, that your phone would sense and would automatically pull you to an informational website, or check you in, or whatever. There's all...

Steve: And people have, like, plastic tags they're selling. You can put tags on things, and you're able to...

Leo: Never lose your luggage, I mean, just goes on and on and on. This is - Apple's going to push this heavily because this is, I think, their response to NFC.

Steve: NFC, exactly.

Leo: Yeah, they like this better. And I think, given the security you just described, maybe it is better than NFC. I think that this is all the, you know, the Fitbit Flex uses it. A lot of the health bands are going to start using that. It's just a natural.

Steve: Right. So Ladar Levison wants to raise - and I don't know where this number came from - $196,608 is his goal. Almost - just shy of $200,000. So that's a chunk of money. It's on Kickstarter, Lavabit's Dark Mail Initiative. And he said, the description there says: "The goal is to clean up and release the source code that was used to power Lavabit as a f/oss" - so an open source - "project with support for dark mail added." The problem is I can find no documentation for Dark Mail. And as far as I know, it doesn't exist yet. I mean, it's an idea. It's gotten a lot of press because of course this is the guys at Silent Circle are teamed up with Ladar on this. He's got a ways to go, but actually he's doing pretty well so far. He's got 1,082 backers when I looked this morning. He'd raised nearly $50,000 pledged out of his $200,000 goal, with 21 days to go. So that's the positive...

Leo: He said on the interview with us, he didn't say details, but what they want to do is write a new mail server, not SMTP, but write a new mail server that has PGP encryption built in. So he understands, I think he understood the issue. I know he understood the issue of there's no such thing as secure email because SMTP servers, while they have encryption, don't generally use it. So what they've said, I believe, is that they're going to use XMPP as the protocol, which does support, can support encrypted communications. And then they're going to have GPG or PGP baked into both the clients and the server so that it uses it by default.

Steve: XMPP could support - I'm thinking OTP. That's not what I mean.

Leo: Perfect forward secrecy?

Steve: No. There's the real-time...

Leo: By the way, they say they want to implement that, as well.

Steve: Oh, yeah, they absolutely should. OTR, Off The Record.

Leo: Oh, yeah, OTR, yeah, yeah, yeah.

Steve: So XMPP, because it is real-time connection, could support Off The Record point-to-point encryption to get you to the server. And then at that point you could use PGP there. But then of course you've got to trust the server.

[Talking simultaneously]

Leo: Well, I would hope they don't want to do that, yeah.

Steve: ...trust the client.

Leo: I want Trust No One.

Steve: Yeah, exactly.

Leo: Well, is that what Mailpile is? Are you going to talk about Mailpile?

Steve: Not this week. But Moxie Marlinspike, who really does know his security, did a posting where he was rather disappointed with this plan. He didn't feature the idea that they were going to go a lot further, but he was responding to the idea of raising all this money to clean up the source code of something which never was secure. I mean, Moxie was assuming that Ladar was only going to do what Lavabit did. And so I created a bit.ly link called "lavanot," bit.ly/lavanot, all lowercase, if anyone's curious. Because Moxie did do a nice job of breaking down why I was never impressed with Lavabit when I went to look, as soon as we heard that Edward Snowden had been using Lavabit, I ran over and looked. And it was like, okay, well, this is nothing.

Leo: Right. You told me that. I had subscribed for a year, and you said, well, sorry, Leo, but your money is wasted.

Steve: Yeah, yeah.

Leo: But I used to use Hushmail in the day, which was Phil Zimmermann, PGP guy's PGP webmail. Same thing; right? Same problem. I think.

Steve: Well, I don't know. I mean, Moxie made a...

[Talking simultaneously]

Leo: Well, go ahead.

Steve: Yeah, Moxie made a point of saying that webmail cannot be secure. And that's not true. I mean, with today's browsers, you really can have very good web browser-based client-side security that encrypts everything on its way to the server. Now, the problem is the infrastructure. Email itself resists encryption at every stage because, for example, it wants - it's inherently a store-and-forward system. So you don't have a real-time point-to-point connection where, for example, you could use secure key negotiation to negotiate an ephemeral key on the fly, and then you both use that to exchange things. I mean, all that technology exists. But the problem is email bounces from one server to the next, sort of going towards its destination - excuse me. Got a little bit of a tickle in

my throat here toward the end of our podcast. And so it's difficult - wow. It's difficult to encrypt. And it's resisting encryption.

Leo: Right. That's the point. And that's why they want to write a replacement for SMTP that would by default, in fact, require point-to-point encryption. SMTP can do it, but very rarely do people do that.

Steve: Yeah. I don't know.

Leo: Now, I remember. With Hushmail they were clear about that. They said, if you mail something from Hushmail to somebody else, all bets are off. But if you email somebody within the Hushmail system...

Steve: Ah, within the system, yes.

Leo: ...you're okay. So that was a good way to do it, I think. And that was...

Steve: Yup, that absolutely makes sense. And that was my problem with Lavasoft is the moment - I mean Lavabit, sorry. The moment the email leaves and is connecting to another server, well, it's decrypted, and the NSA says thank you very much. And this was, of course, the same thing with them sitting outside of Google when they were able to do that. As long as something stayed at Google. I remember we were talking about how Petraeus was clever. He used a folder in Gmail to exchange information with his illicit lover.

Leo: His girlfriend. But that makes sense, and that would work had he not then given his keys, his password to somebody.

Steve: Yeah.

Leo: But if you don't - but that would work; right? That system would work.

Steve: Yes.

Leo: And that's what I'm wondering, if Ladar - remember what Ladar told us on the interview on Triangulation, it was a couple of weeks back, and you should listen to it - I'm not talking to you, Steve, but everybody else should listen to it. What he said was that the feds wanted the SSL keys, just as you had surmised, which meant that then all the mail would be readable, would be in the - they'd be able to look at it in the clear all the time. And I presume that would also include mail stored in a drafts folder.

Steve: Yeah. His mail at rest was encrypted. And Moxie explains this. When email came

in, the system looked up the user's - the system only had the user's public key. So it used the public key to irrevocably encrypt, or irreversibly encrypt the email, which then was stored on the server. They then did not have the ability to decrypt it. The problem is, when the user logged in with their plaintext password to Ladar's server, it then used that to decrypt the user's private key, which it then used to decrypt the stored email and send it to them in the clear. So it really did nothing. So it's like, okay. I mean...

Leo: Had nothing been sent, though, had it been stored in the drafts folder, it would be secure because it was encrypted, unless the FBI says to Ladar...

Steve: Correct. It was encrypted at rest, yes.

Leo: ...give me the keys. And one presumes that's what they were asking for.

Steve: Well, and it's true that Ladar did not have the keys. That was the key. By using asymmetric encryption, he was able to encrypt securely. He could not decrypt until the moment that the customer asked for his email. And then he did decrypt it.

Leo: So that's why they need the SSL keys, because he doesn't have the keys for the stuff saved there. But if you have the SSL keys, can you then intercept the...

Steve: Well, all the mail coming and going, yes.

Leo: But could you read the drafts folder, too? I mean, doesn't that get fed into my browser? Or maybe not. I don't know. I don't...

Steve: Well, okay. But Ladar didn't have a web-based email system. He had a regular...

Leo: Oh, he didn't, oh.

Steve: No. Yeah, it wasn't web-based.

Leo: Then it's moot.

Steve: Exactly. Your client connects to his server...

Leo: Got it, got it, got it.

Steve: ...and off it goes, yeah.

Leo: But it would be secure for Gmail to do that unless you gave them your password.

Steve: Yeah. Yeah.

Leo: I'm not seeing it completely academically, you understand.

Steve: Yes. And Gmail supports secure SMTP and POP and client and web, I mean, Google really is coming up to speed and has been a leader in encrypting these things. And I think now we have a sense for a snapshot into how they feel about the fact that their encryption has been so badly dinged.

Leo: Yeah, yeah, oy.

Steve: And that's really all I have to talk about.

Leo: [Laughing] Wait a minute.

Steve: I do have some more things, but we'll do it next week.

Leo: We'll save those.

Steve: Yeah.

Leo: We'll save those. Very nice. Come on. "Ender's Game." Just one little thing.

Steve: Loved it.

Leo: Yeah.

Steve: Loved it.

Leo: I think if you read the book you loved it no matter what. Because it really was fairly true to the book, with one minor exception. And...

Steve: The problem I had was that, as always, I mean, this is true of anyone who's read a book and then seen the movie, is the book was so much richer.

Leo: Yeah, of course.

Steve: I mean, I almost felt...

Leo: But it has to be. It has hours.

Steve: I almost wondered why we were even introduced to Peter. I mean, Peter played a...

Leo: For the sequel.

Steve: Yeah, well, yeah, good point. Peter played a significant role in the first book, and we had him in one scene where he was just mean. And it was like, okay.

Leo: No, but they kept referring back to that. They said the reason Ender knows how to fight back is because he had a bully brother.

Steve: True. And Peter was washed out of the program because...

Leo: Too vicious; right.

Steve: Yes. He was, well, he lacked the empathy which - and it was Ender's empathy which made him a better commander because how many times did we hear that, when you really, really know your enemy, then that is to love them. So...

Leo: Right. That - I was glad that they made that the key thread through this.

Steve: Yes.

Leo: Because it does become important in "Speaker for the Dead" and the subsequent novels.

Steve: Well, yes. And I was surprised that the movie kept going. It went past the end of the first book into the beginning of "Speaker for the Dead." It was like, wow, okay.

[Speaking simultaneously]

Leo: ...sequel, it was pretty obvious.

Steve: I think that's very clear.

Leo: I wonder what people - I really wonder what people who didn't read the book made of it.

Steve: I wonder, too, because the other thing is, I mean, it was a large story to make into a movie. For example, I was telling Jenny, who did not read the book, but she saw the movie with me...

Leo: Did she enjoy it?

Steve: Oh, very much.

Leo: Oh, good.

Steve: She loves these kinds of movies. I'm just like, how did I find her? So, like, I mean, there was all of this battle competition where they were in a cafeteria in my mind's eye from reading the book where, like, there was a huge scoreboard showing all of the different teams and their rankings and placement.

Leo: And they showed it for a second.

Steve: It just, like, barely blinked on the screen. It was like, oh.

Leo: But those of us who had read the book knew what we were seeing.

Steve: Yes. They lived and died by that.

Leo: I think they only - they only had one or two battles in the simulator. Whereas in the book there are quite a few, and there's a lot more military strategy and all, it's...

Steve: Yes.

Leo: So read the book. I've told you this all along. And I cannot talk with you on the air without really spoiling things about the one difference...

Steve: No, we would never...

Leo: There is a significant difference that I cannot understand why the filmmakers decided to do it this way because it frankly lessens the impact of the movie. We'll save it for another day.

Steve: And I will also say, and you'll get a kick out of this because I was thinking - in thinking about this afterwards I noticed that the strategy, the physical strategy Ender used in one of those battles is exactly what he used at the end.

Leo: And it was nice to see that visually, envisioned, because I of course listened to it, and we envisioned it. But to see it, I thought that the - what did they call the battle, the simulation, the gravity-free simulation, the battle - anyway, to see that...

Steve: Oh, the Battle Room, the Battle Room.

Leo: To see the Battle Room brought to life was really great. Normally I'm not thrilled by visualizations of something that I've built in my brain. But the Battle Room is kind of hard to visualize in your mind.

Steve: Exactly what I imagined.

Leo: It was beautifully done.

Steve: Where they had things, you know, 'bergs floating around...

Leo: Everything's done perfectly.

Steve: Yeah, yeah. Oh, and visually, oh, Leo, the visuals were just spectacular.

Leo: Yeah, I was curious. See, Lisa and Michael and I saw it, and neither Michael nor Lisa had read the book, much to my chagrin. But I think they enjoyed it. Not as much as I think - if you've read the book, it's really worth seeing it, I think, yeah.

Steve: Yeah.

Leo: All right. We're done. The Battle Room is nothing like the ball pit at McDonald's. That's another pit entirely. Thank you, @bookery [ph]. Steve Gibson, as Steven Tiberius Maury Gibson, is the man in charge at GRC.com. That's his website for Gibson Research Corporation. You can follow him @SGgrc on Twitter, where he often tweets valuable links, as you can hear. You can also go to GRC.com to get 16Kb audio versions of this show for the bandwidth-impaired; full transcripts written by a human being, as well. You can also at GRC.com get SpinRite. You didn't mention

SpinRite this week.

Steve: I did mention - nope.

Leo: It is the world's finest hard drive maintenance and recovery utility, and you must have it if you have a hard drive.

Steve: Keeps the drives alive.

Leo: Keeps the drives alive. And lots of other great stuff. His passwords there and all that stuff, lots of insight. It's a really wonderful site just to get lost in, to wander around. You have so many links now, it's so deep now, it's really fun to go: GRC.com. We do this show on Wednesday at 11:00 a.m. Pacific, 2:00 p.m. Eastern time, 19:00 UTC. If you want to watch live, please do. We love having you in the chatroom watching live. I love just knowing you're there. But if you can't make it live, we always have audio and video on-demand versions, high-quality versions on our site, TWiT.tv/sn, and wherever finer podcasts are offered. I don't call it a podcast, but you understand. Thanks, Steve. We'll see you next week on Security Now!.

Steve: Thanks, Leo.