Three Hybrid Cloud Solutions

Description: After catching up with the week's news and Twitter feedback, Steve and Leo closely examine three remote cloud storage solutions whose Crypto was done COMPLETELY right, Offering full TNO (Trust No One) security. And one of them makes Steve wish he were a Mac user!

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-351.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-351-lq.mp3

SHOW TEASE: It's time for Security Now!. Lots of security news from Steve Gibson; I'm back; and Steve has found yet another cloud storage solution that's so good, he says it makes him want to use the Mac. Wow. It's coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 351, recorded May 2, 2012: Back to the Cloud.

It's time for Security Now!, the show that secures you, now. And here he is, the Securer in Chief, our Explainer in Chief, the man with the plan, Mr. Steven Gibson. Hey, Steve.

Steve Gibson: With his feet on the ground and his head in the cloud.

Leo: In the cloud. I want to thank Iyaz for filling in last week, did a great job. But I'm glad to be back. I missed you.

Steve: Well, and we missed you. And I'm so aware of how much I depend upon the continuity of our episodes because what you missed last week was really fun and interesting. It was, first of all, it was nominally a Q&A, but it was the first Q&A where I didn't even have a chance to open the mailbag. So god help me next week.

Leo: It was all tweets. All tweets.

Steve: Yeah. It was 21 tweets.

Leo: Wow.

Steve: It was our first fully Twitter-driven episode of Security Now! because there was so much reaction to the episode before that you and I did...

Leo: Right.

Steve: ...where we did this huge, quick survey of cloud storage solutions. And...

Leo: By the way, I got one complaint, and I'm just going to - I'm going to get you off the hook here about how I described Wuala. And somebody said, oh, you don't understand, you guys don't understand at all. And that was not you, Steve, at all. Steve hadn't looked at Wuala. It was me. So any errors committed in that portion accrue to me, and me alone.

Steve: Well, at least you pronounce it correctly. I have a problem pronouncing it.

Leo: Wuala.

Steve: You got that part right.

Leo: At least I got the name right.

Steve: So shortly after you and I recorded two weeks ago, a couple people responded, saying what about Backblaze? And I looked at Backblaze, and it was a classic example of really good people with good intentions doing crypto wrong. And they didn't apparently understand that they had done it wrong. And so I opened up a dialogue with the cofounder and CEO and made sure that I understood that they had done it wrong. And unfortunately I was right that they were wrong. And then so last week was basically responding to all kinds of the feedback that we had from the episode you and I did, and then taking a deep dive into what it was that they did that was wrong.

And just so you're up to speed, they haven't - first of all, it looks like a very nice company, good people. I have no reason to mistrust them at all. But what I tweeted was, after I looked at it, was they were not TNO. They were not Trust No One. Yet their documentation made that very unclear. They implied that users could add a password that would then encrypt their storage over at Backblaze. But in fact, the way they were doing this was completely broken.

They create a public key pair, an asymmetric key pair. You have the public key; they have the private key. When you encrypt something, the encryption generates a random key, a symmetric key, to encrypt the file. That's all good. But then it encrypts that with your public key and deletes the record of it, then ships it to them, to Backblaze, for cloud storage. At this point you can't decrypt it. Only they can decrypt it.

Leo: Whoops.

Steve: Oh, yeah, just nuts. And so then they say, yeah, but if someone uses a password, then that's safe. Except that you provide your password to them for them to use that to encrypt the private key. And if you ever want to look at your stuff, you've got to provide it again so they can decrypt the private key. So, I mean, the point is that it's all, like, wrong. They are the only people who can decrypt your data once you ship it to them. And even if briefly, they are decrypting it, and they have to decrypt it. So we went into that in some detail. And so it was, I think, a really interesting episode.

This week, one of the things that I said with you two weeks ago was that I could sort of see some pressure toward what I was calling a "hybrid cloud solution." We've got, as you know, since you and I were last together two weeks ago, Google Drive has announced and messed up all of our Gmail. Or Google Docs, rather. And Microsoft upped their free SkyDrive to 25GB for people who were already using it as, like, a loyalty bump. And so there are all these free services. And of course Dropbox is very popular, but we know that Dropbox is not secure. And in their privacy policy they explain that they'll make your data available to agencies that request it under court order and so forth.

So what I'm calling "hybrid solutions" are those where you want the features that these existing providers offer. For example, in Microsoft's case, there's all kinds of things - and Google applies, too, certainly - all kinds of things, special things that they can do when they can see your data. And many people want those features. But at the same time, it'd be nice to have a cubbyhole in that service where you can also put things that are just black. They're just black ops. No one and nothing can see into those. And so this week I want to look at crypto done right, as opposed to last week, where we saw how well-intentioned crypto could go wrong. Three apps, one of which is so good for the Mac that it makes me want to switch from Windows.

Leo: Wow, that good. Wow.

Steve: It's really nice, yeah. And we've got some neat Twitter feedback and news and so forth.

Leo: Excellent.

Steve: So we'll get into it. I wanted to note that v12 of Firefox is out. And that happened, that was announced on Security Now! last week. And what they did with v12, Leo, is they are - they've engineered around the user account control popup in Windows. They've got a process that they're able to start.

Leo: Really.

Steve: Yeah.

Leo: That doesn't seem like a good idea.

Steve: Well, unfortunately, this is - they're trying to get - and I agree with you. And I brought up that point last week because you'd hope that the bad guys can't somehow...

Leo: If there's a way to do that, we don't really want to publicize that.

Steve: So, but the problem is what - and we've talked about this before, where we know Mozilla is trying to go where Google has gone with transparent updates so that it's just continually keeping itself current and fixing problems on the fly without requiring any user interaction. So this, so v12, which is now out, is - it's not quite to automatic seamless updates. But they have now avoided the user account control so that they, presumably with proper protection, are able to update without providing you - without putting that dialogue in your face. And with 13, which is now in beta, they've finished that, or they will when it comes out of beta. The cool thing is that 13 enables SPDY by default.

Leo: Yes.

Steve: Yes. So we now have Mozilla's Firefox and Google's Chrome both with SPDY present, debugged, working, and enabled, which is a good thing. It'll put pressure on the remaining browsers because these guys - and of course it will provide additional incentive for the server side to bring up SPDY support, just to globally and in general support or improve cloud-based experiences.

Now, the other thing that I just saw is really interesting, also. We talked last week about how - or maybe it was two weeks ago because I think I remember discussing with you how, with Apple's Java fixes to deal with the Flashback trojan problem, they're now disabling Java by default. And if you reenable it because you need it, if you don't keep using it, it automatically re-disables itself.

Leo: Good. Re-disabled.

Steve: It goes to sleep again.

Leo: Time out.

Steve: Yes, it's like, okay, well, we're going to go back into protection mode. Now, what Firefox has done, and this has just happened, is they're proactively disabling back versions of Java. So if you aren't updating your Java, you can't use it because, I mean, they've been concerned enough...

Leo: Oh, that's interesting. Wow.

Steve: Yeah. Yeah. They've been concerned enough about the exploits, when studies are done that show the people who are not updating Java constantly being infected due to Java vulnerabilities, they're saying, look, we know that it's obsolete. Let's just - that it's a vulnerable version. Let's just shut that down. And if a user wants to use Java, you've got to update it. And so these are - it's unfortunate that we have to be proactive this way, but it's the only way at this point in our evolution of personal computing on the web to handle this. So I'm really glad for it.

And Kaspersky came out with the announcement a few days ago claiming that Apple is 10 years behind Microsoft on security. And I thought, huh, okay. And this was Eugene Kaspersky's log or blog. And I looked at it, and I guess I know what they're saying, but I disagree. Apple reaps a huge benefit from having the experience of Microsoft. Certainly 10 years ago Microsoft was getting a lot of arrows in its back. It was very slow to adopt the security practices that many people were asking of them. And you'll remember, Leo, I mean, we've been doing the podcast, what, for seven and a half years. How many times did I say, "Why do we have scripting in email? Why do we have scripting in email?" Because, I mean, it used to be so stupid that you could just - that you could receive email that would run code. And it took a long time for that to get fixed. And why is the firewall not turned on? Well, it took a long time to get that turned on. Well, it took a long time to get that turned on.

So what I think is, it is true that the whole ecosystem that Apple has is somewhere lagging behind. But it's not 10 years. And by the ecosystem, I include, for example, the users, who are going to have to understand that it's not the case that Macs can't get viruses. I mean, we know the 600,000 instances of Flashback that infected Macs demonstrate that, well, yes, they can. I mean, they're just computers. In this case, of course, it was a Java exploit that was allowing this stuff to get into them. So I don't think it's 10 years. I don't even know if it's right to put a timeframe on it.

But the good news is I know, even though Apple - I guess anyone is not responding as quickly as we want. We're not happy with Adobe, with anything Adobe does. And we'd like Apple to be more proactive. Flashback happened because they dragged their heels on updating their Java client for Safari, and for the Mac. And they learned the lesson of what happens if you drag your heels. And that was a huge black eye for them. So they may have to learn the lesson a few more times. But they have the substantial advantage of having seen Microsoft dance this same dance and learn from it. So I think that's good.

There is, if you click the link, Leo, you want to show people on the video side this next link at Ars Technica, wonderful and interesting browser adoption graphs.

Leo: Okay.

Steve: For our listeners, I also just tweeted this. So if you go to Twitter.com/SGgrc, up near the top of the feed is some really interesting graphs that just demonstrate over time what's happening with competition among browsers and how the user share is changing, and also some cool charts lower down showing, for example, we've talked about how Firefox's major versions have gone from glacial to almost too quick. And these really nice charts demonstrate and show over time just sort of the user population changes of the various browsers. And I just sort of liked it, so I wanted to bring that to our listeners' attention. I think everyone would get a kick out of just browsing through those and looking at the various percentages.

Leo: Yeah, especially as they change, yeah.

Steve: Yeah. Now, we know that one of the drivers, I guess the most reliable driver of investment in malicious conduct is cash. For the longest time, hackers seemed to be delighting in viruses, just doing them because they could. They didn't make any money. And that was one of the conundrums. People said, well, why are these viruses in our computer? What do they do? I mean, rarely were they really destructive, but they were just annoying. Then we began to see, as of course the web ecosystem in general of money, with Google demonstrating that you could make money with ads and so forth, began to create an economic model. There was a really interesting analysis by Symantec of the way the Mac Flashback trojan worked. They analyzed the ad-clicking component of it to understand what it did. And quoting from their blog, they said:

"The Flashback ad-clicking component is loaded into Chrome, Firefox, and Safari, where it can intercept all GET and POST requests made by the browser. Flashback specifically targets search queries made on Google and, depending upon the search query, may redirect users to another page of the attacker's choosing, where they receive revenue from the click. Google never receives the intended ad-revenue click. The ad-click component parses out requests resulting from an ad-click on Google search and determines if it is on a whitelist. If not, it forwards the request to the malicious server. Intercepted requests show a revenue of $0.08 cents for the click."

Based on the virulence and the number of machines that were known to be affected, and we know what that number was because remember that you and I talked about this, the crypto used to generate the domain names was reverse-engineered. And I think it was Kaspersky, I can't quite remember, somebody reverse-engineered the crypto, registered the domain name, and then for a while had all of the bots phoning in for directions and so was able to count them clearly. The bottom line, when you multiply this all out, is that that botnet was generating $10,000 a day...

Leo: Wow.

Steve: ...for the Flashback gang.

Leo: Wow. But it's not surprising. And doing so for something like five years.

Steve: So, yeah.

Leo: They made a lot of money. It's a profit deal.

Steve: This is a problem. This is a problem because...

Leo: Well, they had four million, at one point they had four million machines corrupted. So that's where - I'm sure that number comes from the maximum.

Steve: Yeah. And if you do the math, I mean...

Leo: It's not hard to figure out, yeah.

Steve: It's a lot of machines. And so there is - now this goes from script kiddies saying, oh, isn't this fun, to organized crime hiring computer professionals or black hat professionals to make this stuff happen. I mean, it really does - it changes it from a lark to a business model, if you can make $10,000 a day while it lasts.

And I did have a note here about all the controversy over Google Drive's Terms of Service. CNET called it a "toxic brew." And they said: "Google isn't about to make your private files public, but that doesn't excuse its sloppy terms of service." And I never got around to digging down and developing my own opinion over what I thought about that.

Leo: I could talk about this, if you want.

Steve: Yes, do.

Leo: You would think that Google would have learned because this happens every single time a service - even Firefox, Facebook. What happens is the lawyers say, well, look, Google, you're going to maintain copies of this. In order to share it, you have to maintain copies on your servers. So they write very broad language that says - and this is what Rafe points out in his article on CNET - that is kind of in conflict with their initial statement, which is we are...

Steve: Are on your side.

Leo: Yeah, we're on your side. You always own your content. We have no intention to publish it publicly. And in fact there's no facility within Google Docs to publish it publicly. However, in the language, the lawyers always take the broadest approach, which says we reserve the right to use this, copy this in any way, in any form, in any fashion. And furthermore - and I think this is probably what most concerns people - we reserve the right to use it to improve our services. And I think that people are always scared when they read this copy. And Google should have known. The point Rafe makes is they could have written it more narrowly. The point he's making is not that Google intends some nefarious use for this, but merely that this was sloppily written. But this is what always happens in all these agreements. We saw it with Pinterest. We see it again and again.

"When you upload or otherwise submit content to our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations, or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content." That's boilerplate. And they should have written that properly.

Steve: Yeah. In other words, our attorneys tell us that there's no way you can possibly

sue us, no matter what we do, based on what we've just said we might do.

Leo: They do then say, "The rights you grant in this license are for limited purposes of operating, promoting, and improving our services and to develop new ones." And they say at the very beginning, in a preamble, "You retain ownership of any intellectual property rights you hold in that content. What belongs to you stays yours." They try to address this. But by now they ought to know the first thing that happens when a new Terms of Service comes out is that...

Steve: Everybody looks at it.

Leo: Everybody looks at it, and the first thing they look for is that line that says, "We retain worldwide license to do whatever we want with your stuff." And everybody says, well, that leaves Google a giant barn door opening to steal our stuff. So while I don't think that's Google's intent, they really - by now you ought to know, guys, when you write one of these things, that somebody's going to look at it and complain. It's always the same. This is the same thing we hear every time because, remember, in order to put this - they have to - your content lives on many, many Google servers; right? And if when you share a doc with me, they have to make a copy into my thing. All of the things they're asking for the right to do allows them to do all that. They should have been a little narrower and say, hey, but this is just for this purpose. This purpose we won't expose it publicly, et cetera, et cetera.

Steve: Which actually that's a perfect segue into today's topic because today's topic is how to make something like Google Drive really safe.

Leo: Ah. That sounds good.

Steve: Yeah, because the idea is you want the services that Google can only offer, as you just said, by having some visibility into your data. But for some stuff you'd like to also be able to drop documents there where it actually doesn't matter what they say because they can't do anything with it. It just looks like pseudorandom noise to them. They can scratch their head. The only thing they could do is delete it.

Leo: Right.

Steve: But presumably they'd have no reason to do that. But they can't see into it. They can't check the copyright. They can't do anything. So that is why I think we're going to see hybrid solutions like what we'll be talking about today, where crypto is done right and you get the best of both worlds. You get all of the features that are only available if, for example, Google can index them, while you also have the option of creating a black box that they just can't see into.

Leo: Very cool. That's what we need.

Steve: So I have a new section that I'm just going to call "Notes from the Cloud" because I keep getting people tweeting me, hey, how about this one, and how about that one? It's like, oh, my god, there's just an endless number.

Leo: There really are. This is a very popular category.

Steve: Yes. And so my goal, just so that people aren't glazing over as they listen to yet a third episode on cloud storage, which is what we're going to do today, is first of all, obviously, we're not covering the same territory week after week. We're taking different aspects of it. My goal is partly to make me focus on this so that I'm able to develop a more mature understanding of what's there because our listeners want to know. And I have to know in order to translate this into, okay, well, is this crypto right or not? And also I'd like us all collectively to get some sense for the state of the art in what is clearly going to be a very important segment in the future and where, arguably, security is one of the most significant things, which just happens to be the topic, the overriding topic of the podcast.

So I got a note from Terry Holman, who tweeted - @terryholman - about something called Symform.com. And what I know about it is only enough to just say - I just sort of wanted - these are just little bullets that, if something I say scratches somebody's interest, then they can go look because this thing is free for up to 200GB. It's plain and simple storage sharing. You get as much as you share. So that's not for me. I don't want that.

Leo: That's the Wuala model. Which, by the way, Wuala apparently has kind of turned its back on.

Steve: Backed away from, yes. What was cool about Wuala was that, as we discussed briefly, is they did a sophisticated - they had a sophisticated system. But it sort of came out of academia, too.

Leo: Right, right.

Steve: I mean, it was sort of like, could this sort of thing work? The idea being - I described it as like a RAID array where, in a RAID, you've got redundancy built into all the copies so that several of them could disappear, and you could still reassemble the whole. So that was sort of a cool academic concept that somebody said, hey, let's sell this. And that's what they're doing.

My argument with them is that they're Java-hosted, and they're making money. And I just think, how hard is it to write a native client? Write one for Windows and write one for Mac. Now you're done. Instead of, like, forcing everyone to have Java installed in order to run your cloud backup service. I mean, if it was free, okay, maybe. But you're making money. So hire a programmer who knows Windows and hire a different one who knows the Mac. Give us a real client.

Leo: That's a good idea. Yeah, yeah.

Steve: Anyway, so Symform.com. If you like the idea of free storage or free backup for up to 200GB, you want 200GB remoted from your machine, you're willing to give as much as you get, then this looks like an interesting service. I don't know anything about it beyond that. So there. And then, oh, my goodness.

And here's one from Craig Schappacher, who tweeted about SMEStorage.com. This thing, my eyes just glazed over with its unbelievable range of options. They say "Manage all your cloud files in a single unified view." You can get, for example, Google's free storage, Microsoft's free storage, Dropbox's free storage, everybody's free storage, and then this thing will hook into all of them at once and aggregate them. So you don't have to pay anybody for over what they offer you for free, yet you get redundancy. It can copy between them in case those go down. And it's able to sort of give you a merged result. And they've got every platform, also. Linux/Windows/Mac for desk drives and for synch, and iOS/Android/BlackBerry/Windows Phone 7. So it's SMEStorage.com. And just wanted to let people know about that, also. But no deeper dive at this point.

And then a couple things from the Twitterverse. Brian Hall, who is a - he's described himself as a husband, dad, geek, and IT professional, also the creator of WishyBox, WishyBox.com. He described it as a "simple, free, universal wish list" of some sort. I didn't go there to look what it was. But he says, "Why is it so hard for online synching and backup services to enable client-side pre-Internet encryption?" And he also tweeted, "If an online backup/synching service were to enable pre-Internet encryption, would that break synching between different machines?"

And I liked this because it highlighted where we're going to go today, which is, if you pre-Internet encrypt, then you are only giving the service completely opaque blocks of data. They can't do anything with it. If they have an intelligent client at your end, and you make changes, they could see that only parts of the blocks changed, and so not be re-uploading the whole thing. If you were to compress it first, the problem there is that then small changes tend to propagate through the rest of the file, causing you to upload a lot of information redundantly. But sometimes, if you've got the bandwidth, these things don't have - they're free for upload. So it definitely is a tradeoff.

As for why it's so hard for them to do the encryption, I can only say that that's a bit of a mystery. I think our audience is, by its nature, in the same way that our audience is over-concerned, for example, with Internet tracking, we're maybe over-concerned with Internet security. Some people just want the backup. They think, hey, no one cares about my photos and my docs.

Leo: Yeah, that's kind of how I feel.

Steve: Yeah.

Leo: And I don't put anything there that I don't want anybody to see.

Steve: Well, and, see, I'm willing to because, given that it's encrypted, I understand it really, really, really cannot be cracked. And so, yeah, it's both ways. We have all that Google, I mean, we have all these docs up on Google Docs. It's super convenient that I can put them up there, you can grab them. We don't care if anyone looks at that stuff. It's just - it's public anyway. So there's certainly applications for it being wide open and unencrypted. Yet at the same time, people are considering, like, backing up their whole

hard drive. And there is stuff there that they would not like to have get out.

I think I'm going to skip some of these, wonderful and tasty as...

Leo: They're all wonderful, but...

Steve: Yes.

Leo: Yeah.

Steve: Oh, there is one thing I wanted to mention. Because we're recording today, today, apparently May 2nd only, so people who get the podcast...

Leo: I did it. I did it. I did it.

Steve: ...or are listening live, Amazon has reduced the price of the Kindle DX, $120 off today.

Leo: Off?

Steve: Yes.

Leo: Oh, wow. Do I want one? You have one. I know you love yours.

Steve: I have one. I got one off of eBay for Mom because I wanted her to have a white one that's no longer available. She loves it. I do all my reading on it, despite the fact that I have every other one they make or have ever made. I just like the bigger screen. I like having more text on there and paging less often. It's not like I don't like to page, but I don't know, it just - it feels right to me. And I got a couple tweets back. I tweeted this, so anybody - there is a funky link that you've got to use to find it, so it's in my Twitter feed - again, Twitter.com/SGgrc - and you'll find it there. It's May 2nd only. They're calling it a Mother's Day, pre-Mother's Day offer, just for today. And so it brings the price down, with their leather cover, to $299. I mean, so it's still pricey compared to the $79 one. But normally it's north of $400. So anyway, I just wanted to let people know in case they're interested.

Also, for those who loved the Lost Fleet series, Robert Spivey tweeted: "Hey Steve, you should mention for the sci-fi fans on Security Now! the latest 'Lost Fleet' book was released on 5/1: 'Beyond the Frontier: Invincible.'" And yes, my copy came yesterday. So I do indeed know. I don't know when I'm going to get to it, though, because I'm deep into health stuff at the moment.

Leo: We should mention, and since you said the word...

Steve: Okay.

Leo: ...that in order to protect the gentle ears of you, our listeners, we're not going to do any health stuff on this show. But Steve is going to do a health special this week.

Steve: Yes. Something since I last talked to you, Leo, two weeks ago, I have had some amazing stuff happen, completely unexpected, completely - I just didn't expect it. I figured out what was going on. I dropped the reading I was doing, switched to something else, have been deep into some new research. I have stats and numbers and something really, really cool. We'll be able to tell people what it was next week. But you and I are going to do a special on Sunday for an hour at 2:00 p.m., between 2:00 and 3:00, from the end of your Tech Guy show and before the beginning of your Sunday TWiT program.

Leo: Yes.

Steve: And anybody who's interested in health stuff, all I can say is you will not be disappointed. This is - and Leo, we're going to have fun.

Leo: Oh, I can't wait.

Steve: I would say it's - the reason I don't think it's necessary to preempt Security Now!, as I did once for the Vitamin D episode. I felt better about that because all I was asking people to do was take a pill. And anybody can do that.

Leo: This is more serious now.

Steve: This, well, this requires you thinking about if you want to do this. But I am never going back. My life has been changed. My life has been changed forever. I'm not kidding you. It's been changed forever.

Leo: Wow.

Steve: And I think yours will be, too, because you're the kind of guy who'll be willing to try this. I'm going to give you the motivation based on what I have learned and what has happened to me that I have measured and documented. And I know we've got listeners who will, if nothing else, find this interesting. And maybe it'll plant some seeds. So we're going to do an hour-long special, the second special about my interest in and hobby in health.

Leo: And we should, well, we'll have all the disclaimers at the beginning of the show on Sunday.

Steve: Of course.

Leo: But tune in, 2:00 p.m. Pacific, 5:00 p.m. Eastern. That is 2100 UTC on Sunday. And Steve won't tell me anything else. It's a surprise.

Steve: Okay. I did want to reiterate something because several people have loved what I stumbled on. I don't know if you know, Leo, that there is a really fantastic web interface for TweetDeck now, web.tweetdeck.com. And it looks exactly, I mean, it's like - it's amazing. And Iyaz just, well, he's no fan of TweetDeck. I guess when they updated it or when Twitter bought it, he lost all of his column settings, and that pissed him off, and he abandoned it. But a number of people agreed with me, saying it is really impressive. I'm just - I look at it, and I'm amazed what we can now do with HTTP. I mean, it runs on - I ran it on Firefox and on Chrome, just as my two browsers that I normally use most. Oh, and IE. It's TweetDeck on a web page, working perfectly.

Leo: Yeah, it is amazing, isn't it.

Steve: So, wow, yeah, I'm just very impressed. Okay. Now, sci-fi update. I tweeted, "Am I the last person to know about this?" And...

Leo: No, I am, actually.

Steve: I think, oh, my god, Leo, this thing looks unbelievable. This is Ridley Scott, who gave us, of course famously, the first "Alien" movie that blew our minds, has done a prequel. And if anybody is interested, it's called "Prometheus." IMDB.com, Internet Movie Data Base, it's right on - it's on the home page of IMDB.com right now, the latest trailer, which is about 2.5 minutes long. And careful, though, because, I mean, it is a spoiler for people - I tweeted this, and I got some people saying, wow, more than tidbits, there's a lot there. But, oh, my god, it looked, oh, it's June 8th is the release. So we don't have to wait forever. So I'm almost glad that I'm the second to the last person to know because otherwise it'd be one of those, like, oh, yeah, in 2014. It's like, oh, well, great. It's soon. And, oh, it is - oh, well, I've said enough. IMDB.com. It's called "Prometheus." It's all over YouTube, lots of really good trailers. And it just looks fantastic. So I'm really pleased.

Oh, and "Chronicle" comes out for release on disk next week, which was the sci-fi movie I did not see in the theater because I assumed it would come out quickly. That's where the three or four teenagers go walk, see a hole in the ground.

Leo: Yeah, I want to see that.

Steve: And then they - something happens, and then they start acquiring superpowers. But this is sort of like the dark side, like what would happen if Henry had superpowers, Leo.

Leo: [Laughing] Noooooooo. Okay, go ahead. Henry's my son, for those of you who don't know. And he does, he thinks he has superpowers, anyway.

Steve: You can imagine that might not turn out so well.

Leo: No.

Steve: Yeah. So, yeah. If there was nothing to restrain him, if he actually could do anything he wanted, oh, all hell would break loose.

Leo: Well, you know, he has been studying UFC kickboxing and mixed martial arts. So I'm terrified of him anyway. He practically does have superpowers. I think he could kill me with a look, if he decided to. But don't tell him that.

Steve: So I did want to say to people, I've had a number of people say, what was that book that Leo liked so much, that you recommended? So I just wanted to - we're not going to spend any time on it, but it's "Deadly Harvest" by Geoff Bond. I like it as much as I did. I think it's the place to start for understanding, for acquiring a really solid view of an approach to diet. And what we'll talk about, you and I, for an hour on Sunday, is some surprises that, I mean, that really, like I said, probably have changed my life forever.

Leo: Wow. But you're not eschewing what we have learned.

Steve: No no no no no no no.

Leo: Okay.

Steve: No. This is all - it was an interesting catalyst and...

Leo: But you've gone beyond now.

Steve: I've really gone - I've gone where many people have gone before, but I'm staying here.

Leo: Okay. Good. I need something, so whatever you say, I'm doing.

Steve: I think you and others will say, wow, that works? I'm going to try it. Speaking of what works, I got a note from John Newcomb, who said, "SpinRite Kudos. Dear Steve, just wanted to tell you how much I appreciate you for all the great info I get from your podcast with Leo Laporte. You have such a wonderful radio personality, and with Leo, you

guys are a great team.

"I recently bought a copy of SpinRite that I have added to my bag of tricks. I'm a computer tech and work for a company who serves the dental industry. SpinRite has already saved me a lot of time. I was in an office the other day working on a machine that would not fully boot Windows. So I ran SpinRite, and it recovered several bad sectors, which then allowed me to image the drive, which I couldn't before, and install a new one. Thanks for making my job so much easier. Your software works so well. In using it and observing all the little details, I think it's clear how much care you put into it. Sincerely, John Newcomb, Oakland, California." So, John, thank you for sharing that with me and our listeners.

Leo: And as I remember, we're going to take a break for our Carbonite ad, and we'll get to your new three cloud solutions, including one that makes you want to go to the Mac.

Steve: Oh, Leo. I think this is the one for you.

Leo: I'm going to have to rethink. I've got Google installed, a Google Drive installed now. And I've got SpiderOak. You're going to throw me a curve. All right. All right. I'm ready.

Steve: Okay. So I went off a little half-cocked about this one, okay, because I loved the cleverness of their crypto. This is one called Cloudfogger from some guys in Germany. Sort of a funky name, like foggy clouds, or the idea being that it obscures what's in the cloud. It's Cloudfogger.com. And I tweeted about it. Bunch of people looked at it. And then when I actually tried to use it, I was a little put off, only because it's very new. And while the crypto is done right and cleverly, it just doesn't feel very mature yet.

For example, a Windows application has to be multithreaded so that there's a user interface thread which keeps the user interface alive while other threads are busy doing stuff in the background. This appears not to have that. So that what it, for example, it is an encryption utility - all three of these are encryption utilities where they allow you to create a virtual drive on your machine which maps to a folder somewhere else. And that could be a folder in the cloud. So, like, a folder in your Dropbox, or a folder in your SkyDrive, or a folder in your G Drive. And the idea being you don't mess with that. You mess with the virtual drive. Anything you put into the virtual drive, it seamlessly encrypts and places in this folder, which then the cloud service says, oh, there's a new file in the folder, and then it separately sends that off to the cloud.

So they, for example, don't allow you to, as they're setting it up, tell it where you want to install. Which really annoys me. It just puts it under Program Files > Cloudfogger. But I've got my hard drive organized differently, so my categories of subfolders under a different directory. And so I like to be able to say, oh, this goes under "Cloud." I have a new category, even, called "Cloud," for cloud stuff. But I couldn't do that. It also, by default, assumes that you want to map "X" as your drive, doesn't give you a choice. But I already have "X" mapped for something, and "W" is a map I already have. And so it worked its way back up to "V," which was the first one free. But it took forever.

Meanwhile, this single thread in the user interface just locked the whole thing up. It's like it - and I'm sure Windows users have seen where up in the title bar it'll say "not

responding" because Windows at some point realized that users would be confused by this, by the fact that the app was not really well written for interaction. And so Windows takes responsibility for posting that into the title bar if the app is no longer coming back and picking up events from the UI event queue.

So these things can be fixed, and I think they will be. It's only Windows, currently, and actually I put "Windows (sort of)" in my notes, and "Android (sort of)." But so they have those. And it's going to get better. And they're promising Mac OS X and iOS. So that's hopefully going to come.

And for me, I let it sit there for a couple days and noticed that it used up a quarter gig of memory, and it was sort of silently creeping up. So I posted an update in Twitter saying, whoops, this things seems to be burning up RAM. And I got some people who said, well, I'm under Windows 7 x64, and it's not doing that for me. And I did see other people say, yeah, me, too. So there's some things that they need to deal with.

Also, I was thinking of, when you were talking about the end-user license agreement problems, they also had a little problem with their EULA. There was a Paragraph 10 that everyone started tweeting about, actually after I brought this to everyone's attention, because it was one of those overly broad, everything that you have is ours statements, which they immediately fixed and backed out of and blogged, we're sorry, we didn't really mean it, we just weren't thinking, blah blah blah. Same sort of thing.

But their crypto, their crypto is right, and the crypto is clever. They've solved a couple problems in a way that no one else has, that I liked. So let's get a little techie for a second. This is file-by-file encryption, when you have them encrypt a file because you drop a file onto the virtual drive. So what you're dropping is a file in the clear, so-called "plaintext" in crypto speak. They use a pseudorandom number generator, and they're using a very popular crypto package. It's [Crypto++], if memory serves me right. I think it's [Cryptopp.com], in fact, is the site. It's a well-vetted, nice, good choice for a crypto library. So they use a pseudorandom generator to generate a 256-bit AES key. So that's randomly generated. And that's the key that they use to encrypt the file. So now the file is unreadable, and we've got this key. When you install the system, they generate a public and private key pair. And the symmetric key which they just - this random symmetric key is then encrypted using your public key so that now the only thing that can decrypt it is your private key. And that's yours to have and to hold.

Now, the cool addition is that you're able to share this with other users of Cloudfogger. So you can set up a community - oh, and I forgot to mention, this is free, 100 percent free, currently. What they say on their site, and I'm sure they'll honor this, is that, if you get it now, what it is and what it does will always be free for you. And it's unlimited size, no random, arbitrary, we're going to make you pay if you're over 2GB or something. So it's completely free. It's one of the reasons I liked it so much was my sense is that, for this class of application, it ought to either be free, or it ought to be pay once. I can't see somebody saying to just do this we want you to pay X amount of dollars per month. That's just not enough. It's like, what, and then also pay the cloud storage provider whose storage I'm using? That doesn't make any sense.

So this is free forever. Their plans are they're wanting to promote this and to establish themselves because they're very new. And then they'll offer additional features. We don't know what. They're not saying what. But that you may have to pay for, only if you want to. What they are offering now, if you get it, you'll never have to pay. So I think that's cool. And I'm sure they'll mature this over time, get more platform support, fix their little Windows UI problems. I mean, it works. Many people played with it after I tweeted about it and had no trouble.

So what's clever is that, if you want to share this with people, then the symmetric key which is used to encrypt the file can also be encrypted with other people's public keys. So, for example, if I want to share this with somebody else, I get their public key through the system, and I encrypt this 256-bit symmetric key with their public key. Now they're the only people who can decrypt it. But the file can have multiple of these public key encryptions in its header. So essentially you very easily, very nicely, with full TNO, full Trust No One security, you can specify which of your group you want to be able to give access to. And since they have the matching private key that allows them to decrypt this, and only they do, and we know how asymmetric encryption works, that is, public key encryption, you encrypt with one, you decrypt with the other, and that's the only way it works. That gives you really nice access control, and the file is then stored in the cloud, wherever you want it to be. And you could control who has access. So I really like it. It's simple, and it's done right. Now, one very clever part is they solved the problem of password recovery. The problem that, as we discussed last week, that - god, I'm blanking on the name.

Leo: Backblaze? Backblaze.

Steve: Backblaze. Thank you, yes. The problem that Backblaze had is, when we were discussing why they did this, the cofounder and CEO said, well, yes, Steve, it's very nice if you have TNO, but then the problem is password recovery. Users who lose their password are, like, they're screwed. There's nothing anyone can do to get it back. And I said, well, yes. There's some responsibility that comes with that. And they said, well, we've decided that we'd rather make it possible to give them their password back. Yeah, by asking for it. Okay.

Leo: Now, that's fine, and then you have the choice, that's all, if you want to do that or not. Right? If you're the kind of person who loses passwords, and you want Backblaze to have access to your password and files, then you choose that.

Steve: Yes. And the problem is they - Backblaze tells you that you can password-protect it. But the way that works is you give them your password, and they encrypt your private key on their server with your password.

Leo: In their defense, this is a very common choice. Lots of companies do this, including Dropbox, by the way.

Steve: Yes. And I did say that their security is better than other people's. It's just not TNO. It doesn't survive the test of does plaintext ever exist outside of your system, systems under your control, and does any secret that is important ever exist outside of your control? And unfortunately, both of those they fail. So TNO says those will always be true.

What Cloudfogger does is clever. If you want to enable password recovery, if you're worried that you might lose your password - and I just don't know how that's a problem. But again, if Jenny were using this, maybe that would be a problem. She'd say, oh, I forgot what I used. It's like, okay, well, now we're in trouble. What they do is they hash your password, and they have secure password hashing. We've talked about doing that 10,000 times in order to make it a slow process. They hash your password into a 256-bit

hash. They take half, they split it in half, and they take 128 bits of it. And that they save. You keep 128 bits on your system.

Now, remember, this is the after-hash password. So you're entrusting them with 128 bits of the hash after the password is hashed, and then the other 128 bits is stored on your system. Then if, at some future time, you can't remember what password you put in in order to generate all 256 bits, you scream for their help, and they say, okay, we will mail you our half to the email address registered on your account. So they use an email loop to provide some security. But they're only giving you half.

And remember, 256 bits today is overkill. 128 bits is just fine. So they're only getting half. But the beauty is you need both halves. So when this comes in through email, that 128 bits is merged with the 128 bits you still have to have on your machine. That generates the 256-bit result of hashing your password and gives you access to all your files, and then you can change your password.

So I thought that was very clever. It's a means of they never have the whole thing. You don't even, on your machine, have the whole thing because otherwise the danger would be somebody else could tinker around with your machine and get access to your files with no password. But and clearly, if somebody has unfettered access and can do the email loop, then there is that problem. So you don't have to do this. But if you want to enable it, it's a clever compromise. But still, in a way, for example, that Backblaze doesn't do correctly, these guys did because they can help you recover, but they still never have enough to decrypt your files.

So anyway, my sense is that it works, it runs under Windows, eh, not ready for primetime, but it's brand new. And so I cut them some slack. We'll keep an eye on them. We'll see how they do. They're going to develop for multiple platforms. But their crypto is good. They've got good, solid crypto.

Leo: Again, that's Cloudfogger.

Steve: Cloudfogger.

Leo: Cloudfogger.

Steve: No. 2, BoxCryptor. I talked about it briefly two weeks ago, but just sort of glazed over it. I have since looked at it. And I am very impressed. This is very mature feeling, very nice guided setup. Oh, one thing about Cloudfogger that I wanted to also remind myself to tell you guys is, due to the way they're doing this, filenames are visible. And that's a problem. So, yeah. So they put their own extension on the filename in order to disambiguate it from those that aren't their extension. And a number of people tweeted back, hey, my filenames are visible. Well, that's a fundamental limitation of their approach. And I don't know if they're going to fix it, or if they can. But leaking filenames is annoying. So, and the reason I've just remembered is that BoxCryptor doesn't.

There is a project that somebody worked on over in the Linux world called the Encrypted Filesystem, EncFS. Wikipedia has a page about the encrypted filesystem. It's a nicely designed, generic, well-documented, cryptographically secure and cryptographically encrypted filesystem. The clients are Windows today, and iOS and Android. And they don't yet have their own clients. But for Mac and Linux there are existing encrypted

filesystem drivers. So, for example, if you were a multiplatform person, you could arrange to mount the BoxCryptor encrypted filesystem so your Mac or Linux machine could see it. But I would not advise it. I would wait for the third solution that we'll be talking about next, if you're a Mac person, because it's the one...

Leo: He's such a tease.

Steve: It's the one that makes me want to switch to Mac, it's so beautiful. For Windows, this is really nice. I've got it running now. I'm impressed. It feels smooth. For free, you get to play with it and to create one virtual drive. I don't think there's a limit on its size. But it's got me wanting to pay. And again, this fits my model for a hybrid solution. You pay once. It's not expensive. I think it's $29. Or I think there's two versions. I think there's a personal and a commercial version. So you pay once for Windows, and this allows you to create a virtual drive. It walks you through the process. They do have iOS and Android viewers, so you're able to use those clients in order to see into your encrypted drive for cross-filesharing.

So I like it very much. There's an advanced mode where you can do some funky things. For example, you can have different passwords for different sets of files in the same encrypted filesystem so that you could arrange to give other people access to parts of your data. And it's all explained. They've got good documentation, nice PDFs for their Windows, for their iOS, and their Android client. And I like it. So I did want to do it justice because I sort of just glazed over it last week. We were doing the alphabetical order, and it's "B," for BoxCryptor, so I looked how far we had to go, and I thought, well, can't spend much time on this. But I've now used it. And I think they've done a great job. So if Windows, iOS, and Android fits, take a look at it. I see no downside. And it does encrypt your filenames.

There's a little bit of leakage inasmuch as you can get a sense for the length of the filename because it has to be padded out to the block size of the encryption. So, for example, I created an !.txt file, and it created a little blurch of pseudorandom characters that were, like, 9 or 10 long. And if I went beyond that, then it jumped it up to 18 or 20, whatever it was.

And there was one other thing. They're still working on support. The encrypted filesystem uses the entire pathname of the file to initialize the encryption for the file and the filename. Their current implementation - and that's called IV, initialization vector chaining. Their implementation doesn't have that yet. So the same filename in different subdirectories has the same cryptographic name, which is like a little annoying. It'd be better if that were different because, I mean, it does tell you that it's the same named file, even if it's different contents. But that's the kind of thing I think they will probably fix moving forward.

So I like it. You can play with it for free and pay for it once. And you've got very solid-looking - oh, and I forgot to mention. When you pay for it, then you get to add drives. So not just one mapping between a virtual drive and a remote folder, but multiples. So if you were using Google Drive and Dropbox and SkyDrive, you could set up different drives and have things scattered all over the place and really confuse yourself. And finally...

Leo: I've been waiting.

Steve: The company is Haystack Software. I think it's a guy or gal. But, I mean, doesn't have a feel of a big organization. And I don't care because he's nailed this. The product is called Arq. And I just tweeted about it so that our listeners, our Mac users could find it. Actually it's funny because I said, "The deeper I dig into this, the more I'm impressed and the more I wish I was a Mac user." And of course you can imagine what came back. It's like, Steve, it's not hard to switch. Steve, it's - just give it a try, Gibson. And it's like, no, I mean, I'm a Windows developer, so I'm stuck here.

Leo: You're stuck. He always says, folks, until he retires, and then...

Steve: Yes.

Leo: Then he can go Mac.

Steve: Oh, my god, I'm so impressed with the Mac. I like it so much more. And Leo, I'm...

Leo: It'll be very different by the time you retire, I just want to say, Steve. We don't know where it's headed.

Steve: Yeah. Someone even warned me, someone said, Steve, you'd better switch now before OS - I think he said OS 9, but that couldn't be.

Leo: He meant OS 11. I think really it's the iOSification of the Mac that we're all worried about.

Steve: Ah, yeah, that's not good. I just - I've come to a formal decision, also.

Leo: Oh?

Steve: I'm never leaving XP. Not even when my three years are up.

Leo: 7's nice. You don't like 7?

Steve: Not even when my three years - no. XP, it's like, it's still in my way. I've tried to get used to it. It's like, there's just nothing I need over there. So...

Leo: It's not supported at all, of course.

Steve: [Indiscernible] down, yeah. Well, it is for three years.

Leo: Yeah. Then you're going to have to make a decision.

Steve: Yeah. I've already made it. I'm not moving. I'm unplugging. We'll set up a telegraph, Leo. Okay. So Arq for the Mac by Haystack Software, HaystackSoftware.com/arq. One-time purchase of $29. It is a beautiful frontend for Amazon's S3 service. And of all of these providers, I just - I like S3. I mean, Amazon is huge. 99.9999999 percent uptime. Any two Amazon datacenters can completely evaporate. They could just disappear, and nothing gets lost. Amazon's doing a good job. You pay Amazon. So you have an S3 account. You pay Amazon.

Amazon has dropped their price, by the way. It used to be $0.15/GB/month. Now it's $0.125/GB/month. And they dropped their upload transit. So there's no fee for uploading. And I mentioned last week, probably the week before also, that I love that because it allows me to send stuff up, to be like continually updating images of my systems with no cost. It's not until I need one that I pay anything. So I just really like it. The guy did a beautiful job of his Trust No One security. He has the full crypto spec and documentation published on his site. There's an iOS app called ArqView for the iPhone and iPad that gives you obviously shared access to it. There's even a command line version which is open sourced and available. So you can see how it works.

Now, one thing that gives you a sense for the thoroughness of this guy is there's a completely independent guy, Nathaniel Gray, who is N8Gray.org. He's got a bunch of crazy stuff on his site. One is called Backup Bouncer. This is an independent test suite for Mac backup utilities to see if they get it right because there's - it's one thing to have the actual file contents. And everybody is obviously going to get that right. But the metadata is often equally important. It's user access...

Leo: It is on the Mac because the Mac relies so much on metadata.

Steve: Yes. Permissions, ownership, timestamps, symbolic links, ownership of symbolic links, hard links, resource forks, finder flags, finder locks, finder creation data, BSD flags, extended attributes, access control lists, all of this stuff. So this guy, he says on his site: "Hey there, OS X user! Do you back up your files? Of course you do. Right? Right?? But do your backups work? Really? Are you sure? Have you checked? Backup Bouncer" - and it's free, of course - "is here to help keep the ugly backup tools out of the club. It's a command line-based test suite that makes it easy to find out how bad (or good, if you're lucky) your backup software is. It aims to be a comprehensive test for preservation of all OS X file metadata. The initial release tests for preservation of" - and then he's got a list of stuff that I partially read just now.

And he says, "Backup Bouncer can do many things to make testing easier for you. It can create test volumes; populate them with interesting files; run a test suite of popular and not-so-popular commandline copiers including cp, rsync, tar, ditto, pax, and xar; verify the results of a copy, either from its own test suite or your favorite command-line or graphical tool," blah blah blah. Anyway, only two backup solutions pass: Arq and Jungle Disk.

Leo: And they both go to S3. Actually, Jungle Disk, now Rackspace.

Steve: Right.

Leo: This sounds like kind of the new Jungle Disk for the Mac.

Steve: I think it is. I really like it. One-time purchase, 30 bucks, actually 29. And I like - I'm liking S3 on the backend just because nobody's bigger. Nobody bigger is going to buy them. I mean, this is what happened to Jungle Disk is they got bought by Rackspace. And Dave left. And so the developer's gone. And it sort of feels a little bit like it's maybe wandered off course. It hasn't been updated for a long time and so forth. And there are people who are having problems with it and having a hard time getting the support. So I really like this. I think this is for - if S3 makes sense for you, that kind of storage pricing, where you only pay for what you use, and...

Leo: You know, I'm impressed by this. They have a - when you install it, it has a little S3 storage budget calculator. So you could say, well, I want to spend $10 a month. Well, that's 71.43GB. Okay, well, I want to spend $5 a month. Well, that's, oh, I have to go back. That's 35.7GB. So you can actually figure out - and it will delete older backups to keep your costs within that budget, which is something Jungle Disk never did.

Steve: Ooh, no.

Leo: I really like that. So you can say, well, I'm going to spend 20 bucks, so I'll get 142GB.

Steve: And then it'll automatically manage that for you.

Leo: Yeah, it'll delete older stuff. You can also - you're right, he knows the Mac. He knows them. He's paying attention. And you can say "Backup my home folder except caches, logs, and trash," or manually add. It has drag-and-drop, which is very nice. Yeah, I agree with you. This is quite nicely done for people who want to use it on the Mac.

Steve: Yes, who want a solution as a frontend for S3. Yeah, and I like it that, I mean, you buy it from him. Amazon's not going anywhere. No one's going to buy them. They are rock solid cloud storage. And this makes it secure because, again, the crypto is done right. Strong crypto, all performed on your own machine, on the client. Nothing but pseudorandom noise goes up to Amazon. Amazon doesn't know what you're doing. It just knows, okay, I've got a bucket of bits that looks like scrambled noise. Like it.

Leo: Right. This is nice. And it's 30-day free trial, so try it. Of course, it's not free. The Amazon will start charging you immediately. But...

Steve: Actually, apparently, Amazon's got 5GB free for a year.

Leo: Ah.

Steve: Yeah, he mentions that on that page. AWS from Amazon, free 5GB for a year. So, although you have to have an Amazon account, and so that gets you over to Amazon. But who doesn't? I mean...

Leo: And of course Amazon today, knowing that you were going to do this story, released an app for their Cloud Drive Solution, so for Macs and PC. So...

Steve: Eh, it's Java-based, Leo.

Leo: Is it? Of course it is because it's cross-platform, yeah.

Steve: Yup, of course it is, yup.

Leo: So obviously this is a category everybody wants to be in.

Steve: Yeah. And again, we're not going to beat this thing to death. But I wanted to spend this time to give people, like, an overview. Certainly cloud security matters. And I'm hoping, I mean, I know that we have some effect, at least on the little guys, that is, this podcast does, because I've gotten feedback from everybody. I mean, it matters. And I just want them to do the security right. It's just not hard. It's just - mostly it takes caring about it. All the technology is there.

So I want to wrap up by talking about this compared to TrueCrypt because TrueCrypt is the granddaddy of filesystem encryption. And there's been some confusion about how these types of solutions interface with TrueCrypt, and how TrueCrypt can be used in the cloud. And TrueCrypt is fundamentally different because TrueCrypt, the way you would use TrueCrypt in the cloud is you would create a container file on your hard drive, and this would be a fixed size. So you need to allocate 10GB, which once upon a time was insane, but now we all have terabytes. So you create a container file to hold the filesystem. Then you use TrueCrypt to encrypt the filesystem in that container file. And then you put that container file in the cloud.

Now, once, initially, you're doing a 10GB upload, that is, the entire container that is a TrueCrypt filesystem goes off to the cloud, 10GB, there it goes. Even if it's empty, 10GB because, when TrueCrypt encrypts it, it turns the entire thing into noise. It all looks like it's got data in it. So off it goes, 10GB. Once it finally gets there, then, if we assume that your client, the client that's managing this cloud service for you, is intelligent, and lots of them are, they're only going to update tiny portions of this large file, if that's all that changed. Almost all of them that have matured look at the file that they've got versus the file that you've got. And when you make a few changes, they only send those up.

So the beauty of TrueCrypt is that, when you make some changes in your TrueCrypt volume, it's like sectors or clusters on the hard drive. Only those clusters that are about the files you're changing and the metadata, like the directory system and timestamps and things, only those change. So they're relatively small incremental changes to the

whole 10GB, for example, TrueCrypt volume. And those get shuttled up to the cloud, and then you're synchronized.

Now, the problem with TrueCrypt is it really wasn't designed for this application. We're sort of stretching it that way. And I have heard, and I have said, and it's since been confirmed, that you cannot leave the TrueCrypt volume mounted. That is, TrueCrypt acquires exclusive ownership of this volume file and won't share it with the cloud client. So it's necessary after doing things to unmount, to dismount the volume from TrueCrypt. Then the cloud storage thing can see that it is available and changed and make the updates. So it's not as transparent.

The other problem is, even if you stored nothing in the 10GB TrueCrypt volume, you've still stored 10GB in the cloud because basically you're storing a whole drive in the cloud. So you're paying for it, even if it's empty. That's where these file-by-file systems have the advantage that basically you're storing encrypted versions of your file. The downside of doing that is you can see that there are files, and there are directories. They've got cryptographic names, but you can sort of - there is some leakage of this metadata, timestamps and structures of the file system. Now, I don't know that that is a big concern. But the beauty of TrueCrypt is there is nothing that anybody can tell from the outside of this blob. They can't tell how many files, how big they are, what's going on. They could detect that you changed something, if they were watching really closely. But it's just random changes, literally random changes, of this big blob, so it doesn't really get them anywhere.

So, I mean, TrueCrypt is maybe the ultimate TNO. There are people using it. They are using it in the cloud. They say, yes, you've got to unmount the volume for it to update. But they like the fact that it is TrueCrypt. And we've talked about it. We've been discussing it in various contexts for years. It's very solid. On the other hand, there's nothing unsolid about these file-by-file systems. And, frankly, that's the approach I take. I'm doing the file-by-file approach rather than the big homogenous drive that TrueCrypt creates.

So I think we're done for now. I'll keep my eye...

Leo: "For now" being the operative...

Steve: Yes, for now. I'll keep my eye out for other tweets, people bringing things to my attention. We'll watch these various things evolve. I think they're going to. Now, I just said that, and I realized I never did yet talk about SpiderOak, which is already mature-seeming, mature-looking, and beautifully cross-platform. I think maybe we'll take a break for a couple weeks, let people catch their breath from all of this. And then, after I have some more experience with SpiderOak, be able to talk about it more knowledgeably. I mean, it looks like a nice utility. I just have not drilled down into it and figured out how they do the things that they do.

Oh, I think Arq is the one, also, Leo, he says on his page that he is doing versioning, and he keeps, like, every file per week for the last month and every file for the last month for the prior year or blah blah blah blah. He's got some nice sort of a hierarchical versioning deal that's...

Leo: Yeah, I'm looking at his folder structure on S3, and it doesn't duplicate my local

folder structure. So he's obviously doing some smart stuff. And that's why that calculator makes sense. It even says, you tell me what's your limit on spending, and I'll keep versions up to that point, but delete the oldest versions at that point. So versioning is very handy. I really like that. And a lot of tools don't do such a good job with that. So that is attractive. And I like the idea of using S3. But I'll be very interested to hear your comparison to SpiderOak because I use that currently. And I don't know. I'm running Arq right now. I don't know. How many backups can one person have? Is there such a thing as too many? I don't know.

Steve: Leo, if there is, you will find it and break it.

Leo: And I have Google Drive and everything else. I just don't - what I'm really looking for, the thing I'm most loathe to lose is my photos. I've got my - documents are small; right? Because that's not - it's just documents. So that I've got backed up in a number of ways. But the photos are large. We're hundreds of gigabytes here. And that's, in fact, close to a terabyte. And that's where I'm a little concerned. I use a service called SmugMug. I don't want to add to your list here. But SmugMug, which is a photo-sharing service for pros, does support S3. So what happens is you can say, when I upload the originals, I want the originals stored on S3 at additional - I pay the S3 charges. But that's nice because now I have the originals stored in S3, SmugMug has the JPEGs and albums that I can share and buy prints of. And so that's kind of how I'm doing it. Although a terabyte on S3 is not cheap.

Steve: Leo, I really want this for Windows.

Leo: Arq.

Steve: That is to say, Arq. He says, under "Wayback Machine," "Arq keeps multiple versions of your files."

Leo: Love that. Yeah, love that.

Steve: He says, "Following the initial backup, Arq automatically makes incremental backups, every hour, every day, uploading just the files that have changed since your last backup."

Leo: Perfect.

Steve: "Arq keeps hourly backups for the past 24 hours, daily backups for the past month, and weekly backups for everything older than a month."

Leo: Perfect.

Steve: So, yeah. So it's like, a beautiful hierarchical staging backup system, allowing you to go back to prior versions of things. No file size limits. 4GB or 40GB, doesn't matter. Backs up your external drives and your network drives. Doesn't delete backups of your external drives just because you haven't plugged them in lately. Oh, there are a couple services that do that. If they haven't seen an external drive for a while, they just remove it from your cloud. It's like, ouch. So anyway, very nice for Windows. Oh, sorry, for Mac. I wish it was for Windows.

Leo: Well, there are other solutions, I'm sure. And we'll find out about them because everybody's going to tweet them at you. And you'll never - this is not done. Remember...

Steve: Leo, I've opened a real can of worms with this.

Leo: A special health-focused Steve Gibson - we're calling him "Steve Gibson, Lab Rat" - episode. This is not a Security Now! episode. We've segregated it for those of you who can't stand yet another discussion of diet and health. But if you're interested, Sunday, 2:00 p.m. Pacific, 5:00 p.m. Eastern, right after The Tech Guy, right before TWiT. That's 2100 UTC. And we'll put it out as a special, not in the Security Now! feed, but in a TWiT Specials feed.

Steve: Right. And next week, when you do know what it was we talked about...

Leo: Then we'll talk about it.

Steve: Then we'll talk and convince those people who haven't yet listened that maybe they should.

Leo: There you go. That's a solution. Steve is at GRC.com. That's his site for SpinRite, the world's best hard drive maintenance and recovery utility. One must have it, if one has hard drives.

Steve: It pays my bills.

Leo: And it pays Steve's bills, so it's a good thing just to buy it anyway. He also makes available freely, at his own expense, 16Kb versions of the audio of this show, for people with bandwidth limitations, and transcriptions, which he pays to have done each week from the wonderful Elaine. Thank you, Elaine. Thank you, Steve. That's at GRC.com. If you have a question for next week's feedback episode, I guess tweeting @SGgrc works.

Steve: It seems to.

Leo: But I think this week we'll also take questions from GRC.com/feedback, since we didn't do that last week.

Steve: Yes. Sometimes the question does need to be longer than 140 characters.

Leo: You know, I like the short ones, though, I've got to admit.

Steve: I know.

Leo: There's something to be said for them. And you can find the full quality versions in video of this show, as always, at TWiT.tv/sn, going way back to Episode - I don't even know what it is. One.

Steve: One.

Leo: 350 episodes ago.

Steve: Yeah. We should have started with zero, but live and learn.

Leo: Hey, Steve, thanks so much. Have a great week. And I will see you Sunday for that special edition.

Steve: Oh, I can't wait. I'll make some notes and organize, and I'm going to blow your mind, Leo.

Leo: I can't wait, either. And we'll see you all next week on Security Now!.