SECURITY NOW!

Transcript of Episode #462

Cloud Storage Solutions

Description: After catching up with an event-filled week of security events and news, we announce and launch the beginning of a multi-part podcast series which will examine and analyze the many current alternatives for securely (TNO) storing our files "in the cloud."

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-462.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-462-lq.mp3

SHOW TEASE: It's time for Security Now! with Steve Gibson. Microsoft gets in trouble because of Canadian spam. Apple updates iOS. Greenpeace flies a blimp. The future smells like your cat. And Steve Gibson takes you through cloud storage. Security Now! is next.

FR. ROBERT BALLECER: This is Security Now!, Episode 462, recorded July 1st, 2014: Cloud Storage Solutions.

It's time for Security Now!, the show that covers your privacy and security online with the one, the only, ladies and gentlemen, it's Mr. Steve Gibson. Now, I've been told that you are the one, the person who knows everything about security, what we need to keep ourselves safe in a digital age. Steve Gibson joining me. Thank you. I'm Fr. Robert Ballecer, the Digital Jesuit, in for Leo Laporte. Steve, what are we going to cover this week?

Steve Gibson: Okay. First I should say that nobody who actually knows about security would ever claim to know everything about security. The nature of security is to acknowledge that it's bigger than we are. But it's the fact that it's bigger than we are which makes this, I think, an interesting podcast. We've often talked about how, when Leo suggested this to me almost 10 years ago, we're coming up on the end of 10, or I guess, yeah, the end of the 10th year, I just didn't think we were going to have enough stuff to talk about. It's like, wait a minute. Every week we're going to talk about security? And lo and behold, here we are with, like, the podcast started off going to be 30 minutes, and it's often two hours. So, yes, we're not running shy of anything to talk about. We've got a whole bunch of stuff.

FR. ROBERT: It's amazing, isn't it? Shouldn't you be done with security by now, talking for 10 years? Haven't we covered everything that's possible to go wrong with security?

Steve: Yes. And arguably, it's getting worse, not better. So as the technology spreads, now we have - we've introduced this whole 'nother real angst-inducing category, sort of generally known as the "Internet of things." Which means that our household thermostats, our refrigerators, our toaster ovens, all this stuff is going to get connected, and already we're seeing security problems with those devices. So, yeah, this is not going to end well, nor any time soon.

So our main topic this week is the introduction of a series that we're going to start to sort of re-cover the whole domain of secure cloud storage solutions. We did this years ago in what was sort of a famous set of podcasts. And that may have been where I coined the TNO acronym, Trust No One, because the notion is there is absolutely technology available which gives us complete control over the random noise that we send up to the cloud so that we're not needing to trust the people who are storing our data for us. We're only asking them to store it. And of course this was years before all the NSA revelations and all of that.

So because it's been years, because the variations on solutions have exploded, pricing has come down, there's been an explosion of offerings, it's been on my list of things to get to for some time. So we're not going to start talking about specifics yet, but I want to introduce the topic, talk about the goal of this project. I've created a publicly accessible spreadsheet where all of the specifics will be maintained so anyone can go there and browse there. And we'll flesh it out over time as we sort of march through the solutions and cover that. But that's what we'll talk about after we talk about the news.

And there was lots going on this week. Microsoft surprised us by saying they were going to stop sending security announcements through email. Then they changed their mind. We've got a new iOS and Mac OS X update. PayPal had sort of a famous security misfire. People have been asking me about ProtonMail, which was the target of PayPal's misfire. So we'll take this opportunity to talk about ProtonMail briefly. Greenpeace and the EFF had an interesting use of lighter-than-air aircraft. Facebook got in the news, unfortunately, for some social engineering mischief. And, boy, there was an amazing announcement from IBM Security with a very disturbing snippet of source code from the Android project. And a bunch more stuff.

FR. ROBERT: Yeah, that's pretty ambitious. You think we could actually get through that in an hour and a half, two hours?

Steve: Well, we'll run full speed.

FR. ROBERT: I mean, just the EFF flying a blimp over the NSA datacenter in Utah alone I think you turn an entire show into.

Steve: Oh, and beautiful, beautiful photos.

FR. ROBERT: Really, I know; right? That was the thing. When I first saw that, I thought it was just a publicity stunt. It was just, okay, yes, I get it, you have a sign saying they're spying on you down here. But the photos they actually took are amazing. They're so much better than the released photos of the datacenter. It actually gives you a little insight into what might actually be in the building.

Steve: Yeah, and I stared at them for a while. I mean, they make great wallpaper, if somebody's, like, into NSA wallpaper. But there are not many cars around. So I've not been tracking yet. I don't think it's up and functional yet. I think it looks like the facility has been built, and there's vehicles sort of staged around in different strategic locations. You can, like, stare at the fence, and there's little pods every 10 feet, and it's like, ooh, I wonder what those do. So, yeah, it's definitely an interesting photo that was taken. But, yeah, it makes great wallpaper. And, wow, quite a facility, as we've discussed, south of, I can't think, it's south of - what's the big town?

FR. ROBERT: Utah? Salt Lake?

Steve: Salt Lake City, south of Salt Lake City, right.

FR. ROBERT: Yeah. One of the things that we actually covered on This Week in Enterprise Tech when we were talking about the datacenter in Utah is they were having issues bringing the datacenter up because they were pumping so much power into that building, they were getting arcs. They were getting lightning in the building jumping from rack to rack to rack. And every time it did that it would destroy a few, $10,000 worth of storage devices.

Steve: Oh, and some precious data. Oh, my god.

FR. ROBERT: Oh, I feel really bad about that. I mean, yeah. I know how bad it is when I lose a hard drive or two. And the NSA losing terabytes of data at a time, it just breaks the heart.

Steve: Well, as a percentage of what's there, eh, they probably wouldn't even miss it.

FR. ROBERT: Yeah. And that's actually the alarming part. The alarming part is the drives that they were replacing, they were replacing while continuing to run the datacenter, at least in its early stages. The other thing I remember about this is how much power and water it drew in. The NSA actually tried to classify how much water the datacenter needed for cooling and how much power it was drawing in over the grid under the National Security Act. They were saying, look, you can't tell them how much cooling we're using because, well, then they could figure out exactly what they're running, and they'll know our capabilities.

Steve: Right.

FR. ROBERT: It's strange. Once you get into that morass of national security, it's amazing how fast it grows into, well, we can't tell you that, we can't tell you this. And, oh, and by the way, we're going to need a 400-mile cordon around the building because anyone could fly a blimp over the top of us, and suddenly it's no longer a secret.

Steve: Well, it's interesting, too. You can see the power center in those pictures. In the back right of the photos is a whole power substation there just for the purpose of servicing that center. So I'm sure experts are able to take - yup, there it is back there. I'm sure experts are able to take a look at it and gauge from that.

FR. ROBERT: It is pretty amazing what they, I mean, look at this. This is an entire electrical substation. And all it does is run servers.

Steve: Right.

FR. ROBERT: And it's just for this one installation. So you can guess what might be in there.

Steve: Yeah, wow. Okay. So on Friday I got this weird email. Microsoft, because I subscribe to several of the Microsoft security announcement feeds, they'll, like, send an email out the week before the Second Tuesday, which would be today because our Second Tuesday of July will be next Tuesday. And they sort of give you a generic, these are the sorts of things that are going to be there. I don't know why they do it because they must, I mean, they obviously know enough to send that email to tell us what they're going to do, but they don't actually announce until they're ready to go.

Anyway, this email said that they were going to cease sending these security update announcement email due to changes in government regulations. Didn't say what regulations or what government, just changes in government regulations. And then it came out a couple days later that this was their response to the July 1st, which was yesterday, it's called CASL. That's the Canadian Anti Spam Law.

FR. ROBERT: Oh, Canada.

Steve: Yeah. It's something that happened on January 1st and had a six-month grace period. So that ended at the end of June. And I was really curious about this so I spent some time looking at what this legislation says. And, I mean, it is onerous if Microsoft were subject to it. And what's bizarre is that there are, first of all, Microsoft worked closely with Canada during the preparation of this legislation. So this didn't catch Microsoft off guard. Microsoft was sending affirmative sort of resubscription email already prior to this. And so it's like they misfired. And in fact Microsoft has subsequently said, oops, never mind, we will continue sending email starting with next month. So I think maybe we're going to miss July's mail, but then we ought to start getting it again in August.

But what this law states is that, after July 1st, you are no longer able - and this impacts Canada resident companies and Canadian recipients of email. So Microsoft in Redmond is impacted if they're sending security announcements to Canadian citizens, except that they're not, which we'll talk about in a second. But anyway, so the law, I mean, it's got some teeth. And you can't even ask people, after July 1st, if they want to stay on your mailing list. That's what the six months was for. You had to ask before July 1st. Afterwards, it becomes a crime to - because I guess the presumption is, if this isn't written really, really carefully and tightly, then the spammers will just ignore the law.

And of course the real problem is that spammers do ignore the law. And this has, I mean, this has been the problem we faced before is it'll be, to whatever degree this causes problems for legitimate companies, this is a problem for them. But the spammers will continue to spam, even though it's antispam.

So Brian Krebs was following this. And, in fact, Brian has a new book out, specifically about spam. I've not had a chance to read it yet. But as a consequence he's really up on this. And he quotes an executive director named Neil Schwartzman, who's the executive director of the Coalition Against Unsolicited Commercial Email, CAUCE, who said the CASL, which is this new Canadian legislation, "contains carve-outs for warranty and product safety and security alerts that would more than adequately exempt the Microsoft missives," wrote Neil, "from the regulation."

And Brian wrote: "Indeed, an exception in the law says it does not apply to commercial electronic messages that solely provide 'warranty information, product recall information, or safety or security information about a product, goods or a service that the person to whom the message is sent uses, has used, or has purchased.'"

And so then quoting Schwartzman again, he said: "'I am at a complete and total loss to understand how the people in Redmond made such an apparently panicked decision,' noting that Microsoft was closely involved in the discussions in the Canadian Parliament over the bill's trajectory and content.'" And finally Schwartzman said: "This is the first company I know of that's been that dumb." And then, famously, yesterday afternoon at 5:40 p.m. Eastern, Brian updated his posting, saying, "In an apparent reversal of its decision, Microsoft now says it will be re-starting its security notifications via email early next month."

From a Microsoft spokesman: "On June 27, 2014, Microsoft notified customers that we were suspending Microsoft Security Notifications due to changing government policies concerning the issuance of automated electronic messaging. We have reviewed our processes and will resume these security notifications with our monthly Advanced Notification Service." Oh, that said on July 3, 2014. So, but the Second Tuesday is July - oh, on July 3rd. Okay, so maybe we are going to get the July 8th announcement. Because somewhere I saw they said "next month," but now they're saying this month. So, yeah, never mind.

FR. ROBERT: You know, if I were to give Microsoft the benefit of the doubt, I would say someone in legal panicked. Someone in legal saw this and didn't know the whole back story, didn't understand what Microsoft had been doing to work with the Canadian government, and they said, well, we don't want this liability. Let's just pull everything. Until we figure it out, let's just say it doesn't exist anymore.

Steve: Right.

FR. ROBERT: But you know, Steve, it kind of strikes me as this is one of those rules of unintended consequences. I understand what Canada's trying to do, but legislation against spam has historically not been a win.

Steve: Right. And again, the spammers use fake domains. They use other people's machines. They use botnets, I mean, they're absolutely lawless. So again, legislating, I mean, for example, here I am, I'll be releasing SpinRite 6.1 as soon as SQRL is finished and 6.1 is ready. I need to send email to every SpinRite 6.0 customer, which goes back now a decade because SpinRite 6.0 began shipping in 2004. So I have everyone's email address. I have a commercial relationship with them.

It's hard to imagine that anyone who received email from me announcing a free upgrade, like a major benefit from 6.0 to 6.1, is going to be upset. But there's all kinds of people. And given enough of them, you're going to find some people who are like, wait a minute, this is spam, and I'm in Canada. Stop this. And so I need to make sure that I'm not crossing the line. So as an example, it's much more dangerous for a legitimate, responsible, lawful company than it is for the spammers who are just going to ignore this.

FR. ROBERT: Well, you know what they've said. The traditional saying has been, if you outlaw email spam, only spammers will email.

Steve: Yes, exactly.

FR. ROBERT: I think that's probably something that they would have said if they thought about saying that.

Steve: Well, and we've, you know, speaking of misfiring, we've often talked about the problems with PayPal over the years. And they really stuck their foot in it just a couple days ago. I'll talk about ProtonMail in a second, and this is a perfect segue for me doing so. But ProtonMail is a Swiss-based, very interesting-looking, secure email startup that is crowdfunding themselves through Indiegogo. And one of their payment options, apparently they use PayPal or a credit card. And they've said that Bitcoin is available. But from looking at the dialogue that this all stirred up, apparently they haven't made it easy to use bitcoin, or as easy as they could, or just bitcoin isn't as easy to use still as PayPal is.

So they blogged. And so their blog says this morning, which I think is yesterday, I mean, this all happened - oh, yeah, it was yesterday. So they said: "This morning we received an email" - and so this is ProtonMail talking. "This morning we received an email and telephone call from PayPal notifying us that our account has been restricted pending further review. At this time, it is not possible for ProtonMail to receive or send funds through PayPal. No attempt was made by PayPal to contact us before freezing our account, and no notice was given.

"Like many others, we've all heard the PayPal horror stories, but didn't actually think it would happen to us on our campaign since PayPal promised very recently to improve their policies. Unfortunately, it seems that these were hollow promises as ProtonMail is now the latest in a long string of crowdfunding campaigns to be hit with account freezes. For examples, just look here, here, and here." And they provide three links.

Now, okay. This was all sort of interesting. But the thing that chilled me, the thing that really caught my attention is the next paragraph, which reads: "While the $275,000 ProtonMail has raised in the past two weeks is a large amount, it pales in comparison to many other crowdfunding campaigns that have raised sums in excess of a million dollars, so we can't help but wonder why ProtonMail was singled out." And here's the sentence: "When we pressed the PayPal representative on the phone for further details, he questioned whether ProtonMail is legal, and if we have government approval to encrypt emails." So I just - I have to - I want to give PayPal the benefit of the doubt.

FR. ROBERT: I don't.

Steve: And say that - I know. I mean, this is really awful. But you're going to have a hierarchy. Out on the front lines are not your sharpest bulbs, or, wait, no, brightest bulbs or sharpest sticks or whatever. So it's horrifying to imagine that PayPal would be making a decision about locking an account by questioning the legality of an email encryption service. I mean, that just staggers the imagination. So they said, finishing, they said: "We are not sure which government PayPal is referring to. But even the Fourth Amendment of the U.S. Constitution reads 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures....'"

So anyway, this caused a huge flare-up on the Internet, and the news as of just a few hours ago is that the account is now unfrozen. But yikes.

FR. ROBERT: It's just it's horrible, horrible precedent. I mean, we know that the U.S. government especially can freeze accounts. They can freeze accounts across the world when there is suspicion of criminal activity. But when a company, a financial company does it proactively, without any direction from any government, but just under the suspicion that maybe what you're doing is against the law, even though there is no clear precedent that says, yes, you can't encrypt, you can't encrypt your email, that's just - that's scary. And that scares me far more than anything the government may do. Okay, NSA notwithstanding. The federal government in the United States is normally pretty clear about when it takes steps to freeze finances. If we're now saying that PayPal or Citibank or Bank of America or Wells Fargo can freeze it because they have questions about what you're doing with your money, that's a whole other level.

Steve: Well, and also remember in the U.S., of course, we have the legal system, and it takes a court order in order to make that happen. So a bank won't just freeze assets because someone from the government phones them and asks them to do that. They need a warrant. They need a legal document which is indemnifying them against any actions that the aggrieved party may have, too. I know, for example, that for an ISP to turn over IP addresses, the FBI needs to get paperwork from a judge saying this is an active investigation, we have a case, and we need to have this information.

So, yes, you're right, it's entirely different for a commercial entity to just decide, oh, we're just going to freeze this account. I mean, without even having a dialogue with these people, without, I mean, they were able to phone them after the fact. Now, of course you can understand why they didn't phone them before because the company could easily immediately drain the account, grab all the funds out of it. So but still, this should have been handled better. And it would be good to, I mean, PayPal does have a reputation for problems.

These little blinking lights over my shoulder are PDP-8 re-creation kits. And during this project, this was also a - it was sort of a privately crowdfunded project organized by just a private individual who's got years of background doing this. And he collected a whole bunch of people. And the idea would be we all pay into this, and if he achieves enough to bring the prices down to make it work, then the project goes forward. And sure enough, PayPal stomped on it right in the middle. And they said, wait a minute, you're charging for something that you haven't delivered yet. And it's like, yeah, and everyone who's involved knows that. Everyone in this understands that their funds will - we will only process this if we achieve critical mass, but this is the way you do it. And so anyway, it was like - it ended up getting resolved, but it was a nightmare. So, wow.

FR. ROBERT: Yeah, and then there was that sentence of, well, do you have permission from the government to do this?

Steve: Oh, god.

FR. ROBERT: I just, I hear that, and I almost can't make the connection of why would you think I would need that? In fact, I should be asking you, do you have permission from the government to freeze my funds? Now, I will say...

Steve: And if we have, asking if we have government approval to encrypt emails. It's like, oh, god. See, that's why I just have to think this is somebody who is just not on, I mean, is on the frontline, but is way down the hierarchy and doing the best they can with what they've got.

FR. ROBERT: Yeah, yeah. We've got people in the chatroom who are pointing out that there's going to be suspicion that maybe PayPal received a phone call from a certain government agency, or they got tapped on the shoulder when they were walking down the street. But it would seem to me that, if that was the case, this decision wouldn't have been reversed so quickly. And in fact, if that was the case, they wouldn't even have answered the questions of ProtonMail. They would just say no, I'm sorry, we have to freeze your account.

Steve: Yes. I actually think this was a mistake by a low-level employee who just doesn't know what's - who has more power than he should, or he or she should.

FR. ROBERT: More power than sense, I believe is what we used to say.

Steve: But this does give me an opportunity to segue into a brief discussion of ProtonMail. I've been getting a lot, there's a lot of interest in it. I'm getting tweets all the time from people saying, hey, Steve, have you had a chance to look at Proton Mail? And I have, but I just haven't had a chance to talk about it. So I thought, okay, let's...

FR. ROBERT: Wait a minute, wait a minute. I mean, the thing that I've heard about ProtonMail the most, and I don't believe this, but there's a lot of people who are saying, oh, so it's just Lavabit. And it's not; right? It's not just a copy of Lavabit. It's actually a slightly different business model.

Steve: Oh, it's not Lavabit at all. So there are some very clever things. First of all, it is end-to-end encryption. And that's, you know, we need to start having an acronym for that because that's going to be important, end-to-end encryption. It is browser-based, so like browser-side and cross-platform, and JavaScript-based. So you have JavaScript crypto running in your browser. And of course JavaScript is universal. Browsers are universal. So you get universal cross-platform compatibility.

So when you log into them, they give you a page containing JavaScript-written crypto and a standard, contemporary, state-of-the-art email web interface. And I've not looked at the details, so this is why this is just sort of a first pass. And in fact they're in beta. I mean, they're still, you know, they're crowdfunding. They're in the process of pulling things together and getting all of the details worked out. So I don't know whether anyone yet knows everything about it.

But a user who is able to send email to another ProtonMail user has end-to-end encryption so that, before the email leaves their browser, the browser encrypts it and sends this pseudorandom noise to the ProtonMail servers, which are located in Switzerland specifically because it's believed that's a better place to put these things these days. And you see that more and more. That's where Threema is, and other people who are wanting to do nongovernment-interferable cloud things. And then your recipient logs into ProtonMail and receives the email.

So, for example, one could imagine, if this existed a couple years ago, in the era of, like, pre-Edward Snowden disclosures to Glenn Greenwald, then Snowden could have said, "Get a ProtonMail account, and that's all you have to do, and we'll be able to correspond securely." Because this didn't exist then, it was necessary for Greenwald to figure out PGP, which is a much higher barrier to entry, a much higher bar than just using ProtonMail. So the advantage to this, now, this assumes everything else is done right. There's lots, I have lots of questions still about the implementation of the crypto, I mean, the specific protocol level, how are they doing things, because I have not seen the documentation for that.

I'm made a little uncomfortable by one of the features that they offer. My feeling is a company like this that is asserting that they're doing it absolutely correctly needs to only offer secure things. And one of the things they've got, one of their features, their bullet points, is self-destructing messages. They said: "With ProtonMail, emails are no longer permanent. You can set an optional expiration time on ProtonMail's encrypted email, so they will be automatically deleted from the recipient's inbox once they have expired. This way there are no trails of sent messages. Similar to Snapchat in a way, we've added a way for you to have even more ephemeral communication."

Well, that's nonsense. I mean, that can't work because all someone has to do is copy the email out of their browser, and then they're no longer able to reach in and get it, wherever it is. So that ought to go away. I mean, that makes me really uncomfortable, the idea that they're selling something that they cannot deliver. They're making a guarantee.

FR. ROBERT: It sounds like such a gimmick. I mean, we see that a lot in messaging apps where - because I live at a school. And I see students who are absolutely convinced that, when they send something in Snapchat, it means, oh, well, I don't have to worry about this ever coming back to haunt me. And it's such a misunderstanding of what's happening when someone reads your message. Again, if you don't trust a person reading your message not to misuse the technology, the technology is useless.

Steve: Yes. So anyway, so I wish they didn't have that because that's something, I mean, that worries me. So the jury's still out. We'll definitely take a look at it once it gets further along and when documentation is available for the protocol. For example, they've got some hurdles to overcome in terms of interpersonal email sharing. That is, the way the keys are managed. For example, Apple has stated that iMessage is secure. Yet we know it's actually not secure because they manage people's keys. And the key management is transparent to the user, but that means that they could provide a key for themselves, and your message would get signed under their key, allowing them to read it.

So the problem is it's difficult to make something that is really easy, I mean, truly easy to use, which is also truly TNO. And as soon as you start involving multiple users, that becomes trickier. For example, the main topic for this week is, of course, TNO Cloud Storage. And that's easy to do if you're the only person who ever needs access to your files. It becomes way trickier - not impossible, but trickier - if you need control, you need to have controlled disclosure of some files to other people. And that's exactly what the email model is, where you want to be able to selectively send email to other, presumably, ProtonMail users and have that done securely.

What that essentially means is you need to get their key, their public key, and encrypt your email under their public key, under the assumption that nobody else will have their private key. Yet key management is crucial, and we have no idea how ProtonMail is doing that. So to everyone who's been asking, it's on the radar. We'll keep our eye on it and, as soon as we know more, absolutely take a close look at it. They have got something clever. And again, no specific details yet, but how do you send email to somebody who isn't a ProtonMail subscriber? The presumption is that you would use - the reason you need to use the web to view mail as a recipient is that you need the JavaScript to decrypt.

Well, apparently it's possible to turn a message into a link and then email the recipient a link, which then they click, which takes them obviously to a web browser session where they then provide a password which you have given them to decrypt the email that's behind that link. So they've come up with solutions for these things. But I'm very uncomfortable about this self-destructing messages feature. The idea that people who are serious about security would even offer that is a little frightening and disturbing.

So I would say it looks like a great thing, we just need to see how it's going to be implemented. And unfortunately, key management is where these things tend to get tricky because you can't trust anyone except the person that you're corresponding with. Ultimately, they've got to provide you with the key. And then it's hard for that to be transparent.

FR. ROBERT: Yeah. Unfortunately, I think we're in that age where trusting that someone is going to offer you secure communications, it doesn't work anymore. I mean, they actually have to show you what the widgets are behind the scene before you can sign off and say, okay, I think you're doing it right. And you're right, I think it worries me a little bit that they're trying to do this ephemeral chat, this ephemeral email. That's more of a marketing thing than it is anything else.

Steve: Yup. And that's, to my way of thinking, that crosses the security line. You don't want to have somebody who's selling you absolute robust security who's also saying, "Oh, and email you send can be made to evaporate." It's like, no, it can't. So don't tell me it can.

FR. ROBERT: It's magic. It erases them from the minds of the people who have seen it. Actually, Steve, this reminds me a little of just a couple of days ago Ars Technica got their hands on a Blackphone. Have you heard about that?

Steve: Heard of it. Haven't seen it yet.

FR. ROBERT: They got their hands on it. But not a whole lot of time. It was basically first impressions. Decent Android phone, decent specs, screen, memory, processor, the typical fare. But of course it's a fork of KitKat which has been integrated with several security enhancements, things that, for example, it automatically will anonymize your searches. It will automatically anonymize your IP. But one of the things that it comes with is the Silent Circle. It's a paid service, and it gives you two years of Silent Circle secure voice, video, and messaging.

Steve: I think that's Moxie Marlinspike's service.

FR. ROBERT: Yes, yes, it is. And the way that they handle the person you send the secure chat to having the same service is they also give you three gifting subscriptions. So you can gift a subscription to three of your friends or family, and now they have the client, as well. It's expensive. It's more expensive. But at a certain level I trust that because they tell you where they're getting their money from. They tell you exactly how the security works. And you actually have to go through a little process in order to make sure that you're set up properly. I kind of like that. It gives me the positive feedback that I've encrypted my communications.

Steve: Yes. Another example, we've often talked about the secure chat application, Threema, T-H-R-E-E-M-A. And they have a system where you have, I think it's like red, orange, and green level of authentication. And the only way to get the green level, that is, absolutely assured privacy between two devices, is if they are physically together and snap each other's QR code so that it's a physical exchange of the devices, of each other's public key. And it's only if the public key is obtained that way, that is, not through a shared server or any weaker form of authentication, only if it's a face-to-face meeting of the devices do you get the green level. And so, yes, that's a perfect example of, yes, it's more difficult. But if you're wanting to chat with friends, and you can arrange to meet them, then it works.

FR. ROBERT: People in the chatroom are asking how much that Blackphone costs. It's not available yet, but I think it's for $629. Now, actually I think this is a good segue for talking about how you would authenticate those devices. Silent Circle, as you said, uses QR codes. So you have to be in the physical vicinity of the other phone in order to grab the code. What do you think, Steve, if they, say, NFC-enabled this software so that you can actually tap someone and have their public encryption key?

Steve: I would say that's probably okay as long as there's no way for the NFC to, like, be enabled in the same sense that Bluetooth is often enabled - and, by the way, always reenabled after we update our iOS, which is annoying. You update any iOS device, and it always turns Bluetooth back on, and so you have to remember to turn it off. So the idea would be, if the way the user interface worked, it was enable a key exchange, like while my finger is on the screen holding down the enable circle, and I tap the devices together. So do something that's convenient, but absolutely be sure that there's no way for a bad guy to bump into your pocket and snag your key.

FR. ROBERT: That's the next version of "The Sting" will have people just bumping into people's NFC pockets with their phone. It's the high-tech version of it. Now of course, Steve, we don't have to worry, though; right? We don't have to worry about at least the government eavesdropping on our phone conversations because the Supreme Court said that the police need a warrant in order to be able to do that. So we're totally safe; right?

Steve: Well, this was a decision that a lot of people were happy to see. It generated a huge amount of news, I guess it was late last week, that the Supreme Court did say - oh, yeah, the cartoon in the show notes. I love that. Right. The Supreme Court did say that a warrant was required, like, for example, if you're pulled over by the police, they can't require you to unlock your phone and let them just snoop around in it. So it was good that those protections were reasserted by the court.

Speaking of iOS updates, we did have an update of iOS to 7.1.2. There's a laundry list of things they fixed. I won't try to enumerate them. But it was enough that everyone should take some time to update. I would say it was an important security fix. They refreshed the certificate root store, which is a good thing to do. We always talk about certificate authority root stores in devices. So they updated that, probably put some new ones in and hopefully got rid of some old, expired, or debris ones. Then there's a long list of fixes. They fixed a bunch of remote code execution problems.

And in fact this fixes many of the things we've talked about over the last couple weeks. For example, there was a famous revelation that email attachments were not being encrypted in the previous iOS 7.1.1. So this fixes that so that email attachments are now being encrypted. There was a way of disabling Find My Phone. That was in the news in the security community for a while. That's been fixed. There were two lock screen bypasses that have been fixed. A Siri hack has been foreclosed on. And then just a ton of things fixed in WebKit.

And interestingly, a bunch of the same things were done for Mac OS X and Apple TV, demonstrating, as a friend of mine pointed out, that they're now using a common codebase. So when they fix these things that are being used across their device spectrum, everybody gets the benefit of that. And then just, again, a reminder, when you do update 7.1.2, for the sake of power consumption and security, if you don't need your Bluetooth radio turned on, by all means turn it off because the update will have, as it always does, reenabled Bluetooth for you.

FR. ROBERT: That's always my favorite parts of updates. And this is not just iOS devices. This works on Android, this works on proprietary OSes, where you may have tweaked it perfectly so it is exactly as secure as you want it to be. You do the update, and how you have to remember what you did to make everything work because of course it's going to reset everything to its default settings.

Steve: Right. And, I mean, I just wonder if it isn't Apple believing that their end-users don't know enough to choose whether they want it or not, and that Bluetooth offers so many features that, oh, it's a good thing, because then our iBeacons are able to track you as you walk through retail stores and so forth. I don't know.

FR. ROBERT: It reminds me of the Adobe update screen. I get it all the time. I have a regular protocol that I follow in order to get the most recent updates. But it has that nag screen that comes up every single time I install which says...

Steve: McAfee?

FR. ROBERT: ...are you sure you want us not just to do it automatically? I'm like, no, I told you 15,000 times, I will do it. I don't want you popping up at random times.

Steve: Yup, yup.

FR. ROBERT: It's nannyism.

Steve: So we talked last week about - actually it was in our Q&A. Someone asked a question about HTTPS everywhere. And I ran across an interesting analysis of the top 50 most used sites in Alexa's ranking. In fact, I created a bit.ly shortcut: bit.ly/alexahttps. So A-L-E-X-A-H-T-T-P-S. It's an interesting analysis. They took the top 50 most popular sites on the 'Net. And some quick takeaways from the entire readout, which you can see at that link, is that 29 out of the top 50 websites, which they note is 58%, worked perfectly over HTTPS. So we're definitely seeing a growth in the use and the availability of SSL/TLS encrypted connections. They noted that Google globally consistently offers SSL everywhere and, in some countries like the U.S. and Canada, even defaults to SSL on its own.

A little anecdote, however. I will note that the only problems people report with certificate revocation, the OCSP - Online Certificate Status Protocol - is Google. For whatever reason, I mean, as we know, Google is hostile, unfortunately, to certificate revocation. They've stated publicly and loudly they don't believe in it, they don't think it works, they don't think it's worthwhile. And so it's interesting also that they also have the crappiest online certificate revocation. I've got mine turned on in hard fail mode in Firefox, as do now tens of thousands of podcast listeners who learned that they could do this. I never get a problem at all. And frankly, I never even get one from Google. But the only problems that I hear people reporting, and they sort of chuckle about it, is, well, you know, Google apparently doesn't have very good certificate revocation services. It's like, uh, no, they don't.

FR. ROBERT: Now, Steve, I've always been a little bit puzzled as to why Google is so hostile to certificate revocation. I mean, it's a basic, basic thing that you need to do in a networked world. And I remember the first time I heard about this was at Google I/O. And I was in one of the developer sessions, and they were talking about it. Some of the Google people were saying, oh, yeah, we don't deal with that. I'm thinking, wait, what? So this is an in-house policy? What is it about revocation that just rubs Google the wrong way?

Steve: I honestly don't know. My feeling is it boils down to one person named Adam Langley's personal crusade. And he is in charge of security, so he's the guy. And so he has the right to have whatever feeling he wants. But he believes that revocation doesn't make sense because anyone who is in a position to take advantage of a revoked certificate is also in a position to defeat the revocation checking. And he's right that it's possible that such a person could be in such a position. But he's wrong in asserting that it's guaranteed. It's not guaranteed. We know it's not. And I also think that there's some history with the crypto libraries and problems. Google also created their own thing called a CRL set, which if you look at the original statements about it, it looked like they were intending to go and create their own standard. And the certificate industry ignored them.

And so I think they're a little pissed off. And they're, saying, well, fine, we're just not going to play then. And I think this is all short-term policy on their part. They've got to bring their browser into compliance. The certificate authority industry is really unhappy with Chrome and Google and their policies. So this isn't a long-term strategy. I think we just saw them last week announce that they were forking the OpenSSL code to create what they called BoringSSL. Well, the OpenSSL code has all of this. It's got OCSP, it's got full revocation, full certificate chain checking. So I think that this - in time we're going to see this coming back and being fully honored because the CRL set that Google uses now is proven ineffective.

FR. ROBERT: I think Google wants to take their ball and go home.

Steve: Yeah, well, they're big, and they're doing very well with their browser. But this was just they got off on the wrong foot. They planted a flag somewhere that has turned out to be quicksand. And I think...

FR. ROBERT: It seems, yeah, it could slow down visitors occasionally. Yes, it might be a slight bit more of a technical hassle. Yes, you can defeat certificate revocation. But it doesn't seem like that's a good enough reason not to honor it.

Steve: Well, and ask users. Ask users would they mind maybe a slowdown. And by the way, I should mention that that's actually old news. All of the major certificate authorities now have CDN support. They've got Content Delivery Networks that have servers near their users. And OCSP is working now. It is not a big slowdown. That's maybe five or more years' old news. So that's not the case. Everyone I know who's turned revocation checking on, and even hard fail, which is available in Firefox, doesn't notice any change. And the end user now knows that their certificates are being checked for revocation.

So the point is, ask the end-user. The end-user wants that on and is willing to make a slight tradeoff. And notice it's not the entire session with a site. It's the very first connection. And after that the credentials are cached so all of your browsing around the site, all of the image downloads, everything else you're getting from that site is not slowed down at all. It's just the first time you check to make sure that the certificate you're receiving is authentic and has not been revoked. So, I mean, I just think Google's wrong on this. But that's okay. They can be wrong.

FR. ROBERT: Yeah, exactly. They can be wrong, and that is a little bit of old news, Steve. So what if we move from old news to a new vulnerability? This one's actually kind of scary. You want to explain what they found?

Steve: Okay. So you're talking about the Android...

FR. ROBERT: Oh, yeah.

Steve: ...deal? Yeah. Okay. Actually what was disturbing about this was that it was arguably by design. So the news came out that 86% of Android devices were vulnerable to crypto key theft. And because that sounds like a bad thing, it made a lot of headlines. Now, it turns out that was never the case. It was 10.3% because it turns out it's only Android v4.3 devices. So all of the 4.4 KitKat devices that are currently in use are okay. And apparently this was introduced in 4.3 so that earlier devices are also okay. So it's only this little window of 4.3.

So this was discovered by IBM security researchers. And their research report is titled "Android KeyStore Stack Buffer" Flow - or, sorry, "Stack Buffer Overflow: To Keep Things Simple, Buffers Are Always Larger Than Needed." And I have to say, it's necessary for me to say I am not kidding because people aren't going to believe the comment block that was in the source code. So this is protecting the Android KeyStore, which contains all of the keys that applications place in the store for safekeeping.

The comment reads: "KeyStore is a secured storage for key-value pairs. In this implementation, each file stores one key-value pair. Keys are encoded in filenames, and values are encrypted with checksums. The encryption key is protected by a user-defined password." And here it is. "To keep things simple, buffers are always larger than the maximum space we need, so boundary checks on buffers are omitted."

FR. ROBERT: I can't tell you how horrible that - actually, that's a surprise. Congratulations. We just found a way to fix all buffer overflows. We just make the buffers bigger than we normally do, and it's done; right?

Steve: Bigger than you need, and then you just don't need to check.

FR. ROBERT: Because there's no way that an attacker is just going to continue to flood the buffer until finally it tips over; right? That's - no, no.

Steve: Who would think of that? Yeah, yeah. So in IBM's disclosure, first of all, they did this very responsibly. This was disclosed to the Android developers on September 9th of 2013, nearly 10 months ago. So they waited this long for the vulnerable version, for 4.3 to sort of drain out of the market because they recognize this is not good.

Now, it takes a lot to exploit this, but it's definitely exploitable by code you load into the device. So you would have to load some malicious software onto your Android device, Android 4.3, and only v4.3. But in IBM's disclosure they said: "Successfully exploiting this vulnerability leads to a malicious code execution under the keystore process. Such code can: Leak the device's lock credentials. Since the master key is derived from the lock credentials, whenever the device is unlocked," then you have access to, essentially, into the keystore. "Can leak the decrypted master keys, data, and hardware-backed key identifiers from memory. Can leak encrypted master keys, data, and hardware-backed key identifiers from the disk for later offline attacks. And can interact with the hardware-backed storage and perform crypto operations, e.g., arbitrary data signing, on behalf of the user."

So just to reiterate, this is not a problem today, not since 4.4. And the Google guys, the Android team was notified 10 months ago. IBM just waited until now to disclose what they found. And the real takeaway here is, oh, my goodness. The idea that someone - I'm just stunned that some coder who is coding arguably one of the most sensitive areas of crypto in Android, could say, "To keep things simple," right, so they don't want to bother checking buffer boundaries. "To keep things simple, buffers are always larger than the maximum space we need so boundary checks on buffers are omitted." It's unbelievable.

FR. ROBERT: To pick a place in your codebase not to check the buffer overflow possibilities, to do it in the encryption module, it kind of boggles the mind. They must have had an intern working on this thing? I don't understand how you do that. And in fact I don't understand how it gets through your team. Someone must have been checking this work. And if anyone I know saw that comment, it should have raised a dozen red flags immediately.

Steve: Right. I mean, the comment is so obvious. You might argue that you'd have to really study the code to, like, be sure that the person wasn't checking buffer boundaries somewhere. But here's the code, I mean, the comment says "I'm not checking buffer boundaries."

FR. ROBERT: The comment should just say "Insert hack here." That's basically what you've done. Anyone searching through this codebase, the very first thing I would do is I would do a search for buffer. I would look, is there anyplace here that's dealing with buffer because that's where I'm going to inject my exploit. This comment is telling you, oh, yeah, if you just make it big enough, it will work. Yeah, just, yeah, this is the only place you should focus on.

Steve: Yeah. And it's funny, too, because after that comment, after citing that comment in IBM's security report, they said, "Though things are simple, buffers are not always larger than the maximum space they need." So, yeah. There's a lesson for you. Wow.

FR. ROBERT: Oh, Steve. Makes me not want to program anymore.

Steve: Last week in the Q&A we had someone ask how it was that he was sharing a, I think it was a spreadsheet, or maybe - I don't remember if it was a document or a spreadsheet, I think he said with his wife, sharing the Google link, and was disturbed to find apparently anonymous users also viewing the same document. And the first person to send me a note about that I grabbed, Charlie Gulf, through Twitter, @CharlieGulf. Thank you, Charlie. He tweeted: "Last week's Google Docs question. New anonymous users seem to be created every time you view the doc link without signing in first."

So that explains the mystery. A number of other people also informed me of that, but Charlie got in first. So thank you, everybody, for making sure that I knew that. So that explains what happened. Apparently, for example, his wife wasn't signed in, and she clicked the link, and that created anonymous users rather than herself, who would obviously not be anonymous. So, mystery solved.

And there was a little bit of news, which is completely off topic. But then so was supercapacitors when I went crazy about that a few years ago. I talked about ultracapacitors years ago, following some story. And we spent some time on it, talking about what a potentially fabulous solution this was for energy storage, for regenerative braking, to put the energy into the capacitor, taking it out of the car, and then using that to kickstart your car and so forth.

Anyway, I ran across a story. I just wanted to put it on people's radar. I created a bit.ly link for the article. And I don't know why I made it upper and lowercase. I shouldn't have. But so it's a bit.ly, bit.ly/NH3-Cracking. So cracking. NH3 is the chemical formula for ammonia. And this is an article which was just published that says: "A hydrogen breakthrough could be a game changer for the future of car fuels."

What's exciting about this is, when you think about it, ammonia. It turns out we have a huge ammonia production capability globally. Actually China makes a huge percentage of the world's ammonia. But we have transport. Ammonia is famously used in the creation of fertilizer, one of the main components of fertilizer. So we're making a ton of it. Well, if you notice, NH3, that's a molecule of nitrogen and three of hydrogen. In other words, ammonia is an interesting storage form for hydrogen. And what these guys have come up with is a very inexpensive and apparently practical means of "cracking," as is the term, of cracking ammonia back into its constituents, meaning nitrogen and hydrogen, freeing the hydrogen from the ammonia. Which you could either, apparently, burn in internal combustion engines with small modifications, or use to power fuel cells in purely electric vehicles.

But one of the problems we've had is how do we carry this much energy around? Lithium ion batteries are what electric cars are using today. And while, if you have them large enough, they can give you enough miles, they're really difficult and time-consuming to recharge. So the idea would be people are talking about a hydrogen economy, the idea of switching to hydrogen fuel. And these guys are arguing that, well, an ammonia economy may be vastly easier and more practical to implement. Anyway, this, as I said, completely off topic, but I wanted to mention it because we had a lot of fun with the ultracapacitor technology some time ago. And this is early-on research, but really looks interesting and promising.

FR. ROBERT: Actually I'm really happy that you mentioned this. I'm absolutely into energy production. And this is one of the most promising technologies I've seen in a while because all it requires is you to be able to split water, pull out the hydrogen, be able to combine it with H2 and N2, so nitrogen and hydrogen to get ammonia, or go one step further and create something like ammonia hydroxide, which is rocket fuel. And then you use a catalyst, like there's zirconium something, there's an alloy that will actually naturally break apart a hydroxide.

Steve: Yes.

FR. ROBERT: So you free up the hydrogen. And that gives you a really easy way to store hydrogen in a stable compound, break it apart, and having nothing but nitrogen and water coming out the tailpipe.

Steve: Yes.

FR. ROBERT: And of course nitrogen is a huge component of the atmosphere. It's completely harmless to us.

Steve: Yeah, and actually we're only putting back the nitrogen that we took out.

FR. ROBERT: Exactly. It's a net zero.

Steve: Yeah, exactly. And it's a zero carbon fuel, which is what's, to me, very exciting about it. It's a nice way of packaging up hydrogen and then giving back the nitrogen that we took out of the atmosphere when we burn the hydrogen. So, yeah. And you're right. And it starts with water.

FR. ROBERT: Right. And we've got people in the chatroom who are saying, oh, but this all requires energy input. Where does the energy come from? This is not a way to generate electricity, this energy. This is a way to store it.

Steve: Right.

FR. ROBERT: That's actually the problem. We've got generation. We just don't have effective, efficient storage methods. And this could be one of them. You could have something that's inert for hundreds of years before you use it. And it will keep the energy that you poured into it to form the ammonia. That's future tech right there.

Steve: Yup. And these guys note in their article that ammonia cracking has been done before. It's very well known. But traditionally it's required extremely rare, extremely expensive rare metals in order to interact with the ammonia and perform the cracking. The breakthrough these guys made is in a very inexpensive, I don't remember, some sort of an oxide that they came up with that makes it very inexpensive to build a very small ammonia-cracking reactor in order to put ammonia in and get hydrogen out. So again, this is years away from us driving this around, but really potentially interesting as a means for getting away from our liquid petroleum gas technology with all of its carbon problems.

FR. ROBERT: Well, I mean, just remember, this is another way to say "fuel cell vehicle," "fuel cell car," because one of the biggest problems with fuel cell, as people point out, is how do you transport hydrogen? Hydrogen is explosive. Hydrogen can be very dangerous. Well, don't transport hydrogen. Transport ammonia. Ammonia is very easy to transport. It's not as dangerous. It's really easy to fill into a tank, and then the reaction takes place in the fuel cell itself.

Steve: Yes, exactly.

FR. ROBERT: Well, Steve, let's get away from that because I want my SQRL update.

Steve: Okay. So I'm cranking away on SQRL. I mentioned the Crowdin site a couple weeks ago, and we generated a few more translators who went over. We're now at 60 languages, people standing by to perform the translation into, well, actually, English is one of those 60, so 59 languages other than English, and 414 translators. So I just wanted to thank everybody for their willingness at this point to participate. I'm now, I mean, it's all I'm doing. I was working on it until I had to stop yesterday to start putting this podcast together. Once we disconnect from Skype, I will return to it.

Essentially, all the pieces are there. All of the protocol design is finished. I just wrapped up the storage technology for securely storing identities, either in files or in QR codes and other forms, in a way that they're secure. Everything is there. So I am now in the process, I'm back working in the user interface, gluing all the pieces together. I haven't published any strings for translation because too much is subject to change. For example, I did the Entropy Harvester, and it worked out so much better than I expected when I designed the user interface that several of the UI panels are just gone. There's no need to have someone sit there watching it generate, like, painfully harvesting entropy. It's able to happen in the background, and we're just overflowing with more than we need.

So it really makes more sense for me to get a reference implementation finished, which is what I'm directly working towards now. Once we have that, then that'll give me all the strings in English that I actually needed. And then all the technology is in place for publishing those to Crowdin, getting people to translate them, and then I'll be able to immediately export those from Crowdin back into the app and create SQRL in 60 different languages. So I'm working on it as fast as I can. That's my project right now.

FR. ROBERT: Not fast enough for humanity, Steve. We need that now.

Steve: Yeah, we do. And we'll have it as soon as I can. I did get a nice note, dated June 26, so a few days ago, from a Steffen Zacher Nielsen, who of course is a SpinRite user. He said, "Hello, Steve. I've just purchased SpinRite as the only tool which was able to solve the problem I had with a damaged hard drive. SpinRite was able to repair the drive so that I was then able to restore about 3,500 very important files to another drive. I must say, it is very satisfying to use a strong and cheap tool" - I'm sure he meant inexpensive - "like SpinRite, and afterwards having such a good experience. Thank you very much. I can wipe off the sweat from my face and take a deep relieving breath."

He said, "I've spread the good news of my experience with SpinRite to all my friends on Facebook, so perhaps your sales will increase in the future. Who knows? Steffen." So, Steffen, thanks for sharing your experience with SpinRite.

FR. ROBERT: I have to say, Steve, I've heard these ads for years and years and years. But I actually - I've had my share of "SpinRite saved my butt" stories. Including...

Steve: Oh, truly?

FR. ROBERT: Yeah, one very recently. Some of the folks in the chatroom were telling me how I could use SpinRite in Level 2 to perhaps fix a problem I was having with a few Samsung SSDs.

Steve: Yes.

FR. ROBERT: It actually worked. So I'm doing a Know How... episode that's - because I had a batch of about 12. And so I decided to try it on one. In six months my read and write speed was cut in half on the same computer, the same variables. I couldn't figure it out. Ran SpinRite, got it all back. So I don't quite understand how it works yet, but I'm going to figure it out. I'm going to figure out what voodoo you've packed into SpinRite, Steve.

Steve: Very cool. Actually, it's funny because it was the reports that we started getting as SSDs became more popular. People began reporting that SpinRite was recovering them, it was fixing them. And so I thought, oh, okay. I guess SpinRite's going to keep on going. I mean, because I had been sort of feeling a little gloomy about the death of the hard disk drive and the ultimate replacement of that with solid state. But it turns out that the engineers of solid state have pushed their technology just as far to the line, as close to the line as the hard drive guys have, so that solid-state technology is needing error correction and maintenance in the same way that electromechanical storage does. So SpinRite has a future. And after 6 there will be a 7.

FR. ROBERT: That's blasphemy, Steve. I've always been told that SSDs will completely remove any need for error correction or looking at the data integrity. I mean, haven't you heard this? Didn't you read the press releases?

Steve: You know? And one of the things that I'm sort of seeing is that it's a little frightening. Certainly hard drives can fail completely. I mean, they can just die. But the sense I get is hard drives fail sort of more softly. SSDs, when they go, they're just gone. And I don't know if you've had that experience. But I'm a little more comfortable with something that begins to sort of have problems and let me know that it's in trouble, rather than just spontaneously no longer having any storage.

FR. ROBERT: Yeah, no, I've seen that, especially on the enterprise level. If you try to put a consumer drive into a server, it will work fine until suddenly it just disappears. Dead. No access whatsoever. The enterprise products actually build in a huge amount of extra memory cells. And the tools, the built-in tools will start telling you, you need to replace this. You need to replace this. In fact, there's a tool from a manufacturer that I use right now in my servers which will actually give error codes like a standard SATA hard drive will, and then it will shut itself off when it feels that it's in imminent danger of losing data. And it's to tell you, look, I'm going to shut down. You get one more chance to turn me back on and copy data off.

Steve: Like, I'm really serious.

FR. ROBERT: No, no, seriously, seriously, no, dude, dude, listen, listen. Take care of me right now.

Steve: Pay attention to this one, yeah. Very cool.

FR. ROBERT: Well, Steve, we've gone through the news. That took a while. But now we need to hear about cloud storage. And this is something that I know is kind of touchy with the Security Now! audience. Same thing with the This Week in Enterprise Tech audience because we've been taught by the best, by the master, to Trust No One. But any time we talk about cloud storage, you don't have that chain of possession of your data, and you don't know if you can trust it.

Steve: Yeah. So I guess what I want to do for the balance of the podcast, and with this sort of as our kickoff of a series, is to sort of lay out my thinking about the state of the art of cloud storage. First of all, since we first talked about it, when we first talked about it there were a few providers. I had found Jungle Disk and liked Jungle Disk. That was probably, wow, I don't know. Certainly it was during the podcast, so it wasn't 10 years ago, but maybe seven or eight [SN-123 2007].

Since then, it's really become a thing. And we've had collapsing mass storage costs. We've had rising bandwidth and falling bandwidth costs. The point being that incredible amounts of remote storage are accessible to individual end-users, not local, but in the cloud. And people increasingly are using it because they've got camera phones. They've got phones. They have photos. They've got movies. They've got media collections. They have stuff that's generally big which they would like to back up. Also there's been of course an explosion of mobile devices, and people are looking at the cloud not only as the backup of a single device, but as a bridging mechanism for cross-device sharing.

So we're more in a multiplatform world today than we used to be. Also, with the continuing rise of the Mac as a percentage of desktops, we're seeing many environments which are multiplatform. And of course Linux is continuing to be of growing popularity. So certainly it's not the case that we're just in a Windows-centric world anymore. And so the cloud can connect all that stuff together.

One of the things that I recognize that will be a focus is that there isn't just one cloud user. There isn't one profile for a user. I mentioned all the different platforms that are available. And so an important feature for cloud storage solutions will be some kind of cross-platform capability. It might be, I mean, my intention is to assemble a spreadsheet, a comprehensive spreadsheet which - and this will be done over time - which is a big grid of features. So people will be able to cross-reference features and providers and see who has what. It's not a resource that we have right now.

But my goal is to build that spreadsheet. And I recognize that there are some people who only use Windows. And there may be, for example, a Windows-only cloud storage client that is feature-complete and provides what they need for that platform. So in this spreadsheet it'll show that it's compatible with Windows, but not with the other things. Which for that person may be fine. Whereas that would be a deal-breaker for anybody else.

Another thing is the issue of cost because people's budgets vary, and their storage needs vary. One of the things that you see a lot in cloud storage providers is this notion of tiered plans, where you've got, typically, there's the free teaser that maybe it's we're going to give you X amount of storage free, maybe for a year, sometimes it's for life. And their presumption is you're going to end up needing more than that, and so that'll get you in the door, get you using their product, and then you'll migrate into a paid tier where they ultimately want to be.

One of the things that I know we've talked about in the past is that the hard drive prices have fallen so dramatically as storage capacity has exploded that the economics of paid cloud storage makes sense. I mean, it makes sense that a company could be buying 4TB drives and chopping them up into many smaller pieces and charging an individual user some percentage of that drive's one-time purchase price per year. And I'm sure there are business plans where they show, oh, look, we're going to capture this many people. We're going to hold onto them for this length of time. And we're going to end up easily recouping our investment many times over. You just know there are business plans like that.

My own model, that is, the model that I've been using so far, is the pay-as-you-go model. Some of them, as I was mentioning, are like tiered plans, where for this amount of money, you get a hundred gigs - this amount of money per year, you get a hundred gigs. I'm partial to the pay for what you use. And actually it's the model that I'm using now. To give people a sense for that, I'm using Amazon S3 as my provider. And my office manager, who maintains GRC's books and does our accounting and has her computer, all of her critical files continually backed up, using Jungle Disk, because I'm still using that as my Trust No One client. She's using S3 for that.

I have a massive archive of antique computer documentation, of course, where I just - I want it to be safe. There are sites that have all this now. We see websites disappear from time to time, of course. TrueCrypt's site disappeared, famously, for example. Anyway, there have been sites archiving documentation of all the old PDP family and early mini computers. I want all that for the future. All of that is up on Amazon S3. Also, all of the Security Now! audio files are there. So we've got 82GB of storage on S3, for which I pay $2.51 a month.

I looked at, in preparing these notes, I looked at June's bill from Amazon. Amazon charges $0.03 per gigabyte for the first terabyte per month of storage used. And so there's a different model. There's the pay as you go. I'm partial to that because that just feels right to me. There's something about the tiered pricing is the same way the cell phone providers charge you for how many text messages you're going to, you know, they set a cap. And if you go over that, you get penalized. And essentially what that guarantees is most people are going to be under that with unused capacity. That doesn't appeal to me as much.

And then Amazon has additional features, for example, for further reducing the cost, which I'm not even taking advantage of. They have reduced redundancy storage. They've got Glacier, which is a write mostly, but slow retrieval system. Both of those allow them to lower their cost, and they pass that on to you. And other features like you can ship a hard drive back and forth to them in order to quickly import or export bulk data. So I don't mean to focus on them, but that's a good example of sort of an alternative model.

And then of course many people also have their own local network-attached storage. That is, they've got their own cloud storage in a local cloud, and they may still want to use external storage to supplement that, or as a backing store for their local NAS, where they have fast access on their LAN to the local NAS, and then that gets backed up to the cloud. And then of course another way of slicing this is do you want turnkey, or do you want toolkit?

I've talked before, Carbonite is a sponsor, has been, of this podcast. And my girlfriend Jenny has her laptop backed up using Carbonite because, I mean, and she's a perfect candidate for that because she just wants her stuff safe. She doesn't want to push buttons, she doesn't want to mess with anything, she doesn't want to tune things. And she's actually not someone who is kneejerk about TNO. For her, maybe the web access would be useful, where you sacrifice the Trust No One client-side encryption. Who knows? But that's not a need she has. If this had to be really complicated for her, she wouldn't use it. So it's far better that her laptop, that she knows her laptop is backed up all the time so that she can get it back when she needs it.

So that's more the turnkey model. And I'll certainly entertain those providers, that is, the providers who offer something you install in your computer, just sort of a "set it and forget it," although it's really not this audience's focus, and it's not my personal focus. My personal focus is I like the idea of a toolkit where we're decoupling probably a multiplatform client from a solid storage provider so that we're able to choose each of those which meets our needs. Maybe, for example, the pay-as-you-go isn't as economical, depending upon how much storage you're using, where a flat rate is.

Or one of the reasons, for example, that my storage is inexpensive with Amazon is there's not a lot of transactions. There's two audio files a week go up. And Jungle Disk is very good in dealing with S3 with its interface with Amazon, backing up only the files that Sue has changed on her machine from night to night. So because Amazon does have a transaction fee, maybe you'd rather have a system where you weren't being charged for transactions, where your bill wasn't varying, you were just paying a flat rate. And that was sort of an umbrella that covered all of your various systems and uses.

So there are many ways to go with this. And then of course there's the notion of a hybrid solution where - and I sort of used Google Drive as an example, where Google Drive gives you a very nice web-based interface which is multiplatform and very convenient to use. Yet at the same time you could use a multiplatform client which is doing client-side encryption, thus TNO, for example, of a folder in Google Drive. So you've got Google Drive, and it's meeting your needs. You're able to work with it through your web browser for moving files in and out very comfortably. Yet in the background a whole bunch of your systems are being operated in a TNO mode where Google Drive is the backend storage provider to something which is more of the toolkit profile, where you've chosen these components yourself.

So at this point, I have a tentative list. What I want people to do is drop a note in Security Now! feedback for next week's episode. We'll do a Q&A next week. On my list, and this is in this week's show notes, so someone could scan it, or if you just hear me not read something that you're passionate about, let me know. You can tweet it to me @SGgrc, of course, or go to GRC.com/feedback in order to get a web form and just drop me a note.

So I know about Air Backup; Amazon S3, as I mentioned; Arq Backup that we talked about once before. I believe that's still Mac only, but I haven't looked recently. Also Bitcasa; BoxCryptor really looks good to me, also. There's Backblaze. There's CloudBerry, CrashPlan, Duplicati, Filosync. Of course good old Jungle Disk. Mega, then Microsoft's OneDrive. There's a system called Tresorit, which looks very nice also. SpiderOak we've talked about, and we'll look at them again. Sync.com. Syncthing.net. Tarsnap, that's Colin Percival's solution. He of course is famous for the development of scrypt, which is the PBKDF2, the password-based key derivative function that I'm using in SQRL in order to create very, very strong, really impossible to crack passwords.

There's something called younited, spelled Y-O-U-N-I-T-E-D. Viivo, or Viivo, I guess, V-I-I-V-O, I think that's from the ZIP folks. And then Wuala is also very popular. And Zoolz, Z-O-O-L-Z dotcom. Those are all the ones, the list I've been maintaining. As people have mentioned them, I've added them. No doubt I've missed some. Let me know.

And then my plan is to tackle probably one a week, maybe two a week. We'll just sort of see how much time I have and how much there is to say about each of these. But essentially, I want to build this, the goal is to build a comprehensive, publicly accessible spreadsheet. It's already up. Since this is called Cloud Storage Solutions, CSS, I created a bit.ly link because this is a Google spreadsheet. So it's bit.ly/sn-css, all lowercase, sn-css. So for Security Now! hyphen Cloud Storage Solutions. That will end up being fully populated with a complete breakdown of all of these services, how they operate, how they compare with each other, what the pricing is and so forth. And I imagine we'll just, once that's established, we'll add to it as new things come along. I'm sure people will point out mistakes or changes. We'll fix those. And we'll have, like, one nice reference for the state of the industry in cloud storage solutions.

FR. ROBERT: Now, Steve, the era of having a dedicated cloud solution, like the one that rules them all, that's kind of over; right? I mean, we talked about that a lot early on, that, oh, well, Dropbox is going to be defeated by Google Drive, and Google Drive is competing with OneDrive, or SkyDrive, as it used to be. That's kind of going away. It seems as if people are starting to understand that you can choose different cloud providers for different things.

Steve: Yes.

FR. ROBERT: Like, for example, my personal setup uses a few Synology drives. It uses an ioSave drive, which is actually a Synology NAS box inside of a fireproof safe so that I could do redundant storage on the same campus with one box that's almost sure to survive any disaster.

Steve: Right.

FR. ROBERT: Plus it automatically syncs to Amazon Glacier. So even though that's not fast, it does store a lot, and it does it over time. And then I have my less secure files, the files I really don't care about, get put on to OneDrive so that I have immediate access to them. And you really kind of custom format your storage setup according to the needs of space, the needs of speed, and the needs of security; right? I mean, you're not going to find one vendor that does it all great. But if you could break down what you need, then you get to choose the vendors that work best.

Steve: Yes. And that's exactly what I mean when I talk about a "toolkit" approach. I think that's the approach that makes sense for this podcast's listeners. I mean, anyone can install - I was looking at my list, and I'm not seeing it.

FR. ROBERT: Carbonite?

Steve: Carbonite. Thank you. Yeah. Because you're right, I didn't have - not on the list here. Anyone can install Carbonite and just have that problem solved. But in fact you've probably seen this. I don't remember the name of the service. There's even one which deliberately takes advantage of multiple cloud providers' free tier plans and spread your storage across all these different providers' free packages, so that you end up with an aggregate large amount of storage being underneath the paid level for each of them, and ending up with something free. That's not really the approach I would take. It's a little more like...

FR. ROBERT: And you could call that "Cheapo Disk."

Steve: It's sort of like RAID 0, where really you've got no redundancy at all, and if anything died, you're in trouble. So, yeah. Cheapo Disk.

FR. ROBERT: Another interesting point to bring up is I get way too many people who think that cloud storage is their backup. And I always tell them, look, it can be one of your backups. But you can't just assume that it's always going to be there. We don't have to reach back very far to see a real case scenario. Do you remember Mat Honen, who had a little issue with his iPad?

Steve: Oh, yeah. Oh, yeah.

FR. ROBERT: That absolutely can happen, where you have one device that issues a delete command across all the synced boxes, and next thing you know it's all gone.

Steve: Well, and remember, too, we're relying on these cloud storage providers to be there, for example. But they could be hit by a denial of service attack, and you have no connectivity to them at a certain time. Or an earthquake could happen and take out someone's datacenter. So the idea being, yes, that's good backup. But exactly as you say, you absolutely don't want to count on them for sure. You want to use them as probably safe, but not mission critical.

FR. ROBERT: "Matwork" in the chatroom has a good acronym for it. He's calling it RAIC, a Redundant Array of Independent Clouds. I guess you could do it that way, as long as there was a way to break the sync at some point so that a deletion in one place doesn't necessarily destroy the archive everywhere else. I guess I could take that.

Steve: Yeah. I think, you know, I guess my role in this, because anyone could put together a big matrix of features, that's not a hard thing to do. You look at web pages with critical eye. But when I looked really carefully before, we found mistakes in the crypto. We found things that were not done correctly. And that's what people want from me is, okay, yeah, so they're saying they're not storing my keys. Well, okay, are they? Or how does that work? And so what interests me is the low-level plumbing of this, the actual crypto technology. And so what I hope to surface on this spreadsheet is that I've looked at it. We'll do a podcast on it. This is how it works. And then we'll capture that for future comparison.

FR. ROBERT: Yeah, yeah. Now, if people want to participate, they just go to the feedback page on GRC and let you know what they're looking for. You want to hear from the audience. You want to hear from the people who are actually using this in the wild. What do you need out of a backup solution? What do you need out of a cloud solution? And who are you looking at? Who do you use on a daily basis?

Steve: Right. And I've had people say, hey, I'm using Duplicati. Are they secure? So I imagine next week's Q&A, because I know this is a topic of huge interest, I mean, I would say cloud storage has become a major factor in what the Internet is offering today. So I want to solicit input to sort of get this thing launched. And that'll help give me some direction. And then I imagine, obviously, we will take breaks when major security events happen. But I hope to just move through this and really cover this territory so that, by the time we're done, people, for example, who want to take a toolkit approach will be able to say, ah, this is the one I want to use because. And they'll know why they're choosing the one that they're choosing.

FR. ROBERT: You know, Steve, one of these days you're going to choose a project that's simple. Looking through all cloud storage providers to find the one or the few, that's a little ambitious. But we don't expect anything less. Steve Gibson is at GRC.com. That's the place that you'll find SpinRite, also where you'll find links over to ShieldsUP!, the essentials if you're going to live in a digital world. It's the world's greatest maintenance and recovery utility set.

Now, you'll also find 16Kb versions of this podcast, transcripts, and of course the tremendous, the talented, the very active forums over at GRC.com, in addition to information about security and, of course, SQRL. You'll also find the forums, aside from the feedback page, where you will be able to contribute to Steve's cloud solution project.

Now, if you have a question you can submit them at GRC.com/feedback. That's the same form that you're going to use to suggest elements of Steve's cloud provider project. And maybe your question will be picked up for one of the Q&A sessions of a future episode of Security Now!. You can also find all of the versions of Security Now! here at TWiT, at the TWiT show note page for Security Now! at TWiT.tv/sn, and wherever fine podcasts are aggregated. You can also use our apps or watch us live. We gather every Tuesday, 1:00 p.m. Pacific, 4:00 p.m. Eastern, 2000 UTC, at live.twit.tv. I'm Fr. Robert Ballecer, in for Leo Laporte. Steve Gibson, thank you very much.

Steve: Thanks so much. This was great.

FR. ROBERT: We'll see you next week on Security Now!.