SECURITY NOW!

Transcript of Episode #726

Steve's File Sync Journey

Description: This week we look at a widespread false alarm about Facebook's planned subversion of end-to-end encryption, still more municipality ransomware attacks, more anti-encryption saber-rattling among the Five Eyes nations, Microsoft's discovery of Russian-backed IoT compromise for enterprise intrusion, Chrome 76's changes, this week's Black Hat and DEF CON conferences, a bit of miscellany, and closing the loop with our listeners. Then I want to share my recent experiences and findings about the challenge of synchronizing a working set of files between two locations, and the tools I settled on.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-726.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-726-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. We've got lots to talk about, including a rare attraction from Bruce Schneier. We'll talk about the Five Eyes. Are they going to get what they want? Steve and I think probably so. And Georgia, once again on my mind. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 726, recorded Tuesday, August 6th, 2019: Steve's File Sync Journey.

It's time for Security Now!, the show where we cover the latest security news, we teach you a little bit about how this stuff works, we talk a little bit about sci-fi, whatever Steve Gibson's in the mood for because he's the man in charge at Security Now!. Hi, Steve.

Steve Gibson: Leo, it's great to be with you again, as always, for our 726th episode.

Leo: Yikes, shmikes.

Steve: This is our annual pre-Black Hat and DEF CON episode because those happen starting tomorrow is Black Hat and DEF CON. And there's no question that next week's podcast will be, well, it's going to be the second Tuesday of the month, so maybe there'll some news, but we're all kind of getting inured to, okay, update because otherwise the sky will fall. But Black Hat and DEF CON always bring us just sometimes weeks of stories to catch up and talk about.

I've provisionally finished a multi-month quest. Because I ended up with a solution, with several false starts, that I'm really happy with, I had it on my mind. I thought, you know, I've got to stick this in miscellany. I want to tell our listeners about this journey because I think people would find it interesting. Some people might find it useful. And it ended up, when I started to put it all together, there was enough there that I just made it the title of our podcast. So today's podcast is titled "Steve's File Sync Journey."

And briefly, the background is that I'm now working a substantial amount of time every day in two locations, here where I've always been for we're closing in at the end of 14 years of the podcast, and I bought my home here in 1984, so 35 years. But I have another residence now with Lorrie where I spend the evenings. And she's a therapist who often is seeing clients in the evenings, so we both work through the evening. We'll take a break for dinner, and then I'm there, and I have another four or five hours' worth of time, which is great for me because I love what I do. I love to work.

But I was having this problem of needing to keep files in sync in two locations. Which you'd think would be pretty simple. And in fact I've come up with a solution that other people had already found, but I wanted to make sure there wasn't anything else. So I want to explain the things I tried and the solution I wound up with, and also one that may be even more interesting for people who can do a completely roll-your-own solution. So we'll talk about that.

But we also have - I wanted to address a widespread false alarm about Facebook's planned subversion of end-to-end encryption that many of our listeners tweeted me about, and then the person who was being retweeted said, whoops, my bad, to his credit. We also have, believe it or not, still more municipality ransomware attacks. We have some increasing anti-encryption saber rattling, this time among the Five Eyes nations that got together. And I think that may have been what the video we played of Bill Barr last week, that might have been where his speech occurred was during this Five Eyes nations meeting because he was there.

We also have Microsoft's discovery, which they will be further describing tomorrow, I think it is, at Black Hat, of a Russian-backed, state-sponsored IoT compromise which is being used for enterprise intrusions. So in other words, the IoT devices are the point of entry. And so we're going to talk some more about network segmentation and Virtual LANs as a means for dealing with that in the real world. Also Chrome 76 happened last week with a couple new welcome features. We've got the Black Hat and DEF CON conferences, some miscellany, a little bit of closing the loop with our listeners. And then, as I said, I want to talk a little bit about, you know, we've not talked about cloud security stuff since, well, actually we touch on it from time to time. But remember Jungle Disk, Leo?

Leo: Oh, yeah, which was S3, yeah.

Steve: Yeah, exactly, good...

Leo: Then they got acquired, which kind of...

Steve: Yeah, yeah. Very good memory, Leo. And of course now we've got bandwidth galore. We've got super cheap mass storage. So anyway, I think another interesting podcast for our listeners.

Leo: And I probably have a few things to add to the file sync security because...

Steve: I had a feeling you would.

Leo: You know, you have been in two locations, but I've been in many locations for many, many years. And I have literally, I think, tried all of them.

Steve: Cool.

Leo: And I have a roll-my-own solution, too. And I've tried, well, we'll talk about it.

Steve: Yeah, cool.

Leo: So, yeah, I'm very curious to see what your conclusions were.

Steve: So our Picture of the Week, I just, you know, these are just too fun. I would really love to know what the story is behind these because we've seen them before. I had this one in my collection of pictures to pull out for fun when there's nothing more topical. So here we have the security door with the wired glass, breakproof glass, and the combination lock with five buttons - 1, 2, 3, 4, 5 - and a big Enter button down below, above a big twisty handle. And of course on the glass it says: "New Door Lock." Then it says: "Push the #2 and #4 at the same time. Then push the #3 and press Enter."

Leo: Clearly not a secure facility.

Steve: And okay, you know.

Leo: That solves that.

Steve: I just don't - and in fact, if you look, Leo, you can sort of see...

Leo: I can see the person taking the picture.

Steve: Well, yes. You can see their reflection in the glass. But also, if you look around the perimeter of the lock itself, there was a different shape lock when the door was last painted. And so it does look like the lock was changed.

Leo: It's new, brand new, shiny new lock.

Steve: Yeah. And so, but okay, what's the story? You know, I mean, is it to slow people down? Is it a fire door? Is it like, I mean, it's not secure because despite the fact that...

Leo: Why even put a lock on it if you're going to do that?

Steve: Exactly. I just don't get that.

Leo: You could put "New door lock. Call me if you don't know the combination."

Steve: Okay. Or maybe it's a reading comprehension test?

Leo: Most of our burglars are illiterate, so yeah, yeah.

Steve: I don't know what the deal is.

Leo: Yeah, yeah. Geez, Louise.

Steve: So Bruce Schneier's blog, which generated a tweet storm, was titled "Facebook Plans on Backdooring WhatsApp." And that's such big news that it was to be the title of this week's podcast. I had it, I mean, I immediately grabbed it, grabbed the link, read the story, thought oh, my god. Thanked a few people who tweeted the news to me when I saw it. And I had provisionally titled today's podcast. But Bruce subsequently learned, from sources who are far more reliable - and Leo, you'll get a kick. You'll be smiling when you learn who it was that gave him the bad information because I similarly was fooled by this same organization a few months ago, and you said no, Steve, they're not very reliable.

Leo: Bruce fell for it, too, huh? Oh.

Steve: Anyway, so he found out from sources more reliable, though not from Facebook directly, that the story, which was sourced from Forbes...

Leo: Oh, there you go.

Steve: Yup. And in fact, when I followed the links, I got a big kick out of that even more so; but I'll get to that in a second. Which brings new meaning to the term "extrapolation" because that's what this Forbes guy did. To Bruce's credit, he immediately corrected the record, once he was confident of what was actually going on. And of course many people know that I often quote Bruce. He's credited with one of my favorite bits of pithy wisdom, which is, and our listeners have heard me say this, "Attacks never get weaker. They only ever get stronger."

Leo: Yeah.

Steve: Which just keeps, unfortunately, being true all the time. So anyway, for those who tweeted and may not have seen his follow-up, I wanted to make sure that the record was corrected. So the bogus Forbes article was titled "The Encryption Debate Is

Over, Dead at the Hands of Facebook." And again, just to make sure everyone knows, that's not true. The four relevant paragraphs of what is now the quite thoroughly debunked Forbes column, within which this author, the Forbes column author twice cites his own previous, also bogus Forbes articles as supporting references, and which quite reasonably set Bruce off last week, those four paragraphs read:

"To solve this problem, Facebook announced earlier this year preliminary results from its efforts to move a global mass surveillance infrastructure directly onto users' devices where it can bypass the protections of end-to-end encryption. In Facebook's vision, the actual end-to-end encryption client itself, such as WhatsApp, will include embedded content moderation and blacklist filtering algorithms. These algorithms will be continually updated from a central cloud service, but will run locally on the user's device, scanning each cleartext message before it is sent and each encrypted message after it is decrypted.

"The company even noted that, when it detects violations, it will need to quietly stream a copy of the formerly encrypted content back to its central servers for further analysis, even if the user objects, acting as a true wiretapping service. Facebook's model entirely bypasses," he's writing, "the encryption debate by globalizing the current practice of compromising devices by building those encryption bypasses directly into the communications clients themselves and deploying what amounts to machine-based wiretaps to billions of users at once."

Now, if you read that, I mean, it sounds reasonable on its face. You would think, oh, my god. And that's what Bruce read. And so he wanted to give this broader attention, which he did. And within the links to that text is a link to the same author's previous story in May, on May 28th, which was titled "Facebook Is Already Working Towards Germany's End-to-End Encryption Backdoor Vision." And to support that, he links to two other of his even more previous articles. One was "Facebook's Edge AI Content Scanning Brings NSA-Style Surveillance and Censorship to the Planet," and second article was "Deep Learning Will Be the End of End-to-End Encryption."

So I don't know if this guy's got some bug up his you know what about Facebook, or if he's starving for things to write about. I don't know what the back story is. But, I mean, it ends up that, I mean, and I was curious. So I read all of that. And, for example, in one of those supporting stories he writes: "Even more worryingly, Facebook's presentation alluded to the company's need to covertly harvest unencrypted illicit messages from users' devices without their knowledge and before the content has been encrypted or after it has been decrypted, using the client application itself to access encrypted-in-transit content."

And then he says: "While it stopped short" - "it" meaning Facebook - "stopped short of saying it was actively building such a backdoor, the company noted that when edge content moderation flagged a post in an end-to-end encrypted conversation as a violation, the company needed to be able to access unencrypted contents to further train its algorithms, which would likely require transmitting an unencrypted copy of the user's device directly to Facebook without their approval." So this is sort of a mishmash of supposition and the extension of allusions that are being made.

Anyway, so one thing that occurred to me as I was reading all of this is to ask the question, is it clear that point-to-point, user-to-user, one-to-one, end-to-end encrypted conversations should be moderated in the first place? I mean, the idea of an encrypted conversation being moderated in any way does sort of seem to fly in the face of the whole concept of a totally private two-party dialogue. You know, I'm having a conversation with one other person over an encrypted channel. So the idea of that being moderated seems, like, odd to me. It's not, I mean, maybe you don't want to use WhatsApp? I mean, maybe it's clear that it's moderated, and there's going to be some sort of a banner? I mean, I don't know, the whole idea of a two-party end-to-end encrypted conversation having moderation by Facebook seems antithetical.

But whatever the case, Bruce, I think, can certainly be forgiven for believing the extrapolations of this Forbes author. And I guess also Facebook does share some responsibility in this because, based on their past and all of the privacy abuses we know that they have engaged in, it's believable to imagine that they might do this. But just for the record, it is wrong. Bruce updated his original blog posting, adding at the bottom, he said: "Edited to add" on August 2nd. He said: "This story is wrong. Read my correction." And then he explained what happened.

So anyway, we know that something is going to be happening before long because there is this tension now between encryption and government that isn't going to be going away. What we don't know is how it's going to end up being resolved. And again, Facebook, the CEO or CTO, one of the top guys at WhatsApp, did officially respond and say no, we don't have any - the Forbes stories are completely incorrect. We have absolutely no intention of doing anything like that.

So anyway, I can understand that Bruce would do that. If I followed a story, and it seemed factual, I would report it. And then, you know, he fixed the record. And we've done the same things in our errata section a few times in the history of this podcast.

Leo: Yeah. And, you know, the guy, I'm looking at his bio, has - he's got good credentials. So I think that the author of the original Forbes article just misinterpreted, misunderstood. I'm not going to - I wouldn't want to impute bad faith on his part because, I mean, he was a Google developer expert for the cloud platform, senior fellow at GWU's Center for Cyber and Homeland Security. I mean, he's done a lot of good stuff. He's not a hype master. I don't - I don't know, but I don't think.

Steve: It may well be that his bringing this to light...

Leo: It's a good thing, yes.

Steve: Yes, yes, that it may well have headed Facebook and WhatsApp away from considering doing something like this by immediately flooding it with light and then allowing them the opportunity to say, whoa, no, that's not what we meant. We never intended to do that. Which would be good.

The Five Eyes alliance we've spoken of from time to time. It's an alliance of national intelligence partners whose members are Australia, Canada, New Zealand, the U.K., and the U.S. And the rhetoric surrounding this issue of encrypted messaging is heating up. There was a story last Tuesday in the Telegraph which was headlined, "Facebook is threatening to hinder police by increasing encryption." And the U.K.'s new Home Secretary is - I guess I would pronounce her name Priti, P-R-I-T-I, Patel. The Telegraph reports that, in the first intervention by a minister, the new Home Secretary says the tech giant, meaning Facebook, tech giant's plans to introduce end-to-end encryption on its messaging platform would benefit, and here she's saying "child abusers, drug traffickers, and terrorists plotting attacks."

Writing for the Telegraph, she says it would prevent law enforcement agencies investigating and tracking down lawbreakers by enabling criminals to hide their messages. And of course, as we know, and what she was responding to, was that Mark

Zuckerberg in March announced what he framed as a major change to Facebook. And we were joking about it at the time, Leo, saying they ought to just scrap everything that they have, rather than trying to fix what they have, and just start over because, you know, they're discovering logs that code had made of unencrypted passwords and all this craziness. But the point was that Mark had said that they were going to be essentially further encrypting, like, everything else, not just having an encrypted WhatsApp app, but adding the same sort of protections to Facebook Messenger and Instagram, as well. And apparently this is the move that has apparently set everybody off.

And of course this prospect is unanimously seen as bad news by the Five Eyes nations. And this warning, if that's what it was, by Patel came two days after a meeting that she hosted. She hosted a Five Eyes meeting in London with Geoffrey Cox, who's the U.K.'s Attorney General. And that's where I think that probably our own Attorney General spoke because in attendance were security and law enforcement officials from all of the Five Eyes nations, who unanimously agreed that they were worried about high-tech companies moving to - and what they said was in quote from their meeting - deliberately designing their systems in a way that precludes any form of access to content, even in cases of the most serious crimes.

So the meeting published a report, or what they called a "communique," coming from the meeting, calling for backdoors. And of course this is a problem we have is that, you know, "backdoor" is a heavily weighted or freighted term. They said: "Tech companies should include mechanisms in the design of their encrypted products and services whereby governments, acting with appropriate legal authority, can obtain access to data in a readable and usable format."

In September of 2018, so just about almost a year ago, the Five Eyes governments had called on their governments to demand that tech giants build some sort of technology in. And they were saying that they would be insisting upon it by force, if necessary. From a memo that the Australian government issued on behalf of the pact a year ago, they said: "Should governments continue to encounter impediments to lawful access to information necessary to aid the protection of the citizens of our countries, we may pursue technological, enforcement, legislative, or other measures to achieve lawful access solutions."

So anyway, Reuters covered this and also spoke with a former senior European security official who said that the Five Eyes is using very general language at this point, at best to demand for government access in telecom systems and wanting some sort of a way of drilling a hole through encryption.

Leo: This battle is coming. We know it's coming.

Steve: Yes. It absolutely is. And as I have said, and I'll just reiterate one last time, that the counter argument I think is sort of equally wrong or overblown on the other side, which is the so-called experts on the security side are all arguing that this cannot be done. There's no way to do this safely. And again, I agree that, if we define what the government wants in the way that a backdoor has always been, I mean, that term has been used, no one would disagree that that's bad, the idea that the encryption itself would be compromised so that there was the golden key or the master key or something that allowed unilateral decryption of the content.

And it may be as a result of the pushback which has already come from the tech community that we're seeing an improvement and a tightening of the language, where governments are no longer talking about golden keys. Now they're saying that, you know, even Bill Barr last week, he was arguing against warrant-proof encryption.

Meaning that, if a warrant were served on some entity, there would be some means of obtaining some content. Well, and as I last said when we talked about this, I think it's crucial to separate policy from technology because I am sure that the technology can provide whatever we decide we want from a policy standpoint. So rather than arguing - and that's been one of the problems is that the politicians hear the Silicon Valley geniuses saying it cannot be done; there's no way it could be done.

Well, the politicians know that's not true. And they're right that it's not true, that there isn't a means to do this if we want to. So again, what we have to do is just decide what it is we want, reach an agreement, and then implement that from a technology standpoint. The technology can do anything we want it to do. We have all the crypto bits we ever need in order to pull this off. It's just a matter of, as we've said, doesn't have to be a backdoor. Doesn't have to be, you know, someone said, I have it in my show notes - Wizner. Who's Wizner? Oh, Ben Wizner, an expert in national security law with the ACLU, the American Civil Liberties Union.

Leo: Yeah, I've interviewed him. He's great.

Steve: Yeah. But he said that, if the U.S. and other nations get access to private messages, Wizner told Reuters in an interview, that means that adversarial nations such as Russia could demand that they get the same access. Well, no, that doesn't mean that. I mean, we could decide if we want to give that to them. But again, it's entirely possible to provide access with whatever degree of control we want. It's not easy. And I won't argue that it's not as secure because, yes, if you're going to add a mechanism to selectively decrypt, by definition that's less absolutely secure. But that may be the cost, you know, the price if we're going to be operating in an environment where we need to abide by the laws of a given government in order to have the technology that we want the rest of the time.

Leo: You've talked about this before, but I think it's important that we at some point talk about how it would be done in a way that doesn't compromise security for non-governmental actors, in other words, allow hackers in.

Steve: Right.

Leo: I know you're convinced that that's possible, but I think you have some convincing to do because you seem to be one of the few that thinks this. So at some point we should delve into that. You've talked about it before, and I understand your point of view. But I think you're an outlier in this.

Steve: Yeah. And you know me. I don't mind being an outlier.

Leo: No, not at all. And I think you're probably right, to be honest. But I just think it would be worth talking about it.

Steve: Yeah, yeah. I mean, you know, the example I've used in the past is - and this is "an" example. This is not universally applicable because not everybody has the control that Apple does. But when we talk about iMessage, the idea that Apple is managing the keys, and in fact this is what the U.K. has talked about with this Ghost Protocol, where there would be the ability to add a silent additional party to the conversation. Right now, iMessage supports many-to-many multiway messaging, not just one to one. And many of these protocols are able to operate that way.

So Apple is managing the keys for us. Apple could create an additional entity that would be joined to an iMessage group that wouldn't appear. And that newly created entity could be created under warrant from the government, and the government given access to that entity as a silent partner, as an invisible participant in an iMessage conversation. In which case they would receive all of the transactions back and forth, and it would be - it doesn't compromise other communications that that user has.

Leo: As long as Apple keeps the keys close to its vest, obviously.

Steve: Exactly. Exactly.

Leo: So I think everybody would...

Steve: And note that Apple is doing that now.

Leo: Well, that's the point.

Steve: Apple has all of those keys now.

Leo: That's the point. I think anybody would stipulate, yeah, okay, but that's not going to be the end of the government's requests because what they really don't like is end-to-end messaging. As long as a corporate entity that they can subpoena, that they can serve a warrant to, has the keys, they're fine with that. What they don't like is end-to-end encryption, which means the only person who has the keys are the parties in the conversation. Is there a way to make that breakable without compromising security?

Steve: No.

Leo: No.

Steve: No. And this is to your point, Leo, that you brought up correctly last time, which is it's math. We already have the ability to do unbreakable encryption. And so...

Leo: I'd be happy to give the government, since they already have it, the right to do whatever they want to do with non-end-to-end encryption - Telegram and Apple's Messages and, well, WhatsApp is end to end; right? WhatsApp, nobody holds those keys; right? It's using Open Whisper's protocols; is that right?

Steve: It's been a while since I looked.

Leo: I think they use the Signal messaging protocol. Signal, let's give the Signal example. Signal, no one has the keys.

Steve: I do know that WhatsApp is using Signal, yes.

Leo: In that case there is no key escrow. There's no one holds that key. You are the key, you and the - the only parties who could access that would be the parties involved in the conversation.

Steve: Well, because that's the design of it.

Leo: So what would you do then - see, the government wants WhatsApp. That's what they want. I don't think they really care about Apple Message because they can already serve a subpoena to Apple. They can warrant Apple and get that message. They know that.

Steve: Yeah, yeah. They want...

Leo: They want WhatsApp.

Steve: Exactly. And so I don't know that Moxie would ever be moved to...

Leo: No, I know he wouldn't.

Steve: ...to add that technology. But what we're talking about here, I mean, it's serious. It would be the government outlawing, formally outlawing encryption that it cannot serve a warrant on in order to obtain access. It would be against the law. And, I mean, the government's made mistakes before. Remember when - I remember you couldn't use more than 40-bit keys once upon a time.

Leo: Right. They called it munition.

Steve: Yes. And so 128-bit keys existed, but you couldn't go outside of the U.S. with more than 40 bits of encryption, presumably because...

Leo: Which led to people wearing T-shirts with the code for strong encryption and exporting it that way.

Steve: Yes.

Leo: It's pretty hard to tie that down.

Steve: So imagine a world where a law is passed by the U.S. government that says, at some point, I mean, and there'll be some sunsetting period, you know, like by 2025 it is against the law to use encryption that there is not a means for the government to obtain a warrant for access to. Now, at that point Facebook needs to decide, are they going to give up encryption, or are they going to soften their encryption? I mean, Signal's open source. So again, and there are other smart people. So it might be that we have no choice but for Apple and for Facebook and for Google, I mean, major commercial organizations to use warrant-compatible encryption...

Leo: I think that's what's going to happen, yeah.

Steve: ...as the only choice. And of course the counterargument is good. And that is that, well, bad guys will use illegal encryption.

Leo: And they'll use Signal, yeah.

Steve: Well, yes, yes. And yes, they will. But still, the government will think, well, this is the best we could get; you know? At least...

Leo: This is my fear. That's not what the government will think. That my government will say, well, that's not enough, we still can't see every communication.

Steve: Well, in that case the only thing they could do would be to put something in our ISPs which block anything that the ISP cannot decrypt.

Leo: Oh, that's interesting. We're done.

Steve: In which case, then the end user gets handcuffed.

Leo: We're done.

Steve: Like then illegal encryption won't work because you won't be able to transit...

Leo: You can't transit.

Steve: ...illegal encryption over the wire.

Leo: Okay, well, you've just drawn a picture of our future.

Steve: I'm afraid. I mean, I'm afraid, Leo, because this isn't going away.

Leo: Yeah, no, they're not giving up on this.

Steve: The government shows no sign. It's too easy for them to make a law. It's like, oh, good, you know, now we have a law. Everybody's got to follow the law now. And it's like, okay.

So I'm starting to wonder, Leo, whether at some point I'll start passing up reports of major ransomware attacks in the same way that I sometimes don't bother reporting on every single data breach that occurs.

Leo: Breach. I've hit that point with breaches, man; right? I mean, every minute there's a new breach.

Steve: I know. Yeah, like there was a Capital One, like last week. It's like, okay, 105 million, like another one, blah blah blah blah blah.

Leo: Every day. Every day.

Steve: I know. And if that happens, it's going to be some sad business because - and unfortunately, as we know, money is the motivator, and the bad guys have figured out that municipalities have deep pockets. So once again we have the state of Georgia. We talked recently, just after the multiple ransomware attacks on Florida, about how Georgia's courts system had at the time just been hit. In the most recent attack, the Georgia Department of Public Safety, the DPS, was hit. And this encompasses the Georgia State Patrol, the Georgia Capitol Police, and the Motor Carrier Compliance Division, which performs safety inspections.

As a result of the attacks, many police functions have been thrown back to the days before the Internet. Steve Nichols, the Chief Technology Officer for the Department of Public Safety, said that they were forced to take all servers offline while the Georgia Technology Authority investigates the attack, including email servers and servers that support the department's public website and backend. As a result, state troopers have had to resort to old-school law enforcement. If a trooper is out on a highway, writing a ticket, they now have to use a pen and paper. Remember that? A pen and paper instead of a tablet. Or, if they're looking up a license plate, they have to radio it in to a dispatcher instead of, again, using a tablet. So, like, all of their network technology is down.

So anyway, the Georgia State Police, the Georgia Capitol Police, the Department of Motor Vehicle Safety, all have had to switch to older radio and phone systems, the way they used to in the old days. I mean, so literally thrown into, like, pre-Internet. And for some reason Georgia has seen more than, I was going to say more than its share, but now that we have Florida maybe it's about on a par.

Back in March of last year, the first attack that we reported on destroyed years of stored police dash cam video, as well as freezing systems. That outage rippled such that a week later Atlanta was still rescheduling court dates. Police and other employees were writing reports by hand. Residents couldn't go online to pay their bills for, like, water, or their parking tickets. That attack a year ago was the SamSam ransomware. And I got a kick out of this because I was looking back at it. The ransom demanded to provide the decryption keys was almost quaint by today's standard. They wanted 52K, $52,000 in bitcoin. They didn't know what to ask for.

Leo: Guess not.

Steve: And as it turns out, the perpetrators of that attack were a pair of Iranian men who were tracked down and indicted in the U.S. We talked about Georgia's court systems being encrypted by Ryuk. And somebody tweeted to me, and I forgot to write it down, so I don't recall. What he was guessing was the way to pronounce it. I think it was - could it be "Reyook?" I don't remember.

Leo: I don't know. I mean, it's made up. Nobody - there's not a...

Steve: Yeah, right.

Leo: They just do it from, like, strings in the code and stuff.

Steve: Something that is found in the code or the way a file is named or something. So a few weeks ago, on July 17th, the government of Henry County in Georgia, which is...

Leo: Oh, wait a minute, though. Wait a minute. Ryuk is a character in a Japanese Manga series, "Death Note."

Steve: Ah, I think that's it. Yes, yes.

Leo: So there must be a Japanese pronunciation of Ryuk. That would be, I guess, correct.

Steve: And so it's not Russian, even though it kind of looks Russian.

Leo: No. It sounds Russian, yeah.

Steve: Yeah. Anyway, so also Henry County in Georgia, which is the fastest growing county in the metro Atlanta area, announced that it had been hit by malware, and that the county officials lost access to the Internet and most online services. And four days before that, on the 13th of July, the police department in Lawrenceville, Georgia, was hit with ransomware where the attackers encrypted most of the department's data, including body camera footage. So, what, like five attacks in Georgia?

And so in covering the news of this, Sophos had some reporting. And they finished with some bullet point guidelines. They said pick strong passwords and don't reuse passwords ever. Make regular backups. Sophos wrote, they could be your last line of defense against a six-figure ransom demand, which we now know is no longer 52K that these guys are asking for. Patch early. Patch often. Lock down RDP. Amen to that. They said criminal gangs exploit weak RDP credentials to launch targeted ransomware attacks. Turn off RDP if you don't need it. Yes, by all means. Use two-factor authentication or a VPN, as I have said. Hide your RDP. That was the title of our podcast in the last couple weeks. And then they said use anti-ransomware protection.

What was missing from their list of bullet points, and I think is glaringly obvious, is educate and test your employees. Which is something we've talked about often, and I think that's important. I mean, there really has to be an effort among the government municipalities to explain to everyone that they will be - they, individually, will be extremely inconvenienced by the loss of computation and network resources.

Maybe to drive home the point, hand out pencils and ask them to practice. Explain that the number one most common entry vector for malware into organizations, especially municipal agencies, is email which is baiting them to click links, and explain that this is not like being at home because deep-pocketed and insured government agencies are now being actively targeted by foreign attackers, and that all some one person needs to do is click on a malicious link in an email, or open a PDF and allow its macros to run, or open a Word document and release it from protected mode, and the entire municipality can get taken down. So it's not just like spam now. People in government are being targeted.

And then the final thing that is often missed, but we've also talked about this, is test. Send out baiting email from your IT department, disguised to look like something people should open, to your own organization, to your own government group, written to look like something that they should open, and see how many people take the bait. And then hold them to account. Certainly the word will spread, you know, at the water cooler that, oh, my goodness, I just got brought in, my manager just called me into his office because I clicked on email that was designed to test me. Make sure you don't do that. And so, again, I think education and sending out some of your own probes to test to see whether your people can be fooled is powerful protection. And that's something that I think ought to be part of a plan.

In something of a tease for its full disclosure presentation which will be occurring later this week during Black Hat USA 2019 in Vegas, Microsoft reported yesterday that it had detected Russia's Strontium Group, and we know them by I think about 12 different names. The most popular alternatives beside Strontium is APT28 and Fancy Bear, but there are several others that they've been named by. Microsoft detected that this state-backed, Russian-backed group are targeting, have successfully targeted VoIP phones, printers, and video decoders. And so these are considered IoT-class devices which are being used to provide them with an entry point into enterprise networks from which, once they gain a foothold there, they then pivot onto the networks' higher value targets.

Microsoft's Threat Intelligence Center said that attackers have been observed in the wild since they first spotted the campaign in April. Microsoft's researchers spotted Strontium attempting to, quote, "compromise popular IoT devices across multiple customer locations," where the hacker group exploited a VoIP phone, an office printer, and a video decoder that had not been updated. And I guess there are some printers which are publicly exposed to the Internet? I mean, that seems crazy to me because we've talked about how insecure printer firmware often is.

Leo: Well, there's a lot of printers on the Internet; right?

Steve: Yeah, that's what I mean, printers on the Internet.

Leo: Mine is because of Google Cloud Print and stuff like that. But they're behind routers.

Steve: Yeah. So as long as they're behind routers, like the printer has reached out to a server where it is maintaining some presence.

Leo: That's right. That's how Cloud Print works, yeah.

Steve: Okay, good. Good, good, good. So it's not something like that Shodan scan will turn up. And of course remember that we know that printers are exposed because there have been, we've talked about it, hacks where people are printing, like, warning pages to your printer saying "Your printer's been hacked, sucker."

Leo: Or "Please to subscribe to PewDiePie."

Steve: That's right, it was the PewDiePie guy. Yes.

Leo: Yeah, yeah. By the way, not to interrupt, but I have spoken to Masako, who works here. She's Japanese. Get ready for this.

Steve: Uh-oh.

Leo: In Japanese, there is no "R" sound. So it's pronounced Dyuku. So from now on, when you say Ryuku, it's Dyuku.

Steve: I'm not saying that. Nobody will know what I'm talking about.

Leo: No. Dyuku. Okay. There you go. I'm just telling you what she told me.

Steve: Leo, I think Skype is dropping out. I didn't hear that correctly, yeah. So anyway, Microsoft said: "The investigation uncovered that an actor had used these devices" - that's VoIP, office printer, or an un-updated video decoder - "that used these devices to gain initial access into corporate networks. In two of the cases, the passwords for the devices were deployed without changing the default manufacturer's passwords" - guys, at least make it hard for the state-sponsored Russian bad guys to get in - "the passwords were deployed without changing the default manufacturer's passwords. And in the third instance, the latest security update had not been applied to the device."

Microsoft said that after gaining entry through the compromised IoT devices, they would then scan for vulnerable systems to expand this initial foothold. They said: "After gaining access to each of the IoT devices, the actor ran tcpdump to sniff network traffic on local subnets. They were also seen enumerating administrative groups to attempt further exploitation. As the actor moved from one device to another, they would drop a simple shell script to establish persistence on the network which allowed extended access for their continued hunting."

Microsoft said it identified and blocked these attacks in their early stages, so its investigators weren't able to determine what Strontium would then attempt to steal from the compromised networks. And again, I'm sure Microsoft had some network surveillance technology they were probably providing some enterprise security. They saw this happen, and they blocked it, as you would want them to because, unless it was a honeypot, which would have been nice to have, you know, you would want to keep them from exfiltrating anything further.

Strontium's targeting of IoT devices, as we know, isn't new. That same group previously created a botnet of tens of thousands of home routers using the VPNFilter malware, which we talked about a few months ago. And in addition to Strontium, other state-sponsored groups have also started targeting IoT devices, primarily routers at this point. Microsoft plans to reveal more information about the Strontium April 2019 attacks later this week at the Black Hat USA 2019 security conference. They'll be talking about the indications of compromise that they found, IP addresses of the Strontium command-and-control servers. And actually armed with that information, organizations might want to block those on their networks, which is always useful.

Remember that one of the CIO people in Florida said - oh, in fact it was one of our listeners. It was our listener who wrote, when we talked about those attacks, that his group were automatically blocking Russian IP networks at their firewall so that there was no way even clicking a link would bring up something from a Russian IP address. You know, it's not perfect protection, but why not? Because you probably don't want the people in your municipality to be either deliberately or, much more likely, inadvertently bringing up Russian websites.

Okay. So what's our takeaway from IoT devices being compromised and serving as a pivot for deeper penetration? Again, it's something we've talked about before, and that is network segmentation, which is really the solution. And of course the problem is it's not easy. It's not the default. It's not automatic. What's automatic is just plugging things into your network and oh, look, it works. It lights up. Everything's connected. Unfortunately, yes, everything's connected to everything else.

I have here in my show notes, the easy automatic default is that, as Khan put it in the second Star Trek movie, "The Wrath of Khan," we're all one big happy family. And he said that just before he blew the crap out of Kirk, who had not raised his ship's shields for exactly that reason, because it was another ship of the Federation was approaching and hadn't responded to call signs or hails that had been issued. And Kirk said, that's mighty peculiar, I wonder why? And of course Khan said, oh, yeah, we're all one big happy family.

So unfortunately, the point is you cannot trust the VoIP system that you have sharing your common network, especially if you don't change the default login credentials for your VoIP system, and you give it an Internet-facing presence for whatever reason you might have. So that's a perfect example of a subsystem in an enterprise that can be on its own network. And network segmentation can be accomplished using Virtual LANs, VLANs. VLANs now have been available and around for so long that they are widely supported. You do need smart switches within an organization which supports VLANs. But those don't cost more.

There is some overhead in terms of management and setting them up and configuring. They're not as, again, they're not as default and automatic as just clicking wires into LAN switches. But they provide you with physical network segmentation. Well, physical at the packet level. The idea is that the Ethernet packets contain a 12-bit VLAN tag which is assigned to the Ethernet packet as it leaves the network adapter. When it then travels to the switch, the switch knows which VLAN the wire on its port is connected to and so is able to block any traffic that isn't that VLAN. So what it allows you to do, it essentially allows you to create within a single physical electrical LAN network, you are able to isolate SubLANs, that is to say VLANs, within the entire LAN.

So, for example, all of your VoIP devices could be on their own Virtual LAN. In that case, if the VoIP device were compromised, then a scan of the network would only show other VoIP devices. There would be no servers. There would be no workstations. There would be nothing else because probably your VoIP system doesn't need to have contact with your printers, for example, or your enterprise servers. They don't need it. And so the point is, unfortunately, the default is everything sees everything else. And if that's the way your network is set up, and an IoT device, some security camera is plugged into your network, then it sees everything else.

Well, it's probably the case that a security camera doesn't need to see everything else. So it should be on a separate VLAN, that is, its traffic should be tagged with a Virtual LAN tag. Since they're 12-bit tags, you can have 4,094 of them. The zero tag and the all ones tag are reserved. So otherwise it's be 4,096. So it's 4,094. So, I mean, you've got lots of tags. Everything can, in groups, can be connected to its own subnet and thus blinding, for example, your IoT devices to your enterprise servers, and maybe your workstation networks. Or if departments don't need to see other departments, you could create VLANs for use within a department. And then it is possible to soften the rules on a per-machine basis where you need to.

But anyway, I just wanted to sort of put this notion on everyone's radar. We have not talked about VLANs a lot from a security standpoint. Because the network VLAN tagging occurs at the Ethernet level on the device driver, or sometimes the tagging can be done by the smart switch so that it's completely outside of the realm of the attacker. There's nothing the attacker can do in order to see or mess with that VLAN tag. So it can be a high-security solution. It has a big overhead. I mean, I don't mean to be minimizing the management overhead because it really increases the complexity of your network. Suddenly now there's another big layer of additional work that is to establish and then to manage lots of subnetworks on your LAN.

So nothing works automatically when you just click it into a network switch. Now you've got to think about where you want to have it participating, what networks it wants to be a part of. But as we know, good security isn't free. Real security comes at some cost. And it just seems to me that this is another one of these things where this is the direction we're heading in. We're moving into a world where - we used a term the other day about IoT. It wasn't Internet of Trojans. It was something, Invitation of Trojans or something, I can't remember what the term was that I used [Installation of Trojan SN-721].

But the point is that, in a large enterprise, where you have lots of things going on, you cannot trust - you should not trust, you cannot trust - the absolute security of every single device on your network. And now, where there is tremendous pressure on the part of the bad guys getting in, they're not just wanting to set up a botnet or to use your servers as a proxy. They're wanting to encrypt everything that they can get their hands on and then hold your organization for ransom.

So it is also the kind of thing that you can start gradually. As long as you have VLAN-aware switches, that would be the first thing to do, if you don't, would be to rotate the hardware through. So there's some hardware expense. But you could start moving things over gradually into individual virtual LANs. It's not the kind of thing where it has to be an all-or-nothing proposition. So it can be done incrementally. So anyway, I just wanted to talk about it because it's not something that we had ever talked about before.

And it's, you know, we've talked about network segmentation. My favorite router was the little Edge router because it had individual NICs instead of just being a switch to creating multiple ports. Each of the ports was a NIC. And my now current favorite is the SG-1100 from Netgate. I love that. And it's got two ports on the inside so you could easily segment to a WiFi and a wired and put them on separate networks, or an IoT network and a non-IoT network and have those on physically separate networks. So it's not easy, unfortunately, but we're in a world now where we just can't trust the devices that we have on our network.

Last week Google released Chrome 76 for, you know, across all of the platforms - Windows, Mac, and Linux. And two things happened. Thankfully, Adobe's Flash, which as we know has caused so much destruction and disruption for decades, they made another change. I mean, they're sort of lowering the boom on Flash. They're not going to fully discontinue support for Flash until the end of 2020. But here we are, a year and a half away from that, and so they've gone another step. It had been the case that it was disabled by default, but you could enable Flash on a per-site basis.

That changed last week with Chrome 76. Now, even had you previously enabled Flash for some sites, Chrome will no longer remember that. Meaning that users of Chrome will now be forced to permit Flash to run on an "every single time they use it" basis. So it still will work. But it's just basically upping the ante further. It's making it further burdensome to run Flash on sites that require it, which clearly is Google's way of pushing back even harder on any site.

I ran across one the other day. I can't remember now what it was. The entire site was a Flash site where you would just go there, and it said - all you got was a page saying - and Leo, you remember those days, I mean, it was like, you know, it hasn't been that way for a long time. But it would be like, "You need to load Flash in order to use this site." Somebody wrote the entire website in Flash. And without it, you didn't have a site. And so, you know, fortunately those days are long gone.

But anyway, with any luck there will be enough annoyance from users that the sites that are still, for whatever reason, running Flash, they'll either just - maybe they just don't matter at this point, if they're still running Flash, and they'll just fall by the wayside. But for now, every time, with Chrome 76, you've got to say yes, I want to enable Flash. And it'll work until you come back the next day, and then you've got give it permission again.

And the other thing that they did is something that we talked about while you were on - it was on your week off, Leo, that I talked about it with Jason, which is that there are sites that have pay walls which plant a cookie on their visitors' browsers in order to track how many times they view what would otherwise be behind a pay wall. And you get a little note saying, you know, this is your third article that you've viewed this month. This is the last one you can view. Please consider paying. The point is that they are storing a little bit of history in the user's browser.

Well, apparently people realized that Incognito mode would automatically flush that, and the pay walls would allow you to have an infinite number of free views. That word spread. And so in order to counteract that, the sites that are behind pay walls, and I think the Washington Post is one of them, would refuse to work at all if they sensed you were in Incognito mode. Well, that was worrisome because people felt that having sites know they were in Incognito mode wasn't very incognito. That is, they didn't want it to be obvious that they were using Incognito mode.

Well, it turns out that what was happening was that in Incognito mode Chrome disables the file system API. And there are sites which are now checking for the functioning of the file system API as a means of sensing whether Incognito mode is in use, and that's what brings up the notice saying, sorry, we're happy to have you use our for-pay site, even on a trial basis, but not in Incognito mode.

And so anyway, with Chrome 76, this changed such that it is no longer possible for those sites, or any sites, to probe with the file system API to determine if you're visiting them in Incognito mode. And Google has said, if sites start doing something else in order to sense Incognito mode, then they will respond again, so don't bother. If users want to be incognito, they want to be incognito, and we're going to support their ability to be so. So anyway, not a huge incremental change in Chrome, but just something.

Oh. I have a link. I'm confirmed to present SQRL in two and a half weeks at Southern California's Orange County OWASP meeting, which is on August 22nd. So I did want to make a note for any of our listeners who might be within reach of Orange County, that I'll be presenting sort of the history of SQRL, where it all came - how it happened, all of the considerations that went into it, how it works, the whole kit and caboodle. And I also did mention that I'll be in Dublin, Ireland and Gothenburg, Sweden in September.

Leo: This is the world tour now. And of course Boston in October.

Steve: And Boston in October.

Leo: By the way, we have just learned who the fourth person on our panel will be, and I'm really thrilled to say it's going to be Bill Cheswick, "Ches," the man who invented the firewall, wrote one of the very first books on firewalls. He's a fantastic security expert. And like you...

Steve: I know the name, yeah.

Leo: Ches is a polymath in all sorts of directions. And he's going to be a great - he's been writing a lot lately about what's next after the password. So it'll be really good to have Ches on that panel.

Steve: Very cool.

Leo: Yeah, it's going to be a fantastic panel. We'll give you more details soon. It's not - all the details aren't in completely. But it'll be the first week in October in Boston, and it will be open to the public. And we'll let you know as soon as people can sign up to come see it. It'll be Steve Gibson, the CISO of LogMeIn Gerald Beuchelt, and now we know Bill Cheswick, and myself.

Steve: Very cool.

Leo: And then that could be another opportunity for us to talk about SQRL because authentication is the topic, you know, how to prove you are who you say you are, and what's after passwords. So couldn't be more right on with SQRL.

Steve: Yeah, nice.

Leo: Yeah.

Steve: So I got a tweet from a listener, Joshua Kelley, who said: "Hey, Steve. I know you've talked about Firefox Send in the past on Security Now!. I found this great command line tool for interacting with it." And I just wanted to give our listeners a heads up. It does look very cool. It's multiplatform. It's on GitHub. It's github.com/timvisee/ffsend. Probably if you just google "GitHub ffsend" for Firefox Send.

Leo: Well, you just go to send.firefox.com.

Steve: Well, that's the browser based.

Leo: Oh, I see, for the command line; right.

Steve: Yeah, yeah. So GitHub says: "Easily and securely share files from the command line. A fully featured Firefox Send client."

Leo: This is somebody's third-party version of it.

Steve: Correct. So it uses the Firefox Send API.

Leo: By a POST command? Yeah, yeah.

Steve: Yeah.

Leo: Oh, okay.

Steve: And so Linux, Mac, Windows, FreeBSD. Other BSDs might work. You need a terminal and an Internet connection. And so I just - I thought it was cool. I mean, I'm a fan of Firefox Send. I have the client for the one I was using. I don't see it in front of me right now. Oh, yeah. No, it's not FreeFileSync. Maybe it's - no. I'm not seeing it. But anyway, the problem with it was that the free version of whatever the thing I was using, it would only give you a couple files in some period of time, and then it would say no more for you. Whereas Firefox Send is limited to a gig file if you don't log into Mozilla, 2.5GB if you do, but there's no limit on the number that you can use. So I just thought I just wanted to - I know that we have listeners who like command line things. So this is a command line tool for using Firefox Send, which I thought was very cool.

Leo: Yeah.

Steve: And Leo, let's take our last break, and then we're going to talk about file synchronization.

Leo: I feel like you could probably use cURL or something like it to do a POST to Send. I'm going to have to look at that.

Steve: Well, there is an API, and it involves client-side encryption.

Leo: I'm looking at this code. There's a lot of code here.

Steve: Yeah. Client-side encryption and synchronization and pulling the API. Oh, and you're able to type in a history, and they'll show you a history of all the things that you've sent.

Leo: So Send encrypts on your end in JavaScript. Is that correct? Yeah.

Steve: Right, yes.

Leo: I've used for years Transfer.sh, but I don't know how well encrypted it is. You're storing a file on a third party's drive. Although you could have your own Transfer.sh running on your system. I've used that for years. Anyway...

Steve: Ah. Filemail. That's the service.

Leo: Oh, yeah, that was the big fat one, yeah, yeah, yeah, Filemail.

Steve: Yes. That was the one I would - that's the one that I was thinking of. But I switched over to Firefox Send because it's a win.

So as I mentioned at the top of the show, I have two workstations now where I spend a substantial amount of time. I don't need to keep everything synchronized. So I don't need, like, cloning of drives or something. I only wanted to have synchronized the things that I'm actively working on at each location. And of course I have plenty of my own resources. So my first thought was to make a Drobo. Actually I have Drobos at each location also. So my first thought was to make a Drobo here at my primary location available to my secondary location. So that would be like my own cloud, and then both workstations would synchronize to it.

So I tried that first. I experimented with a number of directory synchronization utilities and tools. I did not find the one when I was initially looking that I ended up finding, that I will talk about at the end here. So I was looking around for some way of, with mapped drives, of keeping things synced. I found something that I liked a lot that's just called FreeFileSync. And so I want to touch on it for our listeners because it might solve some problems or be useful for some people's purposes. It's free, as its name sounds, FreeFileSync. It's FreeFileSync, S-Y-N-C, dot org. It describes itself as a folder comparison and synchronization software that creates and manages backup copies of all your important files.

Instead of copying every file every time, FreeFileSync determines the differences between a source and target folder and transfers only the minimum amount of data needed. FreeFileSync is open source software, available for Windows, Mac, and Linux. And I liked it a lot. I was using it for a while. And when used manually, it's pretty terrific. It scans, and you can see what it proposes to do before it does it. It's got lots of fancy rules and all the exceptions and controls and bells and whistles that you could want.

But I was never able to get it to work automatically. And obviously, for reliable synchronization, you don't want like a timed recheck for synchronization, or even like synchronization on shutdown. You want it just to be happening constantly in the background. I was never able to get - it sort of has like an automated system, but it just was kind of funky and didn't work right. Then finally, a couple times, I had forgotten to manually perform the sync to the Drobo before I left one end or the other. And so I was annoyed by not having the latest copy of my files that I wanted to work on. So that wasn't the right solution, obviously.

I have secure tunnels between my two locations. That's easy. I'm using OpenVPN. So I did for a while consider mapping a drive - so in that model I had sort of the Drobo as the common store, and I was synchronizing both workstations to that single Drobo. So that was a problem. But then I considered mapping a drive through a tunnel so that my secondary location would simply reach into the drive of my primary location. And so I sort of wouldn't, like, have any synchronization problem at all. But of course that meant that the end that did not have the files, that was reading them through the network, would have to be continuously reading and writing over the Internet. So that was obviously not the right way to go.

And I should mention, too, that it wasn't my intention when I began to solve this problem to make this a career. I just, I mean, I was like in the middle of working on this stuff, and I thought, okay, I just - I don't want to be copying this with a thumb drive and then taking it to the other location, which I was initially doing. That's dumb in today's world. So the first thing I thought was, okay, I'll just turn on Google Drive. I'd used it in the past. I hadn't been that impressed with it. But you get 15GB for free with Google.

As I've mentioned, I use Google Drive. I use Google Docs to create the show notes every week. I have a bunch of stuff up on Google Drive. So I thought, okay, I'll download the client for Windows and see how that works. And I had not had great success with it in the past, as I mentioned, but I was also on XP. So since then I've moved to 7. And I thought, well, maybe it is more friendly, or it works better or whatever. But no. It didn't work for me. I was getting, I don't know if it's because of the apps I was using, but I was getting weird "file locked" errors and complaints from apps that files were locked and kind of weird behavior. So after a while I thought, okay, well, this is an annoyance. This isn't working.

So I thought, ah. If anybody knows how to do a networked drive, kind of a virtual drive client, it would be Microsoft. So I thought, what about OneDrive? Let's give that a try. And I was using the newer Office 2016, which was OneDrive aware. So I was sort of seeing it offering me OneDrive stuff, and I hadn't been paying attention to that. But it was on my radar. So I downloaded the OneDrive client on both machines. And I was just using OneDrive. You get 5GB free from Microsoft. And again, I don't need terabytes of data. I just - I'm only using, you know, the documents that I'm working on. And I'm working on the third of the four SQRL documentation documents now. And so I just, you know, or source code for SQRL also, or other projects and documents. So I don't need a huge amount of storage.

Anyway, it worked for a while. And then I started getting weird merge errors where it would complain. It would say that it was unable to reconcile the differences between files at each end. And I ought to mention that of course the way this whole idea works is that I had local copies of the files on each workstation's hard drive. And so I was working with them locally so everything was quick and snappy and fast. And then the idea would be that file sync would synchronize to a common third cloud store, and so it would just all happen automatically. Except that it didn't work after a while. Finally, it got stuck where I don't remember which of the workstations it stuck on, but all of the little icons showed the synchronizing spinning arrows, and I couldn't get that to stop. I shut it down. I restarted. I rebooted. It just was stuck.

And when I went online, it turns out - this is like a problem with OneDrive that Microsoft has had from the beginning. Oh, and when it was complaining for a while with this merging problem, it was creating duplicates. That's the problem that people complain about online is that Microsoft is saying, well, we were unable to reconcile the differences, so you got two copies of this. And it's like, I don't want some sort of reconciliation of files. I just want, you know, I'm not in two places at once. I'm not changing two files in different locations at the same time. I just want the newer one to replace the older one. So that didn't seem hard, but seemed somehow to be confusing Microsoft.

So also, for quite some time, I've had a free 2GB Dropbox web account. I've had that because sometimes I'll create or edit a video here in my daily workplace, like I'll download something from my TiVo, quickly edit out the commercials, and then it's something that I want to share with Lorrie in the evening. So I had been sticking it on this Dropbox web account because there is an app for the Roku called Roksbox. It's a free app, R-O-K-S-B-O-X, which is a nice little streaming thing that will stream from cloud services. And so I would drop things in Dropbox here. And then when I'm at my other location in the evening, I'd share something with Lorrie that I wanted to share.

So I'd sort of had Dropbox on my mind. And I thought, you know, they've been doing this from the beginning. Maybe they figured out how to get it right. So I figured I would give it a go. But 2GB is not much storage. They're the leanest of any of the free services. So I thought, okay, I'm going to - oh, I guess I did try it briefly with clients on both systems, just using the free account. And it really did seem to work right. And I really liked the features that it had. There are a bunch of extra goodies that sort of made sense, like I could create a video folder within my Dropbox folder and mark that as "Online Only," which meant that it did not keep a local copy when I dropped something there. It only sent it to the cloud, which was perfect for my mode of just wanting to put something there to watch through the Roku later.

And the more I got to know it, the better I liked it. So I bit the bullet, and for $10 a month I went from 2GB to a 1,000GB, which is to say a terabyte of storage, which means I no longer need to be deleting videos all the time that we've watched because I'm running out of room. And I've got, like, more than enough space.

Leo: Is it just videos you want to do this with? Or it's other files, too; right?

Steve: Oh, it's all kinds of other stuff.

Leo: Because for video, I mean, running a Plex server would be the easiest thing to do, and then get the Plex client in your Roku, and you'd be done.

Steve: Okay. But yes. So much more than video. All of my other - so all kinds of, you know, source code, assembly source...

Leo: Stuff you're working on. That makes sense.

Steve: Yeah, exactly, all the stuff I'm working on. So the one thing I haven't talked about with all of this is encryption. But I'll just finish by saying that, until this morning, I was completely happy. Well, I'm still completely happy with Dropbox. It is, I mean, in my opinion, they have nailed this problem. It's not free. It's $10 a month for a terabyte. But I've been using it now for about a month, and it never misfires. It never gets anything wrong. It doesn't complain about synchronization. It's never telling me that my files are locked or, like, I mean, it is beautiful. It's got all the features I want. I can create a directory hierarchy. I can mark things for online and things for local storage.

I have not bitten the bullet and added encryption. And of course we started talking about cloud storage and encryption as we mentioned with Jungle Disk back in the day, the idea of doing client-side encryption and then storing things in the cloud. But at the moment, nothing I'm doing is secret. The SQRL docs aren't secret. My source code for SQRL, you know, I've given big chunks of it, and in fact the entire thing, to several other developers who wanted to use it as a reference.

Leo: You don't use any repository-style, like Git or something.

Steve: No. No. I never have. So I have not added TNO-style encryption to this. Once upon a time, Boxcryptor was a favorite. And like its name, the way its name is, it's an encryption for - it is encryption for Dropbox. And it does client-side encryption. And I looked at it some time ago. What's annoying to me is that today everybody wants us to sign up to a service model. And I'm still a little too old school for that. I'm a little - I have to confess I'm very resistant to that. If I'm actively using someone else's bandwidth or their storage on an ongoing basis, then a pay for what you use model makes sense. But for me, not for software. I'm not ever going to do some charge, like a pay-as-you-go for SpinRite. You get it, and it's yours. You can use it as much as you want forever.

However, there is a free version of Boxcryptor which has otherwise also switched to the service model. There's a free version which does allow you to use one cloud provider on two devices. So if it does the file syncing thing correctly, and it's not something that I've looked at yet, that might be a solution for providing encrypted cloud storage if I'm ever in a - if I'm doing something where I really want TNO, you know, true TNO client-side encryption, and if it would allow me to encrypt a subset of folders under Dropbox. Or, if not, since, for example, if it were the SpinRite source that I will be working on as soon as I wrap up the documentation for SQRL and get that fully launched, then what I could probably do, since my source code is not big, is get a different free 2GB Dropbox account for SpinRite and then use Boxcryptor in that mode from my two locations. So I just sort of wanted to share all of that.

I was also conscious of the fact that we have a cloud storage provider who is a sponsor of the TWiT Network, Wasabi. So I was sort of curious to see what they were up to. I'm impressed by what I saw because I dug through all of their stuff. They look like a very good solution as a CDN. The fact that they don't charge for downloads is huge. And in fact, I'm using AWS, some S3 buckets for some SQRL videos, and I've noticed that, as that's become more popular, my cost has been increasing. That would not be the case with Wasabi. But they're more of an enterprise-oriented CDN profile, as opposed to an end-user consumer profile.

They do export an S3 API. And so I was curious to look and see if there was any sort of a good - and I had looked before, looked for an S3 sync provider. There is something on GitHub called S4 for S3 solutions. So another S, thus S4. But it didn't look like - it was written in Python, and it didn't look like it had all the bells and whistles that I was interested in.

While finishing this discussion for this podcast, I stumbled upon four other solutions: ownCloud, Nextcloud, Seafile, and SparkleShare. And of them, ownCloud looks very nice.

Leo: So you are not party to the ownCloud drama, so I'll just fill you in real quick.

Steve: I am not. So tell me.

Leo: So ownCloud, which is an open source platform, kind of got turned into a business. And a lot of people were unhappy about what happened to ownCloud. Nextcloud was created with a fork of ownCloud.

Steve: Okay.

Leo: And so anything you like about ownCloud should be available in Nextcloud, and then some, in my opinion. I think at this point I would strongly prefer Nextcloud over ownCloud for a variety of reasons. You can read about the drama.

Steve: Okay.

Leo: You'll find it if you do a little search.

Steve: And so is it as feature-complete and a good client?

Leo: Yeah, yeah.

Steve: Because what I wanted to mention was - so I will take your advice immediately, Leo. Oh, one reason I liked it was I thought I remembered that I saw it as an app on Drobo, and sure enough, there is an ownCloud server for Drobo. So maybe there is a...

Leo: Yeah. There's probably a Nextcloud client, as well. That's pretty usually common. But there's nothing wrong with ownCloud. I think it's fine. I think a lot of the drama has to do with personalities as much as anything else. But I'll send you a link or two, and you can read it online.

Steve: Okay. So what I like about ownCloud, well, first of all, so...

Leo: There were also security issues with ownCloud which you should read up on. I don't know if they've been resolved.

Steve: Oh, good, good, good. Well, I should also mention there is no way I would ever publicly expose any of this. I mean, I just...

Leo: Right, so it doesn't really matter, yeah.

Steve: Exactly.

Leo: Do you not have a Synology or another NAS solution? Is Drobo your only NAS?

Steve: Drobo is my only NAS.

Leo: I would look at Synology. I think you'll be really impressed. And a lot of these things will be solved.

Steve: Well, actually, yeah. What I'm thinking of is FreeBSD and...

Leo: Do it yourself, sure.

Steve: And stick a FreeBSD server up at Level 3.

Leo: There's also FreeNAS, which is open source Linux NAS software.

Steve: You know, I tried that first.

Leo: Oh, really.

Steve: And I didn't find that it added anything. It was, I mean, it's on top of FreeBSD.

Leo: Right.

Steve: And so it gives you sort of a GUI, but...

Leo: Right, headless interface, yeah.

Steve: Yeah, exactly. So where I ended up was, if I were a person who did not have the storage and networking and other resources, I am just bullish on Dropbox. I mean, for, like, what - I know I'm, like, probably telling people things they already know. I mentioned this to Lorrie yesterday, and she looked at me, and she said, "Yeah, that's what everyone uses." I said oh.

Leo: I love Dropbox. I use it, too. But I use them all. There's also Tresorit and SpiderOak, which are both Trust No One, that you probably should look at. I like Tresorit a lot.

Steve: Well, but do they do sync?

Leo: Yeah. Absolutely.

Steve: And, I mean, because that's been the problem is I had not found a really good sync solution. So I thought that SpiderOak...

Leo: SpiderOak is less desirable because I think it's Java based. But look at T-R-E-S-O-R-I-T. They also have a file send capability much like Firefox Send.

Steve: Okay.

Leo: I used them for a while. I don't need eight different clouds. But I was very happy with Tresorit. And it claims to be end to end, Trust No One.

Steve: Okay.

Leo: Which I know you would like.

Steve: Yeah, yeah, yeah. So anyway, I had not found, until this morning, when I stumbled on ownCloud and Nextcloud, I had not found a robust sync that really seemed to work for me. And of course I like the idea of having my own server that I'm not having to pay Dropbox $10 a month. And I just feel much more comfortable with my own data in my own cloud. And of course everything is TLS and secure. So anyway, if that's of any use to anybody, if the story of my journey to synchronize two different systems - I mean, again, maybe this is like, duh, Gibson, where have you been; you know? But I had never had the need before. And finally, thanks to Dropbox, I found something that works and is not very expensive, and maybe even a free solution.

Leo: Yeah. You know, this is a universal problem. It's just now, because you finally left the house...

Steve: Yes. That's what happened. I finally left the house, Leo.

Leo: Almost everybody at least goes to a job; right? So you just stay there. So you don't have to worry about this.

Steve: Correct.

Leo: So, yeah, I'm really interested to watch your journey on this because you're tracking through all the things that we have kind of piecemeal tracked through. So it's nice. It's really, in a way, you have an advantage by doing it all at once. You can really go head to head and see what does what.

Steve: Well, and I was disappointed because, like, Google was having these problems, and then OneDrive was having these problems. And it's like, I thought these things would work. But no. It turns out it's not an easy problem to solve. So I have to say I will try these other things. And I have no experience yet with ownCloud and Nextcloud.

Leo: I think either would be fine. There was a schism.

Steve: Ah. As there sometimes is.

Leo: In open source it's very common.

Steve: Yup.

Leo: But they started with the same code base a few years ago, probably Nextcloud, and they've probably diverged quite a bit by now. It's interesting because one thing that I do, and I think a lot of other people do, is depending on the type of data, that's why I was saying for videos I use Plex. Video, audio, podcasts, I use Plex. For source code, I use Git. You know, so I think a lot of people have said, well, I'm going to, for this kind of there's this.

And then for just my standard, I have a standard data folder, a documents folder that's on every system I have. And I have more than a dozen. And it's hosted on my Synology NAS. And Synology has synchronization software that I put on everything at the beginning. And at that point I have a common documents folder that is stored on every computer. And that is really great if you're moving around a lot and you want to make sure that whatever laptop or phone or whatever that you bring with you will have a common set of data. And at this point it's several hundred gigabytes, I think. I don't know exactly how big it is. But it does a good job.

Steve: And so when you do that, you're not bringing local copies to the machine?

Leo: I am. No, no, no, no, no, no, no. The first time I sync.

Steve: Several hundred gig comes onto the machine.

Leo: Yeah. I mean, I could if I want copy the documents folder from one machine to the other. Sometimes I'll do that.

Steve: Hah, right.

Leo: The sync is smart enough to say, oh, you have these, but you don't have this. I don't have a big duplication problem. The Synology does an excellent job. It's called Synology Drive. And it's on the Synology. So my Synology at home has the master copy. But this laptop, that desktop, these phones, they all have access to it and to a greater or lesser degree will have - something with enough storage will have the full documents folder.

Steve: Right.

Leo: And that's great because then I never have to say - and you could use it as a poor man's Git because, you know, if I'm saving code, that's fine. If you're working with somebody else, it's another matter. Then shared code you want to keep track. You want to source - you want somebody to blame, to be honest.

Steve: Right. Well, of course, so one of the other nice things, I've been talking about the fear of ransomware. And Dropbox does versioning. So you can...

Leo: Yes, that's nice.

Steve: You can reach back in time.

Leo: I love that.

Steve: And on the other hand, both ownCloud and Nextcloud presumably, I know that ownCloud does, they also do versioning.

Leo: Yeah.

Steve: So you have that. And I'm still using, you know, I'm old school. I've talked about it before, FileBack PC. It's only PC hosted. But the guy's still there. It's still supported. And it does very sophisticated versioning that can be well tuned. And so that's what I use right now is like, whenever I'm working in assembly code, incremental versions are going to my Drobo just all the time because I don't ever want to lose anything.

Leo: If you went to FreeNAS or a FreeBSD solution, you'd be on ZFS. You'd be doing snapshots, so you'd have that versioning.

Steve: Yes.

Leo: With Synology, I've never had occasion to use it, but Synology's on Btrfs and so it does snapshots, as well. So there's behind-the-scenes versioning, even lower level than just that app running. Which I think is a very handy thing because you could say, oh, crap, I just cryptoed everything, blast it away, and restore from a snapshot. And that would be a really nice thing to have.

Steve: Yeah. I'm just in the process of getting ready to put another server up, a big NAS up at Level 3. And now that I've run across these open source, I mean...

Leo: Oh, there's some great stuff out there, yeah.

Steve: Given that it works reliably. Again, I was hoping for Google, and I was hoping for OneDrive, and they both screwed up. So far, Dropbox is the only thing I've found. But I'll give the ownCloud or the Nextcloud a try.

Leo: Nextcloud will do a lot of the things that you want to do, including, by the way, for a lot of people, when Evernote went commercial, they replaced Evernote. My Synology has a note replacement that's every bit as good as Evernote, but I host it.

Any NAS is a great backup solution, too. And because they tend to be giant storage units, I back up all my music, all my photos, all my data on the Synology and still use it to do my notes and my documents. So a NAS is a wonderful thing to have, I think.

Steve: And the one other nice thing I forgot to mention about the open source cloud solutions, ownCloud and Nextcloud, is they allow you to designate other directories on your systems to be synced. Whereas Dropbox...

Leo: So annoying.

Steve: ...everything is under, yes.

Leo: The Dropbox folders, yeah.

Steve: And that's really what I want because I have a whole assembly code tree, and I would just like to be able to say, instead of having to move all of my work underneath Dropbox, I'd like to be able to say "keep this thing current."

Leo: I seem to remember Tresorit also will let you designate arbitrary folders, as opposed to OneDrive, Dropbox, and Google Drive, which say it's all got to be in this special folder. Being able to designate arbitrary folders, say "back up my assembly folder and my music folder and this," is, I agree with you, very important.

Steve: Yeah, yeah.

Leo: Nextcloud will also do calendaring, so you can have a shared calendar that's not running on Google. I mean, Google works fine for me, but, you know. Same thing with address book. If you wanted to go really full private, that's the kind of solution, those are the kinds of solutions you want to look at, I think, running your own NAS.

Steve: So Tresorit Personal, oh, try it free for 14 days. So it's not free.

Leo: Yeah. It's only a gig. Oh, no, it's not free. It's just like Dropbox. It's a Dropbox competitor.

Steve: $30 per month.

Leo: That's for teams, I think. Look at the personal.

Steve: No, that's personal.

Leo: Really.

Steve: Tresorit Solo is designed for individual users.

Leo: That's ridiculous.

Steve: Yeah.

Leo: But you get 2TB. I see. That's why. I wonder if they have a smaller tier because that's an awful lot.

Steve: Yeah, that's the bottom one, designed for individual users.

Leo: Oh, maybe that's why I didn't - wait a minute. No, no, no, no, no, no. 200GB is $10 a month.

Steve: Oh, okay.

Leo: Yeah, yeah. I think you're looking at the 2TB, which is nice. But if you're going to go that big, go with a NAS.

Steve: So 200.

Leo: 200GB is $12.50 monthly, or $10.42 if you do it annually, 120 bucks.

Steve: So I guess, if you needed end-to-end encryption, because that's more expensive than Dropbox, but you do get encryption.

Leo: You know, if you're price sensitive, Google Drive's probably the cheapest. But it doesn't do what you want it to do, so...

Steve: It doesn't work. Yeah. And actually, I'm not price sensitive. But, as I said, I also like - I imagine a lot of our listeners are, like, already downloading copies of Nextcloud.

Leo: Yeah, Nextcloud is pretty amazing. And by the way, that will run on another sponsor, Helm. They're going to add Nextcloud capability to turn Helm into a NAS, basically. But again, if you really want to do it right, I would get a NAS. Either roll your own, because Steve likes to roll his own, or get Synology.

Steve: And Leo, a NAS is nothing these days but a PC with a whole bunch of hard drives.

Leo: Yeah. Right.

Steve: And you run FreeBSD or Linux and ZFS, and now, yeah, I mean, so it's not a big deal.

Leo: No, no, no, not at all. I think you probably, you know, if you're going to build it yourself, you can put more horsepower in it, a lot more RAM, stuff like that. That tends to be pricey on these commercial NASes.

Steve: Yeah. And I am a little annoyed that the Drobo's processor seems to be a little slow.

Leo: It's anemic, yeah.

Steve: They did not, yeah, like you're sitting here waiting for the web page to come up. It's like, come on.

Leo: In Synology you can get a better - it's still an Atom. It's not the super fastest processor. You can put cache memory in. You can put additional memory or a little NVMe cache card which speeds up small file writes. I have not had an issue with Synology. I think it's sufficient for a single user. I don't think we would use it here for...

Steve: For an enterprise, yeah.

Leo: For enterprise, yeah. But I think it's...

Steve: And again, it's easy to give a big, beefy machine a bunch of drives.

Leo: Why not, if you've got a machine.

Steve: Like here you go.

Leo: Yeah, that's right, yeah. And then you can choose your own RAID card. You can do hardware RAID, and you can get a good Promise card or something. You have a little more control over it. But that takes some more work; right? So it's whether you've got the time or not.

Steve: Well, yeah. And I didn't start, I mean, I started just trying to stop carrying a thumb drive back and forth.

Leo: You know, it's funny because you have gone through in a month the evolution that's taken the rest of us decades. You've gone from thumb drive...

Steve: Only because I'm, like, so old school. And as you said, I never left the house, so I didn't need - there was nowhere I was going anywhere, so...

Leo: When you get around to trying Keybase, one of the things that I use and I love the best about Keybase is they have a private encrypted Git that's all yours. And so I use that for taxes, financial information, stuff like that. Because it's a Git, I can sync it, which is fantastic. And it's fully encrypted, end-to-end encrypted, which I really like. And that's free. I don't know, eventually they've got to start charging for that. But that's a really remarkable solution. They don't have nearly the storage capacity, though, of these big cloud companies. It's a great subject. I would love to hear your continued notes as you evolve.

Steve: If I come up with any - and I imagine our listeners have probably enjoyed hearing us talk about these things, too.

Leo: You'll hear a lot more from them at GRC.com.

Steve: Oh, I knew that was going to happen. Oh, Steve, try this, try this.

Leo: GRC.com/feedback or, even better, the Twitter DM. He accepts DMs from anybody at @SGgrc on Twitter. Of course, if you go to GRC.com, my god, it's just an endless treasure trove of information. Starts with the bread and butter, which is of course the world's finest hard drive maintenance and recovery utility, SpinRite. Buy a copy. Just say thank you, Steve, I'm buying a copy. And that way you'll get the update when it comes out. But you'll also want to read all the free stuff he's put up there, all the information. And you can get a copy of this show there. He's got 64Kb audio. He's got such a low quality audio we don't even want it, the 16Kb audio for the bandwidth impaired.

He also actually has the smallest version of the show, which is beautifully written transcripts Elaine Farris puts together every week. So if you like to read along while you listen, that's a good suggestion. And the best value of that is that it makes it googleable. You can search into the shows and find the part you're looking for. So that really is a boon. All his shows are up there, all the shows, 726 of them are up there.

We also have audio and video at TWiT.tv/sn. But of course we always encourage you to subscribe. That's the best way to get our shows because that way you get it automatically. You don't have to think about it. It'll be on your phone when you get in the car tomorrow morning. And you can do that in any podcast application.

It's funny, I was talking to my physician, who is a podcast listener and listens to a number of our shows. And I don't think he knew that you could do that. He was like, downloading it to his computer and then syncing it over to his phone. I said, "Get a podcast app. Any one will do. Overcast, Pocket Casts. Google or Apple both have podcast apps." Subscribe. That way you'll get it automatically.

Steve, always a pleasure. What are you watching on TV these days?

Steve: We just sort of wind down at the end of the day. Lorrie had never seen the series "Medium," which I really liked.

Leo: Oh, what a great show. Yeah, that was a good show, yeah.

Steve: Seven seasons, and we just finished that.

Leo: So it's kind of fun to go back in time and look at the old shows.

Steve: Yeah. And she also had never seen - what was the one with Simon Baker?

Leo: I don't know.

Steve: "The Mentalist" she had never seen.

Leo: Oh, fun.

Steve: And that was really, really fun also. So we're just sort of watching old stuff and staying...

Leo: Till something great comes along, huh?

Steve: Exactly. Although we're going to watch the Showtime series, the Roger Ailes.

Leo: Roger Ailes, "The Loudest Voice" in the room.

Steve: That sounds fun.

Leo: It's so good. And to see Russell Crowe, who's a great actor, he really embodies Roger Ailes in this, in the biggest fat suit you ever saw.

Steve: Well, and didn't he...

Leo: Did he gain weight, or is it a fat suit?

Steve: I was assuming he gained weight because I saw like a preview, and I thought, oh, my goodness.

Leo: I have to think it's a fat suit because...

Steve: But his face is full. I mean...

Leo: Well, they put - it's prosthetics.

Steve: Wow, okay.

Leo: You remember the Dick Cheney movie, "Vice."

Steve: Yeah?

Leo: Same thing. I've gotten his name. They got one of our best actors they got to do him. And it was all prosthetics and a fat voice.

Steve: Wow.

Leo: A fat suit. Or a fat voice. I'll find out. I hope Russell Crowe didn't gain weight for that because frankly, if he did, he doesn't have long to live. It's a couple hundred pounds. You know?

Steve: Woody Harrelson.

Leo: No, not Woody Harrelson.

Steve: It wasn't Woody Harrelson, huh.

Leo: He was Batman. What's his name? I don't know. The chatroom. Christian Bale. Thank you. The chatroom would know.

Steve: Ah, that's right, that's right, that's right.

Leo: Steven, have a great week.

Steve: Okay, my friend.

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

Steve: Right-o.