Considering PGP

Description: This week, Steve and Leo continue covering the consequences of the Snowden leaks and, with that in mind, they examine the Pretty Good Privacy (PGP) system for securely encrypting eMail and attachments.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-418.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-418-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson, our security guru, is here. This is a show everybody has to watch. In fact, share it with your friends, your neighbors, your colleagues: Using PGP to protect your email. Steve talks about it next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 418, recorded August 21st, 2013: Considering PGP.

It's time for Security Now!, the show that covers your security, your privacy, your safety online with this man here, the 'Splainer in Chief, Steven Gibson at GRC.com. Hey, Steverino.

Steve Gibson: Hey, Leo. Great to be with you for Show No. 1 of Year No. 9.

Leo: Wow.

Steve: We begin our ninth year.

Leo: Wow. Episode 418, and you've only missed one, and that was because we made you.

Steve: Yeah. So we're not going to do that again. That was not pretty. There was an uprising among the natives.

Leo: Well, you've got to fight it out with Lisa because I don't - I never had the cojones to stop you, but she does.

Steve: We'll figure out something to do. Oh, yeah, I got it. No question. There was, like, there will not be a podcast. Oh.

Leo: Well, start getting ready. Here we are, we're almost at the end of August. Christmas is just around the corner. That's usually when we try to take a week off. But if you want, we'll record ahead. We'll do something for you. You know what we're going to do...

Steve: We're here for our listeners, Leo. Ultimately, they run - they rule the roost.

Leo: There were here for you, that's right. What we are going to do on, see, this might impact you because your show would be on New Year's Day.

Steve: [Strangled sound]

Leo: And what we are going to do is this thing I've wanted to do for some time, the 24 hours of New Year's because we have listeners all over the world. We're going to start, it'll be 4:00 a.m. our time New Year's Eve, and it's New Year's Eve in a tiny little island in the Pacific. And what we're going to try to do, and I hope everybody listening will participate in this...

Steve: Get people to connect?

Leo: ...is find somebody in every time zone.

Steve: Oh, neat.

Leo: And get them on and say, okay, let's do the countdown.

Steve: Neat.

Leo: And we'll actually have more than 24 countdowns because there are some areas that are on the half-hour and even the quarter-hour time zones.

Steve: There are, really?

Leo: Yeah.

Steve: They're not all even hours?

Leo: No, time zones being what they are, there are some odd ones. So if you're in a time zone - what we're going to - we're putting up a page. We're going to put up a page. It'll be TWiT.tv/nye. And we'll ask people to sign up in every time zone. And I suspect there'll be a few like that very first one where nobody listens to us on this little island. But maybe we can find somebody in a lighthouse or something and talk with them.

Steve: How about you get your rowboat girl to...

Leo: Yeah, Roz can row out there, yeah. Yeah, in fact, that's where she ended up when she did the Pacific was, I think, Tarawa, which is in the second time zone, second - the 5:00 a.m. time zone. And we'll go all the way through from 4:00 a.m. New Year's Eve to 4:00 a.m. New Year's Day, which will be, I think, Hawaii.

Steve: So you're going to sit there on your ball for 24 hours.

Leo: Yes, and we're going to have...

Steve: You're going to put in a full cycle.

Leo: A full cycle. Every hour, sometimes even more, we'll have a countdown and fireworks and confetti. And we're going to have guests; we're going to have music. It'll be a lot of fun. It's our New Year's Eve because we realize the people who listen to these shows really don't have a social life. So we're going to give - myself included. We're going to give you a little party here at the TWiT Brick House for New Year's Eve. I think it'll be fun. But...

Steve: Given some of what we hear from our listeners, Leo, we are providing a social life.

Leo: Oh, yeah.

Steve: For some of our listeners.

Leo: For me. If it weren't for this, I'd be living in my - I'd be in my underwear at home watching TV. So but...

Steve: Glad you're not.

Leo: I know, there's an image, huh? But you, my friend, would be six hours later, seven hours later on New Year's Day doing the show, if we do it live. And I don't know if I'll be in any condition to do a show.

Steve: Oh, no, no. I wasn't suggesting live. I assumed that TWiT Land would do a hiatus, but I'd come up with something for us to fill...

Leo: Christmas week is our Best Of week. And so that Wednesday, which is Christmas Day...

Steve: Oh, I see. We do have a problem, Leo.

Leo: Yeah, you see, we have a little problem here.

BOTH: But we'll figure it out.

Leo: Yeah, we'll figure it out. So, yeah, this is my social - I've created this entire network for my social life, so I'd have some friends. I'm so lonely.

Steve: Well, and I remember, too, that when you and I first discussed this, it was in the studios of Rogers Cable...

Leo: That's right, that's right.

Steve: ...up in Toronto. And the problem was that the way they recorded was you would do four shows Monday, Tuesday, Wednesday, and was it Thursday? And then when we...

Leo: Yeah, it was the other way. I would fly up - I would fly from San Francisco to Toronto on Monday, arrive in the evening on Monday. We'd do 15 shows Tuesday, Wednesday, Thursday, Friday, and the 15th show I would collapse into a puddle, and the car would pick me up and take me to the airport, and I'd be home that night.

Steve: Well, and the key was...

Leo: It was crazy.

Steve: ...you then had three weeks with nothing to do.

Leo: With nothing to do.

Steve: Essentially you crammed a month's worth of programming material into one week. And so you were kind of sitting around thinking, huh, you know?

Leo: Anybody sensible would have just said, gosh, this is great. I get three weeks off a month. Work really hard for five days, and then take it easy. But no. No. I said, oh, I think I'll start a whole 'nother business.

Steve: And Leo, we're...

Leo: I'm glad I did.

Steve: Hundreds of thousands of people.

Leo: And now nine years later, eight years later, beginning our ninth - I can't - that's so great, Steve. That is amazing in any business. But broadcasting especially. But when a show is in its ninth year, that's a long time.

Steve: Yeah.

Leo: That's a success. So, and this show, I have to tell you, there's been zero attrition, and it's only grown over those nine years.

Steve: That's neat.

Leo: It is larger now than it was when we started. So, and I think that says something to, obviously, you and the content, but the people's need to know about security, as well. In fact, that's what we're going to do today. We're going to tell you how to secure your email.

Steve: Well, yeah. What I want to do, I'm - as promised, we're going to talk about PGP. And I thought long and hard about the title. And I decided I would - we would title this podcast "Considering PGP" because I definitely want to talk about what it is and how it works and the protocols and all of that. But I still think it's fighting an uphill battle. I still come away thinking, eh, you know, the Internet is full of protocols that clever people put together, that have niches, but just kind of never got off the ground. I mean, they never got traction. They never got critical mass.

And I'm afraid that I have to put PGP there, that it's, I mean, I want to say it absolutely does what it promises. And it passes every test of serious security. So, I mean, and Phil, right out of the gate, designed it beautifully. He made one little mistake which is a typical mistake that's hard to avoid. And that is, he did design his own cipher, which ended up

not to be a good idea.

Leo: Everybody does that. I wish they would just use the stuff that...

Steve: Yeah. And you could - back then you could argue that, okay, you weren't just like wading around in really good professionally designed ciphers. And I have in my notes what he called it, and I can't - I'm blanking on it right now.

Leo: I thought he was using Blowfish and 3DES. But maybe I'm wrong.

Steve: Oh, no, no, those are all available. I mean, this thing is...

Leo: Well, now, yeah, now you can use RSA and everything.

Steve: Absolutely state of the art. And there were problems with - oh, he called it BassOmatic.

Leo: [Laughing] You know, I don't think that survived too long because I started using PGP in 1997 and I don't - and I've interviewed Phil many times. And I don't remember BassOmatic. So that quickly...

Steve: It was from Dan Aykroyd's "Saturday Night Live" skit.

Leo: Yeah. He was putting a bass in the blender.

Steve: In a blender.

Leo: Yeah.

Steve: And he said that's basically what this does to your data is what the blender does to the bass.

Leo: See, it's a good name. It's a descriptive name.

Steve: So he called it BassOmatic. Anyway, we're going to talk all about PGP. But as is still happening, there's a bunch of news relative to the continuing blowback and consequences of the Snowden leaks. And several things happened this week that were interesting and help to - this is a little bit of a thinking piece at the top of the show because there's this whole question of, if you don't have anything to hide, why do you need privacy? There have been a couple events which have induced some smart people to make some comments that I want to share. So I want to share some writing of a

couple people.

And also, of course, we have the sad news that it has turned out for Ladar Levison - whom we discussed last week, who decided to close down Lavabit - it turns out that, shortly after his announcement, but enough afterwards that we didn't pick up on it last week, has come the news that he received essentially a threatening letter from the powers that be in the federal government for shutting down his service. And this was reported by a very good reporter with NBC News, an investigative reporter whom I'm sure you know, Mike Isikoff.

Leo: Yeah, who's very good. Used to write at Newsweek. Smart guy.

Steve: Yeah, yeah, yeah, I mean, this guy is top of his game. So he wrote, and then Techdirt reported on it, saying: "The saga of Lavabit founder Ladar Levison is getting even more ridiculous, as he explains that the government has threatened him with criminal charges for his decision to shut down the business..."

Leo: But he can't have been surprised because the reason he shut it down, he wanted to erase the database, and that's what the government wanted. So it's not that he shut down, it's that he erased the database, of course.

Steve: Well, apparently not, because he says: "...the decision to shut down the business, rather than agree to some mysterious court order." So what Isikoff has concluded is that they wanted continuing surveillance in the future. And so if you read this this way, they're upset that they lost him as a resource.

Leo: Right. We're really excited about being able to tap into your ability. But, you see, this is what you speculated is that they wanted ongoing keys. You said this.

Steve: Oh, yeah.

Leo: From Lavabit. And so I think you're probably right, yeah.

Steve: Yeah. So they said: "The feds are apparently arguing that the act of shutting down the business itself was a violation of the order." And then Isikoff says: "A source familiar with the matter told NBC News that James Trump, a senior litigation counsel in the U.S. attorney's office in Alexandria, Virginia, sent email to Levison's lawyer last Thursday, the day Lavabit was shuttered" - so that's Thursday before last in our timeframe - "stating that Levison may have 'violated the court order,' a statement that was interpreted as a possible threat to charge Levison with contempt of court. That same article suggests that the decision to shut down Lavabit was over something much bigger than just looking at one individual's information, since it appears that Lavabit has cooperated in the past on such cases," as we said last week.

"Instead, the suggestion now is that the government was seeking a tap on all accounts. Levison stressed that he has complied with 'upwards of two dozen court orders' for information in the past that were targeted at 'specific users' and that," quoting him, "'I

never had a problem with that.' But without disclosing details, he suggested that the order he received more recently was markedly different, requiring him to cooperate in broadly based surveillance that would scoop up information about all the users of his service. He likened the demands to a requirement to install a tap on his telephone."

And so - and we know what the architecture is because he was public with the architecture. And the fact is he didn't have keys to his database. He only acquired them as people connected in order to download the contents of their inbox. And so that's what we - from a technology, purely technology standpoint last week, it was clear to me that they couldn't capture his database. It wouldn't do them any good. That part he got right. That was useful, that he didn't have the keys to the data. But the problem was he would always receive them at his end in order for the user to then decrypt the data on the server and download it. So it must have been that, if he was upset with something, it was that he was going to be asked to provide this on an ongoing basis. And now they're saying we're not happy with you for doing that, for, like, deciding not to be in that business.

Leo: It's really getting bad.

Steve: It is. And you know, Leo, there are - I've seen people say that, like, why are people getting upset? We've all known this was going on. And first of all, I think it's very clear we didn't all know this was going on, and also that...

Leo: Only cynics knew it was going on.

Steve: Correct, correct.

Leo: In some ways, this is what really pains me the most, is that the most cynical, conspiracy-minded people in this country have been proven right. And that bothers me because I wanted to believe in the government. I wanted to believe.

Steve: Yes, I did, too. I mean, I've, you know, yes. I was literally a Boy Scout, and we pledged to the flag.

Leo: Yeah. And we really need to get back to that, a government we can be proud of, that upholds the Constitution in this.

Steve: Yes. And that's the other thing, too. There is this sense now of our own government being adversarial.

Leo: Yeah.

Steve: And that's really uncomfortable.

Leo: And I'm sure you're going to talk about what happened to the Guardian and Glenn Greenwald's spouse. And that is, now, that was the British government, but this is what we fear.

Steve: Yes.

Leo: And it's coming true, I'm sorry to say.

Steve: That is what I have up next. That is what I have up next because the second part of this is the government's response. That is, it's one thing for them to be doing this, but they're really being very graceless in...

Leo: Oh, they're insisting on their prerogative to break the law, essentially.

Steve: Yeah. So the editor of the Guardian wrote a good piece. I also - he also put together about a - it's six minutes and something, I think it's 45 seconds, so a little bit less than seven-minute video which I just tweeted the link to before the podcast. So if anyone wants to see Alan Rusbridger in front of a camera, speaking and explaining himself, there's that, too [bit.ly/13RuIet]. But I want to share two pieces from a larger posting of his that he put up yesterday, discussing exactly what you were saying, Leo.

So jumping into the middle of what he wrote, he says: "On Sunday morning David Miranda, the partner of Guardian columnist Glenn Greenwald, was detained as he was passing through Heathrow Airport on his way back to Rio de Janeiro, where the couple live. Greenwald," of course, "is the reporter who has broken most of the stories about state surveillance based on the leaks from the former NSA contractor Edward Snowden."

Leo: That word "reporter" is extremely important.

Steve: Yes, yes, because his partner David Miranda is not a journalist. "Greenwald's work has undoubtedly been troublesome and embarrassing for western governments. But, as the debate in America and Europe has shown, there is considerable public interest in what his stories have revealed about the right balance between security, civil liberties, freedom of speech, and privacy. He has raised acutely disturbing questions about the oversight of intelligence; about the use of closed courts; about the cozy and secret relationship between government and vast corporations" - and of course just this morning The Wall Street Journal, Leo, disclosed, gave some numbers, put some numbers to the relationship the NSA has with major top-level telco providers. And continuing, "...and about the extent to which millions of citizens now routinely have their communications intercepted, collected, analyzed and stored.

"In this work he is regularly helped by David Miranda. Miranda is not a journalist, but he still plays a valuable role in helping his partner do his journalistic work. Greenwald has his plate full reading and analyzing the Snowden material, writing, and handling media and social media requests from around the world. He can certainly use this back-up. That work is immensely complicated" - and this is really interesting, Leo, that this guy's writing this - "That work is immensely complicated by the certainty that it would be

highly unadvisable for Greenwald (or any other journalist) to regard any electronic means of communication as safe. The Guardian's work on the Snowden story has involved many individuals taking a huge number of flights in order to have face-to-face meetings. Not good for the environment, but increasingly the only way to operate. Soon we will be back to pen and paper.

"Miranda was held for nine hours under Schedule 7 of the U.K.'s terror laws, which give enormous discretion to stop, search and question people who have no connection with 'terror' as ordinarily understood. Suspects have no right to legal representation and may have their property confiscated for up to seven days. Under this measure - uniquely crafted for ports and airport transit areas - there are none of the checks and balances that apply once someone is in Britain proper. There is no need to arrest or charge anyone, and there is no protection for journalists or their materials. A transit lounge in Heathrow is a dangerous place to be."

Leo: Unbelievable.

Steve: So, but I thought it was really interesting that he talks about the, as a consequence of what journalism now understands to be the case - and we'll talk about Groklaw here in a second, Leo.

Leo: It's a huge chilling effect on what is a very important function of journalism, which is to keep an eye on government.

Steve: And to be able to guarantee your sources their own privacy and anonymity. And how...

Leo: Or we'll have no sources. Which is what, frankly, the Obama administration wants. It's why they're so aggressively pursuing whistleblowers.

Steve: I know. Well, anyway, we have - there's a fabulous blog posting that I'm going to share in a second here, an open letter to Obama from an IT security expert in Silicon Valley who presents one of the most interesting analogies of pervasive surveillance that I've seen, that's also thought-provoking. But I want to finish with this. In the second part of what I wanted to excerpt from what Alan wrote, he says: "A little over two months ago I was contacted by a very senior government official claiming to represent the views of the prime minister. There followed two meetings in which he demanded the return or destruction of all the material we were working on. The tone was steely, if cordial, but there was an implicit threat that others within government and Whitehall favored a far more draconian approach.

"The mood toughened just over a month ago, when I received a phone call from the center of government telling me: 'You've had your fun. Now we want the stuff back.'"

Leo: Ugh.

Steve: Oh, I know, it is just so bad. "You've had your fun." That's the way they're

characterizing...

Leo: It ain't fun.

Steve: ...what the Guardian is doing.

Leo: It ain't fun.

Steve: "There followed further meetings with shadowy Whitehall figures. The demand was the same: Hand the Snowden material back or destroy it. I explained that we could not research and report on this subject if we complied with this request. The man from Whitehall looked mystified. 'You've had your debate. There's no need to write any more.'"

Leo: No, no, no.

Steve: Period.

Leo: No, it's just beginning. Got bad news for you, Whitehall.

Steve: Thank god. "During one of these meetings I asked directly whether the government would move to close down the Guardian's reporting through a legal route - by going to court to force the surrender of the material on which we were working. The official confirmed that, in the absence of handover or destruction, this was indeed the government's intention. Prior restraint, near impossible in the U.S., was now explicitly and imminently on the table in the U.K.

But my experience over WikiLeaks - the thumb drive and the First Amendment - had already prepared me for this moment. I explained to the man from Whitehall about the nature of international collaborations and the way in which, these days, media organizations could take advantage of the most permissive legal environments. Bluntly, we did not have to do our reporting from London. Already most of the NSA stories were being reported and edited out of New York. And had it occurred to him that Greenwald lived in Brazil? The man was unmoved."

Leo: Which is, by the way, where his partner was headed.

Steve: Yes.

Leo: He was transiting England. He wasn't even in England.

Steve: Yup. "The man was unmoved. And so one of the more bizarre moments in the Guardian's long history occurred, with two GCHQ security experts overseeing the destruction of hard drives in the Guardian's basement..."

Leo: Morons. Morons. That's who's running this.

Steve: I know, "...just to make sure there was nothing in the mangled bits of metal which could possibly be of any interest to passing Chinese agents." Then one of the guys jokes, "'We can call off the black helicopters,' joked one as we swept up the remains of a MacBook Pro." Ha ha ha, yeah.

Leo: They're just making it real. Quite the contrary...

Steve: I know. Leo, mark my words, there will be technological consequences that will take on the...

Leo: Oh, absolutely.

Steve: There will be. You heard it here. I mean, we technologists, the people who get technology and the Internet, are not without recourse. There will be - it's going to take months because these things take months to happen. There will be a technological response that none of these agencies will view positively as a consequence, more than anything, of the fact of this kind of action and that they lie. We cannot have, in a democracy, we cannot have our government lying to us.

Leo: The response I was thinking of was the chilling effect it has, which your next story will talk about, on technology. Already Germany's saying, well, you can't use Windows 8 because the TPM module gives a backdoor to the United States government. So there's that chilling - that's the effect I was thinking of. You're thinking of consequences, and I certainly don't want to be in a position where we're threatening consequences. We have no control over that. But I think...

Steve: No, no, no, all I mean is empowerment.

Leo: Yeah.

Steve: There have been, and we've reported here, and I keep reading it, there has been a tremendous upsurge of interest in secure solutions. And my point has always been, they exist. You can do pre-Internet encryption, and you can do TNO. I mean, we'll be talking about it later.

Leo: Right.

Steve: PGP is absolutely bulletproof.

Leo: Right.

Steve: I mean, but you have to use it in order to be protected. But I predict that this puts pressure that we have never had before on the need for privacy, and all of the technology is there. It just needs to get mobilized.

Leo: Yeah, we've been talking about, I've been talking about PGP and putting my key on the front page of my website since literally 1997. No uptake, never, nobody was ever interested in it.

Steve: No.

Leo: All of a sudden there's a lot of interest.

Steve: Yeah.

Leo: Which is good.

Steve: So in another piece of news earlier this week...

Leo: This is depressing as hell.

Steve: It is, Leo. I was so shocked.

Leo: I think Pamela's overreacting, but I understand her - anyway, go ahead.

Steve: Yeah. So anyway, this is about Groklaw, which we've touched on for years.

Leo: Fabulous website. Really good.

Steve: Yup. And she's - Pamela Jones, P.J. as she goes, got very upset by this. And from her...

Leo: Groklaw, we should mention, is a site that discusses the law as it applies to technology, and it's hideously useful. It's one of the resources I use all the time to understand lawsuits, patent issues. She's really good. DRM...

Steve: Really informed legal discussion.

Leo: Yeah.

Steve: Yes. So I'm not going to read her whole posting. It's at Groklaw.net, G-r-o-k-l-a-w dotnet, for anyone who wants more. But I excerpted a couple things because she, while I agree that she overreacted, Leo, she said a couple things and also quoted an author that I thought had some very interesting things to say. So summarizing what came before, I put in brackets here, "[I feel betrayed]," so I could walk into the sentence I wanted to start at, saying "knowing that persons I don't know can paw through all my thoughts and hopes and plans in my emails with you."

So she's really disturbed, she writes, by the certainty now that - she maintains email with an international community. And by definition international correspondence, email, is being captured. We now know that. So she says: "They tell us that, if you send or receive an email from outside the U.S., it will be read. If it's encrypted, they keep it for five years, presumably in the hopes of tech advancing to be able to decrypt it against your will and without your knowledge." And of course we know, Leo, that since security certificates expire at most every three years, keeping encrypted content for five, if you get the expired keys, guarantees your ability to ultimately decrypt everything.

Leo: Does perfect forward security prevent that?

Steve: Yes.

Leo: Okay.

Steve: Yes. So she says: "Groklaw has readers all over the world." She says: "I'm not a political person, by choice, and I must say, researching the latest developments convinced me of one thing - I am right to avoid it." And then she talks about her feelings after 9/11 and how hugely upset she was by the events of 9/11, the 9/11 attacks. And so she says: "Part of my anguish was that there were people in the world willing to do that to other people, fellow human beings, people they didn't even know, civilians uninvolved in any war. I sound quaint, I suppose. But I always tell you the truth, and that is what I was feeling. So imagine how I feel now, imagining as I must, what kind of world we are living in if the governments of the world think total surveillance is an appropriate thing?" And this was one of the sentences that really got me. She said: "What I do know is it's not possible to be fully human if you are being surveilled 24/7."

And then she quotes Janna Malamud Smith, the author of a book, "Privacy Matters." And I guess Janna quotes Alan Westin in his book, "Privacy and Freedom," saying: "In his landmark book, 'Privacy and Freedom,' Alan Westin names four states of privacy: solitude, anonymity, reserve, and intimacy. The reasons for valuing privacy become more apparent as we explore these states," reading from the book. "The essence of solitude, and all privacy, is a sense of choice and control. You control who watches or learns about you. You choose to leave and return. Intimacy is a private state because in it people relax their public front either physically or emotionally or, occasionally, both. They tell personal stories, exchange looks, or touch.... They may ignore each other without offending.... They may speak frankly using words they do not use in front of others, expressing ideas and feelings, positive or negative, that are unacceptable in public. When shielded from forced exposure, a person often feels more able to expose himself."

And anyway, so I really liked that. I thought that helps to understand sort of the creepy feeling of wanting to send an email to someone with content that is really private, I mean, that you intend only to share with the other person, and the sort of sense of self-censorship which is now sort of pervading, or the idea of maybe needing to self-censor whenever you use the Internet because this - maybe, I mean, maybe we were wrong not to be cynical enough. But now we know exactly what's going on, and I'm self-conscious about doing searches for things that interest me just intellectually because of the problem of false positives.

Leo: Well, so there's a consequence. We're losing one of the best law blogs out there, Groklaw, because she doesn't want to be exposed this way. She's actually, it sounds like, trying to get off the Internet entirely.

Steve: Yes. And unfortunately she did recommend a, quote, "secure email service." For what it's worth, it's absolutely not. So she mentions Kolab as, like, being the best secure email solution available. Well, secure email is close to being an oxymoron.

Leo: Yeah. We're going to show you the most secure way to do it in this show.

Steve: Yes. That is the content of the...

Leo: There's no way to hide metadata. And as we know now, metadata can be very, very revealing.

Steve: Well, but Kolab does nothing. I mean, it's...

Leo: She likes it because it's in Switzerland, so somehow that's magical, yeah.

Steve: Yes. That's exactly why. She said that she believes that they're in Switzerland, and doesn't understand that there's no encryption as it heads out to Switzerland, which is where the NSA has stationed their listening posts. So, and Kolab's onsite. I really got myself worked up when I looked at this. I was like, oh, my god. I mean, they say: "We offer secure email accounts including calendars and address books that synchronize to all your devices. The data is stored in our very own data center in Switzerland."

Leo: Ooh. Wow.

Steve: This is like...

Leo: So is Google's.

Steve: ...Silent Circle has Navy SEALs. It's like, oh, and we have our own datacenter in

Switzerland. BF - oh, excuse me.

Leo: But, no, and so I feel like Pamela's overreacted, P.J.'s overreacted a little bit. I understand her concern, and I don't know what it is that she's worried about people finding out. I wish that Groklaw could continue because it's very useful. But...

Steve: She did try to shut it down a few years ago and brought somebody in to help her out.

Leo: Yeah. There may be - there are other reasons in addition. Might just be a good opportunity. But it's a good protest. It's sad.

Steve: Yeah. Now, I want to share this open letter to the President. And I don't know how to excerpt from it. It's not very long, and I think it's worthwhile. And this is where there's an analogy that I think is really interesting. So this was posted day before yesterday, addressed to Dear President Obama: "My name is Ben Adida (A-d-i-d-a). I am 36, married, two kids, working in Silicon Valley as a software engineer with a strong background in security. I've worked on the security of voting systems and health systems, on web browsers and payment systems. I enthusiastically voted for you three times: in the 2008 primary and in both presidential elections.

"When I wrote about my support for your campaign five years ago, I said: 'In his campaign, Obama has proposed opening up to the public all bill debates and negotiations with lobbyists, via TV and the Internet. Why? Because he trusts that Americans, when given the tools to see and understand what their legislators are doing, will apply pressure to keep their government honest.' I gushed about how you supported transparency as broadly as possible" - actually there was a funny tweet that I saw. Someone said Obama's presidency is so transparent, now we can't see anything.

Leo: Yeah.

Steve: And so anyway, it says: "...transparency as broadly as possible to enable better decision-making, to empower individuals, and to build a better nation. Now, I'm no stubborn idealist. I know that change is hard and slow. I know you cannot steer a ship as big as the United States as quickly as some would like. I know tough compromises are the inevitable path to progress. I also imagine that, once you're President, the enormity of the threat from those who would attack Americans must be overwhelming. The responsibility you feel, the level of detail you now understand, must make prior principles sometimes feel quaint. I cannot imagine what it's like to be in your shoes.

"I also remember that you called on us, your supporters, to stay active, to call you and Congress to task. I want to believe that you asked for this because you knew that your perspective as Commander in Chief would inevitably become skewed. So this is what I'm doing here: I'm calling you to task. You are failing hard on transparency and oversight when it comes to NSA surveillance. This failure is not the pragmatic compromise of ObamaCare, which I strongly support. It is not the sheer difficulty of closing Guantanamo, which I understand. This failure is deep. If you fail to fix it, you will be the President principally responsible for the effective death of the Fourth Amendment and worse."

He says, with his topic Mass Surveillance: "The specific topic of concern, to be clear, is mass surveillance. I am not concerned with targeted data requests, based on probable cause and reviewed individually by publicly accountable judges. I can even live with secret data requests, provided they're very limited, finely targeted, and protect the free speech rights of service providers like Google and Facebook to release appropriately sanitized data about these requests as often as they would like. What I'm concerned about is the broad, dragnet NSA signals intelligence recently revealed by Edward Snowden. This kind of surveillance is a different beast, comparable to routine frisking of every individual simply for walking down the street. It is repulsive to me. It should be repulsive to you, too.

"If you're a hypochondriac, you might be tempted to ask your doctor for a full-body MRI or CT scan to catch health issues before detectable symptoms. Unfortunately, because of two simple probabilistic principles, you're much worse off if you get the test. First, it is relatively unlikely that a random person with no symptoms has a serious medical problem, i.e., the prior probability is low. Second, it is quite possible not likely, but possible that a completely benign thing appears potentially dangerous on imaging, i.e., there is a noticeable chance of false positive. Put those two things together, and you get this mind-bending outcome: If the full-body MRI says you have something to worry about, you actually don't have anything to worry about. But try convincing yourself of that if you get a scary MRI result.

"Mass surveillance to seek out terrorism is basically the same thing: very low prior probability that any given person is a terrorist, quite possible that normal behavior appears suspicious. Mass surveillance means wasting tremendous resources on dead ends. And because we're human and we make mistakes when given bad data, mass surveillance sometimes means badly hurting innocent people." And then he quotes the case of Jean-Charles de Menezes, who was shot seven times in the head in the U.K. after the bombings, just because of false identification.

"So what happens when a massively funded effort" - oh, and then, and this is another great point, he says: "So what happens when a massively funded effort has frustratingly poor outcomes? You get scope creep. The surveillance apparatus gets redirected to other purposes. The TSA starts overseeing sporting events. The DEA and IRS dip into the NSA dataset. Anti-terrorism laws with far-reaching powers are used to intimidate journalists and their loved ones." And he was talking about what happened over the weekend. "Where does it stop? If we forgo due process for a certain category of investigation which, by design, will see its scope broaden to just about any type of investigation, is there any due process left?"

And then he adds something else that I thought was interesting. Under Wrong on Principle, he says: "I can imagine some people, maybe some of your trusted advisors, will say that what I've just described is simply a 'poor implementation' of surveillance, and that the NSA does a much better job. So it's worth asking: Assuming we can perfect a surveillance system with zero false positives, is it then okay to live in a society that implements such surveillance and detects any illegal act? This has always felt wrong to me, but I couldn't express a simple, principled, ethical reason for this feeling until I spoke with a colleague recently who said it better than I ever could:

"'For society to progress, individuals must be able to experiment very close to the limit of the law and sometimes cross into illegality. A society which perfectly enforces its laws is one that cannot make progress.' What would have become of the civil rights movement if all of its initial transgressions had been perfectly detected and punished? What about gay rights, or women's rights? Is there even room for civil disobedience? Though we want our laws to reflect morality, they are, at best, a very rough and sometimes completely

broken approximation of morality. Our ability as citizens to occasionally transgress the law is the force that brings our society's laws closer to our moral ideals. We should reject mass surveillance, even the theoretically perfect kind, with all the strength and fury of a people striving to form a more perfect union." So anyway, I thought there was some really...

Leo: It's good. It's really good, yeah. I like the MRI analogy because I think that's exactly what's happened, and I think...

Steve: Yes.

Leo: That's Ben Adida writing, and his blog is Benlog, B-e-n-l-o-g, dotcom. Yeah. I think - I don't know where you found that, but I think that that's kind of - those are words that I would have said, as well.

Steve: Yeah. And it was that - that was what I meant when I talked about the analogy, the analogy to a scan.

Leo: It's an excellent analogy, yeah.

Steve: It really is. Because it is the probability, this low probability that has a high tendency for false positives. I know from just my own eight years of doing a lot of medical research that scans are really frowned on for that reason.

Leo: Right.

Steve: First of all, not the MRI...

Leo: It's counterintuitive. But these full-body scans which are - they're selling now, you know, there's these - this is a business. And most doctors say don't do it. It's a bad - it's a bad idea. And it's not intuitive why it's a bad idea. I think he described it quite well. And it's precisely what's wrong with mass surveillance. And we see it all the time. I really...

Steve: Well, and Leo, yeah, and the fact that the Patriot Act has now allowed us to suspend habeas corpus, I mean, the idea that you can be, I mean, people make mistakes. Government makes mistakes. The idea that goons can show up at your door and take you away without recourse, without needing to explain themselves, simply saying "terrorism," just under the Patriot Act, essentially, we have unleashed and unbound agents of the government in a way that has never happened before. I mean, and it's a fundamental principle of the country.

Leo: Fortunately, we still have the right to debate this in public without fear of

knocks coming on the door. But I don't know how much longer that's going to go on. When I see the kind of harassment that Glenn Greenwald is receiving...

Steve: Well, yes.

Leo: ...I start to worry that in fact just speaking out will in fact make you a target.

Steve: And doesn't this feel like harassment?

Leo: It is.

Steve: For his partner to go through nine hours of detainment?

Leo: No, it's pure harassment.

Steve: Yes.

Leo: And it's just the beginning, I think. Now, it's always been a little worse in Britain. I hope that, you know, we have, I think, a Constitution that is more protective of our individual rights. I hope that that wins in the end.

Steve: Well, only if it's followed. And when...

Leo: I thought what he said is, that you don't want to be the President who goes down in history as the guy who overturned the Fourth Amendment, is right on. And I hope that somebody's paying attention to this.

Steve: And I forgot. I didn't want to keep reading because I know this was getting long. But later on he comes back and makes it personal. He says, Obama, Barack, if you were still a professor teaching constitutional law in Chicago, what would you be saying? I mean...

Leo: Yeah, well, as a senator he was very critical of this.

Steve: Yes.

Leo: He was extremely critical as a senator. I don't understand what happened. I mean, I think that this is - the blog post is accurate. And I think it's very generous to the President, frankly. But we've got to do something. This can't go on. It really can't

go on.

Steve: So I did want to mention that I was disappointed in Google. And maybe I was more disappointed in the reporting. I'm not sure. But Google, since we last spoke, made a very big deal about now they are encrypting their drives. And I - it caused me to coin a new acronym. We have TNO. We have PIE. We now have ZVE.

Leo: ZVE.

Steve: Zero-Value Encryption [laughter].

Leo: I like it.

Steve: This is Google's very disappointing ZVE.

Leo: It makes you feel better, though. That's the importance.

Steve: Oh, don't we all need that, Leo. We really - we need to feel better, yeah. Anyway, they did a blogspot posting on the Google Cloud Platform, made a big deal about how they're now encrypting their data on their drives. Now, it is true that it raises the bar for somebody physically stealing the drive. I mean, they rotate keys. I mean, they're doing the key management. Oh, don't worry, we'll handle the keys. You don't have to handle - well, it's like, hello. ZVE. It means nothing. But the way the media covered it, my Twitter feed went crazy with people saying, hey, Google's encrypting their data. It's like, yeah. And decrypting it. So...

Leo: Yeah.

Steve: Big deal. And so the bad news is, remember that about a month ago I picked up a rumor that this was happening, and I got excited, thinking maybe they were going to do some form of TNO encryption.

Leo: They'd have to give us, let us determine the keys and hold them.

Steve: Yeah.

Leo: But you can always do that. You use TrueCrypt on your end and store it on Google Drive. It's TNO.

Steve: Precisely. Or Boxcryptor is another great solution. We've talked about those. Oh, and, yeah.

Leo: But you have to have the key. They can't have the key or it's zero-value encryption. I like it.

Steve: ZVE.

Leo: ZVE, another ZVE.

Steve: Okay. So a consequence of the April 8, 2014 discontinuance of XP's updates didn't really sink in last time I mentioned - I mentioned it last week that now we're at 229 days and counting, so there's time. But remember I mentioned last week that Microsoft actually sent out a note saying, just want to make sure everyone understands that we're not going to be continuing to update XP SP3 after April 8th of next year. Well, what's significant is - oh, and when I talked about it last week it was under the context of the security community beginning to wonder if maybe bad guys are not holding their exploits back, not using them, but waiting.

Leo: Mmm. That's what I'd do.

Steve: Yes, exactly.

Leo: Wait'll after April 8th, and everyone's golden.

Steve: But here's the second part of this problem, and that is, almost all of these bad problems affect all supported versions of Windows. We see that, I mean, not always. Sometimes it'll just be Server 2008 or a Windows 7 thing. But normally it's everything. Because we know this is just one OS, and they keep putting different candy colors on the outside and give it a few more features. But there's a core operating system that hails from NT that has had more crap glued onto it over time, but basically it's the Microsoft OS. And they come up with new versions because they need us all to give them more money for upgrades. The point being that, after April 8th, there will continue to be problems found in the remaining operating systems, Vista and 7 and Windows 8. And those same problems will still be in XP.

So the other thing that we know happens is that bad guys reverse-engineer the patches. Patches will continue coming out for all supported operating systems that should be coming out for XP, but Microsoft won't any longer. So when those are reverse engineered, those newly discovered vulnerabilities, discovered by the act of patching the newer OSes, will give the bad guys vulnerabilities that will never be fixed in Windows XP. So arguably, unfortunately, much as I hate to say this, because they're continuing to have - we're continuing to find fundamental problems with Windows even now, it's going to be important to really be careful about how you use XP after it is no longer the recipient of security patches.

Leo: I'm sure Microsoft will have a page, as they did, remember, with IE6, saying stop using it.

Steve: Yeah.

Leo: Stop using XP.

Steve: Okay. So I just need to talk about this little Facebook bug and...

Leo: Oh, this is a good story.

Steve: So, yes. So a security researcher in Palestine by the name of Khalil Shreateh finds a problem that allows anyone - and he is anyone - to violate the security, I mean, a Facebook bug, to post onto anyone, any other Facebook member's private timeline and wall. And so to verify this he posts something on Sarah Goodin's private wall.

Leo: Does he know her? I mean...

Steve: I don't know how he chose her. The article I read said that she was the first woman ever to sign up for Facebook, so she's certainly an...

Leo: Oh, she must work at Facebook, yeah.

Steve: Probably. And I guess maybe a friend of Mark's. But nothing happened. So he does that. Then he contacts Facebook security to report the problem and to collect his $500 bounty. And he's told, sorry, this is not a bug. And he thinks, what? Well, okay. So he posts to Mark Zuckerberg's timeline.

Leo: It's a bug now, baby [laughter]. He was quite polite.

Steve: Within minutes, within minutes Facebook security engineer Ola Okelola contacts Khalil to request details of the exploit. Khalil's Facebook account is frozen, later unfrozen. Then Khalil is denied his $500 bounty on the grounds that he violated Facebook's terms of service.

Leo: Oh, come on.

Steve: Which disqualifies him for receiving compensation.

Leo: Oh, that's funny.

Steve: Then Facebook acknowledges that they should have asked for additional information initially.

Leo: You think?

Steve: Now, anyway, that's the story.

Leo: That's pretty funny.

Steve: And I can, I mean, probably the person on the frontline who Khalil first contacted, you can imagine how many false positives this poor person has to field. And, I mean, especially when you offer money. If it was free, then, eh, bogus people wouldn't bother. But if it's a way to get a quick 500 bucks, you're just going to be trying to come up with all kinds of nonsense. And so those poor guys on the frontline of Facebook security must just be like, I mean, "This is not a bug" must be something they, like, have nightmares that repeat in their heads at night. So anyway...

Leo: It's a feature.

Steve: Okay. Now, listeners of this podcast...

Leo: Yes.

Steve: You need to go listen to something Leo did last week [bit.ly/19kYAEh].

Leo: Uh-oh. Am I in trouble?

Steve: Triangulation with Esther Dyson.

Leo: Oh, wasn't she great? Yeah.

Steve: Oh, Leo. I knew she was going to be good. It did not disappoint. She is...

Leo: I didn't get a chance to say hi. I'm sorry. You were in the chatroom, and I apologize.

Steve: That's fine. I've known Esther for about three decades. I did a presentation for - there was a weird conference, Roger von Oech, who - the whack on the side of the head guy.

Leo: Oh, yeah.

Steve: Sort of creative thinking and creativity and things. Somehow he invited me to speak at his conference. And at one point I dropped down onto my knees to pray to IBM.

Leo: [Laughing] That I want to see.

Steve: I told the story, this was before the PC Junior was going to come out. We knew that IBM was working on a home computer. There was the IBM PC and XT and so forth, the industrial computers. And IBM, who had launched the computer industry, I mean the PC industry, finally, after the first sort of sputtering prelaunch with the Apple II and the Ataris, now IBM had made it happen. Clones were out, I mean, this was - we were moving forward. So now they were going to do something for the home. And so my point to this conference was that whatever IBM did was really, really important. So I sort of set it all up, and I dropped to my knees, put my hands together and looked up at the sky and prayed to IBM. I said - oh, I guess also beforehand I talked about how - oh, and you may remember the nickname for this thing was the Peanut, for some reason.

Leo: Oh, yeah.

Steve: Remember? It was the Peanut was like their code word. Like Macintosh was supposed to be the code word at Apple, but it became the actual name of the machine. This was the Peanut, the IBM Peanut. That was their - and I guess because it was small and downscale and so forth. And so at one point, as I'm talking behind the podium, I talk about the experience we've all had at the zoo, where we've got - we're feeding the animals. Or I guess maybe we're feeding ourselves with peanuts because you crack open the shell and there's nothing there. And so that ties in later, when I'm on my knees, praying to IBM, beseeching them to please give us - please do not give us a peanut shell with no nuts. And anyway, so it was a bunch of craziness. But Esther liked it a lot and so invited me to speak at her conference in Phoenix.

Anyway, the point is, Triangulation No. 115, listeners, go watch it. Listen to it, watch it, whatever. It's 45 minutes, and it is so full of just - I don't know what Esther has. Esther has a way of distilling stuff. I mean, it's sort of her job. It's what she does. But, and I love - I thought maybe I would go back through and try to find a lot of her little one-liners, but I didn't have time. One thing that I did love was that she's explained that her goal in weightlessness was she decided I want to be weightless long enough to be bored. Of weightlessness. I thought that was perfect.

Leo: She's been weightless seven or eight times. I don't know if she has - I think she still enjoys it. I don't know if she's bored yet.

Steve: But she's an avid swimmer. And wherever she is, she swims. And so I thought, well, I wonder, like, swimming and weightlessness. But I love that concept. Because, I mean, if I were weightless, oh, my god, there's all kinds of things.

Leo: It's exciting, yeah.

Steve: I want to try spinning axially. And I want to spin, like, I want to do all these

different things. But imagine getting to the point where you're bored with it. That's like the perfect, I mean, like...

Leo: Now we're talking.

Steve: Now we're talking, exactly.

Leo: She wants to go to Mars. You saw that.

Steve: She wants to end her life at Mars.

Leo: Yeah, because there's no coming back, yeah.

Steve: Yeah.

Leo: I would go. I'll go. Yeah. I'm available.

Steve: Okay. I did want to wrap up, because I had not caught up, with "Breaking Bad." I saw a couple of tweets from people who said, Steve, you're a little slow on the uptake here. To which I say yes. Leo, it's the best thing I've ever seen [indiscernible].

Leo: Aw. It's really - it's a great show. And the last season is fabulous, yeah.

Steve: Oh, my god. It is, I mean, I'm not kidding, this is one, I was trying to think of this is something I will repurchase the box set. We have six episodes left, and they're shutting it down. I will purchase the box set and probably watch the whole thing through a few more times, in the same way that I can read Peter Hamilton novels after - with a spacing of a few years. It is fabulously written and acted and assembled. I'm just stunned. It's up for 13 Emmys this time. Bryan, the lead, Cranston, has won three times for Best Actor in a Dramatic Series.

And what's really interesting is how they evolve his character over six seasons from sort of basically a good guy who's in a bad situation, to somebody who can pretty much justify anything he does. And I also love it that it's also got that whole - the whole Mafia don-esque thing happening because it's like an overriding theme with the Mafia types that their families come first. Family is so important. And that is exactly where Bryan always goes, or the character, Walt, always - Walter White - goes for his justification for things.

Anyway, for what it's worth, for those who didn't see the "Talking Bad" segment - it's an hour after the show airs on Sundays. I watched them both because now I'm a serious fanboy. And the creator is very happy with what they did. I mean, everyone, huge tension now exists among the community of us, of which I now proudly count myself a member, of people watching "Breaking Bad," what is going to happen? How are they going to wrap this up? And the writers are tickled to death. They are extremely happy

with how this wraps up. Sort of like every aspect of this apparently gets tied up. So, and we don't know any more than that.

But anyway, it's just, wow. I will say again, I tried to watch it once, and the first couple episodes just didn't get me. I just thought, eh, I don't think this is for me. If you've had that experience, push on. Give it - the first season I think was only seven episodes. Yes, the first season was seven because they probably weren't too sure. AMC was like, eh, well, we'll give you a commitment of seven. Then they had three seasons of full-length, full-season seasons. So, wow. Just wanted to say it rocks.

Speaking of that, I did make a faux pas, a minor one, last week where I mentioned Bitmessage and blockchain in the same sentence. I only - I know that Bitmessage does not use the blockchain technology. Someone said, "Steve, not the blockchain," because Bitmessage does not keep everything forever, whereas the blockchain is everything forever. Bitmessage uses a variation where things expire after a couple weeks. I did mention that last week, but I shouldn't have used the term "blockchain." So for people who are watching that closely, I apologize for that and wanted to correct that.

SpinRite continues to run fabulously forward. We are now beginning - yesterday I posted a test release that is beginning to transfer data. We have found and killed the weirdest anomalies that people have found. People have 133 MHz Pentiums, Leo, that we're testing this on because of course SpinRite needs to go all the way back to the dawn of time.

Leo: Where did you find that?

Steve: Oh, I mean, they're there.

Leo: That's fun.

Steve: And there was a subtle problem I had on a machine that had less than 16MB of RAM because it went looking down in conventional memory for an additional allocation, and I had forgotten to remove that from the allocation bitmap. So we're finding all kinds of things. It is looking like, with the first release of SpinRite, I'm going to at least look into incorporating the AHCI controller support, the advanced host controller interface, which I was thinking I was going to put off to 6.2, because I look at everything I've done so far, and it's all the perfect foundation for supporting that next-generation controller also. And I would love to just have both of those bases covered. So anyway, we're moving forward really well, doing lots of testing. And now people - we're beginning to transfer data from drives.

Leo: Very exciting. All right. We're going to learn about PGP, and I'm looking forward to this. We should say, by the way, PGP is a commercial product created by Phil Zimmermann and sold by, now, by Symantec. I presume you're going to talk, not about the commercial project, but the PGP protocol and its various implementations, including...

Steve: Right, and its history and so forth.

Leo: History, yeah. Because I use the open source GNU Privacy Guard and find that to be an excellent choice, a non-commercial choice. So let's talk about PGP.

Steve: Okay. I always wondered where the name came from because it sounded like modesty, you know, Pretty Good Privacy.

Leo: Eh, it's okay.

Steve: And I thought, well, can I have better than that?

Leo: I'd like Really Good Privacy, RGP.

Steve: I'd like RGP.

Leo: Yeah.

Steve: Yeah. It turns out that the wonderful fictional community of Garrison Keillor's Lake Wobegon sported, among many other memorable locations, a grocery store named Ralph's Pretty Good Grocery. And apparently Phil Zimmermann was a fan of Lake Wobegon, and he drew his inspiration from Garrison's whimsy, calling his effort Pretty Good Privacy.

Leo: You also know Phil was not the best namer of things. But that's a - he was a good coder, though.

Steve: Yes.

Leo: That's what really counts.

Steve: So the good news is the privacy is actually quite a bit better than just pretty good. In fact, it's truly state of the art. And we'll talk about some of those details here in a second. There was one little mistake which hurt the privacy in the early days, before this really happened. Actually this was at v1.0 that really didn't see much attention. It wasn't until PGP 2.0 that it really took off. But in v1.0, Phil made the mistake, which is always tempting for someone who's interested in cryptology, of doing his own cipher. How many times on this podcast have we warned people.

Leo: Yeah, please.

Steve: Do not write your own bit-mixing technique that you're sure is the best thing anyone has ever come up with, and your mother can't figure it out. That's not the bar

you will need to get past.

Leo: No, no.

Steve: Phil did, unfortunately, invent his own symmetric cipher named BassOmatic in PGP 1.0, which was rather quickly and embarrassingly found to be insecure. Over a discussion at the Crypto Conference in 1991, someone said, uh, you know, Phil, I was looking at BassOmatic. Uh, maybe that's not such a good idea. And in the source code Phil explains that BassOmatic got its name from an old Dan Aykroyd SNL ("Saturday Night Live") skit involving a blender and a whole fish. Apparently the BassOmatic algorithm does to data what the original BassOmatic blender did to the fish. Thus the name.

The good news is BassOmatic is no more the cipher. And as is the case for all good state-of-the-art crypto systems, it is multi-algorithm completely. What happened was initially it went with RSA and IDEA, which is - the IDEA is a very good symmetric cipher. It was unfortunately intellectually encumbered, intellectual property encumbered, as was RSA, as we know. Of course RSA had patents on it. But patents have all finally expired. There were non-encumbered alternatives that were available. And so PGP was able to fall back and use those.

So the way to think of PGP, and thus really the reason for its success, is it isn't just by any means about email encryption. That may be sort of like the plane on which most of us have some intersection with PGP. But it is truly a generic, nicely designed, complete crypto system. I spent some time, read the RFCs, dug into the format and semantics. And I came away feeling very impressed. Anybody could confidently use PGP for any application that it is intended for. It's had, because it began back in '91, it's had a long history. And we're now at PGP 5.0, sort of like in the formal versioning. Leo, you mentioned GnuPG, which of course is GPG, which is that version. There's also OpenPGP. OpenPGP is sort of the standards body of which the other PGPs are then implementations.

Leo: It is a standard. It's RFC 4880. So, yeah.

Steve: Right, right, and is embodied in a library of code so you can put command line frontends; you can put GUI frontends; you can use this block of code as your reference code for PGP. So it supports multiple algorithms for signing, for authentication, for encryption. It originally had a non-hierarchical flat keying system. And I didn't realize until I read the spec, you can use a shared secret key...

Leo: Hmm, I didn't know that.

Steve: ...or an asymmetric key, either way.

Leo: Right, which is how most people do it.

Steve: Exactly. And so here's, I mean, and what I like about this is the protocol is the

kind of thing we've talked about often. I will describe it to you, and I have described exactly the same sort of thing in, like, 10s, 20s, 30s, maybe not hundreds, but tons of different contexts.

So you have text. Now, because textual content is normally highly compressible, doing something like a deflate or a zip, doing compression is probably the first thing you want to do. You cannot compress encrypted data because it's inherently pseudorandom, if it's good encryption. So you need to compress it, if you're going to, beforehand. And most PGP content is compressed because, once you encrypt it, it becomes binary. And binary is often not safe to pass through email gateways if email is the conduit you want to use. So that requires that the binary be inflated back into ASCII - and we'll talk about how that's done - making it larger. So it makes sense to first make it smaller, then encrypt it, then ASCII-ize, it which is going to inherently make it larger. The result, though, is going to still be smaller than if it was non-compressed because you're only making it a third larger. And typically text compression generates huge levels of compression.

So you take the text and compress it. Then, if you want to sign it, you hash that result and then encrypt the hash with your, that is, the sender's, your private key. So what we have at this point is a hash of the text which is encrypted with your private key. So obviously at the other end, if somebody wanted to verify that it hadn't been modified and that you were the sender, but if it wasn't encrypted, that is, you could sign without encrypting, then all they would have to do is they would hash what they receive and then decrypt the encrypted hash that you sent using your public key.

And because of, as we know, the nature of asymmetric keys, in order for it to properly decrypt, it had to have been encrypted with your private key. So decrypting the hash with your, the sender's, public key guarantees that the hash was made with someone having your private key. So, and then, if the results match, if the hash that was sent matches the hash that was computed right then, then we know that the document has not been altered.

So that's the signing side. And again, nothing special about this. I think one of the nice things about this is that Phil just stayed with standard, by-the-book protocol, doing nothing fancy. So once that's done, if you do want to get - so that gives you authentication and verification that it hasn't been altered. If you also want privacy, then you get privacy from encryption. So then a pseudorandom number is pulled out of thin air, only meant to be used once, so nice and long. And that is used as the key for symmetric encryption.

So a nonce, as the term is, n-o-n-c-e, is grabbed from a pseudorandom number generator that is a random one-time use string of bits. That keys a symmetric cipher, and the cipher could be - the cipher is specified in the headers so that the recipient knows which cipher to use for decrypting. And there's the standard range of ciphers. AES is there. There are some stream ciphers, and there's IDEA, 3DES, and a number of others. So again, it is cipher-agnostic within the protocol, and the headers describe which ciphers were used, whether signing is there, whether privacy is present and so forth.

So a random number is generated. That's used as the key to encrypt the document. And then, much as with the hash, the random nonce is encrypted with the recipient's private key. So you know where this is going to be sent to. So you use their public key - did I just say "private" a second ago? I might have said "private." With emphasis. Which made it extra wrong. The recipient's public key.

Leo: You can see why this is challenging for people.

Steve: Yes. Yeah, you ought to be very careful with this. So again, the nonce, which was chosen at random and used to encrypt the document, is encrypted with the recipient's public key, which is all the public, all anyone has. So that protects the key while it's being sent. So all of this is bundled together and shot off to the recipient. The recipient receives this blob, and the PGP technology at his end looks at the headers, sees which ciphers are used, is it encrypted, is it signed and so forth, and basically reverses the process. There, bound in, will be the key that was encrypted with their own public key. So they use their private key, which only they have, to decrypt it. And so what this is doing is this assures the sender that nobody but the valid recipient can view the contents.

So you're saying, I want to send something. Yes, I want it to be encrypted. But, whoa, I want to make sure only the person I'm sending it to can decrypt it. Well, given, if it's true, that the recipient is the only one who has the private key that matches their public key, then you use the public key to encrypt the encryption key so that at the receiving end the recipient can use their public key to decrypt the encryption key. That gets the nonce back at their end, and then they use that with the same symmetric cipher specified in the headers to turn it back into compressed text, assuming that it was compressed, and then they decompress that in order to get readable text. And so that's it. I mean, nothing, there's no other craziness. It's just standard, by the book, this is the way the world has figured out how to do crypto.

Now, there were some extra challenges, though, in the use of email because email has traditionally been ASCII. And if you start moving binary data through email, you quickly find out all the horrible things that the email channel does. Gateways, for example, sometimes they'll just change the line endings from UNIX-style to DOS-style, or DOS-style to UNIX, meaning that UNIX just uses a linefeed; DOS uses famously a carriage-return linefeed. And so the idea, well, we're UNIX here, so we're going to strip the CRs and just make them LFs. Well, okay. But if this is not readable, if this is encoded somehow, then you've just broken the signature, at the very least, and probably caused all kinds of havoc.

So in the OpenPGP spec which is now sort of the standard specification, as you said, Leo, enshrined in RFCs, they call it "ASCII armor." They take this very seriously, the problems that email gateways present. And so it's certainly well known that many of the links on the Internet traditionally were seven bits. Many people may, old-timers among us, may remember that modems sometimes operated with, like, you had seven or eight bit of data, and then one or two bits of stock bits, and then sometimes parity. And so actually you might even have a channel. Your actual channel wasn't even a byte wide. It was seven bits wide. And so you could only send the first half of the 256-bit set.

And the good news is text, the ASCII character set, fits all within that first half. The first 32 are all the control characters. And then you've got special characters, uppercase ASCII, or uppercase alpha, lowercase alpha, and then the numerals, and then tildes and backslashes and so forth. So what they do in order to convert something which is - by the time PGP is through with it, it is definitely binary. I mean, you've taken this - you'll have readable headers. You'll have ASCII headers. But the actual content, the body that is described by what's inside has been turned into absolute pseudorandom noise that is binary. So that cannot safely be moved.

I mean, if you were storing it in a file, if you were using it in a file system, it can remain that way. Or, if you were uploading it somewhere for someone else over a channel which

is inherently binary capable, again, you don't need to change it. But if you're emailing it to someone, they're just, essentially, because email was designed for text, it will preserve case, we know that, and it will normally not mangle printable characters. But unprintable characters, very much like white space of various sorts, tabs and spaces sometimes get transliterated. Character terms can be removed, as I said. So you just can't let that happen.

So this ASCII armor approach uses a well-known approach known as Radix-64, where we want to - what we're sending is essentially Radix-256, that is, they're 8-bit bytes of binary data. We need to reduce those to six bits because six bits gives us a choice of 64 symbols that map into six bits. And we can easily find 64 symbols that are printable that we know no email gateway will mess with. And we use uppercase A through Z, lowercase A through Z, zero through nine, plus, and forward slash. And so that gives us that, I've just described, that 64 symbols.

We know that email maintains case, so it's not going to change the case of things. And so the way they convert this is sort of clever. Imagine that you take three bytes together. Well, three bytes of eight bits per byte is 24 bits. So you can take that 24 bits and divide - which starts off as three sets of eight. You can subdivide, you can re-divide that 24 bits as four sets of six because six times four is 24, just as three times eight is. So now, simply by chopping that 24-bit string into four chunks of six bits, then we take each chunk of six bits and use a map to look up which of the 64 characters we want to translate it to. And that allows us to take a binary blob, which is not safe to email to someone, turn it into text, essentially, and that's where I said it increased the size by a third because it's going to take every three bytes and turn that into four characters. So that's a third larger than it starts out. But it can move through email safely.

At the receiving end, the process is simply reversed. Sets of four characters are then converted back into three bytes in binary. That allows PGP to reconstitute the original binary. And then it just reverses the process, as I described before, at the recipient end.

So as we said, there's flavors of PGP, OpenPGP, GnuPG. Leo, you and I talked last week about Mailvelope, which is a plugin for Chrome and Firefox. There is a nice OpenPGP compliant client for iOS called iPGMail. Android has a number of apps, not surprisingly. There's APG...

Leo: Yeah, we use that one, yeah.

Steve: ...which is an OpenPGP implementation.

Leo: Still not ideal on mobile, unfortunately.

Steve: No, agreed. There's also OpenPGP Manager, and there is even a PGP-based secure messaging solution, an SMS that uses asymmetric encryption.

Now, stepping back from all of that, there's, like, the problem that we have with it is, my sense is, and I've articulated this before, is the fundamental problem that the world has, not just PGP, not just us here on the podcast, but the problem that the Internet has is authentication. And it's one of the topics we talk about all the time. That's where YubiKey came from, where all of our one-time passwords, the time-based passwords, the multifactor authentication, I mean, we're talking about authentication all the time

because that is the problem. We have the technology to establish between two people an absolutely secure channel.

But when the people are remote from each other, there's no way to prevent a man in the middle from bifurcating that agreement of, for example, a secure key by pretending to be the other end to each of the other ends, and creating two links with the so-called "man in the middle." The only way to prevent that is if we mix in authentication because the man in the middle presumably cannot authenticate himself to each of the endpoints as being the people they think they're connecting to. So this is, no matter what we do, we keep coming back to this problem.

Now, the novel approach which Phil took - because he understood about PKI, the standard Public Key Infrastructure, and there is now in the later versions of PGP the notion of a hierarchy of keys. You can have a key which is like a certificate authority, which is able to sign other keys. And then you could have a key above that. They're called "levels," Levels 0, 1, and 2. You can have a Level 2 which is able to create Level 1 keys, which is like, so it's able to create certificate authorities, which are then able to sign other keys. So there is a notion of a hierarchy within the later versions of PGP.

Leo: Which is generally not used. It's really the Web Of Trust, or WOT.

Steve: Right. I could see maybe in a corporate setting...

Leo: Yes, yes.

Steve: ...where there you would want essentially to run your own certificate authority. You'd use a key able to sign other keys in order to create the keys which your employees would all use. And then they would all trust keys signed by the level - they would trust the Level 0 keys signed by the Level 1 authority, if it was like a corporate authority.

Leo: I mean, my - what we do informally, and I've asked people to do that, is to sign my key. And they ask me to sign their key. You do some verification of some kind. In fact, the signing process is interesting because you are asked how much verification you've done.

Steve: Yes. In fact, that's formalized in the specification, Leo.

Leo: Yeah, yeah.

Steve: There is a series of levels of how sure you are that this is the person who the identify assertion binds to.

Leo: Your choices are: I will not answer, I have not checked at all, I have done casual checking, I have done very careful checking. And then you can look at people's signatures - on my key, for instance, I have 20 or 30 - and see how

confident they are in that signature. I think this is a good system, mainly because it eliminates this Hong Kong Post Office problem.

Steve: Yes, yes, exactly. And therefore, I mean, that is the problem with the public key infrastructure, the formal PKI that we have where, exactly as you say, there are some certificate authority - I mean, there's many problems. There's, like, you have to trust them. You have to trust what they do. You have to trust that no one is impersonating them and so forth. So as you say, Leo, this Web Of Trust is essentially sort of a self-bootstrapping sort of community agreement. Lots of people have made the assertion that you are you. And so when someone looks at your key they go, wow, this seems reasonable. But...

Leo: You can see my current key if you - by the way, the other thing, and I get a lot of people sending me encrypted email, saying can you read this, and is it working, and will you sign it and send it back, et cetera, et cetera. And I'm certainly open to doing that. My key is public, as it should be, on my web page, Leoville.com. But one thing I find people often forget to do, and all of these tools will let you do this, is upload your key to the key server. It's easy. You can attach it to an email. But when you create a key, there's always a command, send key to server, public key to server, that is safe, in fact encouraged. That's how other people can sign it, and it's how I can get it.

So if somebody sends me an email, and I want to see if I can talk to them securely, I can check for their key on the public server, add it to my keychain. I have almost a hundred keys now from people who've sent me email in the last few weeks. And I will continue to add names to that because I think we all ought to use it. And of course every email we're encrypting is completely stupid and trivial. That's not the point. In this case, it's to use this system so that we have it.

Steve: So, yeah. So I guess where I come back to is I wanted to absolutely give our listeners every confidence that PGP in all of its various flavors - now, that's, I mean, understanding that, as I said last week, a mobile platform is inherently a little scary.

Leo: It is, yeah.

Steve: Because it's mobile. We were talking about Bitcoin and keeping your whole Bitcoin fortune on your phone. That's, eh, I don't know. Mobile platforms are - they're just exposed to more danger. And we know that exposure is unfortunately a concern for security because we don't have perfect security. So, subject to implementation mistakes, the fundamentals of PGP are as good as any known. I mean, it is serious, it's been seriously vetted. It's mature. It's old. Real security people have looked at it and said this works. And it has, there has been versioning evolution over time. Subtle, small, and sometimes just theoretical mistakes in the definition have been found, have been fixed and eliminated, and PGP moves forward in versioning. So it's everything that's there is absolutely solid. So if somebody has a use for it, I would endorse it without reservation.

Leo: Let me just show you, for those who are curious, this is what you see on

encrypted email that has not been encrypted. And the important point here is that the metadata, the to and from information and the subject, data, and time, along with all the other headers, are visible. But the message itself is just gobbledygook.

Steve: Right.

Leo: That Base64 gobbledygook that you were talking about. All in ASCII, yeah.

Steve: Right. So anyway, so that's really where I stand is the technology is solid; the spec exists. Because it's been around for so long, it's cross-platform. It's available with - a friend of mine was saying that he looked at IMail, and it's very easy to add PGP technology to the Mac platform.

Leo: Yeah. This is so simple. GPG Mail is the easiest tool ever. And there's GPG for Win, as well, that is very easy for Windows. It's tougher on iOS and Android, unfortunately.

Steve: Yeah. So I guess where I could - I've asked myself, okay, well, probably most of us are not using it.

Leo: Nope.

Steve: And, like, why? And it's like, well, okay, I'm - I do have instances where I'm feeling self-conscious about my mail going in the clear. And so - and I have a couple very close friends who I communicate with. And I'm sure that sometimes I'm writing things, and I find myself thinking, huh, when is this going to trip any false positives because I'm writing what I am? So there, if I had my friends set up with PGP, and I were, then I could be corresponding with absolute comfort knowing that that wasn't happening, that there was absolutely no leakage of my mail.

Now, it is the case, as we discussed previously, that the fact of my communicating is public. But that's a consequence of email. We were talking about the metadata headers that route the mail from sender to recipient. Well, that has to be visible. So the fact that I'm communicating, of course, with a couple of my friends, that's - I'm doing that all the time. Who cares? So it's important to remember that that isn't being protected. And we will be talking about, initially about Bitmessage because so many people who are listening want to know the details of Bitmessage. But I'm absolutely certain that before long we're going to start seeing some solutions surface, just because I think unfortunately the climate has created a demand.

Leo: Yup.

Steve: And we've got all the technology we need to fulfill that demand.

Leo: Yeah, it exists. In fact, in the early days of PGP, the government was very, very nervous about it, forbade its export and so forth, because they knew this is strong encryption.

Steve: Well, and Phil famously printed the source code on pages of a book that the MIT Press published because the First Amendment protects the export of books.

Leo: There you go.

Steve: And so he just thumbed his nose at the government and said...

Leo: It leaked out, and it's everywhere.

Steve: ...here you go.

Leo: And they gave up on those restrictions. The other thing I would say I don't wait until it's just private stuff. Use it all the time. Otherwise...

Steve: It'll never get critical mass.

Leo: Well, and when you use it, it's like saying, hey, by the way, this is the one you want to try to decrypt.

Steve: Oh, right. Oh, exactly [laughing].

Leo: The answer is not to only encrypt stuff that's private, but to encrypt everything. And that's what I do. If I have your key, you will only get encrypted mail from me. The other thing that you didn't touch on but is also important, and one of the reasons I started using PGP 16 years ago, is it has as one of its features the ability to sign mail to verify its identity. And because people from time to time impersonate me and so forth, I've used that for a long time. It confuses the hell out of people when they see this signature. But if you have PGP running, you can verify this came from Leo. Otherwise, as you well know, it's very easy to spoof email. So that was the main reason I started using it is merely - and it might be a good reason for everybody to use it - a cert, this is authenticated, this is me. And there's also a certificate system, S/MIME, which I suppose one day we should do a story on, a show on, as well.

Steve: Yup.

Leo: Because that's another way a lot of - it may be easier to use.

Steve: That's, well, yeah. That is the - I know that many clients have that built in as opposed to needing it added on. And it is a traditional PKI-style, public key infrastructure...

Leo: With a signed certificate from VeriSign or...

Steve: Exactly.

Leo: Or the like.

Steve: Oh, and I did forget to mention that PGP now also supports expirations on keys, so that you can get a time-limited key that will - like your corporation may issue it to you, just as, again, because it's good to keep them fresh.

Leo: If you look at my keys, only use the most recent one, folks, because I didn't set a time limit on most of my keys. There's many since 1997. You can also now, and this is really good, this is new, create a revocation key.

Steve: Yup. You can revoke them.

Leo: So that's what I would suggest is perhaps not set an expiration date, but do make sure you get and save in LastPass or somewhere a revocation key. That way you can from time to time revoke old keys. Because all my keys are up on the key server. And I do occasionally get email from people that is encrypted with an older key that I no longer have access to. So use the most recent key. Or just get it from my web page, Leoville.com. And if you've got an old key for me, get a new one, update it.

Steve: Pushing back for a minute, I know we've got to go, but if we only had a solution for authentication. And I don't know...

Leo: Well, guess what? All the strong rumors are going forward that September 10th Apple's going to announce a new iPhone with this AuthenTec fingerprint reader built into it. And this is more than rumor, in my opinion. I've heard it now from sources that are unimpeachable. So that's going to be widely available is a strong authentication, we hope, a strong authentication system built into the phone. Half the people who use smartphones use iPhones. So that could change things.

Steve: Yeah.

Leo: That could change things. I'd like to see Android, though, do that as well. Apple's a little bit...

Steve: Oh, I agree. And it has got to be - it's got to be universal.

Leo: It's got to be universal.

Steve: It's got to be something. For it to work, everybody needs it.

Leo: Yeah. Thanks, Steve. Great show, as always. Maybe one of the most important you've done. I have a feeling this will be oft downloaded. Encourage people to get a copy of it and share it with your friends. Steve has transcriptions, text transcriptions by a human, so they're very good, on his website, as well as 16Kb audio for people who really have limited bandwidth. That's GRC.com. While you're there, get SpinRite, the world's best hard drive maintenance and recovery utility, getting better all the time. And lots of other freebies there. It's worth browsing around.

If you like Steve, if you like this show, visit GRC.com. You'll find plenty to enjoy there. And of course you can follow him on Twitter: @Sggrc. We also have high-quality audio and video of the show available for download on our site, TWiT.tv/sn. Or you can watch us live. Some people do. They want the latest. 11:00 a.m. Pacific, 2:00 pm. Eastern time on Wednesdays. That's 18:00 UTC on TWiT.tv. Please stop by. We love it if you watch live. And if you can't, you can always get a version from us or Steve, or subscribe in your favorite podcatcher. You'll get it downloaded.

Steve: And again, a strong urge to go see Triangulation Episode 115, Leo and Esther Dyson together.

Leo: Thank you. It was really fun.

Steve: It was just really delightful.

Leo: Today we're going to interview Phil Rosedale, who founded Linden Labs, the creators of Second Life. That's going to be - he's a very interesting person. You know, Steve, I kind of want to close with this. We talk a lot about engineering, computation and so forth. There's a video going viral. You know I sent my son off, Henry, to University of Colorado Boulder this morning, his freshman year in college. And all over the country kids are going back to school. This is a video that was posted on YouTube of a speech given by a senior engineering student to the incoming freshmen at Georgia Tech, one of our great schools. And I think it's a great, inspiring way to end Security Now!. Steve...

Steve: Cool, thank you.

Leo: Thanks for the show. We'll see you next week on Security Now!.

Steve: Thanks, Leo.

[Clip] We chose Georgia Tech because we want to do the impossible. And this school is equipped with the resources and faculty to help us do just that. And so, in the words of Sir Isaac Newton, if I have seen further, it is by standing on the shoulders of giants. Georgia Tech is proud of its many traditions, but the one I find most exciting is our tradition of excellence. Our mission as students is not to follow in the footsteps of the astronauts, Nobel Prize Laureates, and presidents who graduated before us, but to exceed their footsteps, crush the shoulders of the giants upon whom we stand. We here are all such innovative people. So I am telling you, if you want to change the world, you're at Georgia Tech. You can do that. If you want to build the Iron Man suit, you're at Georgia Tech. You can do that. If you want to play theme music during your convocation speech like a badass, we're at Georgia Tech. We can do that. I am doing that.

[Laughter]

Leo: And that would be true of MIT, Cal Poly, Rensselaer, and all the great technology schools in this country. If you're going to college right now, the world is yours to change. We need a lot of help.

Steve: Yup.

Leo: To do it. Thank you, Steve.

Steve: Thanks, buddy.