Listener Feedback #102

Description: Steve and Leo discuss the week's major security events and discuss questions and comments from listeners of previous episodes. They tie up loose ends, explore a wide range of topics that are too small to fill their own episode, clarify any confusion from previous installments, and present real world 'application notes' for any of the security technologies and issues we have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-269.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-269-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 269, recorded October 6, 2010: Your questions, Steve's answers, #102.

It's time for Security Now!, the show that covers your security online, your privacy online. And who better to do that than our good friend, our mentor, our security guru, Mr. Steve Gibson from GRC.com, creator of SpinRite.

Steve Gibson: Hey, Leo.

Leo: Hey, Steve. How are you today?

Steve: Great. Great to be with you again, as always.

Leo: So today I think we have, if I'm correct, we are Mod 1; right?

Steve: Yeah, we are odd parity today. It's our Q&A #102.

Leo: Yikes. And we've got some great questions.

Steve: Yeah, we had, as you can imagine from last week's episode where we talked about this very troubling potential new legislation that's being pushed on Congress by the FBI, and apparently with the support of our current Obama administration, a huge

amount of response. I've tempered it to - I selected three out of literally hundreds of responses which turn out to be sort of representative of the different things everyone was saying. So I wanted to acknowledge everyone who wrote and to thank you for that. And so about midway through today's Q&A we've got those three people who were pretty much representative of what everyone had to say. Not much in the way of updates, and actually not much in the way of news. So, but I think we have a bunch of interesting observations from listeners, and questions.

Leo: I can't wait to hear. Now, the good news was that the piracy initiative, COICA, was dropped, was tabled. So...

Steve: Yeah.

Leo: That at least we don't have to worry about until next time because it's not - they're going to bring this up, the recording industry's going to bring this back every single session until they have a positive Congress. But this other one, the Obama administration and the FBI said they would bring this to Congress in January. So...

Steve: When it reconvenes after the midterm elections. And I'm - we'll talk about this in the middle of our Q&A. But many people have just said, oh, don't worry about it, it'll never pass. And it's like, eh, you know, folks, you mention terrorism, and the problem is the FBI's not wrong about this being a problem. I mean, this is a problem. I mean, as we discussed last week, it's a viable issue that they can make. And we have had troubling legislation like the DMCA pass which really causes trouble. So I'm less sanguine about this not being a problem going forward. So we'll see.

Leo: Well, one way or another, you've got to pay attention to it. I've learned never assume that something you think couldn't happen, won't.

Steve: Yeah.

Leo: I mean, I never thought we'd elect a movie star President. And so there you go. Before we get into this subject - or a movie star governor, for that matter.

Steve: There you go.

Leo: Pretty soon we'll have a movie star president of the Internet. Maybe.

Steve: Nobody will know or care about him.

Leo: Nobody, yeah. Did you know that I am the president of the Internet? You didn't know that, did you.

Steve: I'm glad, Leo. I'm glad I know you.

Leo: Duly elected. By a vote of about a thousand people who heard about it.

Steve: Apparently nobody there at the TWiT Cottage voted for you, though.

Leo: No, no. They know me...

Steve: They're a little upset from yesterday.

Leo: They know me far too well to vote for me. So before we get to questions, and I'm sure we have some great ones, do you have anything you want to talk about, Mr. Gibson?

Steve: Well, we have some updates and some news. Actually very few and not much of either. But as Adobe promised, due to the fact that they had that very bad buffer overflow vulnerability - why does that surprise anybody - a zero-day which has been known for about three weeks. As we know, last week they pushed out a quick fix to their Flash Player, which was one of the ways that this was causing problems. This week on Tuesday the 5th they pushed a week ahead of their normal quarterly patch cycle. Normally they've said that they're only going to be patching on the second Tuesday of the month every three months, so quarterly. Reader and Acrobat versions 9.34 and earlier have now been brought up to date a week ahead of time. So this fixes the zero-day vulnerability that had been actively exploited in targeted attacks since it was discovered in the wild.

And I'm seeing here that I've got a - I have Acrobat installed on this system, and so I'm seeing that it's got a little red icon on my tray saying, okay, update me, update me. So I did notice that it said it's going to have to do a restart. So it's like, okay, well, I'm not doing it now during the podcast, or just before the podcast.

Leo: Yeah. Do like Leo does, yeah.

Steve: Learned that lesson.

Leo: From me.

Steve: And then I just wanted to mention that Google Chrome continues to quietly move itself forward. The news that I saw was it had gone to 6.0.472.62. And when I thought, oh, I wonder if that's what I have, mine had already moved to 63. So it's creeping forward. And in the move to 62, I know that they fixed two remote code execution vulnerabilities, one involving scalable vector graphics, SVG, which is one of the newer technologies. And they're experimenting with a protocol to replace HTTP called "SPeeDY." The letters are SPDY. So this is sort of an experimental protocol.

Essentially many things have changed on the way the web works since even HTTP was developed, and even moved from 1.0 to 1.1. There are problems like, yes, you can slipstream or - I don't mean slipstream. You can issue requests sequentially ahead of time in a pipeline, "pipeline" is the word I was looking for, and get the responses back. But many things are redundant, like the browser headers are, like, being re-sent over and over and over with every query. And queries are small relative to the browser headers that are often much larger even than the thing you're asking for, as all this metadata that no one ever sees. And it's highly repetitive, and it's uncompressed.

And so Google is sort of leading the way in looking at what can be done here to make web interaction better. Of course, they've got a strong motivation for doing so because their whole model is a web-centric model, which frankly I'm finding myself more and more a fan of, this idea that apps are going to be in the cloud, data is going to be in the cloud, and we'll be using lighter-weight clients to access our apps and our data remotely.

Leo: And updates will be in the cloud, which is the main point; right?

Steve: They'll just be transparent.

Leo: They're automatic.

Steve: Yes. The problem, of course, is the bad guys will be in the cloud, too.

Leo: Oh, of course.

Steve: So, and there's the whole question of data integrity and safety and all that stuff, which is no small issue. I'll go kicking and screaming into the cloud. I like to have my data here and to move it around between devices. But I have to say, as I'm using things - for example, LastPass. We talked about it, of course, several episodes ago [Episode 256]. I should mention that I'm just loving it. I mean, I'm really liking it. And the fact, for example, that I can change a login username and password on one system and then realize when I'm using my iPad, for example, it's like, oh, shoot, I changed that, didn't it. And I go, oh, wait a minute, I've got LastPass. And so it's maintaining synchronization among all my instances. I mean, it really is working. And I've had a lot of very positive feedback from our listeners also in our Security Now! feedback mailbag about how much they're enjoying LastPass. So that's been a win. And so there's a perfect example of a cloud-based app that I think makes a lot of sense.

Leo: Of course it's cloud and local because the storage is local. So it's a nice - it's a great mix. They've solved some of the things that you talked about - availability and issues of my data being somewhere else - by a hybrid solution that works well.

Steve: Right. And so, exactly, if you're disconnected - well, on the other hand, if you're disconnected, it's not clear what...

Leo: Well, you can't do it.

Steve: ...what you're going to be logging into. But, yes, it's certainly good to have it stored locally, as well. If they happen to be down briefly, that would be a big problem for everyone using it.

Leo: Right, right.

Steve: So anyway, so Acrobat Reader updated. Chrome is sort of just sort of taking care of itself. And frankly, as I look at Chrome doing this, and I was thinking about this this morning, it's like, that's not such a bad thing, just to have it not making a big deal about updates, just having it doing it in the background, so that it's fixing itself for you.

Leo: I think IE9 is going to do that, too. And people get upset about the idea. They don't like the loss of control that that represents.

Steve: Yeah, I know. Especially, well, especially when it's, like, rebooting your machine without your knowledge or permission, or making other big changes. It's one thing for it to just sort of like, I mean, Chrome behaves itself very well. When you fire it up, it's already updated. It's like, oh, okay. It's really not ever telling you you need to reboot your system, so.

Leo: Can't do that with an OS, though.

Steve: No. RIM, our famous BlackBerry publishers, are going 'round and 'round with India. They have just succeeded in giving India so-called "manual access" to the BlackBerry Messenger data, meaning that if specific entities that are authorized to do so in India ask for audit trails, essentially, of BlackBerry Messenger dialogue, within four to five hours after making that request, BlackBerry is now able to provide those entities with paper printouts of Messenger text. Then they're promising what they're calling fully automated, real-time access to the same data by the start of 2011, so the start of next year.

The problem is, RIM continues to assert their technological architectural limitation relative to email. Email is different than Messenger, and email enjoys point-to-point encryption, where RIM's technology just simply doesn't let them provide what India wants. So it's not clear what's going to happen with that. I mean, it's been mentioned that alternative phone systems, for example, like the iPhone, don't use the same kind of certificate-based, point-to-point encryption which literally, I mean, there's nothing RIM can do. They're saying the architecture doesn't permit any sort of a man-in-the-middle decryption. So we're going to wait to see what happens. And India is still saying that they are on the verge of approaching Google and Skype and saying, you guys are next. We need to have access.

Leo: Wow. Yeah, well, this is very similar to what's going on in the states.

Steve: It's very, exactly, it's very...

Leo: In fact, I think it inspired it.

Steve: Well, in fact, yes...

Leo: The FBI says, well, if India gets it, we want it.

Steve: Yes. I did read, in preparing the podcast last week, preparing the production of that, there were some comments where people were feeling that, behind the scenes, the three-letter acronym agencies here in the U.S. were looking at what other countries were getting, the concessions that they were getting, saying, hey, those look pretty good. We'd like some of that, too.

Leo: Yeah.

Steve: And of course we do it here by writing a law and enacting it in Congress, and then having the Obama administration sign it. My last note of news is that Comcast, that has been testing in limited geographic markets so far an automated, proactive bot notification system, is now taking it nationwide. Comcast is the largest U.S. residential ISP. And they've got something on their - they have sort of an umbrella called Constant Guard, which is their service. There's a page, constantguard.comcast.net, where they sort of talk about the different services that fall within this Constant Guard umbrella.

Under Proactive Bot Notification, that page says: "As a new feature of the Constant Guard service, we may email a 'Service Notice' to your Comcast email address if we believe a computer behind your cable modem may be infected with a type of virus called a bot. A bot is a malicious form of software that could use your computer to send spam, host a phishing site, or steal your identity by monitoring your keystrokes. The email will advise you to go to the Comcast Constant Guard Center at http://constantguard.comcast.net, where you can access resources to help you remove the bot from your computer. The Service e-mail will look like this." And then that page gives you a sample, which I think is smart because they're wanting to help you recognize it when you receive it and help you take it for, I mean, treat it as authentic email. And it says:

"Dear Comcast Customer: The Constant Guard service has identified that one or more of your computers may be infected with a bot. Please read on.

"A bot, also referred to as malicious software or malware, is used to gain control of your computer, typically without your knowledge. Online criminals can use bots to collect your personal and private data, such as Social Security numbers, bank account information, and/or credit card numbers by monitoring your keystrokes. This can lead to identity theft and fraud."

And then lower down on that page, about "Virus-Bot Information," it explains that, "According to the National Cyber Security Alliance, bots are the Internet's fastest-growing cybercrime, and 71 percent of consumers don't even know what bots are and what they can do about them. Comcast wants to help its customers stay educated,

informed, and safe online. A bot is a type of virus that allows an attacker to force your computer to perform actions, usually without your knowledge. Once a bot is in control of your computer, it can be used to send spam, host phishing sites, or infect other computers. Online thieves use bots to collect personal data such as Social Security numbers, bank account information, credit card numbers, et cetera. When this personal data is collected without your permission, it's often used to steal your identity, withdraw money from your bank accounts, and make fraudulent purchases on your credit cards." So I think this is fantastic. I mean, this kind of...

Leo: Yeah.

Steve: Yeah, this kind of - first of all, two things. The fact that they're now rolling out automated detection of bot infection for their customer base is great. But from an educational standpoint, the fact that people who are infected will be proactively notified and begin this education, I mean, this is the kind of stuff we really want people who are infected to be informed about and to take seriously. So this is just - this is wonderful news.

Leo: You can't see anything wrong with anything they said? Sounds all right and sounds all good?

Steve: Well, yes. It does. And again, I mean, the reason I wanted to spend a little time on it is that this is just - this is really proactive and great news.

Leo: I guess one of the reasons - Comcast is I think the largest Internet service provider in the U.S., with millions and millions of customers. So it's important that they do this from the point of view of everybody else because they're protecting the rest of the 'Net from their customers, who are a prime target. But one of the reasons they haven't done this in the past, in fact, remember they were reluctant to block port 25, outbound SMTP, which was used for spam forwarding, is because of the cost to them in tech support calls, all the people calling, going, agh. And I know because I answer these calls on the radio. It's literally millions and millions of dollars. So a pat on the back to Comcast for biting the bullet and doing what they really need to do.

Steve: Yeah, and essentially cleaning up their own network that way, too.

Leo: I think we've said, certainly I've said it many times, that if we wanted to stop spam, clean up the networks, the first place to start is ISPs. If ISPs implement these kinds of policies and block this kind of stuff, it stops.

Steve: Well, and they're in a perfect place to do it. They're at a point where all of their customers' traffic is focused down into one center. If they deploy the technology which they have to do some behavior profiling, to look at the kind of traffic coming from individual customers, it's very clear when there is a bot on someone's machine. There is specific behavior, specific easily identifiable activity.

Now, of course there will be a reaction on the bot manufacturers, or the bot makers, that the fact that this kind of profiling is happening will cause them to change the bots such that they don't show up on the radar as much as they do right now. Because there hasn't been this kind of profiling, there's been no need for them to pretend to be more legitimate. Unfortunately, they can do that. So it'll be a back-and-forth. But Comcast can follow that, too, and continue to move that bar forward. So I think it's great they're doing it. And I love it from a consumer education standpoint as just really good news.

Leo: Yeah.

Steve: And I did have - and this is a different sort of testimonial, sort of a little sideways. The subject was "SpinRite Acclaim," although it's a little different than the, well, like I said, the type of email I normally read. It says, "A few weeks ago my Mac Mini claimed it could not log me on. Nothing I could find at Apple.com could help, and I realized I had moved my home folder to an external USB 2.0 hard drive. Along with my home folder, I had my entire iTunes collection on that drive. It was immediately obvious that the external hard drive had a problem. In iTunes I not only had thousands of music files, but also lots of purchased TV shows and full-feature movies. I use this Mini only for iTunes, so I moved this hard drive to a PC and could still not access the iTunes library.

"I thought I was going to be ill after realizing the impact of losing all that data. But I decided to spring for a license for SpinRite. I went through the purchase and downloaded the software and set to work on another spare PC. I had heard it could take days for the defects to be repaired. Well, after three days, the progress was stuck at 0.05 percent. I figured I was screwed. I at least expected some progress, but I stopped the process. Desperate, I went to the GRC.com newsgroups to read about this. I saw that external drives usually took an extremely long time to be processed, and that users should attach the hard drive inside the external drive directly to a motherboard, if possible.

"So I sacrificed the drive enclosure - it wasn't exactly user serviceable - and took the hard drive out, placing it inside a spare PC, and started SpinRite again. In less than four hours it had completed the pass, reporting that four errors could not be repaired. Unfortunately, those were areas I needed, so I ran SpinRite a couple more times, and eventually there were no errors. I have my iTunes library back!" Exclamation point.

Leo: Wow. Now back it up.

Steve: He says, "I quickly moved everything to a NAS server I have at home," a Network Attached Storage server. "Now I'm a believer and will be using SpinRite regularly to maintain my drives. THANK YOU," all caps, "Bobby Irvin in Rogers, Arkansas."

Leo: But I want to say something to Bobby because he said something that makes me nervous. He moved everything to the NAS.

Steve: Uh-huh.

Leo: Like that's safe. One copy of anything, I don't care if it's a RAID 5, which is better than a regular hard drive, is still only - it's not a backup, it's one copy. Right, Steve?

Steve: Yup.

Leo: Back me up here. So you need two copies. Maybe three copies. But not one copy. And just because, you know, sometimes I think people say, well, I backed it up to a hard drive, so I've deleted it on the main drive, like they're backed up. How is that better?

Steve: Right.

Leo: So putting it on a NAS is marginally better, I guess, if it's RAID 5. But I've had enough RAID 5 failures in my life to not think that that's sufficient. Make another backup. One more, at least. All right, Steve. I've got questions.

Steve: Great.

Leo: Do you have answers? We'll find out. Presumably, since you chose the questions, you do. Question 1 comes from Gary in the Motor City, Detroit. He mourns the end of the PayPal plug-in, which we talked about not so long ago. PayPal plug-in is discontinued. What do we use now? I'm very disappointed that PayPal chose to discontinue the plug-in. It was a great feeling to be able to pay for online purchases with their secure card without revealing my credit card, and have the funds come out of my PayPal account. Is there an alternative? Gary.

Steve: Well, first of all, his sentiment was also expressed, as are many of these sentiments that I choose to share, from many of our listeners who commented that the PayPal plug-in had discontinued. And I share the sentiment. I mentioned a while ago that GoDaddy was frustrated, thanks to my use of a temporary credit card number which I obtained from the PayPal plug-in, when I registered a domain as sort of an experimental domain a little over a year ago. When it came time to renew, they first sent me email. And then, when I didn't respond, they complained that they were unable to charge my card. And then they did it, I didn't mention it again, but they've tried several more times and complained. Gee, we're unable to authorize your card. We really want to charge you for a domain that you have not authorized us to renew.

Leo: You can't win.

Steve: So this is a plea or a question to our listeners, who are spread far and wide. If anyone knows of a replacement, we all want to know. I don't know of one. I know that some credit card companies themselves offer this service. Unfortunately, none that I'm using, and presumably none that Gary's using, our questioner and listener here. So if anyone knows of something like this from some accredited, reliable service, I'd very

much like to know, and I know that our listeners would, and I will pass the news along because this idea of a one-use credit card, it just makes so much sense.

Leo: Yeah. I'm trying to think. I think, is it American Express, one of my guys does do that, or at least used to do that. This would be a great service to offer.

Steve: Yes.

Leo: Visa does. But again, it's not all Visa cards. I think it's just some Visa cards. So you should check with your credit card company.

Steve: Oh, in fact I'm sure, because I'm a big Visa user. I use Chase and a couple others; and Chase, for example, doesn't.

Leo: It's up to Chase to do it, not Visa to do it; you know what I'm saying?

Steve: Correct.

Leo: Citi Cards, my chatroom is saying Citi Cards do do this. So if you have a Citibank card. I have to say, it would be worth moving...

Steve: Oh, it really would.

Leo: ...just for that.

Steve: Yes, it really would. I mean, it's such an advantage to be able to - I mean, and frankly, I'd rather use my main credit card company rather than a third party. But if a third party is not available, then - I mean, if a credit card can't do it, and a third party can, I'd sign up for such a service.

Leo: Right. So, good. So at least we know Citibank does. Of course inquire before you transfer your account over there.

Steve: Yeah, make sure you qualify.

Leo: Make sure you qualify, all that stuff. Great question, and a great point. Paul in Montreal, Quebec with Question 2 for you, Steve: Some troubling information about iPhone apps. Steve and Leo - he's given us a link to a story in h-online.com, and we'll put the link in the show notes, concerning Droid and iPhone apps. Actually I should say "Android" because it isn't just Droid, it's Android and iPhone apps and how a good chunk of these free apps are conducting data collection from the devices

they are installed on. I've seen this story, talking about Android. I didn't realize iPhone did it, as well.

He says: I've never been an iPhone user. Apart from the device being very pretty, with apps to help you find your socks, I have no urge to get one. I've always been a little put off by its lack of security and Apple's carefree attitude when it comes to security in general. Apple might dispute that, by the way.

Steve: Yeah.

Leo: I don't think they're carefree at all. But I do think, and I know you agree, Steve, that the next vector for malicious software is absolutely going to be portable devices.

Steve: It's why this question is on our Q&A today.

Leo: So this "Study: Many free iPhone apps pass device ID to the app vendor," in the Android sphere it wasn't just the device ID. Some of them were passing GPS coordinates to ad networks, where your user is, and in theory even phone numbers and other data, personal data.

Steve: Well, so this study referred to in this story echoes a number that I've seen. And I've sort of been letting these things go by because I haven't known what to do about them. And I just decided, okay, we ought to just take a moment to address this whole domain. It is the case that Android may be more troublesome than iPhone, but it's also the case that a group of researchers took a look at iPhone apps which were asking for permission, and selected I think it was 30 apps that looked like they may be doing communication, and only 14 percent, so a very small number of apps, were what they called "clean," meaning no communication back to the - while you're using the app for sort of other things, back to the publisher's server.

So we've talked a little bit about this, that these apps generally do ask you for permission. But they often don't tell you why they need the permission. It's not clear, if you deny them permission, what's going to happen. So essentially we're in a situation where I'm afraid that we're going to be spending more time than we want to be spending in the future talking about this particular area of application privacy vulnerability. Everyone wants to use these phones. It's all anyone's talking about. It's a super hot market. And this notion of third-party apps being added to give us additional functionality is what makes it so fun. But I guess the only thing we can say is, and I know probably our listeners more than any others understand the inherent vulnerability of apps which are, by their nature, bound to a radio, which are able to communicate on the Internet and back to home base.

Leo: No. 3, Sean in Woodside, New York has given a lot of thought to the technical consequences of - drum roll, please - his death. Hmm. Steve, I'm trying to figure out if I'm taking "trust no one" too far. I've been thinking about how to make sure people have access to my online accounts in the event that I'm either incapacitated

or die a horrible death in a blimp accident over the World Series. I guess he's a blimp pilot. I think we do have several blimp pilots in the audience, actually.

Steve: I guess we would have to.

Leo: As a matter of fact. But you know, we should all think about this. I think about this all the time.

Steve: Exactly. It's why I chose this. I think he makes some very good points.

Leo: I'm a LastPass user, and I considered giving my lawyer a one-time password. But after thinking more about it, I've decided I want things to be a little more secure, and I'm taking a lesson from nuclear missile silos. Here's the plan I'm thinking of using: Generate three one-time passwords. Select three trusted family members or friends who don't know each other well. Divide and combine the passwords so any combination of two people have one complete password. For example, assume that the one-time passwords are 0123, 4567, and 89ab. Yes, I know that's really 32 characters, it's just an example.

First key is the first half of password one and the second half of password two. So that would combine 0123 and 4567 to 0167. Second key is the first half of password two and the second half of password three, 45ab. The third key is the first half of password three and the second half of password one, 8923. Give each of the three - and on. Third key - anyway, you get the idea. Mix and match. Actually it's kind of clever because the first key is first half of one, second half of two. Second key is first half of two, second half of three. Third key is first half of three, second half of one.

Steve: Yeah, so as he says, he's got three family members, and he's divided the keys up so that any pair of those three are able to, together, synthesize one of those three keys because there's three ways of taking a pair of three people.

Leo: Right. Give each of the three trusted folks one of the new keys, tell him to hold it until approached by my lawyer. They don't know anything else. So they, by themselves, don't have the information they need to reconstitute a key. Give my lawyer the URL and account name for LastPass, the list of people who have the keys, and instructions on how to assemble them.

Steve: Clear instructions, I hope.

Leo: Take one from column A. Of course, part of the appeal of this is to hand a friend a card with a 32-character key and say, "In the event of my death, my lawyer will reach out to you. You will need this passcode." He just wants to say that. Most of my friends are already freaked out when I add additional authentication factors like PPP or the grid on LastPass. Giving them a secret code with instructions to wait until contacted will have them thinking I'm in the CIA. Is this too much? I'd love to hear

what you think. Well, it does the job. I can see some problems with it.

Steve: Well, okay. So, stepping back a little bit from Sean's details, I do think he raises a very good point.

Leo: Yes.

Steve: And that is, as we have, especially those of us who are tech savvy and listeners of Security Now!, who are probably, if anything, overprotecting ourselves from various threats, either locally physical, like with TrueCrypt, for example, or using LastPass with one-time passwords and so forth, I mean, we understand the world that we've created for ourselves, and we're having fun securing it.

But imagine, I mean, really run the scenario of you disappearing. Let's not give you a horrible death, but you disappear. And the people in your life need access to your world. I mean, really, how would that be done? How would that happen? If you use a fingerprint to access your laptop, and there's information on it that would be necessary for people, I mean, in your disappearance, imagine that you want them to have access to these things. I mean, you're gone, so it's important. How does that happen?

And so, I mean, it really, in taking everything into cyberspace, and taking advantage of the uncrackable technology we have now, which of course was the controversy the FBI's trying to deal with here, you can be in a situation where you may wish that people had access to this, if you're no longer able to make it happen. So I think it's worth just sort of pausing for a second and saying, you know, it's sort of the equivalent of a last will and testament, but it's how to get to the parts of my technology that I would want my family, for example, or my attorney, to usefully have access to, like bank account logons and numbers and where stuff is and so forth, which is all locked down tight. And that's well and good as long as we're here to unlock it. But what about when we're not?

Leo: I think for most people it'd be sufficient - the lawyer, look, do you trust your lawyer? Maybe a spouse? A close friend would be sufficient. I think that's enough. Although I have to admit I haven't done this. But it would kind of behoove me to write this all up and give it to my wife and say, you know, honey, if something happens to me. And then what if the two of us die, I guess I'd have to give it to my lawyer, as well, to go with the wills that the lawyer has. That seems sufficient. I'm not worried that my spouse or my lawyers are going to break into my accounts.

Steve: No. And I think that's the proper level. I think Sean's having fun dividing passwords up among his friends and freaking them out. But the point is that, do our attorneys have this information? And my guess is most of them don't right now. And arguably, maybe they should.

Leo: I don't. I haven't.

Steve: Yeah.

Leo: Edward Rosales in Springfield, Oregon wonders about the security of wireless keyboards and mice. Steve, I use a wireless keyboard and mouse with my Dell laptop. Just wondering if doing so creates a weakness and/or security hole. By the way, I'm a licensed SpinRite user, thanks a bunch. We talked about this a while ago.

Steve: Well, yes, and I thought it was due for a renewal because it's been a long time ago. What we learned was that the wireless keyboards have such weak security that essentially, when you turn the keyboard on, it chooses an eight-bit byte randomly and XORs the data that's being sent with that byte. Now, what that means is an XOR, an exclusive-or operation, inverts specific bits of the byte. So it is the case that the data is not technically in the clear. It's not plaintext. But, boy, I mean, it would just be a fun and relatively short exercise to decrypt that stream. It would be trivial to decrypt it. You simply take a look at the data and begin to play some games with a pencil and paper, and you can pretty quickly figure out what those eight bits are.

So the encryption of wireless keyboards is virtually ineffective. And it is transmitting at a distance of many meters, so 10, 20 feet, enough so that it's been shown that neighbors, like apartment neighbors, somebody who shares a wall with you, or a floor or a ceiling, is able to receive the output of your wireless keyboard. Are they doing that? Probably not. Could they do it? Absolutely.

Now, a mouse is a much different proposition. It's just sending its relative movement. As you move it up, down, left, right, it says oh, I just got moved over this far, or up this far, or over. So there's really no information of the same kind that can be captured from a mouse. But a keyboard is a different matter. So it certainly is the case that there is a security tradeoff being made when your keystrokes are jumping through the air over to your computer. There is not strong encryption happening in wireless keyboards. It's almost no encryption, and so something to be aware of.

Leo: Yeah. And there are well-known attacks on this.

Steve: Yes.

Leo: Although I think there are encrypted keyboards. Wasn't - I mean, well, but not very well encrypted.

Steve: I do remember, yes, I think I do remember that there were some that were better than others. The XORing is, like, of the weakest flavor. But I think we did hear at the time from either the chatroom or from our listeners that there were keyboards that were doing a better job.

Leo: Yeah. Brian M. in Edmonton, Alberta, Canada says Steve doesn't have to stop writing CryptoLink. Oh, because there's a Canadian audience for it. Hi, Steve. I'm glad I'm not the only one losing sleep over that proposed bill in the U.S. But I don't think you need to stop writing CryptoLink because of it. In fact, you likely won't have to change much of CryptoLink in order to make it comply. Let me explain.

At some point you're going to be using symmetric crypto with symmetric keys to encipher the data. You could just encrypt the symmetric key with a special, high-security "Steve Gibson" public key, and then include that in the stream. You won't have to shunt the traffic off to yourself. That way, it requires both you and the FBI to actually grab someone's data. That is to say, they can't decrypt it without a court order to you, and you can't decrypt it as you won't have a copy of the data. You wouldn't have to protect that key, either, as it is merely a public key and cannot be used to attack others. My understanding is that's how PGP works already, so it should be safe. Thanks for a great podcast. Yeah, PGP does some wrapper stuff; don't they?

Steve: Well, okay. So I'm not at all concerned about the technology of doing this. I mean, we've got technology coming out of our ears.

Leo: A backdoor is easy.

Steve: Yes, yes. And I argue a little bit with the people who are against the legislation taking the position that installing backdoors weakens, like, will be exploited by the bad guys, for example. I can definitely create a backdoor that no bad guy can take advantage of. And in fact, I would do it exactly as Brian suggests. CryptoLink, when connected, will use the symmetric key which the two instances at each end share. They use that to negotiate a so-called "session key," a temporary session key which is used just for that connection. All that has to be done is that that session key is encrypted with a public key which is universal for CryptoLink and which only I/GRC has the matching private key for.

So that, exactly as Brian suggests, if the FBI brought to me some captured traffic and a court order - and, see, here's where things get really screwy because it's like, how do I know that the traffic they captured is associated with the court order? I mean, the practical side of this, the doing this safely, is so full of, is so fraught with problems that it just - it goes exponential pretty quickly. Because then, as I've also said, how are they even going to know that the encrypted traffic is CryptoLink? It could be Skype. It could be anything. Anything encrypted looks like pseudorandom noise. So how do they know what it is, if they're on the wire somewhere?

So, I mean, if nothing else, when this law occurs, we're going to have a field day looking at what it is that it says and what it means to the industry. We certainly can hope that it doesn't happen. As I said, my fingers are crossed, but I'm less sure of that. But so it's not that we don't have the technology to do this. Certainly there are ways that backdoors could be unsafely installed. But we've got, we're just steeped in technology that would allow all kinds of ways for this to be done. That's not the problem.

It's what does it mean for us? I mean, and do I - how do I feel ethically about having the master unlocking key? I've had people say to me, since the story came out, Steve, we trust you. CryptoLink's features are what we want. And if all such things have to have a key, well, then, we'd rather use yours than somebody else's. So I say, okay, well, I'll take it into consideration.

Leo: Well, there's more to say about it. And our next email comes from Sweden. Dennis Astergren in Karlskrona, Sweden notes the world view according to the U.S.

Congress: Off and on during the previous years, the likes of Pirate Bay have published letters from U.S. authorities where the lawyers from the rights holders of media have stated that according to the DMCA and whatnot, they absolutely have to stop their business because they're in violation of U.S. law. Every time the same answer is given back: U.S. law does not pertain to companies or individuals outside the U.S., thank you very much. Now go away and leave us be. One sometimes gets the notion that that catches the MPAA or their attorneys off guard and by surprise. I'm sure that's not the case, it's so obvious; and yet they try.

So in terms of your episode regarding encryption and the demand for installing backdoors, it's the same thing all over again. What's stopping any U.S. company from merely selling their product via any other country or registering their company elsewhere? I don't expect the big ones like Microsoft moving shop, but still.... I'm absolutely sure both you and Leo know this, but it could be worth mentioning on the air, U.S. law pertains to U.S. citizens and U.S. companies alone. It's very easy to get the idea from listening that what you discussed has an impact on everyone. Did I miss something obvious? May I suggest you moving to Sweden?

Other than that, many thank-yous for everything. Longtime user of SpinRite and constant lurker in your newsgroups. Also many thank-yous to you for pointing me in the direction of Leo. It was your promo videos for SpinRite, visiting with Leo and Patrick, that introduced me to the world of netcasting. Regards, Dennis.

Steve: Well, so this is the other comment that I've had, both in the GRC newsgroups and from many of our listeners, who said, Steve, just move. Well...

Leo: Well...

Steve: No, I mean, they're serious. They're saying, don't you realize this is just a U.S. law, and you could just move somewhere? And someone was suggesting Aruba or something, which actually sounds pretty nice.

Leo: It's lovely, yeah.

Steve: [Laughing]

Leo: Trinidad and Tobago.

Steve: The problem is, I like it where I am. And I don't have to do CryptoLink. I have other things I can do. SpinRite could use some attention. It's been now six years since SpinRite 6.0 was launched, and it could use some updating. And I have other ideas and things that could keep me busy, that I would find interesting. I would love to do CryptoLink. I'm hoping the law is not going to happen.

But for me, moving is not an option. Nor is developing a product that I cannot myself use in my own country. So someone had also said, well, just make one that's only for export. It's like, well, okay, that's just not interesting to me. I want my friends to be able to use

it, and for me to be able to use it, and all of our U.S.-based listeners to be able to use it. So I do recognize - I will say one thing, though. And that is that it may not be elsewhere today that a law like this exists. But if the U.S. passes such a law, in the same way that we know that the three-letter agencies are looking at what other countries are demanding from RIM and saying, hey, we want some of that, too, we're precedent-setting here. And it might very well be that, unfortunately, we pave the way. I mean, this is all very disturbing. I would like to say it has no chance of ever happening. But I think it has a chance substantially greater than none. So we'll see.

Leo: Well, and I'd like to point out that, yes, the Pirate Bay thumbed their noses, thumbed their noses, and then were prosecuted by Swedish authorities, no doubt due to pressure from the United States.

Steve: Yes.

Leo: And you can say, well, that U.S. laws don't apply to us, which is of course technically true. But these content rights holders are putting pressure on every country in the world. Look at the ACTA agreement.

Steve: Yeah.

Leo: The World Intellectual Property Organization, WIPO, and others. I mean, this is - if you want to be a participant in the modern world, you're being required to be a signatory to the WIPO treaty and pass laws in your country that duplicate American laws.

Steve: Yes. And the DMCA did happen specifically because of these, the rights holders like the MPAA that pushed this thing through Congress. And we got a law which is so overly broad that it's being used, and you might argue abused, for example, to keep professors from being able to do research on copy protection.

Leo: Right.

Steve: Yeah.

Leo: Precisely.

Steve: Bad laws do happen.

Leo: Yeah. And they affect everybody globally. So, yeah, Steve could pretend he's in Aruba, but that's not a solution.

Steve: Maybe I could get some palm trees in the back here.

Leo: Well, SlySoft, which is a company that sells, a commercial company that sells, commercially available in the U.S., DVD breaking software, it's illegal in the U.S., but they operate I think out of Trinidad and Tobago. And so there you go. And sjeffn6 [ph] is saying that Pirate Bay was not taken down before Swedish law was changed. But that's the point is it starts here, and it spreads like a virus, like a bad idea.

Griff in Columbus, Missouri shares his take on encryption backdoors, Question 7. I just watched the TWiT.tv Security Now! Edition 268. You mentioned the new proposed law might not allow point-to-point encrypted traffic. Forcing encrypted traffic through an encryption vendor's server isn't necessary, I think, for the government to achieve real-time wiretapping. I suspect the government intends to obtain the encrypted traffic as it goes through each ISP's servers or routers - by the way, most ISPs already are collecting this data for the government - or maybe somewhere on an Internet backbone. Also require the encryption software vendor to provide some master key or other means to allow the government to decrypt the messages in real-time. That's the backdoor.

This wouldn't require, for example, Skype or CryptoLink's point-to-point encryption to go through a central server somewhere. Even point-to-point messages already go through a relatively small number of Internet backbones where the wiretapping could occur or maybe already occurs. And that is one of the objections is, well, you've got to change the entire way Skype works. But...

Steve: Yes.

Leo: Is that true?

Steve: Well, the story that was written - and of course we don't have a law yet, we don't have final text of one as far as I know. But, first of all, again, I chose this one because many people made the comment, and I've read this from people responding many times. So this is the third of our trio that sort of represent a consensus of opinion and feedback from this. And so there's two points.

What was specifically addressed was the nature of peer-to-peer communications, meaning point-to-point, where no third party is involved with the traffic. Skype was highlighted or mentioned specifically because we know that Skype's technology is a point-to-point encrypted stream. You and I right now are talking with Skype, and there's a flow of encrypted UDP packets directly between our two endpoints. So it's certainly true that it is - I'm using bandwidth which I purchase from Cogent, which peers with Level 3. You're using bandwidth that peers with your ISP. So it's true that there are locations on the 'Net where this communication that we're having is available. Virtually all the routers, I think there's 13 routers between you and me, Leo, so any of them represent access points.

But my reading of what was said indicated that re-architecting this kind of communication was what this law would require, that is, so that somehow the FBI doesn't have to go to, like, an ISP in order to get this, but is able to somehow present me with a court order saying that they want wiretap access to a given person's, a given customer of mine's use of my product. That's the way I read this. And frankly, I don't know how to do that. I mean, literally, well, I can't. The architecture doesn't provide it.

So, I mean, certainly there will be, I hope there will be Senate meetings where representatives of Skype and other high-profile companies sit down and explain to the senators or the representatives, with diagrams that are really clear, that this is just not a matter of flipping a switch. And yes, we would like to comply, like with the FBI's well-meaning and understandable need to have access to our technology. I just don't know how to make that happen.

Leo: Somebody's pointing out it puts your life at risk. If the bad guys say we'd like to know what this person is saying, and they come to you, they don't need a subpoena, they need a brick.

Steve: Yeah.

Leo: And that's not good, either. Let's not forget that.

Steve: Yeah.

Leo: I'm going to take a break, on that lovely note.

Steve: Anyway, so this is the last we're going to talk about it. I think we've beaten this thing to death, knowing as little as we know about what we're ultimately going to have and the way it's going to work. So I don't want our listeners to worry that this is going to be a constant theme. We'll probably come back to it early next year, if the legislation happens, or doesn't. But I did want to follow up because many people had similar thoughts about here's workarounds. And we'll just have to see what we end up with.

Leo: Oliver Stengele in Heidelberg, Germany says welcome to the rest of the world with COICA. We talked about this last week. Steve and Leo, as it is common for the listenership of your podcast, I'm a computer science student in Germany, and I'm here to bring you bad news and more bad news. The idea behind COICA, the government-controlled Internet censorship via DNA blacklists, that's not new. Not long ago we had the exact same brain-dead proposition in our political organs. They called it - now, let me see if I can get my German together because this is one of those omnibus words that the Germans love to make - "Zugangserschwerungsgesetz." "Access complication law" is the literal translation. It was headed by Ursula "Zensursula" von der Leyen and reasoned with the killer argument of fighting - they always bring this, they always truck this one out - child pornography. You watch. It'll be brought out again because nobody can stand up and say, well, I'm for child pornography. You've got to say, "Of course I'm not for child pornography."

Long story short, the whole thing went through and is currently in effect in Germany. I would like to point this out, that we take full blame in the U.S. for this because what they do, what the record industry, motion picture industry do is they try this out outside the U.S. This is what ACTA is all about, is to get it passed across the world so that the U.S. Congress has no choice but to ratify.

Steve: Yup.

Leo: And so it's a very backdoor way of sneaking this through the U.S. He says, well, not quite, because a short time after the proposition became law, some politicians realized what they had done and, due to an incredibly huge public opposition, which peaked with an online petition to the German Bundestag with 134,000 supporters, the largest petition to this day, they delayed the censoring part of the law, but did not cancel the whole thing. The details are mostly disturbing, but one thing is clear: It is a huge mess.

And guess what? Not long after "Zensursula," a member of the European parliament named Cecilia Malmstrm got hooked on the same thing, this time for the entire European Union. I do not need to repeat the reasons against Internet censorship. You and Leo named quite a few in your recent episode. But seeing now that even the U.S. is no longer safe from this Pandora's box really bothers me. If COICA gets through - by the way, tabled for now - it will become a shining example for all those countries that want to implement Internet censorship in the future, a very scary prospect in my opinion. I just hope the land of unlimited possibilities does not become the land of impossible limitations. Oh, so well said. Best regards. Keep up Security Now! and GRC. We really need you these days. Oliver. Oliver, what a great - I'm going to say that one more time. "I just hope the land of unlimited possibilities does not become the land of impossible limitations."

Steve: [Sighing] Wouldn't it be sad if we are looking back, decades from now, at an Internet which is fully censored and where encrypted communications is no longer safe from random people who are prying. It'll be sad.

Leo: Yeah, no kidding. By the way, for our Swedish correspondent, Cecilia Malmstrm, Swedish. So there. If these ideas spread, and I have to say I think we in the U.S. should take blame because most of these content companies are U.S. companies. That's who really is promoting this agenda.

Kris Ackermans in Kortenberg, Belgium, reminds us of Rijndael's 10th birthday: Steve, on October 2, 2000 the Rijndael cipher was announced as the winner of the contest the National Institute for Standards (NIST) held in their search for a cipher for AES. At least that's what I'm reading in the press today. No one has come close to cracking Rijndael in the 10 years that have passed, despite full publication of the algorithm. I thought it would be fitting to remember this occasion on Security Now! in times when governments no longer seem to be in favor of true security. Disclaimer: I am a Belgian. Ask Leo why that matters. Well, Frederique's Belgian. Maybe that's why. I don't know. I love Belgians, I don't know...

Steve: Well, and I think the Rijndael designers were.

Leo: Oh, Rijndael's probably Belgian, of course.

Steve: Yeah.

Leo: I really enjoy listening to Security Now!. It's one of the few places I know of where things are actually explained. That's true. We pull no punches in our quest for true geek explanations.

Steve: We keep the propellers spinning.

Leo: Yes. Thank you, Leo and Steve.

Steve: So I did want to acknowledge, I've talked about with regard to the crypto problem that it's math. I mean, we have now the math required and a full understanding of how to do unbreakable crypto. And it is, again, an understandable dilemma that states, as in governments, have a problem with the fact that they are not able to police and monitor what the bad guys are doing. And that as more communications is done digitally rather than in the analog world, this math, which is all it is, can be applied to communications in order to prevent it from being intercepted and understood while it's in flight. This is just the way the world is.

And I love the Rijndael cipher. We did an entire episode on it [Episode 125] where we dissected it and looked exactly at how it operates and how clean and simple and beautiful and pure it is. I mean, it's just a spectacular piece of math. And we're, as Kris says, we're not close, I mean, it's withstood a decade now of scrutiny. It is the basis for most new crypto that is done because we all know we can rely on it. And it's not going away. I mean, it's happened. It's existed now long enough that open source software has incorporated it. Nobody has to be smart in order to be able to use this uncrackable crypto. It's just available.

So the best thing that could happen, I think, when this law is up for consideration next year, is that people make the point that, yes, a huge problem could be created by legitimate publishers of software like myself and Skype and anyone else doing a VPN, if a law required that a third party be able to intercept that communication. A tremendous inconvenience would be created. Yet virtually no change in access to any communications that anyone was determined not to have eavesdroppable on because that technology is out there. It's now out in the public domain.

Leo: Rijndael, Rijndael, rah rah rah. And for people who are wondering, it's R-i-j-n-d-a-e-l, okay? It's definitely Belgian. It's not just Belgian, it's Flemish. If you're going to Google it. I bet you - I should try this. I bet you if you typed "Rijndael" in any kind of Anglicization of it, like "Rhine doll," it would say, "Did you mean...." Nope.

Steve: Well, and I do remember in the early papers that were written, when it was first appearing, they would spell it correctly, and then, parens, it said "Rhine-doll," as in Rhine-doll.

Leo: How to pronounce it, "Rhine doll."

Steve: They'd tell you, exactly, how to say it.

Leo: R-i-j-n-d-a-e-l, Rijndael. And I know how to pronounce it only because of one thing: you, Steve Gibson. Finally, our Up and Comer of the Week [fanfare]. Alec Thompson, from British Columbia, writes: Dear Steve - he's 16 - I was listening to your recent podcast, Episode 267. I was really enjoying listening to the response from 17-year-old JR Hallman. I'd like to make a sort of shout-out here that I hope you'll mention on the show. I'm 16 myself, and so far I've learned a variety of skills - C, PHP, Python, XHTML, MySQL, and even recently Assembler.

Steve: Yay.

Leo: Yay. My personal inspiration came from a site called Hell - I'm not sure I'd even want to visit this site - HellhoundHackers.org.

Steve: Hellbound.

Leo: Oh, good. Only slightly less bad.

Steve: That's better.

Leo: HellboundHackers.org. Don't be thrown by the name. The site is full of supporters for ethical hacking. Good. I like hackers. Hackers are it, man. And the majority of the site's users are younger than 25. That's why "hellbound" attracts them. Actually, if you look at it, this is a very typical kind of site for hackers where it's very focused on content and text, lot of forms, lot of information. Looks really great. Together we have a pretty strong bank of knowledge, and I thought I'd mention this in hopes to inspire other kids my age into learning programming skills. Henry, I'm looking at you, my son.

The site teaches the ins and outs of how to break into sites - I love it. But that's attractive to kids. They want the - Henry has asked me, can I learn how to hack? I will send him to Hellbound Hackers. But the reason they say is so you yourself can learn how to keep malicious hackers out. Writing secure code, as you would know, very important stuff. And I figured you might be interested in passing along the link to everybody. Whether you're under 25 or not, there's probably something for everyone to learn. I'm going to - thank you, Alec - I'm going to check it out. Thanks, Steve, and keep up the great work.

Steve: Well, so I just wanted to acknowledge Alec. We did hear from JR Hallman, whose site we brought to its knees...

Leo: Oh, sorry.

Steve: ...by mentioning his CryptScript site last week, or I guess maybe the week before. So we got a nice note back from him. And I just wanted to say I think it's great that young people are listening to the podcast and, again, to encourage people just to

get out there and do stuff.

Leo: This is great.

Steve: Because it's the future.

Leo: They have simulated security challenges, so you can really test your chops here.

Steve: Very cool.

Leo: This is great. Boy, you know what, I want to check that out. That looks like a great site. Steve, we have completed our 10...

Steve: Our mission.

Leo: ...fabulous questions, and your 10 fabulous answers, once again. If you want to know more about Steve's work, you go to his website. You'll find out a ton of stuff there, GRC.com. You can follow Steve on Twitter, too. He is SGgrc. Do you still do updates on the iPad, or Pad stuff? Because, you know, I think there's a lot of new stuff to talk about.

Steve: I haven't, except initially. For me, I mean, I'm a daily Pad user. I absolutely love it. But I haven't really run across anything that I thought was significant enough. So it's just sort of a quiet account.

Leo: Well, it's going to get active. Microsoft just announced they're shipping Windows 7 tablets by the end of the year. SGpad, that's that one. And then for the official corporate account of the Gibson Research Corporation, just @GibsonResearch. Steve also sells a very fine and must-have hard drive maintenance and recovery utility which we talk about every week, I hope you have a copy, SpinRite. You can get that directly from GRC.com in his custom-built and hyper-secure eCommerce system. You'll also find there lots of free stuff like ShieldsUP!, and CryptoLink will be there someday, maybe.

Steve: Yay.

Leo: God and Congress willing.

Steve: Yes.

Leo: GRC.com. Go to GRC.com/feedback if you want to leave a question for our next feedback episode. And you also, by the way, at GRC.com/securitynow, find 16KB as well as the full flavor of this show, and transcripts from Elaine, so you can read along, and all the show notes. That's GRC.com. We do this show, you can watch it live every week at live.twit.tv at 11:00 a.m. Pacific, that's 2:00 p.m. Eastern, 1800 UTC, live.twit.tv. You can chat along as we go. You hear me from time to time mention the chatroom. That's irc.twit.tv. And I think that's it.

Steve: Boy, you covered all the bases.

Leo: All the bases, dude. You covered all, you, YOU covered all the bases. Steve Gibson, it's always a pleasure. Thank you so much, and we'll see you next week on Security Now!.

Steve: Talk to you then, Leo. Thanks.