Security Now! Mailbag #1

Description: Steve and Leo open the Security Now! mailbag to share and discuss the thoughts, comments, and observations of other Security Now! listeners.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-102.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-102-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 102 for July 26, 2007: Steve's Mailbag.

It's time for Security Now! with Steve Gibson. We're going to talk about securing your computer, securing your access, securing your lives, locking things down. Steve Gibson, today is our first Mailbag edition, yeah?

Steve Gibson: Yeah, actually there was one - I got a piece of email that I just loved. Unfortunately I read it a couple weeks ago, I think, and I can't give credit to who wrote it because I don't remember where I saw it or where it was. But the subject caught my attention. He said, so sorry you won't ever do any mailbag episodes. I was like, what? So he made the very accurate comment that, when we refer to mod 4 episodes...

Leo: Those are our question-and-episodes.

Steve: Exactly. What we're saying is, the episode number mod 4 equals 0. That's the formal equation. So I've been calling it mod 4 plus 2. So he says, okay, well, episode number mod 4 plus 2 will never equal 0. It's like, okay.

Leo: No, he hasn't put the parenthesis in the right place. It's (mod 4) plus 2.

Steve: Well, yeah. He's correct. It ought to really be episode number plus 2 mod 4, yeah, equals 0. So it's like, uh, got me on that one. So I got a big chuckle out of that.

Leo: Oh, they are geeks. They are.

Steve: Actually, in the mail I've been reading - I didn't choose this one for today. But some guy was saying, Steve, you are such a geek. When I grow up I want to be as geeky as you are. And then he had a bunch of examples of - and you were sort of lumped in there, too, Leo. It's like...

Leo: I am not a geek. I'm not in your class, anyway, that's for sure. Nowhere near your...

Steve: Is there a difference between geek and nerd?

Leo: Oh, yeah. We're not nerds. A nerd is, well, I mean, I don't know what the technical difference...

Steve: You mean, like, thick glasses, antisocial person?

Leo: When you talk about Nerds On Site, I think they think they're geeks. So I don't know, you know, if we went to Wikipedia we might find a technical difference. But in my mind, I'll tell you what a difference is between a nerd and a geek. A nerd is like a Stars Wars fan, the Harry Potter fans who lined up. Those were nerds.

Steve: And that includes people who, like, have Captain Kirk costumes.

Leo: Yeah. And many of them are geeks, as well. But not all geeks are nerds.

Steve: Oh, so we have a subset-superset situation here.

Leo: Yeah. And geeks, I always think of geeks as more technical, technologically focused. So nerds are fans, sci-fi fans, so forth. But that's just in my head. I don't think there's any - a geek's a guy who bites the head off chickens. It has nothing to do with technology at all. So I don't really know what the...

Steve: Okay.

Leo: No, that's the technical derivation of that. You know that.

Steve: It is?

Leo: Yeah.

Steve: Geek means something - no, I never knew that.

Leo: Those are - in carnie talk. A geek is a kind of carnie. The one in particular that bites head off chickens. Now, let me go to the definitive geek resource. According to Merriam-Webster, by the way, geek is, one, a carnival performer often billed as a wildman whose act usually includes biting the head off a live chicken, bat, or snake; two, a person often of an intellectual bent who is disliked; three, an enthusiast or expert, especially in technological field or activity.

Steve: Oh, good. So it took us three down...

Leo: We're three down.

Steve: It took till the third one to get to us.

Leo: And what a negative. But until we took it back. Right?

Steve: Right.

Leo: And I think that that's the thing, is we've taken it back and made it something positive. But I think it was for a long time, it's, ugh, a geek. Now, I don't know - I have to really see if they have - let's see. See also nerd. A stereotypical, archetypal, and frequently used informally as a derogatory designation, refers to someone who passionately pursues intellectual or esoteric knowledge or pastimes rather than engaging in social life. So, you see, there is a difference.

Steve: Yes, there absolutely is. And you're right, it is the sort of over-the-top fanatical fan person certainly fits in that, yeah.

Leo: A nerd is often excluded from physical activity and is also considered a loner, or often considered a loner by peers. Dr. Seuss invented the word "nerd," did you know that?

Steve: It's a perfect Seuss word. When you think about it, just that's beautiful.

Leo: In "If I Ran the Zoo," the narrator, Gerald McGrew, claims he would collect "a nerkle, a nerd, and a seersucker, too." So there you go.

Steve: I confess to really being enamored of Dr. Seuss when I was that age.

Leo: Me, too. And that makes us nerds.

Steve: Those wacky machines. I just loved those bizarre Seuss machines.

Leo: Oh, yeah, absolutely.

Steve: Very neat.

Leo: So a little more than we ever cared to know about nerds versus geeks. So do you have any errenda or adata - errata or addendum?

Steve: Before I get into specific Mailbag issues, because this is our - with our modified formula, this episode has survived as our Mailbag episode. First of all, a ton of this is about CAPTCHAs, that is, about our prior week's Episode 101, because the response was just fantastic; but not only because of the fun stuff we had talking about CAPTCHAs, but also my own personal discovery - in many cases, I don't know, I guess a few people knew about it among our listeners, but of that PayPal security key. I got a ton of responses from people who noticed that during our recording, Leo, we couldn't find the location of the key. And I actually think...

Leo: It was on your front page, but it wasn't on mine. That was the problem.

Steve: Right. And so on the show notes, my show notes of 101, and I moved it also into this week's show notes, up at the very top of the page is a link directly there. Or it turns out it's just paypal.com/securitykey.

Leo: Well, that's easy. That'll do it.

Steve: Yes. That will take you directly to that page. And so I wanted to make sure people knew where it was because there were a lot of people who - in fact, some thought that maybe we had slashdotted them, which is of course the industry term for drawing so much attention that they ran out of keys, because many people reported - actually I think it was only our Canadian listeners reported that PayPal was saying that the key was not currently available, I think was the exact language. And so they thought, well, what, did they run out after Steve and Leo talked about the PayPal security key? But I believe it's just a Canadian exclusion for reasons that are not immediately clear, although I do have some Mailbag comments about that. So I wanted to clarify that. Also I had one really fun little SpinRite story, but it's so horrendous in one particular way that I felt I had to compensate with a second little quickie. So...

Leo: One happy, one sad.

Steve: You'll see what I mean. Well, they're both good news; but, well, anyway. So Michael Cann in Melbourne, Australia, and I put in here in parentheses "has plenty of patience," which I added. He says, I run a small business in Australia fixing computers called The Computer Surgeons, and recently we had a customer who worked from home as an accountant who kept all his clients' bookkeeping records on his PC. And of course we already know where this is headed. His PC as at least seven years old, and his hard drive had decided to cease working. He also had no backup from within the last six months. So I quickly hooked up the hard drive to another PC, whipped out my copy of SpinRite, and hoped for the best. Ha. He writes...

Leo: Why do you laugh?

Steve: Well, it was a long haul, but good things come to those who wait. Three months and six days later I was able to recover all of his clients' files, and some files that he didn't even know were there. He now is recommending me to everyone he knows. He says, thanks, Steve. You

and SpinRite made my customer's day. It has been one of the best investments I have made. Regards, Mick the Computer Surgeon. So I thought, okay, three months, that's a little extreme. But, you know, the guy apparently, I mean, who knows what happened to his hard drive. But it must have really been in serious shape. But on balance, Jeff Harrison in Kentucky wrote, I recently purchased SpinRite based on listening to it being discussed so much on the podcast. I support our office and mobile users in my job and recently had one of our laptop users have their drive completely fail. Of course they did not have any backup of their data, even though we had provided instructions and even USB drives to help them do it. I decided this would be a good test for my new purchase, since I haven't needed it yet. It ran for about 1.5 hours.

Leo: That's not bad.

Steve: Exactly, and was able to recover all but one of the files. And even then I was able to get the backup file that that application creates. So they only lost about three days' worth of data in this one particular file, much better than losing everything. I was happy to know that SpinRite works as advertised, and the user was happy to get their data back. I enjoy the podcast and look forward to it each week. Keep up the good work.

Leo: Isn't that nice. Now, where was the horrific story?

Steve: No, it was the first one. The first one ran - this thing cranked for three months and six days.

Leo: Oh, I missed that part. Three months?

Steve: Three months it took.

Leo: Have you ever heard of it going that long? I mean, the patience that person had.

Steve: Yeah, well, and it recovered the drive, and he got everything back. So, as I said, he must have done something horrendous to the drive because SpinRite just worked and worked and worked.

Leo: I must have - my mind mustn't have accepted the three months.

Steve: It couldn't have been three months.

Leo: I must have - I heard three days. You said three months, six days. That's unbelievable. What, he put it somewhere and just ignored it for three months? Wouldn't you have given up after a few weeks?

Steve: Well, I guess he must - well, you know, he's a computer guy. He runs this Computer Surgeons operation. And he said he took the drive and stuck it on a PC. So he has boxes around. And probably he was curious, too, to see what would happen. And so three months later he calls the guy up and says, hey, I got all your files back, and some you didn't even know you had.

Leo: Unbelievable. So you knew that it could run that long? Did you know that?

Steve: Oh, yeah, it'll run until it's done. I mean...

Leo: What's the longest you've ever heard?

Steve: That's pretty much up there.

Leo: Got to be it. I can't believe it. So what's it doing for so long?

Steve: When SpinRite hits a troubled sector, as I mentioned in last week's podcast, it will sit there and do everything it possibly can to recover the sector. And that may take as many as - it'll try up to 2,000 times in the so-called DynaStat mode, the Dynamic Statistics mode that SpinRite switches into. And the specification states that after a failed read it is necessary to reset the whole hard drive subsystem.

Leo: Ah, okay, that could take a while.

Steve: Oh, it does. And so it's one of the things that's really frustrating is that you really have to do a full reset in order to know that the next read could succeed. I've been so tempted not to do that reset. But then I'm not sure that the drive would actually fully recover from the prior failure, so maybe I would never really be able to catch the sector. And my feeling is that I've got to follow the spec in this case. So actually it's not reading, like, boom boom boom boom boom boom boom boom, 2,000 times. It's reading, and it's going through a complete upheaval reset before I'm really able to conscientiously try again.

So it does, I mean, it can run slowly on a drive which is really in trouble. Some people have asked is there a way to speed that up. In fact I did read a piece of email since I mentioned this last week who said, boy, you know, I don't want to wait for 2,000 reads on a drive that is heavily damaged. Is there a way to speed SpinRite up to get it past, like, a really bad part like that? And you could do a couple things. You can interrupt it at any time and then notice what percentage of the drive you've completed - and that's accurate, by the way, to four significant digits - and then move SpinRite manually past that spot. Or, if you have something where you have an editable medium, meaning a floppy drive or a USB dongle that you're booting, SpinRite does accept a command line option. You say SpinRite space DynaStat space and then the percentage. The normal default percentage is 100, that is, you're running DynaStat at 100 percent. But you could set it to 10, and it would only do 200 reads; or you could set it to 1, and it would only do 20 read attempts.

Leo: Oh, interesting. Oh, okay.

Steve: So you are able to sort of scale that up and down, if you really want to.

Leo: Three months. That's kind of unbelievable.

Steve: Patience.

Leo: And one hour, that's a lot better. But it is usually somewhere in between those two times.

Steve: Yeah, it's normally a few hours.

Leo: Yeah. And I've run it overnight many times.

Steve: Yeah.

Leo: That's fine.

Steve: And that's pretty much typical.

Leo: Yeah. Well, as drives get bigger, right.

Steve: So get a load of this. Bob, whose last name I have, but I didn't know that he'd want me to use it, so we're just calling him Bob, is in San Jose, and he works for PayPal. He says: Thanks for the recent plug for the PayPal Security Key. I'm the product manager for the program.

Leo: Oh, that's great.

Steve: I'll be happy to answer any follow-up questions you may have. Response to the program has been very positive. It recently came out of beta in June. Although I think mine - I think when I got mine a couple weeks ago it still, I mean, I think it was in July, or maybe it was at the very end of June, and I think it still said it was in beta. But anyway, he says it's out of beta, and we're planning marketing campaigns to let more users know about the program. Which is a good thing because, you know, you were unable to find it, Leo, even when I told you where it was. And in fact many people went on a hunt. I mean, I think our mention of this certainly gave PayPal a boost because it's such a cool thing, and it's $5 to have this really neat security dongle. But you really have to dig around. And so I want to acknowledge all the listeners we have who sent in detailed navigation instructions for how to find this page, which apparently you can also go directly to, just by doing paypal.com/securitykey.

I wrote back to Bob and said, hey, the response has been fantastic from our own Security Now! listeners; and I've invited him to jump onto the show, maybe next week, to spend 5, 10, 15 minutes with us talking about this and answering some further questions.

Leo: Oh, that'd be great. I haven't gotten mine yet, but I'm looking forward to using it. And it's a great way, for those who didn't hear the show, you can now get one of those security dongles that generates new passkeys every few seconds, or few minutes, I'm not sure how often it is.

Steve: Every 30 seconds, I believe.

Leo: 30 seconds. And you add that to your PayPal password to give you double factor authentication. And really, I mean, that is a great idea. No one can hack your PayPal account at that point.

Steve: Yeah. I just, as a matter of fact, well, they're unable to hack it from a position of...

Leo: From logging in. They can't hack your password, let's put it that way.

Steve: Exactly. I mean, even if you had a bad password, your last name or something really, really obvious, like "password," your password could be "password." But the addition of six digits to the end of it, which is the way you log in - oh, and by the way, I forgot that the other day, and I logged in just with my normal password. And, well, what it did was it took me to a separate screen because it knew that I had now authorized myself to use and require the PayPal security key. And so I got an intercept screen saying please type in the six digits currently showing on your security dongle. So it's like, oh, good, if I don't - you can do it all in one phase by adding those to the end of your password. But if you forget, then it'll just say what's your current six digits. And of course if a bad guy ran across that, he'd think, oh, well, I'd better go somewhere else because I'm not going to guess some six-digit number that's changing every 30 seconds.

Leo: Yeah, I'm looking forward to getting it. I worry about what happens if I lose it or I don't have it with me, et cetera, et cetera. But better to have that security.

Steve: It's funny, too, Leo, because that's exactly what I was feeling, too, when I authenticated myself and committed to always having it. Because first it was sort of a cool thing to have. And then I thought, okay, well, what's the point of having it unless I lock it into my PayPal account, which you're able to do separately from receiving it. And then I thought, okay, but if I do this, then I just can't use PayPal randomly wherever I am. It's like, yes, Steve...

Leo: That's the point, Steve. I guess I'll probably not keep it on my keychain because that's too heavy. I already have, like, 83 things on my keychain, including some keys, actually.

Steve: Well, and we're going to have some great Mailbag comments about that, too, so...

Leo: All right, I won't say anything, then.

Steve: Okay. So Phil Aylesworth in Windsor, Ontario, Canada says, sorry about the email yesterday - that apparently he sent me - about the PayPal security key not being available. A Google search reveals that it is only available in the U.S., Germany, and Australia right now. Of course I said he's in Windsor, Ontario. He says, I'm in Canada. I guess other countries don't need the extra security. And then he's got a frowny face here.

Leo: It's probably, you know, this is encryption. There's just probably some export restriction, I would guess.

Steve: Yes. And hopefully Bob who's the product manager will know - I'm sure he'll know exactly why. And he says, it would have been nice if PayPal had told me why it was not available. And in fact that would have been nice for hundreds of people who wrote to us, Leo, saying what happened? It says it's not currently available. So, yeah. So I hope we'll get a definitive answer. I presume you're right. But if it's Germany and Australia, that seems - it seems strange that Canada would say no, or somebody would say no.

Leo: It does seem odd. I don't know. That is odd, yeah.

Steve: We'll get the whole scoop, and we'll let our listeners know. Jim Kramer, who's a listener, says I just wanted to let you know, I've also been - I just wanted to let you know. Okay, that's how he starts.

Leo: Period.

Steve: I've also been very interested - oh, oh. I've also been very interested in how the brain works and read Hawkins's book - Jeff Hawkins' book that we talked about, "On Intelligence," last week - as soon as it came out. I also bought the audio version. I agree, it's very well done. I've been actively looking for information about how the brain works and have found many good pieces of information. None, however, are as good as the information from Hawkins. I recommend you check out the following videos after reading the book. And then he has - he provided three links which I followed. And each is to a really interesting presentation, very different from each other, and about an hour long each.

So obviously I can't, I mean, these are links from hell, I mean, these are not links that I can even attempt to verbalize. So for anyone who's interested, they are on my episode notes page for this episode, 102, are the three links from Jim Kramer. One is on the Numenta site itself. I think the other two are Google videos. So anyone should be able to watch them. And they're definitely interesting. They'll make much more sense after you've got the introduction that Jeff provides in the book. But it is, you know, for somebody who's not interested in reading a book, or if you're curious about more of the content or what his whole HTM, the Hierarchical Temporal Memory architecture is, the videos will be a quick way to dip in. And then you could decide, hey, I really want to start at the beginning and then read and understand this stuff.

Leo: Yeah, it's great. When I talked to Donna Dubinsky, who's his partner at Numenta and my Yale classmate, about it, she mentioned there's a good white paper also on the Numenta site about what they're up to, their specific implementation here. So that's also another place to look.

Steve: Oh, cool. I'll see if I can find that and link to it.

Leo: She said read that white paper before you interview Jeff. You'll have a very good idea of what we're up to.

Steve: So listener Peter Lilley in Sydney, Australia, he prefaced his note saying is it safe to go without AV if you "know what you're doing." And of course I have sort of suggested that a number of times over the last year and a half, Leo, coming up on two years here. He says, I wanted to share an anecdote from a few weeks back as it relates to something that's come up on Security Now! a few times. I've been working in enterprise software for some 15 years and consider myself pretty careful and conservative when it comes to security online. I'm the sort of

person who checks certificates, never opens attachments I wasn't expecting, et cetera, because I don't like inviting unknown people to come play on my computer.

So recently I was looking for information about a new component for my home PC online, using my wife's laptop. I visited the website of a large and reputable manufacturer, then clicked a link to get more info about a certain product. Okay, so that took him to - he went from this large, reputable manufacturer to a specific product's website. Immediately avast! alerted me to a virus on the laptop. I hadn't downloaded any file, followed any external link, or clicked yes on any dialogue. I simply viewed the page. At first I didn't think much of it and assumed the issue was with the PC and not the site. I simply invoked my usual remedy of rolling the PC back to a disk image that I knew was okay, ran a virus scan, and all was good. While all that was happening, I broke out my work laptop to continue my surfing. I visited the same site and immediately Symantec corporate edition reported the same virus, now on my work machine. I don't remember exactly which virus it was, but my investigation into the virus indicated that it was some unpleasant file infection. The infected file was in my Internet cache in both cases, meaning the actual file on the web server was infected, and I was downloading that file simply by looking at the page.

A moment of panic ensued. I do not run any AV at all on my primary machine, as I, like you and Leo, believe my safe practices should be the best protection. It seemed likely that I might have visited that manufacturer's website from that machine at some point, so I ran a scan via the network, and, yup, that machine had been infected, as well. Now, I have no idea how long that machine had been infected or how much time would have passed before I discovered it had I not happened to be using my wife's laptop that particular afternoon. I now run AV on all machines (by the way, I discovered NOD32, which is apparently written mostly in Assembly and feels very light) - and of course that's one of our favorites, Leo - as I no longer believe that simply being mindful and playing safe is enough. I guess the lesson here is even sticking to the reputable places on the web and being mindful of the dangers is quite - I think he missed a negative. He says, I guess the lesson here is that even sticking to the reputable places on the web and being mindful of the dangers is not quite enough.

> **Leo:** Well, of course, in order for something like that to happen you have to have a hole in your operating system; right?

Steve: Well, yes. What it probably means, given that...

> **Leo:** Well, of course if there were an infected image...

Steve: That's what I was going to say.

> **Leo:** Yeah, go ahead.

Steve: And you're right. It would be an image which is exploiting, and of course there have been image-based exploits before. I think there was a JPEG parsing error in Windows...

> **Leo:** And the problem is it's not just Windows. It was in the Windows - the Visual Studio library file. So it extends to many apps.

Steve: I think it was the GDI Plus file, if I remember. And you're right. So in that case just viewing that image, which of course any browser will do, I mean, most users certainly do surf

with images enabled, even if they've got Flash disabled and scripting disabled and everything else, generally you're going to be surfing with images. And so you're right. It would only be a problem if that was a known - if it was an unknown exploit that was - or unknown vulnerability that was being exploited, or if you had not patched your machine and then your browser displayed that. So, I mean, he makes a good point. And that's why I took the time to read his rather long note is, you know, going through his anecdotal report, here's an instance where all of his machines had a bad image on them. On the other hand, I would imagine that, if you and I were to scan our machines, and I don't often enough, maybe we'd find something, you know, something...

Leo: Well, but there's a difference between a bad image in your cache and actually a virus infection. In other words, that image by itself isn't going to do anything. It needs to inject some software in there. And that's my question. He may have found that image; but if it infected his system, there'd be a trojan there, as well. The image by itself is not the problem.

Steve: But displaying the image would have been the vector. And so presumably when he went to this manufacturer's website, he...

Leo: No, I understand that. But what he's found, according to what he describes, what he's found is a JPEG image in his cache. That by itself is harmless. That by itself is harmless.

Steve: Yes, given that his system is patched, and the image was not displayed.

Leo: Right. Well, even if it was displayed, if the hole was patched, which it may or may not have been, it would be harmless. And what I'm saying is, if his antivirus only found that image, there's two possibilities. One, he didn't get infected...

Steve: I see. I see, right, because...

Leo: Or the other, he did get infected, and it didn't detect it.

Steve: Yes, I exactly see what you mean. So it wasn't also finding a trojan that the image was the entrance vector for.

Leo: And that's kind of one of the reasons that I am so emphatic on emphasizing behavior as opposed to antiviruses. Because the antiviruses may have missed the trojan, frankly.

Steve: And behavior always protects you. As long as you don't misbehave.

Leo: Right. Good behavior protects. You know, this has happened to Tom's Hardware site, which is a very reputable site. This has happened on MySpace, partly because these sites accept ads unverified from ad services.

Steve: Oh, very good point.

Leo: That's the vector on these.

Steve: Anytime, yes, anytime your server has links to offsite images, you're trusting that the image you're sucking in is going to be okay.

Leo: And so that's what happened to MySpace, and they were using a service that wasn't, you know, that allowed anybody to buy an ad. The advertiser provided the image, and of course it was infected. They estimate in that case that a million people got infected. And the Tom's Hardware, which is more recent, hundreds of thousands, they guess, because it was there a day or so. So, yeah, that just points out that you can even go to a reliable, a presumably reliable site and have this happen to you. I don't know what the right answer is, frankly.

Steve: And it's interesting, too, because the nature of the way this is being done, that is, the web page you're visiting never sees that image. The server never sees it. The page contains a reference to the advertiser supplier. So, for example, it's not possible for Tom's Hardware to somehow proactively take responsibility. In order to do that, his server would have to be accessing...

Leo: Serving the image, yeah.

Steve: Exactly. His server would have to be serving the image and doing a virus scan of the image itself prior to offering it, which is typically not the way this is done. Instead, his pages simply have links to that third-party server, and the user's browser goes and does the fetch of the image. So it's really a difficult thing for the hosting website to take responsibility for the image content, even if it really wanted to.

Leo: And that's why this JPEG hole is such a significant hole, because you can patch Windows and still be vulnerable. And it's hard to know what applications you're using have used that library with the flaw in it. So it's just a mess. It's just a mess. I don't know what the right answer is there because behavior may not protect you, and an antivirus may or may not protect you. I certainly don't say don't have an antivirus. What I say is, don't consider it your first line of defense. But it's a great idea to scan periodically, absolutely.

Steve: Yes, yes. We have a listener, Nils Andersen, who comments that in our last episode, Security Now! 101, we mentioned the PayPal version of the RSA SecurID. He says, I have a SecurID from E*TRADE, and it seems to me one SecurID should be usable on multiple sites. I ordered the PayPal key, but I can envision a future where I'll have a pocketful of dongles - there's an interesting title for a song.

Leo: [Singing] I've got a pocketful of dongles.

Steve: A pocketful of dongles, and have to hunt for the right one.

Leo: Now, he's a geek.

Steve: Yup, that's a geek. He says, got any information on sharing one dongle between sites? And that would be a great question if we can get the PayPal product manager on because several people mention this. It's like, hey, you know, yeah, I'd love to have a dongle; but I'd only like to have one, thank you very much.

Leo: But wouldn't that - that would compromise your security because it would be a shared password among multiple vendors; right?

Steve: Yes. Well, in fact this really harkens back to our recently discussed OpenID. What you'd like to have is everybody using a common repository, an OpenID, and then you use your single dongle with OpenID to authenticate yourself to everybody else.

Leo: Yeah, I like that.

Steve: So Bill Holton says - his subject line was "I'm still human." And he says, I just listened to your podcast. Actually I really liked his little blurb here. He says, I just listened to your podcast about CAPTCHA. And it occurs to me there's a bit of confusion when people refer to CAPTCHA as a Turing Test. My understanding is that a Turing Test puts a human judge in one place. And he attempts to see if the judge can tell the difference between a computer in one room and a human in a different room. CAPTCHA seems to turn this on its head and puts the computer as the judge and asks it if it can tell the difference between a human and another computer. If we had the resources to put humans back into those rooms, I don't think authentication would be a problem. But so long as there's the possibility that my computer is smarter than your computer, which I love that phrasing, he says there's always going to be some way my smarter computer can trick your less smart computer into believing it's human. Or has this all just been some computer-generated response, he says, meaning to say he's still human.

Leo: Right, right. So it isn't technically a Turing Test; he's right.

Steve: Yeah, really I thought that was kind of clever, that he's correct in saying that we're replacing the human judge with a computer judge. And of course that's the CAPTCHA server which is trying to make the decision between human and computer. And basically you just need, you know, if you have a smarter computer, which again is what we're talking about when we talk about all this work being done to crack the CAPTCHA, that's exactly the case. So I thought that was sort of a neat way to look at that.

Now, we've got a long posting, but I thought an important one, from Darrell Shandrow, who calls himself an "accessibility evangelist." And it's actually, Leo, somebody you've spoken with, as you'll see. He says, thanks for your Security Now! Episode 101 discussing CAPTCHA and multifactor authentication. I appreciate your talking about the needs of people with disabilities, specifically those of us who are blind or visually impaired. CAPTCHAs and multifactor authentication schemes that provide their output in only a visual format represent a clear and present danger to the blind, deaf-blind, and visually impaired. Each time a CAPTCHA or multifactor authentication system fails to accommodate our needs, it results in our inability to participate. At a minimum, this means a blind person can't sign up for an account on a website. On the other hand, it sometimes means we may be unable to make a purchase or even access the money in our own checking accounts.

Back in the '60s here in the United States we decided it was wrong to segregate African Americans from the rest of the population. For more than 40 years it's been illegal to deny service to African Americans in restaurants, schools, and other public accommodations based

solely on skin color. Similar protections are now in place to prevent discrimination against gender, race, religious preference, sexual orientation, et cetera. We even have the ADA and other laws to protect those of us with disabilities, though their effectiveness is a controversial issue for quite another forum. He says, many of us feel strongly that the way in which visual-only CAPTCHAs and multifactor authentication systems discriminate against us when no alternatives are provided to reasonably accommodate our needs for access is tantamount to the same type of segregation experienced in the past by African Americans. Since visual-only CAPTCHA presents a clear and present danger to the blind and visually impaired, and since it is often used to protect resources we need or want to utilize, we are absolutely insistent that every CAPTCHA and multifactor authentication scheme reasonably accommodate our needs for accessibility.

It's interesting, I'm going to interrupt here for a second, Leo, because I hadn't considered the fact, but it's certainly true, that the PayPal dongles and the SecurIDs that prevent a visual-only token are inherently discriminatory in that sense. I mean, there isn't - they don't have a little audible speaker on the back of them, for example, that will speak out what the code is they're currently showing.

Leo: Yeah. I think it's really important to be sensitive to this. And I think what the ADA requires in many cases is at least some form of access. It may not be the same one. So, for instance, PayPal is not forcing you to use the dongle, so they're not discriminating against people who can't see.

Steve: Exactly.

Leo: But I can see that perhaps, as an example, there may be some sites that require this visual dongle. And, you know, the CAPTCHA that I use has visual and audio, but he brings up the deaf-blind, or deaf-blind people. And I don't know what the answer is to that. I'm baffled at that point, I don't know what...

Steve: I was thinking about it also last week. And it seemed to me that, as long as you have some accessible fall back, that is, for example, if you could use neither the CAPTCHA nor the audio version, then allow them to do an email loop or some less technical solution that has inherently lower bandwidth, but where at least they're going to be able to do what they want. If, for example, if GRC's ecommerce system were protected by any CAPTCHAs, which it's not at the moment because it doesn't need it, it's got all the ecommerce authentication there, I would certainly not want to lose sales to people who were being stopped by some sort of CAPTCHA system. So I really can understand.

He says, at this point the state-of-the-art method of providing reasonable accommodations to CAPTCHA is, as you two - that is, the two of us - mentioned on the show, an audio CAPTCHA. Over the past year there's been an explosion of commercial and free products and services offering audio as well as visual CAPTCHA. And some manufacturers of multifactor authentication schemes are now getting to the point they must become accessible. At this stage I believe it is inexcusable for there to exist any CAPTCHA without at least an audio equivalent attempt to reasonably accommodate the needs of the blind and visually impaired. And, I might parenthetically say, or some solution that would allow them to still use the site. Companies like AOL, Google, and Microsoft now provide this accommodation. And some of us in the blind community are working tirelessly to insist that others do likewise.

Aside from the privacy issue, which I don't buy, since sighted people can also use the audio CAPTCHA, and that's a point that I had made last week, the real problem with both audio and visual CAPTCHA and multifactor authentication is that it does not meet the needs of the deaf-blind. Ultimately we need precise laws and regulations requiring accessibility combined with

significantly more research and development to devise non-sensory schemes that can reliably tell computers and humans apart, while recognizing everyone's humanity and discriminating against no one. Then he says, Leo, in November of '05 you interviewed me live on TWiT at the Portable Media and Podcasting Expo...

Leo: I remember that.

Steve: Yup, to discuss accessibility in general and CAPTCHA in particular. You seemed to really understand the issue and get the reasons for the need to accommodate the blind and visually impaired. I believe my appearance on your show, along with your linking to Blind Access Journal, helped to further spread the good word about accessibility. Thank you for making that happen.

In January of 2006 I initiated a petition asking Google to make an audio equivalent of their visual word verification scheme available to reasonably accommodate the needs of the blind and visually impaired. It was completely rolled out to all Google services by May of '06. Earlier this month a blind man from Brazil started an online petition asking Yahoo! to make an audio version of their CAPTCHA available. While Yahoo! does provide a form one may fill out to receive a call back, this promise is almost never fulfilled by the company's personnel. And most requests for help made by blind users of Yahoo!'s services have gone completely unanswered. I am taking the lead in promoting this new petition and of course ultimately insisting that Yahoo! simply do the right thing by providing an audio CAPTCHA. The petition is available at http://blindwebaccess.com.

Steve and Leo, I would ask that you mention this initiative, place your signatures on this petition, utilize your vast influence in the technology industry to convince Yahoo! to do the right thing, and that you link to both blindwebaccess.com and blindaccessjournal.com to help us attain more petition signatures and further spread the good message of equal access to technology for everyone, regardless of visual acuity. I thank both of you for your time and anticipate your responses. Keep up the great show. Sincerely, Darrell Shandrow.

Leo: I think most of the time Yahoo! does not have a CAPTCHA. So I'm trying to think of where - I guess maybe it has a CAPTCHA sometimes? I'm not sure...

Steve: Probably on subscribing for an email account, to prevent you from getting...

Leo: Oh, maybe it does, automating that, yeah.

Steve: Yeah. In fact, I think we talked about that last week.

Leo: Once you have an account, it doesn't require it. But I see as signing up it would. In fact, let me just check that, out of curiosity. Yeah, it does. And it doesn't - let's see. More info. It doesn't seem to have a audio version, yeah. They really - that's surprising, frankly. I wish more people would just use the CMU reCAPTCHA, which has audio, and also has this additional feature, as you mentioned, of typing in books.

Steve: Well, yes. And in fact, remember, too, that the benefit of that is by having everyone using a centralized source, what it essentially means is that, if bots become good at this, and in fact it's one of the things that the servers are monitoring, the reCAPTCHA servers are monitoring the access patterns to detect whether it's being cracked. And the beauty is that

they'll be able to respond immediately, and everyone using their system immediately gets the distributed benefit of not only feeding information in about any hacking attacks, but getting any benefits of upgrades to the system as any are needed. So I will absolutely, if at some point I do something where I need to have that kind of protection, I will use reCAPTCHA and have some sort of automated second-level authentication for people who are able to use either.

Leo: What happens with SiteKeys? I mean, SiteKeys are very visual. Does that...

Steve: That's a good point.

Leo: All right. Anyway, thanks for writing. I think that's good points, and we all need to be aware of accessibility. And frankly, I fall down on this frequently. Our website is not nearly as accessible as I'd like.

Steve: Matthew Middleton is a listener who just signed up for his first PayPal account thanks to us. He says, hello, Steve and Leo, just wanted to let you know that after Security Now! 101 - that was sort of a fun numbering coincidence, Security Now! 101 - I am ready to take the plunge into online shopping. Up to this point in time I had never purchased anything online from a place that didn't take checks that I could send them because I have heard so many horror stories from people losing money through online purchases.

To give you some background on myself, I'm a 22-year-old software developer who spends a good deal of time listening to tech podcasts (most from the TWiT network). So I do have a good grasp on how online security works, or more appropriately, it's supposed to work, as very few sites really provide the security that is needed. So my fear of online shopping is based more on knowledge than ignorance. This, however, all changed when I heard that PayPal now offers security keys you can purchase. As soon as I listened to SN-101, I jumped on PayPal and set up my account, ordered the key, and am now waiting for it in order to make my first online purchase. I'd like to thank you and Leo for all the information that you provided on Security Now!. It has helped a lot. Not only do I know that PayPal offers security keys, but I also know why that is important.

Leo: That's neat. And, you know, I get a lot of email from people who say, I can't contribute to TWiT because I don't have a PayPal account, and I never will. And I suppose I should look into other payment systems. It's just so easy to use PayPal. And frankly, if you don't want to donate, or you can't donate because you're uncomfortable with PayPal, that's fine. I understand. Only about 2 or 3 percent of the listeners donate anyway. It's not going to - I don't expect or hope for, even, anywhere near a hundred percent participation. But I don't know, I've looked at other systems, and I can't find one that works as easily, so.

Steve: Yeah, yeah. A listener, Robert Gauld in Aberdeen in the U.K., says, like you guys, I have a lot of problems with the visual CAPTCHAs, to the extent that I take my browsing elsewhere if I'm presented with one. Take that, you nasty CAPTCHA. He says, what I'm wondering is why they don't just present the user with three pictures of things, for example, cat, dog, house, post office box, boy, girl, bird, dot dot dot and a selection of dropdown boxes to choose what each picture is showing.

Leo: That's a great idea because a computer would have a terrible time with that.

Steve: Well, except that the problem is, if the choices are limited, then the computer could be

programmed to recognize each one. And so it ends up being trivial, actually. If you're shown, you know, the same dog is showing all the time, or the same house, the same post office box or boy or girl, all you have to do is not even image recognition. You just do a CRC or a hash of the GIF or the JPG which is being repeatedly shown. A human goes through each of them one time matching up that this CRC or this hash is this answer to the question; and then, wham, you've got it cracked.

Leo: You have an evil mind.

Steve: Well, believe me, the hackers do, too, so...

Leo: Oh, I know, you need to. Recently, I wish I could remember, and I can't remember who it was, but I recently ran into a CAPTCHA that did an interesting twist on this. But I think you're right, this might have had the same problem. Instead of showing you a CAPTCHA, they showed you four images. And then below it had a key. Now, the images change. I've done it a couple of times, and so it's always different. But they had a key, you know, castle equals one, star equals two, and then you were to enter a number based on taking those images, figuring out the key, and entering the number. It took some time, but it was a little more legible than a CAPTCHA. And I presume they're changing the numbers randomly so that it wouldn't have this same issue, problem with yours.

Steve: And were the numbers in images also?

Leo: No.

Steve: Okay, see, the problem is then the bot could read the text and see what the associations were. And again, it would have it cracked, so...

Leo: You're right, never mind.

Steve: I mean, as we concluded last week, it is surprisingly hard. Surprisingly hard to tell a computer from a person these days.

Leo: Yeah, isn't it funny.

Steve: Yeah. Chris Ackerman is an IT manager in Plymouth, Minnesota, has an update and thoughts about AVG. He says, I use AVG 7.5 Network Edition as my corporate AV solution. With 300-plus users, the other antivirus (Symantec, McAfee, et cetera) have become absolute resource pigs, and the cost has become prohibitive.

Leo: That's true.

Steve: I switched from Symantec last year and find AVG to be much better, he says in all caps. You sounded kind of upset with AVG for returning a false positive on SecurAble.exe. AVG immediately removed it from the def file.

Leo: Oh, good.

Steve: I had SecurAble on my machine and was getting a positive hit for it. AVG was showing it as infected with the sheur.apy trojan. Anyway, AVG is no longer showing your program as a threat. I'm not sure we would have received such a quick response for removal from - and he says "crappy" here - Symantec or McAfee.

Leo: That might be true, too, you're right.

Steve: Then he says, go easy on AVG. They are the best thing going these days in the AV world. So if I sounded upset, I apologize. I certainly meant nothing against AVG because these false positives occur from time to time from everybody. I certainly do appreciate knowing - and believe me, Greg, my tech support guy, will really appreciate knowing - that AVG updated their patterns, and people aren't going to be worried that SecurAble's got something bad going on.

Leo: Now, you make sure you update your virus, your antivirus.

Steve: Yup. Oh, and we had another person, whose name I'm going to pronounce Poojan Wagh of Chicago, Illinois. He said, I heard you discuss on SN-101 that PayPal has security ID dongles available. I wanted to let you and your listeners know that E*TRADE has offered RSA SecurID to their banking customers for quite a while now.

Leo: Much better than a SiteKey. Let's all do this.

Steve: He says, I estimate a couple of years. Then he says, what would be great is if RSA/PayPal/E*TRADE would allow you to register a single dongle with multiple accounts.

Leo: See, that's the problem, because I don't want to have ten of these.

Steve: Exactly. And he says, I mean, who wants to have both a PayPal dongle and an E*TRADE dongle on their keychain?

Leo: A legitimate thing. But on the other hand, it compromises the security if it's the same number for multiple sites.

Steve: Now, the only thing you could do, and there are some RSA SecurID tokens with this, and that is, they're like a credit card with an LCD display, and they have a keypad on them. And the advantage there would be that you could do a challenge response, so that when you were wanting to authenticate yourself, you would receive from them something to type in. That would get mixed in cryptographically with what they know about your card and produce a result. And so that would help to back off on that problem somewhat.

Leo: Yeah. Interesting.

Steve: Let's see. We've got, oh, this was funny. A real quickie. Simon in Exeter in the U.K., his subject was "Funny Error." And he said, Steve was joking that they could clone you and get your fingerprint. But clones and identical twins have different fingerprints.

Leo: Oh, I didn't know that. You would think they'd have the same one.

Steve: I filed that under "good to know." When we get to the point where we're cloning people, you'll have different fingerprints.

Leo: So your fingerprint is not nature, it's nurture. Or something. Or a combination thereof.

Steve: It's certainly not a pattern of cuts that I received on my finger as a child. I don't know. But I guess, you know, Simon was so definitive, I'm going to take his word for it.

Leo: I think I'd heard that about, well, I know that twins don't have the same fingerprint, so that's where that would come from, because identical twins are genetically...

Steve: And we of course know that clones are, by definition.

Leo: Twins, they're twins. Very interesting.

Steve: Dan in Oregon has provided us with some feedback. He's an avid TOR user. We'll remember that TOR is an acronym that stands for The Onion Router, which is a very powerful anonymizing technology where your traffic bounces through a series of publicly available onion routers. And the technology is extremely neat and well implemented for preventing anyone from being able to backtrack those links in any feasible fashion. So he says, hello, Leo and Steve. I've been listening to you talk about IP spoofing on Security Now! and have been a user of TOR, The Onion Router, for several years. And my IP address when using TOR shows up as the IP of my exit point from the routed network. Which of course it would because that's basically his public IP, that is, the IP of that router. He says, with proper configuration you could choose to always use the same exit point and have a consistent IP that is not mine or even geographically close to me. Your choices of IP addresses is limited, of course, to TORified systems that have a policy to allow them as an exit point from the network. I have verified this on GRC.com, and you cannot detect my true IP address when I am TORified. So that's very cool.

Leo: Okay. Wow. All right.

Steve: Steve Hiner in Phoenix, Arizona still doesn't like biometrics. He says, in Episode 100 I think you missed the point on one of the questions. One of the questions was about the security of fingerprints and retina scans and whether or not we want something that permanent as a digital ID. You came to the conclusion that it was okay because they will only store a hash of the data, so our fingerprint or retina can't be reconstructed if a bad guy got to the data. I don't think that's what the listener was concerned about. I think his concern is that, if the bad guy got that close to the data, he could switch his hash code with mine, or duplicate his hash code into my records. This could have two very bad results. First, as far as the criminal database is concerned, I have become him and could get arrested for his crimes. As far as the

bank is concerned, he has full access to my accounts, since they will think the biometric information cannot be duplicated. It would be the ultimate identity theft. It's already tough enough to convince a bank that you didn't make a purchase, without them having proof that it was you because of more robust biometric data match. What is a bank or a police officer supposed to believe, that you faked your driver's license, or that you faked your iris? I think you'd have a tough time proving...

Leo: I faked my iris.

Steve: I faked my iris. I think you'd have a tough time proving that your iris has been hijacked.

Leo: I think you're right.

Steve: Okay. Well, first of all, what you would do, if it came to it, would be you would rescan your iris, which would then be rehashed, and you could then affirmatively prove that your hash was not the one in your file, and that someone had changed it. So in fact, in this example, it actually gives you proof of identity theft rather than having less strong proof. And again, the power is that this hash, it's a nonreversible lossy process. And you always keep your own iris, so you're always able to reaffirm what your hashed value is in any given situation. So anyway, I thought he had an interesting point, but we still are protected. And in fact, in those examples, we end up being able to more affirmatively demonstrate to the cops that somebody else went to the trouble of pretending to be us because, you know, they don't actually have our iris. We can always reassert ownership of our own iris.

Leo: Does your iris change over time?

Steve: I don't know. I hope not because then it would be a bad biometric.

Leo: Well, it might change a little. I know your fingerprint changes sometimes.

Steve: Oh, I got a kick out of this one. Brian Hogg of Kitchener, Ontario, Canada...

Leo: And a good friend. He made a puppet of me, you know.

Steve: Brian Hogg did?

Leo: Yeah.

Steve: Oh, well, you have - wait a minute. For what purpose? There's that problem with voodoo, Leo.

Leo: It's got my perfect iris. No, Brian is the creator of the incredible dotBoom podcast, the video podcast with puppets. And I'm...

Steve: There's a Leo puppet jumping around some video podcast?

Leo: Next time you're up in Vancouver, Brian sent it to me, I will show you.

Steve: Oh, cool.

Leo: Yeah, I'm in a podcast along with - there's a Kevin Rose and an Alex Albrecht puppet, and I think an Amber MacArthur puppet...

Steve: Oh, my goodness.

Leo: ...is due for their season finale.

Steve: I hope I stay off his radar.

Leo: We want a Gibson puppet. You're in trouble, Steve. No, you'll love it. You're just like a Muppet. It's very cute.

Steve: Okay. Anyway, he says, excellent show on CAPTCHAs. I was just leafing through my spam folder, and I noticed one about Cialis. We don't wonder why he chose to open that particular one.

Leo: I get them all the time.

Steve: But he says, it was just an email with product shot photos. I noticed that the image itself had all sorts of visual distortion on it. It looked like the image had been sprinkled by confetti. Would this be the spammers attempting to subvert detection?

Leo: Oh, interesting.

Steve: Isn't that cool? Basically perhaps by using the same method as CAPTCHAs. And I thought, yeah, of course. I mean, that makes - I don't know that. But I think his guess is exactly right, and it's very cool. So the spammers are doing image degradation because certainly antispam filters would lock onto the photo, a nondegraded photo, just like we were talking about before, and do a checksum of it and say, hey, any email containing an image that matches this checksum is absolutely spam. So these guys are obviously throwing some confetti noise in the image in order to prevent it from being captured. Or CAPTCHA'd. Which I thought was pretty cool.

Leo: No, they do all sorts of - if you want to know the cutting edges on this stuff, look at the spam. These guys, I mean, because they have a lot of incentive in keeping one step ahead of whatever. The filters.

Steve: Justin in San Antonio, Texas says, I think it would be great if you guys did a segment on digital signature/electronic signature technology. Going paperless and addressing the approval process for security requests is something that would be of great interest to myself and other information security administrators. Well, I wanted just to address the fact that we really did, Justin - we did justice, Justin, to electronic digital signatures back in our security series earlier on in Security Now!. So by all means go back and take a look at hashing and crypto stuff.

Leo: You might want to look, though, I mean, we might want to update it because there are - for instance, Adobe Acrobat now has a signature module in it for legal document signatures.

Steve: Oh, could mean, like, legally binding document signatures.

Leo: Well, it said so, and it's from Adobe, so I figure it's probably widely adopted. I don't know.

Steve: But I guess I mean cryptographically strong.

Leo: Well, I presume that you can't tell because of course Acrobat does all its encryption internally.

Steve: Right. For what it's worth, I was going to follow up and explain to Justin very, very quickly that the way this is done - uh-oh. That was somebody coming or going.

Leo: Somebody's calling.

Steve: Thought we'd lost you, Leo.

Leo: No, I'm here.

Steve: Because that's my Skype sound. The way this is done is that you would take the document, and you would make a cryptographic hash of it, like an SHA-1 or some other strong crypto hash. Then you use your private key to encrypt the hash. And that is a digital signature. And the idea then is anyone who wants to prove that the document is not changed, they acquire your public key, that is, the matching key to your private asymmetric key. They acquire your public key because only your public key can decrypt what your private key encrypted. So they decrypt the so-called signature and get the hash value. They then perform the matching hash function. And only if the document, this whatever it is, Adobe Acrobat or PDF or whatever electronic document, only if the hash exactly matches then do you know that it hasn't been changed since it was signed, and you also affirmatively know who signed it because only the person who signed it would have the matching public key that would successfully decrypt the hash. So that's how signatures work.

Leo: We should at some point look at what Adobe's doing because as far as I know this is new in 8. I hadn't seen it before, and it's clearly for using Adobe Acrobat to distribute

electronic documents where you certify the validity, and then you can sign and certify changes. Looks like either you can get a certificate from a third party, or you can create your own certificate, which is kind of interesting. You could certify the original document and then certify changes to the document. It actually has a signature, like a hand signature, but I guess it's attached probably to a digital signature, as well. It's interesting what they're doing. I mean, clearly they're trying to set a standard of some kind for commercial use of digital signatures.

Steve: Right, right. And it's certainly possible for people to create a so-called "self-signed" certificate, like your own certificate, if you don't want to get one from a certificate authority. The advantage of doing the acquisition of a certificate from an authority is then that you're having to prove to them that you are who you say you are, so they're representing that this is signed, not just by somebody who claimed to be whoever they are, but that the certificate authority is saying, yes, we verified through some offline process that this person really is who they are claiming to be. But it's certainly not - you don't need a certificate authority. And so that was what you were referring to, Leo, the idea that you're able to create, instantaneously create a certificate. You could certainly do that because lots of code is able to create a key pair, an asymmetric key pair, one which you would keep private and use for signing, the other which you would publish and use for verification.

Leo: Got time for a couple more, if you have a couple more to do.

Steve: Yeah. We got two more, as a matter of fact, that I had. We had actually 20. And so we're at - No. 19 is Will Morenz of Wheatfield, Indiana says, I just listened to Episode 100. And about the listener who asked about the security of allowing users to enter any email when asked for a new password because the users might have forgotten the password to the email they had used. Okay. What he's referring to was the question two episodes ago, remember, that somebody wrote in asking if we felt it was insecure - I think he was with a large educational, an academic environment, a university, and both students and faculty were forgetting their passwords, and then they were forgetting which email address of their many email addresses they used in order to perform the authentication loop. So the university had taken to allowing people to enter an email address to which the authentication would be sent, along with some additional questions. And the guy was asking do you feel that's insecure.

Anyway, so Will suggests, why don't they let the user verify multiple email accounts at a time, then give them a choice of those emails instead of using any. They would also need to give them a way to deauthorize email when the user no longer uses them for one reason or another. Of course, all of this would require that the user keep the email list up to date, but the people they're trying to cater to might not do this.

Anyway, so I thought it was an interesting idea. His notion was, instead of only having one email address which you register with, why not register all of them? Then when you need to, like you do I forgot my password, please send me an authentication to my email address, well, it would send them to all of them so you don't have the problem of having to remember which one you registered with. I thought, well, that's clever. And I don't really see that it significantly weakens the security. It could be a one-time process. As soon as any one of them is used, all the other ones become deauthenticated and cannot be used. So it's an interesting idea.

Leo: Yeah. Our last email.

Steve: Yeah. I end this on sort of an interesting sort of bizarre Catch-22. Eric Sarratt of Asheville, North Carolina shares this AT&T statement on NSA warrantless wiretapping. And this

is, like, formally posted. The AT&T statement on the NSA, issued in San Antonio, Texas on June 27th says: "At AT&T we vigorously protect our customers' privacy and only share information as specifically authorized by the law. The news media have carried reports alleging that AT&T is participating in an unlawful NSA terrorist surveillance program. Unfortunately, the law does not permit AT&T to respond to those allegations. The U.S. Department of Justice has stated that AT&T may neither confirm nor deny AT&T's participation in the alleged NSA program because doing so would cause 'exceptionally grave harm to national security' and would violate both civil and criminal statutes. Under these circumstances, AT&T is not able to respond to such allegations. What we can say is AT&T is fully committed to protecting our customers' privacy and would not provide customer information to any government agency except as specifically authorized under the law." Thank you very much.

Leo: Well, I'm glad we cleared that up.

Steve: Oh, yes. We might be spying on you, but we can't tell you whether we are or not because doing so would be bad, too. So Catch-22.

Leo: So I would just say assume they are.

Steve: I think probably, yeah.

Leo: From that response, I think that's the assumption; right?

Steve: I think probably, yes.

Leo: Not that that's a surprise, either. Steve, you did it again. I mean, this was a big, 20-question Mailbag, and a lot of interest...

Steve: Yeah, I just love our listeners. We've got smart people listening, and they're engaged and involved and have some interesting things to talk about.

Leo: Yeah, I think it's really good to give them that opportunity to get clarifications and so forth. So I'm glad we're doing that more often. Next week do you know what we're going to be doing, or will it be a surprise?

Steve: It's going to be a surprise as much to me as it is to you, Leo.

Leo: But we know we'll be here; we know we'll have a great show for you. Episode 103 next week. Thank you so much for joining us. Make sure you check out the fine sponsors of this show and give them your support because they give us their support, and they make Security Now! possible. And don't forget, Steve's site is GRC.com, and that's where you can get your copies of all of his free programs, SecurAble, Shoot The Messenger, DCOMbobulator, of course test your firewall with ShieldsUP! and LeakTest, and customize your shutdown with Wizmo. All sorts of great stuff. That's all for free, and then his bread and butter, the great SpinRite, the ultimate disk maintenance and recovery utility. Even if it takes three months, six days, SpinRite can do it.

Steve: Right. You use one of those old beige computers...

Leo: Put it aside, put it in the closet, let it go.

Steve: Exactly. The good news is, it's normally a few hours.

Leo: Yeah. That is definitely right at the end of the scale on that one. Also by the way at GRC.com, 16KB versions of this for the bandwidth impaired, and a great transcript thanks to our friend Elaine, who writes this all up for us. We thank you so much for joining us. We'll see you next time on Security Now!.