Listener Mailbag #2

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-106.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-106-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 106 for August 23, 2007: Mailbag #2.

Time to talk about security, and it's a listener mailbag episode. Steve Gibson is here from his secure lair, soon to be tented and fumigated secure lair, in Irvine, California.

Steve Gibson: Yes, indeed. I've got to tell you, Leo, when I'm going through the email we receive in order to pull questions and actually comments, listener comments for the mailbag, it gives me such a great feeling because we get so many people who are saying that this podcast matters to them so much. I mean, I had one guy who just said, I just wait for Thursdays. I look forward to Thursdays.

Leo: That's so neat. Wow, I love that. Well, and that's why it's nice that you're so consistent with it because nobody is ever left behind. No podcast left behind. That's our philosophy here.

Steve: Yes, come rain or sleet, snow or termite fumigations, there will be a podcast.

Leo: Now, are they doing poisons, or are you going to have, like, orange peel injected into your home?

Steve: No, it turns out there was a huge amount of anti-fumigation sentiment among the homeowners. People just didn't want the inconvenience of being pushed out of their home for a couple days. And there are, it turns out, a whole bunch of spot treatment type things, one of which you mentioned is this orange oil. And it turns out that spot treatments can function -

unfortunately I'm way more of an expert on this now than I needed to be. Spot treatments can function when you know exactly where the problem is, and if it's a localized problem. But you have to be able - first of all, you have to know where the problem is, and you have to have access to it. There's also actually an effective approach is heat treatment. You can actually just heat the little buggers to a point...

Leo: Right, cook 'em.

Steve: ...where they, exactly, they get cooked. And speaking of that, there's microwaves. There's electrification. You can...

Leo: I've seen, yeah, there's a lot of different things.

Steve: ...shock them. But the problem is, nothing really deals with whole structure problems better than fumigation. And frankly, we've got spiders coming out of the woodwork, literally, also, and those little mud wasp nest little things that...

Leo: Oh, yeah, you know, it's - yeah, don't mess with it.

Steve: It's just, you know, it's a wild life over here. So I'm really looking forward to, like, the day after I can come back in, I'm going to knock down all those little mud huts that the wasps have created because I know that they will be empty and/or deceased, and they're not going to come out and get me for knocking their little igloos down, so...

Leo: They won't be mad.

Steve: Anyway, yeah, it's never a dull moment. So as a consequence you and I are doing two podcasts today, since next week I will be away from my machines. Actually I'll have a laptop at Starbucks, so I'll be hooked into the world; but, yeah.

Leo: You're going to spend the night at Starbucks, as well, or just...

Steve: Actually I was joking with a friend who was saying, where are you going to be staying? I said, oh, I'm going to stay at Starbucks.

Leo: Just keep those quinti venti lattes coming.

Steve: Exactly.

Leo: Let's see. Do you want to do - I know we don't have any errata from last week.

Steve: We don't. Although I did get a nice note that I wanted to share with people, sort of a reminder of an unusual application for SpinRite. This was actually the result of a posting on our

newsgroup server. When I was up in Canada with Mark Thompson a couple weeks ago, one of the things that he brought up was he said, you know, Steve, you really ought to consider affiliate marketing for your stuff. And it's not something that I had thought about. But I thought, well, let's discuss it in the newsgroups because, I mean, the GRC newsgroups are just, I mean, I will again commend our listeners to think about it as a - if they're interested in security and technology and this kind of stuff, it is a traditional news server, a so-called NNTP news server. But anybody with Outlook, Outlook Express, what's the - is it Thunderbird, I guess, is the communications tool like from the open source folks, you know, these are all very good, workable news readers. I use Gravity, and just because I have for years, and it's powerful and does what I need.

But anyway, the point is we've got a fantastic bunch of newsgroups and, mostly, people. Of course it's, you know, the people that make the newsgroups. And so I said, hey, guys, this affiliate idea, the idea of giving essentially a commission to people who forward people to our site, who end up purchasing SpinRite or other stuff in the future, that's sort of the concept, you know, what do you guys think about it? Well, what ensued was a long discussion that ended up putting me off of the idea, just because to do it really right and prevent there from being a problem of, like, flaky affiliates, or spamming affiliates who would become an affiliate and then spam in order to, again, in a shotgun fashion, sort of get people to go to GRC, I certainly don't want any affiliation - no pun intended - with such people. So...

Leo: And that often happens. I have to say I've seen, you know, a lot of antivirus companies use affiliates. And it tends - it's hard to control them.

Steve: Yeah. And that's just not my thing. I don't want to, I mean, I love the fact that I've kept my life and my operations of my little company as simple as I have. And, you know, just adding some wildcard that has a strong possibility for failing seems like a bad idea. Anyway, Skip was responding in this thread and actually quoted me saying, "My feeling has always been that SpinRite was too narrow an appeal for shotgun marketing to work well enough." And he responded, "Yes, always purchased in time of need." He said, "Saved my hard drive when I bought SpinRite in distress, and two other family drives a year later." He said, "Now for the testimonial. My father bought SpinRite preemptively," he put in quotes, "because of my experience." And he says, parens, "(It didn't hurt that he was already a Steve Gibson fan for years, for reasons I am not sure of.)"

Leo: I have no idea why.

Steve: We don't know why, but he seemed to like you. "Did not use it much, if at all." And then Skip says in parens, "(He and I are like this. Buy a good product on principle if we are likely to need it in the future. In this case, he has never used SpinRite to recover lost data or fix a problematic hard drive.)" So then he says, "Then his TiVo failed. Random skips and jumps in recorded programs. From Steve's Security Now! podcasts, I suggested that my father dismount the drive from his TiVo box and run SpinRite on it. Voila. One VERY," in all caps, "happy father who did not lose a couple of programs he didn't want to go without." And he said, parens, "(And they are not soaps. They're science programs.) And now a rock solid, fully functioning TiVo. Without the Security Now! podcast 'advertisements' about working even with TiVo, I would never have thought of suggesting SpinRite in this situation."

So that was Skip's note. And I just wanted to remind people of that. The fact is that, you know, essentially SpinRite will run on any drive anywhere, and even in the increasingly popular DVRs that can get hot, that do tend to use their drives extensively. And, you know, I've gotten lots of email from people who said, hey, you know, SpinRite fixed my DVR. I didn't know it would, but I'm glad. So I just want to remind our listeners that that's the case, in case people haven't heard me mention that before.

Leo: It's operating system and file system independent. It doesn't operate at that level.

Steve: Right.

Leo: Way below that. And so, yeah, because people have used it on iPods, use it on a Linux box, doesn't matter.

Steve: Yeah, in fact, in reading through email this morning to prepare the set of - I don't want to call them questions. Questions is what we tend to call them. But mailbag are more sort of commentary stuff, you know, interesting things that our users are feeding back to us about their discoveries or their solutions or whatever. But one of those was a guy who discovered that SpinRite would run in a properly configured VMware box on his Linux machine. He was using Linux, and he had VMware running on it, and there's a mode in VMware where you can give that virtual machine direct physical access to the drive, which is what SpinRite needs. Now, this has raised a question that I haven't answered, is would VMware running on a Mac so configured also allow you to run SpinRite on a Mac because the...

Leo: Without booting out of it.

Steve: Well, the problem is the Mac is EFI based. The Intel Macs use another generation of the BIOS from what SpinRite was born and bred on, the B-I-O-S, the basic I/O system, input/output system. And SpinRite is still dependent on some of the BIOS functions which are not present in the EFI. So you can't boot SpinRite on an Intel-based Mac directly. And what we tell people is, well, I mean, if you're - well, of course it means that it's very inconvenient to run it just occasionally to prevent, in a preventive maintenance fashion, to prevent there from being problems.

Leo: You'd have to pull the drive out.

Steve: Right. And people do, and it fixes their Macs that way. But it's, you know, it's a pain in the Mac, so...

Leo: Right. I don't know. We'll have to try it. This new VMware, I've been playing with it on the Mac, and it's pretty impressive.

Steve: Version 6?

Leo: Fusion, they call it. It's the Mac version. And it's only $80, which is nice because the big boy VMware is very expensive.

Steve: And that's different, obviously, than Parallels because I know that Parallels has this new feature where you can run Windows, like, windowed right there alongside your Mac application.

Leo: And VMware does that, too. They have a different name for it. But it's the same thing.

And I would say, feature for feature, VMware is pretty much identical to Parallels. The only thing, of course, VMware adds is those appliances, that you could run the VMware appliances, which is kind of neat.

Steve: And actually we're going to have a mention of that in our mailbag.

Leo: Well, let's get to the mailbag. This is our second mailbag episode, and Steve's asked me to read the questions after the first one. So I'll be your voice.

Steve: You're the reader, Leo. You do a great job with that.

Leo: It's my profession. So Mike Gunn starts us off. He listens in San Francisco. And he says irises do change. We were talking about irises as a biometric tool. And he says, the last time I went to the optometrist with my kids, he told me that they suggest taking a picture of the iris. As you age, things like diabetes and the like changes your iris and how it looks, and they can even see signs of disease by comparing the original picture, the baseline picture, with a new picture. And he mentions Robert Heron, who came back, I don't know, did he have a detached retina? He had to have some sort of eye surgery. So that would have changed his iris, I guess, as well. He also says, you might ask the optometrist for a copy of your iris for an extra-special desktop picture. Irises are pretty. It would actually be beautiful, wouldn't it.

Steve: Yeah, in fact there was a - I was looking at one the other day, coincidentally. The most recent issue of Scientific American has an article about how the movement, the twitchy movement of our eyes which actually Jeff Hawkins talks about in "On Intelligence," and how it's necessary that images be in motion against our retina, and our eye is constantly twitching in order to create a delta, essentially, a changing image on our retina, which is what our brain needs in order to process images. Anyway, there this one photo of just a spectacularly, and I guess it's unretouched, but it's a spectacularly symmetrical-looking iris. I know that when I stare at mine, as I do from time to time because I'm a hard contact lens wearer still, you know, my iris does have some character to it. It's, you know, it's got some wigs and wags. And, you know, I could see how mine may not look like anybody else's. But this one in Scientific American was just, like, just beautifully symmetric and clean-looking and different than mine. Maybe it was a young iris, and mine's getting old.

Leo: And we should point out that your fingerprint changes also. But I think it's if they're looking at basic fundamentals, then those don't change significantly. I wouldn't - I don't think they expect it to be identical any more than they expect...

Steve: Right.

Leo: Martin Yeomans of Memphis, Tennessee has, speaking of Jeff Hawkins, an interesting question. He says he's an occupational therapist and a member of Mensa. Big brain-type guy. He had some interesting thoughts after reading "On Intelligence" by Jeff Hawkins. He says he heard an article on NPR a couple of years ago about research at Dartmouth relating to the auditory cortex. He actually gives us a link to the story. It's still up on the NPR.org site.

[http://www.npr.org/templates/story/story.php?storyId=4533543]

But it's interesting, what they would do is they would play music while monitoring the activity in the auditory cortex, the part of your brain that's hearing the music. When the music stops, so would the activity. And except if you knew the song. If you knew the song, your brain would continue along as if it were filling in the gaps. Which is, I think, fascinating. So he suggests this might be useful in national security. Get this.

Steve: Uh-huh.

Leo: While monitoring a subject's brain waves, with or without his knowledge, expose him to iconic music from the various regions of the world - the U.S., Europe, the Middle East, China. Determine which ones he's familiar with, based on his involuntary audio cortex response.

Steve: Isn't that kind of a cool idea? I thought that was really interesting.

Leo: It is.

Steve: It's like a way of extracting whether somebody is familiar with specific music that they would be familiar with or not based on their history. And it's a way that your brain gives that away involuntarily.

Leo: Well, and by extension, as you get better at monitoring the brain, there's all sorts of things you can learn. I mean, you could make a pretty good lie detector test that way, I would imagine. Anyway, he says, do you think this technology could be used as part of a multifactor security system? Instead of a password, get this, you learn a song. When I want access, the system plays snippets of music to me and measures my brain's reaction. In a few seconds I can prove that I'm me in a way that could not be spoofed or defeated. What do you think?

Steve: Well, I read the story, or I listened to the blurb on NPR and tried to poke around and do some more research so that I could find out exactly what it means to do a brain scan. As we all remember, there is, like, you know, you can attach electrodes all over your scalp, and you can pick up so-called brain waves. And we've all seen the medical shows where they say, oh, no, this person is in a coma, he's got no brain activity because he's got, you know, 12 lines are all flat, and there's no little high-frequency or low-frequency stuff. And then of course there was alpha waves that would show this, and beta and theta and so forth. But in order to determine specific auditory cortex functions, you need either little probes that have been poked down into your gray matter or some sort of, you know, the article just refers to it as a brain scan, and there's no other detailed information.

So it seems to me this is going a little far to acquire something you know. And actually he makes a point of asking the question, should this be considered something you know or something you are, because of course the nature...

Leo: Right, it crosses the line.

Steve: Exactly, it really does because the nature of this is we're asking your brain, which is something you have...

Leo: And you are.

Steve: ...or I guess something you are, it's asking your brain involuntarily whether this is something you know or not. But anyway, I thought it was just a fun comment from a listener that I wanted to share because I think it's impractical from the standpoint of we don't currently have the technology to, without a great deal of inconvenience, do a scan of a particular region of the brain at the level of resolution and specificity that this kind of test would require. But, you know, a cool idea.

Leo: Interesting, absolutely. Absolutely. Daniel Barber must be a sysadmin because he's worried about U3. He's even more worried about U3 than we are. We talked about these USB U3 drives. He says it's even scarier, it's possible - just to remind you, they're the drives that automatically - the thumb drives that automatically load software using this U3 technology. He says it's possible to create a custom CD ISO, use the U3 updater application to flash the drive with that custom CD-ROM ISO, thereby allowing any application that can normally be run through the autorun command on a regular CD-ROM to be executed when the U3 drive is inserted. Basically that's how U3 works, is it mounts a CD-ROM ISO.

Steve: Right.

Leo: He says there's already an online community creating USB appliances using this technology. There's one called Switchblade that allows a user to quickly grab Windows logon hashes, stored passwords from IE and Firefox and so forth, and store that info on the thumb drive. Another, USB Hacksaw - this is a good one - installs a compromised VNC server on the host machine, opening it up for further attack and remote control. We've actually demoed this on Call For Help some time ago, over a year ago, with a U3 drive. It's really scary. He reminds us about iPod slurping, too, which has been around as long as iPods have been around. And for a while people would go into the Apple Store with their iPod, plug it in, and copy the software onto the iPod and then leave. He's looking into ways to disallow USB drives completely through group policy, GP edit on my network to try to mitigate the threat. I agree. I think an autorun, automount drive is not a good idea.

Steve: Well, and I guess this caught my attention because it brings up a good point, which is that USB - the whole USB interface, as convenient as it is, is also a potential serious security threat, which of course corporations are now becoming increasingly aware of as time goes on. I mean, the drives are called thumb drives because, you know, obviously they're the size of your thumb. So they're very easy to get in and out of somewhere. And something like this USB Switchblade, where literally you could approach a machine, plug this thing in, thanks to the fact that it's U3-based technology which automounts a CD, you could have that CD run anything you want to. And in this case the idea is you approach a machine, you just stick this little USB thumb drive into the system, it immediately runs software which sucks out a whole bunch of potentially incriminating and private information from the machine, and then dismounts itself.

Leo: Well, it's worse than that, Steve. Actually Darren Kitchen on Hak.5 showed us a very common hack, where you walk up to a library, plug in this USB drive, it autoruns. What it does is it copies a trojan onto the system which logs everything for the next week or

whatever. Then you come back, plug your drive in, it says, oh, the trojan is already installed, and then copies the data from the trojan. So it's an even worse attack because it's basically a keystroke logger.

Steve: Right. It seems to me, and I know of many corporations that are now deliberately disabling the oh-they're-so-convenient USB interfaces on the machines that they deploy throughout their enterprise, you know, again because their policy is, look, employees, we do not want you bringing your stuff from home. Of course a USB, even in a benign application, is a potential vector for infection. If someone brings infected applications or spyware-laden applications from home because they want the convenience of having access to those things at work, then USB is the means by which those can travel and transit. And so it really does represent a growing security threat to machines that you want to have otherwise locked down.

Leo: It's fairly easy to turn off autorun, however. It's a simple reg hack, or you could do it in the autorun setup, and then it wouldn't autoboot the...

Steve: Right. And, you know, many security-conscious people, it's one of the first things we do is we say, hey, I do not want a disk inserted in, even a regular CD, inserted into my computer to take off and run. I want to have the opportunity to open a browser, you know, the Windows Explorer and look at the disk and then deliberately run what I choose to run.

Leo: Yeah. Abhi Beckert of Cairns, Australia says - he has a good point. We talked a little bit about how videos and JPEGs could be dangerous. We even speculated you could be infected by going on YouTube. And of course he points out that that's not possible. He says, first of all, that sites that allow you to upload JPEGs often resize the JPEG and change the compression level. And at that point that would damage any buried malware in there. YouTube, of course, converts everything you upload to Flash. So if you're looking at a YouTube Flash video, it's been munged enough that anything that was embedded in the original video would no longer be a vector of attack.

Steve: Yeah, I really liked his comment. And he's absolutely right. And I thought it was very useful to sort of share this notion with our listeners, the idea being that what it is in a, for example, in a JPEG, we do know there are JPEG exploits. And it's certainly conceivable that there would similarly, and this was what we were talking about two weeks ago in Q&A #22, that there could be video exploits, the idea being that an otherwise valid image, for example, in the JPEG case, would have deliberately corrupted, that is to say deliberately designed data that would force a buffer overrun, a buffer overflow, just like data coming in over the Internet is able to do so in, unfortunately, so many Internet-connected applications and components. So you would have something that looks like a JPEG image, inasmuch as its extension is .JPG. When Windows then, or whatever operating system was the target of this, tried to display it, because of a vulnerability, a bug in the display code, this deliberately crafted, sort of pseudo-JPEG would allow program code contained in that JPEG file to be run on the computer.

So the point is, and this was the point that this listener was raising, is that when you do anything to this image which is going to reprocess it, for example you're going to resize it, you're going to change the compression level in the JPEG, you're completely interpreting the image back into image form and then recreating it again in a valid format. So that process of making any change to it would completely just blow out any malware that had been hidden in the image. And so he really makes a very good point. He also says that, you know, if you went to some maybe off-the-mainstream site - he called it a "knockoff site," that, well, if they weren't doing reprocessing, if they were just posting these things up, then you'd still have this problem. But it's certainly the case that any time you convert that to a real image and then

recompress it, you know, the bad stuff is gone.

Leo: In the example we used, which was an embedded JPEG in a banner ad, the most notorious one is the one that happens on MySpace, but it's also happened to Tom's Hardware, those are being served up complete and full of the hack by the ad server, so...

Steve: Yeah, that's a very good point.

Leo: That's very different. So you shouldn't assume that video is safe. But you're right, if it's on a site where you upload something to the site, and the site modifies it, that modification kills any bad germs in there.

Steve: At this point it really would. Now, it's worth mentioning, just to sort of cover the bases, that from early 2006 the Windows Metafile exploit was not a buffer overrun, remember, it was a function of Windows Metafiles which had been designed in from the beginning. So there's an example of a valid image format which would survive this kind of change.

Leo: Oh, interesting, okay.

Steve: So I guess the point is that there are two types of problems. There's a valid use of something that Microsoft didn't want to keep in that format, which was designed in from the beginning, which was always the point that I had made; and there are flaws in the image rendering code which can be exploited, which is a very different kind of problem. And of course that would get completely pruned out.

Leo: Right. Jared in Calgary, Alberta, Canada has a clever web spam bot avoidance trick. We were talking about CAPTCHAs as a way of avoiding spambots. He's come up with a solution that blocks 99.9 percent of the spam sent to his blog. Well, wow. I want to know about this. So does the world. He calls it a "double honeypot." My online web form has three email fields, one that is hidden using CSS styles. In fact, to add to the complexity, inherits it from a parent container. So it's not even immediately obvious what's going on if you look at the CSS. I found that most bots fill in all the email fields, just one, or just the first two it encounters. The hidden one is the second one. So, he says, if it doesn't fill in the second visible email field, the form rightly complains, as if he were a regular user. However, if the data is filled into the invisible field, which I guess only a bot can see, it will assume a bot, as there is warning text if the user has CSS disabled to not enter data into the field, and the form reports success in sending the comment even though it just goes straight into the bit bucket.

Now I don't have to go to WordPress anymore to filter out the cruft nearly as often, it just automatically goes straight to the garbage. The few spam comments that do make it through my honeypot I think are actually people plugging in the spam - by the way, it's happening more and more, it's not robots, but anyway - but I have the time to moderate those comments easily now. I find this an ideal compromise that won't turn away potential commenters with confusing and/or frustrating games. Interesting idea.

Steve: I thought it was a cool idea. So he clearly has the typical, put your email address in here, and then for confirmation put it in again, which we're all used to because people have a tendency - in fact, Leo, you'd be surprised how often people don't type their email address in the same way twice. It's...

Leo: I'm not surprised.

Steve: It's amazing. Anyway, so he's got that. But what he cleverly did was he essentially created, in terms of the flow of his page, he has a second field in between the first and what looks like the second, but which is actually the third in terms of his actual HTML. And naturally bots will tend to either fill in two or fill in all of them because they, too, need to confirm that they've specified their email address properly each time. But by deliberately making the second one invisible, humans will only fill in the first and third, and the bot doesn't know to do that. Anyway, I just thought it was very clever and a sort of a simple way of dealing with at least bot spam on websites.

Leo: Very interesting. Brendan writes from Bismarck, North Dakota with a discovery. I discovered something that may be of interest to you. You may recall the thumb drive discussion, it was unlockable via biometrics. Here's a thumb drive that is only accessible using the correct built-in keypad combination. Oh, a combination thumb drive. It's a combination lock thumb drive called Flash Padlock, made by Corsair. Any thoughts or opinions on a thumb drive like that? Well, see, I think that would work great.

Steve: Well, actually it is pretty cool. It's either $29.95 for the one-gig version or $39.95 for the two-gig. It's got five buttons. So you've probably seen those, like, door locks on cars where they have buttons, one and six share the same button, and then two and seven, and three and eight, and so forth. So instead of being a ten-key pad, it's a five-key pad. It's a dongle...

Leo: Is that any better than a five-key pad, because it's got two numbers on it?

Steve: No, no.

Leo: It's five keys.

Steve: Exactly. I think the only reason they do that is that someone can say, okay, my combination is 32678...

Leo: They can use all nine digits so that they can make it be something, anything they want.

Steve: Maybe they want it to be, like, their birthday or their date of birth or their social security number or something, you know, horribly insecure like that. But still we want to give them all their numbers that are on there. Anyway, so okay. This thing, it's a longer dongle, so that it's got room for all this. It incorporates a three-volt lithium cell.

I should mention, Leo, that I've ordered two of them, they're now on the way, because I need one to play with and one that I'm going to open up because I just want to see what's inside. It doesn't apparently actually encrypt the contents. The company they got the technology from has a more fancy powerful one where the code you enter is used as the cryptographic key to perform on-the-fly encryption and decryption as the data is flowing to and from the flash ROM that's also contained inside. So this one is somewhat less secure in that I'm almost positive, although I couldn't verify this from any of the documentation on their site, it basically functions as a traffic cop in between the flash ROM and the USB connector so that only if you enter all

this in do you end up being able to connect to your flash drive. Which would mean that, if the NSA or the FBI or somebody really, really wanted to get at the data on this drive, they would be able to do so by...

Leo: They just open it up.

Steve: ...opening it up and then rewiring it and bypassing the out - there's a little extra security chip. But for many people I think this really functions as a very nice solution. Of course there's no software running on your system. It's platform neutral - Windows, Mac, Linux, anything. You could plug it into a Coke machine that had a USB connection, and it would work just fine. So it's a neat idea. It uses this little battery because sometimes it might be inconvenient to have to dial the combination when the USB drive is in its, you know, like mounted on the computer. It might be behind your laptop or upside down or something.

So the way it works is you're able to press - there's a sixth button that has a little key symbol on it. So you press that to sort of wake it up and turn it on. Then you have five seconds to begin dialing your combination, which can be up to 10 digits long. I was very glad to see that. It's not like it's a three-digit PIN or something. It could be really hard to brute force. And then, once you do it, that little - it's got also three lights, a red, a green, and a blue light. The blue is for access, and then the red or green have different UI functions, saying I'm locked or I'm not locked. So it then unlocks it, and you then have 15 seconds, which actually, if you look at the clock tick, 15 seconds is a long time, to get this plugged into your computer. So you don't have to have it plugged in while you're unlocking it.

Anyway, I really think it's a cool solution that'll have many nice applications. So I wanted to bring it to our listeners' attention. The company is Corsair. And if you just put into Google, my favorite starting place always, you just put in "flash padlock," you get a bunch of hits. I got mine from Amazon. It's actually more expensive on Amazon; but I like Amazon, and they know who I am and all that, so I was willing to pay a little more for the security. There's a company that I've used in the past, called ATACOM.com, is another good supplier. And they've got them at that $29.95 and $39.95 price. And, you know, on first blush, this looks like a nice little gizmo. I'll report back after I've received mine and had a chance to play with them.

Leo: Miles Bosworth of Asheville, North Carolina says he's dubious about PayPal. He's one of the people who, he says, purchased SpinRite without a need at the time I purchased it, but in appreciation of the effort you put into Security Now!. Incidentally, since he's purchased SpinRite, it's paid off. He repaired his wife's laptop that wouldn't boot and fixed a friend's PC which was stumbling over multiple disk errors, so he's glad he had it.

But actually he's writing about PayPal. We were talking about the PayPal Security Key, and of course I use PayPal for donations. He says, as a very infrequent PayPal user, using it only for purchases that I make online, with no plans to sell stuff or transfer money to family, et cetera, I use PayPal only when it's the only option, primarily because I disagree with their policy of arm twisting for me to submit what I see clearly as unnecessary and potentially dangerous, to me, information to anyone, including PayPal. Specifically, why is PayPal so darn insistent about having me verify my account by sending them information about my checking account? I only use a credit card for payments. And there's never been an issue with any transactions. Yet I continue to be hounded by PayPal about verifying. I noticed this myself. They always ask you.

Steve: And Leo, the reason this is here is I feel exactly the way this guy does. But let's keep going with his comment.

Leo: He says, I have a very low comfort level with sharing additional financial account information, specifically my checking account, which in turn links to my credit and savings in the form of overdraft protection I have in place. I'm not going to grant what I see as excessive and possibly very dangerous access to a checking account that'll never be used in any manner in any transaction with PayPal. I'm not even comfortable that, when I enter my credit card information, I don't have the option not to add this information, which PayPal automatically retains. I'm never given the choice. I got into a fix with them several years ago where, after going back and deleting a card, I could not use that card again on PayPal. I don't know if they still enforce that silly little rule. Otherwise I never leave my credit card info on sites that have that feature, such as Amazon, which gives you a choice at the time of purchase. At the bottom of the last email I got from PayPal confirming my transaction - and he pastes in the whole "get verified" pitch, which basically means you give them checking account information.

The way they verify it, by the way, is they deposit two random, very small deposits of just a few cents into your account; and then they ask you, did you get these deposits? And if you say yes, then they say, okay, it's your account. Or something like that. Or they ask you what the amount is, and if you tell them the proper amount, then they say, okay, you've verified it. And he says, maybe I'm being a bit paranoid, but I'm not about to let PayPal or any other company have access to my accounts when there's absolutely no need. Multiple communications with PayPal questioning this has only resulted in some canned, boilerplate responses and nothing I would see as a valid reason. You know, we should have asked that of our guest a couple of weeks ago.

Steve: Yes. I wish we did. This is exactly - this is what bugs me so much is I don't understand - maybe you do, Leo - what it is about PayPal that has them desperate for my checking account information. But there are sites that will, for example, only ship to a so-called "PayPal verified address." And then there's this notion of not being verified. I finally had to do exactly what this guy did, which was, okay, fine, and gave them checking account information. They did exactly as you said. They deposited some little specific amounts into my account; I had to tell them that they had. Well, then, I'm verified. Yay.

Except that now this PayPal always defaults to wanting to pull money from my checking account, which, you know, which is a problem because my bookkeeper runs that for me. I don't want to have to be constantly telling her what I'm doing. It's so much more convenient to have PayPal pull from my credit card. And, you know, once money is pulled from your checking account, it's gone, as far as I know. I don't know how much, you know, insurance or protection PayPal gives. But basically I don't want money pulled from my checking account. The problem is there's no way to change the default that I have been able to discover. And I've looked around PayPal's site. So every single time I now buy something from PayPal, I have to go in and, when I'm authenticating myself, change the funding options, go in, tell it no, don't take it from checking, take it from credit card. Then they give you like an "are you sure" screen, telling you why this is really not what you want to do. I mean, it is just infuriating.

Leo: Well, I could tell you a couple of things, not to justify it, but I can tell you a little bit about...

Steve: To explain it.

Leo: To explain it. First of all, they have to pay credit card fees, and so they prefer not to. So the transaction is cheaper for them if it's directly from your account. So that's the primary reason. You'd think they'd offer you the option, and I see no reason not to. The

verification, I think is - they might have a case here for it being a legitimate security thing. Remember, the biggest problem that PayPal and any system like this has to face is fraud, somebody...

Steve: Credit card fraud, right.

Leo: Yeah, and somebody posing as somebody else. So the authentication really does then verify your person, who you are. They've got your credit. They've got information. Right? And I think that that's, you know, that would be the excuse they would give. I agree with you, and I wouldn't verify for the longest darn time. At some point they stop you from - they won't let you do any more transactions. You actually have to verify after some...

Steve: Or I think maybe is there a transaction limit, where you can only do a certain amount of money...

Leo: Yeah, something like that.

Steve: ...unless you're verified?

Leo: Yeah, something happens. I ran up against a limit. And I think I finally verified. And of course it's been completely safe. I think they have a safe system. And I think the verification is one way they have of making it safe. I mean, at that point it would be much more difficult to defraud people once you've been verified, right?

Steve: Yes, and I'm glad I'm verified. I mean, it is a benefit to be that. I just wish that they didn't constantly fight you over where money is going to be...

Leo: They should allow you to choose your default money source. That's ridiculous. And frankly I think that that's, you know, it's unfortunate - I understand his reluctance to give that information. I was very reluctant, too. And PayPal has in the past certainly had not the best - a checkered past. And I think a lot of people still remember those days and aren't sure that they want to trust PayPal.

Steve: I do think they're doing better.

Leo: Well, they are. And one of the ways they're better is things like, you know, if you take a credit card out of the system, they don't let you put it back in. I mean, they're a little strict. And I think that's one of the ways that they make it more reliable. But I'm certainly not making apologies for them because I...

Steve: I would say that we've just made it very clear how we feel about that aspect of PayPal.

Leo: And having said that, I verified, and you verified, and I never do - I only transfer money into my checking account. I never use it to pay for anything. Now, I have to think. I

pay from my PayPal account. And so it never asks to take money out of my checking account because I have money in my PayPal account.

Steve: Ah, right, you have a positive balance in your PayPal account.

Leo: Right. And so it always uses that by default. So I don't have the same issue you do with it trying to take money out of my checking account.

Farren Constable of Manhattan, Kansas has a note about encrypted hard drives. Just an FYI, he says, I seem to recall that when you discussed these new hard drives with built-in hardware encryption, you said they weren't available and probably wouldn't be for a while. Just wanted to let you know that ASI, a computer distributor, is currently selling laptops with the encrypted hard drives. He says, I seem to think that ASI had some sort of exclusive deal on these drives and/or systems. Is that so?

Steve: Well, I wanted to mention, because I don't remember predicting when they would be available, but I have one. I discovered a few weeks ago that they existed. This is the Hitachi drive. I don't know whether other manufacturers yet have those. But you may remember that Hitachi purchased the hard drive business from IBM and for a while was still selling under the Travelstar label, but now it's largely under their own. Anyway, they've got a full range of standard laptop drives with this very cool, on-the-fly, built-in 256-bit AES encryption.

And anyway, the drive is here. It's still in its little static protection sealed plastic silver bag. I have not yet had a chance to play with it and learn whether - the thing I want to find out is exactly how does it work, and does it require any BIOS support in order to be used. I haven't determined that one way or the other. But that'll be - certainly I will close that loop with our listeners as soon as I get there. I did want to let people know, though, that they do exist.

Leo: Excellent. And would it be more secure because it's built into the hard drive?

Steve: Oh, yes. Well, the beauty is, somehow you give it a password, and maybe it's the standard BIOS unlocking password. When you give it that password, then it hashes that into a 256-bit encryption key so that every sector it writes to the drive runs through AES 256-bit encryption so that the data physically stored on the drive is encrypted. And then of course the reverse process happens upon reading.

The point is that literally no force on earth can then obtain the data for that drive if the password is not known. So unlike hard drives which lock themselves, I mean, that locking - in fact, we were just talking about this with regard to that Corsair flash padlock. You know, it's locking the contents of its EPROM, but it's not encrypting the contents of the EPROM at this level, at this stage. Similarly, the hard drives that have been around for many, many years, they have locking technology that will prevent somebody from easily reading the drive. But at the "here's a subpoena to the drive manufacturer, unlock this drive" level, that can still be done. But not if you're actually encrypting all the data that goes onto the drive. And I just think it's very cool, especially in a laptop mode, that that would be offered.

Leo: Yeah, yeah. Edward, just up the coast a little ways, about five miles, in nearby Santa Rosa, shares a discovery. He says, just a quick note to let you guys know that VeriSign's OpenID platform - that's the one that we were talking about with the Security Key that comes from PayPal, it's at pip.verisignlabs.com - now supports the use of PayPal Security

Key. Well, I think we knew that, didn't we, that it was part of the PIP...

Steve: Actually I told you about this. I wanted to share it with our listeners.

Leo: Oh, okay.

Steve: And we're going to talk about it in detail next week.

Leo: So here's the email he got from VeriSign. It says "...strong authentication support via second-factor credentials from the VeriSign Identity Protection Network. PayPal tokens can now be used with PIP, along with the ability to have a one-time PIN sent by SMS or email if you've forgotten your credentials." I like that.

Steve: Yeah, it's very cool. And again, I want to - it's one of the two topics, or actually maybe three topics for next week. PIP stands for Personal Identity Provider. And I just wanted to give our listeners a heads-up about this. Actually several people wrote in, so not just Edward in Santa Rosa, but a couple other people said, hey, I was poking around. And you may remember that, when we had our friend on from PayPal - I hope he's still our friend after what we just...

Leo: Well, I'm sure he is.

Steve: I'm sure he is, too. He was talking about how PayPal is essentially using the VIP, the VeriSign Identity Protection technology, as their backend behind their whole token deal. And what I had mentioned to you, Leo, was that I did some follow-up research. I found VeriSign Labs and the fact that they sell their own tokens, and I bought three more because they will sell you as many as three of them. I don't know if it's three at a time or three total. But what's very cool is that you can register multiple tokens at the same time, and this solves the "I've got one at home and one..."

Leo: Ah, and they'll work the same way.

Steve: Exactly.

Leo: Ah.

Steve: Exactly. So anyway, this will be what we're talking about in greater detail next week. But I just wanted to acknowledge the people that had written in and said, hey, I found VeriSign Labs is doing this stuff.

Leo: He also says he's now using pip.verisign.com as his primary OpenID account, changing from ClaimID. I use ClaimID, too. So I will switch over because that means when I do my OpenID verification I'll use the dongle. Right? A fob.

Steve: Exactly. Whatever we call it.

Leo: Whatever you call it.

Steve: There was some discussion about that, too, in our mail. Apparently the official word is that a dongle is something that you plug into something, like the old parallel port dongles that were used for protecting high-value software, and in fact even to this day are still used for, like, expensive vertical market software. Whereas a fob is a freestanding, you know, standalone thing that you don't plug into something. So, like, okay.

Leo: That actually is what I thought. Well, to me a fob is something you put on your watch chain or your watch. But anyway, that's another matter.

George in Ohio has discovered something great about our sponsor, Astaro. He said, I'd like to point out there is a really positive piece of information about Astaro that you're not mentioning in the advertisements Leo does in each episode. Well, there you go. I'd better find out, huh. He says, I recently lost my long-running and until now flawless SmoothWall box. Patrick and I have been talking about SmoothWall since Screensavers days. It's a great, great solution for an open source firewall. He says his processor fan died, cooked the machine. I thought this would be a good time to check out Astaro. He has a faster machine he just recovered, so he put it on that. He wanted to make sure he actually liked it before committing.

So while he was out shopping online for a hard drive to throw into it so he wouldn't have to nuke the current OS, he dropped by the Security Now! page, Astaro.com/securitynow, to make sure the hardware would be compatible. And I was actually going to mention this in the ad. But he noticed that there's a download option for a Virtual Appliance for VMware of the software. So if you're using VMware, there is an Astaro - in fact, it's one of the most popular appliances. He says he already has VMware Player, which is free, installed on the system for running Linux distros I'm testing, so I thought it was a perfect solution. I downloaded it and ran it, and I like what I see. I'm impressed that they had the foresight to package it that way for people like me who like to feel out the interface before we commit to installing it. Bravo, Astaro. Just thought you might want to mention that to your listeners.

I found that in fact this week, too. When I was testing out VMware Fusion for the Mac, I noticed that I could run Astaro Security Gateway on it. It's like the No. 5 appliance of all.

Steve: Oh, very cool.

Leo: That's neat, yeah. In fact, you can try a lot of - that's one of the neat things about VMware is those appliances. And that's something that they have over Parallels. Parallels also might be in some doubt. I think there's a lawsuit over the Parallels technology.

Steve: Uh-oh.

Leo: The company that the Parallels guys worked for before they worked at Parallels...

Steve: Oops.

Leo: ...says that's our software, what are you doing? And now a European court has not issued a preliminary injunction against the sale of the software, but it's something to be aware of. At least we have a choice. If you haven't bought Parallels yet, I think VMware is a good contender. I bought Parallels, so I don't see any reason to run to VMware. It's very similar. Although some say it might be a little bit faster.

Steve: Actually that's Mark Thompson's contention, Mark Thompson my friend from AnalogX. He believes Parallels just runs circles around VMware, although the performance is not something I have verified.

Leo: I don't know. I don't know. They seem pretty similar.

Steve: They really ought to be. They ought to be.

Leo: Yeah, I mean, it's the same thing. They're both using this hypervisor mode and all that. But I did see a number of comments from people who said VMware was faster. So, you know, it's one of those things. There's a lot of psychology involved in this. If you feel like it's going to be faster, it's going to be faster.

Danny in Ogden, Utah enjoyed our last podcast about leaktest. He said, I very much enjoyed the firewall leaktest issue. One thing you might want to remind your listeners is that, while this is an important thing, it only applies to software-based firewalls. I currently work for Juniper, one of the big companies doing this.

Steve: Router company.

Leo: Yeah, he does tech support for their firewall and intrusion detection and prevention products. I'm proud to say our firewalls are not affected by such tactics. But then again, you already knew that. Well, that's why we recommend routers, frankly.

Steve: Yes, that's exactly the case. And I did want to mention that certainly Danny is correct, that by being a box outside of the PC, you get a lot more security from a standpoint of software not being able to go in and disable your firewall. And in case of the router, that's one of the reasons that I strongly recommend people disable the Universal Plug and Play support because that is a vector by which software running in a PC could disable the security prevention and features of a router by deliberately opening incoming ports statically on the router. That's what UPnP was created for. And unfortunately it was created without any security model at all. So it's just - that's just a sore point for me.

But on the flipside, the problem that external firewall hardware has is it can't tell anything about what application generated the traffic. So what we were really talking about in the leaktest episode was that the whole idea was a personal firewall, meaning a firewall software running on your PC, it had the ability to go back and figure out which process was generating the traffic and then check its configuration to see whether that process had been authorized to send data to and from the Internet, which of course isn't something that an external piece of hardware can do because there's no way for the hardware to know what process is emitting the traffic from the PC. All it sees is packets coming out. But it can't tell where they came from.

Leo: Although a high-end router like a Juniper certainly does monitor outbound traffic.

Steve: Well, it does. But again, for example...

Leo: Can’t figure out who did it, though.

Steve: Exactly. And that’s the real leverage that people who like personal software firewalls get behind is they like the idea of knowing who was controlling or who was generating whatever traffic that they’re seeing.

Leo: Even if a bad guy could be lying about it.

Steve: Exactly.

Leo: Which to me obviates the whole point of it. I mean, yeah. Okay, cool. It can tell you what the process is. But it has no way of validating that that information is accurate.

Steve: Oh, and the other problem is, when you have something like servicehost.exe, which is...

Leo: Meaningless, yeah.

Steve: It’s just a container for a whole bunch of Windows services. You lose the granularity of knowing, well, what service in the service host processor is doing this. So, yeah, that’s a problem.

Leo: Mark Paynter, Sydney, Australia, has an interesting observation, again about the fob/dongle/key.

Steve: Doohickey.

Leo: Doohickey. He says, I obtained a PayPal security fob dongle key, which is a good idea. But it occurred to me that a spoof PayPal site could do a pop-up window for the key and simply accept any number that is entered. The way to test it would be to enter a completely wrong number, and if it accepts it, then it didn’t check. So security needs to be checked by using "not" logic rather than "and" expressions.

Steve: I thought that was sort of an interesting observation. Of course the point this brings up is that there are two different things that we would like to have happen. The dongle fob key doohickey is used normally when you’re trying to authenticate yourself to the remote server. Mark’s point is that, by lying, by deliberately lying to the site which may be spoofing, you’re authenticating it.

Leo: Right. Which is a good point.

Steve: Which is sort of an interesting point, yeah.

Leo: I'd like to point out that most of the time when you do, if you were to log onto a phishing server, after you entered your name and password it really doesn't go on. It's not like it says, okay, good, let's do some more stuff.

Steve: Yeah, let's enter your security key. It's glad to have you that far.

Leo: Bye. Thanks. See you later. And of course you're protected if you have a dongle because even if you entered your dongle number it's only good for the next 30 seconds. I've shown my dongle number on our UStream feed during the radio show. People go, what are you doing? I say, don't worry.

Steve: And in fact you and I talked about this on your KFI syndicated radio show last week. And we had fun reading off our numbers...

Leo: Don't worry.

Steve: ...as they changed. It's like, it's okay because it's not going to be good.

Leo: I have to say I love that feeling. That's just so cool. And I'm going to right away go to pip.verisign.com and make that my OpenID provider because that means - I'm correct in thinking that that means that whenever I did an OpenID login, I'd have to use the fob now; right?

Steve: You would have to use the fob, exactly, given that you use VeriSign as your OpenID provider. Nothing would prevent you from having also a different OpenID provider. And what I like about the VeriSign approach is that they do have the ability to simultaneously register multiple credentials and non-fob - I just hate that word, but you know - non-fob authentication alternatives also. So, I mean, they're really coming up to speed nicely. And we're going to be talking about it in greater detail next week.

Leo: Cool. Steve Gibson lives, breathes, and eats security at GRC.com. That's where you'll find ShieldsUP!, Shoot The Messenger, DCOMbobulator, UnPlug n' Pray, Wizmo. One day I'll read them all. One day I'll read every single thing that you do, and this will be a three-hour podcast. Also SpinRite, of course, his daily bread. And that is SpinRite. In fact, you want to read the testimonials, SpinRite.info. Or just go to GRC.com. That's also where you'll find 16KB versions of the podcast, transcriptions by Elaine, notes, and every Security Now! episode, all 106 of them, going way back two years.

Steve: And counting.

Leo: And counting. Congratulations once again, you are listening - you have the good taste to be listening to the best technology podcast in 2007, thanks to the Podcast Awards.

Steve: And I thank our listeners once again for making that happen. That's really cool.

Leo: Yes. Yes. Okay. Had a little macho moment there, but I'm feeling better. I'm going to grab my fob, and we're going to get out of here. We'll be back next week. What are we talking about next week, Mr. G?

Steve: Next week we're going to talk about, as we mentioned here in passing, VeriSign's Identity Protection, the VIP program. I also want to talk about some changes I recently made to GRC's very popular Perfect Passwords page as a consequence of some feedback that I received, and the fact that I'm currently dipping in and doing a whole bunch of work on the GRC site in general. And so I'm going to talk about that a little bit.

Leo: So you're saying the Perfect Passwords page wasn't perfect?

Steve: They were perfect enough, but they're even more perfect now.

Leo: Even more perfect than ever before.

Steve: And in fact, if Even More Perfect Passwords wasn't too much of a tongue twister and too long, that's what I would have called it. But obviously made it perfect.

Leo: Okay. Steve, we'll talk again next week on Security Now!. Thanks for being here.