SECURITY NOW!

Transcript of Episode #373

Listener Feedback #152

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

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-373.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-373-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here with the latest security news. We'll talk about Microsoft's Second Tuesday Updates, which happened yesterday. And then we answer your questions: 10 questions, 10 answers, coming up on Security Now!.

Leo Laporte: It's time for Security Now! with Steve Gibson, Episode 373, recorded October 10th, 2012: Your questions, Steve's answers, #152.

It's time for Security Now!, the show that protects you and your loved ones online with Mr. G., Steve Gibson, our Explainer in Chief. He's the host at GRC.com, the inventor of, well, the coiner of the phrase "spyware," the inventor of the first antispyware. He's also the author of SpinRite, the world's best hard drive maintenance and recovery utility. A very good day to you, Mr. Gibson.

Steve Gibson: Hey, Leo. It's great to be with you again, as always.

Leo: A Q&A episode today.

Steve: And before we began recording I mentioned to you something that Elaine had mentioned to me, that, well, it's belated and then some, but we sort of let an anniversary of the podcast slip by unnoticed, unmentioned, unobserved.

Leo: This must be our third or fourth year by now.

Steve: [Choking]

Leo: [Laughing] Well, let's see. Let me do the math. Modulo 52.

Steve: [Still choking]

Leo: You and I can do that because you've only missed one show per four, so it wasn't your idea. We made you miss a show.

Steve: Oh, and believe me, I've never been forgiven for that, Leo. That was...

Leo: Who does not forgive you for that?

Steve: The listeners. Oh, they were quite upset.

Leo: Oh, come on.

Steve: Well, it's just that we had - we'd never missed a week. And I like that kind of absolutism.

Leo: I know you do because you're an engineer. And it's like, perfection is the only option.

Steve: It's either true or it's false, and it had been for a long time. Suddenly, never again.

Leo: So missing one episode is as good as missing 500, really, from your point of view.

Steve: Anyway, at one point we were talking about our anniversary, which slipped by in August. We ended our seventh year and began Year Eight, which we're already well into.

Leo: Episode, what, 364 would have been the seventh year.

Steve: There's a lot of controversy about that, Leo.

Leo: Did we begin with one or zero?

Steve: You can't do any kind of a 52 thing. You've got to just look at the date. And that's what Elaine did. She said, "Your first podcast was on August" something or other [August 19, 2005]. And another one of those went by. It's like, oh, well, I guess that would be the end of the seventh year.

Leo: Happy Anniversary, Mr. Gibson.

Steve: Leo, we're going strong.

Leo: Wait a minute. We finished seven years. We're in our eighth year.

Steve: Yes.

Leo: Jiminy.

Steve: Yes.

Leo: Jiminy Christmas. Wow.

Steve: And we just haven't run out of anything to talk about.

Leo: We've said this before, but you were very worried when we began this that there would not be enough. And we only did a half-hour show when we first started. We're now doing four times more each week.

Steve: I know. It's freaky. I look back at the early podcasts, and I think, whoa, 29 minutes? Really. Okay. Wow.

Leo: So it's almost four times longer, and we still haven't run out of stuff. So there was considerable misjudgment on the amount of horror that lay out there on the Internet, waiting for us to reveal it.

Steve: Yes, the horrors just keep on coming.

Leo: The horror, the horror.

Steve: Speaking of which, well...

Leo: Go ahead. Go ahead.

Steve: We have interesting news. This is a Q&A episode, our 152nd Q&A, Episode 373. So I think we've got a good podcast for everybody, as always.

Leo: All right. Let's get the security news here.

Steve: Okay. So we are here on, what is this, the 10th of October, meaning that we had our second Tuesday just yesterday. Microsoft did a relatively small update. There were seven updates, which fixed a number of security issues in Windows Office and SQL Server. Interestingly, the big problems were not in IE and Windows, as is usually the case, but some sort of an exploit that affected Office and their Server products. That was the only thing that was rated critical, which was a remote code execution problem somehow involving RTF, Rich Text Format, files. So, as always, keep Windows updated and you'll be okay. And then they just had five other miscellaneous security things, privately reported vulnerabilities.

Interestingly, RSA - the inventors, well, the pioneers of early asymmetric crypto and famous RSA - have been warning of an impending attack on online banking. In a post from, I guess it was actually last week, their head of cybercrime communications, Mor Ahuvia, wrote: "In one of the most interesting cases of organized cybercrime this year, a cyber gang has recently communicated its plans" - now, they've been monitoring this quietly and sort of in the same way that Brian Krebs has established himself and is sort of part of that underground so he can see what's going on. "A cyber gang has recently communicated its plans to launch a Trojan attack spree on 30 American banks..."

Leo: Oh, great.

Steve: Yeah, "as part of a large-scale..."

Leo: Don't mind the grinding. I'm just making my coffee.

Steve: Okay.

Leo: I'll turn off the mic.

Steve: "...as part of a large-scale orchestrated [crimeware] campaign. Planned for this fall" - so coming to you before the holidays, "the blitzkrieg-like series of Trojan attacks is set to be carried out by approximately 100 botmasters," who therefore are independently running about 100 bot networks. "RSA believes this is the making of the most substantial organized banking Trojan operation seen to date." And remember, this is RSA blogging this. This is not some random nobody.

They said: "By investigating the group's forum-post announcement and analyzing the Trojan, RSA has managed to link the cyber gang's weapon of choice to a little-known, proprietary, Gozi-like Trojan" - that's G-o-z-i - "which RSA has dubbed 'Gozi Prinimalka.' Derived from the Russian word meaning 'to receive' and alluding to a Trojan drop point, the word 'Prinimalka' appears as a folder name in every URL path given by the gang over the years to its [crimeware] servers. According to underground chatter" - which RSA has been monitoring - "the gang plans to deploy the Trojan in an effort to complete fraudulent wire transfers via man-in-the-middle manual session-hijacking scenarios."

And we've talked in the past about how that works, where if you've got something that has infected your local machine, as these Trojan bots would, then they're intercepting your browser's communication to your bank prior to it being encrypted and sent over the 'Net. So this is not a man in the middle decrypting your SSL communications. This is a man just on the other side of your keyboard and screen, closer to you really than the middle, but...

Leo: Man over your shoulder, really.

Steve: Man peering, exactly, cyber-wise over your shoulder. And they said: "Previous incidents involving this Gozi Trojan, handled by RSA and other information security vendors, appear to corroborate the gang's claims that, since 2008, their Trojan has been at the source of siphoning $5 million from American bank accounts. Gozi Prinimalka's similarity to the Gozi Trojan, both in technical terms and its operational aspects, suggests that the HangUp Team - a group that was previously known to launch Gozi infection campaigns - or a group closely affiliated with it may be the troupe behind this ambitious scheme."

Leo: Wow.

Steve: "If successfully launched, the full force of this mega heist may only be felt by targeted banks in a month or two. The spree's longevity, in turn, will depend on how fast banks and their security teams implement countermeasures against the heretofore-secret banking Trojan."

Leo: Not to put it down or anything, but $5 million in five years is not like, I mean...

Steve: Correct.

Leo: It almost sounds like the scheme in "Office Space," where they were skimming pennies off the top kind of.

Steve: Well, and remember, too, that they don't have any control over whom they infect and over the quality of the...

Leo: So it's hit or miss, yeah.

Steve: Right, it's hit or miss. The Trojan may not be able to intercept the bank that that particular person who is infected by it deals with. And they may not have much money to lose. So, I mean, if there's not anything in their checking account except low-level transactional amounts, that's all they're able to get. So anyway, what RSA is talking about is they're seeing the chatter in the forums as these groups organize. And apparently they're actually looking for, quote, "investors," unquote, who would be fronting the money to build the backend infrastructure to accept the payments and process them once they've been transferred.

Leo: Oh, yeah. Sure, they need a fence.

Steve: Yes, exactly.

Leo: So to speak.

Steve: Crazy. Oh, also Adobe, Monday of this week, a couple days ago, did an emergency out-of-cycle update to Flash, fixing 25 security vulnerabilities. And an hour later, Microsoft released news of their update to the Flash player which is now bound into IE10. Because, with Flash having been such a success in the security space, why wouldn't you just build it right into your browser?

Leo: Now, it's built into Chrome, but it's sandboxed. It automatically updates. Well, see, this is the problem, Steve. I mean, we may not like Flash, but everybody needs it and uses it. So they're going to install it eventually.

Steve: Right. It's probably going to - you're right.

Leo: So better to do it this way.

Steve: There are still enough sites on the 'Net which require Flash that you're going to end up with it in your browser.

Leo: I mean, I wish it would go away. But it's here to stay. Not to stay...

Steve: Yeah, well, I mean, and anyone with an iPad is annoyed by their lack of Flash, frankly, on the iPad because you're away from your main machine somewhere, being mobile, and you come to a site that is just dead without Flash. So it's like, okay, well, I wish we were migrating to HTML5 more quickly. But anyway, so...

Leo: Same with Java, too, by the way.

Steve: Yeah, it's true. That's absolutely right. And so Microsoft has been in the past criticized for their lack of speed. In this case they were only 60 minutes lagging Adobe. So one can hope that, if they're going to have Flash bundled in, they'll be taking responsibility for it, as they seem to be doing now with IE10, and being much more quick about updating.

And in another little blurb, this got past me a few weeks ago. And I meant to bring it up, but then I think that someone else must have tweeted it to me. I went, oh, that's right, I forgot to mention this. Okay. Every fingerprint reader on laptops everywhere comes from the same company, UPEK.

Leo: UPEK.

Steve: Yeah. I mean, I'm a big Lenovo user for my laptops, and I like the fingerprint scanner. We've talked about how nice it is to sort of drag your finger over the little capacitive reader, and it logs you in and unlocks the BIOS, logs you into Windows and so forth. And it's like, oh, look, we've got multifactor.

Well, a security company, ElcomSoft, just noted back in August that there was a problem with UPEK's software because, when you're setting it up and giving it the ability to log you into Windows, you need to give it your credentials. Now, the assumption is - and unfortunately that turns out to have been all it is - is that they would do something secure with those credentials. Turns out they're stored in the registry, not very well encrypted. ElcomSoft did not disclose any details, but they put out a warning that, for what it's worth, anyone using any biometric fingerprint reader with UPEK software - and I remember when I saw this it was the Who's Who of laptops. I mean, all the laptops. And there was Lenovo of course listed, and all the other ones because this is the company that cornered the market on fingerprint software, and nobody else seems to have thought it was worth competing with them.

So last week a security researcher, Adam Caudill, he described himself on his website - he blogs. And in his description he says, "I'm a software developer, pen-tester" - meaning penetration tester - "and manager. I'm currently located in Southern Virginia. I write about development security and anything else that I find interesting, from Microsoft's .NET stack to Ruby, security and exploits, and even a little about photography and lasers." So he blogged: "On August 28th, ElcomSoft announced that they had determined a method to extract Windows passwords from the registry of users of UPEK's fingerprint readers and Protector Suite software," and he says in parens, "(UPEK is now owned by AuthenTec, which is now owned by Apple). What they didn't announce..."

Leo: Apple Computer?

Steve: That's - I didn't verify that.

Leo: Apple doesn't even have any fingerprint reading hardware.

Steve: Isn't that interesting.

Leo: That's bizarre.

Steve: But AuthenTec does other things.

Leo: They must do other, oh, yeah, yeah, that's kind of - that name sounds familiar.

Steve: Yeah, it does. He says: "What they didn't announce was the technical details of how they did it. Myself," he writes, "and Brandon Wilson have been working to recreate their research - and we have. We have not been in contact with ElcomSoft, so this is an independent rediscovery of this vulnerability." Of course they also knew where to look from what ElcomSoft wrote. He says: "ElcomSoft has committed to not release details, which I understand. But given how likely it is that others will determine this technique, I believe that this information should be available to penetration testers and auditors so that these insecure credentials can be identified." Adam then goes on to describe this in detail.

So it's AdamCaudill.com. Just go there and look at his blog if you're interested. I'll give a brief summary of what he found, and that is that there was crypto applied. But UPEK says, and he found, that they just sort of made up their own. And we always know that's never a good idea. They have what they call AES-56. And it's like, wait, there is no such thing as AES-56. Well, there's AES-256, of course. Well, what they did, apparently, because they operate on an international scale, they needed to comply with international export restrictions, or they needed their software to be able to operate within countries that legislatively restrict the security of software. So even though it's not a problem, for example, in the U.S., they have one solution global. And what they did was simply pad all of the other 200 bits of AES-256 with zeroes, drastically weakening the crypto.

Leo: That's moronic. That's actually moronic.

Steve: Oh. And so...

Leo: I mean, it would have been better to us - oh, that's just moronic.

Steve: So it'd be better to do anything. I mean, you could...

Leo: Anything.

Steve: 3DES, for example, would have, I mean, this ends up being...

Leo: Is it because they don't have hardware to do the calculation?

Steve: No. The only reason, the only rationale that makes sense is that they did this for export restrictions, in order to comply with export restrictions. Because there is legislation in some jurisdictions which state that you cannot use crypto greater than 56 bits because the powers that be within those regions are able to crack that. And so what ended up happening was that, without even understanding all of this, Adam and his buddy Brandon knew where to look because ElcomSoft had provided enough breadcrumbs for that, and they just independently cracked it. So on his blog posting he provides all the details.

So the takeaway, of course, for our listeners is that we should not overly rely on the security of these fingerprint readers; but, more importantly, in providing this information to the fingerprint software to allow it to log us into Windows, we have inadvertently dramatically weakened the security of the system because this is now widely known. And so if malware gets into our machine, it will know where to look to see if we happen to be on a laptop with a fingerprint reader and UPEK software, and they could grab the key and then decrypt it and get our Windows credentials, which there otherwise isn't a simple way to achieve. So this is not good.

So it's a classic - what I liked about this as a lesson for our Security Now! listeners is this is a classic case of a bad implementation of a potentially secure technology where the implementation results in greater weakness than if you had never used it in the first place.

Leo: Well, we saw that a couple of weeks ago where they were storing passwords in the clear in the registry; right? So this is the second flaw. I don't know if it's the same company, but the second flaw with fingerprint readers.

Steve: Yeah. This is, well, this is in the clear. Well, this is not, I'm sorry, this is not in the clear.

Leo: Not in the clear, but it's just stupid encryption.

Steve: Yes, exactly.

Leo: Just badly encrypted.

Steve: Weak, roll-your-own encryption. And the point is that you end up with worse protection because you now have your Windows logon credentials, badly encrypted in a way that everyone understands, sitting in the registry. That's normally never the case. So essentially you told the software how to log you into Windows, and it's not protecting that from anything that had access to the registry. So any malware that got into your system could look to see if this was there and acquire your Windows credentials that way. So that's not good.

I guess if this is of concern to someone, then what you have to do is stop using UPEK's fingerprint reader software. I would check in with AuthenTec and look for updates or news. They're not saying anything. People have asked AuthenTec what they think, and so far no official response from them. So until this gets fixed, what you would want to do is change your Windows password, your logon credentials, and don't tell the UPEK fingerprint reader about it. Disable its logon because...

Leo: It cannot be trusted.

Steve: ...you don't want to use that anymore. Yeah, you can't trust it. You can't tell it what your new credentials are. And then once this gets updated - it's got to be updated.

I would imagine somebody's working on this now. And then you can move forward.

Leo: Dr. Mom wonders, because fingerprint readers are routinely used in things like pharmacies and hospitals to keep unauthorized people from taking medication, if this applies to other fingerprint scanners.

Steve: No, it would just be Windows with this UPEK software. In fact, I mentioned before the podcast, Leo, that I was helping a neighbor who needed some medical care yesterday, and I was watching the security in ER. And I thought it was interesting when the nurse...

Leo: Of course you were.

Steve: ...when the nurse, she dialed in the automated IV metering. And I watched her scan her badge and have her thumb scanned in order to take responsibility for, essentially log into the fact that she had just been the person who set this up. So it's like, oh, interesting, cool.

Leo: Right. Yeah, that's, I think, what Dr. Mom's talking about.

Steve: But no problem, just Windows.

Leo: Just Windows. As long as they're not using Windows with Internet access.

Steve: And I did run across a nice note from a listener who ended up posing a question that I thought our listeners would find interesting. Robert Osorio in Lady Lake, Florida, he said - the subject was "Another SSD/SpinRite testimonial." He said, "Steve, just to let you know that you can add me to the list of SpinRite users who have found SpinRite useful for reviving SSD drives. I'm an IT consultant and have been using SpinRite for a couple of decades. I have an older Intel X25-M" - which is very nice - "SSD drive that was the boot drive for my main workstation. I recently upgraded to a much faster SSD and relegated the old Intel drive to a laptop. However, in time, I started getting OS issues that, on a spinning drive, would have indicated bad sectors and would have had me running SpinRite on it immediately. Since this was an SSD, I thought all I could do was update the firmware, which I did. And it did help for a while. Or I could just write off the drive.

"Then I heard you mention on a recent podcast that running SpinRite Level 1 on an SSD could help, so I gave it a shot. It made a dramatic difference, and now this drive is running smoothly once again. I have now run SpinRite Level 1 on all my SSDs and will continue to do so on a regular basis for preventative maintenance." He says, parens, "(I religiously run SpinRite Level 4 on all my spinning drives every six months or so, as well.) I did want to get a clarification from you, and I'm sure other listeners would appreciate this, as well. You recently read a testimonial from someone who recovered an unreadable Flash drive using SpinRite Level 2, and you indicated that was a valid procedure. Am I correct in assuming, then, that it's okay to run Level 2 on an SSD or Flash drive for preventative maintenance? Or should I use Level 1 for preventative maintenance and Level 2 for data recovery only?

"My concern is avoiding excess writes, which would prematurely wear out the memory cells, thus your admonition against running Level 4 on solid-state media, since it performs aggressive writes. Reading from your documentation, it appears that Level 2 is only performing writes if it recovers data from a damaged sector and then has the drive relocate it. As such it seems that Level 2 is not much more aggressive on writes than Level 1 and should be safe to use on a regular basis on SSDs. Thanks again for a great product and a great podcast."

And Robert's exactly right. The difference between Level 1 and 2 is that Level 2 will perform some pattern testing on the area, so doing some writing, if it runs across a problem. And that's probably more useful on magnetic physical drives than on SSDs. So I would advise using Level 1, which is sufficient on SSDs, where you want a read-only process. Level 2 makes more sense on magnetic drives where you want maximum speed and just a read pass over the drive, and then SpinRite will do more work with testing the surface if you end up with a problem at Level 2, which it does not do at Level 1. Level 1 is meant to be just a read permission-only pass.

We'll remember that a week or two ago I read a note about SpinRite recovering data even when it was run at Level 1, but that was the drive essentially doing the recovery, not SpinRite. And with SMART drives now that can happen. So again, Level 1 for SSDs, Level 2 for hard drives. And it's great to see more evidence that SpinRite can be useful on SSDs because of course that's where the world is headed at some speed.

Leo: Yeah. It's good for you. Yeah. Good. Well, I'm not surprised. I mean, I guess it just means that there's certain things it couldn't do.

Steve: Well, the fact is, SSDs actually share a surprising chunk of hard drive technology. There is error correction going on because those cells unfortunately are - or I guess, well, yeah, unfortunately are being downsized to the smallest degree possible, or downsized to the greatest degree to make them as small as possible in order to get the highest density to be competitive. So it's the same kind of problem where hard drives are less than completely reliable, purely due to competitive pressure to squeeze as many bits as possible into the smallest cost possible. In the case of SSDs, what that means is that the size of the tank which is storing the charge which is remembering whether that's a one or a zero bit, they've just made that incredibly small. And so they've made it so small that you are then relying on error correction to sort of pull you out of the gray area.

There's gray unfortunately now designed into these SSDs because they figure that's the right tradeoff to make. And so to something like SpinRite - well, actually there is nothing else like SpinRite, so SpinRite is able to make a read pass over the SSD, show it that, okay, this is becoming too gray, essentially, not clearly black or white, but a little too gray. And so then the SSD controller says, uh-oh, and will either rewrite that data to strengthen it; or, if it doesn't look like it's safe, it'll essentially map that out and map in new space. So, I mean, it's very much like the way hard drives have evolved. They just don't spin.

Leo: Right. And that's one of the reasons they're fast.

[Talking simultaneously]

Steve: ...calling it SpinRite, Leo. I don't know how I could change the name. Even though nothing is spinning, it sounds right.

Leo: Yeah, no, SpinRite, it's SpinRite. It's SpinRite. Are you ready, Steve?

Steve: You betcha.

Leo: You've got your thinking cap on. Let's go to our questions, as proposed by Steve Gibson, who's collected them from his feedback form at GRC.com, starting with Carl Bolstad in Seattle, Washington. He declares - and I'm happy to hear this one - Carbonite wins. Thank you for putting this one in. Hi, Steve and Leo. I've been enjoying the Security Now! podcast since the beginning. I'm about three months behind right now. I've also been a Jungle Disk user, like you, Steve, until recently. When I had to reinstall Jungle Disk because it wasn't working anymore on my XP machine, I discovered it wouldn't install at all. So I went to the website to post a help ticket and was shocked at all the complaints not getting any response from the Jungle Disk staff. It got sold; right?

Steve: Yeah.

Leo: To Rackspace.

Steve: And what happened was what we worried was going to happen, apparently.

Leo: Just fell off the face of the earth. So I started looking for a new online backup solution. Luckily for me you'd recently done a podcast on exactly that. I tried several of the ones you recommended. By the way, that's a great show, where you just list all of the cloud storage solutions pros and cons.

Steve: And go through them all, yeah.

Leo: In the end I just couldn't resist Carbonite's plan of just backing up all the user files on the internal drive without worrying about how big it may be or how much your backup will be costing this month. It's less than five bucks a month for everything. It's such a relief to know that everything's backed up. The only time I'll have to worry about it is if my hard drive fills up. Thought you and Carbonite might like to know. Thank you, Carl. Thanks for the great podcast. It's amazing it's still relevant and entertaining after all these years. Carbonite, of course, is one of our sponsors, and I'm sure they'll appreciate that.

Steve: Well, and I did, I've also, the thing that caught my eye not only was that he appreciated the cloud storage podcast we did and that he chose Carbonite and his rationale for doing so, but I have had a bunch of people complaining about Jungle Disk.

Leo: That's sad.

Steve: Our listeners. Remember it was Dave, I remember he called himself "Jungle Dave."

Leo: Jungle Dave, that's right.

Steve: And he was the founder and creator and evangelist. And I'm sure it was good for him that he was able to sell Jungle Disk. But, unfortunately, it doesn't seem that it's been good for some of its long-time users. So I was sorry to hear that. But there are alternatives now.

Leo: Yeah, do listen to that show because everything has a - there's pros and cons on all of the things.

Steve: Yes.

Leo: And Carbonite's a sponsor. It's not necessarily the right choice for everybody. Some people prefer pay-as-you-go. Some people want to have external drives. And there's all sorts of things.

Steve: Yeah. And we know that we do not have a homogeneous set of users. We've got all kinds - varying skills, various needs, varying configurations. Some people want to get things remotely. Some people want web access. So there is a spectrum of different solutions available.

Leo: Our next question from Scott Reeves in Phoenix. He shares his OAuth/Facebook login idea: I heard last week's Q&A where you discussed your concerns with the Facebook login spoofing, and I had an idea. What if Facebook combined their login with a CAPTCHA of several of your friends' faces? Hey, that's a good point. They know our friends, don't they. People could instantly recognize friends' faces, in theory, and it would be very difficult for bad guys to spoof. I don't think it'd be much of a burden on users to recognize their friends as long as it wasn't somehow taken as a product endorsement. Thoughts? Hey, I like that idea.

Steve: It's a cool idea. I mean, this follows on the very valid point that I think was raised, that one of our listeners raised, probably the last Q&A we did, was where the point was made that what's becoming very much in vogue is when you go to a site and it says, oh, would you like to log in using your Twitter ID or your Facebook ID or one of the other accounts that you probably frequently use. And so, because it's such a simple and easy thing to do, rather than create a new account in that other place, people are doing that a lot. They just say, yeah, I want to use my Facebook login. So that's the danger is that you're clicking on that site. It's bouncing you over to Facebook to authenticate. And the problem comes that, if that site were malicious, it could easily bounce you to a Facebook clone login and then capture your authentic Facebook data. And so what Scott noted, and I was put in mind of, Leo, I think it was your BofA, remember years ago when they were, like, showing you some picture.

Leo: SiteKey. They still do it.

Steve: Okay. And the problem there is that you're having to provide them with that or choose from among a grid of, like, puppies or kittens or whatever.

Leo: You choose, yeah, yeah.

Steve: Giraffes. And here Facebook does have information that they could show you that you could expect them to be able to show you. Now, this is a good idea. And I like this. The problem is that, again, it's the nave user that we're trying to protect themselves from. And I just don't, I mean, this puts me back in mind of recognizing that there is always going to be a tension and a problem between convenience and security. And this notion of one click bounce to another site, it is really convenient. But I don't think there's a way to make it secure. What Scott suggests is a nice idea. And again, it's worth doing things that improve security, even if we can't get to a hundred percent. And I don't think we're going to get to a hundred percent. But it's neat to make it better.

Leo: Yeah. No, we're never going to get to a hundred percent. You can think of man-in-the-middle attacks and stuff like that. Keith Takayesu in Ottawa, Canada wonders about breaking passwords into bits: Steve, I love your show. Thought you might be interested in this article. It's from the MIT Technology Review: "To Keep Passwords Safe From Hackers, Just Break Them Into Bits." And it's a long URL.

Steve: Yeah. A number of people picked up on this and were tweeting it to me. So I bet you Ars Technica and other people also picked up on the story. So it's probably around a bit. This actually is what I was referring to at the top of the show about RSA having developed something that they call "distributed credential protection." And the short version of it, I mean, it is deep crypto. But the idea is do not store - it's exactly what it sounds like, distributed creden- distributed - I'm tripping over this - distributed credential protection. So do not store all of the information about a person's credentials, like their login password credentials, on a single machine. Arrange to spread it around so that, in order to obtain all the credential information, you would have to attack multiple different servers.

And they even talk about, in their description of this, RSA's description, that you could have the credentials stored on different OS platforms so that, again, even if there was a vulnerability that affected one OS, it wouldn't be applicable across their distributed protection suite. And there's additional technology which apparently changes the way the credential is distributed among its different nodes over time. So if you attack one of these nodes that had part of the credential, and then later attacked another node, the fact that it hadn't all been done at the same time would also prevent it from working.

Now, RSA has applied this for their own use, and they're going to be offering it on some terms for sale in the future to enable companies to better protect themselves. I'm a little skeptical about what this will really mean in the real world. I mean, this is cool technology. And in fact we've discussed something like this many, many moons ago. I remember when we were talking about, like, it was how could you control access to information by a group of people where you want more than one person to be required to access something.

Leo: Yeah. It was like, if I die, I'll give half my password to my attorney, the other half to my...

Steve: Yes. And, for example, say that you had three people, and you wanted access to require any two. So you would take a really long password, and you'd break it into three pieces, and you'd give the first and the second piece to the first person, the second and the third piece to the second person, and the first and the third piece to the third person. So each of those people is missing one of the important pieces, a different important piece. Yet any two of them are able to reform the entire unbroken password. So we've talked about this kind of thing.

I'm glad, actually, because I'm sure that RSA has got patent protection on this. The good news is enough similar things like this have been done before that RSA is not going to be able to corner the market on this approach. And yes, I think this is a good thing that they've done. But look at the companies that are still just storing things in the clear or still saying, oh, no, you can only have a 10-character password, and it has to be all lowercase. I mean, we have a long way to go before we even need something like distributed credential protection.

It's nice to know that it's there. And for high-value login, for example, certificate authorities that really want to protect themselves, there are certainly instances of companies that are looking for the best protection available. And I would imagine this would make sense for them, whereas so many other companies just haven't even woken up to the idea.

Leo: Yeah. Interesting. Question 4, Michael Walther in Berlin - oh, a famous German name, wonder if he's related to the Walther PPK - wonders: No NFC? Are you sure? Bist du sicher? From what I found out so far about the A6 chip in the iPhone 5, I'm pretty sure it does have NFC. It's integrated in the A6 chip, waiting to be released via software, thus giving Samsung a harder time to clone it. Just my two cents. Yeah, it's not - so there's some - he's got it wrong.

Steve: Okay. I thought maybe you would know. I poked around and looked to see if I could find any confirmation of that rumor, and I didn't.

Leo: First of all, it's not - so the deal is that Apple is using a custom fab that's based on an ARM v7s platform, but it's completely custom fab. So unless he has a very good inside source at Apple, because I think this is probably guarded like Fort Knox, about what they put in the chip is not a standard ARM implementation. So is he basing that on a standard ARM implementation? Because I don't see where he would get that information.

Steve: Yeah. It caught my attention and my imagination because I love the idea of it being there, but unimplemented, so that at some point it could be in a future...

Leo: Does it need to be implemented at that level anyway? I mean, isn't it just software?

Steve: No, there would have to be a little radio somewhere.

Leo: Yeah, not in the system on a chip. It would be a separate thing.

Steve: It would be asleep right now. And then of course the other counterargument to that is, as the Samsung commercials are making very clear at the moment, Apple really does like to drag its users forward phone by phone by phone.

Leo: It's your parents' phone, is apparently what Samsung wants you to think.

Steve: Yeah, and so the fact is Apple may very well at some future time add NFC and use that as the reason to upgrade to iPhone, what, 9, 10, whatever they are at that.

Leo: Yeah. I mean, I don't - A, I think he's just mistaken about the capability of the chip. I certainly don't think we could know. But it needs to have some more hardware put in there, including a radio, which is not in there. So even if it were in the chip, they'd have to make an iPhone 5S or a 5N or something with a radio.

Steve: Yeah, and actually, as we discussed last week, NFC requires a short, small-wire loop antenna. And it has to have an electromagnetic field to radiate. It has to be a multiturn wire loop per the spec and per the frequency and radiation characteristics. And there's no way, there's no obvious way to conceal that. So anybody who did an iFixit take apart deal...

Leo: It's been torn apart, yeah. There's no antenna. There also is the issue of this being an aluminum back. And of course NFC does not go through metal. So Samsung and others have plastic backs...

Steve: In order to solve that problem.

Leo: ...in order to solve that problem. So in fact, once people saw the case, they said, oh, I guess Apple's not going to do NFC. We knew this because - I guess you could put it at the top or the bottom where there's still...

Steve: Oh, you can also - you could bump faces rather than bump butts.

Leo: Right. You can do...

Steve: Because, you know, I mean, it is a radio. The phone itself is a radio. So...

Leo: Right, there's ways to get signals out, RF out, yeah. That's a good point.

Steve: Right.

Leo: Anyway, there's no transmitter. There's no radio. There's no antenna. So there's no way they could just flip a software switch and make this thing NFC capable, sorry. Bad news. Russell in London with a tip for Verizon users. Oh, you know what, I just heard about this. And I am shocked. I'm so glad he brought this up. Colin Weir, our streaming engineer, or, no, I'm sorry, it was Josh Windisch just told me this. Verizon customers have 30 days - I hope that you've looked into this because maybe it's just Snopes worthy. But according to the rumor going on the 'Net, Verizon customers have 30 days to opt out - to opt out - from Verizon selling your web history and device location history to marketers.

Steve: Now, I am a Verizon customer. So I went to www.vzw.com/myprivacy. What I found was a page that said "Customer proprietary network information settings. Verizon Wireless and its affiliates (the Verizon companies) provide services to you."

Leo: Holy cow. This is the default is on. It's...

Steve: Yes, it is.

Leo: Oh, my god.

Steve: "In doing so we may collect certain information that is made available to us solely by virtue of our relationship with you."

Leo: Holy cow.

Steve: "Such as quantity, technical configuration, type, destination, location, and amount of use of the telecommunications services you purchase. This information and related billing information is known as Customer Proprietary Network Information (CPNI). The Federal Communications Commission and other regulators require the Verizon companies collectively to protect your CPNI. In order to better serve your communication needs and to identify, offer, and provide products and services to meet your requirements, we need your permission to share this information among our affiliates, agents, and parent companies (including Vodafone) and their subsidiaries." So on that page, after I logged in, it showed my two cell phone numbers, one for my BlackBerry, the other for my iPhone 4. And both of them were set to "Okay to share my CPNI."

Leo: Geez. Mine was, too. I just went there. I've never seen it before.

Steve: Yup.

Leo: Holy cow.

Steve: Yup. So anyway, for any of our Verizon listeners, vzw.com/myprivacy will get you to a login page. Log in and then, if you choose to say don't share my CPNI, you can select that and save that setting. So thank you, Russell.

Leo: Apparently this has been going on for a while, although I had not heard of it. Now, I just got a Verizon iPhone, so I wouldn't have known about it until now. But I've had a Verizon account for years. So apparently they've been doing this all along. That's shocking. That's just shocking. It's not, I mean, you know, it's one thing, I think Facebook and Google, which offer free services and need to monetize, that's one thing. I'm paying a hell of a lot of money to use this Verizon service. They make plenty of money off of me. And for them to...

Steve: And selling your location. It's like...

Leo: Horrible. Wow. Well, I just decided not to - I was waiting on the Galaxy Note 2 because I wanted to get a Verizon one. Nope. Although I wonder if AT&T is doing the same thing. Maybe Verizon is to be praised for at least telling people they're doing this and giving them a way to opt out.

Steve: Giving you an opt out, yeah.

Leo: Does anybody know? By the way, relevant mobile advertising right below it is defaulted on "It's okay to use my demographic info for banners"? I mean, there's stuff you may want to look at here. At least it's all on one page.

Steve: Yeah.

Leo: Business and marketing reports, okay to use my information for aggregate - I guess aggregate's okay. I don't know. I'm going to opt out of it all as long as I can. I'm paying these guys.

Steve: Yeah. I think, if nothing else, expressing our sentiment is a useful thing to do, saying, uh, no. You get 100-plus bucks a month from me. That's more than you need.

Leo: Don't sell stuff. Yeah, don't sell my stuff to make more.

Steve: Yeah.

Leo: Good. Let's see, AT&T. The chatroom has given me a link for AT&T, too. It's a longer link, not as easy. "Customer proprietary network information restriction request." They're doing the same thing.

Steve: Yup, CPNI.

Leo: CPNI. You have to complete and submit a form to restrict AT&T's use of your customer proprietary network information.

Steve: Oh. And lick the stamp.

Leo: Yeah. Yeah. So you know what? Kudos to Verizon, because both Verizon and AT&T are obviously doing the same thing.

Steve: Yup. Well, and that means probably everybody.

Leo: Which means everybody is. Which means really we should praise Verizon for at least giving us a checkbox.

Steve: Yes. And letting us do it online.

Leo: And sending us an email. Yeah. Holy cow. That sucks. And you have to do it for each of your AT&T numbers, by the way.

Steve: Yeah. Actually, in the case of Verizon, it says all cell phone numbers.

Leo: They show you them all. But on AT&T I have to know my numbers, go through them, and one by one check them.

Steve: Multiple stamps to lick.

Leo: Rethink possible. "We were unable to match the account and zip code." Oh, they are evil. Evil, evil, evil. Oh, it's not your phone number. It's your customer ID. Go ahead and try to find that.

Steve: Oh, yeah.

Leo: Holy cow. Thank you for bringing that one up, Steve. Shocking. And Russell in London. Wonder how Russell in London knows? Maybe it's London U.S. Maybe it's

New London. I don't...

Steve: It just said London.

Leo: London, I presume England. He's an expert on U.S. privacy issues. Lance Reichert, who is re-crossing the Adirondacks, wonders about hashing speed improvements. That's what happens when you go on long walks.

Steve: Well, and you've got to get back to the other side, so.

Leo: Announcing new faster secure hash! A couple of months ago you were discussing hashed storage of passwords, emphasizing that proper storage used hundreds, if not thousands, of rounds of hashing to make the generation of rainbow tables prohibitively expensive. This made sense. But in the Security Now! episodes both before and after the announcement of the new SHA-3 algorithm, it seemed that its chief benefit was that it's faster than the existing SHA-256. Surely the fact that Keccak has little in common with SHA-2 is a good thing, but have we stepped backwards as regards throughput? Lance, professional nitpicker and itinerant engineer.

Steve: So this gave me an opportunity just to, first of all, address Lance's point and to expand a little bit on the issue of strengthening that aspect of password testing. We've sort of gone beyond the point where what Lance points to is a problem. I think it is a very good thing that we have a strong, chosen, standard, agreed-upon, next-generation hash, which also has the benefit of being faster to implement in hardware and running faster and every bit as securely, we believe, as our current standard. We've solved the problem of speed by replacing iteration with, well, by using iteration in order to deliberately slow the process down.

One of the tools that many people use is a tool called "bcrypt," the letter "b," c-r-y-p-t. Bcrypt is often cited as a solution because, by design, they start with a very slow process. They actually use Blowfish, which was Bruce Schneier's invention. That predated Twofish, which predates Threefish and, you know, Red Fish, Blue Fish. And the reason they chose Blowfish is that it has a very slow key setup phase. So remember that, with all of these symmetric ciphers, before you can actually do any encrypting, you've got to feed in the key. And it's normally expanded to create a much larger array of bits which are then mixed in as the cipher iterates in order to perform its crypto function. In the case of Blowfish, that's a very slow process.

So bcrypt is deliberately designed to strengthen password hashing. But the cool thing about it is it's designed to be scalable from the beginning so that, as machines get faster, as GPUs get faster, as we continue this obvious evolution towards ever greater speeds, you can simply and easily turn up the number of iterations in a smooth fashion. Now, you don't need bcrypt to do that. You can use any iterative secure hash. And what's cool is that there's nothing to prevent you from storing the iteration count along with the hash. So, for example, so what's stored in the database is here's the hash that resulted from here's how many iterations. And so that doesn't weaken security at all to say this is how many times we iterated the user-provided password in order to result in this hash. Which means that it's trivial for servers to scale themselves up so that, as they get faster, and as the technology evolves, we just iterate more.

Now, it's true that, if you have a faster hash, that iteration count needs to scale appropriately. But who cares? You're basically tying up your machine for a certain amount of time, which is a burden for the good guys because you have to do that every time you need to authenticate. But that's much less often than a bad guy who's trying to do millions and billions of guesses of a password, who then has to iterate all of that many times for every single guess.

So anyway, it certainly changes the iteration count for hashing, if we get a faster hash. But at this point we should be, and for all intents and purposes are, we're past the point of not iterating when security is set up correctly, so it really doesn't matter. We just iterate more on a faster hash.

Leo: Speaking of hash, I'm just going to grind some more...

Steve: You grind away, Leo.

Leo: This is really cool. I have a...

Steve: I love the idea of a hand burr grinder.

Leo: Well, you know, it is. And it looks like it's ceramic in there, I mean, it's beautiful. It really is beautiful. And there's a certain - and it smells good. There's a certain joy - should we send one to Steve? Steve, we're going to send this down to you.

Steve: Oh, cool.

Leo: You already have, well, we'll send it down. You can do the ad next week. I shouldn't have probably opened this because then we could have sent it as a gift box. But we'll repack it up.

Steve: Hey, I don't mind if it's regifted. That's fine.

Leo: Mmm, it smells good, too. I mean, that's kind of - yeah, I like that. That's cool. Speaking of hash. Ricardo in Brazil wonders and worries about the NFC threat we talked about last week: Steve, I was very concerned about what you said. You talked about NFC being a new surface of attack for mobile phones - true. But I think you left out an important characteristic of NFC, which is to potentially replace all the contactless cards, that is, the standard credit cards we may already have in our possession - payment cards, corporate facilities entrance badges, transport cards, and so on. The interesting thing about NFC is the presence of a "secure element," which is a microprocessor with an application behind it that interprets commands coming from the reader and acts upon it, even by rejecting the command should there be a failed mutual authentication.

So my question: Considering that smartphone mobile NFC is just replacing something that has already existed, which is acknowledged to be completely insecure, is the possibility of using the handset as a reader/P2P device the main new threat? Or will this card emulation, with new players like Google, or maybe even the mobile phone companies that are not used to operating within a secure environment, posing a threat to the existing well-established ecosystem? He makes a good point. I mean, you're handing your credit card over to people. This is at least there's a PIN number, and there's a little more security involved; right?

Steve: Yeah. I think that, okay, so...

Leo: So is the problem then - what he's saying is, is the problem the technology, or the people who will be in charge of it?

Steve: I think he's also saying that he's sort of assuming that there's a way to put your existing contactless cards or replace your existing contactless cards with a phone-based NFC system.

Leo: I think that's the intent.

Steve: And so, yes, I think we do have a new threat because we are now, as we predicted we would be, we're talking about threats to smartphones, which are in the background, in the same way that there are threats to regular PCs. So that has happened exactly as we knew it was going to. And so, for example, there's no way for malware to infect a contactless credit card. I mean, it can't get in there. It's not prone to attack. Yet if you assume that responsibility with your NFC-enabled smartphone, so that it has your credentials, then we need to be really, I mean, really careful with the way this gets implemented.

So my concern is - I don't have any problem with the technology. But then we almost never do. We look around in the history of security problems is the technology being just what it is, technology. And it's always the implementation. Sometimes there are protocol errors. Most of the time it's...

Leo: It's implementation errors.

Steve: The designers forgot something or missed something or didn't see a backdoor.

Leo: You know, maybe I'm foolish, but I like Google. I think that Google is really engineering focused. These are smart people. So far they have not made any, and correct me if I'm wrong, security blunders a la WEP or UPEK. But so in some ways I would trust them to do an implementation of NFC.

Steve: Now, I did look at Philips's chips. Philips has a line of chips. It was a Philips chip they called the NTAG203 was a little, itty-bitty chip that was in the paper NFC labels that I had that I showed last week. And so that sort of got me into the Philips zone. And they actually have crypto available in this form factor. So although this NTAG203 didn't have active cryptography, it had the ability to lock regions of the EEPROM so that they were, after once written, they could not be rewritten, they could not be changed, they could only be read. But and so this particular NTAG203 chip did not have this higher level, what I think he's talking about, the so-called "secure element."

It does look like we will be seeing NFC devices in the future that may actually be performing more crypto. And I think that's all good. Except that doesn't solve the problem of smartphones still needing to be implemented correctly. And I agree with you. I think Google, so far they're doing a great job.

Leo: Yeah. I look forward to it. I think just the idea of replacing pieces of paper and plastic in my wallet with something a little more digital on my phone, I just like the idea.

Steve: And I think we're going to go through a rough patch, as we always do. But, yeah, being able to wave your phone at the gas tank and have it say, oh, I know you.

Leo: I'm ready. I'm ready.

Steve: Go ahead and fill up.

Leo: Yeah, and the way Google Wallet works is it does ask for a PIN. So it's two factor. You have to have the phone, and you have to have the PIN. That's more than my wallet. Lose the phone, it's not like losing your wallet.

Steve: Yup.

Leo: Stephen in Glasgow, Scotland shares his recent NFC experience: I think I know of a problem with NFC. When I first got my Galaxy S3 it would quite often beep for no apparent reason. Every time I put it in my jacket pocket or on my table, it would beep. Then I noticed it was when I put it on my table resting on my wallet that it was beeping. I felt like an idiot for not figuring it out. Some of my newer credit cards have RFID chips inside for the new contactless payment systems. We don't have these in the U.S. yet; or, if we do, they're in very limited areas.

Steve: Yes.

Leo: One of the problems I had, when you go to Europe it's hard to buy gas because our credit cards are dumb, and you need a smart credit card to buy gas. And the Galaxy S3's reader was shouting out, "Hey, I found a tag." And sure enough, when I downloaded an NFC app from the Android store, the beep would then be accompanied by the card info displayed on the screen when I put my S3 near my wallet. If these phones are going to go crazy when we put them near a wallet with RFID cards, no wonder Apple is holding back. As far as I can see, there is no way to tell Android to ignore a tag. And even if you could, would that use battery as the RFID tag in your wallet was constantly shouting out, "Hey, hey, I'm here," and your phone listened to the details before ignoring it again? Love the show. That's a great question.

Steve: Yeah. And again, I don't have a Galaxy S3, but I would be surprised if in the configuration...

Leo: Let me look.

Steve: ...you didn't have the ability to turn off NFC.

Leo: Oh, yeah, you certainly do.

Steve: And so what I would tell everybody, no matter what phone you have, if you are not actually using NFC on a daily basis, absolutely turn it off. Just turn off the antenna. Turn off the receiver. You'll save power, and you will clearly be more secure. If you do use it, then it's not going to be convenient to be flipping it off and on all the time until someone writes a little app that makes it easy to do that. And, boy, I really hope that we're going to see people implement a physical verification that you want a near field transaction before the phone just goes off and does it because we sure do need that.

Leo: There will definitely be that kind of thing.

Steve: Which actually leads us into our next question, surprisingly.

Leo: Ah, which is Brian in Michigan. He notes that NFC attacks are trivial with many current implementations: I was a bit shocked at your "benefit of the doubt" about NFC. There is no doubt because I would think it would be almost trivial to attack. Here is my quick scenario: Several of the implementations will automatically go to a URL in an NFC tag without any user interaction. There will be browser vulnerabilities to browsers in the phone. The attacker places several NFC tags that have been crafted to send victims to their attack site. They head to the airport, subway, or any other crowded location at peak traffic time. They "accidentally" bump into people. Most phones are in pockets, so it's the target height of the tags for the attack. The victim's phone goes to the attack site while never even leaving their pocket. The site takes over the phone to copy contacts, send premium SMS messages, destroy data, or whatever else they feel like doing. I may be a bit overreacting, but I feel NFC has all the security problems of QR codes - which can do the same thing - but with the added attack of not needing line of sight.

Steve: Yup. And I think Brian's right. I mean, again, this is why there's so much temptation on the part of the "gee whiz" people, ooh, look at this, just wave your phone past the poster, and then automatically, whoop, look, automatically takes you to the website. And it's like, oh, I know, but Brian's scenario will come to pass if we let things be that easy. You have to back off and say, oh, my NFC radio is off unless I'm using it, which is, like, first choice. Or it prompts me for do you want to go to this site and waits for permission before it does so. I just don't see a way around that.

Leo: Well, that's an app-specific implementation. I was trying to look at the Samsung TecTiles, but I don't have it installed yet. I redid my phone. But I'm sure that, for instance, Foursquare doesn't automatically check you in. It just takes you to that point. I'm sure that what it could do and should do is say, here's a URL, do you want to go to it?

Steve: Yeah.

Leo: Now, if the phone is locked - Tinfoil Hat says, as far as I know, Android NFC does not take action if the phone is locked. That is correct, by the way. You have to unlock the phone for NFC to work. I do know that for a fact.

Steve: Yay. That's a very nice...

Leo: That's sufficient.

Steve: Yes.

Leo: I mean, my phone is always locked when it's off. I press the Off button, and it locks it. So don't worry about it. You have to open the phone, unlock...

Steve: Well, do...

Leo: Do worry about it.

Steve: Do worry about it.

Leo: But, I mean, it's got it implemented in a way that is better than that scenario.

Steve: Yup.

Leo: Nathan Cooprider in Bedford reminds us that Russinovich gives us answer to AV problem in Episode 371: In Listener Feedback #151, our last Listener Feedback episode, Vern from the Bismarck Public Library - remember this? - shared his continuing frustration with all traditional antivirus products. You and Leo expressed sympathy, proposed some incremental improvements. But it seems like you felt a complete solution did not exist. But actually, Mark Russinovich actually mentioned and endorsed a solution when he was on the episode before. He calls it "whitelisting." I like whitelisting in general. A default-deny approach which only allows authorized apps will complement AV and address the issues Vern raises. By the way, this is what Apple's doing in OS X Mountain Lion. Whitelisting is the future of security as AV continues to falter.

I'll confess I'm a little biased here, since I work for Bit9. Our security product, Parity, provides the best whitelisting solution for endpoints and servers. But we aren't the only ones in this important space. He gives the link to his Bit9 v7. Be happy to help you with any research into this area, or set you up with people in our company who could answer questions, as well. Whitelisting has arrived and works.

Steve: Well, I saw Nathan's note, and I thought that we really - we sort of skipped over that and didn't really give much attention to it. And it's not something we've ever talked about before. While Mark was on the show I related the analogous situation, which Mark thought was actually a really good analogy, which was to firewalls, where in the beginning firewalls were to allow everything and deny specific protected ports. And we realized, oh, we're not good enough to do that. Stuff gets through. So now everybody is a deny everything and allow only those things through that we know we need to, which is the whitelisting approach as it applies to networking traffic. And Leo, I agree with you. This is the notion of the, I've forgotten the word, where you have someone tending a museum.

Leo: Curation.

Steve: Curation, yes. The curated model, where you have, like, corporate IT says these are the apps that we're going to allow you to run on your system, and we're locking it down. So...

Leo: Corporate IT or Apple Computer. That's exactly what the App Store does.

Steve: Well, and isn't Microsoft aiming there, too?

Leo: I think so.

Steve: I'm seeing some grumbling.

Leo: Not as dramatically. But there is an app store.

[Talking simultaneously]

Steve: ...completely wide-open frontier.

Leo: Right, right. There is an app store. But right now, if you upgrade to Mountain Lion on your Macintosh, you have new security settings that give you - now, the default is not the most draconian setting. But you have the option to - there's three options. You can say I will only allow applications downloaded from the Mac App Store. I will only allow applications downloaded - so that's fully curated; right? Apple curates.

[Talking simultaneously]

Steve: Yes.

Leo: Of course there's the argument does Apple, can Apple fully curate. But that's the presumption. Certainly it's better than just wide open. The second choice, which is the one I've made, and it's actually very easy, is not onerous at all, and it does have some security, is Mac App Store and identified developers. Apple has a certificate they give developers that they approve of. And I think that is a great middle ground.

Steve: Yup.

Leo: And you do have the choice of, yeah, you download whatever you want any time. But this is the same - now, Apple is fully curated on the iPhone. And without jailbreaking there's no way not to do that. Android is curated by default, but you can check a box that says allow third-party sources. So this is nothing new. The mobile platforms are already doing this. As is Microsoft on Windows Phone.

Steve: I do think that someday we'll look back and remember the days when you just ran whatever software you wanted to and held your breath.

Leo: Yeah.

Steve: Because it's just, as we've become increasingly dependent upon our systems, as we wire this all more deeply into the social fabric, we'll become - well, and as bad guys continue to be more and more aggressive about taking advantage of what used to be a free and open environment, we're probably going to have to be more conscious of the threats that exist. And I wouldn't be surprised if we see whitelisting becoming more and more relevant. And I have to say also, completely random, Bit9, when I saw Bit9, I thought, you know, I think there was a Bit9 graphics card for the Apple.

Leo: Oh, that sounds familiar.

Steve: For the Apple II. I think, you know, I just, like, oh, I bet you that that's the same company...

Leo: You think?

Steve: ...because I think they were in Massachusetts, he said. I tried to Google Bit9 Graphics because I was curious. But, I mean, this was, what, 30 years ago. So it's been a while. But I absolutely remember Bit9 Graphics, and I wouldn't be surprised if it was the same company. If Nathan is listening to this, maybe he can drop me a note and say, yes, that's us, we're still here.

Leo: What's the history of Bit9? Isn't that interesting.

Steve: Yeah.

Leo: Yeah. They're now in security, for sure, but maybe they were doing other stuff. That happens all the time.

Steve: Hey, I was doing light pens once. So things evolve.

Leo: That's right. That's why you know Bit9. They are in Waltham, Mass., so maybe it's the same. Steve, we've come to the end of our Q&A. Thank you so much, as always, for making this show possible. We couldn't do it without you. Steve not only spends a lot of time preparing the show and answering your questions, but he also makes, on his own, 16Kb versions available, audio, for people who just want the smallest possible file size, and pays to have it transcribed. And Elaine does those great transcriptions. Those are both available on his site, GRC.com. And if you want to thank him, well, just buy a little SpinRite while you're there. That's where you'll find the world's finest hard drive maintenance and recovery utility. Now for SSDs, too.

Steve: Yay.

Leo: Yay. He's also got lots of free stuff there, lots of security programs, information, diet information, "The Sugar Hill." People have been asking, when are you going to do Sugar Hill Part 3?

Steve: Leo, I get so much of that. We're going to have to do that. I've been continuously in ketosis now for six months, and it's the best thing I've ever stumbled into.

Leo: You're looking so thin.

Steve: We need to come back and revisit that.

Leo: And Dr. Mom is now steaming once again. Doesn't take long. Sorry, Dr. Mom. What else? Just lots of great stuff. Visit GRC once in a while. That's also where you can ask questions, at the feedback form there: GRC.com/feedback. You should also watch the show live because it's more fun that way. You can talk back. And as you can see, I refer to the chatroom, I use information from the chatroom. It's really great. By the way, the chatroom's saying that the graphics company was Number Nine, not Bit9.

Steve: Oh, that's correct, yes.

Leo: Very good. See? See?

Steve: Very good.

Leo: That's why you've got to watch live. We do it 11:00 a.m. Pacific, 2:00 p.m. Eastern time, 1800 UTC, at least until our summertime goes away. Then we'll be at a different time, but for now 1800 UTC. On Wednesdays.

Steve: And are we losing you soon for...

Leo: Next week I'm going to see Madonna. But I'll still be here on Wednesday.

Steve: Oh, that's right. So, yes, Sarah was talking about you not doing...

Leo: It's iPad Today I'm going to miss.

Steve: Right, right, okay.

Leo: No, and then I'm going away for a few weeks in November.

Steve: But not till November.

Leo: But that's November, yeah.

Steve: Okay.

Leo: And so I'll be back next Wednesday to do the show, 11:00 a.m. Pacific, 1800 UTC. You can get it after the fact, though. On-demand versions always available of all of our shows. Because really that's how we started. We flip-flopped it. I mean, really it was originally on demand, and you can watch us do it live. Now I want people to think, watch it live or get it on demand.

Steve: And look at where our listeners are, as evidenced by their locations that they talk about in the mailbag.

Leo: All over the world.

Steve: I mean, they're global. So many of them, Leo, I'm sorry to say, are asleep right now.

Leo: No, I know. And one of the things we do is we try, and we're trying, we're getting better and better at this, to do reruns. What we want to do is be 24/7. But we're live at some eight-hour juncture. But then repeat.

Steve: While we're awake.

Leo: While we're awake. And then repeat and repeat. So that, if you tune in at any time - we are not quite perfect at this yet. But the theory being, you tune in whenever it's appropriate for you and just watch for eight hours, you'll get everything. And if you do that every day, you won't miss a thing. You laugh, but there are people who do that. Dr. Mom is...

Steve: You'll get no work done, either.

Leo: I don't know. Yeah, exactly. So we've decided to make this as convenient as possible because I know that, if it's not convenient to watch or listen or participate, then you won't. So I hope you will. Thank you, Steve. We appreciate it. You're the best. Seven years down, seven more to go.

Steve: Absolutely.

Leo: At least.

Steve: You betcha.

Leo: Well, it was so easy doing the first seven, I could easily see going another seven. I mean, this first seven went by like that.

Steve: I didn't even notice it passing, Leo. It's all good.

Leo: Yeah. I don't know if I'll do a third seven, though. I haven't re-upped for three terms. I'll let you know. Hey, thank you, Steve.

Steve: We'll take it one seven at a time.

Leo: One seven at a time. That's good. I like it. Seven-year terms. There's something about seven that's good. Thank you, Steve. We'll see you next week on Security Now!.

Steve: Thanks, Leo.