SECURITY NOW!

Transcript of Episode #320

Listener Feedback #127

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-320.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-320-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 320, recorded September 28, 2011: Your questions, Steve's answers, #127.

It's time for Security Now!. The Kindle Edition, I have a feeling, this week. Steve Gibson is here. He is the man in charge at GRC.com, a security guru and expert. He's done 320 of these shows talking about protecting yourself online. And a good day to you, Steve.

Steve Gibson: Well, it would be 320 had we had the foresight of numbering from zero. As it is, we've done 319, and this one is #320.

Leo: I'm including this one. This is an extra one.

Steve: I'll tell you, it's those little details that trip up programmers an unbelievable number of times, like how many numbers are there between numbers 7 and 10? It's like, okay, wait a minute. Now, you mean inclusive or exclusive? Do we want to, it's like, is it 4 or is it 2 or is it 3? It's like, oh, got to be real careful with that stuff.

Leo: See, that's Steve for you, right there. He can turn anything into a teachable security moment, even numbering of podcast episodes. Did you watch - I'm sure you did - the Kindle announcement this morning? And I'm sure you had some thoughts on it.

Steve: Yes, I did. As we mentioned before we began recording, like you, Leo, I ordered one of everything.

Leo: No, I only ordered the Fire.

Steve: Oh, no kidding.

Leo: I'm tempted to order that Classic. Not the Touch. So there's three new Kindles, for those who were not paying attention. There's the new Kindle Classic, which is basically the same as the current Kindle except they kind of cut off the keyboard.

Steve: Yes, thank goodness.

Leo: They still have a jog thing and some buttons at the bottom, but nothing like that. And then there are still switches on the side, but they're smaller. Then there's the Kindle Touch, which is like the Classic, but you could touch the eInk screen to turn the page. And then of course there's the new Kindle Fire, which is a seven-inch tablet, looks a lot like a BlackBerry Playbook, but with specialized software on it.

Steve: And since you have given people the go-ahead for saying that the sponsored editions are really not obtrusive, we should mention that there is now a $79 Kindle. That one that has the XY, the little what-do-you-call-it, navigation pad down on the bottom, and then buttons on the side for turning the page, which I think is going to be my absolute favorite Kindle. It looks like the color is silver, too. It's not either that graphite or the white. So I think there's a new color. But $79. So they've broken the hundred-dollar barrier by a good margin for a top-of-the-line eBook reader. Although that's WiFi-only, I think.

Leo: It is.

Steve: So not 3G.

Leo: But again, not something that bothers me because I load it up with books before I hit the road. So I'm usually pretty happy on it. So that's interesting. You ordered one of each.

Steve: Yeah, because I have, I mean...

Leo: Now, how many Kindles do you have? You have a DX. You have one, two, three generations...

Steve: I have two DXes because I wanted one of each color. I don't remember why now. Oh, because there was a second - they, like, updated the DX to something that was supposed to change the screen fast or something. I said, oh, well, that sounds good. So I got two of those. I have my first-gen, the second-gen, the third-gen. And I got them in white because I like that better than the graphite color. And, I mean, I actually - I really use my Kindle when I'm - the first two Honor Harrington books were read entirely on my Kindle 3.

And I'll be switching to the one without the keyboard. I like the small size. So it's mostly just screen that you're getting. And then you hold it and then just flip the pages with your thumb sitting on the edge of the device. So I think for $79 it's going to further accelerate what Amazon is doing with the Kindle. And of course I did also pre-order - oh, and that comes tomorrow, by the way. This new one, the $79 one, is available for immediate shipping. So I'll have it tomorrow and be able to talk about it next week.

Leo: Now, of course one of the things that we knew that you would be talking about on today's episode is the new Kindle Silk browser.

Steve: Yes.

Leo: Go ahead. I mean, this is a browser that's somewhat like Opera Mini in that it intercepts all your browsing on the Amazon EC2 cloud servers. And then, if it's got a cached version, it sends you the cached version. And it also does, it sounds like, some digesting of the content.

Steve: Well, yeah. What Opera Mini does is they do things like deliberately re-render images, knowing that it's going to go to a mobile device. So very often websites will have large images which are dynamically downsized for, like, when it gets to - after it gets to your browser, then the browser sizes it down to the size specified in the HTML content, which wastes a lot of bandwidth and of course slows things down.

Here, I've read everything that's available online at this point since this morning. And there isn't a lot, and there is some ambiguity which I think is a consequence of them just trying to dumb it down for the typical Kindle Fire user. So what's controversial is that they do seem to say that they're going to be filtering secure connections. Under the Amazon Silk info on their topic, "What about handling secure HTTPS connections?" they say, "We will establish a secure connection from the cloud to the site owner on your behalf..."

Leo: Aha.

Steve: Yes. Aha.

Leo: Although I'm telling you, I read this paragraph, too, and I have no idea. So I'm very curious what the hell that means.

Steve: "...for page requests of sites using SSL. Amazon Silk will facilitate a direct connection between your device and that site." So we don't know what "facilitate" means because then they say, "Any security provided by these particular sites to their users would still exist." It's like, okay. Then, elsewhere, under their Terms & Conditions, they say, "You can also choose to" - and this is good news potentially. "You can also choose to operate Amazon Silk in basic or off-cloud mode."

Leo: Oh, that's good. I didn't know that. That's good.

Steve: Yes. "Off-cloud mode allows web pages generally to go directly to your computer rather than pass through our servers. As such, it does not take advantage of Amazon's cloud computing services to speed up web content delivery." So users can opt out of having Amazon essentially being a man in the middle.

Now, one thing that is possible, and I'll know - the day mine comes I'll know everything about it. But that's about six weeks away, so we're not going to know everything about it for a while. But it is also possible that using the Amazon filtering would actually increase your security in the case of being an open WiFi hotspot because we would have to imagine that Amazon's services will establish a secure connection to the Kindle Fire tablet and then negotiate even insecure connections from its cloud services out.

So we ought to back up a little bit and explain that what Silk does - and they call it "Silk" because they say a silk thread is invisible but strong. So they're saying that their - I was hoping they were going to do more than I think they are. I was hoping they would actually be rendering pages on their servers and sending us post-rendered or pre-rendered content. That would be exciting because it would mean that our Kindle Fire tablets would be completely protected from security problems. That is, if the rendering is actually being done by Amazon servers, then we're not subject to infection through any browser problems. For example, they'd be running JavaScript there rather than locally. Well, I just don't think that's practical.

So what they say they're doing, and I also listened to their 5.5-minute video where they pretty much only repeated what they already had in print, they talk about how - and we've talked about this often. The model of a browser interaction with the 'Net is that you download the page's HTTP content, and then the browser parses it, figures out all the other things that are necessary, and then sends out requests far and wide, often having to look up, do DNS requests to get the IP addresses to make the connections, negotiate connections, which will be slower if all this is over SSL for encryption, then go and get all of the content and so forth.

So what Silk does at the least is you have one connection between your Kindle Fire browser and Amazon's network technology and web servers and so forth in the cloud. So you request the page. Amazon fetches the page and all of the assets. They're able to do DNS lookups much faster. They're sitting with peering relationships with all of the main backbone providers. They, in fact, often are hosting the websites that you're going to, so you even stay within Amazon. It never even leaves their big aggregate services.

Leo: Because so many people use their EC2 and S3 services.

Steve: Precisely. So potentially your requests for all these other assets don't even leave them. They're instantly available. So Amazon pulls it all together and then shoves it all down in a single response to your browser. And we'll be able to play with this. We'll be able to turn it off and on and see how it feels. The immediate concern that people had was that even absent the issue of them intercepting SSL, which they have to do in order to do what we just said, but even if SSL wasn't brought into the picture, there's a privacy concern because everything is going through Amazon. We know that they're doing tracking and polling and content filtering and no doubt building statistics. And they talk about how, if they notice that most of the people who go to The New York Times home page then click on a certain link, they'll recognize that the chances are - and I think they used the metric 80 percent - that you're going to click on that link. They'll preload that down this back channel to your browser so that the content is already there.

Well, that's some cool stuff. So if the experience really was much snappier with this on than off, then users would at least have the option of having a faster web surfing experience. The problem is that people may be concerned that bringing up a secure, like, form submission, assuming that Amazon intercepts form submissions, well, that would be username and passwords, which would be briefly decrypted at Amazon before being reencrypted from the cloud. I mean, basically Amazon's being an SSL proxy that we've talked about in various contexts over time, and they would be doing this with our knowledge and permission. But it can be turned off, if you don't like that. And if it doesn't make it that much slower, then maybe some users will choose to do that. It looks like a very nice device.

Leo: So it might even be that when you add all that stuff together it's actually more secure, especially since you might trust Amazon. They already have, in many cases, our credit card numbers. It's not like breaking - we don't even know if they break SSL. But if they break SSL, well, it's Amazon.

Steve: But I'm sure they're establishing a secure connection to your browser, which gives you total protection when operating in a WiFi hotspot for browsing things. And that's very cool.

Leo: So will you leave it on? Will you trust it?

Steve: We'll have to see how it works either way. I mean, if it's...

Leo: I think they're not clear. We talked about this with Opera Mini before. It's kind of a man in the middle. They have a certificate that they use when they go to the SSL site, and then you have a certificate with them. But they have, during the interim in the middle, access to all that content. And of course that's how they can cache it and squeeze it and so forth. If they do this. We don't know. It's not clear from their prose. I wish they'd been a little clearer what they're doing there.

Steve: Yes, because they say, "Any security provided by these particular sites to their users would still exist."

Leo: Well, but that could just mean it's still SSL.

Steve: Yeah.

Leo: It's just that it's our certificate and not theirs now. Right? I mean, they're all weasel words, and I wish they would just be very clear and say what they do. Opera does, so you can make that decision on the Opera browsers.

Steve: Yeah. And it must be, Leo, that they are doing this. Otherwise, why make it clear that we can turn this off?

Leo: Good point.

Steve: In order for it not to - if it had no downside at all, then they just probably wouldn't bother to have us turn it off. It's got to be for people who are concerned about it.

Leo: But then again, you have to just ask, "Well, do I trust Amazon?" Because they're the only people who'd have access to it as a man in the middle.

Steve: Right. Now, this tablet doesn't have 3G, so it's WiFi only. Right?

Leo: Right. Although we were speculating that that might be a next-generation version.

Steve: And apparently it has no Bluetooth.

Leo: Right. So you can't use battery life. Remember, they only get eight hours of battery life.

Steve: Yeah. So what I'm wondering is, what's the status about Smartphone WiFi tethering? For example, the iPhone 4 will do that now. But will it do it to non-Apple products?

Leo: Oh, yeah. A hotspot's a hotspot.

Steve: Okay.

Leo: So if your question is could I then use my smartphone as a WiFi access point, use its 3G, yeah, I'm sure you could do that. And that would solve that issue on those particular times when you wanted to, say at an airport or a coffee shop, oh, I've got to get this magazine before I get on the plane, you'd still be able to do that, yeah.

Steve: Right. And I did want to mention that the screen resolution, because I'm super sensitive to that issue - that's why I'm so excited about the iPad 3, where we seem to get increasingly confirmation that it's going to be quadruple the pixel count of the current iPad. The current iPad is 1024x768. iPad 3 is going to be 2048x15 whatever it is.

Leo: Maybe.

Steve: So it's going to be the same "retina display" that the iPhone 4 is now. I like the feeling of the screen on the Kindle Fire because in a seven-inch diagonal screen it has the same large-dimension resolution as the iPad 2, which is to say the iPad 2 is 1024x768. The Kindle, the new Kindle tablet, is 1024x600. So it's a 16x9-ish aspect ratio, so it's got the same horizontal pixel resolution in seven inches that the iPad 2 has in 10 inches.

Leo: And it's the same IPS LCD, which works so well on the iPad.

Steve: Yes, the in-plane switching. So, yeah, I'm glad it's on its way.

Leo: I think it's a hell of a product. I think they did the right thing.

Steve: And $199. So here we have a dual-core, state-of-the-art, full-day battery life, color LCD touchpad at $199. So that's really significant.

Leo: Yeah. And well below what we were hearing predicted. They showed some real aggressive pricing there. And I think that's what it's going to take. The teardown folks say that's about what it costs to build. But that makes sense. If you sell everything - it's a portal to buy everything on Amazon. So that makes a lot of sense.

Steve: And you may know this. We know that Amazon has an Android store. We know that it's, we think, Honeycomb based. Does this mean that you can run Android apps that you buy from Amazon on that tablet?

Leo: They showed Plants vs. Zombies. They showed Fruit Ninja. So, yes. But they have to be the apps that you buy from the Amazon store. I would guess. We don't know. But I would guess that they would not allow you to buy apps from third parties, including the Android marketplace. You have to buy them from Amazon directly because they vet them. They're secure. They probably can have a - I would guess they'll have a special Fire section that's written specifically for the Fire. They may even restrict you to that section. But they showed a lot of apps in both their videos and at the demo today. So, yes, absolutely.

Steve: Okay. So I restarted Firefox and was told that there was a new version. Oh, no. I went to see if there was a new version, and it immediately moved me from 6 to 7. So any users who checked, if they're still using Firefox 6, and you just looked under the Help About...

Leo: Well, since you asked, yes, here.

Steve: Exactly. And suddenly, whoosh, okay, now I have 7. And we were being told we were going to have superior memory management. And it looks like that's somewhat true. What I was finding with my handful, or large handful of tabs open, like 40-something tabs open, oddly enough, when I would unblank my system at the beginning of a new day, after it had been idle all night, it had used up about a gig and a half of memory. So Firefox itself was just slowly chewing through memory. I got out...

Leo: Geez. That's not good. You think it's a leak?

Steve: Well, 6 was. 7 does seem to be behaving itself better. So I'm glad for that. And then just after - in also security updates, just after we put last week's podcast to rest, Adobe pushed an emergency, out-of-cycle Flash Player update out. This was to deal with a number of security problems, one of which was an actively being exploited in the wild, and Adobe felt it was critical, cross-site scripting vulnerability which existed in all players before 10.3.183.10. So that is the current version, 10.3.183.10. You can go to Adobe.com/software/flash/about, and that will show you the current version number.

So I just wanted to give everybody a heads-up about that. I think probably all of our listeners are up to speed on Adobe updating itself and keeping itself current and themselves, but that did just happen just minutes after we finished recording the podcast last week. And Leo, I heard you talking, and I don't remember now which show it was, about the issue of secure boot. There was a flurry of issues...

Leo: Yeah. Microsoft announced that Windows 8 would be using UEFI instead of BIOS - actually it sits on top of BIOS - which is an Intel standard. And in fact Apple uses EFI. But this UEFI would validate the booting operating system. And in order to put a stamp that says "Certified for Windows 8" on your hardware, the hardware manufacturer would have to support UEFI and turn it on. There would be a way to disable it. But the concern was it would keep people from launching Linux or other operating systems on that hardware.

Steve: Right, which turns out not to be the case.

Leo: It's not.

Steve: Because you are able to disable it. So I wanted to make a comment, that this has been something that has been

moving along slowly, as everything Microsoft does regarding security tightening, because they want to make sure they don't horribly break anything. And so it's just very...

Leo: Right. But you don't want a bad guy putting a bug, a malware in the master boot record and have the machine blithely boot up.

Steve: Correct. So this is all based on TPM, the Trusted Platform Module. And the acronym itself, Trusted Platform Module, the idea is that all of the critical components that exist in your system would have - if you want to use this, if you want to take advantage of this, they all have to have digital signatures, and they have to be verifiable by the TPM module.

So the idea is that from the moment you turn the power on your system, the BIOS itself uses this Trusted Platform Module as the anchor. And we've talked about a lot recently when we were talking about Certificate Authorities and the way that works, and even the Convergence or the Perspectives approach that we talked about last week, where you had a federation of servers that were all giving you different perspectives onto the web servers that you were looking at in order to all agree about the validity of the certificates that they were offering. Even there, there was an anchoring sort of overseer whose private key you had.

So the point is you always have to anchor trust somewhere. And the problem with the traditional SSL Certificate Authority model is that there's too many anchors. There's 600 individual entities that we have to trust in order for us to trust the certificates that they all issue. Well, so with the Trusted Platform Module, that itself, this piece of hardware on the motherboard which has been carefully designed so that it cannot be attacked by software, it is the anchor. And so the BIOS says to it, do you know this hard drive? Has the first track of the hard drive or the boot region been altered?

And so the system is able to, step by step, sort of creep forward, verifying every phase of the boot process in order specifically to prevent it from booting if there's been any change to the boot record. Then it will check that the various core components of the OS, each one in turn, is digitally signed, verify the signature before it loads it into RAM. So it just builds this house of verified trustable modules step by step until the operating system gets going and is then able to implement all of its own security systems which are normally what a boot time rootkit subverts. It gets in there and, like, does an in-memory alteration of the kernel of the OS in order to subvert some of the functions before they're even used the first time. And so when this all works together, that kind of problem ends up being nipped in the bud. And so...

Leo: So this is all a good thing.

Steve: It's all a good thing, yes. It really is.

Leo: There was some concern in the early days of TPM and so forth that Microsoft would use this - and the same kind of concern that you're having now...

Steve: For control.

Leo: ...for control, so that Microsoft would prevent using Linux or prevent you from using a different operating or different word processor, for instance. Or TPM would be used to revoke documents after the fact, delete them from your hard drive, things like that. None of which has emerged. And it is a sensible thing. It's hardware security. And this is a good thing, locking down the boot process.

Steve: I mean, we could certainly argue that this is a huge annoyance. I mean, it's like...

Leo: Well, if you want to run Linux, yes.

Steve: Well, yeah, I mean, just sort of like it just adds more baggage. There's going to be some overhead in terms of boot time. I heard Paul, I guess it was you and Paul who were talking because I heard Paul just sort of like with his head in his hands, thinking, "Oh, who doesn't think this is going to misfire? And I'm going to be told that I don't have a trusted module when in fact I do and so forth." So it's like, and it is, it's more things to break. But sadly, this is what we've been brought to because the hackers are so good and our systems are so prone to this kind of problem. So this is the future. We'll all end up with this kind of trusted boot strapping in order to get our systems to go.

There was an interesting blog post because Moxie Marlinspike's Convergence.io, which was his Firefox add-on implementation of the Perspectives work from Carnegie Mellon that we talked about last week, many people said, hey, what about Chrome? It's available for Firefox. But I'm liking Chrome, and I'd like to have this, too. So I wanted to share with our listeners the blog posting from the Chrome guys who are in charge of this. And their posting dated September 7th was titled "Why Not Convergence?" And they said, "In light of recent events" - or he said, the poster. "In light of recent events, I've had several requests to implement Convergence in Chrome. For those who don't know and, frankly, for anyone interested in SSL, I highly recommend watching Moxie's talk on the subject from this year's Black Hat. You can also check out the project website.

"Moxie, having actually thought about the issue and coded something up, has already done a thousand times more to address the problem than almost anyone else." So he's given a tip of the hat to Moxie for this. He said, "But I don't think that Convergence is something we would add to Chrome. Although the idea of trust agility is great, 99.99 percent of Chrome users would never change the default settings. (The percentage is not an exaggeration.)" And thus, remember, Leo, how many times - the phrase I have coined is the "tyranny of the default" because we just know most users leave everything alone. It's sort of, if it's not broke, don't try to fix it.

So here's this guy who's able to monitor all the settings in Chrome because that's one of the natures of the feedback that Chrome provides them. 99.99 percent of them would never change the default settings. And he says, and that's "not an exaggeration. Indeed, I don't believe that an option for setting custom notaries would even meet the standards for inclusion in the preferences UI.

"Given that essentially the whole population of Chrome users would [therefore] use the default notary settings, those notaries will get a large amount of traffic. Also, we have a very strong interest for the notaries to function, otherwise Chrome stops working. Combined, that means that Google would end up [having to run] the notaries. So the design boils down..."

Leo: That's not good.

Steve: Yeah, "...the design boils down to Chrome phoning home for certificate validation. That has both unacceptable policy implications and very high uptime requirements on the notary service. It also doesn't address the two problems that Moxie highlights: internal servers and captive portals. It's not clear how either would work in this design, at least without giving up on security and asking the user. (Those two problems, captive portals especially, are the bane of many an idea in this area.)

"None of the above argues against allowing Convergence as an extension for those who wish to run it. We don't currently have an extension API for controlling certificate decisions, and I'm not inherently opposed to one. It would be additional complexity and something that we would have to support in the future, so it's not without costs. But mostly it's not there because nobody has written it, and I'm afraid that I don't have any plans to do so." So that's the status.

Leo: Good response, actually. That's a great, thoughtful response.

Steve: Yes, yes. Great response. And I think in our Q&A today I do address the issue that he brought up, so I won't preempt myself. But there are some problems with Convergence.io and Perspectives, which everyone who's looked at it closely recognizes, that we'll be talking about in today's Q&A.

I did want to note that I saw the news that the MySQL.com site was...

Leo: Oh, this one's horrible.

Steve: Was, yeah, breached on Monday, two days ago, for the second time in a year. Now, the first breach was a little ironic, and we did talk about it at the time. That was earlier this year due to an SQL injection fault.

Leo: Hoist with their own petard.

Steve: Exactly. Now, the nature of Monday's breach still remains unknown. It just happened. However, our friend Brian Krebs noted that administrative access to the site was being offered for $3,000 on an underground hacker site. So perhaps somebody said, oh, great, I'll pay three grand in order to have admin access to the site. And the nature of the breach was that, until it was removed, JavaScript code known as the Black Hole exploit kit was attempting to launch a series of known browser attacks against all of the site's visitors.

Leo: Wow.

Steve: So, whoopsie.

Leo: Was it a MySQL injection - it must have been; right?

Steve: No, well, the first time it was, definitely. But we don't know...

Leo: We don't know.

Steve: ...and no one has yet said how people got in there. It may have been that they decided, hey...

Leo: Could be something was left there.

Steve: Yeah. May have been. So under the title of - this is my name - "The Devil Made Me Do It!" alleged LulzSec member Cody Kretsinger was identified by the "Hide My Ass" (HMA) VPN and web proxy service, which acknowledged that it had provided information that led to Cody's identification and subsequent arrest last week.

Leo: Hide My Ass until the police ask for it.

Steve: Exactly. And that's why I wanted to bring it to our listeners' attention. Hide My Ass said it was complying with a court order requiring it to disclose the IP address with which Kretsinger had logged into its VPN service. HMA notes that its terms-of-service agreement stipulates that it will not be used for illegal purposes. HMA logs users' IP addresses at the beginning and end of their VPN sessions. So here's a real-world example of a company responding to a subpoena which then got a person arrested who was using this for some illicit purpose. So, whoops.

Leo: Whoopsie.

Steve: Yeah. And I did want to mention we're seeing, and I'm sure you're noticing, Leo, more and more Mac malware things beginning to happening.

Leo: That's sad.

Steve: Yeah. SANS reported that a Trojan horse program masquerading as a Flash Player installer has been detected in the wild. The malware, which targets Mac users, does not exploit a vulnerability but simply relies on users who do not have Flash installed clicking on the offered link. The Trojan disables some security software and installs a dynamic loader library with auto-launch that injects code into applications the user then runs. It also sends information about the infected computer out to a remote server.

And SANS Editor William Hugh Murray commented that "Adobe sets users up to be victim to such attacks by encouraging Flash-powered websites to offer it from their sites. While most of the sites that offer Flash of course are legitimate, the practice is a dangerous one." And so he says, "One should download Flash only from the Adobe site." And this put me in mind of that fantastic rule that I saw Brian Krebs write about. And I'll remind our listeners: Never install software you don't seek out.

Leo: Oh, very good. Perfect.

Steve: That is just a golden rule. Any time you are offered software, just, uh, no thank you.

Leo: Yeah, very good advice.

Steve: Don't install it unless you go seek it out. A couple little blurbs from the Twitterverse: Mike Lopez in Coconut Creek, Florida said - he tweeted - "Honor Harrington Book 3, 'A Short Victorious War,' is amazing." Well, I think he must have said that to taunt me because...

Leo: You haven't read it, Steve?

Steve: I know.

Leo: You've been saving it.

Steve: I have got to finish "FreedomTM first." And I will not, I refuse to start another Honor Harrington book because it just takes my life, and I just can't have that happen. So, and then Ken Knight in Michigan tweeted, "I'm listening to 'On Basilisk Station" - I'll talk about that in a second - "on Audible." He said, "@SGgrc is right. This is VERY" - in all caps - "good."

Leo: Oh, great.

Steve: And finally, and that's the first of the Honor Harrington series. And then many people tweeted about the old-school mechanical keyboards that they noted I'm using, which they were able to see on that KABC TV clip. And of course we've talked about this a number of times. These are my original Northgate OmniKey 102 keyboards that are now about 25 years old and going strong. I just - I love them, traditional clankety, clickety-clank keyboards.

Leo: Well, I've got questions. Oh, I'm sorry, go ahead. More tweets?

Steve: We have a few more. I did note that - I tweeted out the news before it happened, on Monday morning, that there was going to be a new, maybe interesting, sci-fi series aired and premiering, a two-hour premiere on Fox called "Terra Nova." I watched it, having TiVoed it, Monday night.

Leo: That looked really cool, except for it says it's a family show, which kind of scared me off.

Steve: Yeah. And...

Leo: It's like a Swiss Family Robinson meets the dinosaurs kind of a thing.

Steve: Yeah, it's like a Jurassic Park meets maybe Lost or something. There were some, you know, they were trying to set us up for some spooky, we're not sure, stay tuned to find out what happens about this, and so we're being teased forward. It's like, okay, well, Monday night's sort of a dead night away, so maybe. But anyway, I wasn't blown away by it. But I do have some information that will blow, hopefully, us away. This is not it. It's the one after this.

But Elaine wrote to me, our illustrious transcriber. She said, "Steve, before I forget yet again, I hear you having problems uttering the book title 'On Basilisk Station,'" because I had been called it ba-SIL-isk. And I had been careful to pronounce it correctly and was doing so wrongly. She said, "I'm starting to think that either you don't know what one is, or you've never heard it pronounced." And I said "Yes, Elaine, correct on both counts." "It's a legendary reptile reputed to kill with a glance, pronounced BAS-a-lisk," she did phonetically. Signed Elaine. So Elaine, thank you for that. It's Basilisk Station.

Leo: We know, by the way, from this that she's a Harry Potter fan because in book one of Harry Potter, I think book one or book two, he meets a basilisk.

Steve: Ah, cool.

Leo: Yes, there you go. Probably, considering that she transcribes it, when you pronounce something wrong, it probably grates on her greatly; right?

Steve: Yes. So my big news - and this was posted yesterday afternoon. Thanks to @fryguy451 for giving me a link to and the news: David Weber, the author of the Honor Harrington series, says, "According to my 'Hollywood representative,' we have officially closed the deal on the movie option for the Honorverse series. I should be seeing the contracts in the next few days, and there are a couple of other legal documents that need to be traded back and forth. But we have a deal.

"The studio involved is headed by people who have actually read the books, who like the characters, who know the characters, and who have pulled up blocks of actual dialogue from the books in face-to-face discussions with me to illustrate their understanding of Honor's character and the reason they're excited about the project."

He said, "Although the studio is a cutting-edge CGI/3D studio, what they said to me more than once when we were discussing the option is that 'All the special effects in the world cannot make a successful movie. Special effects make a visually satisfying spectacle. But a successful movie requires storyline, and a successful series of movies requires characters. It's the characters and the fully developed background of the Honorverse which have drawn us to this project.'" He said...

Leo: That's a good sign.

Steve: Oh, Leo. Oh, wait. But, see, you don't know how amazing these books are. Remember I was in tears as I was finishing the second one. I was so choked up, it was like, oh, my god.

Leo: I've been skeptical. I'm sorry, I just can't believe. They sound like fantasy books. But all right. I mean, I know you have good taste, so...

Steve: Oh, I haven't steered you wrong yet.

Leo: Not yet. Not yet.

Steve: And he said, "The producer and the studio are the same entity, which is going to preclude or at least hugely reduce the kinds of pissing contests producers and studios can get into. They have not simply hired me on as a creative consultant, but we've already been in fairly intensive coast-to-coast video conferences about the characters and the story line, and they are clearly listening to me. They are thinking in terms of not a single feature film, but a series of films."

Leo: Well, how many are there? There's like 20 of them; right?

Steve: There's 12 books.

Leo: 12, all right. By then there'll be 20.

Steve: But oh, my god. And he said, "...based not on generated-for-the-movie plots but on the actual storyline of the series."

Leo: Oh, great.

Steve: "As a result, they have a very strong interest in treating the characters and the story line with respect." And finally he said, "The critical thing to me is that these people are interested in the Honorverse and in the characters who live in it, and they clearly don't see it as the opportunity to make just one movie and then get out. I think these people are going to treat Honor and the Honorverse with respect, and they clearly really, really know the characters and the books."

So all I can say, listeners, is that David Weber's Honor Harrington series, it's among - it's different than any of the other stuff we've talked about. It's yet another sort of dimension of sci-fi genre, different than the Lost Fleet series, different than the Peter Hamilton stuff, different than the other books we've talked about. But it's some of the best fantastic space opera I've ever read. And, oh, goodness, the idea that we're going to have these as movies is beyond exciting. So I will say again, I encourage everyone to read these. And the first two are available for free as eBooks.

Leo: [Yawning] Oh, I'm sorry. I've downloaded "On Basilisk Station" from Audible, and I will listen. I'll be listening to it as soon as I finish my current book.

Steve: Good, good.

Leo: So I'll give you a book report.

Steve: Yes, we need to hear what you think, Leo, because so far I'm the only one raving about it.

Leo: No, you've got the correspondents love it, your Twitter fans.

Steve: That is true. We have had that, too. A listener, Mike Goodrich - his subject was "Happy User" - was able to save a USB drive from the trash can. He said, "I've owned SpinRite for years, but never used it much. (Takes too long to run, does it really work, et cetera.) The boot CD just sat on the shelf.

"Yesterday one of my important USB hard drives failed to read. I believe the problem was caused by too much fragmentation, and the drive got too full. And he says, "(Thanks, Microsoft, for your inadequate defrag utility.)" And he said, "I said, what the heck, I'll try the SpinRite CD and see if I can do anything. Yep. In less than two hours I had a working drive again. SpinRite had never seen this drive before. It just went in and did the repairs. Well worth the 89 bucks that I spent several years ago for the program. Thanks." Mike Goodrich, Columbia, MO - what's that? Missouri. Columbia, Missouri.

Leo: Missourah. I'm from Missourah, he says.

Steve: So thank you for the report.

Leo: Well, and thank you, Steve, for your questions and answers. We've got them coming up in just a sec. All right. I have questions, if you have answers.

Steve: Yeah.

Leo: I'm ready to launch into the Q&A portion, #127 in a continuing saga of, "Wha....?"

Steve: Which, by the way, is seven 1-bits in binary, Leo.

Leo: Oh, that's right: 111 111 1 0.

Steve: Actually be zero, if we're going to have a byte...

Leo: I'm sorry, 01111, yeah, yeah. The other way around. Matt Bailey, who is @VidioGeek with an "i," says: Steve, if people are testing potential real passwords on your Password Haystacks page, shouldn't that page be secure, using SSL?

Steve: Many people have asked, and so I just wanted to take a moment to say that the link on the menu at GRC is HTTPS, and so I do have the page come up on HTTPS. But I don't force it, if for some reason somebody wants a non-HTTPS connection. It is not a concern, though, because that page never transmits anything. That is, the passwords are - they exist locally in the user's machine. So it's just the browser and local JavaScript which is running that does all of the computation and all of the calculations. There's no conferring back and forth with GRC. Now, having said that, HTTPS is potentially significant because you would like to make sure that the JavaScript code is not altered on the fly. So if the page is...

Leo: Ah, good point.

Steve: Yes. So if the page is not secure, then it could be altered to drop HTTPS from the JavaScript. And then when that's coming in, it could be altered in order to send the person's passwords out. So bringing up HTTPS is a good thing. I'm sort of transitioning to move GRC to 100 percent enforced SSL. I'm doing it incrementally to make sure I don't break anything in the process. For example, the Off The Grid site, all of its pages live underneath the OTG directory, and that directory itself, it has enforced security so that every page there is. And so I'm experimenting, and over time I'll be moving more and more stuff over to the point where eventually you won't be able to get to GRC without being over SSL.

Leo: Good.

Steve: Which, you know, more and more sites should over time.

Leo: Yeah, I think that's great. I'm glad to hear it. Question #2. Wait a minute. I put them away. Let me bring them back. From Seth Anderson in Fruitvale, Texas. He has lost his fleet. Uh-oh. Thank you, Steve, for recommending so much of The Lost Fleet series. I ordered them a couple of weeks ago. When I got home after church last Wednesday I found them waiting for me. I literally could not put them down. I was up till 2:00 a.m. Thursday morning reading the first one. I went straight home, hurried through my workout so I could start Book 2. I stayed up till 2:30 a.m. Friday morning reading it. I read book - this guy, man. I read Book 3 Friday night after work. These are not little tiny novellas, either, are they.

Steve: Unh-unh.

Leo: And started Book 4, staying up until 3:00 a.m. Saturday I finished Book 4 and read Book 5 that night, staying up until 2:00 a.m. again Sunday morning. Needless to say, I was very tired at church Sunday morning. As I was able to read some during the day, I was only up till 1:00 a.m. Monday finishing the last book. I loved them. Oh, my goodness. While recent events kept me from a long-weekend mini-vacation over Labor Day, the Lost Fleet provided the mental getaway that I needed. I mean, five books in three days. Thank you so much. I've been a regular listener since the Password Haystacking episode. Well, so he's a relatively new listener. That's great.

Steve: Yes, he's a new listener. So anyway, I just wanted to share that. I thought - the problem I've had when I've read books too quickly is I don't really feel like I get as much out of them as when I read a little bit and can sort of think about it, and then I'm anxious to get back to it. So I'm glad that my stair climber will be metering the rate at which I'm able to read the rest of the Honor Harrington series. The Lost Fleet series is great. Honor Harrington is better. So if anyone...

Leo: Really, it's better. Wow.

Steve: Oh, it's better. Oh, Leo, it's...

Leo: Don't tell Frank or...

Steve: It's really good.

Leo: Don't tell this guy. He's not going to go to church or anything.

Steve: No, Seth will drop off the map. No one will see Seth for...

Leo: Seth will waste away. Hey, this could be a good diet. Read all 12 of the Honor Harrington books without eating.

Steve: So, Seth, wherever you are, I know you finished the Lost Fleet. Know that there is a sixth book now. There's a next series beginning, but be aware that it is the next series. The Lost Fleet series is a single contiguous story spread out, which is of course why probably Seth didn't sleep for five days. The good news about Honor Harrington, you will not be left hanging. So don't fear. I mean, I really am annoyed when I start in on a series that isn't finished by the time I start them because I want them to all be there. The good news is these are not cliffhangers. And he also doesn't drag you through a lot of the prior book at the beginning of the next book, which I really appreciate. He very cleverly sort of tells you just as much as you need to know for continuity. But I just - we've got to get Leo to read the first one so that you can add your opinion.

Leo: Oh, I have it.

Steve: It's really good stuff.

Leo: Well, I could just stop reading what I'm reading. Actually I'm reading two books on Audible right now. One is a history of the Inca Empire. That might take a while.

Steve: Okay, yeah, forget that. Stop that. That's ridiculous.

Leo: The other one is "American Gods," which is kind of a dramatization of a classic Neil Gaiman book. But maybe I'll pause that and - it won't take me long to read the first one; right?

Steve: No. And then they're not huge tomes. Later on they get bigger. But, I mean, we need to know next week if you're sucked in, even if you haven't finished.

Leo: All right.

Steve: Although I bet you will.

Leo: By next week I will - all right. I will start today, and I will let you know.

Steve: See if you can.

Leo: And if I cry, I'll tell you. You don't cry for the first one; right? It's the second one.

Steve: No, the first one didn't make me cry. Second one I was verklempt, as they say.

Leo: Question 3 from Frank in Mnchen, Deutschland, or Munich, Germany to us English speakers, reacts to Moxie Marlinspike's Convergence: I love the idea behind Convergence. By the way, you talked about that last episode; right?

Steve: Right, that was last week.

Leo: People want to know more about that. I actually thought of a similar thing myself, so it's great to see I can come up with good ideas myself sometimes. But I have a question, and an annoyance in the implementation. What keeps someone from faking the responses from all of the notaries that you queried? Obviously, they're in different geographic locations. But if the man in the middle is your ISP, that isn't going to help. Are the notary responses encrypted with an asymmetric key for which you have the public key stored? That's his question.

Here's his annoyance: Convergence doesn't work with Intranet sites. Obviously the default notaries don't have access behind my firewall. I could of course have set up my own notary that has access to the sites, but then I won't have the advantage of using notaries in multiple locations anymore. Thanks for providing an excellent show. So why would you even want to use it on the Intranet?

Steve: Well, and that's been a very good point. This is one of the problems. Remember that the cool benefit of the traditional Certificate Authority model is that we trust these CA roots, and we trust everything they do. Well, that's the dubious part of that. The good news is that we're able to verify the authenticity of the certificates that they have signed ourselves. We don't have to ask anybody else any questions. So we have full privacy, and we're able to do this verification locally.

The whole problem with the Perspectives approach, which is the same as what Moxie has done with Convergence.io, the problem is the benefit. And that is we're doing dynamic trust, which means we have to ask somebody else what their opinion is. That has to happen on the fly. So that creates, first of all, a privacy concern because that somebody else we ask knows that we're doing so. But most importantly, it means there is non-web-related traffic. And there's a problem with many corporations that are now filtering everything. They run an email server inside their firewall. They run DNS inside their firewall. They proxy your web traffic. I mean, they are locked down tight.

So remember that this technology wants to send random UDP packets off. Well, many corporations just don't let you do that. So the whole Convergence/Perspectives system won't run at all inside of such a locked-down network. And that really is a problem for intra-web sites. But you are right, Leo. I think that the idea of having to verify the trust of a server that's in the closet next to you...

Leo: You've got a bigger problem if you don't trust it.

Steve: Exactly. Exactly.

Leo: Ken in New Orleans - did you answer his question, too?

Steve: Yeah.

Leo: Yeah. Ken in New Orleans wonders whatever happened to IPv5? We went from IPv4 to IPv6. I'm a new listener. I've been listening to past episodes to get caught up. Love the show. Happy user of SpinRite, da da da da da da. During your discussion of how the Internet works, you went over the creation of IPv4 and briefly mentioned that 1, 2, and 3 came before and were developed and obsoleted when the Internet was just in its infancy. My question is, with all the talk about needing to move to IPv6, whatever happened to 5?

Steve: Well, and that's an often-asked question because people who are somewhat savvy all know that we've been using 4 and that we're now talking about IPv6. What happened was that a long time ago in Internet history, in fact when IPv4, well, IP at all was still not very well known, we're talking in the '70s, there was another project begun to experiment, believe it or not, Leo, with streaming. Even back in the '70s there was this notion of, well, you know, we've got this all packetized stuff happening, so how could we stream voice and video? And whereas we've talked about how the IP system, IPv4 is based on packets that only have an IP source and destination address, and then they can contain other protocols within them. UDP, for example, is not connection oriented. TCP is connection oriented, although with a lot of buffering and really not oriented toward real-time streaming. So IPv5 was actually a streaming protocol.

Leo: Was it related to MBONE? I remember the MBONE Multitask.

Steve: No, that's multitask...

Leo: Multicast backbone.

Steve: That's multicasting; right. No, it predates that, even. It was, like, way back before any of us were on the Internet, before it existed really. They said, okay, IPv4 will have this architecture, and for streaming voice and video we'll have IPv5, where those packets, the IP packets themselves will have a completely different construction, and it will be inherently connection oriented. So it was - the idea is that the first four bits of the packet are the version number. So IPv5 would have a 0101 at the first four bits that came in, which would tell the routers what the rest of the packet was. And it wouldn't look anything like IPv4 because it would be entirely different, a streaming connection-oriented protocol.

So some companies messed around with it a little bit. IBM, NeXT, Apple, and Sun sort of considered implementing it and playing with it, but it just - it never got off the ground, never made it out of the lab, never was, like, really even at the point where it could be used publicly. And then it just sort of died. Nothing further happened. But the number had been consumed, and so it was no longer available. So we had to skip over it and do 6.

Leo: Question 5 we did not skip over. Dave Fugleberg from Minnesota provides some additional information about Moxie's Convergence.io implementation of the Perspectives concept: In Episode 319 you talked about Perspectives and Convergence.io. I heard Moxie Marlinspike's talk on this at AppSec USA today, and he explained a little about how his concept protects you from leaking your browser history. Basically, your client would encrypt the domain name you are trying to validate with the public key of Notary B, but proxy it to Notary B through Notary A. That way Notary A knows your IP, but not the domain you're checking; and Notary B knows which domain you're checking, but not your IP. The notaries would need to collude to match your IP with the domains you're checking.

The most interesting part of the concept is it's up to you as the user to decide which notaries to use, and you can change them any time. This is very different than the current CA system, where dropping a CA from your trust list can cause large parts of the Internet to suddenly be untrusted.

Steve: So this is a little bit like, I mean, first of all, I'm not surprised by that. It makes sense. And it's what I would describe as a kludge-y solution to the problem. I mean, it's better than nothing. And it's a little bit like The Onion Router, like the TOR project, inasmuch as your traffic goes to a first node that is unable to interpret what you want to protect about it and is forced to forward it on to another node that then is able to protect the next layer.

In this case we only have essentially a one-layer onion, that is, one layer of encapsulation, that being the domain name you're querying. But it does bounce through the first notary and then goes to the second. That one then, if it's going to obscure your IP, it would do the lookup for you, decrypting your packet using its private key, and then would return the response to that first notary that would reflect it back to you.

So it's like, well, okay. You are inherently going to have some privacy leakage with the system. It's what's so nice about, as I said, about trusting root authorities. And if you're going to do any kind of probing in real-time, whether it's this or if it's the OCSP technology which we already have, which is making per-site queries, you're going to be leaking the fact that you're going to those sites. There's sort of no way around it.

Leo: Question 6 from Matthew in London. He worries about insufficient entropy: Steve, I'm a little worried about the ultra-high entropy pseudorandom number generator you're writing for Off The Grid. This is exciting. You've promised us this. From what I understand, you're using the local source of entropy from JavaScript as entropy is quite scarce on a PC. This can be seen by observing /proc/sys/kernel/random/entropy_avail, which gives how much is available from /dev/random. Is this in Windows, or is this - this must be Linux.

Steve: That's Linux.

Leo: Yeah. Now, I'm not a security expert, but from what I understand from the theory of information, you cannot "create" entropy. So isn't the total entropy available to your PRNG dependent upon the implementation of PRNG in JavaScript? If so, I worry - he's from London, that's why he talks that way. He talks funny. I worry that the implementation of the default JavaScript pseudorandom number generator (PRNG) wasn't given enough scrutiny to be the basis for our Off The Grid system. I understand you've tested it against automated tests, but would it pass on all browsers? Regards, Matthew.

Steve: Okay. So he's absolutely right.

Leo: Isn't this why you're writing this, so that you don't use Java's PRNG?

Steve: Correct. Although, and this is where it's sort of confusing, and I wanted - it brought up an interesting point that I thought was a great opportunity for some clarification. There's two different aspects to a pseudorandom number generator. There's the initialization of it with starting entropy, and then there's the quality of the random numbers it generates once it's been initialized.

So, for example, say that you just initialized a high-quality PRNG to all zeroes. Well, if it were high quality, it would spit out the same stream of high-quality pseudorandom numbers every time you did it. Remember like in BASIC we had the "randomize" command. It would sort of cause the very poor random number generator that was in BASIC to start in a different place, at least, so that you would get a different set of random numbers each time.

So the problem with JavaScript is that its pseudorandom number generator is known - well, okay. First of all, there are different implementations on different browsers, on different platforms. Some of them are really not very good. And then the other issue is they may not be initialized with high entropy. So I needed two things. I needed a pseudorandom number generator that itself could possess enough entropy to allow us to reach as many of these Latin Squares, at least as many as the minimum we know are possible. And I also need, for that to mean anything, for it to be initialized with high entropy. Thus Matthew's question is a really good one.

And the source code that I've published so far is just sort of a simple demo that does initialize itself only from the local machine's JavaScript source. That is, it uses the local machine's JavaScript pseudorandom number generator to get itself going. The sequence of numbers it produces, however, from wherever you start it, we've now proven, is ultra-high quality. It passes every test of randomness, and many of them are excruciating. So the pseudorandom number generator itself has been proven.

Now what we need to do is make sure that, in production use, that we're initializing it with enough entropy. Otherwise we're not going to be able to access all of the possible Latin Squares that may exist. And there I will do what I have done elsewhere, which is I get a starting entropic seed from GRC over an enforced secure connection, so no bad guys can get to it. And then we locally alter it.

So the idea is - and again, Matthew is right - you cannot create entropy out of thin air. That is to say software cannot. Software is unable to produce pure entropy. But at GRC we will take, like, a starting pool of entropy to initialize the page. And then in order to get protection from GRC knowing anything about your grid, we'll then mix in the entropy from the local JavaScript PRNG and a bunch of other stuff, like mouse movements and size of your screen and, like, all kinds of other stuff that is unknowable by GRC. So you get the best of both. You get a guaranteed minimum amount of entropy because that - so you're not reliant on your local computer because that you get as an initial blob from GRC. And you get protection from GRC knowing anything about your grid because you immediately pour a bunch more entropy in on top of it. And we solved the problem that way.

Leo: Will in the United Kingdom wonders about disk drive deterioration, something you know a lot about because of course SpinRite. You've been a hard drive expert for a long time. Steve, I work at a software security company, and a discussion came up the other day when we were discussing backups. Now, I know it's foolish not to have backups of all my drives. However, I've taken the position that a hard disk drive that is in a locked drawer will not deteriorate or fail. At the office they said

I was foolish, and I should back up everything. However, why do I need to back up a drive I rarely access, and I know it's safe from knocks and bumps? Could anything happen to that drive in his drawer? He's got drives in his drawers.

Steve: Well, the one thing that can happen, if you do not use a drive for a long period of time, is stiction. You can actually get a molecular level, like a "weld," it's called, between the drive's heads and the platters. And that can be a problem. Traditional or contemporary drives have solved the problem, more or less. In some cases they move the head all the way in. In some cases they pull it all the way off of the disks.

What I have found is that the moment of truth for a disk drive is when it is first starting up because, if anyone has listened to drives, they go through a lot when they're starting up. They're full subsystems. I mean, the idea that they store the kind of data that they do still boggles my mind. And they're just not as simple as drives used to be. Drives used to be a motor that spun the disk, and then another motor that moved heads in and out, and then wires had amplifiers hooked to them in the drive. But that immediately went out to the controller. So there just wasn't much that could go wrong in the drive. Today's drives are full microprocessors, amazing microcosms of technology in this little box. And sadly, there is a lot that can go wrong.

So, I mean, on one hand I feel that your drive is going to last longer in a drawer than maybe if it's spinning 24/7. But you still just never know when the drive is going to die. So, Will, I have to sort of agree that there is no substitute for a backup, which is - that's the wisdom that Leo and I follow and what I would really recommend to everyone. If there's only one copy of that data, it's just not safe.

Leo: And of course there's always theft and fire and all that stuff. But I guess the other question that comes to mind now is, well, assuming no stiction or startup issues, is it possible that the magnetic media would deteriorate over time, that it would start to lose its signal or whatever?

Steve: I don't think so. What used to happen was that drives did not have servos on them. That is, or the servo platter was on - it wasn't a platter. The servo information was on a separate layer or surface in the drive. And you could get some mechanical wear and tear that would cause the alignment of the head to drift over time, which is one of the famous things that SpinRite did. Because it was able to re-low-level format the drive, it would electronically realign the drive. Well, that just isn't - that doesn't happen any longer because all drives have servo, that is, head positioning, head tracking data mixed in with the data so that they're self-servoing, essentially.

So I just - and I don't really think that you do have bit decay over time. The technology is such that it's really very strong. SpinRite, running it on SpinRite does reread and rewrite all the data to sort of reverify and make sure that you're not having any problem with defects. But typically it's the head flying over the surface that does create a little bit of wear. Just it flying over is putting some wear on the surface. And that can grow defects over time. So you could argue that having it not running in a drawer is better. But I still don't think there's any substitute for having extra copies of it, if it's really important.

Leo: Right. Question 8 from Karl Kranich in Indianapolis. He wonders about Latin Square mobile apps. This is your password-generating technique. Some people seem to be suggesting Latin Square mobile apps that don't also involve printing out the square. Is there any point to that? Don't they just need a hash algorithm that's keyed to a password and has a 12-character output? In other words, he's saying your whole idea of your portable passwords is they're non-electronic, Off The Grid; right? So if you're putting them on a mobile device, well, clearly they're on the grid. And at that point, why do you even need to do Latin Squares? Just do a hash.

Steve: Exactly. And he's right.

Leo: Of course.

Steve: I mean, you could certainly do that. The advantage, I think, first of all, there's a disadvantage of Off The Grid being on the grid because then it's potentially subject to somebody - to a malware attack, to somebody getting it. The flipside is it's convenient to have Off The Grid on the grid, that is, to have it automated, because you could just put in a domain name, and it would give you the matching password. And then the benefit of that, which you don't have with a hash, is that it's still an electronic version of a printed grid, so you have that as backup. So if you ever had a device that didn't support the Off The Grid system on the grid, then you'd still have it as a grid in your wallet, for example. So it's sort of the best of both worlds, which you don't get if you have to run a hash algorithm. Lord knows how you'd do that on paper. I don't think you really can.

Leo: All right. Put your beanie on now because we're going to get a little wacky. This goes back to our conversation last week about the Monty Hall dilemma. Marv Schwartz, who is at Case Western Reserve, so he knows where he's talking, he says: The source of the Monty Hall problem is provided on Wikipedia in the article about Marilyn vos Savant.

Steve: Whose name I haven't heard for a long time. Remember her?

Leo: Yeah. She used to write a column in Parade. I've interviewed her. She was billed as the smartest woman in the world, and she would pose these really tough brainteasers in Parade. I think it was Parade magazine.

Steve: It was. Good memory.

Leo: So here you go. Assume - I thought we did a very good job describing it last week. But anyway, assume there's a shiny new car. See, he's already left out the most important part. You're playing "Let's Make a Deal." Now, if you've ever seen that TV show, they give you three doors, and there's prizes behind each, but you don't know what they are. Presumably, in fact for this to work, Monty has to know what they are.

There's a shiny new car behind one of the three doors in front of you, goats behind the other two. The key to understanding the answer is that initially you have one chance in three of choosing the car. Three doors, 33 percent chance of success. But Monty knows, see, Monty knows what's behind every door. He's the host of the show. After you pick a door, now there's a 100 percent chance that one of the remaining doors has a goat. He opens a door that he knows has a goat behind it. This gives you no new information, and your initial odds don't change. There's still a one in three chance that your initial choice was correct.

When asked whether you want to keep your initial choice or switch, this is the key. The odds are not 50-50. Nothing changed your initial one-in-three odds. Therefore you double your chances of winning by switching. I know that seems counterintuitive. But the point is that Monty has added information into the pot here because he knows where the car is. You had one in three. You had a 33 percent chance of picking the right door. Now, by eliminating a door that has a goat, Monty is saying you now have one in two.

Steve: Right.

Leo: David Singer, a wonderful professor of mathematics at Case, helps people see this by taking a deck of cards and asking to pick one without looking at it, then asks if they would bet even money that they chose the ace of spaces. Of course they won't. The odds are one in 52. He then takes the remaining cards so that only he can see them, placing all but one of them face up on the table, boom boom boom boom, except for one. He then asks if they would bet even money that they have the ace of spades. Nothing's changed the odds. They're still one in 52. Hopefully people can see this.

The Monty Hall problem is exactly the same. One car - he's not helping. This is not helping, I can tell you right now. One car card and two goat cards, pick one face down. The odds are one in three you chose the car; right? I pick up the two remaining cards so that only I can see them. There's a two in three chance that I have the car and a 100 percent chance that I have a goat. The odds that you have the car didn't change, not even when I place a goat face up on the table. You don't know. Is that card that I'm still holding a goat or a car? You don't know. You don't know if the card you chose is a goat or a car. But the odds that you have the car don't change when I place a goat face up on the table. There's still a one in three chance you have the car and a two in three chance that I do.

[Laughing] Where's something? I've got to hit myself in the head. I hope this explanation is clear to you and Leo. He actually said that. I had a lot of fun with this problem in an introductory programming - the problem is, if you understand it, it's clear. If you don't, it's not. I had a lot of fun with this problem in an introductory programming course at Case and would be happy to send you the code if you tell me how. We were able to do simple automation of doors opening and play sounds of a car horn or a baaah. Thanks once again to you and Leo for a wonderful program. It's been a high point of my week for 6.09445585 years.

Steve: So I did a little research because I was curious, and it turns out that Marilyn did this in a Parade column, and she had professors and academicians disagreeing with her.

Leo: People went crazy. I remember when this happened. Lots of mathematicians wrote, "No, you're full of it. The odds can't change."

Steve: So our listeners should not be chagrined if they don't get it because professors and academicians the world over were sure she was wrong. And so here's the final takeaway. If you are ever presented with the opportunity to get a car or a goat, you do change your choice. That's all you have to remember.

Leo: And if you do that over and over and over again, in time you will do much, much better because you have a 50 percent chance of getting it right on that second choice compared to a 33.3 percent chance of getting it right on the first choice. I think that makes sense. Monty has put information into the system, and it's that information you're basing your choice on at this point. Right?

Steve: Yup.

Leo: Seems simple to me. Steve, our last question comes from Peter in Brisbane, Australia. He waxes philosophical about the social hacking "I'm from Windows Support" callers. Remember this? We had a guy, where was he from? He was from - one was from Scotland, and one was from Australia.

Steve: Oh, and Leo, you wouldn't believe how much - the mail bag was full of people who have been contacted by these clowns.

Leo: Very common. And so they call up to say, I'm from Windows Support. We can tell, we can see there's a problem on your system. Do this, do that. They scare you. And then they hack you. Steve and Leo, I've been listening to your FAQ Episode 318 where you read a letter from a listener who had received a phone call from somebody claiming to be from "Windows Support." I had a quiet laugh about this. I get one of these calls almost every day when I'm at home. I had just settled back into the study after listening to the show, and the phone rings. Would you believe it? [Indian accent] "Windows Support" is calling.

I've got a number of ways I handle these calls, ranging from just hanging up to letting them have their way, all the way up to when they ask me to download something from the web. By the way, this is why Bruce Schneier's recom- or is it Brian Krebs? - Brian Krebs's recommendation that don't put anything on your computer that you didn't go out and get? Well, this would be something you went out and got because you were socially engineered. So that's my only kind of caveat on that advice. That's why I don't say that on the radio because people say, "But I went out and got it." Yeah, you nitwit.

This time I tried something different. The Indian fellow went through his script as before, saying they had detected problems with my computer, which was in fact a Linux machine - [Indian accent] "You are running Windows, I can tell" - and asking if I was the main user. I said yes and then decided to ask him, "Are you happy with your job?" Silence, then he tries to get back on the script. I asked if he thought he was doing a good job. He had obviously lost track, as I was not following the script. I asked if he thought stealing from people was a good job because he certainly knew that everything coming out of his mouth was a lie.

I got a little carried away. I told him I thought he was a bad, bad person - "You're a bad person" - and should be ashamed of what he was doing. I asked if he would go into an old lady's house and steal her money because that's exactly what he was really doing. Silence. Then this small voice: "But I need a job." I think he may have been crying. Oh, heck. What could I say? It was obvious he was well aware of what he was doing, but he had little choice. I hung up the phone feeling a little guilty.

I have recently been reading Cory Doctorow's "For the Win," and this got me thinking about how things must be for people who have no choice but to take on these jobs. The problem is not that these people are out there trying to take advance of people's ignorance of technology. The problem is the systems we use are so bad that they can ring up a random person and be fairly sure their computer will be behaving so poorly that the person who answers, anyone who answers, will be ready to believe the caller has magically appeared to assist them. He's absolutely right. It's no surprise that the iPad and to a lesser extent Mac computers are selling so well. People are just looking for a computer that will run well without an IT support team on call 24/7. Steve, thanks for the show. Leo, thank you very much for your excellent network. I listen every day. Peter.

Peter, thank you for that. That's very thoughtful. And he's thinking about the other guy on the other side. And you know, it's true. He probably needs that job desperately.

Steve: Yeah. And I guess I hadn't been focused on the fact that it is so clear that the person doing these calls absolutely knows how illegitimate they're being. I mean...

Leo: Oh, of course. You'd have to be an idiot.

Steve: Absolutely, yeah.

Leo: Not to know. I liked that email. Thank you, Peter. It's a very good point. And there's two points. One is these guys probably have no choice. They're in a third-world nation. It's hard to get jobs, whatever. But the other point is it only works because our systems are so crappy.

Steve: Yup. We have set ourselves up for this kind of call because, exactly as he says, most systems are limping along, barely functioning. And people are grasping for the idea that they could get some help and make it better.

Leo: The chatroom just published an article. Apparently Microsoft was doing business with one of these scammers and recently terminated their relationship, possibly - I haven't read the article, but I would guess that sometimes these guys are in fact Microsoft support houses.

Steve: Ooh.

Leo: That realized there was no money in it. And they thought, well, we can do some other things, too. As long as we're here. As long as we've got the phones.

Steve: Yes, we've got their numbers.

Leo: They never showed that on "Outsourced."

Steve: Wow.

Leo: Wow is right. Steve, thank you so much, as always. What a fun show to do. I learn so much. I appreciate your working so hard on it, putting this all together. Next week what do we have on the docket?

Steve: Next week we're going to talk about the BEAST, the hack that has recently been sort of implemented. It's a problem that has been known with SSL and TLS for about a decade, but not really believed to be a problem. Well, a couple of researchers showed how it could be done, and we're going to talk about the need to update SSL and TLS to give us the privacy that we think that we're getting.

Leo: Fascinating. If you want to know more, of course, go to Steve's site, GRC.com, the Gibson Research Corporation. It's awaiting you. Steve keeps 16KB versions of this show there, and transcriptions as well. We have audio and video on our site, TWiT.tv. And of course you can watch us do this live every Wednesday at 11:00 a.m. Pacific, 2:00 p.m. Eastern at live.twit.tv, or actually just TWiT.tv works now, as well. And 1800 UTC, if you're tuning in from outside the U.S.

But again, GRC.com. And while you're there, get SpinRite. That's Steve's bread and butter, his great hard drive maintenance utility. There's lots of free stuff there, like the Perfect Paper Passwords, the new Off The Grid, of course the Password Haystacks. I was on the radio in San Francisco on Monday, Steve, and somebody called and asked about passwords, and I used that as a way to - and you know what, you can fairly easily describe how it works. I said, "Here's a way to beef up your password strength." So we're spreading that word. I think it's good.

Steve: Yeah, and in fact NPR is going to get a studio for me because they want to do a story on it, too.

Leo: Wow.

Steve: So the word is spreading.

Leo: Well done.

Steve: Yeah.

Leo: GRC.com. Do come back and join us next Wednesday when we do this show all over again. Thank you, Steve, and I'll see you next week on Security Now!

Steve: Thanks, Leo.