SECURITY NOW!

Transcript of Episode #322

Listener Feedback #128

Description: Steve and Tom 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-322.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-322-lq.mp3

TOM MERRITT: Hey, everybody. It's time for Security Now!, the show that helps you stay safe online. I'm Tom Merritt, filling in for the vacationing Leo Laporte, which is always a treat for me because I get to hang out with Steve Gibson, the man from GRC.com. Steve, great to be on with you again.

Steve Gibson: Well, this time, or this week, I would say better late than never. I don't think we've ever been late. We've never missed one. Actually, last Christmas was the first time we ever deliberately repeated a podcast, and we got a lot of flak from listeners who said, oh, Steve, you've broken your record. You went six years with never having missed one. But in this case I was performing my civic duty, as many of our listeners will all probably already know. Spent the day in court, or in the courtroom, at least.

TOM: Right, as a prospective juror. You weren't subpoenaed there.

Steve: No, no.

TOM: But you didn't get on the jury, so I'm sorry to hear that.

Steve: Yeah, it's a mixed...

TOM: Actually, I'm not sorry to hear that because it means you can keep doing the show on time.

Steve: Yeah. It would have been an annoyance, and it was going to be a long trial. They were guessing about an 11-day trial with lots of witnesses. And it sounded like it was going to be interesting. But on balance, I think I'm glad that I had those 12 espressos in the morning, and they seemed to think I looked way too interested in the trial.

TOM: That's the key.

Steve: I was way more present than I should have been. So we don't know what this guy's going to do. Anyway...

TOM: All right. Well, we've got some Microsoft and Apple updates to get to today. The fighter drone cockpit story, we talked about that on TNT. I'm very interested to get your perspective on that. Germany deliberately installing some malware. Well, let's get into Security Now!. Security updates, we've got a Patch Tuesday on the way.

Steve: Yup. We went through the second Tuesday of the month, and there's really no earthshaking news: 23 vulnerabilities fixed by Microsoft, nine of which were ranked critical, meaning that no particular action on the user would be required. And eight of those nine were in IE, which got updated. And Microsoft did make a comment that they are expecting some flaws in Media Center, which were fixed in this round, to be exploited soon. So if you have a habit of not rebooting your machine for a while after you've installed updates, I would say probably better to do it sooner than later because Microsoft is even saying themselves that they're expecting this not-yet-exploited problem in Media Center, which they have fixed, to go live out in the wild and catch people who have not fixed it. So good to do. And of course Apple has had a big week this week.

TOM: Yeah, a bunch of software coming. Not just...

Steve: Yeah, right. iOS 5 is out. iTunes got a major update in support of that. But it also fixed, over on the Windows side, they fixed 75 different security flaws in the Windows version of iTunes. There's a new Safari. It is at 5.1.1, which is reputed to improve JavaScript performance by 13 percent.

TOM: That's not bad.

Steve: They backed that up with some metrics somewhere. And then we also got an OS X update. And that, for me, it was 142MB, so it was a sizeable replacement of a chunk of the OS. And hopefully in the future one of the changes with iOS 5 is that it will be able to do incremental updates. One of the reasons they've been reluctant to untether it from iTunes and landline-based broadband bandwidth is any time they had to change it, they had to replace the entire thing. So them now being able to update over the air, even for people who don't have a wireless connection, or who have a cellular connection, the only way they can do that practically is to finally introduce what everybody else has, which is little bits and pieces update only the bad parts and leave everything else there, which iOS 5 now has.

TOM: OS X, I got a Lion Recovery Partition update, as well, which I think updates that part of your hard drive that you can recover from if you have a problem with the operating system, but the hard drive is still intact.

Steve: Right, right. And then of course we had two big stories this week, one that you mentioned - I was sure you were going to be covering it on TNT. And that is that Wired magazine reported first, as far as I know they were the first people out with a story of a drone cockpit keystroke-logging malware infection that affected the installation at Creech Air Force Base in Nevada, which is the location from which our military flies or conducts the drone missions overseas. And I had heard...

TOM: Not only was Wired the first one to report it, but they were the first one that some people in the military heard about this from.

Steve: Well, and they got a few of their facts wrong, but not substantially. So the military was quiet sort of from a policy standpoint for a few days. But so much flak was generated by Wired's story that the military finally broke their silence. They explained that they have two separate systems that are involved, their ground control support and then the air support, and that they are separate, and that at no point were the air aspects - the whole system is called RPA, Remotely Piloted Aircraft. And so at no point was the air mission side affected by this. And what was happening was it was portable drives that were being used to transfer data between systems not networked, for security, and systems that were networked. So what's a little freaky is this is exactly what we used when we reverse-engineered the famous virus that attacked Iran's nuclear enrichment facilities.

TOM: Stuxnet, yeah, yeah.

Steve: Stuxnet. Stuxnet was similarly designed to get itself propagated onto non-networked machines that were deliberately not connected to anything in order to keep them safe. Yet, as we know, Stuxnet was able to jump onto thumb drives and catch a ride over to those machines. Well, apparently that's exactly what this thing was doing. Now, no one is saying that this is targeted. It's very likely that the systems, well, the one thing we do know is that they were Windows based. And so many people groaned at the idea that down in the heart of this flight control center they were using Windows as the core of these arguably mission-critical systems. But it wasn't a keystroke logger. What the military...

TOM: Which is what Wired had reported. Wired had reported it was a keystroke logger.

Steve: Yes, right. The military characterized it as a credential stealer, and they said it was similar to the type used to steal login and password information for online games such as Mafia Wars. So anyway, Colonel Kathleen...

TOM: This was run-of-the-mill malware. This wasn't Stuxnet. This wasn't targeted...

Steve: Correct.

TOM: ...at stealing military secrets, per se.

Steve: Yes. I would say there's absolutely no reason to believe this thing did anything other than to behave as it does for its own purposes, and it just happened that its propagation model matched that of the environment that it fell into. And a Colonel Kathleen Cook, who is a spokesperson for the Air Force Space Command, said that it was important to, she said, quote, "declassify portions of the information associated with this event to ensure the public understands that the detected and quarantined virus posed no threat to our operational mission and that control of our remotely piloted aircraft was never in question. So it's because of all the interest that was generated by Wired's story that they finally said, okay, look, what we'll tell you is we've got separate systems for ground control systems and flight control. They are not related, and flight control was apparently never at any risk.

TOM: And flight control makes sense. That's what you pilot the drones with. Do we know what ground control systems do?

Steve: No. We could just use our imaginations; but I don't have any, like, enumeration.

TOM: But it still makes me wonder, if this was a credential-stealing system, could it have stolen logins and passwords for the ground control system?

Steve: Yeah. One wonders, I mean, we know nothing about the system, although it's unlikely that you could log into that from somewhere else. I mean, they clearly...

TOM: Right, because it's not networked.

Steve: Right, exactly. So it was an embarrassment and an oops. And they'll have to, I mean, the good news is it sounds like it did not damage to anything but their reputation. And with any luck they'll figure out how this got in and prevent that from happening again.

TOM: What I heard is that this system was not under the ban against thumb drives, and that since this occurrence it has now become under the ban against thumb drives.

Steve: Well, makes sense.

TOM: Yeah, exactly. And that doesn't mean they can't use anything to put software on there, but it means you can't just use a random thumb drive, which they probably shouldn't have been to begin with.

Steve: You never know where that thumb drive has been, Tom.

TOM: That's right, you really don't. This is an example of that. Also some malware in Germany, but this is on purpose?

Steve: Well, yes. There's a well-known German hacker club, the Chaos Computer Club, which uncovered Germany's apparently deliberate use, installation and use of spyware on its own citizens' laptop computers. The Chaos Computer Club was quoted as saying: "The malware can not only siphon away intimate data, but also offers a remote control or backdoor functionality for uploading and executing arbitrary other programs. Significant design and implementation flaws make all of the functionality available to anyone on the Internet." So it wasn't even well designed and secure spyware that was being installed.

TOM: It was open spyware. A little too open.

Steve: Yeah. They said the spyware could even be used to plant evidence on a computer, and they said: "Functions clearly intended for breaking the law were implemented in this malware." And a number of AV companies got a hold of the source code and looked at it and confirmed that, among them F-Secure. One of the F-Secure guys said: "We have no reason to doubt the Chaos Computer Club's findings. The CCC has a long history of trustworthy research," adding, "I think it's more than likely that the German government developed the malware." And since this report initially broke, a number of German states have admitted to using the malware in the conduct of various investigations and data gathering.

TOM: This is pretty disturbing.

Steve: Well, it is. And the one instance where it was discovered, what was alleged was that the customs officials planted this on a traveler's laptop when the traveler was going through customs. So, I mean, I have not dug in and looked at the legal implications. I don't know whether there were warrants in place, whether this was legal or not based on German law. I'm much less familiar with that than I am with the law here in the U.S. So I can't judge that. But all the evidence points to the fact that something was going on, that there's definitely poorly written malware - oh, it was also able to turn on webcams, to record conversations, to load any other software into a user's computer. And the allegation was made that it could be used to plant evidence on people's machines.

TOM: Sure.

Steve: So a full-on backdoor.

TOM: I have to say I don't know whether this is technically legal or illegal either, but it shouldn't be. I don't believe that a government should be able to plant malware on anyone, even if you're a suspected criminal. You shouldn't be able to infect someone else's device.

Steve: Well, yes. And there has been, unfortunately, over the last decade, a general, I think, sort of a softening of that, just as a consequence of the so-called U.S. "War on Terror" and the Patriot Act and so forth. But I well remember having discussions with our government in the days when Code Red and Nimda were prowling around the Internet and being a huge problem. And many of our own listeners, because when we talked about this, the question came up is why couldn't we use the same backdoors in vulnerable machines that the worms were using to disinfect them? That is, why wasn't it possible or wouldn't it be possible for a government-endorsed program, even if it was put together by private industry, to go and disinfect these machines, where we have the IP of the machine because it's out scanning around for other ones?

So there are online honeypots collecting incoming traffic. We know the IPs of these machines. And I remember I was actually in a teleconference with someone high up in Justice at the time, and she made it very clear that she understood the issue, it was oft talked about, but clearly against the law. So you couldn't do it even if it was for reasons of, like, benefiting the people who were your targets. It was still illegal.

And so if we end up with a situation where it's legal for the government to install spyware - and, I mean, there have been similar situations where for data-gathering purposes the FBI has been involved in various types of surreptitious monitoring of targets of investigation. As I understand it, here in the U.S., at least, you can - obviously you can get wiretap warrants that formally allow the FBI to listen in on conversations when a court has been convinced that the evidence that the FBI has so far merits that. So again, I don't know where...

TOM: But that's not what was going on here. They weren't going to court and getting a warrant, saying I want to place a piece of software. Then it would just be about the fact that they put some pretty bad faulty software on it. But this was just unilateral action; right?

Steve: We don't know. I don't think it's known. From what I saw, reading the individual reports from the states that acknowledged they were doing it, they weren't explicit, either. But the sense I got was that they were taking the position that this was, I mean, they weren't admitting to criminal action. They were saying, yes, we've used it, and we believe we have legal foundation for having done so.

TOM: Yeah, just I find the most disturbing part of this story being that it was put on machines at customs because that has become the get-out-of-jail-free card for governments. Oh, you're crossing an imaginary line? Well, then you lose all your rights. And I think that's a horrible precedent to be set. And it's one of the things people fear. When they actually go through customs, and they want to look at your laptop, it's like, well, what, are you going to steal my data? You going to put some malware on there? Well, apparently yes. Sometimes they might be putting malware on there, if they think, without any justification to you why, but they just happen to think that you might be worth investigating for any reason, they might do that. I mean, they can't open your mail, can they? I guess customs officers can open your mail. So if you were shipping your computer to yourself, you'd still run into the same possible issue. There's really just no way around it if you want to cross a border.

Steve: Yeah, I mean, and we've talked about the problem of customs officials having the legal right to force you to turn on your machine and look through your files. And there were some cases a few years ago where files and filenames got people in trouble at customs. And I remember that being walked back a little bit. But it certainly is an issue of some tension.

TOM: All the more reason to use a hidden volume and TrueCrypt.

Steve: Yup.

TOM: And you know what? The really nasty people are going to do that.

Steve: Right.

TOM: What have we got from the Twitterverse?

Steve: Well, last week we covered in some detail this really neat technology that was - the acronym for it was BEAST, Browser Exploit Against SSL and TLS, which two developers, Juliano Rizzo and the guy who posted a detailed chronology of their development, Thai. I read Thai's post. And apparently Juliano is either following me or he was tipped to it because I got a really nice tweet from him, who said: "Awesome. Steve Gibson @SGgrc explains B.E.A.S.T. and reads Thai's post." Then he gives a URL for the YouTube link, and then he says "includes jokes about bikinis and me." And our listeners from last week will remember that there was some conjecture on Thai's part that maybe Juliano was busy looking at bikinis, and so there was not as much code being written at one point as was being hoped. But prior to that, Juliano was not being distracted by bikinis because he was actually reading the detailed operation of SSL while on the beach in Buenos Aires. So I think that all ended up working out for the best.

TOM: All right. Sounds good.

Steve: And I wanted to give all of our listeners who are not fed up with the whole story of the passing of Steve Jobs - I'm not yet - I wanted to give everyone a heads-up that Discovery Channel has commissioned the MythBusters guys to a one-hour documentary titled "iGenius: How Steve Jobs Changed the World," which will be airing this Sunday, October 18. So, wait, October 18th. This is the 14th.

TOM: Yup. So is it...

Steve: No, it's October 16th, sorry.

TOM: Okay. It's on Sunday, for sure.

Steve: Yes. It is this Sunday. I verified the schedule. I tweeted about it earlier, and some people sent back, well, what time? It's like, I don't know what time zone you're in or when.

TOM: Check local listings for show time.

Steve: Thank you very much. So it's "iGenius: How Steve Jobs Changed the World." And what I do know is that they managed to score some very significant interviews from many of the people who were present in the early years, the founder of the famous Homebrew Computer Club in Silicon Valley where Jobs and Steve demonstrated their first Apple I machine. And so, anyway, I'm not going to miss it, and I didn't want any of our listeners who would have wanted to know about it to miss it, either.

TOM: Sony Pictures has apparently gained the rights to the Steve Jobs biography that was written by Walter Isaacson that's still - that book comes out later this month. But we might see a movie in the offing.

Steve: Was that the authorized or unauthorized?

TOM: That was the authorized one. That was the one that Steve apparently gave unprecedented cooperation with.

Steve: And access, yeah.

TOM: Yeah, yeah, exactly.

Steve: Well, I did have a nice note from a Mark Ping, who is a listener in Chico, California, and the subject caught my eye. It said, "SpinRite Saves the Sawmill."

TOM: The sawmill. Like a "Twin Peaks" story, huh?

Steve: He said, "Steve, I'm new to a lumber company with lots of automation in the sawmills. This morning we were getting started on day two of a software fix onsite, where there is a ton of vibration. It's a hard drive's worst nightmare." And actually he's right about that. We've talked about vibration in the past. Vibration can really cause a problem because the drive, in order to get the density that modern drives have, the track density is incredibly high, meaning that it's super delicate to keep the head over the data and not skipping over to adjacent tracks. So the drives are designed to be as vibration tolerant as possible. But a good friend of mine had a situation where just the fans in a server case, the vibration from the fans was causing much lower drive performance because the drives were having so many errors and having to retry and reread their data. So vibration is not good.

Anyway, he said, "The lead programmer's laptop was doing the" - and he says, quote, "'boot almost to Windows, then blue screen' dance." He said, "Well, I've been a Security Now! listener since Episode 100 and a SpinRite owner for nearly as long. I knew what to do. I OpenVPN'd to my home computer to get my ISO file, which I've built on top of MS-DOS instead of FreeDOS, and burned a CD onsite. I booted SpinRite into Level 2 and let her rip. At about 5 percent I saw the progress stop, and DynaStat" - that's SpinRite's Dynamic Statistics system - "kicked into gear. After one R" - meaning that it recovered that data in the sector - "it sped right up again.

"Figuring the odds were good that the problem was fixed, I canceled out, crossed my fingers, and booted. Windows came up the first time, and we were able to copy off the source code and were right back in business. I'll be talking with my boss about site licenses later today. Thanks, Steve, for a great product and the best netcast out there." Sorry, Tom. "You saved us a lot of time and made me look great at a very good price. Plus I'll get home to my wife and kids sooner. Did I mention this mill is a 12-hour drive from my house?" No wonder he used OpenVPN. He said, "Keep up the good work, and hurry up with CryptoLink. Mark Ping in Chico, California." So thank you, Mark.

TOM: Wow. Great story. I don't mind if he calls it the best. It's one of my favorites, for sure. Shall we get a little Listener Feedback #128 going, Steve?

Steve: I love it. Let's do it.

TOM: All right. #1 is part feedback, part question. Feedback part - this comes from Mark Botner in Little Rock, Arkansas. He wants to know: Where's my SNU diploma? I believe that I have met all of the requirements for my Security Now! University diploma. I have, #1, starting on or about May 24th of 2011, listened to all of the Security Now! episodes. I listened to Security Now! while I was walking my dogs, commuting, et cetera. I have switched from a DDWRT-based router to an Astaro Gateway system for my home firewall. I moved my SSH server to a non-default port. I use two-factor authentication for all my bank accounts, Gmail, Facebook, et cetera. I started using LastPass with a YubiKey for all my online accounts.

This is a big one. I taught my wife to use unique random passwords for each site with LastPass and YubiKey. I used ShieldsUP! and reconfigured my DSL router until I achieved a perfect scan. Boy, this list goes on and on. He talks about DNS Benchmark, enabled hardware DEP on his systems, uses NoScript in Chrome and Firefox - I guess he's using NotScripts in Chrome - uses Amazon's S3 for backup. Installed Carbonite on his parents' and sister's PCs. Already said he was Netflix customer.

Started taking daily vitamin D supplements. Cabernet Sauvignon is his favorite wine. Turned off JavaScript and external program access. Uses WPA2 on his wireless router, switched Windows over to Microsoft Security Essentials, scanned Windows system with MRT, scanned Windows with Microsoft System Sweeper. And finally, I use my licensed copy of SpinRite regularly to maintain all of the hard disks in my house. So I ask you: Where do I go to receive my SNU diploma? Where does he go, Steve?

Steve: Well, boy. Consider also that he began on or about, he says, May 24th of this year.

TOM: And caught up on everything.

Steve: Yes. So he listened to, what, 320 episodes in that period of time.

TOM: Yeah, exactly.

Steve: So congratulations, Mark. That's quite an accomplishment.

TOM: Now, he also has a serious note, a crypto question. He says: A couple of days ago for me, which was a few weeks ago for you two guys, I listened to Steve discussing a possible reduction in strength with an attack on the AES cipher. My question is, in a manner much like cipher block chaining, why can we not chain multiple encryption ciphers together? For example, one could encrypt a block of data with AES, then Blowfish, then triple DES. By chaining multiple ciphers in a manner like this, even if one cipher is completely compromised, your encrypted files would be safe, I think. I realize that each cipher would add some amount of processing overhead. But if secrecy was really important, why not consider doing multiple encryptions? I'm not a crypto expert, but wondered what Steve thinks of this.

Steve: Well, he's exactly right. And people who are familiar with TrueCrypt will have probably seen the option which TrueCrypt offers for doing exactly that, for choosing a collection of ciphers and sequentially running through them in one direction for encryption, and then of course you have to run through them in the reverse order for decryption. And it is suggested that, if somebody were really, really just, I mean, over-the-top concerned with security, they could do that. And exactly as Mark suggests, really the only downside of doing so is performance.

In the measurements I've made of recent versions of TrueCrypt, I've seen no measurable slowdown from TrueCrypt's operation because with current state-of-the-art chips, especially the newer Intel chips, for example, which support AES in the instruction set itself in order to speed up that encryption and decryption operation, the speed of the drive is the limiting factor, rather than the process of getting the data on and off the drive, even if you throw in the overhead of ciphering. So you really don't see much performance overhead. Probably when you layer on additional ciphers you would start to see that.

But it has the advantage, again, exactly as Mark hypothesized, that if by some bizarre coincidence, from out of the blue, a huge problem was found in the cipher you were using, if you were only using that cipher, you would be vulnerable at that moment. By using even two - I would say three is really, I mean, first of all, the chances of any problem like that occurring in a really well-known, well-tested, well-proven cipher is so vanishingly small that, if you were really concerned about it, then do two. I can't imagine the reason to do three because there just - the worst that could happen is that one of the two might be rendered useless, but you'd still have the other one, and then time to change that first one that had been rendered useless for a different one, if you still wanted to have two. So I can't ever see a point in going beyond two. But frankly, I'm quite content with AES and just using one. Still, his point is a great one.

TOM: And you made this clear on that episode that he's talking about, reduction in strength of AES does not in any way make AES weak.

Steve: Correct. Correct. In fact, AES uses multiple rounds where the rounds are identical with only the difference of the intermediate steps mixing from different key-derived data. So, for example, one round of AES is easily penetrated. It doesn't provide enough scrambling to confuse cryptographers. And that's true for two and three and four and five. And generally what happens is that the cryptographer will analyze some number of rounds to determine really quantitatively how much strength that offers. And then they add a padding.

And in fact I read some commentary by Bruce Schneier, a favorite cryptographer of this podcast, and he has suggested that all that we have to do to settle the whole issue of AES once and for all is just all agree that we're going to do a second version and just increase the number of rounds. That's just - that's really all you have to do. No fundamental weakness in the underlying algorithm was found. It was just we've pushed ourselves a little further than we expected to by this point in time in the number of rounds we need to obtain as much strength as we would like. Therefore the margin, which was always deliberately built in, has been shaved off a little bit. And so Bruce says, just do some more rounds, and problem solved.

TOM: Yeah, here, easy. Lars Mikkelsen in Denmark writes: Hey, Steve. This might be of interest. This is how Windows got infected. And he has a link that we'll include in the show notes [http://www.csis.dk/en/csis/news/3321/]. It's from csis.dk. There it is on the site there. But I didn't open it in a new tab, so I have to leave it now - sorry about that, Alex - to go back to the notes. But Lars continues by quoting the site, says: "CSIS has over a period of almost three months actively collected real-time data from various so-called 'exploit kits.' An exploit kit is a commercial hacker toolbox that is actively exploited by computer criminals who take advantage of vulnerabilities in popular software. Up to

85 percent of all virus infections occur as a result of drive-by attacks automated via commercial exploit kits."

Steve: So this was a great link. And to help our listeners I tweeted a number of links this morning as I was assembling the notes for the podcast. So everyone who's interested can just go to Twitter.com/SGgrc. And since I'm not tweeting often, these will not be pushed far down in my stream, if at all. And there is the link there. And as Tom said, it'll also be in the show notes.

This was interesting because it made a very clear exposition of how in the real world people were getting infected. And so, not surprisingly, IE, Internet Explorer, takes two thirds of the vector for the way people are getting infected. But Firefox was at 21 percent. So IE was at 66 percent, Firefox about one third of IE, but still it's substantial just for no other reason than due to its popularity. Google Chrome, though, was in there for 8 percent, Opera at 2 percent, and Safari at 3 percent. But what's probably most interesting is the third chart, which talks about the way that these tools are allowing people to be infected. That is, it's the programs that are being invoked. And the largest percentage of that pie, 37 percent, was the Java Runtime Engine.

So we've talked about this before. We've talked about removing Java from your system if you know you don't need it because what's happening is browsers are being caused to invoke Java, and mistakes in Java are being leveraged into exploits. And in fact we were just talking about the BEAST exploit where those developers were, for them to do what they needed, they needed to find a brand new zero-day fault in the Java Runtime Engine that no one knew about, that would deal with the same origin protection which keeps browsers from allowing scripts to run from one site and then getting data on another. So just by going to the Java source code and looking for a specific problem that they were hoping was present, they found one.

And so you have to wonder, I mean, if that's the state of the world, then bad guys get an idea for a way they might be able to exploit something and just go and take a look, and look for what they're trying to find, which is fundamentally not the mindset that the developers have. The developers don't expect there to be a problem, don't think there's a problem. So, what do you know, they don't find any problem. So Java Runtime Engine was the largest share at 37 percent. Not surprisingly, #2 was Adobe Reader and Acrobat at 32 percent, so just a little bit less than the Java Runtime Engine. And Adobe Flash was #3 in line at 16 percent. Again, no surprise there. So we don't really - we don't see anything we didn't expect, but it's interesting to see the numbers and the breakdown, and they did a really nice report that I wanted just to bring to people's attention. So thank you to Lars for bringing it to ours.

TOM: Yeah, good stuff. Thank you, Lars. I had a conversation on Google+ the other day about I started a virtual machine of Windows 7 that I hadn't started in a couple months, and I was complaining about all the updates that you have to go through when you have - just even after a couple months. And someone's like, well, why don't you just say no to them? I'm like, well, that's pretty bad security practice because if you're talking about zero-day Java Runtime, I definitely want my Java up to date before I start doing anything important. But you've got to sit there and wait through all that stuff.

Steve: Well, yes. And of course, as we know, we talked about this just earlier in this podcast, the older the problems are that are not fixed, the more likely users are to encounter them in the wild because the bad guys know that there are machines that, for whatever reason, are not being updated. So if you deliberately aren't updating a machine, you're increasing the window of opportunity for bad stuff to fall through it.

TOM: Yup. A listener who wished to remain anonymous, did not share a name or location, commented about lithium ion batteries: Steve, following up on discussion of the care and treatment of the lithium ion batteries, HP, for example, says to discharge to 5 percent now and then so that the "smart battery" technology can recalibrate, as you say. But if the calibration is already wrong, wouldn't the 5 percent be impossible to guess? I recently bought a secondhand HP NC4400 with a battery that said it only had 40 minutes left, even after I charged it. So I fully discharged it until it went off and then recharged it, and now it says four hours, 20 minutes, almost like new.

Apple seems to say that it isn't full discharges that cause the trouble, but a deep discharge - for example, the result of a battery left fully discharged. HP says: "Remove the battery from the notebook if the notebook will be plugged into AC power continuously for more than two weeks." So perhaps it's not a good idea to leave laptops always plugged in. Now, this is almost a religious controversy in some ways. But what do you think?

Steve: Well, okay. So I wanted to explain a little bit more about the need to cycle lithium ion. First of all, I don't disagree with any of that. But it needs to be sort of explained a little bit more. And I mentioned - this was just my - I brought the point up myself last week, out of the blue, because I saw a friend who was draining some electronic device of hers, I think it actually was a Kindle that had "I am discharged" on the screen, and it wasn't happy. And I asked her, I said, "So do you just read your Kindle day in, day out, day in, day out until that happens" - and frankly I know that my mom does - "and then you plug it in?" And she said, "Uh, yeah." And I said, "Okay, that's not good. Lithium ion batteries do not like to be run that way. It is much better for them if you keep them charged up."

And so that was the point that I wanted to make, and I generated a bunch of feedback through our mailbag and also on Twitter of people wanting links, people asking me if I was sure and so forth. So relative to this recalibration, the reason it's necessary to do that is the lithium ion batteries do not produce anywhere near a linear decrease in voltage as they discharge. If they did slowly drop down their output voltage as they're losing charge, then it would be easy for the battery management technology to simply measure the voltage on the batteries to determine what percentage of them that they were full.

Instead, lithium ion as it's discharging from a full charge initially drops its voltage by a few tenths of a volt, from 4.2 down to about 4 or 3.9, 3.8. Then it's absolutely or nearly absolutely flat for the bulk of its lifetime. And only at the very end does the voltage then suddenly drop off. Which means that the battery gauges that we have on our laptops, which I love, just handy to be able to look at it and say, okay, you've got about three hours left. I mean, it's much nicer than not having any indication of when the lights are about to go out. So they can't, there's no feedback they can use from the battery itself because the battery is just giving them the same output voltage all the way along, except at the very beginning and at the very end.

So they use timing. And so there's been a lot of human effort that's gone into developing this technology, the idea being that the system monitors the total amount of current being drawn, that it's able to measure moment by moment. And so in software it integrates the instantaneous current drawn from the battery in order to determine how many total amp hours have been taken from it, estimated against its known full size of the battery. So basically it's just - it's knowing when you're running it, and it knows how much current you're pulling it over time. It knows when you plug it in, for how long you plug it in, how much current is put back in.

So it's sitting here looking at this straight line of voltage and just sort of juggling, saying, okay, now we just added 10 percent. Oh, now we took out 17. Oh, now we put in 12. Oh, now we took out 20. Now we put back in 15. And so you can imagine that all of that is better than nothing, but it's a little error prone. You're going to, over time, it's going to become desynchronized. Thus the need to occasionally, and only occasionally, bring it all the way down. If you leave your laptop on, that allows your laptop to drain the battery into that final drop-off. Then when the battery sees that, then it knows, ah, now I'm able to realign myself with that discharge point. And that allows it to reset its otherwise just sort of ad hoc tracking of energy in, energy out.

So that's the reason why occasionally you need to bring it all the way down, so that your battery management technology is able to synchronize. But the rest of the time it is much better for it, as I originally said, to keep it charged up near the top because just the way the chemistry works, that's what the lithium ion battery is happiest having.

TOM: Yeah, I think a lot of people get confused because nickel cadmium batteries had memory, and they kind of - they mix that up with lithium ion. I'm not saying that that's what our emailer did. In fact, I'm pretty sure he didn't. But, yeah, that does confuse the issue. Lithium ion doesn't have memory. And what you're saying is it's okay every once in a while to drain it all the way down because you might want to recalibrate. But you don't want to drain it down all the time.

Steve: Correct.

TOM: But it's really tempting with an Amazon Kindle because it doesn't need to be plugged in that often. A laptop, you use it unplugged for a while, a few hours, maybe six hours it's going to start giving you alerts. A Kindle won't, and so you kind of forget it needs to be plugged in.

Steve: Right. And I think that's a perfect example because when we were talking about it last week, a cell phone is the same way. Most people, because you don't really get more than a day of use out of your cell phone, you're in the habit of docking it at night and charging it back up. It would be a little better for it if it was convenient to charge it at the office or during the day at some point, if you weren't using it, to sort of give it a midday boost just to keep it up because it's continuous deep cycling that ends up aging the lithium ion chemistry faster than the same total amount of current flow which is kept more up near the charged state.

TOM: I keep my batteries plugged in as often as possible. I don't see any shortness in their life. The only thing I've run into with lithium ion batteries, a couple of times I have forgotten to turn them off. I've put them into sleep, just closing them, and forgotten to turn them off when I got on an airplane, and they have swollen up because of that. Now, over time that has gone away, if I don't do it again. But I actually had to replace one battery because it swelled up so much from being on during takeoff.

Steve: Yeah, there's gas that is produced, and that will cause the individual cells to bubble up.

TOM: Yeah. Question #5 from Frijol in Houston notes that Apple is not rolling in the hay. He says: Guys, I'm sure you've heard this, and my apologies if that is the case, but I found this interesting enough that I had to share. It appears that Apple doesn't buy into the Haystack concept. In fact, they explicitly forbid it. In trying to create a new iCloud account, I tried to use a variant of an old MobileMe password but was denied. The text read: "Passwords must be at least eight characters, including a number, an uppercase letter, and a lowercase letter. Don't use spaces, the same character three times in a row, your Apple ID, or a password you've used in the last year." I assume that meant three or more times in a row. Anyway, I found it interesting that they would include this in their rules, especially knowing what we know now, thanks to your analysis. Regards, Frijol.

Steve: Okay. So this brought up a good point, and that is that, in my example, because I sort of wanted to use an extreme example of a really simple password on the Haystacks password page, which is also very easy to remember, in my example I use just a string of dots. So that clearly, as we see, would be denied by Apple. But I would recommend that in practice you did something like alternating characters or a pattern of three that repeats or something else. So that still gives you largely the same benefit of something that's easy to remember that you add on to the end of an already strong password to make it stronger, yet not always repeating just the same character endlessly. Be a little more creative. Have some fun. You could make some pictures or do whatever you want. And that'll avoid the problem but still give you the benefit and actually make the result a little bit stronger, as well.

TOM: This doesn't bother me so much. I understand why they're saying don't use the same character three times in a row because they're not concerned with Haystacks, they're concerned with people who are only making six, eight-letter passwords using the same character all the way across, or three characters...

Steve: Like 0000000 or something.

TOM: Yeah, and I think that's probably a good policy. What really frustrates me are the sites that won't let you use non-alphanumeric characters. That just - because I have got a system, based actually very much on the Haystacks principle, that non-alphanumeric characters are essential for me to use. And then those sites are making it harder for me to be secure and also making it harder for me to remember the darn password.

Steve: Well, and they are actually less secure sites.

TOM: Exactly.

Steve: Because a site that won't let you use a password with a large alphabet, the bad guys know that, and it makes their brute-force cracking that much more efficient because they don't bother trying passwords which they know the site doesn't allow in the first place.

TOM: Abe in Chicago comments about changing passwords and government interference. He says: I am sure that you have heard of HIPAA, but you may not know about some of the things it requires of companies who are forced to follow its guidelines. One of them is that the IT department cannot know the users' passwords. That's of course good, but they also require that users be forced to change passwords every six months with no guideline on password strength. What do you think?

Steve: Well, we've talked about this, I think, once before. But I saw the question, and I thought, okay, this is worth just going over again because I cannot for the life of me understand what the threat model would be that would bring some security person to think that requiring people to change their passwords every six months was beneficial. You want to do that because there's some problem that you're solving. Certainly it's an inconvenience to users because you are suddenly telling them that the password you have finally memorized, which was strong enough to be a pain to memorize, they now have to change. So not only do they have to come up with a new one, but they have to remember to forget the old one and then remember to remember the new one.

And, okay, so the only way this makes sense - so how could this be good news, or beneficial? The only model I can imagine would be one where a user's password becomes compromised, and something endemic to the world prevents the bad guy from using it for six months. That is, there's some, for some reason, bizarre six-month delay before the bad guy can try to use it. In that case, obviously, changing your passwords every six months would always mean that your change would occur between the time the bad guy got it and six months later when they were first able to use it. So if the world worked that way, with this weird six-month delay between the time an exposed password could be exploited, this makes total sense. But it's not the way the world works. Passwords that are compromised are tried that afternoon, that night, I mean, at 2:00 a.m., immediately. So...

TOM: That's what they want you to think. The clever hackers are holding onto them for seven months.

Steve: So it's only the model that, like, imposes some fictitious, wacky delay allows that advice to make sense. It makes absolutely no sense. And in fact there are companies that have policies, for example, where you must change your password every X weeks or months or whatever.

TOM: Every three months, and you can't use the same password you used for the past three times. Place I used to work at drove me crazy with that.

Steve: Yes. And in fact I remember telling Leo in our podcast, I once overheard, when I was having breakfast somewhere, a group of guys with laptops, and one of them was talking about how he was getting around that policy. He realized the system didn't keep track of when the prior passwords were used. So every time he hit against this, he changed his password immediately, once, twice, three times, and then back to the same thing he always had. Which satisfied the system, he was always able to use the same password, and basically he hacked around the policy and got what he wanted and so defeated the ridiculous imposition of the IT department. Which some survey showed recently, and we talked about it, Tom, that the IT department is the most despised group in most companies.

TOM: It is, because...

Steve: They're not seen to be adding much value. They're just in everyone's way.

TOM: And the IT department should be the most respected because you need them. But, yeah. Question #7 comes from Gary McCleery in a small house on Clyde Street, Oamaru, New Zealand - kia ora! - ponders a question about Ethernet switches. Go All Blacks. Hi, and greetings from Oamaru, New Zealand. I love your broadcast. Pity you can't do it at least five days a week. I'm with you, Steve, I prefer XP and hate Win 7. I tried Win 8 and hate that, too. Yes, Leo and Paul, I realize it's only a developer's edition. But the whole concept sucks, think Microsoft has lost their way.

Anyway, my question has to do with Ethernet network switches. I work for a school, and one day every computer connected to a particular switch lost access to the network. I tracked it down to a classroom where someone had plugged a network cable into two live ports of the same switch. I have since disabled one port to stop this happening again, and I understand some switches can be configured to deal with this problem. Could you tell me at the packet level what is happening? Does the cable plugged into two live ports cause something like an infinite loop, creating so much traffic that it overwhelms the switch? Thanks and cheers, Gary.

Steve: Yes.

TOM: He answered it, didn't he.

Steve: What happens is Ethernet switches have a little bit of intelligence in them. When an Ethernet packet comes into an Ethernet switch, its job is to only send that packet down the arm or leg of the switch where its destination Ethernet adapter is located. So in order to find that, it needs to send out a broadcast, if it doesn't already know. Now, "doesn't already know" means that there is some memory in an Ethernet switch, which there is. There is typically, like, 4,000 entries, 4K entries in an Ethernet switch, the idea being that the switch associates specific MAC addresses, the Ethernet MAC addresses with individual links, so it learns on the fly which connections are connected, which of its ports are connected to, downstream, which Ethernet adapter or adapters.

So what happens is it sends this broadcast out and looks for a response from whichever port contains the Ethernet adapter. Then it adds that to its table so that in the future it has learned which MAC address is on which port and doesn't need to do that again. Similarly, switches have to be transparent; that is to say, in an Ethernet network, broadcasts have to be broadcast. So any Ethernet adapter is able to send a broadcast which needs to be heard, by the definition of Ethernet, by every adapter. Which means when a broadcast comes into a switch, it has to forward it out of all of the other ports. And what that does is that makes the switch transparent on the network, transparent to broadcasts. It's not transparent to directed traffic because there the switch directs specific packets, as we were just saying, only down the port that contains the target adapter with a MAC address.

Okay, so we put those two things together, and you can see where the infinite loop comes in because, if you have two ports connected to each other, and the switch is not sharp enough - and exactly as Gary says, he had heard that there were switches where this wouldn't be a problem. But it does require extra intelligence. So a packet comes in the switch addressed to a MAC adapter, or a MAC address that is not currently in the table. So the switch broadcasts a query out of all of its ports for the adapter with that MAC address. Well, that broadcast goes out of one port, and it's looped back immediately into one of the other ports, coming into the job queue as a broadcast, which because we were just talking about broadcasts, has to be sent out of all ports. So it is exactly like a data short circuit. One unknown destination will cause the switch to lock up in an infinite loop of broadcasting to itself and just flooding itself with its own data. And it quickly just ends up filling its queue and essentially crashes.

TOM: So it's shouting the MAC address to itself.

Steve: Yes. Well, it's shouting the question to itself.

TOM: Right, right.

Steve: And then saying, oh, I've got to repeat that question.

TOM: Where is this MAC address? Like someone kind of rocking in the corner shouting until you unplug that Ethernet cable. So how do you find a router that is smart enough to figure out that that's going on?

Steve: You know, I've never seen that in a spec sheet. So the only thing you could do is short circuit one and see if it collapses.

TOM: See if it works, yeah, okay.

Steve: If it collapses, then it's like, okay, I don't want to use this one.

TOM: That's not the one. You see people going into Fry's, trying to short circuit routers. Question #8, Nathaniel Hall in Springfield, Missouri - that's where my uncle lives - suggests a correction regarding TCP and UDP port 0. Hey, I was on that show. Steve said: I have been listening to the show for many years and love each and every episode. Unfortunately, I tend to get behind on episodes and am just now listening to Episode 317. Steve doesn't say this, Nathaniel says this. But I had one minor correction to make. When describing TCP you said port 0 was not a valid port. This is not correct. Zero is a valid number for TCP and UDP packets, but it is a reserved port that cannot be used. I find this important because some attacks actually utilize port 0 as the destination or source port in order to fool the destination host and/or security devices in the middle. Thanks for all the work you and Leo do to educate the community. It's a big help to keep up on things that I otherwise may not be able to keep track of.

Now, when I'm reading this, I start to think, well, maybe that's a distinction without a difference, if it's a port that could be used, but is reserved for un-use. But does he have a point here because of the man-in-the-middle thing?

Steve: Well, I would say we're - it's exactly as you said. We're mincing terms a little bit. First of all, he's absolutely correct. As I have said about TCP and UDP packets, the port designation is just a 16-bit field which can contain values from 0 through 65535. And port 0 can occur because obviously you could send a packet onto the Internet that had all of those bits set to zero. And in fact the most recent version of ShieldsUP! - and when I say "recent," I tend to do things that last. I mean, SpinRite was finished in 2004. ShieldsUP! was before that. And I haven't touched it because as far as I know it all works perfectly.

But my point is, it tests for port 0 because I understand that you can have packets that have all zero bits in the port number, and that such packets have been known to sneak through firewalls and NAT routers because they're not designed properly to say, wait a minute, this is not valid to have a port 0, and just to ignore the packet. So ShieldsUP! has, for a decade probably, checked to make sure, I mean, I generate port 0-based packets from my site to make sure that I get no response from them over at the user end. And if so, they don't pass. So thank you, Nathaniel, for clarifying that and giving me an opportunity to talk about port 0.

TOM: Question 9 from Fausto in Mexico City. He says: I would like you to share your thoughts on Steve Jobs. I admire him, and I would like to know what did you learn of him, if anything; what do you think he contributed to our tech world as we know it; and, important, how do you think we can make a tribute to him? Buy Apple stuff? Or even better, try to incorporate some of his ideas into our daily lives. Thanks, Steve.

Steve: Well, I'm sure this has been talked to death, and everyone knows Jobs, or knows of him and his work and so forth. I met him on a couple occasions in the early days of the Apple II at the various Apple Fests which Apple sponsored in order to pull vendors together. I had designed a hardware and software combination, a high-resolution light pen for the Apple II, and was selling it. And actually I got to be very good friends with Woz at the time because he appreciated the technology that had gone into it at my end. And I've watched Jobs. And I think my feeling is sort of the consensus which has evolved, which is Apple is probably going to be fine for three or four years because they've got enough products in the pipeline and there's enough Jobs-ness already imbued that the inertia of Steve will continue.

But it really - I'm skeptical about the idea that it's really possible for Apple never to drift. I'm afraid it will because it was very difficult to be Steve Jobs. I mean, it was who he was, so it wasn't difficult for him. But there was some controversy always surrounding him because to be that much of a perfectionist, to scream at engineers because the radius of curves was obviously wrong to Steve, but looked fine to everybody else, I mean, to have that kind of personality, which is why we got, it's how we got the products that we did here after Steve's return, and especially lately as he really ramped up and got enthused about the consumer side, I just don't see anybody replacing him.

And I really think it's so difficult to demand this kind of quality. There are prices that are paid, and most organizations ultimately aren't willing to pay it. It was because he was running it, he was in charge, and he would accept nothing less. And he was willing to stop the presses, he was willing to stop production, he was willing to, I mean, look how late Apple was with a tablet. They talked about it a long time. Many tablets were tried. And I remember reading that in engineering they were scrapping their own products before even getting it to the point of even showing it to Steve because they were afraid of what his reaction would be, until they had something that they really thought had a chance. And even then it was rejected many times.

So without Steve there to really be that, I'll be surprised if the future continues. He was unique, which is why there's a documentary about him on Discovery Channel this Sunday evening, and why I almost selfishly am sorry for losing him because I loved what Apple's been producing. I mean, it's been uniquely wonderful product in this industry. And again, I'm going to get my iPad 3 with its quad res display. That's all I really want. I just marvel at how good the iPad 2 is. I was just shaking my head, playing with it with iOS 5 this morning when I was having my 12 shots of espresso. I think I was happy because of the iPad. Might have been the coffee, but...

TOM: The espresso doesn't hurt, but, yeah.

Steve: Yeah. It's just, it's such a perfect device. I mean, it's just a joy to use it. I've used other touch tablets, and they don't respond. They're clunky. There's a delay. They're not sensitive enough. I mean, just everything about them pales in comparison to the iPad 2. And it's because there was somebody there who demanded nothing less. And I think here's how I would prove this point, prove my feel for this. And that is there is no other Apple. That is, Apple is unique in doing this. It's not like they're in a herd, and so one of the herders died. They're not in a herd. They are unique. They came late. They enter late into whatever market they're coming into, and they do right what other people have done wrong. If it was easy, if it was even possible to do this without Steve Jobs, somebody would have because there's a tremendous need for it. But Apple was the one, only Apple. And it's because only Apple had Steve Jobs.

TOM: Yeah, I mean, we've talked a lot on the network about it, and because of timing you haven't gotten to talk about it here, which is why we're talking about it. But I agree that Steve Jobs's legacy is his passion and his uncompromising nature. And I think that's the test of Apple is, now that he not there, how much was he able to, as you say, imbue them with that spirit to be like that. Not to try to be him, but try to be like him as far as being uncompromising and being passionate and only accepting it when you think it's right. And that's what we're going to have to wait to see in a few years because I think there's a lot of criticisms you can make of Steve Jobs. He was not a perfect man in any way. None of us are. But the things that you can take positively from his life were his philosophy. He was a philosopher.

And I think that's why people use that Stanford speech that he made so often in memorial was because that really laid out the way he approached life. He may have been able - because he didn't surround himself with yes men. A lot of people who are uncompromising and dictatorial just want a bunch of people to say yes. He didn't want that, either, from what I understand. And I never got to meet him. He wanted people who were just as uncompromising and passionate as he was. And so if he was able to pull that off, then Apple should be in good hands. But it will never be the same. That's the one thing I would say.

Steve: Yeah. And, again, if I can have my iPad 3, and my iPhone 5, I think I'll be happy.

TOM: We'll get that iPad 3 in March, I have a feeling. I don't know when iPhone 5 is coming, whether that's - might have to wait till next October for that. All right. Our final question from Jason in Torrance, California asks: Where can I get the free copy of Honor Harrington, "On Basilisk Station"? I'm going to start buying the books, but wanted to read the first one's free copy, if possible.

Steve: Okay. Now, our listeners thought they were going to get through an entire podcast without hearing about Honor Harrington. [Buzzer sound] Sorry about that. Okay. I just, again, for our listeners, it turns out the page where you can download the first two eBooks free is a little tricky to find. So it is in my Twitter stream, both that first book and also the parent page, which you can also reach by clicking on the blue UP arrow on the "Basilisk Station" page, to get to the page where that, the second free book and all the other non-free eBooks are available with no DRM, in every eBook format imaginable, even PDFs and HTML. So there's just - anyone ought to be able to read them.

I wanted to take a moment to summarize in just three pieces of feedback what I've received from a phenomenal number of listeners. These are representative, and I'm going to try not to mention it again. I think maybe next week we actually will have a podcast where Honor Harrington's name does not come up.

James Troutman in Philadelphia, Pennsylvania sent on the 4th, he said regarding "On Basilisk Station": "Steve, I want to thank you for your *repeated*" - he has that in asterisks - "recommendations of the Honor Harrington series. When you first mentioned it, I decided to give 'On Basilisk Station' a try, since I thoroughly enjoyed 'Daemon' after you praised that. I downloaded the free version to my iPad but was dismayed when the opening prologue was unnecessarily confusing. It seemed to introduce a new character in every other paragraph and was so jam-packed with exposition that it was hard to follow. So I stopped reading.

"Then the following week you praised it again, so I thought I'd give it another shot. This time the prologue didn't seem confusing at all as I reread it, and I made it through nearly 20 percent of the text before I got distracted and put it aside. Although I was enjoying it, it didn't grab me. It just didn't seem so compelling that I had to know what happened next.

"Then for the third week in a row you sang its praises once more. So I decided to try again. Literally, and I do mean literally, within two pages of where I had left off, the author introduced a character conflict that piqued my interest and curiosity. Within just a few more pages I was hooked. I see what you mean about David Weber's writing. He's a master of plotting. He lets events unfold in a way that you think you know where the story is going, and then in the next chapter he completely subverts your expectations in a good way. Anyway, thanks again for *repeatedly*" - again in asterisks - "recommending this series. I'm hooked now, and I wouldn't have been if you hadn't talked about it three weeks in a row." Okay, count 'em, four now. But this is it, I promise. "Thanks. And tell Leo that he's crazy if he doesn't drop everything in his reading queue to read 'On Basilisk Station' right away." Okay. That's one. The next two are shorter.

TOM: Okay.

Steve: James Ford on the 7th of October in Apple Valley says: "Based on your enthusiasm and recommendation, I read 'On Basilisk Station.' I absolutely loved it and immediately knew I had found a series that I was going to complete. Then I read 'The Honor of the Queen,' and I only have one word for it: 'Wow.' I understand why you had tears in your eyes. And I had them also, but they were wiped away with the culmination of the final battle. The few words that describe the battle's culmination provided me with a big internal cheer and a visible fist pump. I've started 'The Short Victorious War' knowing I will enjoy it, but I am wondering how any of the rest of the series is going to top 'The Honor of the Queen.' I'm a Trekkie from way back, watch and love a number of programs on Syfy, but for some reason I've not been much of a reader of science fiction. But this series changes that. Thanks for turning me and the other Security Now! listeners on to the Honorverse series. P.S.: David Weber is a very good writer."

And finally, just a tweet: Mike Lopez in Coconut Creek, Florida, he tweeted me that Book 3 was amazing. And so I sent back something like, "Oh, great, thanks," because I'm not allowing myself to read anymore until I'm - only now when I'm on the stair climber am I allowing myself to read these. Otherwise I will get nothing else done. So he sent, "Sorry, Steve, but I had to share. Honor Harrington Book 3 is awesome. I know you have many projects to complete, but this book really kicks it up. I'm listening to the books on Audible, makes it easier when trying to watch a three year old. And the narrator does an amazing job portraying all the characters. I am excited to continue the series and look forward to your feedback on Security Now!. Thanks for the great podcast. I'm a Citrix admin for a large health insurance company, and the info provided in Security Now! is vital to my role." So there you go, folks. I've said all I'm going to say about Honor Harrington. You can read the first two for free.

TOM: Don't believe him, folks.

Steve: [Laughing] You're heard from our listeners. They're really good. So we're done.

TOM: Well, you know what, I'm not going to give you a hard time because I was going on about "Ready Player One" by Ernest Cline for about the same amount of time after I read that.

Steve: Okay.

TOM: So I understand the impulse. I'll definitely have to check these out. I'm reading "Reamde" by Neal Stephenson right now.

Steve: Okay, right.

TOM: I want to finish that.

Steve: I just did finish "FreedomTM," and so I have now been able to start on Book 3 of the Honor Harrington series. I'll be taking it slowly because I only read while I'm on the stair climber, which is good because it paces me, and it's going to keep me from just sitting down and reading them all in a week and getting nothing done, as one of our listeners did. So, oh, no, that was the Lost Fleet series. He read all six in, like, less than a week. So it makes it go over - it makes it end too soon. So I'm happy it's going to be strung out a little bit.

TOM: Hey, before we wrap up, I just wanted to note the passing of Dennis Ritchie. We just found out about it. He passed this last weekend, creator of C, big contributor to the founding of UNIX.

Steve: UNIX, yup.

TOM: And you want to talk about somebody who affected your life, if you're watching this show, you're using something that Dennis Ritchie helped to make possible.

Steve: Yup, absolutely.

TOM: So it's sad to see him go, as well. Yeah, it's been a sad couple of weeks in technology, for sure.

Steve: Yeah, our pioneers and founders.

TOM: Yeah. Well, thank you, Steve. It's been great hosting Security Now! again, and I really enjoyed it.

Steve: And you go to do Feedback #128, nice power of two episode.

TOM: That's right.

Steve: And I'm sure you'll be back next time Leo is not.

TOM: I will, absolutely. You know I love it. Don't forget to try out ShieldsUP!, try out SpinRite, all the great things at GRC.com. Anything else we need to mention before we take off?

Steve: I think everybody knows they can send me feedback at GRC.com/feedback. I did ask people to, if they want to send me feedback about Honor Harrington, just put that in the subject line. And that's how I found these and many, many others from people who are really having fun doing reading when they're not listening to the TWiT podcast family.

TOM: Excellent. Well, Leo will be back from vacation next week. Until then, stay safe out there. That's it for Security Now!. We'll see you next time.

Steve: Thanks, Tom.

TOM: Thanks, Steve.

Copyright (c) 2006 by Steve Gibson and Leo Laporte. SOME RIGHTS RESERVED

This work is licensed for the good of the Internet Community under the Creative Commons License v2.5. See the following Web page for details: http://creativecommons.org/licenses/by-nc-sa/2.5/