SECURITY NOW!

Transcript of Episode #231

Mega Security Update & CES Observations

Description: Leo and Steve catch up on two busy weeks of security news with a "mega security news update" ... and Steve, who watched Leo's streaming video coverage of CES, weighs in with his own discoveries and findings from the big annual consumer electronics fest.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-231.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-231-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 231 for January 14, 2010: The Security Omnibus and CES Update.

It's time for Security Now!, Episode 231 in a continuing saga of pain, sorrow, and insecurity. Here's the man protecting us from it all, Mr. Steve Gibson of GRC.com. Hi, Steve.

Steve Gibson: Just what everyone wants.

Leo: Tune in for the...

Steve: A chronology of pain, sorrow, and misery.

Leo: Yeah, it's a real uplifting show. Actually, it is, believe it or not, it is an uplifting show because one of the things you get out of it is a sense of what you can do, what's really going on. So I think that that's not an unreasonable description. It's just not sad.

Steve: Well, it's funny because when I was killing some time before we started, before we got online, I went over into the chatroom. And my handle there is Steve Gibson. And they said, "You're not Steve Gibson." I said, "Yes, I am." They said, "TNO. You taught us, trust no one."

Leo: Yup, yup.

Steve: And it's like, okay, I guess you have been listening.

Leo: And how did you prove your...

Steve: Well, I didn't have a chance because you showed up. But I was saying, okay, let me think. Someone type a really long number, and I'll put that on GRC's home page.

Leo: Oh, that's one way to do it, yeah.

Steve: Yeah. Since I have control of that, and hopefully someone pretending to be me doesn't.

Leo: So we have, because we pretaped a little bit because of CES last week, we have quite a bit of news to talk about.

Steve: Well, yeah. And there were even some, not Y2K, but some Y2KX problems you probably heard about.

Leo: Oh, all right.

Steve: Microsoft has apparently solved the concern people had about the end of the world occurring, as you know, in 2012 by sending text messages from the future, from 2016 back to the present.

Leo: Just to see what would happen, huh?

Steve: Well, the fact that they were, these text messages are coming to people from 2016 proves that the world didn't end in 2012.

Leo: Well, there you go.

Steve: So I guess we've got that problem solved.

Leo: It's a little bit of sci-fi.

Steve: And anyway, we've got so much stuff to talk about that we're just going to do sort of a mega, one of our mega security updates. And then I was very impressed, Leo, with - I hope you were as happy as I was, as a viewer, of your CES coverage.

Leo: Thank you.

Steve: I think it went really well.

Leo: I believe it went very well, indeed, yeah.

Steve: Yeah, I saw Geordi and Data.

Leo: Wasn't that fun?

Steve: Live while they were - while you were interviewing them. It was really fun.

Leo: We've had Geordi - LeVar Burton - on the show several times on TWiT. But I had never met Brent Spiner, who played Data on "Next Generation." And he is a funny, cool guy. I really liked him.

Steve: Yeah, he was neat. Very relaxed and, you know, not - his skin is not silver tone, either.

Leo: No, no. Although he's extraordinarily pale.

Steve: Anyway, so I wanted to sort of chat with you about CES stuff. And I did prepare a page that is the show notes for this episode of just sort of a collection of links of interesting things that I ran across, that you and I will discuss and that our listeners can grab that page themselves, the show notes on GRC for this episode, if their curiosity is tickled by any of this.

Leo: I'm looking at our outline, and there's a big security story. And I'm sure because it broke so recently you probably haven't had time to digest. And I would love it if sometime, maybe next week, we could talk about it, which is Google announcing that massive attempts had been made to break into it and other major U.S. corporations - apparently Adobe is the other one - from China to get information about Chinese dissidents. And this so infuriated Google that they finally did the right thing, which is to say, well, that's it. We're not going to send search results anymore on our Chinese version.

Steve: Right. And in fact they're thinking maybe about just shutting down their operations entirely. They've got a beautiful shiny building in Beijing, and they're saying, ah, well, maybe this is not where we should be.

Leo: I think they're hoping that the Chinese government will say, okay, you don't have to - because I guess what they're saying is, if this may violate the law and probably does in China, we don't want to be in a country where we're violating the law. So we'll just exit China, if they say so. Or they'll give us an exemption. But I think this is great. I'm very pleased that Google is doing this. And you can now search Google.cn and find, for instance, pictures of Tiananmen and the massacre 20 years ago. You can find Falun Gong, all of these things that the Chinese government does not want.

Steve: Oh, so Google has lifted their constraints at this point, their own search censoring. And now they're waiting to see what China's going to do.

Leo: Apparently. Because if you go to Google.cn and search Tiananmen massacre - well, wait a minute. Let's see. Do you find - maybe you don't. Maybe you don't yet - yeah, you do. Standoff at Tiananmen, you do find - this is an image search. Somebody just sent me a link from Google.cn of Tiananmen massacre, in fact you do find some links. StandoffatTiananmen.com, yeah, you find quite a bit. So...

Steve: I did read also, as part of this, that Google will be changing the way they operate. And apparently there were initially a bunch of press stories that talked about this. And then those sort of disappeared off the web. And now there's the official story from the official Chinese news agency with something that sort of says, well, we're not really sure what's going on. We're going to be taking a look at this, and we'll get back to you, so...

Leo: Yeah, yeah. Be very, very interesting to see what happens. And of course I'd love to hear from Microsoft and other search engines to see if they are willing to go along because of course that's when you have the force, the clout, is when everybody says, okay, see you later. Google only has 31 percent of search in China, so it's not the end...

Steve: And they're losing market share, actually. Their share is dropping relative to the official Chinese search engine.

Leo: Yeah. That's kind of odd, isn't it.

Steve: Well, I mean, fundamentally the Internet poses a problem for a government such as China's that wants to constrain and constrict and control what its people can see. I mean, that's the problem. Google happens to represent an aspect of it because they're the searching technology that allows people to find stuff. But fundamentally the problem is the Internet is at odds with the...

Leo: Absolutely.

Steve: ...policies of the Chinese government.

Leo: There's the problem in a nutshell. And I just - I'm thrilled that Google did it. And what I'd like to know more about, and of course we don't really know yet, is what hacking was going on. They said that dissidents' Gmail accounts have been hacked, but because of phishing scams or trojans that have been placed on their computers, not through Google; and that Google believes that nothing of importance was stolen. However, they do say intellectual property was stolen by China. And boy, did that piss them off.

Steve: Well, and they said it was very sophisticated attacks. I mean, not just random hacking quacking guys, but, I mean, people who really understood how these things work apparently really, really came at them. So...

Leo: Yeah, boy, it's fascinating. All right. While we were gone, let's see, there was a Patch Tuesday.

Steve: Oh. Yeah, I mean, all kinds of stuff.

Leo: Lots and lots of stuff. Mega security update.

Steve: Two days ago we had, not only Microsoft's Patch Tuesday, but Adobe's Patch Tuesday. But they've also announced, Adobe has announced a change that we'll be talking about soon. I knew, and we were talking about, how this Adobe's quarterly security update policy, well, it didn't even last the first quarter because they had an emergency update. And they decided, okay, we're going to change the way we do that.

But Microsoft, two days ago, we had the second Tuesday of the month, which was Patch Tuesday. They fixed only one vulnerability, which was only critical under Windows 2000 due to the way the OS used the problems. This is something that we had talked about before previously that had not been patched, which was a problem with the OpenType vulnerability. There was a - when OpenType is compressed, as it normally is as it's, for example, shipped to a web browser, the decompression algorithm had a buffer overrun which was exploitable. There was also something strange they did. In the font structure there is something called a name table where text could be put in. And a previous security update limited the length of the strings in the name table to 5,000 bytes. And since this is all Unicode, which is to say two bytes per character, that was 2,500 bytes. Microsoft apparently thought, oh, that's, you know, no one's going to have font name metadata that's longer than 2,500 bytes. Eh. Wrong. It turns out that some fonts have the entire license agreement from the font vendor stuck in the name table.

Leo: Oh, great. Of course. Why not. Sure.

Steve: [Laughing] So that previous - it was back in '09 - that security update broke this particular font family for anyone who had, believe it or not, strings larger than 2,500 Unicode characters. So one of the other things that they fixed was they restored it to what it should have been, which is 64K, if you can believe it or not, which is to say 32K Unicode characters.

Leo: Which is good until somebody decides they want to put "Moby Dick" in the font name space.

Steve: It's just nuts. Now, significantly, we did not get something that we were hoping for with this Patch Tuesday, which is the zero-day flaw in the SMB, the Server Message Block protocol. That's still hanging out there, flapping in the breeze. And it's not a huge problem, only because today very few systems will be exposing their SMB ports to - that's Microsoft windows and filesharing ports, essentially.

Leo: It's ironic because this is what got you started, way back when...

Steve: Yeah.

Leo: ...is when you saw all those open port 135s and all those open shares.

Steve: Exactly. I realized, okay, this is really a bad idea.

Leo: Now, that was NetBIOS. SMB is different; right? It's [indiscernible]. Or no.

Steve: Well, that was NetBIOS. But it's the same set of ports.

Leo: Oh, okay.

Steve: And Microsoft has dramatically overloaded the role of those ports. They use them for all kinds of things. For example, remote registry is there, and all kinds of sort of intermachine services...

Leo: Just the words "remote registry" send a chill down my spine.

Steve: Yeah.

Leo: What a terrible idea.

Steve: But just, Leo, you really have been paying attention.

Leo: That's just a nasty idea.

Steve: Getting the hang of this security stuff. Yeah, it's like, that's a really bad idea. Why, you know, let's just have our registry...

Leo: Sure, let your registry...

Steve: And it's running by default, too. I love that. It's like, by default...

Leo: What? Wow.

Steve: ...remote registry service is running in Windows. Now, the good news is, with Windows Firewall and of course being behind routers, we've got multiple layers of protection. So those ports, even though they are open and this SMB protocol flaw is there, you can't get it from the outside. The problem is that you can get it within a LAN. That is to say, so one of the things that we're seeing is, we're seeing trojans which we know like to spread within a Local Area Network once some employee brings an infected laptop into work and plugs it into his hub at his desk. If there's something bad there, it'll just go like wildfire. We've seen trojans that use open window shares to jump from machine to machine. Unfortunately the Server Message Block protocol flaw is available and exposed within a LAN.

So anyway, I can't explain Microsoft not fixing it because it's not good. There's proof-of-concept code. It's in the wild. It's being exploited. But we didn't get it this Tuesday. I'm sure we'll get it next month. But it's going to be a long month.

Now, Adobe also patched another bad Reader vulnerability which is being actively exploited. It's one where it's being used both for targeted and sort of just widespread use. It uses a problem with Reader that's exploitable by opening a PDF, which of course has become now the universal document-sharing format. On my system, I went from 8.1.7, which was the last update I had, to 8.2, although I'm still on the v8 track, and there's a 9 that is the most recent. Strangely enough, too, I thought, well, this morning I thought, I ought to update myself to that, because I had some problems under Firefox with PDFs not opening smoothly. And I thought I'd update myself to the 9 because it's time. And I went through all the download process and update, and it didn't happen. I'm still at 8. I don't know where it went or what's going on. But I'll figure that out.

However, I wanted to bring this up to our listeners because I had to go ask for it deliberately. That is, I didn't get an automatic notification from Adobe. So I had to open a PDF document to get the Reader running, then under the Help menu did a check for updates. And it said, oh, what do you know, we fixed this horrible problem, so you should get the update, which I did. And I'm now at 8.2. Significantly - and we'll talk about this a little bit later in the show - the expectation is, among the security community, that Adobe this year, in 2010, is going to surpass Microsoft as the number one target for attacks due to the continuing problems.

Leo: Well, because they suck.

Steve: Yes. The huge number of vulnerabilities that are continually being found in Reader and in Flash. So, I mean, it's no surprise.

Leo: Of course, yeah.

Steve: The one thing I would reiterate saying, and I imagine people have probably already done this if they're going to, but I have to say it again, is disable JavaScript in Acrobat, that is, in the Acrobat Reader. There just is no need for scripting. I mean, we understand there's a need for scripting on web pages because it's being actively used by more and more websites, with it being a mixed blessing. But there's just no need for scripting in a PDF document.

I mean, maybe there are corporate settings where corporate IT uses scripted PDFs for some business-oriented infrastructure glue, I mean, I don't know. But typical PDFs just sit there. They don't have to run code. There's no code in them. And so you don't want your Reader to have scripting enabled when you virtually never need it. And if you do need it, you probably know you do. If you don't know you do need it, then you almost certainly don't need it. So disable it. Now is a good time.

And on the topic of Adobe, they've announced that they are going to be beta testing silent updates. They've been watching Google with Google's Chrome browser sort of succeed at that, where Chrome just sort of checks in with the mothership every so often, and pretty often, and quietly keeps itself current. So this is Adobe's new strategy, apparently, for not waiting three months between major updates, which they've never succeeded in doing because the problems they're having are so critical that this notion of updating quarterly, which we knew when we heard about it a year ago being ridiculous, turns out to have been exactly that.

So what'll happen is, if the "silent update," as they're calling it, beta test works as well as they expect it to, then with perhaps the next major update, for example to Acrobat Reader 10, they expect that technology to be in there and enabled by default. Users will have some control over it. You could go in and turn it off if you wanted to. But basically...

Leo: Do you think it's a good thing? Silent updates?

Steve: I have mixed feelings about it.

Leo: Me, too. Isn't that funny.

Steve: Yeah.

Leo: Yeah.

Steve: Yeah, you know, I don't have any of my systems completely automatically update my Windows updates. I have them download them and notify me because I want control over when this happens. The other problem you have is, as we know from lots of practical experience, updates don't always work. Sometimes, you know, for me I still have, on my main system, I can't put Service Pack 4 of XP on. It just doesn't work. For whatever reason, the configuration is hostile to it. So the problem with silent updates is, if you had a silent update which caused a problem, there's a break in the causality. You wouldn't know why something suddenly wasn't working, something broke. But if instead you say, okay, now's a good time to reboot my system, I shut things down, install updates and do a reboot, if when it comes back up something's broken, I know why that is. I know what I was just doing that caused the problem. So there's that problem. And, I don't know, I guess I'm still of the school that would sort of like to have a little more control.

Leo: Most businesses, I would imagine, wouldn't be thrilled about this; right? They'll turn it off right away.

Steve: Yeah, I imagine. And they may have something at the gate that will automatically turn it off.

Leo: Ah, yes.

Steve: In the same way that, for example, it is possible for Microsoft's updates to be aggregated by corporate IT, and then for them to be vetted and tested on the default corporate platform. And then they're pushed out locally to all the systems in the corporation.

Leo: Right, right.

Steve: And I know that you talked about this. I actually, while I was watching a rerun of you talking with, I guess it was MacBreak Weekly probably, you mentioned that Mac OS X, and it happens to be .5 and .6, is like the last standing OS that hasn't fixed a potentially very bad problem.

Leo: It's a significant problem.

Steve: And it was finally put - a proof of concept was put out on the Internet because security firms just got tired of waiting. It was in June of '09 that the industry was informed of this problem. It's actually in a string to floating conversion. It's the strtod. It stands for string to double precision. So that's the - it's fundamental code in the standard C library that converts a floating point string into a double precision binary result. And that's a tricky thing to do. You can sort of see, okay, that would, you know, you'd want to make sure you were doing that right. And so it's in this string text parsing that they've got.

Well, OpenBSD, NetBSD, FreeBSD, they all jumped on it and fixed it immediately. It was possible for the browsers to make sure that they were doing it correctly. So the various browsers - Chrome, Firefox, Opera - they got their acts together. And we talked about this months ago. Well, for whatever reason, Apple just didn't address the problem. And it's still there now. It is a remotely executable exploit. So it's something that Apple needs to get on the stick about. And...

Leo: It's unfortunate because Apple is not communicative. And this is what we talked about in the podcast is just tell us. But that's not how they do it. And so are they working on it? What's going on?

Steve: Yeah, well, and we've talked about this, too. Apple has a different approach to security. I would say that the open source guys like Mozilla, they're probably the most open because their source is open. So they lay out everything about what it was that they fixed. Next less open is Microsoft, that because they've just been in the vanguard of problems for so long, they developed a security process that is, eh, it's pretty open. They announce the things they're going to fix in a very vague way before Patch Tuesday. And then, when the fixes are actually there, they tell us a lot more about them. And because they're just such a high-profile target, pretty much the industry knows a lot about what it is that they are fixing at that point. And then arguably among the most closed is Apple, that just says, eh, we fixed some things. Trust us.

Leo: We'll get there.

Steve: It's better than it was.

Leo: Yeah. You don't want to - you don't need to know. Just trust us.

Steve: Just click on Okay and move on.

Leo: You don't need to know that. It's nothing you need to know.

Steve: So it's their choice that that's the way they want to be. And I'm just, you know, I think it's unfortunate that, well, I don't know. I mean, it's good that they're fixing these things. This one they've got to get onto now. And I think with all the attention that it is now getting, thanks to the fact unfortunately that someone had to say okay, here's how you would do this on a Mac OS. So, Apple, fix it.

Leo: They'll get on it. And when that happens, Apple always gets on it; you know?

Steve: Yeah. Also something that we talked about last September, early September, in our Security Now! Episode 213, was about - the title of the episode was "Cracking GSM Cell Phones." And that was a follow-up to a conference that was held in August where the announcement was made that a group of hackers were going to pursue the issue of cracking GSM further. We talked about, then, how it's an old crypto technology. I think it's - I think 1988 was when the GSM cipher was created. And on 1988's hardware it wasn't feasible to do really powerful crypto. So they came out with sort of a lame pseudorandom number generator based on feedback loops whose security was based on secrecy. Well, we know how well that works, especially when the world's got all these GSM cell phones.

It turns out that 80 percent of cellular traffic is over GSM. There are a total of 4.3 billion cell phones in general use, 3.5 billion of which are GSM phones. So what's happened is, at the 26th Chaos Communication Congress in Berlin, the lead person, Karsten Nohl, he made a presentation announcing that a group of, I think it was 24 hackers, working since August, had produced the full GSM codebook. It's a 2TB blob of data. But it essentially reverse-engineers the effect of the pseudorandom number generator so that using that, and with sniffed GSM cell traffic out of the air, in a matter of hours you can now decrypt and hear the audio of that conversation.

Leo: Wow.

Steve: So the GSM Association made the powerful point that what Nohl did was illegal. Okay, well, that didn't stop him any. They have a site that we talked about before. It's Reflextor.com/trac/a51. And again, referring back to our Episode 213, the A5/1 cipher has technically been obsoleted. There is an A5/3 which is state-of-the-art security. The problem is, no one has moved to it because of inertia, because there's this huge install base of existing cellular GSM infrastructure that doesn't know about /3. It only knows about /1.

So once again, these guys are - the hackers have been very careful. They've been explicitly trying not to break laws, that is, they say, for example, we have never deciphered a single anyone's phone conversation. We've made our own audio using GSM, and we've decrypted it, we've verified that we can do this. But we're not promoting illegal action. We're trying to say, you know, trying to further our message that GSM, this 80 percent used technology is unfortunately no longer safe enough, so to basically crank up the tension on GSM to get people to move, not off GSM, but just up to the /3 standard, which is strong enough for today.

I noted that my Firefox updated. This is actually my last system that had Firefox 3.0 on it.

Leo: It's about time.

Steve: [Laughing] Yes, Leo. It no longer does. But it was on January 5. And I thought, well, isn't that interesting. I thought we weren't going to get any more updates of the Firefox 3.0 line in 2010. But this was important enough that the Mozilla guys decided, okay, well, we'll do this one last time. I do urge our listeners to move to 3.5. When I originally tried, when it first came out, I got a bunch of complaints from the add-ons that I had installed. I held my breath and did it again at the beginning of this year. Not a peep.

Leo: Yeah, everybody updated.

Steve: All of the add-ons that I have worked without any problem at all under 3.5. So if anyone has been lagging behind, I would say now's the time, since Mozilla will be dropping further support of it. And be a good thing to do.

Leo: That is what slows people down is you want to make sure all your add-ons work. But everybody's updated. If they haven't, then they're not going to because they're just not paying attention anymore.

Steve: Well, and I was similarly slowed down. Remember that, you know, here I am now, Mr. Firefox. But I was way lagging behind, staying on IE just under some irrational fear that I didn't want websites not to work. And I've been now on Firefox...

Leo: Oh, everything works.

Steve: It absolutely does, yes.

Leo: So let's talk about banks. Geez.

Steve: Well, I just got a kick out of this. The American Bankers Association...

Leo: This is so crazy.

Steve: Not the ABA that we're normally - the Bar Association. This is the Bankers Association has made a formal recommendation for businesses to use a separate PC...

Leo: A clean machine.

Steve: Yes, a clean machine for whenever they're doing any online banking.

Leo: Oh, please.

Steve: The problem is that banking trojans - and this is one of the trends that we're going to talk about a little bit later in 2010. There's the expectation that these banking trojans are going to become increasingly sophisticated. Already they're pretty amazing. The Torpig trojan is the one that I've got on my list of things to do a complete forensic analysis of and to talk to everybody about in a future podcast. But the problem is that there have been now several security advisories warning about the so-called ACH, the Automated Clearing House transactions, the idea being that a corporation uses the much-encouraged online banking interface to do their major work now, to move funds from one account to another, you know, wire transfers and fund management. And the problem is that there are an increasing number of exploits that are getting into machines and doing increasingly sophisticated work.

I should say that when I first ran across this report, maybe that these ACH transactions were being victims, I immediately literally called my operations gal, and I said, Sue, I want to make sure that we don't have any of that enabled. I mean, even though, you know, our operations are pretty simple, we're not a big corporation, I know that, you know, when we move money from one place to another, it's just not a burden for us to require that a check gets filled out and physically taken to the bank to move funds from one place to another.

And so I don't know if all of our accounts had that explicitly disabled, but they do now because it just, you know, again, it's you don't want things turned on that you don't really need to have turned on. And so we formally verified that our bank would never accept any kind of electronic funds orders from us or anyone, I mean, not even from us, because of course the whole idea is that our own identity would be spoofed if something ever got into any of our machines. So anyway, I did get a kick out of the fact that the solution the ABA has is use a clean machine.

Now, I understand that, too, because when I've been speaking in front of groups and have been giving presentations, I remember I spoke actually once to the American Bar Association. I was a keynote speaker at a conference they had in Chicago many years ago. And I said to them there, I said, here is my number one piece of advice. Give your kids their own computer. Now, back then that was a big deal. Today...

Leo: No kidding. Now it's obvious.

Steve: ...all the kids probably already have one.

Leo: Right.

Steve: But back then, like, two computers in the family - this was, I don't know, 10 years ago - was a much bigger deal. But I said, there's no way you can control what your kids are going to do on the Internet. You can imagine you're going to control them, but you can't. Their friends are going to bring over some software. They're going to stick a CD in the computer, whatever. I said, the idea of Mom and Dad then sitting down and doing online banking with a machine that's been in teenagers' control for the last four hours after school is nuts. You don't know what it's got in it any longer. So my advice then was give the kids their own computer, and make it an official policy that this is Mom and Dad's machine.

Leo: Don't touch it.

Steve: Exactly. This is not a toy. This is for serious work. So anyway...

Leo: You know, it's funny, I use EFTs all the time. Am I really crazy? Should I stop? I mean, look. I'm using a Mac. C'mon.

Steve: You're - right. So you're a smaller target. That's definitely the case.

Leo: Are those - wait a minute. Okay. I'm sorry to interrupt. Are those PDP-8s behind you? I just noticed on the video. You've got blinking lights over your left shoulder.

Steve: Yes. I've got that as a topic toward the end of our...

Leo: Okay. We'll just talk about - and for those not watching the video, forget I said anything. But for those watching the video, it looks like war games behind Steve.

Steve: For those not watching the video, I now have online videos. I've got Flash videos of my PDP-8 project.

Leo: Oh, that's wonderful.

Steve: We'll be talking about it at the end of the show.

Leo: Okay. We'll talk about that later. I didn't mean...

Steve: Yeah. If it won't distract you, there's a new menu item on the GRC main menu, "Other." And it has a link to the front page, and there's some videos there. But we'll talk about that in a minute.

Leo: That's great. I love it. Go ahead. I'm sorry. I didn't mean to interrupt. I just noticed. Oh, my goodness. So, yeah. So you think EFTs are, well, I think they're risky. I'm on a Mac. But I guess I should know I'm taking a risk.

Steve: Yeah, I mean, I can't say that it's - I would agree with them, that is, the American Banking Association, that having a machine, you know, what's a laptop cost now? Five or 600 bucks for one which is certainly powerful enough to do online banking.

Leo: And you should do nothing else with that machine.

Steve: That's the key is that you have to really behave yourself. And I would even go further and say maybe install the Microsoft, what was the thing that Microsoft has that...

Leo: SteadyState.

Steve: SteadyState, exactly.

Leo: So it resets itself. Of what if, how about this, what if I use a virtual machine on my Mac? Because I don't want to use Windows. Now, which is more risky? Using virtual Windows on my Mac, or just using the Mac?

Steve: Yeah, see, now, the question is whether that creates protection for you because the virtual environment has to pass out through the nonvirtual environment.

Leo: True, true. Good point.

Steve: So if the outer wrapper were infected, it's not clear that the traffic coming from the protected inner machine would get any protection at all.

Leo: Right.

Steve: So, I mean, again, I don't want to overly alarm people. But it's worth being aware that what we've seen over the last couple years is a clear change in orientation from hacking for sport to hacking for money. And it's about money. If the hackers, the bad guys believe that there's some way they can transfer funds from your account to theirs, gee, that seems like something that's going to get their attention more than, oh, look how many copies of this worm has spread around. So...

Leo: Somebody in the chatroom suggested this would also work very well, a Live Linux CD.

Steve: Ah.

Leo: Because you can't write to it, and you know it's known good every time you boot it.

Steve: That's an absolutely - that's a superb idea, is a CD that you're booting that brings the OS and a file system, basically in a frozen state. It comes up. The browser's going to be clean. Because you've rebooted, anything that was there in the OS has no chance to seize your system. So yes, that's a great solution.

Leo: Of course now banks kind of defeat this because I know, at least when I log onto my bank, if it says, oh, I haven't seen you before, and you have to go through some extra steps, and then it stores a cookie in Flash, probably...

Steve: Good point. So...

Leo: So I'd have to do that every time. That's all right.

Steve: Yes, you would lose the authentication. On the other hand, that's really what you want because it's the authentication hijack which is what these things use, is the fact that your computer is known to the bank. So behind your back...

Leo: Right, starting over is good.

Steve: ...it's able to open up a session and do whatever it wants to.

Leo: So from now on, boot a Live CD operating system of your choice and put up with the extra authentication. And that's how you get online. That's how you bank.

Steve: It would make sense...

Leo: That's a good idea. I can...

Steve: ...to do just that. It was actually a great idea.

Leo: And that's not a hard thing to do. I could do that.

Steve: Yeah. And how often, you know, couple times a month probably.

Leo: Yeah, right. I think it's worth doing.

Steve: The BBC reported that France's new antipiracy law went into effect on January 1st.

Leo: This thing's ugly.

Steve: Yeah, it is. It's caused a lot of controversy. It's going to be interesting to see, I think the whole industry is going to watch now to see what effect it has. The people who are for this are stating that, okay, well, first of all, the way it works is, if you are - if an Internet end user is found or believed to be breaching privacy, or piracy, sorry, piracy laws by downloading copyrighted content...

Leo: Believed or accused? Really accused is the word. If the third parties who create content decide that you've done it, that's it. You've been accused.

Steve: Well, through your ISP you first receive an email notification and warning to cease and desist this behavior. If you fail to cease and desist the behavior, again you receive...

Leo: Again, according to the accusation of these third parties.

Steve: Exactly. Then you receive a written notice in the mail. And then, if you still persist in being accused of this behavior, then you need to appear before a judge to explain what's going on. And he has the opportunity to fine and/or suspend your Internet access. So the proponents of this believe that there will be a major reduction behavior.

Leo: They also believe in fairies, I might add, but okay.

Steve: I think they said they expected almost 85 percent of...

Leo: Oh, please.

Steve: ...people who receive the email notification would abide by it. It's like, oh.

Leo: Well, yeah. You don't want to take a chance of never being able to get on the Internet again.

Steve: That is a - that's...

Leo: The point is, you know, this is this horrible ACTA Treaty. And the French modified it slightly to add the judge part at the end because the original plan, and this is a plan they're trying to get through in a lot of countries, including ours, is just three strikes and you're out, with no judicial oversight and in fact no due process.

Steve: Yeah.

Leo: Pure accusation. And you can see how it starts. They only have to accuse you three times. They don't have to prove it. They don't have to do anything. Then the judge gets to decide.

Steve: Yup.

Leo: It's a terrible law.

Steve: Yeah, I mean, it seems to me, I mean, I'm with you, Leo. I'm really glad they added the human element with the judge because at least you're able to say, Your Honor, I have no idea what you're talking about. Now, he can choose to believe or not based on what evidence he has and so forth....

Leo: Well, and Dr. Mom's pointing out that France uses the Napoleonic Code, which presumes guilt until proven innocent. It's the exact opposite of ours. And this is exactly what this is. You're guilty until you can demonstrate you didn't steal.

Steve: So this thing has been in effect now for 13 days, 14 days. We'll see what happens. I'm sure people are going to be watching to see what effect this has. Don't know.

Leo: It's appalling, appalling.

Steve: A six-member bipartisan group formed from leaders of the U.S. House Ways and Means Committee, Energy Committee, and Commerce Committee wrote a formal letter of criticism to the proposed regulation for what's called the Protected Health Information Act, the PHI Act. The Secretary of Health and Human Services, Kathleen Sebelius, posted what they were going to propose for managing breaches of health information. And believe it or not, the language in what they were proposing said that organizations who had an information, a health information breach could decide not to notify patients of that breach if the organization determines that it, quote, "...presents no significant risk of harm." So anyway, so I got a kick out of an editor who writes for SANS who commented that the banks also believed that their investments offered no significant risk several years ago.

Leo: Right.

Steve: So, I mean...

Leo: We're safe. You're safe.

Steve: It's ridiculous to propose rules where somebody who lets their personal, private, protected health information escape can then say, hmm, gee, you know, there's this rule that we're supposed to let people know, to disclose that we've had this breach of health information, unless we determine that it doesn't really present any risk of significant harm. I don't think this does. So let's not tell anybody.

Leo: Don't worry about it.

Steve: It's just, yeah.

Leo: No big deal.

Steve: Anyway, the good news is it doesn't look like that's going to stand.

Leo: You should be compelled to notify of all security breaches, period.

Steve: Yes. Yes, exactly.

Leo: Every case.

Steve: And this constitutes a security breach. And people whose personal information has been disclosed, I mean, and here we are, one of Obama's main thrusts is automating medical records management in order to reduce costs and prevent duplication of procedures and so forth. And so I've talked to my own M.D. about this during my annual physical. And I said, so what's your story? Because, I mean, when I walk by his front office he's got, you know, a wall of paper records and, you know, manila folders. And whenever he comes into my little - in the little patient room, it's all paper. He's not bringing my stuff up on any kind of a laptop screen or anything in his office. He's all paper records.

Leo: Oh, it's all digitized for me. All of my records are in the computer.

Steve: Interesting. Anyway, he has said - and he actually is very tech savvy. He was bragging about the size of his network storage that he's got in his home. So it's like, okay, well, that's cool. You know, I have a tech-savvy M.D. And he's also very leery of stuff going online. So I said, well, believe me, I'm Mr. Security. I'm all for being cautious about it.

Leo: Yeah, and of course it's the big governmental initiative to put everything online. That's what they're doing.

Steve: Yeah. It'll happen sooner or later.

Leo: It's going to happen.

Steve: Yup. McAfee does an annual security predictions report. Theirs is out for 2010. And I referred to one of their predictions earlier. They have stated that Adobe will surpass Microsoft as the most-often-hacked target in the industry. And of course, again we're...

Leo: Our friends at Adobe.

Steve: ...constantly seeing problems with Reader and Flash. One of the things that is attractive to hackers is this solves the multiplatform problem to some degree. Now, it's still the case that the hacks tend to be platform-specific. So even though Reader and Flash are multiplatform, you and I have talked about this before, where there have been exploits which have leveraged, for example, recent Flash vulnerabilities. They only worked on Windows because, even though the vulnerability allowed an in, the exploitation of that into the operating system was Windows specific. So it's not clear to me that their multiplatformness means multiplatform risk. At least we haven't seen that so far. We haven't seen a true multiplatform exploit of these multiplatform vulnerabilities. But I wouldn't be surprised if that happens in 2010.

Also it's expected per McAfee's security predictions report for 2010 that banking trojans will continue to increase in their sophistication, again, because it pays. These things are transferring money into nonlocal accounts away from users. And in fact, for example, one of the ways these trojans work is that they get into a user's machine, and they remain dormant until the user brings up a banking site that the trojan knows about. Current banking trojans are aware of hundreds of banking sites.

Leo: Oh, interesting.

Steve: They contain a configuration file where they're able to recognize hundreds of banking sites. And they're able to mimic the design and layout of those banking pages. One of the things they do, and this is the episode that we talked about where SSL, that is, the "S" of HTTPS is stripped off of the URLs so that without the user knowing, they don't actually have an SSL connection to the bank. They believe they do. But what that allows then is the trojan to filter the returning pages. Trojans are smart enough to add fields for the users to fill out, such as their credit card number, their ATM PIN, and so forth.

Leo: The appropriate ones, too.

Steve: So it's just literally, where you would normally be filling out a form, there's some extra fields that have just been slid in by the page coming, as the page comes back to your computer. And so, you know, what user wouldn't fill that out? They would think, oh, well, the bank needs to have this as part of the information that I'm filling out.

Leo: Absolutely, sure.

Steve: And this stuff is actually happening today. So that's the level of sophistication that we're beginning to see. And then the other, the final prediction was that McAfee expects to see more targeted attacks. They're seeing targeted attacks on the rise, using email as the increasingly preferred vector. The idea being, for example, that a PDF will be sent to journalists as a link or an attachment in email. And a journalist will receive email that's, you know, a press release, the kind of things that journalists receive all the time who are covering the news. And because of the nature - I mean, and it'll be made to look like it's from IBM or a known company with a good reputation. Easily, that's easy to spoof. And so the journalist says, oh, cool, here's something new from a company I know really well. Click on the link to get the PDF and, bang, you're hacked.

Leo: Boom.

Steve: So it's this notion of sort of demographically targeting your audience that allows things, you know, like malicious email to slide under the users' actual radar. And in fact it was Bruce Schneier who was recently quoted as saying that amateurs attack computers; professionals attack people. That is...

Leo: Oh, that's good. I like that.

Steve: Isn't that good?

Leo: Yeah.

Steve: It's the human factor that is going to be the long-term enduring weakness that we see. We can tighten our computers up as much as we want to. But as long as there are users who will click links, and vulnerabilities floating around that those links can exploit, we're still going to have problems.

Leo: Very interesting. And the chatroom is telling me that - they're saying France does not presume guilt until proven innocent. So I stand corrected.

Steve: Ah, well, that's good to know.

Leo: Yes. I want to make sure that I don't get any...

Steve: And they're not using that guillotine anymore, are they.

Leo: They're not, no, they gave that up a couple of years ago. However, this law, this act of law does presume guilt. And that's the thing that really is offensive about it, you know, with no due process.

Steve: True. Again, you would see somebody so accused needing to stand in front of a judge and explaining...

Leo: Right, I didn't do it, I didn't do it, Your Honor.

Steve: Really, I mean, convince the judge, against whatever evidence has been presented, that it wasn't them. So...

Leo: Right, right.

Steve: 2010. We're in it now. We didn't see many Y2K problems. But there have been some funny and very not funny Y2KX bugs.

Leo: That's bizarre.

Steve: The most significant is that 30 million German credit cards stopped working on January 1st.

Leo: Really.

Steve: They were from the French company Gemalto, which is a well-known security firm. Fact, I think I've got one of their little time-based dongles around here somewhere; one of the one-time password deals came from them. They issued 30 million credit cards to a whole range of banks which included, not just the mag stripe, but also a chip. And when the chip is present, it overrides the stripe for authentication. And the chip has a bug, a Y2KX bug that caused 30 million cards to stop working.

Now, there are various hacks that people have come up with. Some retailers have put scotch tape, or some tape, over the contacts on the card reader so that the card reader can't see the chip, which is faulty, in which case it falls back to the traditional mag stripe authentication that doesn't have the problem. So there are some workarounds for it. The problem is that it's 30 million cards. And I think I read that there was a replacement cost of 6 or 8 euros, which is...

Leo: Per card?

Steve: Per card.

Leo: That's, like, $15.

Steve: Which, yeah, well, times 30 million.

Leo: Jiminy.

Steve: [Laughing] So this is an expensive problem. Now, there's research being done to see whether the chips can be reprogrammed and be left in the cards, in which case special ATMs would be created which would update the firmware in the chip on the card. Now, I'm a little nervous about the idea of...

Leo: Come here, let me reprogram your card.

Steve: Well, about actually, even more so, about having a card which is reprogrammable.

Leo: Right.

Steve: Because then you open yourself to all kinds of hacks. So, you know, if it turns out that these cards can be reprogrammed, well, that's a new problem that we've got because you don't want your chips, which are being used for authentication, to be reprogrammable. Who knows what'll happen?

And then in the other sort of funky story, Windows Mobile users, starting in January, began getting messages from the future.

Leo: [Laughing] Okay. I'm going to get Windows Mobile. Now, that's a good selling point.

Steve: There was a bug in the texting such that, when you received messages, the timestamp says 2016 rather than 2010. So I liked that because, since these messages are obviously coming from the future, and 2016 is four years after the end of the world in 2012, clearly the world is not going to end in 2012.

Leo: Whew. Well, that's a relief.

Steve: So we can all breathe a great sigh of relief. Now, in what has got to be the biggest screw-up of all time...

Leo: Wow.

Steve: I can't say that.

Leo: That's pretty - them's big words.

Steve: This is big. The good news is...

Leo: There have been some bad ones.

Steve: ...all of our listeners who have been following along and have picked up on a lot of the crypto technology that we've talked about are going to love this.

Leo: Okay.

Steve: Unless they have one of these devices. In which case they're going to love the fact that they can fix it, but they need to know about it first. So get a load of this. There are three producers of AES 256-bit encrypted drives.

Leo: Okay.

Steve: Kingston, SanDisk, and Verbatim. The Kingston DataTraveler BlackBox, ooh. The SanDisk Cruzer Enterprise FIPS Edition.

Leo: Okay.

Steve: And the Verbatim Corporate Secure FIPS Edition. Now, FIPS is the National Institute of Standards and Technology, NIST. That's its federal security rating system. These devices have all received the FIPS 140-2 Level 2 certificate which validates devices as being secure for use with sensitive government data. And...

Leo: That's pretty good. I'd take...

Steve: ...they are completely hackable.

Leo: Oops.

Steve: They've got hardware AES-256 encryption in the key. So they're not inexpensive. But get a load of this, Leo. You use some software that comes with a key, which of course prompts you for your password. You put your password in. And it does some mumbo jumbo with your password, whatever it is it does. But every single one of them, no matter what your password was, sends the same key string into the AES-256 cipher engine.

Leo: You'd think something at FIPS, at NIST, might have noticed.

Steve: Uh, yes. In fact, embarrassed by this, NIST has said that they will be considering whether they should make changes to their validation process because the USB drives in question met all their criteria.

Leo: Oh, boy.

Steve: So once again, so it's true that if, as a user, you did not put the right passphrase in, the software would say, oh, sorry, that's the wrong passphrase. But a security company reverse-engineered the software, wondering what was going on inside. And what they discovered was that there was a fixed key.

Leo: Did they have a reason to suspect? Or were they just banging on it, just because...

Steve: Apparently they were - well, I'm glad they did.

Leo: Oh, yeah.

Steve: 'Cause they were just sort of curious. And so, I mean, who knows what their motivation was. You know, they may have been wondering if it was hackable, or just wanted to see...

Leo: Well, as soon as you see something secure, black box security, I think every security company wants to look at it; right? That's what they do.

Steve: Well, yeah. And what boggles my mind is, again, our listeners understand this.

You take and hash the passphrase with a secure hash, and that's what you use as the key. This is not hard. I mean, that's all there is to it. In which case the key would be derived from the passphrase through a secure hash and, bang, you've got it. I mean, sure, you want to put minimum security requirements on the length of the passphrase and all those things, and it wants to be nonguessable because it would be prone to a brute-force attack, blah blah blah, all the things we know about. But the idea that the passphrase isn't being used to generate the key, but that the key is fixed, that's just, I mean, actually it's a really good lesson because it demonstrates that just saying AES-256 means nothing.

Leo: Right.

Steve: The fact that you've got a hardware cipher engine in your, ooh, powerful USB key means nothing if you always give it the same key.

Leo: Right.

Steve: I mean, oh. Anyway, so this company created a little shim that just - you plug the key in, and you don't have - it doesn't matter what you type in, it unlocks your data. It's like, okay.

Leo: That's terrible.

Steve: That's not good news.

Leo: It's a good proof of concept, though.

Steve: Yeah, however. So for what it's worth, if anyone owns a Kingston DataTraveler BlackBox, the SanDisk Cruzer Enterprise FIPS Edition, or the Verbatim Corporate Secure FIPS Edition, all three companies have varying degrees of - have taken varying degrees of responsibility. But they do have updated software. I would imagine that, in fact I'm sure, if they've done it right, you would have to empty your key, that is, get all your data off the key onto your hard drive temporarily, then update the software. And we hope they did it right.

I mean, again, it's just so trivial to do it right. You simply hash the passphrase that the user enters and use that as the key. So you would then update your software, which would change the key, thus scrambling the contents of the drive, which is why you had to remove it. Then I would imagine you would have to reformat the drive and then copy all your data back. If they don't put you through all that, then there's something still not right because, you know, that's what it would take. But the good news is, if you own those, all three companies do have updated software. So you can get your key working the way it should have been.

Leo: Boy, that's a funny bug.

Steve: And we're beginning, I think we're going to have news this year and next year and maybe from now on about concerns for cloud computing. I just sort of wanted to put that on our listeners' radar. I'm already seeing sort of in the ether some troubling reports. There was a report where some hackers were able to use - in this case it was Amazon's Elastic Computing Cloud technology to - okay. And what that is, is it's a bunch of big iron servers where virtualization is heavily used, so that you've got all kinds of virtual operating systems running on the hardware. And clients of the cloud computing elastic server technology are able to dynamically expand the number, like the amount of computing resource they're using, by allocating servers on the fly. So these are not physical servers that are being allocated. These are all virtual servers.

Well, there was report where, as an experiment, some clever hackers, security research types, I mean, good guys, were able to penetrate the virtualization boundary and know what was going on in other servers that they did not own, that were sharing the same hardware. So, you know, that's not good.

Leo: That's not good, to say the least.

Steve: Yeah, you don't want...

Leo: Because, I mean, everything's on EC3. Or EC2, I should say. Everything's there.

Steve: Yes.

Leo: I mean, tons of stuff. Tons of websites you and I use with so-called private information. I back up data to Jungle Disk, with Jungle Disk. We've talked about that.

Steve: Yeah, now, the good news is, the only reason I'm using Jungle Disk...

Leo: Because you can encrypt.

Steve: It encrypts before it leaves your machine. So, yes, somebody there in the cloud who crossed over the virtualization boundary would see debris. But, I mean, that's pseudorandom noise is what comes out of any good cipher. So that's all they're going to get. And that's the only reason I'm using it. I mean, I fundamentally don't trust all of this cloud computing technology. It is brand new. And we know our lessons about brand new security stuff. It's an interesting idea. The whole world's all gung-ho and gaga over it. But it's not clear to me that it's ready for primetime yet. And researchers are saying, uh, we're ready to show you that it's not. So I do think we're going to see that in the future. I just sort of wanted to put a little bullet point on our listeners' radar about that.

I did see another little article that was interesting where a Federal Appeals Court panel is questioning the FCC's authority to impose 'Net Neutrality rules on Comcast.

Leo: Oh, dear.

Steve: And it's like, yes, yes. So a Federal Court of Appeals is saying we're not sure whether the FCC has the authority to tell Comcast they are not supposed to, or that it is illegal, that they are not allowed to filter their customers' traffic and prevent them from using BitTorrent.

Leo: You know, it's funny because I was at an EFF event. And EFF, Electronic Frontier Foundation, which is, you know these guys are legal eagles, and really all they do is go to court to try to protect our freedoms.

Steve: Yes.

Leo: They were saying there's some real question about whether the FCC has the right - we like 'Net Neutrality. We believe in 'Net Neutrality. They were internally debating whether government involvement in the Internet in any form was a good thing. And they did point out there may not be any legal precedent for this. So I'm not surprised that the court is actually getting involved.

Steve: Well, I think it was inevitable because Comcast is going to push back hard. Providers like Comcast, including Comcast, are saying that they are entitled to seek returns on their investments by offering premium services.

Leo: Yeah. And we're entitled, as customers in a free market, to move elsewhere.

Steve: If we had a free market.

Leo: But the problem is, exactly.

Steve: Yes. I mean, it's like the situation with healthcare insurance. You really don't have any competition. I'm a Community Cablevision, a Cox user in Southern California for my cable modem. I don't have a choice. They're the provider that's on the other end of the wire. So...

Leo: Yup. It's a really interesting...

Steve: And then I got a kick out of something that SANS put out over the holidays. This is just sort of something that they do from time to time in one of their newsletters that they call "Ouch." And this was the Top 10 Reasons Computers Don't Have Security.

Leo: You mean this is like what people say when they're asked why you didn't put security on your system.

Steve: Yeah, why don't you have security on your computer? No. 10: I just use my computer for email and web browsing.

Leo: Of course. That's safe.

Steve: Good. No. 9: I've never had any virus problems.

Leo: Right.

Steve: It's like, okay, so?

Leo: Never. Never been a problem.

Steve: 8: Well, I did have some security, but it kept popping up all the time.

Leo: Yeah, I hear that one a lot.

Steve: Hate that. It's so annoying. No. 7: It might crash my system. Okay, well, we're sort of beyond that point, actually. 6: My subscription kept expiring. It's like, oh, well, yeah, that'll happen.

Leo: Yeah, that's the good news about Microsoft and others offering free security software. You can't really use that as an excuse.

Steve: Actually I've got that on one of my - a note in my errata is that I noted that both Paul Thurrott and also Jerry Pournelle in his most recent letter, both of them agree with me about Microsoft Security Essentials.

Leo: Oh, I can't wait to hear your thoughts. All right. We won't telegraph those. We'll get to them.

Steve: So six was my subscription kept expiring. 5: It slows down my system. 4: I thought it came with the computer. Well, not yet. But one of these days, before long, it probably will. No. 3: It's too expensive. No. 2: Macs don't need security. And No. 1 is: I don't know what to buy or how to install it.

So for many of those I do think that Microsoft Security Essentials solves the problem. I mean, it's one of the reasons I'm bullish about it is that I've got friends who are not savvy, who would probably, if they even knew enough to cite some of those Top 10 reasons why they don't have security software on their computer, it's like, I feel reluctant to tell them to sign up for some $39.95 a year deal. I mean, they would. But it's like, eh, you know. And, you know, they'll buy a computer, and it'll be in demo mode for 90 days. Then it'll start popping up, telling them they have to buy something.

I just, you know, at this point Microsoft Security Essentials is not the end-all, be-all. But Microsoft is committed to this. We've seen what happens when Microsoft is committed to something. They come out with version 1.0 is sort of an also-ran, not very impressive. Version 2.0 gets better. By about Version 3.0 they have it nailed. And I just think the idea that it's from Microsoft, it's managing security in the background, it's free, no annual or monthly fees of any sort, it's just it's the easy solution to recommend. I do, I am running it on all of my machines. And I'm having no trouble with it. And I know that now that Paul Thurrott and Jerry Pournelle are both onboard with that, too.

Leo: Yeah. It seems like a pretty good solution. And free is good.

Steve: Free is all right, yes; free is good.

Leo: Free is good.

Steve: I got a nice note from a listener of ours. And I can't pronounce his last name. Michael Nordamrk. He's in Des Moines. And I got a nice - the subject was "SpinRite Saved My A." And it's like, okay. And that was in quotes. And he said, "I'm a networking student at Highline Community College. While we have some fairly new equipment, a lot of our equipment is either surplus or donated. Last quarter our four-person team had built a small network" - this is an advanced course, I guess, because listen to this - "built a small network consisting of seven computers. Our domain controller, a Windows 2K3 Server R2, had dual 40-gig hard drives. We also had an Exchange Server and a web server which are accompanied by four clients..." - so it's sort of a little demo network of Microsoft gear. He said, "...all of which back up to the domain controller's second hard drive. We had been working on this network, configuring it and tuning it, for 10 weeks and were getting ready to present the network to our instructor for our final grade." I know where this story's going.

Leo: Yeah.

Steve: "On the day of the final, our teacher presented us with a situation. Restore your network from your backup."

Leo: Love it. Love it. Love it.

Steve: "Sure, no problem, we thought."

Leo: Easy.

Steve: "While trying to restore Active Directory, we got a series of error messages saying 'File location is corrupt or damaged.'"

Leo: Oh, boy.

Steve: "'Please select new location.'"

Leo: Oh, boy.

Steve: "My team and I immediately started to panic. After several minutes I remembered that I had my copy of SpinRite. I told the instructor that this may take several hours, or even days. I said that if I could get back the info by tomorrow, could we continue the presentation. My instructor was more than understanding. It turned out that SpinRite only needed 45 minutes."

Leo: Woohoo. That's a great story.

Steve: "There was not much on the disk, so SpinRite just plowed through effortlessly. By the end of class we were able to restore the network completely from the failing drive. My instructor was so impressed with SpinRite and our ability to get the data back up and running that we got an A for our final project."

Leo: Oh, SpinRite got 'em an A.

Steve: "The moral to this story is, purchase a copy of SpinRite because you will never know when you'll need it. And if it is not backed up in at least two locations, it's not backed up at all. Thank you, Steve, for your wonderful product and all you do for your listeners. And thank you, Leo, for you and the TWiT network. Happy holidays."

Leo: That's a great story. And he's right. In fact, Peter Krogh, who we've had on the show before, who wrote a book called "The DAM Book: Digital Asset Management," is working with the Library of Congress - I'll have to find the website. Now, he's a photographer, so they focus on photography. And the LOC is of course interested in preserving digital archives. But they have a thing on workflow, and particularly on backup, that's so good. I'll find a link for you. And that's exactly what he - Peter calls it 3-2-1 Backup, where you have to have a local, you know, your original that you're working on, a local backup, but you also have to have a third in the cloud, or offsite, as you do with your mom. Because if you don't have that, you know, 3-2-1 system, no matter what you do, you're running a huge risk. So I like to have two backups.

All right. CES. You didn't go. Now, have you gone, do you go to CES? I'm sure you went to Comdex regularly.

Steve: Oh, yes. I mean, that's my only exposure to Las Vegas because I'm not inherently a gambler.

Leo: Yeah, me, too. I've never gone there for fun.

Steve: No, and in fact, you know, and I heard some commentary, I think it was you on the floor, talking about how Vegas never likes these geek conferences because we're not gamblers. We're up and out and on the show floors, not putting quarters in the slot machines.

Leo: Precisely, yup, yup.

Steve: So, yeah, I've done CES a number of times. And I guess back when I was writing the InfoWorld column I was at CES...

Leo: Oh, sure.

Steve: ...and Comdex, both.

Leo: Okay.

Steve: And CES, I mean, CES is a special show. And...

Leo: Well, it used to be more consumer-y. And now it's folded in all of Comdex, with Comdex gone. It's everything. It's the whole technology industry is there. Everybody's there.

Steve: Right. Well, and I think we've seen a consumerization of computing. I mean, remember once upon a time there was Honeywell, and there was Burroughs and, you know, companies that never transited into the consumer genre. And, I mean, this was a computer show as much as it was...

Leo: Oh, yeah. NVIDIA is there, AMD's there, Asus is there, MSI, all of the motherboard, hardware manufacturers. I mean, it is a computer show, absolutely.

Steve: Now, I thought it was really interesting that the whole industry is holding its breath for the end of January.

Leo: I know, it's kind of funny.

Steve: It's just like, okay, well, yeah, nothing really matters until we see what Apple does.

Leo: You can argue that the two biggest announcements at CES weren't at CES. It was the Google phone...

Steve: Which occurred before CES...

Leo: ...the day before, and the Apple announcement, putative Apple announcement at the end of the month. It's just hysterical.

Steve: Well, and Andy had a great story that he posted somewhere, where he was saying that, he says, well, I've booked my plane reservations to come to San Francisco at the end of January.

Leo: He took a flyer.

Steve: For what I think will be an announcement of the Apple Tablet. But I don't know.

Leo: No one knows.

Steve: All we know is Apple has reserved the space.

Leo: We don't even know that for sure. That's just what somebody says.

Steve: Oh [laughing].

Leo: But the thing that's I think telling, and the reason people like Andy, and I include myself, are pretty sure this is going to happen is because there have been significant leaks to The New York Times and The Wall Street Journal. And in the past Apple has used these two major newspapers as kind of ways to float trial balloons and stuff. The leaks are not sourced. They're not sourced as within Apple. But I - there's no way the Times and the Journal report these stories unless they're really sure. And I think it has to have come from within Apple.

Steve: And one of my favorite quotes was - it was either - I think it was The Wall Street Journal because I get that on the Kindle and read it pretty religiously. Someone was quoted as saying, "I cannot" - and this was a person relatively high up in Apple. "I cannot confirm or deny or say anything about a tablet except that Steve really likes the new tablet."

Leo: Right. Then that's kind of like, okay.

Steve: Okay.

Leo: They're saying we're going to do it.

Steve: And like all of you guys over there who you have on MacBreak Weekly, I want one.

Leo: Oh, yeah.

Steve: I don't know what it is. I want one. And, now, I have to say, though, what everyone was gaga over at CES, I don't get. And maybe it's because I didn't hold it and have it and look at it. But that's the Lenovo...

Leo: It's really cool.

Steve: Where the screen detaches from the keyboard, and then you've got a Linux-based tablet, essentially.

Leo: Yeah. Running Snapdragon, yeah.

Steve: Okay. So it's wonderful?

Leo: No. There's no, you know, there's no use, reason for this. And in fact, no use case. And in fact, Steve Jobs himself said, I don't want to design something that people - it's just so people can take their computer to the bathroom. And that's basically what this is; right? Let's face it. So, no, there's no use case for this. I thought it was - we loved it because it was cool.

Steve: Okay.

Leo: And had some really cool technology. And if you saw it, it was beautifully designed. But I don't see people buying it. In fact, I bought a tablet, Windows Tablet PC some years ago, trying to figure out what the point was because so many people had told me, oh, this is so cool. I don't even think a Windows tablet makes a lot of sense.

Steve: Yeah. In fact, I'm a little bit with Jerry. Jerry and I both own the HP Compaq TC1100.

Leo: That's what I have.

Steve: And I used it...

Leo: It's fine.

Steve: ...for a while when I was taking notes in local association board meetings. It's great for, like, note-taking. But now it's sort of my mail station. I have it...

Leo: Me, too. It's my VPN to the radio station. It's how I take calls. It's not that useful. And Colleen for our, you know, for her portable Skypasaurus at CES bought - we bought the latest, greatest Dell touch tablet. And I played with it last night for a while and had the same reaction. It's like, well, that's nice. But I just want to use it like a laptop.

Steve: What I feel like we have at the moment is, first of all, CES was full of phones and tablets and crossover products that were bridging different levels. And I really think we have a continuum now of portable technology that's almost without any kind of a break in it. It goes from a little clamshell phone that you can make a phone call on, sort of seamlessly all the way up to a big, multiscreen, desktop workstation. We've got everything now. All these little niches and holes are filled in.

And so I think people, depending upon how much money they have to spend overall, what their lifestyle habits are, I mean, what I still want is a PDF reader. And I'm hoping that whatever Apple does will allow me to read PDFs. Because I looked closely at the specs for the new Plastic Logic QUE, which I had been holding my breath for, thinking, oh, this could be the PDF reader. But it falls short from a spec standpoint. You know, my Kindle DX, I can read PDFs on it. But really the only way to get the resolution I need is to do it in landscape orientation, in which case I'm only seeing, like, less than half of the page height, but I'm seeing the whole page width.

Now, the problem there is that all you can do with the eInk technology is page at a time. You really want to be able to scroll. I think if you had that resolution, which is to say about 1200 points of horizontal resolution, then you've got enough to view a PDF. But you need just to be able to sort of position the portion of the page that you can see where you want it to be, instead of being forced to just, like, do ka-clunk, ka-clunk, ka-clunk. And the way it works where you then, on the third one you get, like, the last inch of the page. It just - it's just broken. I mean, it doesn't work right. And it turns out that the QUE doesn't have substantially more resolution than the Kindle. The Kindle DX with its 9.7-inch screen is 1200x824, which is 150 pixels per inch. QUE is exactly the same thing.

Leo: Even in a bigger size.

Steve: 150 pixels per inch. The screen is a little bit bigger. It's 10.5-inch diagonal. So they go from 1200x824 to 1264x944.

Leo: So it does have a little higher resolu- well, same PPI, but higher, yeah.

Steve: Yeah, so you get a little more pixels. But it's eight levels of gray, whereas the DX is 16. And it's got huge margins. The box itself is 8.5x11. So if you see a picture of it, it's got, like, big, like, 2-inch all the way around dead space. So you're holding this big thing that's got a little screen in it. Anyway, I was unimpressed. And I've already got a DX. And it's not enough more resolution, and it's still going to be eInk. So it's just like, okay.

Leo: Everything that was there was just a me-too product, to be honest. It was another Kindle.

Steve: Yeah.

Leo: And I, you know, I like the Kindle relationship, the Kindle content relationship enough that I don't really feel any need to move. The Kindle works for me, as well as any eBook reader is going to.

Steve: I am so happy with my Kindle right now. I mean, absolutely.

Leo: I do think Apple might have something to say there. But we don't know what. I mean...

Steve: Oh, I do. I'm just - I'm holding my breath. So I prepared a page for our listeners that I wanted to go over with you. It is the show notes for this episode. So it's the notes for Episode 231. The URL, I'll just say it, although it's also linked from or will be linked from this podcast item at GRC. So it's GRC.com/sn/notes-231.htm. And these are just some interesting things. The well-known audio company, Klipsch, came out with something that I thought was an interesting gizmo. They call them LightSpeakers. You know how people sometimes have recessed lighting in their ceilings where they've got, you know, you have like the light bulb that screws up into the ceiling, or even in a...

Leo: Or a track light, yeah.

Steve: ...a track light can. They put LED bulbs and speakers...

Leo: Oh, that's a good idea, so you don't lose the light. And you screw it in, and you've got it mounted.

Steve: Yeah. And so it uses carrier current. It uses your house wiring to carry the audio.

Leo: Oh. That may not be a good idea.

Steve: Well, I know. I mean, the thing's a little flaky. But I just, as a weird - I'm not saying that I think these are wonderful. As you'll see, some of the...

Leo: It's a good form factor, though. I like the idea.

Steve: But it's a sort of a cool idea, that you would - you unscrew the light bulbs. You screw these things in. And now you've got speakers where you didn't before. So maybe for, like, for background music, or maybe in a dentist's office, I don't know where. Or maybe at home. But it's just sort of a wacky thing that I saw. The second link is bizarre. It's a waterproof case for the Kindle. And I say under my notes, okay. How addicted to this reader are you?

Leo: I swim with my Kindle all the time. That is pretty funny.

Steve: I mean, it's waterproof, and it floats. So you put your Kindle in it, it looks like a bathyscaphe that, you know, that it was just amazing...

Leo: That's crazy.

Steve: ...you could still see the Kindle in there. I mean, it's huge.

Leo: I guess if you're in a pool - how do you - does it have a membrane over the switches?

Steve: It looks like it must. I mean, that can't be an opening. Otherwise it wouldn't be waterproof. So it must be like a thinner membrane.

Leo: Right. It's hysterical.

Steve: I don't know. But it's just, anyway, loony. And I just got a kick out of that one.

Leo: That is a crackup.

Steve: Then there's a, almost looks sort of holographic. They compare it to the Minority Report UI. But this is a projector, a little thing that you sit on the table, and it projects a full-color video image onto the table in front of it, and it's able to see you touching things and gesturing. So you can, like, type on a virtual keyboard and move things around. They need more software than they have. And it's - I think it has Windows CE built into it, Windows Mobile, and a Flash player. So it's sort of meant to be, you could, like, load it up with content, and it does things all by itself. Anyway, it's just sort of a wacky gadget that caught my attention, that I thought was interesting. And then - I didn't see it. Did you see this helicopter that you fly...

Leo: I did.

Steve: ...with your iPhone?

Leo: I did. And it got, you know, it's one of things that, if you wanted to design something that would get attention at CES, it's this. It's made for television because, when you see it, it seems just to be floating in the air. This, the one I'm looking at is a little different from the one I saw. Let me show you the one that CNET's showing. But they had one that has kind of four - I guess it's the same thing, but it was in four kind of protected - it was in its protected shell, I guess, so it wouldn't chop anybody's ear off.

Steve: Oh, okay. Maybe they did that for the show.

Leo: That must be, yeah, that's the indoor hull. But what's cool about it is it's self-righting.

Steve: Yes, so it has a computer-based leveling and, like, local management.

Leo: So you can pull on it, and try to pull it down, and it goes right back.

Steve: And it's WiFi.

Leo: Yup. Uses the iPhone.

Steve: And so you tilt your iPhone, and you use - so it uses the inertial sensor in the iPhone in order to get, like, flying instructions.

Leo: Right.

Steve: And as you tilt the iPhone, this thing flies around.

Leo: It's pretty cool because when you see it, it looks - it's this weird effect of this thing floating in space. So that's - look, we've seen these things before. It's not that unusual. But it certainly attracted a lot of television attention because it's great video.

Steve: Okay, right. It makes a great demo.

Leo: It's a great demo. There's a little video on the CNET page. I saw it all over the place, you know, at parties. They were showing it everywhere. They got a lot of attention. Now, $500.

Steve: Yeah.

Leo: You've got to really want this thing.

Steve: And there's a camera in it, too; right?

Leo: Yes.

Steve: Okay. So it feeds video back to your iPod?

Leo: It must use the WiFi to feed the video back. Yeah, I guess so. It streams to your iPhone screen. So, yeah, I guess so. And I guess, I mean, in theory you could probably - I was thinking maybe we should get one for the TWiT Cottage.

Steve: So like a little spy drone kind of thing.

Leo: Yeah, let people - yeah. I mean, it's pretty cool that it just hovers there. It's kind of a weird effect to see that thing just hovering there. But ultimately it's an RC helicopter.

Steve: Yeah. I mentioned that Ray Kurzweil was at CES.

Leo: Wish I'd known that. I would have loved to have met Ray. Or seen him again, actually.

Steve: And he has a nice interview that is linked from the CNET page that I've linked to on my page. So you can see him being interviewed. Turns out he's a big believer in the future of eBooks. And he's not doing hardware; he's just written some software, which is apparently multiplatform. And it has an interesting sort of page-turn UI. So, I mean, maybe this is going to be runnable on the tablet, I mean, on Apple's thing. Apparently it's not released yet. He calls it Blio, B-l-i-o. And it's, I mean, it's nothing that I would use because I looks like it's for nursery rhymes and watching farm animals jump around, I mean, I don't know. It's strange-looking.

Leo: I have to point out that our friends, the beloved Adobe, their PDF format is capable of all of this thing. Web content, clickable links, audio, video, multimedia. Nobody does it, but you can build all of that into a PDF.

Steve: No kidding. That much interaction.

Leo: Oh, yeah.

Steve: And what about, like, really nice page turning?

Leo: Oh, well, I've seen it. I don't - there have been applications that do that, as well. I don't know if PDF does that. But PDF is a very rich format. I've been thinking, in fact Amber and I were thinking of doing a podcasting book a couple of years ago that would have audio and video in it and all of that interactivity in it.

Steve: Right.

Leo: So, I mean, of course you could make this software better. But then you have to figure out how to put it on a Kindle with its limited power and screen and so forth.

Steve: Yeah, it was just, I mean, this is not Kindleable.

Leo: No.

Steve: This is something that you could run on a PC. And he says, oh, and of course it comes with a million books. It's like, okay, yeah, fine, they all have that now.

Leo: It's the Google web stuff, that's all, yeah.

Steve: Exactly.

Leo: Meaningless, yeah.

Steve: And then I thought - I just got a kick out of, sort of for old-timers, the Psion is not dead.

Leo: Somebody asked me what my favorite computer ever was, and it was the Psion 3a. I loved my Psion.

Steve: Yup. And I've got one in my own personal history museum, I think the 3 and the 5, also. And this is the same sort of form factor still, a little pocket sort of...

Leo: I like it.

Steve: ...open it up, and this one's running Windows.

Leo: Oh, I don't like that.

Steve: Yeah, I know. It's no longer the Psion OS. But no, for like taking notes and outlining and stuff, there was a time when those little Psions were cute little machines. So I just got a kick out of the fact that it hadn't gone away.

Leo: It's basically a Netbook for 700 bucks, though.

Steve: Yeah, I know. And then you've got to take a look at this picture, Leo, that is this "goo pad," is what I called it. It is the weirdest looking thing.

Leo: This is crazy.

Steve: It's got some guy, it's like - it looks like a hand-size pad of goo that you put your hand in, and somehow it's like...

Leo: That's just nuts.

Steve: ...supposed to be used as a control surface, literally a surface, for computers. It's from Suma, who are, like, real people. And they've got this demo where they sort of show on the screen in 3D, using a false color image, like what areas you're pressing down on.

Leo: Right.

Steve: And they're sort of saying, oh, this is the future of computer control. I'm like, okay, you know, take your shoes off and put each foot in one of these goo pads.

Leo: Well, I like, you know, I like seeing innovation.

Steve: Exactly.

Leo: Who knows.

Steve: I just thought it was a kick. And then I had to link to what your discovery of during the show...

Leo: This was a really, you know, I liked it. People thought I was joking when I said I liked it.

Steve: Yeah. It's a fingerprint-controlled, carbon-fiber wallet. And literally. So it's a wallet-sized box with a standard swipe fingerprint reader. It looks like it's got some little LEDs on the front of it. And it's not inexpensive.

Leo: No.

Steve: It's pricey. But I just thought, okay, in the weirder than...

Leo: I think it's an interesting - I think if somebody gets it, they can get into it; right? I mean, you can't make something that's impervious if somebody's got physical access to it.

Steve: Good point. You'd just bash on it until it breaks.

Leo: Right, right. So, and it has a fingerprint reader. It also has, I thought this was kind of neat, it bonds, pairs with your Bluetooth phone.

Steve: Yes.

Leo: And as you wander off, if you go more than 30 feet away, if it loses the Bluetooth signal, it starts going - an alarm starts going off.

Steve: Yeah. So anyway, it's iWalletUSA.com, just for anyone who wants to see something wacky.

Leo: I just loved - I loved that. And that's one of the most fun parts of CES is just the innovation.

Steve: Yes. Speaking of which...

Leo: It's trying something.

Steve: ...we have the YoYo battery charger.

Leo: You know what? Believe it or not, Dick is doing this on the Daily Giz Wiz in a day or two.

Steve: I just, again, it's like, okay. So this thing is a generator with a cord wrapped around a pulley, hooked to a generator. And so it's very much the same way as you starting your old lawnmower in the old days, where you pulled a little T bar until you get the lawnmower engine to start. This is a generator that works the same way. So you pull this a few times, and it generates enough power for you to send your final tweet before your battery...

Leo: Your final tweet. That sounds bad. The final tweet.

Steve: Anyway, it has a picture of it. And I just thought okay, this is wacky.

Leo: This is really, really fun.

Steve: And then the weirdest thing of all, Leo.

Leo: Okay.

Steve: RCA.

Leo: I'm taking you to CES next time, by the way. You found so many really interesting things that I missed entirely.

Steve: RCA is showing a WiFi-powered gadget recharger that cannot work. I don't understand. I mean, if this was anyone but RCA, I would be so much more skeptical. But on the bottom link of the page for our listeners is a link to the CNET article that has a YouTube video of a very sober - and he looks like you did when you were doing your interviews with the CES.

Leo: He does. Yes, he's got a suit and a blazer on and everything, yeah.

Steve: He does. And he's holding this little thing up. Now, get this. Their claim is that this thing just sits around. It's just, you know, on the table. It's in your knapsack. It's in your pocket, whatever. And it's sucking in WiFi...

Leo: C'mon.

Steve: ...which it turns into DC current.

Leo: Yeah, at the rate of a volt a year. I mean, what, a watt a year. I mean, how much current could there be?

Steve: That's the problem. I mean, it's loony. But it's RCA. And they did a demo apparently during the show. And so this thing sits there, I mean, maybe if you sat it on the hotspot, and there's a reason it's called a hotspot. Or, like...

Leo: You'd get more power out of collecting the energy from my body heat than you're going to get from WiFi.

Steve: Oh, god, I guess I just - I look at this thing, and it's like - and the guy's very serious. Oh, no. We call it Airnergy.

Leo: Yeah, Air-nerd-gy.

Steve: Airnergy WiFi Harvesting Charger that harvests power from the WiFi signals all around you. And it stores it up. And if you need a little - if your cell phone needs a little boost, and you don't have your YoYo charger with you, then you just plug this in.

Leo: Or buy a battery. That is so goofy. How much power do they claim you can get out of that? Not, I mean, it's got to take all day.

Steve: They're serious about this. And then in the demo they say, and then our advanced laboratory future evolution of this will be to actually replace the battery, where you take out your normal old-school battery, and you put this thing in. And so...

Leo: This is a joke. This is from The Onion. Come on.

Steve: No, no, no. I mean, it was there. Look at the booth behind them. When you play the video you'll see.

Leo: That looks real.

Steve: This was RCA. It was just - and it got four stars in YouTube ratings. Like, oh, come on, do the math. There's just not enough power.

Leo: Well, if there were, then WiFi would be a real danger.

Steve: Yeah.

Leo: Let's face it. You don't want that much energy floating through the air.

Steve: Yeah. It's crazy.

Leo: It's bad news.

Steve: And then my final announcement is I just finished a major chunk of work which, as you mentioned, Leo, you can see it blinking...

Leo: That is so cool.

Steve: ...blinking behind me. When I got through with the DNS benchmark code, the PDP-8 project that I had been working on around this time last year, actually, was - the parts were beginning to get scattered. And I thought, oh, I just have to finish this before they all get completely lost. You know, my cleaning lady comes in and vacuums things, and I hear little things rattling up the hose, and I think, oh, no, what was that? So I just - I spent 90 days. I finished building the kits. I also put together a bunch of pages. They're linked from GRC's home page under the "Other" menu item off of our main menu. Nice picture of the original PDP-8 front panel. I talk about the instruction set. And sort of it's a little bit of a walk-through nostalgia.

Leo: This is so neat.

Steve: And I also did three videos because most people aren't going to have these. But I wanted to be able to show, for example, the program called Deep Thought. It's what you see running behind me. It's a sophisticated blinking light program that I put more time into than you would imagine because you can characterize the way the lights blink. They're not just random. It looks like they're actually doing something. And so you...

Leo: Well, are they?

Steve: Well, yeah. But they're not accomplishing any work.

Leo: Not much. They're thinking. It's thinking.

Steve: So anyway, I put videos on the site.

Leo: This looks like WOPR out of "War Games."

Steve: Yeah, exactly.

Leo: [Mimicking WOPR] Shall we play a game?

Steve: And there is a - if there is sufficient interest, this kit can come back.

Leo: Oh, good. Because I really love that front panel. I know he had a limited edition of that.

Steve: That was the problem. Well, the problem is that they're just being made custom order. The front panels are gorgeous. You can see in my videos, I do a little show-and-tell video, and I also show Deep Thought and Lights Out. Lights Out is a puzzle that I wrote. You know, I wrote all this in the last few months in PDP-8 code.

Leo: You must be having so much fun.

Steve: It was really fun. I have to say I just - I had a great time. So I wanted to formally announce, though, that if we can get a total in the world of 50 people who want to go for more of these, Bob has said - Bob Armstrong, who made the kit - he will do another run of however many. It just doesn't make sense to do many fewer than that.

Leo: Right.

Steve: But so on my page is a form where people can say, hey, you know, it explains the kit, what you get, what you don't, what it costs and so forth. And if people want to, you know, if they look at my videos and think they want one of these things, too, then we can make it happen.

Leo: This is really, really cool. So if you go to GRC.com, under the, what is it, recent?

Steve: It's actually - there's "Other."

Leo: "Other." It's under "Other." There's a PDP-8 entry. And there's Steve in front of his - these videos are great. They look like they're high-def. They're really nice.

Steve: They came out nicely. I spent some...

Leo: Yeah.

Steve: Actually it's a prototype for a SpinRite video that I'm going to do to...

Leo: Good.

Steve: Because I've never done any documentation. And people - the problem with SpinRite is you can't get a sense for it until you own it. And so I thought, I ought to do a video to, like, do a walk-through to show everybody what SpinRite's all about. So I wanted to sort of beta test the concept here. And...

Leo: This is great. I like it. Yeah, it looks really nice. Well done. Bravo. And we get a good, close-up, detailed look of those PDP-8s, which we can see, if you're watching the video of the show, you can see over Steve's left shoulder. But they do look cool. That is really neat.

Steve: They're wonderful.

Leo: Yeah.

Steve: I do think one would look nice behind you, kind of just...

Leo: I do, too. Put me - make me one of those 50, anyway. Maybe I should have two or three.

Steve: Well, Colleen would get a big kick out of building it. The kits are professionally built. I mean, they're just...

Leo: Need some soldering; right?

Steve: You've got to be able to do some soldering. Bob orders the face plates that are all custom. They're, like, five-color silkscreen multilayer laminate. The silk screening is behind a front laminate. There are laser-cut openings for the switches. I mean, it's just - it's a 100 percent professional result. I was really impressed with it.

Leo: Nicely done. Nicely done.

Steve: So our listeners can check out the videos on GRC. And I'm back to the DNS benchmark documentation now. The PDP-8 is completely closed and finished. So I will get that done, and we will do a podcast here before long about benchmarking DNS.

Leo: Very good. That should be fun. Well, this has been a marathon edition. I tell you, you give Steve a week off, and he gets more than twice as much material together for the next week. Thank you, Steve. A lot of fun. Great stuff. Show notes, as always, on Steve's site. But also we've got it on FriendFeed.com. I take show notes as we're going. And this is a long one. If you go to the TWiT conversations room, that's FriendFeed.com/twit-conversations. Eventually I'm sure it will get migrated by our note-takers to our wiki.twit.tv.

But you know you can always go to GRC.com because all this great stuff is kind of hidden there. You know, you just browse around. You'll find all sorts of cool stuff. GRC.com. That's where you can also find of course the great SpinRite, everybody's favorite hard drive recovery and maintenance utility. And 16KB versions of the show, transcripts, and more. GRC.com. Steve...

Steve: And our bandwidth is being pinned right now.

Leo: Is it really? You can see people go there.

Steve: Yup. We're definitely delivering some videos right now. That's great.

Leo: It's awesome. Thank you, Steve, so much. We look forward to next week. It's Q&A time. So while you're there, you might want to go to GRC.com/feedback. And if you've got a question or a comment about anything you hear on the show, that's a good time to do that. And Steve will respond to as many of them as he can next week. Thanks, Steve.

Steve: Talk to you then, Leo. Thanks.

Leo: See you next time...

Steve: Bye bye.

Leo: ...on Security Now!.