SECURITY NOW!

Transcript of Episode #216

Listener Feedback #76

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

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-216.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-216-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Music and Spinner.com, where you can get free MP3s, exclusive interviews, and more.

This is Security Now! with Steve Gibson, Episode 216 for October 1, 2009: Listener Feedback #76.

It's time for Security Now!, the show that covers all things secure and security-wise, protecting yourself online with Mr. Steve Gibson, the king of security, the guy who discovered spyware, coined the term, wrote the first antispyware program, has ever since been writing great free utilities for all of us to protect us, and for the last four years has been educating us. Episode 216. Hello, Steve.

Steve Gibson: Hey, Leo. Great to be with you again, as always.

Leo: In our fifth year of broadcast excellence.

Steve: And apparently no sign of slowing down because the industry keeps throwing new, bizarre things at us that are fun to share. So, yes.

Leo: Oh, I tell you.

Steve: It's not getting any better.

Leo: We've got a good Q&A. Our listeners are really good at coming up with questions for Steve, and he'll be answering those. Our 76th feedback episode. I'm sure we have secure - and in fact I know we have security news.

Steve: Yup.

Leo: In just a little bit. And probably some errata, as well. Real quickly, before we get to the errata, let me mention our friends at GoToMyPC, who - it's really our friends at Citrix. You and I, Steve, were talking, it was kind of fun, about the good old days of trade shows and the late-lamented COMDEX.

Steve: Yeah. I remember when the text used to scroll up the screen, Leo.

Leo: Yeah, those were the days.

Steve: Those green screens.

Leo: Those were the great old days. So I was just - I was thinking, because you said COMDEX really was, you know, it was the big computer show, which went out of business about four or five years ago. We're going to go to CES, that's why I asked you, and we're going to be broadcasting from there. But it's not the same.

Steve: Oh, cool, cool.

Leo: Yeah, it's not, it's not the same. COMDEX was computers. CES is everything. But I remember, as you said, you would hang out with Gates and...

Steve: And Ballmer and Philippe Kahn and, I mean, lots of people who, you know, the contemporary PC industry has forgotten.

Leo: Absolutely. Absolutely. And it reminded me of a guy that I met, that Gina Smith introduced me to, probably it was in 1996 or '97, Ed Yakabuchi. You remember Ed at all?

Steve: Oh, of course.

Leo: Great guy.

Steve: Yeah.

Leo: I mean, one of the - he reminds me of Philippe Kahn, one of the - just a big, vibrant, exciting guy. He was the founder of Citrix. He actually worked for IBM. And I believe it was he, you know, the joke at the time was that IBM wrote Windows NT for Microsoft while Microsoft was writing OS/2 for IBM. They were kind of - they traded engineers. So he was working on the NT team and while doing that really created, you know, learned about the kernel and became an expert in remote access. He wrote the original remote access stuff for RDP. Actually I think Microsoft licensed RDP from his company, Citrix.

Steve: That's correct, Microsoft did get the original remote desktop code from Citrix.

Leo: From Citrix, yeah. Citrix was the company, the remote access company. They've grown. They've expanded. They've produced not only high-end enterprise solutions, but also consumer solutions.

Steve: Well, I'm wondering why you're going to Dubai. You didn't...

Leo: I didn't tell you that, did I.

Steve: No.

Leo: I am speaking at TEDx Dubai, which is a great honor. You know, TED is the big conference in Long Beach, down your way.

Steve: Right.

Leo: This is a - they do a franchise, so they're all over the world. They just had one in Toronto. And when Giorgio wrote to me - I don't say his last name because I don't want to mispronounce it. He's Italian, but he lives in Dubai, as a lot of people in Dubai are expats. Giorgio Ungania - I hope I'm saying that right, Giorgio - organized TEDx Dubai. And I'm going to be speaking there on the 10th.

Steve: Cool.

Leo: So Jennifer and I fly out Tuesday. It takes - it's a long flight. I think it's 15 or 16 hours. We'll arrive - we'll leave Tuesday afternoon, arrive Wednesday night in Dubai. And but I can't wait. I've never been there. I'm dying to see it. And then Saturday I speak, and then Monday I fly back, and I'll be here next - the following week. But so next week it'll be Alex Lindsay doing the show.

Steve: Right. I've heard lots of things about Dubai. Like it's got 90 percent of the world's super tall skyscraper cranes because they had to, like, ship all the cranes to Dubai to make the buildings, the place is growing so fast.

Leo: It was just the desert, you know, it was a very - and they've just, you know, poured tons of money into it to make it kind of this global business marketplace. They have the world's tallest building, the Burj, just opened, like just opened. So I'll be able to see that. I'll go up there.

Steve: Yes. I think it is, it's just massive money. It's just money, money, money, money.

Leo: Yeah, it's a lot of money. So I can't - it's going to be great. And really full of expats, people from all over the world there. It's become kind of this, you know, it's like the marketplace, the global marketplace. People just kind of go there. So, you know, it's continuing in my world journeys to see the interesting new places to be. So I couldn't say no. I can't wait.

Steve: Yeah, cool.

Leo: It's going to be fun. So let's - should we do the security news before we get - go too far [indiscernible]?

Steve: Oh, of course, of course. Many listeners wrote in to bring my attention to Carbonite's license agreement. And I wasn't sure whether we had gotten carried away in talking about the level of security and encryption that they apply. But, you know, they're a sponsor. They have been a sponsor of the show.

Leo: Yeah. They told me, and I'm going by what they told me, that they told me that they use AES-256 on the local machine and then SSL to upload. Is that not the case?

Steve: Well, what's the case is that they can decrypt it.

Leo: Really.

Steve: And that's what's important is that their license says that if they believe there's child pornography, or if they're under a government subpoena for whatever - or if they need to for technical support reasons to make sure their stuff is working, they have the ability to decrypt the data. Now, I assumed that because one of the features is you're able to log on from elsewhere on the Internet and get access to your backed-up files.

Leo: Right.

Steve: Well, that means that they have to be able to decrypt it and send it.

Leo: They must have the key, yeah, yeah, yeah, yeah.

Steve: Yeah. So anyway, I wanted to make sure that we were clear about that caveat. I mean, the benefit is for a certain class of user. It's transparent and in the background and easy. And it protects you from your hard drive cracking, or crashing, rather. But it is the fact, it is the case that they would have the ability, they have the key, the encryption key used for your data being stored. And a bunch of our listeners who are on the ball, and of course that's why they're listeners...

Leo: Right on, yeah.

Steve: ...checked that and said, whoa, wait a minute, just make sure that that is...

Leo: So I correct - I'll correct myself because I went too far. They didn't tell me that. I was just reading into it. But of course you're right. They would have had - they would have to have the key to be able to send you a clear copy.

Steve: Exactly. If you log in somewhere else, then they would have to be able to do it. And it's interesting, their agreement says that, if you do that, then your data will be sent in the clear. And it's like, whoa, wait a minute. I would think that would be SSL-encrypted so that it wouldn't transit in the clear. But their paragraph 15 at the bottom does state that, if you access your data from another location other than your main machine, then it won't enjoy the encryption that they normally apply. And so you acknowledge that, you know, you're allowing that to happen. So...

Leo: Yeah, I mean, I would check and see if it's HTTPS. It may still be HTTPS. You know how lawyers are. They want to hedge everything, just in case.

Steve: Yup, yup, cover themselves.

Leo: So, you know, and I think probably - I would bet they for legal reasons don't want - they do want to be able to respond to subpoenas. But this is, if you're worried about that, that's why you use TrueCrypt or something else where you and only you have the key.

Steve: Well, for what it's worth, yes. I mean, that's why I...

Leo: You could also TrueCrypt before you upload it, if you want.

Steve: No. Because their system runs autonomously. They explain that they look at the files, they examine the headers, I mean, they're looking into your data on your machine to, like, make sure the file size is right, look for changes. They may be doing checksums or something.

Leo: Oh, they'd have to do that, you're right, otherwise they wouldn't know if it was new or not.

Steve: Right. So they're doing autonomous, you know, in the background work. I'm a Jungle Disk user because - and we had the author on the show. I know exactly how it works, where only I have the key. So Amazon with their S3 data storage service, they're storing completely pseudorandom data that they have absolutely - that is completely opaque to them. So I'm comfortable with that. But it's a more techie and not an automatic solution. So again, I think there's certainly...

Leo: It's also more expensive. You pay the price. If you have the same amount of data, you're going to pay more.

Steve: Yeah. I think, you know, there's certainly a class of user for whom Carbonite makes absolute sense. So I think - but I just - I did want to respond to our listeners and make it very clear that it would take a court order, but that that can be done at their end.

Leo: Well, I found - I learned this week that the same thing is true of Twitter. We had a little incident with somebody posting death threats on Twitter and tried to get the information. I was just hoping I could just send a note to Twitter saying, you know, just tell me if the kid's - this person's in California, so I know if I should worry. And they said no, you can't, we need a - you need a court order. So we contacted the local police. He's getting a court order. But, and that's how it's - I guess that's how it's supposed to be. I think that that's kind of the normal circumstance for most of this stuff.

Steve: Well, and for example, once upon a time, years ago, there was someone who I knew was nearby sending denial of service noise at GRC.

Leo: Right, right, I remember that, yeah.

Steve: And so I could tell from their IP that they were a local Cox Cable customer. And I had some contacts here with the local FBI. And I said hey, you know, I've found these four machines. I'm sure it's not anybody who owns the machine. They just have some junk on their machine. And so they had to produce a subpoena to allow Cox to tell them the owners of those IPs. And then they called and said, hey, we've got a person we work with who would like to come take a look at your machine. You probably don't know it, but it's infected with some stuff, and wouldn't you like that fixed? And so they said, oh my goodness, we had no idea.

You know, it's funny, too, because the kids were complaining they could no longer burn CDs because the machine was so - it was so overrun with junk. I mean, it took, like, an hour to boot because it was the war of the malware, it's like who was going to play king of the hill inside the machine just every time it booted. It was a disaster. And they were using Kazaa back in the day. They were like, well, we like free music. It's like, oh, yeah, I bet you do.

Leo: Well, very - yeah. And in fact I got the - we also talked - I talked to the FBI in San Francisco, too, so.

Steve: Yeah.

Leo: I guess if it's on the Internet they count it as interstate or a federal thing despite [indiscernible].

Steve: Yeah. Well, and in general, I mean, the thing to look at is that these companies that have records, they want to be protected against their customers suing them for disclosing the information. So, for example, in my case, even though Cox would have happily, I mean, it wasn't like they were trying to hide the information, but they have an agreement with their customers to maintain their customers' privacy. So the company has to ask for the - has to literally say, please make us give you this data. They have to ask to be compelled to do it so that they're able then to say to the customer...

Leo: Privacy. You have privacy.

Steve: We were subpoenaed. We had no choice. And again, for example, that's why this paragraph 15 of the Carbonite agreement says if we are subpoenaed, we will turn over your data. Just, you know, FYI.

So the top of the news is for me very exciting. Yesterday, which is - or day before yesterday, given that the podcast is released on Thursdays, that is to say, Tuesday the 29th of [September], Microsoft Security Essentials was released. That's - and you can just put Microsoft Security Essentials into Google, or it's Microsoft.com/security_essentials. And this is the awaited first Microsoft free antivirus and antimalware scanning and monitoring overall prevention utility from Microsoft that I'm very excited about. I like the idea that it is small and lightweight. I like that it's from Microsoft, so I have the sense that it'll integrate properly with Windows and won't be in the way. It's not going to be jumping up and down, trying to get my attention and reminding me that it's time to re-up my license or anything. All of the reviews that have been done so far have been positive.

Having watched it, the one thing I can say is in full system scan mode, it makes SpinRite look fast. It is very slow. Now, its speed is a function of the type of file it's looking at. I've noticed that it just whizzes through a block of JPEG image files. Boy, when it hits an EXE or a DLL or something executable, it spends some time. Now, I think that was the right choice because, first of all, you're not having to do a full system scan all the time. You want to do, I would say, that once when you first install it because then it's able to look at changes and new things coming into your system and check them incrementally, in which case it's not a problem.

The benefit of it being so slow is that it is being thorough, and it is not generating false positives. You can imagine with Microsoft being as security, well, as customer support shy as they are, you know, we've talked many times how unfortunately Microsoft leaves things turned on by default because they don't want people calling them, asking them how to turn them on. So they're just on. Well, the last thing Microsoft wants is a technology which is going to be generating false positive alerts. And many of the looser, faster heuristic technologies do have the problem of generating false positives. Every few months our support email starts getting reports that some random piece of my freeware, which hasn't changed in a decade, suddenly has spyware in it. It's like, no, it doesn't.

Leo: Do you think there's something about your software that lends itself to that? Or why is it?

Steve: No, I hear about it from everybody. Mark Thompson has the same thing happen.

Leo: Everybody, okay.

Steve: The problem is, these scanners are trying to be very fast, and they're trying to be sensitive enough, but not too sensitive. Microsoft has clearly taken a different approach, where they're really affirmatively identifying, rather than just sort of scanning across the top and saying, oh, look, this might be a problem.

Leo: It's a much slower scanner than most. I mean...

Steve: Oh, it's painfully slow.

Leo: Even the, quote, "quick scan" is slow.

Steve: Like I said, it makes SpinRite look fast. SpinRite is known for taking its time and being thorough. And this thing is really slow. But again, you would do the full, deep scan, I would say, once upon installing it. Then you can set it up with a schedule, and it is watching your system on the fly. I'm just excited about this because I've got friends who for the last couple months I've said, like someone will buy a computer and say, hey, I got some notice that Trend Micro wants to bill me $39.95. I'd say, okay, just hold on. In a couple months there's going to be something from Microsoft which is free, free, free, free.

Now, we'll remember that this is only for the client machines, not server platforms. They have their full-strength commercial product from which this is descended for their server platforms. But for all of us running XP and Vista and Windows 7, here's I think going to be a great solution. Now, I've only looked at it at this level at this point. I've got the next four weeks of Security Now! shows mapped out. So, and in fact we're going to have John Graham-Cumming come on in three weeks...

Leo: Oh, good. Oh, great.

Steve: ...and talk about in great detail JavaScript, which he knows inside and out, and he gave a presentation about it in a recent virus conference. So I said oh, John, Leo and I need to have you on. So he's agreed to do that.

Leo: Fantastic.

Steve: And so it'll be the week after the Q&A following that one. I will have had time to really spend a lot more time and will do certainly a podcast about this.

Leo: Do you think this is going to put the commercial antiviruses out of business? I can't imagine, why would anybody - of course there have been free antiviruses for a long time, and that hasn't put the commercial guys out of business. But this one's from Microsoft.

Steve: Yeah. And I - for example, there really isn't a commercial competitor for Internet Explorer. There are free competitors for Internet Explorer, but not a commercial browser. I think it would be - it'd be hard to sell one, you know, for money. I think this changes the game. I think that Microsoft gave everybody a long run, that is, in the AV world. But if this is as good as it seems to be, and it doesn't cause problems, and it updates multiple times a day, it uses the current connected always model, I just - I know that it's what I'm going to recommend to all of my own friends who are - who I just sort of try not to get involved with their computers because I don't want to be their go-to guy. But they know they should be doing something. And I think this just solves the problem.

So I would say, if a person has an existing relationship with an AV company, they're comfortable with it, they like it, they've gotten to know it, they know its quirks and so forth, they may be inclined, for the sake of inertia, just to stay there. But I would be surprised, if a new machine started to try to charge you money for the AV that was preinstalled for 90 days, and then it wants money from you, I'd be surprised if people didn't say, wait a minute, is that what I should do? Or should I just say remove this and install Microsoft's free one? Before long the world will be out that Microsoft provides this. Microsoft has solved this problem. And I think that changes the game.

Leo: Right, well, good. I mean, who better to than Microsoft?

Steve: And I like it because it's lightweight. I mean, here I am with my cookie manager that the only thing it does, my little Permit Cookies extension for Firefox, is it just brings up a little lame little dialogue that says allow or disallow. I mean, that's all I want. So I always prefer a tight minimal solution. And from what I've seen, that's what Microsoft has given us. Because they're not having to compete with the major AV players. I look at, for example, how ZoneAlarm - or Zone Labs destroyed Zone Alarm by having to compete with Symantec and their Norton Suite and had to put everything but the kitchen sink, in fact I think maybe that's an option in the firewall. It's just they ruined a good personal firewall, and it just became a horrible thing. So I really like the idea.

Leo: Well, there's two parts, I guess, to an antivirus. One is the scanner, usually doing that by signatures; right? And the other is heuristics, where it's looking for bad behavior. Does this do both of those?

Steve: Don't know yet.

Leo: See, that's the problem. We don't know how good the scanner is. We don't know how sophisticated the heuristics are. I'd like to see some tests on that, although it's very hard to test, of course.

Steve: Well, a lot of tests have been done.

Leo: Oh, they have, okay.

Steve: And Microsoft has come out on top.

Leo: Oh, good. All right.

Steve: I mean, it's like as good as anything else, from everything I've seen.

Leo: That's all that matters.

Steve: I know. I think it's a win. So...

Leo: Where did they get this? Is this a rewrite of OneCare, of the giant antivirus that they bought? Or is this something...

Steve: Yes.

Leo: It is.

Steve: It's their - it's a - I don't know how to characterize it. Not really a rewrite. It is the engine behind their commercial product, their mainstream commercial product. And so they spun out this free one after proving the technology. It's like, okay, we got it nailed. Now we're confident that we can - because they recognize that it is going to be a hit. They opened the beta, and they were providing 75,000 downloads, and they closed it partway through the first day because just everyone went nuts for it. And I've been waiting for it.

I'm excited. I think this is - this changes the game in the same way that, for example, that Microsoft having a really good firewall in their products do. Now, their firewall does not do outbound monitoring; so some would argue, well, it's not really good because it doesn't do that. But it's like, well, if you're careful about not letting anything in, then you probably have the security you need. And this will help prevent things from getting in.

Leo: It makes sense they'd release this right, as it is, a couple of weeks before the release of Windows 7. They've got now an anti - pretty much a complete security suite. Windows 7 implements User Access Control and other security features. It sounds like that 7 might be really the holy grail, which is a version of Windows that just is not prone to this stuff. I hope. We hope.

Steve: Well, to hear Paul talking about - it wasn't Paul, it was a Mac person who was saying of Windows 7 that this was good enough that he was kind of finding himself thinking, wow, I could actually use this.

Leo: Oh, yeah. I love it. I mean, I'll probably still use a Mac as my personal computer, but I love Windows 7. I think it's the best version of Windows they've ever done. And a thing to remember is that the key really to protecting against infections is widespread antivirus use. It's like vaccination. The more people that are running antivirus is that damps down the spread of the antivirus; right?

Steve: Very good point because it is machines that are infected that are actively working to infect others.

Leo: Right. So by giving away - I wish they'd install the darn thing. I guess they feel like they can't do that to their partners. But it should come with this.

Steve: Just give it time. This always starts this way. And then it'll just be built in. It'll just be like, look, we've got - you can't not have automatic updates now. You have to fight Microsoft to get control of that.

Leo: And look what a boon Service Pack 2 was for XP because it turned on the firewall.

Steve: Right.

Leo: That in itself was a huge improvement.

Steve: It was everything, just to block that, yes.

Leo: I think this will be comparable to that. I hope.

Steve: I think so, too. This is really big.

Leo: Right.

Steve: The only other security news I had - it was a quiet week - was just a little tiny mention. This is not a big deal at all. But I know that the VLC Media Player is popular for a lot of users who like to have a third-party, more format-expansive media player. And there are a bunch of multiple buffer overrun vulnerabilities that exist in everything up to and including version 1.0.1. So anyone using VLC, again, I don't even think that the attack surface is very big on this. Who's going to create a piece of media specifically hoping that you're running it under VLC Media Player? But I just did want to mention that there is an update to that. Otherwise it's been very, very quiet on the security front. I'm sure in a couple weeks we will, when we get to the second Tuesday of October, things will pick up, and we'll have some more news. But that's it for now.

Leo: That's good news. I like that.

Steve: And then I had one really fun little short SpinRite story that caught my eye. Actually I encountered it just this morning when I was running through the mailbag, looking for our Q&A questions. The subject was "SpinRite saved our lawsuit." And I thought, okay, well, there's one I haven't heard before. And so, and he asked me to leave his name out if I read this on the air. So he said - but he's located in Minneapolis, Minnesota. He said, "Hi, Steve. Thought I'd say how awesome SpinRite is. I needed to copy some .pst files" - which is really interesting, too, because my homeowner association was sued by a bunch of homeowners who were disgruntled, and all the members of the board were using Outlook. And they all came to me because unfortunately I had been identified, I'd been uncloaked as someone who understood computers. And they were all needing - the attorneys all needed everyone's email dialogues that were related to the last X number of years of their service on the board. And so it's like, okay, so I had to figure out how to do that.

And so he said, "I needed to copy some .pst files from the CEO's laptop for some discovery our lawyers wanted. When I tried to back up his main file, I kept getting a CRC - Cyclic Redundancy Check - error. After working the lump out of my throat, I tried creating another .pst file to copy the email into. But that failed with the same error. So I pulled out the SpinRite disk. I know management gave me a hard time when I needed to buy four licenses..." - because the way that works is a single license allows the licensee, the user, to use it on any machines that they own, any machines and hard drives. But we ask people to have four licenses for, like, we call it the "corporate site license," to then use it, for example, on all the machines within a corporation. And so he says, "...but I told them it was worth it and that it is a good product. Thank goodness I was right. After running it on Level 2 for an hour, the original file copied without any problem. Thank you so much. P.S.: Please don't use my name on the air if you read this."

Leo: That's great.

Steve: So thanks for the positive feedback.

Leo: Good news.

Steve: As always.

Leo: SpinRite saves the day.

Steve: And in an hour this time, instead of a year.

Leo: Yeah, we should mention that. The time varies depending on how bad the drive is, right, what kind of shape the drive's in.

Steve: Yes. It can - and in fact it's funny, too, because SpinRite estimates, continually estimates how much longer it has to run based on how far it's gotten, given how much time it's had so far. So it assumes that the whole drive is going to be exactly like what it has seen so far, which is often not the case. It's very often the case that the drive may have some problems at the beginning, which is why it's Blue Screen of Deathing and having - can't get booted or whatever. But then after working through those, it just takes off like a bat out of hell. So people say, wait a minute, it says it's going to finish in the year 2020. It's like, no, calm down, it's probably just hit a rough spot right off the bat which has caused it to project its completion time as not in your lifetime. But it'll - as soon as it gets past that, it fixes its estimate and then starts getting much more accurate. So that's good.

Leo: Well, we're going to get to 10 of your questions - we've got some great ones - in just a second. But I do want to mention Audible.com. Have you watched the new "FlashForward" yet? Are you interested in this show?

Steve: I don't think so. I saw the previews, and it's like, eh. And I tried to watch "Defying Gravity" for a while, which was the summer sci-fi show. And it was like, eh, this is just too much soap opera in space for me, so...

Leo: I'm not a big, as you know, and we've talked about this before, I'm not a big fan of sci-fi on TV. I just feel like they never give it the budget or the time that it needs.

Steve: Oh, except for...

Leo: "Stargate," I know, you like...

Steve: "Fringe," "Fringe," "Fringe."

Leo: And "Fringe," no, I will watch that when that comes out on DVD.

Steve: Oh, it's so fun. And we have a new "Stargate" this Friday, in fact. I'm glad you mentioned...

Leo: I saw that, yeah.

Steve: Yeah, "Stargate Universe." I know nothing about it, but it is premiering this

Friday, the day after the podcast. So we should let all of our listeners know - I'm sure they do now - that "Stargate Universe," which is, you know, the Stargate franchise I've really, really enjoyed. It's a little cartoon-y sometimes, but fun. But, oh, "Fringe" is just always delightful.

Leo: "Fringe" is kind of like "X-Files"; right?

Steve: Yeah, it's very much so. In fact, it's funny, in an episode last week, the premiere episode of this new season, they were - there was a Senate Finance Committee meeting where they were going to cut off the funding for the Fringe Division. And the guy said, he said, "You know, we've spent so much money in these X-Files and this Fringe Division." I thought that was really great.

Leo: That's a nice touch.

Steve: Yeah.

Leo: I like that. That's a really nice touch. Well, the reason I brought it up, for those who do want to watch "FlashForward," I guess the plot of this is that humanity goes to sleep and just has, like, a vision of 20 years ahead of time and then comes back. And now everybody knows what's going to happen for the next 20 years.

Steve: Everybody in the world has a two-and-a-half-minute blank-out where they see into the future, except some people apparently see nothing. And that's - they're worried. Does that mean I'm not going to be around in there or what?

Leo: Right, right. Well, it's based on a novel. And, see, to me, if you get inspired by the show, and you want to, you know, you say, oh, I like this, I say read the novel because...

Steve: Oh, because it's always going to be better.

Leo: I think it's always going to be better.

Steve: Yeah.

Leo: I mean, I can't think of anything where the original book that it was based on isn't better.

I have for you, in my hands, a passel of questions. Are you ready, Mr. G?

Steve: I am.

Leo: All right. Starting with Brian Dort from Alpena, Michigan. Brian says he's got some news about PayPal's multifactor authentication, which we have spent many, many moons talking about: Steve and Leo, I'm another long-time listener since Episode 1 of Security Now!, also a happy SpinRite owner. It has saved many hard drives for me. I now have a USB thumb drive with SpinRite loaded on it - oh, that's a good idea, I didn't know you could do that.

Steve: Yeah. SpinRite will set up a USB thumb drive as a bootable drive. And then you can put any other files on it that you want to. But when you boot that thumb drive, SpinRite just takes over and runs.

Leo: Brilliant.

Steve: Yeah.

Leo: Couple years back, after Episode 103 on the PayPal security key - that football that we talked about - I ordered one for myself and immediately started using it. By the way, as a side note, I gave the football to our business manager, so she has it now.

Steve: Good.

Leo: She's got the football, like the atomic football. Since then it's worked perfectly until one recent day I pressed the button to receive my token, and nothing happened. My assumption is the battery died. No worries, though. I can log onto PayPal, answer a few questions, and order another. This time, emulating the master - he means you, Steve.

Steve: I think he does.

Leo: I ordered three, with the intention of placing two in the freezer for future needs. Well, they're only five bucks each. Why not? To my surprise, when they arrived, the dongle was not to be found. Instead a thin, credit card-size security key was found. It has a circle that says "Press" on the front, along with an eInk type of display that shows the number. I'm going to pull mine out because I have the same exact thing.

Steve: As do I, in my wallet.

Leo: Yeah. I know what he's talking about. At first I thought this was a great thing. It fits in my wallet easily, and I usually have my wallet with me, more than I have my keys with me. However, after using this new format for a short period of time, I'm convinced that PayPal has made another mistake. My first one stopped working after about one month, probably due to me sitting on the security key while it's in my wallet. The second one continues to work, but one day PayPal wouldn't even recognize it. In fact, when I called PayPal, the customer service rep said it wouldn't work because I didn't buy it from PayPal, even though I did. In fact, their logo is plastered on the front. She sent me the new security key, and I'll try to get this one working. I asked about the football-shaped dongle that used to be available and was told they don't sell them anymore, only these new credit card formats. I hope you and Leo get back to reality sometime soon; okay? I don't know what that means. Can you - care to explain? I've been using this, but I got this one. This is the VIP thing that you and I have talked about from VeriSign. But I presume that's what PayPal is now distributing, something like this; right?

Steve: Yes. I thought this was interesting. Apparently what happened is that the footballs are dying, and the batteries, as he says, are dying. Now, I have one of each. And I've got the football next to me, which I use every couple days. Now I'm a little anxious about whether it's going to die because that would be a problem. Although I do also have the credit card format. Now, remember that the football, I think the problem with the battery life on the football is that it has a clock in it which is running all the time, even when we're not pressing the button. Pressing the button basically just causes it to perform a little calculation based on the current time of day and then display the code, which is valid for 30 seconds, and it changes every 30 seconds.

The credit card approach has the advantage of consuming zero power. And even when it - so when you press the little "Press Here" button, it briefly fires it up, and it produces an incremental next code which is not based on time, but which is based strictly on a cryptographic sequence. So there's a counter which is driving a cryptographic algorithm based on a secret key which it knows and which the authenticating agent at the other side - and VeriSign is behind all of this. VeriSign is the technology that PayPal uses, and VeriSign provides the gateway. So this is exactly the credit card that we've talked about before.

I've never had mine die. Mine's in my wallet, too. When I take it out, I notice it does have sort of a slight curve to it. And I think, well, okay, it seems to be working just fine. So anyway, I just wanted to apprise our listeners of the fact that that's what's going on, that PayPal has apparently backed out of the football that we've talked about and enjoyed in favor of this credit card, probably because it's got a greater lifetime. This little clock is running in the football whether you're using it or not, whereas the credit card probably lasts many more years.

Leo: I've been sitting on this for a long time. I keep this in my wallet, the credit card, and it's been pretty reliable. So...

Steve: Yeah, I do, too.

Leo: Yeah. Hmm. But we got ours, well, I guess this is the same. Ours say VeriSign, not PayPal. And you can use it with PayPal. Maybe that's another solution. People might want to go to the VIP program at VeriSign and get that one and use it with PayPal. You can use that one with PayPal. Not with eBay, oddly enough.

Steve: Yeah, it is odd. I don't - I'm not quite sure how they're hooked together.

Leo: What PayPal's been doing lately, which I prefer, frankly, is sending me a text message on my phone. So you can add a cell phone to your authentication means and have it - and then when you log into PayPal it'll say, well, what do you want to use - your football, the card - and now three devices - football, the card, or the cell phone. And now I just always say cell phone, just send me a text message, because I always have it with me.

Steve: Right.

Leo: And that works fine.

Steve: Right.

Leo: Maybe that's, in the long run - in fact, before your football dies, set up your cell phone to do that.

Steve: Well, and what's interesting, too, is if somebody were to choose that who was trying to pretend to be you and log onto PayPal...

Leo: I'd get a notice.

Steve: You'd get a call.

Leo: Yeah.

Steve: Yeah, and it's like, wait a minute, why am I receiving a confirmation code from PayPal? I'm not trying to log in.

Leo: There's not much you can do about it. Somebody's - I get at least once a week a French language email from somebody trying to get my Gmail account because my name is French. And obviously somebody thinks that's their account, even though it's not. And it must drive them - I'm sure it's driving them crazy. I keep sending email, I never get it. Yeah, because it's the wrong email. I'm getting it. And so it is a warning. But what are you going to do? Question number - let's see. Oh, I jumped ahead there. Wait a minute. Hold on.

Steve: That's...

Leo: Oh, no, you didn't - you jumped ahead.

Steve: I did?

Leo: You went from one to four. Unless I've made a terrible mistake. Oh, I see what happened here.

Steve: I've got a page two. I mean, I have a Question 2.

Leo: My pages are all messed up. Question 2, Zane Killingsworth. Is that correct?

Steve: Yes.

Leo: From Dawsonville, Georgia, wants help securing a new PC. He says: Hi. Hello. I'm a young PC enthusiast who is getting a new PC in the near future, and I want help with what security software I should get. Well, I think we now know what the answer is going to be. But I thought I was fine with Norton's 360 [gasp] until I started putting a lot of files on my desktop and read the book "Little Brother" by Cory Doctorow. I was so shocked by my lack of security that I tried to put Paranoid Linux on my PC. I didn't know there was such a distro. That's funny. But since the book used a version of it on a future Xbox, I thought that, like almost everything in the book, it was real, but it was just a little startup that died. I guess there is no Paranoid Linux.

Since then I've listened to every Security Now! podcast to try to be more secure. Also very happy to say that because of my listening I've helped my school. I'm home schooled and take science classes out of my home at a local small school for homeschoolers. I helped them determine that their WiFi network was compromised and helped them pick a new, more secure WiFi router. Yay. So help me pick a better solution for security, for antivirus, and what other software I need. Steve?

Steve: Well, in the beginning of Zane's note he - it felt to me like he had gotten himself overly concerned.

Leo: Yes.

Steve: And so I wanted to address that because I do see that in email and in our newsgroups, you know, people who really, it's like the concern for security is consuming their life. They're afraid to go out of the house, or only want to do so between the hours of 11:00 and 1:00 when they're sure that the sun won't set too quickly on them. And it's - so I just wanted to address that, the issue of it being possible to be so concerned about security that you're not having any fun anymore. And this should be fun.

All of the evidence indicates that there are agencies and individuals and groups that are taking advantage of mistakes being made in the design of our computer technology as it exists today for their own advantage, and hurting other people in the process. There's a story that I'm going to share next week about a company, a construction company that is suing a bank because they feel that the bank's security, like the log-on security wasn't good enough, and $588,000 was stolen from their account as a consequence. So, I mean, these things do happen. But you really do want to keep some balance, I think.

So the idea of not using Windows in favor of something called Paranoid Linux, I mean, I know that there are people who enjoy being this focused on security. But I wouldn't ever promote the notion that it's necessary to be this focused on it because you still want to be able to have the freedom to do what you want to do. I mean, it's a little bit like you, Leo, having a problem with NoScript, or like turning scripting off. There we're sort of in a gray zone. You need to be able to see sites in general that you're reviewing, running the way they're meant to by the bulk of the population who do have scripting on; whereas I and many Security Now! listeners have said, wait a minute, I need a little more control. I'm going to turn scripting on selectively. When I notice that there seems to be something wrong, then I'll permit a site to operate. So again, you could have somebody who refuses to ever run scripting. But then, arguably, sites that you need or want to use won't work at all. So I'm thinking, okay, compromise. Yes, unfortunately, scripting is a mixed blessing; but it's one that we need.

So anyway, I just sort of wanted to respond to Zane's, he uses the word "paranoia," and say, look, you know, don't get yourself too scared about this. I hope that we strike a balance here during this last 216 podcasts of saying, look, here's the issues; here's the facts. We want to let everyone decide for themselves where they fall in the spectrum of really concerned and not concerned at all.

Leo: It's very easy to get paranoid about this stuff.

Steve: Which, not surprisingly, takes us to our third question.

Leo: And by the way, just to answer his question about what security package, I think it's pretty clear from our conversation at the beginning of the show that Microsoft Security Essentials would be the right choice. Yes?

Steve: Until we know otherwise, yes. I don't want to say anything until the jury's in or out or back or wherever the jury's going to go. But, yes, I have high hopes.

Leo: So far, so good.

Steve: Yes.

Leo: John in Ontario, yes, this is the next one, says - Ontario, California, by the way - says we're "so silly." Steve and Leo, we have been using Mac OS 9 since 1998 with an open IP address. We are now on OS X. We have 12 Macs on this via Verizon, each with its own public IP address. Always have, for over 10 years now. We have no protection of any kind, yet have never, ever been hacked. I think all this paranoia about hacking is just that: paranoia. And you and Leo just propagate it, the fear factor. And furthermore, why would any of us need your advice? After all, we're not harboring nuclear secrets or planned attacks on some geographic location. Would you two just get real? Wow. I'm hurt.

Steve: Well. There's the other side of the spectrum.

Leo: [Laughing]

Steve: I thought...

Leo: That's kind of head in the sand.

Steve: This really anchors both ends. Well, first of all, I would comment that OS X has a firewall, and it's turned on. And so you do have, automatically, protection from incoming threats. He's obviously not behind a NAT router. He says he's got individual IPs for each of the machines, and so each machine has a public IP, and it's out there on the 'Net. And that he's been doing this for, what, the last 10 years? I think that's great. I would feel...

Leo: It's kind of - I would liken it to somebody who says, you know, I never go to the doctor, and I've never had any vaccinations, and I'm just fine.

Steve: Yes.

Leo: Until you're not.

Steve: Yes. And here I am saying, yes, but if you take a little Vitamin D every day, the statistics show that you have much better prospects for the future.

Leo: Right. You're fine until you get hacked. And then, you know...

Steve: Yeah. I mean, it absolutely is the case that these problems are real. If you put a Windows machine on the 'Net with its own IP, with nothing protecting it, it will get commandeered. Security researchers do the experiments. There's just so much junk on the Internet. Now, it's true that he's in a better position with Macs than he is with PCs today. But we know that that's also a moving target, that as Macs become more popular we're seeing a greater incidence of acknowledged potential problems with Macs. So...

Leo: I should point out, though, that if he had done this with a Windows 98 machine he would indubitably have been hacked at this point. Yes?

Steve: And may not have known it.

Leo: May not know it. And may be hacked now, we don't know it.

Steve: Exactly. I mean, it's difficult to say. It's clear, you know, we talked last week about what's the relative security of different OSes and agreed that they're all soft. They're all softer than we wish they were. They've all got problems, a different nature of problems, different sorts of problems. The open source model has some. The closed source model has its. They're different. But fundamentally, complex software is going to have a problem with security, and complex software is what we have in all of these systems today. John's got very sophisticated software in his systems.

So I don't know really how to respond to him except that I would feel, with everything I know, extremely uncomfortable with machines that weren't behind a NAT router, that weren't behind - I guess I'm just - I'm used to it. I know how that technology works. I like the idea that it's protecting me from the outside. I know what's out there.

Am I paranoid? Well, it's certainly the case that millions of machines, Windows machines, were infected by the Conficker worm. I mean, we absolutely know that. It's taken down whole systems of hospitals over in England. And that's not illusory; that's real. And we've - people are having their machines infected by their actions as they click on links in email all the time. I mean, on several occasions I've had to spend a long weekend scraping stuff off of people's machines. And in some cases, there was one, a female friend of mine from Starbucks, about six months ago I referred to it, that I just - I looked at it for a while, and it was clearly just beyond recovery. So I formatted the disk and set it up for her, and she's now using Eudora and Firefox because I decided, okay, let's try to prevent this from happening again.

So these things really are out there. I'm glad John hasn't been bitten by one yet. And I hope if it does happen, it's not bad because he clearly believes that - for some reason he's listening to the podcast. But he believes that we're sort of a self-fulfilling prophecy. And I don't think that's the case. We happened because of the need, not creating the need.

Leo: I wouldn't feel too defensive. And in his defense, and this is kind of like we talked about with the last question, there certainly is - it can happen that people listen and go agh-agh-agh and just feel terrified and become an agoraphobic. And we're not trying to do that, either. I think...

Steve: Right.

Leo: ..the idea is reasoned information about the risks, and you be the judge. We're not, well, first of all, we should say we gain nothing. Neither of us make a security program that we sell. We gain nothing by you being afraid. We don't work for an antivirus company. So we're - and I'm not the security expert, Steve is. But I'll speak for you, Steve. You're just getting the information out there.

Steve: Well, and I really do think we maintain a balance.

Leo: We certainly try, yeah.

Steve: I think this is not the, oh, go screaming for the hills paranoia podcast.

Leo: And I'm the guy who says, eh, what the heck, I'm not - I'm going to run scripting. I'm not going to - you know.

Steve: And the fact is today on a Mac you're safer than today on a Windows machine.

Leo: Oh, yeah.

Steve: There's no doubt about it.

Leo: No question about that.

Steve: Yup.

Leo: Bob in Connecticut wants to know if we have seen and have had a response to an article. He says: I'm a longtime listener, love the podcast. Have you seen anything on this one-time password being defeated? Here's a link to the occurrence I read about. The title of the article, it's on TechnologyReview.com, which is - is that the MIT Technology Review?

Steve: Yes, yes.

Leo: That's a good journal. The title is "Real-Time Hackers Foil Two-Factor Security."

Steve: And a person who we both know as an author, Leo, Robert Lemos...

Leo: Oh, okay.

Steve: ...wrote the article. So this is MIT's Technology Review magazine. And I wanted to highlight it because, first of all, it's really interesting, and it's a perfect topic for us to discuss, and many of our listeners are apparently reading this or saw the link and said, hey, what about this, because we've talked so often about the strength of multifactor security.

Leo: Right.

Steve: And so the subtitle is "One-time passwords are vulnerable to new hacking techniques." And so Robert Lemos writes, he says: "In mid-July, an account manager at Ferma, a construction firm in Mountain View, California, logged in to the company's bank account to pay bills, using a one-time password to make the transactions more secure." That is, to log in.

"Yet the manager's computer had a hitchhiker. A forensic analysis performed later would reveal that an earlier visit to another website had allowed a malicious program to invade his computer. While the manager issued legitimate payments, the program" - behind his back - "initiated 27 transactions to various bank accounts, siphoning off $447,000 in a matter of minutes. 'They not only got into my system here, they were able to ascertain how much they could draw, so they drew the limit,' says Roy Ferrari, Ferma's president.

"The theft happened despite Ferma's use of a one-time password, a six-digit code issued by a small electronic device every 30 or 60 seconds." Well, we know what that is. "Online thieves have adapted to this additional security by creating special programs - real-time Trojan horses - that can issue transactions to a bank while the account holder is online, turning the one-time password into a weak link in the financial security chain. 'I think it's a broken model,' Ferrari says.

Security experts say that banks and consumers alike need to adapt - that banks should offer their account holders more security and consumers should take more steps to stay secure, especially protecting the computers they use for financial transactions.

"'We have to fundamentally rethink how customers interact with their banks online,' says Joe Stewart, director of malware research for security firm SecureWorks in Atlanta, Georgia. 'Putting all the issues with the technology aside, if [attackers] can run their code on your system, they can do anything you can do on your computer. They can become you.'"

So, and I'm not going to read the rest of the story because we've got the gist of it. So what happened was that an infected machine went online. And the software was clearly sophisticated enough, it used the fact that a one-time password had authenticated the session, the log-on session to - and this is amazing to me that this is, I mean, it's clearly possible, but that you would - that this manager would happen to have software that understood how to perform transactions behind his back using the credentials, the transient log-on credentials that he had established. I mean, it's chilling. And so again I would say to our prior questioner, [John] in Ontario, California, who thinks this is all paranoid, that, well, this stuff really does happen. So it's interesting because the title for next week's podcast is already "The Fundamentally Broken Browser Model."

Leo: Oh, boy. Can't wait.

Steve: Because that's what we'll be talking about when you're in Dubai, Leo, is that - because there was another presentation at the Black Hat conference recently in D.C. that I haven't been able to get out of my mind because it talks about breaking SSL, and it really doesn't do that. It leverages the fundamentally broken model of using a web browser for these sorts of things. And that really is the problem.

For example, if there was more granularity in the security transaction, for example, if you not only had to use the one-time password to log on, but you had to use it every single time you performed a transaction, well, then this particular breach would have been prevented because this breach was hijacking the user's current state, their logged-on state, and performing this work at the same time in the background that they were doing other things with their bank. But this does highlight the level of sophistication that we've now arisen to. I don't think this - I would be a little less harsh in criticizing multifactor authentication except that this does say to us, if this is the level of sophistication, then we need to push multifactor authentication even closer to what we're trying to authenticate.

The problem was, this was being used to authenticate the session. It's clear that, in the presence of this kind of malware, we need to authenticate the transaction and get closer to what it actually is we're trying to protect. We're trying to protect the transactions, plural. So we're assuming that the fact that they're wrapped in an authenticated session provides that protection. Well, this demonstrates that assumption is no longer valid. Now we need a per transaction authentication, which is a little more annoying. But if you've got the football right there, and you want that level of protection, if the bank said do you want to authenticate per transaction or per session, now you know you say per transaction. I want to have to - I want to challenge every single time I do something.

Leo: I suppose there's still a window, though, even if you're doing it per transaction. I mean, as long as there's 30 seconds, if their system is quick enough they can sneak in there while you're authenticating.

Steve: Yeah. You'd have to, I mean, I'd have to think about that, whether something could, I mean, it would be authenticating - you'd need something at your end that the malware couldn't get to that was tied to the details of the transaction. So you're basically - you provided the details of the transaction. Then the other end said, okay, I need you to sign the details of that transaction in a way that the malware could not sign its own transaction, which would be different from yours. So there are certainly ways to do this. But again, it's like, whoa, this clearly ups the ante.

Leo: Yeah. Very interesting.

Steve: And it's being done. Malware out there, we now know, is becoming that good. And so it does say, what the article went on to mention was that banks needed to provide consumers with, like, secure computers. It's like, well, okay. How's that going to work? It's not clear how we get there from here.

Leo: It's really, that just shows how determined and clever bad guys are.

Steve: Well, and this - actually this does set me up. I didn't - I ran across this in preparing today's Q&A. But, I mean, this sets me up for next week's discussion of the fact that, unfortunately, convenient as it is - remember, this all kind of happened to us. We had browsers that were going to allow us to look at static websites. And then it's like, oh, we can submit information. We can use forms and the "get" and the "post" commands to send stuff back. Suddenly now it's interactive. And then the banking said, oh, we really don't want to see you because it's expensive for us to hire tellers. So we're going to automate all this and put this online. And besides, we've been told that SSL is safe. Well, yeah. SSL is safe. Well, we know that there are caveats even there. But so the problem is this notion of using something as convenient as a web browser is really broken. And next week we're going to talk about some very clever approaches that demonstrate just how broken it is.

Leo: Yikes.

Steve: Yeah.

Leo: Question 5, Jacob Theobald in San Francisco. He wonders about the security of Internet Explorer tabs. Oh, I'm sorry. No, no, of the IE Tabs Firefox plug-in. That puts IE in Firefox.

Steve: Right.

Leo: Recently, by the way, I don't know if you saw this, Google put Chrome inside of IE, saying IE's never going to support HTML 5 well enough for us to use Google Wave, so we're just going to put a plug-in that puts Chrome in there. For people who want to keep using IE, but not give up Firefox, this is the same in the other direction. Hi, Steve and Leo. I've been wanting to ask this for a while but never got around to it. I've been using this IE Tabs Firefox add-on. From the looks of it, it can switch a specific tab to use the IE engine to view web pages, if you're in a case where you need IE, like Windows Update, for instance. Could any security vulnerabilities that affect IE affect Firefox through the use of this add-on?

Steve: Absolutely.

Leo: Yeah.

Steve: This is exactly like the problem of using the HTML viewer, which is IE, in Microsoft Outlook email, the infamous preview pane where you just select the email and it comes up in the preview pane. That's all it takes, if you happen to be viewing malicious email, for something to get a foothold in your machine. The idea is that, and this is Microsoft's whole - it started with OLE and became ActiveX. The idea is that the application has become basically sort of a window, literally a window frame and controls surrounding the code which displays the content. So essentially what Firefox is doing with the - or I should say the IE Tabs add-in to Firefox is doing is it's instantiating, creating an instance of the full Internet Explorer viewer that just happens to be wrapped with Firefox's borders and controls and window dressing, rather than IE's. But it's in no way more secure. It's sort of the lowest common denominator approach. So, yes, I can see the appeal.

So my advice would be use it as little as possible. Use it for Windows Update and only for websites that you trust that won't run in Firefox. I have IE, even though I'm exclusively using Firefox now, I use IE to run Windows Update, and that's it. And very rarely I'll see some site that just is really badly written that absolutely requires IE. And, I mean, I call it badly written because they're really restricting themselves to a subset of the Internet. Firefox is increasing its market share all the time, and for good reason. So, yes, it's absolutely you are vulnerable to all IE vulnerabilities if anything uses that IE ActiveX control, whether it's email or any other browser who says, oh, look, you get the benefits of both. It's like, well, and the liabilities of both.

Leo: Right. Of course IE's always running on all Windows machines. So that's why, if you look at HTML email or anything, it's always there. The engine's always there.

Hard to get away from it. Moving right along to our next...

Steve: It's not in my system, Leo.

Leo: How do you get rid of it?

Steve: I just - I use Eudora, which doesn't use the process at all.

Leo: Oh, I see. Yeah, but IE, if you've got Windows, the rendering engine is there at all times. And it's kind of hard - I'll give you an example. It's kind of hard to know when it's being used. Quicken, for a long time, Intuit - and may still, for this matter - would embed an IE window inside its Quicken so that you could see online data from the Intuit website.

Steve: Yup, and in fact there have been programs that will say "Requires Internet Explorer v6 to be installed in your machine," in order for something entirely non-web browser-y to work because they're relying on that component. So anyway, I wouldn't say that it's always running. But it's certainly the case that it has the ability to pop up, literally, when you're not expecting it.

Leo: Yeah. It's almost always running. Well, okay, I'll give you another example. When you're using Explorer to explore the hard drive, and you enter in a URL in that Explorer window, it will then open the web page.

Steve: Ah, yeah.

Leo: Isn't Explorer, I mean, I don't know what the difference is, IE and Explorer.

Steve: Well, they're very different. So...

Leo: Okay, so it's just the rendering engine just says, oh, never mind, I'm going to use IE instead to do this.

Steve: Right.

Leo: Okay. They're different programs.

Steve: Right.

Leo: But they have a direct link.

Steve: They do.

Leo: Donald Burr in Santa Maria, California has some feedback to our answer, "Should I run my own server?" Remember we talked about that a couple weeks ago. Well, in fact he says...

Steve: Two weeks.

Leo: Two weeks ago. In your Listener Feedback #75 episode you answered Dax Mars' question - I love that name; and he says, and I love it, too - about running his own server at home. Your response recommended going with the most secure distribution of a UNIX-like operating system and specifically mentioned NetBSD or FreeBSD. While I agree with the overall concept of shying away from Windows, I would instead recommend that he goes with a Linux distribution, specifically one based around Debian's package management system. There is, for example, a version of Ubuntu specifically tailored for servers that would be ideal for this.

One of the most important things that a person as a server administrator needs to do is to keep up on software updates. I'm sure you'll agree with me on that. However, unless I'm mistaken, updating a BSD system is difficult and involves having to rebuild the kernel, user space tools, et cetera, and even for an intermediate-level user can prove to be a daunting undertaking.

Debian-based distributions, on the other hand, have a very easy way of upgrading the system involving only two shell commands, apt-get update and then apt-get upgrade. These two simple commands will download the latest version of all Linux tools, including any third-party programs you may have installed like Apache web server or MySQL database. The Debian and Ubuntu folks are very proactive when it comes to incorporating the latest security fixes into their packages. Just my two cents. Love the show. Love that SpinRite. It has saved my bacon on more occasions than I can count. So that's a good point. But there'll be a debate over this, I think.

Steve: I think it's a very good point. Well, the issue of OS is religious. Everybody has their own, for their own reason. And so I wanted to share Donald's recommendation. And I don't disagree. I mean, I've used Debian Linux, and I like the packet manager that Debian has. And obviously Ubuntu is a very popular solution, as well. So one thing that I might add is that for a non-UNIX or Linux user, someone who's moving from Windows, all of this stuff is a lot less obvious and easy to use than Windows is. And so one thing that may - I mean, I guess I feel a little bit like it's six of one, half a dozen of the other. Except if you've got some friends who have a bias or experience, it could ease the transition a lot to say, well, what are you guys using? I'd like to use the same thing so I have someone I can call when I have a question.

Leo: Right. Yeah, that's, of course, true. But was it you or was it, no, I think it might be Randal Schwartz who prefers - he says the most secure network operating system is NetBSD, or I can't remember.

Steve: Well, and that takes us into Question #7.

Leo: Oh, well, let's move along, then. Let's move along. OpenBSD. Randal says OpenBSD. He's in our chatroom. He's getting ready for Floss Weekly.

Steve: Then he's going to like Question #7.

Leo: All right. Donald, no, that was Donald. This is Bob Carneim in Oak Ridge, Tennessee. What do you have against Theo? Okay. I should have read that. I'm just listening to the latest Episode 214. At one point you recommend running a web server on the securest version of UNIX available. I certainly agree with that, especially versus any Windows OS. But you only mentioned NetBSD and FreeBSD. What about OpenBSD?

A little while ago I did research on what OS to try to use for some applications where security is particularly important. I eliminated Windows, I eliminated Mac OS, and I eliminated Linux. I don't think I need to explain any of that decision-making process. I thought about Sun's offerings - Solaris, I guess - but decided that, since I'm a Mac guy, I'd probably have an easier time acclimating to one of the BSDs (Berkeley Software Distribution). I read the mission statements for the big three: FreeBSD is all about getting everything to work, lots of applications ported to FreeBSD, lots of device drivers, that sort of thing. NetBSD is mainly about working on anything. You could probably install it on an abacus, he says. Finally, OpenBSD claims itself to be, among other things, secure by default.

That last statement caught my interest. I read about what they claim to try to do - specially and strictly formatted code that makes it easier to audit, and auditing code for correctness and security even before a flaw or exploit is known. That's the attitude I was looking for and wish everyone had, and I didn't see any reports that OpenBSD was not doing as they claimed, so I'm going with it. It's a little more difficult to do certain things; but I, like probably most Security Now! listeners, understand that it's necessary to give up a little bit - sometimes a lot - of convenience for the sake of security. I don't consider that a hardship. The classic example is that, when you enable Apache in the default install, it runs chrooted - so does BIND, by the way - so creating dynamic, database-driven websites takes an extra bit of planning and work.

Anyway, I'm not associated with the project other than as a user, and I don't know Theo. Theo, by the way, is the guy who wrote it. But so far I think OpenBSD is great. Should I maybe not? Is their claim of proactive security all hype? What have you heard? Should I panic? Argh! Thanks.

Steve: Well, it's interesting because his comment parallels some dialogue that popped up immediately in the GRC newsgroup, the Security Now! newsgroup, saying, hey, wait a minute, what about OpenBSD, Steve? Why didn't you talk about that? And again, it's just a matter of familiarity, which by no means means I wanted to slight OpenBSD. I just ended up first using FreeBSD, and that's where I'm comfortable. And I've looked at

NetBSD and just sort of haven't gotten around to OpenBSD. I haven't needed to. But I absolutely wanted to give it its due and its moment in the sun. And apparently Randal Schwartz is an OpenBSD advocate, also.

Leo: Yes.

Steve: So that says a lot for it.

Leo: We've had this conversation, Randal and I. And I think that - I'm trying to remember, and I've asked Randal. But as I remember, there have been two exploits, two exploits total, since OpenBSD was created.

Steve: Which is a phenomenally low number.

Leo: That's amazing.

Steve: Yeah.

Leo: So that kind of obviates the whole need for patching. And remember, patching - if you've got exploits, you've got to patch. But patches as frequently as not, I think, introduce other exploits. So patching isn't the magic panacea, either. It would be like...

Steve: Patching, yes, patching is something that unfortunately we've all become abused into accepting. But it doesn't, I mean, you'd much rather have something that didn't need it than something that was like, oh, look how often we're patching. Aren't we wonderful. It's like, okay.

Leo: Right. Patching can just introduce some new problems.

Steve: Absolutely.

Leo: So OpenBSD, yeah, I think that everywhere I've heard, that's kind of the - everybody says, yeah, it's true. Leo's got it right.

Steve: So by no means did I mean to exclude it by having just said, when I did, FreeBSD or NetBSD. Open BSD.

Leo: Right. Emil in Denmark, our Question #8, found an overlooked feature in TrueCrypt: Hi, Steve and Leo. I think I found a feature in TrueCrypt you have not previously mentioned in Security Now!: TrueCrypt => Settings => Preferences =>

More Settings => System Encryption. When preboot authentication is configured, the log-in screen says "TrueCrypt Boot Loader" and asks you to enter your password. With this menu item you can change this however you like so that no text appears at all. Or you can write a short custom message such as - I like this one.

Steve: I love this.

Leo: "Missing Operating System." I guess you could even write your password as the message in case you forget it, but that's not a good idea. It could still be technically possible for an attacker to prove that TrueCrypt is installed on the drive, but I think this is a cool feature, perhaps even worth mentioning in the show. What a great idea.

Steve: I just - I thought it was so clever, I mean, all of us who have used computers for a long time are, you know, we see our life pass before our eyes when you boot the system and it comes up "Missing Operating System." It's like, oh, what now. Or sometimes you'll move a drive to a different machine, and it'll be the wrong - it'll be a primary on one machine and a secondary on the other. So there are various reasons you can get that. But frankly, if I turned a machine on, and it said "TrueCrypt Boot Loader," I'd go, oh, okay, now I know...

Leo: Now I know something.

Steve: Yeah. And again, where no one is endorsing security through obscurity, this isn't that because you still have all the security that you would have if it loudly proclaimed itself to be TrueCrypt Boot Loader, but instead you've just sort of thrown everybody right off the scent by saying "Missing Operating System." It's like, ohhh. It's like, don't even bother going any further.

Leo: There's a difference between security through obscurity and not giving people more information than they need. That's why you say stealth your ports.

Steve: Right.

Leo: Why volunteer information? Why volunteer that TrueCrypt's installed? In fact...

Steve: I have a buddy who's got his WiFi router's SSID set, the beacon that you can see whenever you browse, like, WiFi in your area, he has it set to NORAD Missile Command or something.

Leo: Now, that could go both ways. That might encourage somebody to try to break in.

Steve: I just think someone says, oh, crap, I'm not going to touch that. They're going to get me. So I just like "Missing Operating System." That's classic. That's just beautiful. I wanted to give Emil a little nod of the head for that one.

Leo: That's really good. Bobcat in our chatroom says his TrueCrypt login, boot login is "NT Loader Is Missing." Another good one. Make it look as much like the real thing; right? Paul Dove in Hampton, UK, Question #9, our penultimate question, is using WAN router administration. Oh, we were talking about disabling that. And we said, well, who would use that? Who would ever...

Steve: Who would ever want that?

Leo: And in fact he's quoting you from Episode 214 saying, "It's very distressing, Leo, if there are still routers that have WAN admin on. I mean, nobody needs it." Well, Paul says, I have three routers connected in a Y with a WPA router on one branch of the Y - this is what we talked about as the way to do WEP securely.

Steve: Yup, the ultimate WiFi security.

Leo: So he's got WPA on one, WEP router on the other, and then they are connected, the two of them, to a third router. He says: I only have the WEP router so my kids can connect their Nintendo DS. That's exactly why you do it.

Steve: Yup.

Leo: I would never want to connect any PC to this router, so I have it set to WAN admin so that I can change settings by accessing it externally. But I'm still behind the router and firewall at the base of the Y. And when I'm accessing the settings this way I don't think there's any way data can get from the WEP device to my main WPA network. Am I safe?

Steve: I thought that was a really interesting and great reaction.

Leo: It's a good use, yup.

Steve: Yes. He is certainly safe. What you don't want is the Internet to have access to your WAN admin because without other provisions there's nothing to prevent someone from just pounding away on its login, trying to get in. But here he's using - he's got WAN admin on one of his internal or interior routers, so that he's able to access it from outside of the WEP protected network but still inside his own local area network because that's inside the router which is interfacing that Y to the Internet.

So, yeah, I thought that was a great reason, and he should be completely comfortable with that. There's no way bad guys can get to his WAN interface. And certainly no way anybody on the WEP side can get to it, either. So it being enabled is fine.

Although you definitely want to make sure that you've got a very strong password on your LAN side login for the WEP router because we know how broken WEP is. And so by catching some packets while your kids are using their Nintendo DS, they would be able to get the WEP key, and that would allow them to try to log into the WEP router on the LAN side using the web interface. So you would absolutely want to protect that.

Leo: It's already more broken just because it's using WEP than WAN administration; right? I mean...

Steve: Right, right. That's a very good point. That's a good way of looking at it. That's the bigger concern than the WAN side being exposed, which is only exposed internally. So I thought that was very clever.

Leo: Good. Our last question, Steve, from Dave and Max in the UK. And they want to know, can we watch Security Now! after it's been broadcast? I know you guys broadcast it live. Yes, we do. We do it every Wednesday at 2:00 p.m. Eastern.

Steve: Actually, Leo, that's right now.

Leo: Oh, yeah. 11:00 a.m. Pacific, which is 1800 British standard, actually British daylight time. But is there any way I can watch the episode after it's been recorded? We're in UK, so due to the time difference we're unable to watch Security Now! live. I'm sure other listeners would like to watch live after it's been recorded. So keep up the good work. Well, I have good news on that count.

Steve: This was one for you, Leo.

Leo: And we're kind of pre-announcing it. So it's not ready yet. Right now, the way we do Security Now!, we do record it live. And as with all our shows, you can watch that live recording. You know, think of it as a spy cam into my studio, although it's a little fancier than that. And we in fact replay it again and again later in the day. So Wednesday evening and - Steve, Steve, Steve. Steve's playing with the camera now. Wednesday evening and Thursday in the early morning hours you can probably catch it with other shows being rerun. But that's not very satisfactory. So some of our viewers have for the last year been capturing the Flash and putting it on their website, with our permission and encouragement: ODTV.me. ODTV.me. So you can, in fact, go back and watch reruns there. But we're about to announce, in a couple of weeks, at Blog World we're going to announce this...

Steve: What, what, what, what, what?

Leo: That we're going to offer video of this show and our top five shows, and then slowly roll out video of all the shows, both for download on iTunes or whatever you use for your podcatcher, the Zune, you can watch it on the Zune HD. That will be one way you can get it. But we're also working with a company called Mediafly. They're going to put it on the Roku box. I know you know about the Roku Netflix player. So you'll be able to watch us. And I think - again, this is a pre-announce, so I probably shouldn't even say this. But I think you'll be able to watch both live or after the fact, so on that Roku box. And then we're going to slowly roll it out on a lot of platforms.

And my hope is, my plan is that, on whatever platform it rolls out, whether it's your portable phone, your television, your TiVo, whatever, that you'll both be able to watch what's currently live or what was live, so that you have kind of the choice. You know, you can either - it's like on-demand or live. So that you would be, Dave and Max, you'd be able to go there, and you'd say, well, I missed the live broadcast, but I want to see it again, and be able to press a button and be able to watch it. Now, Roku's not available in the UK, but this is coming your way soon.

And we're rejiggering everything to make this possible and spending a lot of money. We have to get a SAN device. We're going to change all of our editing from just audio editing to audio and video editing in Final Cut. We've had our little - our squirrels, Colleen and Erik and Tony, working like crazy to get this ready. And we hope to have it ready in the next few weeks. So we'll let you know when that is available. But, yeah, this will be - I'm pretty sure this will be one of the shows that we roll out right away. I can't remember what the list is. But it's certainly on the list.

Steve: Where is Security Now! in the ranking? Because once upon a time TWiT was number one and...

Leo: TWiT's number one.

Steve: ...we were number two. Are we still?

Leo: You were the - this was the second show. No, I think it's TWiT, MacBreak Weekly and Windows Weekly in a close tie, Net@Nite and Security Now! in a tie for third place, and then - actually, you know, TWiG, our newest show, is now I think in third place.

Steve: Wow.

Leo: It's going up very fast, yeah.

Steve: And that's This Week in Google?

Leo: Yeah. Yeah. And that's because of the subject matter, but also because of our host. We have Gina Trapani and Jeff Jarvis are so good and have lots of fans in their own right.

Steve: She's neat. I saw a replay of that. I'm thinking, okay, who is this, and what show is this?

Leo: She created Lifehacker. I mean, Gina is like, you would love her. She's a programmer. She's a productivity guru. Just a great person. She lives in San Diego, kind of down your way.

Steve: Yeah, she's neat.

Leo: Yeah. So it's my goal to do two things. I think in the long run, I mean, the audio podcasts are what got us started, and they still pay all the bills. But in the long run it's my goal to create a 24-hour kind of CNN for geeks that all of our shows would be part of, and additional shows, you know, almost 24/7, as close to that as we can get.

Steve: And would always there be live streaming? Or could it be that it would end up just being download on demand shows?

Leo: I want to keep doing live streaming because I think that the idea of being able to just go somewhere and press a button and whatever's on you watch, and that would make us more - for instance, in about 20 minutes we're going to check in, at 1:00 o'clock we're going to check in with The New York Times and see what they're working today. So I want to be - I want to have a live kind of network that, whatever's going on, you're always kind of apprised of what's right now because people like live. But at the same time we realize that, if we do it live, everybody's gotten conditioned to being able to TiVo everything on television. So we've got to make it, you know, some way for you to be able to get the stuff after the fact. So we'll make - that's really what's going on here. That's why we're doing the downloads.

Steve: I think it's perfect. It sounds like it's - those bases are covered, Leo.

Leo: Well, it's a project. It's quite an investment financially and in terms of manpower. You know we've got - there's now seven full-time people working here, and a goodly number of part-timers. So it's expanding very rapidly. But I won't ever be as big as - you are the cautionary tale on getting too big. I don't ever want to be so big that I have to go to meetings all day.

Steve: No, especially when your meetings have meetings.

Leo: There is a staff meeting now, in about 15 minutes, however. We now have a staff meeting. Of course, when you say all hands, we can fit around a small round table. So it's not so bad.

Steve: That's good. Well, we're going to talk next in two weeks, since you're going to be in some big, high, highest building in the world in Dubai when Alex Lindsay and I are talking about the fundamentally broken browser model.

Leo: Oh, that'll be fascinating. And then I'll be back in time for Q&A #77.

Steve: Yup. And then we're going to do a really neat episode about the innards of JavaScript...

Leo: Oh, that's going to be fun.

Steve: ...and its fundamental problems with our friend John Graham-Cumming.

Leo: Creator of "The Geek Atlas."

Steve: Yeah.

Leo: He's the guy, too, when we interviewed him on TWiT, who got the apology from the British government for Alan Turing's prosecution. Really neat guy.

Steve: Very cool.

Leo: Love John. So that's going to be fun. I can't wait for that. Steve, always a pleasure. Don't forget, Steve's at GRC.com. That's the place to go to get your copy of SpinRite and all those free, wonderful utilities that Steve is just cranking out all the time. GRC, that's short for Gibson Research Corporation, GRC.com. And if you go to GRC.com/feedback, you can give Steve questions for future episodes.

Steve: Please do.

Leo: Yeah. You can also get 16KB versions of this show for the bandwidth impaired, full transcripts, and show notes there, as well as on our wiki - wiki.twit.tv - and our FriendFeed conversation pit. That's FriendFeed.com/twit-conversations. Follow along there in real-time. And our chatroom. Let's not leave that out, as long as I'm giving you everybody - IRC.twit.tv. Steve, we'll see you next - I won't, but everybody else will see you next week.

Steve: Thanks, Leo.