
# Listener Feedback Q&A #59

**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-182.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-182-lq.mp3

---

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

**Leo Laporte:** Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 182 for February 5, 2009: Your questions, Steve's answers, #59. This show is brought to you by listeners like you and your contributions. We couldn't do it without you. Thanks so much.

It's time for Security Now!, time for us to talk about protecting yourself online and off, protecting your privacy, protecting your special precious assets. And there's no one who knows more about this subject than Steve Gibson from GRC.

**Steve Gibson:** Hey, well, I don't know that I would put it that way. But I'm the only one you can get in front of a microphone with.

**Leo:** That can actually speak. No, that's true. I mean, there are security researchers, there are wonderful security researchers out there.

**Steve:** Oh, I worship them. They're...

**Leo:** I should finish the sentence. You know more about it, and you're better able to explain it, than anybody else.

**Steve:** I enjoy communicating what I have figured out and learned. That's definitely the case.

**Leo:** I did an interview last night with Marc Germain, who's been in L.A. radio for years. And he said, well, you know, I listen to Steve, but I don't understand. It goes right over my head. And I said Steve is not for everyone. I'm not saying this is a show that everybody should listen to, although everybody should learn from it. But this is for people who really want to know the inner workings of this. But you're very clear and very explicit about how it all works.

**Steve:** Well, we have a Q&A episode this week. And I just - I love reading the feedback from our listeners. And once again I ran across somebody who had written in the last two weeks - because I normally dump the mail bag every two weeks. And there were 384 submissions from the last time I'd dumped it two weeks ago.

**Leo:** Wow.

**Steve:** And, I mean, I'm just - and I'm so heartbroken that I just - I can't respond to them all. Just there isn't time. I mean, if I did nothing else, then I could. But then nothing else would happen. So, but once again, I ran across one person who'd written that the podcast had inspired them about computers to go back to get their degree. They're doing some post-degree work. And, I mean, because of the podcast. Which is way cool. I really like...

**Leo:** Wow. Wow.

**Steve:** That's spectacular.

**Leo:** Yeah. Well, and that shows that people really want to know this stuff. And I guess that's what I would say is this is the show, if you really want to know this stuff, this is where you're going to hear it.

**Steve:** Well, and I know that we talk about this all the time. But life is more and more on the Internet, and more and more of our life is on the Internet. And one of the other things that I keep running across as I'm reading feedback from people is they comment that they're so much more aware now, after listening to the podcast, of the issues. I mean, and certainly, it certainly raises some concern. But on the other hand, you can't be concerned about what you don't know. So in knowing what's going on, it's natural to get more concerned. But I would argue, well, people should be, I mean, to some degree. Not all freaked out and paranoid. But, I mean, take reasonable steps, given that you know what the dangers are.

**Leo:** Yeah, that's one thing Marc said is that I don't do everything Steve recommends. I just find it overwhelming. And I said, you know, I don't either. But it's good to know. It's good to know, in other words, instead of just wandering

blithely...

**Steve:** Make an intelligence choice.

**Leo:** Yes, exactly. The more you know, the more you can make that choice. So that's really the value of this.

**Steve:** Yeah, we were talking before we began recording a little bit about some of the issues that we're going to discuss today. And I mentioned that we've got a couple more new bonehead security moves on PayPal's part. And I was saying they're so dominant and so important that they really ought to hire someone who knows security to, like, fix this stuff. Because it's just - the two things we're going to wrap up the Q&A with at the end of the show are just, I mean, it's like, oh, my god, you're kidding.

And I was mentioning to you that I've been using PayPal a lot recently because I've been doing some antique collecting of old machines. You started this, again, because you held up that damn plane of core memory, and I thought, I gotta get some of that. And that of course led me back to the PDP-8 and the whole PDP-8 construction project. But then, as I sort of remembered those machines, I thought, well, now, what about an 11? And what about a VAX?

**Leo:** Oh, no.

**Steve:** And so, and I have been reading a couple books about the history of Digital Equipment Corporation and remembering that the PDP-11 is one that I never had the chance to program. I sort of just stepped over that into the microcomputers, you know, the 8008, the 8086, and the 8088, and never got into the VAX. But DEC deliberately designed the instruction sets of the VAX and, well, of the PDP-11 and then the VAX, which was sort of an expansion of the 11's instruction set, to be pleasant to program in Assembly language. I mean, they designed them for me. And a consequence of that was that they would be efficient for compilers to produce code for.

But I thought, okay, I gotta get me some of these before they all disappear because they are, I mean, they are beginning to disappear. These machines are, unfortunately, even collectors who end up with a collection that they're proud of, you know, they die, and their wives don't know what to do with them, or the family doesn't know what to do, I mean, they end up just being scrapped one way or the other. So I thought, okay, I've got to get busy now, protect this equipment. Because I figure in about 30 years, when I'm 80-something, that'll be about the time that I want to sit down and do some PDP-11 programming and some VAX programming. So anyway, I've been using PayPal a lot. And I've got my little football with me all the time. And I'm happy with it. But I'm less happy with it now than I was yesterday, before I read the two things that we're going to wrap up this Q&A with.

**Leo:** Oh, oh, oh.

**Steve:** Yeah.

**Leo:** Okay. So just off the top of your head, you've got, you said, how many, two PDP-8s...

**Steve:** No, actually, I ended up - the gal that I connected up with tossed in a couple others in unknown condition. And they're not nearly as nice as the ones I had, but they're workable. So at some point I will - I need to do some restoration because they're - I couldn't - you couldn't plug them in and use them right now.

**Leo:** And you bought three kits.

**Steve:** So then I bought three of the really neat PDP-8, the SpareTimeGizmos kits.

**Leo:** So you've got, like, five or more, five-plus PDP-8s.

**Steve:** Yeah. Well, on the other hand, I mean, consider how many PCs I have.

**Leo:** I'm not knocking you. I'm trying to get an inventory here.

**Steve:** Oh, okay. And then there was...

**Leo:** I just bought two laptops. Believe me, I'm not the guy to knock you.

**Steve:** Okay, yeah. And then I also got, sight unseen, a pair of PDP-11s.

**Leo:** Now, how big are those?

**Steve:** They're, well, they come in a whole range of sizes. I mean, and in fact the 11 was designed deliberately to be a scalable computer. And one of the things that I've really enjoyed about reading the history of this is that - I can't think of his name. Not Gordon Moore. That's Intel.

**Leo:** Oh, Gordon Bell, yeah.

**Steve:** Gordon Bell, exactly.

**Leo:** Of DEC, yeah.

**Steve:** Gordon Bell, who was the original DEC guy. He really understood about Moore's

Law, and that in their terms Moore's Law means that about every - I don't remember now what the numbers were exactly. But it's like...

**Leo:** Every 18 months, I think, it doubles, yeah.

**Steve:** Every year and a half you needed two more bits of addressing, from their standpoint.

**Leo:** Ah, interesting.

**Steve:** And so they literally looked at it in terms of, as computers grow, the one thing they keep outgrowing is memory. I mean, Bill Gates, as we all know, famously said that you would never need more than 640K in a PC. 640K.

**Leo:** K. K. K.

**Steve:** Not even a meg. So, and that was when the Apple II had 64K.

**Leo:** Right.

**Steve:** And so this was, oh, 10 times that much. You could never fill that up with anything. So anyway, it's been an interesting adventure. The PDP-11 was - it also outgrew itself. But it grew for many orders of magnitude and lasted for a long time and was a really popular machine. So, sight unseen, I bought two from the same gal. And one of them has all of its boards, but it's pretty banged up. I mean, it's just sad to see a classic machine just brutalized. The other one is in better shape, but is empty, no boards. So I figure between the two I've got a nice chassis, and then the other one's got the boards. But again, they need - it needs to be, like, completely taken down to its constituent parts, everything cleaned. Probably I would have the cases repainted. And I would like to restore them to, like, museum-grade mint condition. I think that'd just be really fun.

**Leo:** Very cool.

**Steve:** So sort of like somebody who, like, works on old cars, that kind of thing.

**Leo:** You going to get any VAXen?

**Steve:** I have some.

**Leo:** You've got VAXes?

**Steve:** I have VAXen. The VAX went from being a really monster machine - it also lived a long time and got well into the LSI microcomputer era. So there are MicroVAXes which are cute little one-inch-high things. There's even called - there's a VAX Station 4000 VLC that stands for Very Low Cost. And they literally go for a hundred dollars.

**Leo:** Wow.

**Steve:** On eBay. They run a strong flavor of UNIX, so you can run UNIX on it, and a lot of people do. But also VMS was the operating system DEC created special, I mean, they wrote VMS for the VAX. And it's often called VAX VMS. And then, of course, DEC got purchased by Compaq that got purchased by HP. So now HP has it, and it's called OpenVMS. And there's a hobbyist license for free. You can sign up for and get everything, the whole - the VMS and all what they call their layered products, which are, like, all the languages that are available, and everything is. And there's a really nice macro language which is the macro assembler. So anyway, I've sort of been pulling all that together in the background.

**Leo:** You going to stick with minis, or you going to go to - you're not going to have VIC-20s and Commodore 64s and...

**Steve:** Oh, I have all those already. I've got the whole Atari line, the Apple line, I mean, all of that stuff I had because I was using them. And I just - I never threw them away. I kept...

**Leo:** Where do you keep them? Do you have, like, a storage locker? I mean, how do you keep all this stuff?

**Steve:** Yeah, they're all offsite in a good, well-secured location, so...

**Leo:** It'd be really cool to - I think we need to set up a Steve Gibson Computer Museum.

**Steve:** Well, and to put this in perspective, too, there are many other collectors. There are collectors where you think, my god, this guy must have his own warehouse. I mean, where they've, like, got multiples of every PDP machine ever created, I mean, just phenomenal collections. And the question is, what's going to happen to that collection when they lose interest, or when they need money because the economy is in bad shape or whatever. So it's like, okay, I can't count on other people's collections to stay around. And I've also been scraping the 'Net for all of the software and documentation, so I'm getting my own copy. Because you run across lots of broken links, links of people's sites who used to be - who used to have all this documented and aggregated that are - they're just gone.

**Leo:** Right.

**Steve:** So I said, okay, now I've got to get it before it goes away any further, so.

**Leo:** There's, of course, it can be - in fact, we've been thinking about doing a show, and if we do this, we'll get you to come up, at the Computer History Museum in San Jose, which is a great place. In fact, it was Gordon Bell's wife, Gwen Bell, who founded that, with Gordon's help.

**Steve:** Well, you know, he's now at Microsoft.

**Leo:** Yeah, I know, he's a...

**Steve:** He's a Microsoft researcher. And in fact some of his pages from Microsoft are what I was reading where he was, like, talking - he has papers, you know, "What We Learned From the PDP-11." And, like, of no interest to anyone but someone like me, who's like, oh, I want to know what you learned from the PDP-11.

**Leo:** Yeah, no kidding. And then there's also the DigiBarn. We've interviewed them. I think they're up in the Santa Cruz Mountains. And he's, like you, he's just collected a ton of stuff and has people come up and so forth. It's Bruce Damer who does that. So he has a Cray in there, among other things. He's got an amazing collection. So I think you're right, I think there are a lot of hobbyists like you who do this. I think one of the big differences with you is that you really want to program these things.

**Steve:** Yes, exactly. I don't want to just run it. I mean, I actually want to write code for it. I think that would be really interesting.

**Leo:** I agree with you. I hope you get around to that project.

**Steve:** I will.

**Leo:** But not soon, because that means you'll have been retired for some time. And we don't want you to retire.

**Steve:** Yeah. I'm sure it's necessary for us to keep ourselves active and keep our brains going. And there are a number of things, projects that I would like to execute on those classic machines. And the fact is, newer machines are just not so fun to program in Assembler. They're all getting very sort of RISC-like, and they're not designed to be really people friendly at the machine level. And these DEC machines, they really were, the 8 and the 11 and the VAX. It's funny, too, because I actually read where Gordon Bell was saying, you know, our customers are programming in Assembly language, writing code for our minicomputers in Assembly language. So we need it to be a good Assembly language. It's like, wow, when did you last hear that? I mean, I'm the only one I know who programs in Assembly language still.

**Leo:** No kidding, no kidding. Well, do we have any notes...

**Steve:** Oh, we've got a bunch of notes and stuff here, Leo.

**Leo:** Okay. All right.

**Steve:** Security-wise it's been a very quiet week.

**Leo:** Hallelujah.

**Steve:** Of course, it was...

**Leo:** Patch Tuesday is coming next Tuesday, so...

**Steve:** That's true. And so we'll have news of that. But at this point the only really interesting story that I ran across and I thought our listeners would get a kick out of, and I'm sure you probably picked up on it because you're wired into what's going on, and that was about the road sign in Austin, Texas that was hacked. A temporary electronic road sign near, probably not coincidentally, the University of Texas at Austin, was hacked in the wee hours of the night to say "The end is near! Caution, Zombies Ahead! Run for Cold Climates!" And the reason this is of interest to Security Now! listeners is, get a load of this. The hack depended upon the fact that the equipment was using its default password.

**Leo:** No.

**Steve:** No one who had ever set this up, the city employees don't change the passwords on these things. So a lock was broken that gave the vandals access to the computer inside, which they were only able to reprogram because the password was the default for...

**Leo:** "Caution! Zombie Ahead!" is what it says. Oh, that is so funny.

**Steve:** Yeah. Yeah. So because the password was default, they were able to change the text. Oh, and then they changed the password to non-default, which further thwarted the city's efforts to change the text away from the zombie warning.

**Leo:** They had to take the thing home, back to the shop, to reprogram it.

**Steve:** It took a number of hours for the manufacturer to get involved and reset the password so that the employees could then put the text back to what it should be, so...

**Leo:** "Zombies in area! Run!" What do you think? Do you think people saw that and believed it?

**Steve:** No, I think people got a kick out of - I hope. I hope just the fact that it was on sort of an official electronic billboard wouldn't give it too much credibility. I think in this day and age people are like, okay, we're near the university, gee, what a coincidence.

**Leo:** "The end is near! Zombies in area! Run! Nazi zombies! Run." That is very funny.

**Steve:** Now, in other errata, I was listening to you a few days ago when you were going through a dictionary definition. You were saying that you had some show where you read definitions...

**Leo:** Oh, I was joking around, but I have - somebody gave me this book, "Radio-Television Electronics Dictionary."

**Steve:** Well, and the word that you jokingly talked about, but then did not answer...

**Leo:** Hysteresis? Was that it?

**Steve:** Was very close to my heart, hysteresis.

**Leo:** Well, now, why is that close to your heart?

**Steve:** Well, because it's the way core memory works, and I've got core memory all over the place at the moment. Hysteresis refers to a feature of magnetization and other properties where it's sort of difficult...

**Leo:** Well, I can just read - shall I read the definition out of here?

**Steve:** Okay.

**Leo:** The response of a magnetic material to an alternating magnetic field. The lagging of the induced magnetism behind the magnetizing force. 2. of an oscillator, a behavior that may occur in which multiple values of the output power and/or frequency will correspond to given values of an operating parameter. In radiation counter tubes, the temporary change in the counting rate versus voltage characteristic caused by previous operation. And then there's, you know, hysteresis error, hysteresis heater, hysteresis loop, loss, motor. This is clearly an important part of the "Radio-Television Electronics Dictionary." It's almost a quarter of a page

there.

**Steve:** One way to think of it is if you, for example, in the case of magnetization, if you apply a magnetic force against something which is ferrous, and you don't reach a threshold, then you haven't, like, pushed it over this hump. And so when you back off, you end up with no residual magnetization. But if you do reach this hump, it sort of - it pushes it past a point where - in the so-called "hysteresis curve" such that then it takes a greater reverse force to get it back. So it's sort of a - it's a nonlinear response in the case of a magnetic field, and so something that you're magnetizing. And it's the reason we have magnetic memory back in the old days. You know, core memory.

**Leo:** How interesting. Hysteresis.

**Steve:** So, hysteresis. Yeah, I mean, it's a well-known concept in engineering. And I can sort of, you know, close my eyes and see this sort of a boxlike curve which is called the "hysteresis curve," where it goes - you follow one path on the way up. And instead of retracing your path on the way back, you take a very different path on the way back, due to the fact that you've affected some object of physics. Through moving up you've changed something such that coming back to where you came from, you take a different path. So it's cool.

**Leo:** I guess once they discovered it, they thought of ways to use it.

**Steve:** There's some sci-fi news that I wanted to bring to our listeners' attention. Our old friend Joss Whedon is back. He's our old friend because he gave us "Firefly"

**Leo:** Yes.

**Steve:** Which was a spectacular series. What I was surprised about is that his new series is premiering on Fox, even though Fox screwed him.

**Leo:** You would think he'd have learned his lesson.

**Steve:** It was Fox who, after 11 episodes, canceled his series, even though there was already, what, three more that had been made. They didn't even bother to finish airing what he had made. And they played them all out of order, so they didn't make as much sense as they should have. I mean, they just really messed him up. And he was pissed off at the time. And then there was a huge fan outcry because "Firefly" was just so fun. And then it was generally regarded as having been a mistake for them to have canceled it because, I mean, it was like this - it was like, okay, why did you cancel this tremendous show?

So of course, as sci-fi followers know, he did produce a feature-length film, "Firefly," which I thought was fantastic, although I don't think, at least in terms of box office revenue, it did not even break even. I don't know what's - I haven't kept track of it. I

don't know if, like, in long-term DVD sales he ended up making money on it. But the point is, he's back with a new series that is premiering this coming Friday the 13th, February, Friday the 13th, 2009, at 9:00 p.m., obviously on Friday, which follows the new timeslot for "Terminator" on Fox, you know, "The Sarah Connor Chronicles," which I'm also loving. I think it's a good show. Anyway, I've seen a premiere of it, and it's about what they call "programmable people." And Wikipedia has a nice treatment of it. Reading from what Wikipedia wrote, it says "Eliza Dushku plays a young woman named Echo, a member of a group of people known as 'Actives,' or 'Dolls.'" Oh, and the series is called "Dollhouse."

**Leo:** What?

**Steve:** "The Dolls have had their personalities wiped so that they can be imprinted with any number of new personas, including memory, muscle memory, skills, and language, for different assignments. They're hired out for particular jobs, crimes, fantasies, and occasional good deeds. On missions, Actives are monitored internally" - whatever that means - "and remotely by Handlers. In between tasks they are mind-wiped again back into a childlike state and live in a futuristic dormitory/lab, a hidden facility nicknamed 'The Dollhouse.' The story follows Echo - or I guess the series, the series story arc follows Echo - "who begins in her mind-wiped state to become self-aware." So I don't know anything about it. I'm not saying it's...

**Leo:** Sounds cool. Sounds really cool.

**Steve:** And Josh has done good things.

**Leo:** Joss.

**Steve:** Josh. Joss?

**Leo:** I think it's J-o-s-s, yeah.

**Steve:** Okay. Oh, you're right. I wrote "Josh," that's why I'm reading it, but it's Joss. He's done good things. My tech support guy, Greg, was a big fan of "Buffy the Vampire Slayer." And I used to tease him about it endlessly. I'd go, Buffy? Really?

**Leo:** I have to go back and watch it because people loved that show.

**Steve:** Well, and apparently it was the writing. He kept saying it's the writing.

**Leo:** The writing. Joss Whedon, again.

**Steve:** The writing is so good. And then "Angel" was spun off from "Buffy." And Joss did

those things, too. So anyway, I have hopes.

**Leo:** I like the idea of dolls that can be programmed with your...

**Steve:** Oh, I love it. And I saw, in this preview, it's wonderful looking. It's like, okay, we're good. I hope 9:00 o'clock is a late enough timeslot for this because looks like it could be way good. And during the Super Bowl I picked up, I saw, it was toward the beginning of the game was a new Star Trek trailer that's got me, you know, panting yet again. The good news is we don't have to wait forever. The new Star Trek movie comes out on May 8th. And the existing trailer that everyone has seen, I hope has seen, has the young Jim Kirk at maybe, I don't know, age 12, driving that classic red - is it a Corvette, I think? Have you seen that trailer?

**Leo:** No, I haven't seen it yet.

**Steve:** Oh, I can't give it away, then.

**Leo:** I know it's there. Well, yeah, we have to be careful because not everybody's seen it. But it's Jim and Spock back at Starfleet Academy; right?

**Steve:** Well, I mean, that is the - this is when they meet. This is when Kirk and Spock first meet. And apparently Kirk grabs some people and commandeers a ship and runs off with it or does something...

**Leo:** Oh, he was always bad, wasn't he.

**Steve:** He was always, yes, he was always different.

**Leo:** Always a rebel.

**Steve:** And so, okay, so that's May 8th. On the 22nd of May is the fourth "Terminator" movie. So we get the fourth installment of a feature-length "Terminator" movie, "Terminator Salvation," that of course I'll be there for. And finally what's interesting is that that was the weekend that another much-anticipated major sci-fi movie was going to be released, but it got bumped back to Christmas. In fact, that same week that his other major movie, little something called "Titanic," was released. And this is James Cameron's "Avatar," that he's been wanting to do and working on for 12 years.

**Leo:** Holy cow.

**Steve:** This is his major return to the big screen. The plot is something like a wounded veteran goes to some planet where there's an indigenous people and somehow combines or merges or does something. A bunch of this is computer generated. So it's a hybrid of

live actors and computer-generated characters. And we have Sigourney Weaver, one of Cameron's great friends, is going to be in. They were going to - for a while they were going to call her Shipley in "Avatar."

**Leo:** Oh, that's her name in "Aliens"; right?

**Steve:** Well, no, Ripley, of course, famously.

**Leo:** Ripley, that's right, yeah, yeah.

**Steve:** So but clearly making it similar as a little play on that. But they ended up changing her name to something else. So, and it's some sort of 3D technology. One of the benefits for Cameron is that, by moving it back from May until December, that will allow more theaters the opportunity to install 3D screens, whatever that means. I've not looked into what this 3D technology...

**Leo:** Yeah, I'm not crazy about those 3D things, but...

**Steve:** Yeah, I'm not, either. I'd rather not bother with it. But, you know, what the hell. And that's all of my random news.

**Leo:** That's the sci-fi news of the week.

**Steve:** The sci-fi update, yeah. I did have a very short little fun quip about SpinRite. John Salter wrote - I ran across his note when I was going through the mail bag. He said, "Hi, Steve." Oh, interrupted by Fred. Coincidentally, he's just sold a copy of SpinRite, and I'm reading a SpinRite story. "Hi, Steve. I was making a video for Yubico on using the YubiKey for TrueCrypt whole-disk encryption using a YubiKey preprogrammed for generating a static 44-character password. While TrueCrypt was encrypting the disk for this video, it started complaining when it reached a bad sector. Of course I just deferred the encryption." He says, "TrueCrypt has really thought of everything. Rebooted from my SpinRite CD and let SpinRite do its stuff. Sure enough, a bad sector was found, and DynaStat kicked in. I rebooted, and TrueCrypt came back and offered to complete the decryption from where it was interrupted. Which it completed successfully. Very cool." He says, "When I finish the video, I'll send you a link."

**Leo:** Wow.

**Steve:** So, and I remember when I was myself vetting TrueCrypt, I mentioned some time ago, some versions ago that I was really wanting to put TrueCrypt through its paces. So I used some tools that I have, some proprietary hard disk technology that I developed for SpinRite, to deliberately damage sectors, making them unreadable on the drive, which I'm able to do, which is part of what I do for testing SpinRite. And sure enough, TrueCrypt ran across, stopped cold, refused to go any further. Then I fixed the sector with SpinRite, and I basically deliberately did what John inadvertently did, which

was he actually had a bad sector on a disk. And TrueCrypt can't go past it. But running SpinRite on the disk fixes it, of course, and then TrueCrypt is able to proceed.

**Leo:** Well, there you go. Pretty cool. Thank you, SpinRite, once again. Steve, you ready for some great questions from our great audience?

**Steve:** No.

**Leo:** Okay, well, then, thanks for joining us, and we'll - no, I'm...

**Steve:** I'm actually not. I forgot one. I forgot...

**Leo:** You forgot something?

**Steve:** I forgot something that I wanted to bring to our listeners' attention because I am just so excited about it. This is dumb. But strange things get me excited. You know?

**Leo:** We learned that.

**Steve:** You know how I love my window borders to snap to the edge of the screen and to each other. I mean, that little allSnap utility, a-l-l-S-n-a-p, that I've talked about a couple times, I just, when I'm using a machine that doesn't have it, I'm thinking, okay, what's wrong with this? Something's broken. Well, I was - I've been allowing myself to spend a couple hours every morning working on the - laying out the protocol for CryptoLink, even though I can't really start working on CryptoLink full-time because I've got to get the DNS thing finished and the cookie thing finished, and I'm going to get those things done first. I've just, when I was working on the SSL protocol stuff for Security Now!, I kind of got myself all wrapped up again in security protocols. And I thought, okay, I just have to spend some time getting this stuff down on - getting it down. To do that I wanted to use an outliner that I had not used for years called ECCO, which was purchased by NetManage for a long time. Many people still consider it the ultimate PIM of all time. The problem is it's old, and...

**Leo:** You still use ECCO?

**Steve:** Well, I've gone back to it. I've been using it now for the last week, just as an outliner. It does all this other kind of stuff. In fact...

**Leo:** Oh, yeah. Oh, it's the most complicated PIM ever.

**Steve:** I was going to say, I don't even understand how it works. I never really did.

**Leo:** I tried it. I love it. But it's one of those things, it's a lifestyle. It's not a program.

**Steve:** Yeah. Anyway, but what happened was, ECCO doesn't know about the mouse wheel. And I didn't realize until running across ECCO how much I take the mouse wheel for granted.

**Leo:** Yes.

**Steve:** It is a wonderful thing to be able to scroll like a web page just, I mean, it's - the mouse wheel is as correct as you can get a UI. The definition if a good user interface is one that disappears, one that you can use without thinking about it. And when you have something that isn't mouse wheel aware, it's annoying. And so, for example, I deliberately build mouse wheel support into all the apps that I write now...

**Leo:** Oh, that's neat.

**Steve:** ...just to make sure that, if you're on a - I'll embed a little rich text format, an RTF control, in my app for, like, help or information or whatever. And it's just nice to be able to scroll it with a mouse wheel. And of course what that saves you is needing to go over to the scroll bar and find it and then drag it. I mean, it's just a win.

Okay. So after five days of frustration, I thought, I'm going to go - there's got to be somebody who's, like, maybe has made a better mouse wheel. Sure enough, this thing is free. I cannot recommend it highly enough. Windows, of course, only, unfortunately. Sorry, Leo. It's called KatMouse, K-a-t-M-o-u-s-e. Just put it into Google, "KatMouse," and you'll find it. It is very tiny. It's free. It does exactly what you want and even more than I was hoping for. It mouse wheel-enables everything that scrolls. And you're able to even - you don't even have to give the thing you're scrolling focus. In Windows, one control or another always has so-called "focus." You know, when buttons have focus, they're highlighted. Normally, like when scrolling areas have focus, you can't see them. You can't see that it has focus. So you'll - and this is something that even people who use the mouse wheel are experiencing all the time. You've got to click on the thing first, and then the mouse wheel will work on it because, until you click on it, it doesn't have focus.

This little KatMouse knows what you're hovering over and scrolls that, even if it's not on top. So you could have - in fact, I'm looking right now. I have the PDF of our Q&A is underneath the notes that I had. And so I'm able to simply move the mouse over either of these two windows. And when I scroll it, the proper pane scrolls. Anyway, I love it. I mean, I'm addicted to this thing. It's so nice to be able to scroll whatever the mouse is over. So I just wanted to let our listeners know, if they're similarly mouse wheel people as I am, that this little KatMouse, it really makes the mouse wheel much better under Windows.

**Leo:** Very cool. I'll have to give it a shot. That looks really cool.

**Steve:** It's perfect.

**Leo:** Yeah. I'll see if it works with Windows 7. I'm pretty much Windows 7 everywhere now.

**Steve:** And Leo, that's just a miracle.

**Leo:** Well, no, I still use Macs. I just say when I use Windows I'm using Windows 7. It is a miracle. It's the most, you know, in some ways it's Mac-like. It's very clean and simple, and you will like it. You will be glad. In 12 years when you move to it.

**Steve:** That's right, when I get ready...

**Leo:** You will be very happy. All right.

**Steve:** It's funny because I have heard you talking about it, like with Paul, often. And I just - I sort of smile because when you're talking about, like, oh, no driver problems and all this, it's really clear, and I'm sure it is to you, too, that it's just Vista.

**Leo:** It's Vista. That's why there's no new driver model.

**Steve:** Right.

**Leo:** But I'm not praising it for its lack of driver issues, I'm praising it for cleaning up the UI, primarily.

**Steve:** Yes. I think they clearly did that. On their web page they talk about how they listened to us. And I think it's interesting, too, that they changed the name. It reminds me of when OLE, that was just stillborn at Microsoft, you know, the Object Linking and Embedding technology, OLE, so-called OLE...

**Leo:** Right, right, which became DOM, and which became...

**Steve:** Well, they couldn't get it off the ground. It was - it initially was - it was so confusing and strange that programmers disliked it. And nothing Microsoft could do could change that. And then Microsoft applied, as they often do, marketing. When technology fails, fall back to marketing. And so some guy at Microsoft said, hey, you know, we've got this new thing. And the other person said, well, what? And they said, it's called ActiveX.

**Leo:** [Laughing]

**Steve:** And the other guy [gasping]. ooh, ActiveX, I love that. What is it? And he said, OLE.

**Leo:** OLE.

**Steve:** And the other guy, well, really? But it sounds so much better. And the marketing guy says, I know. And so people will love it, even though it's the same old dried fruit we had before. Still...

**Leo:** That's Microsoft right there.

**Steve:** So now we have Windows 7. Basically it's Vista with less noise.

**Leo:** Right. Right.

**Steve:** But I'm really glad you like it. That's good news.

**Leo:** And it has some window-snap features. You'll probably like them.

**Steve:** Ooh.

**Leo:** Yeah. You just stay tuned.

**Steve:** Okay.

**Leo:** All right. Now it's time for our questions. We're going to begin with Iain Alexander from Nottingham, England - always a great place. We get lots of letters, it seems, from Nottingham, I'm not sure why - wrote to Leo, and it says Paul.

**Steve:** Yeah, Paul Thurrott. You forwarded his note.

**Leo:** I did forward this to you, that's right, okay.

**Steve:** Yup. And so I figured, oh, we ought to talk about it.

**Leo:** I thought you might want to know and share with your listeners - we were talking about the Microsoft Malicious Software Removal Tool, the MSRT. He says you can run the MSRT utility on demand in Windows 7, but it ain't called MSRT or even

MRT. You have to, to manually start it in Windows, you have to type kb890830 in the Start Menu Search box. You'll see the results, hit return, and there's MSRT. Knowledge base 890830.

**Steve:** Yeah. Now, okay, this was - I thought, well, okay. You forwarded this to me and to Paul. I thought we ought to discuss it because essentially you're not putting it into the Run box because that's not the name of a program. You're putting it into the...

**Leo:** You're searching for the name, which is longer, yeah.

**Steve:** Exactly. And so windows-kb890830-v2.5.exe is, you know, is the full name. So it's just sort of a quick way to get it. And of course the danger is that I don't know how static that name is, whether they're changing that every month. The fact that it says v2.5 leads me to believe that they're evolving that particular entry.

**Leo:** Right.

**Steve:** So for Windows 7 people, you can run MSRT also. And the way you do it for now is with this kb890830. Just, you know, a little FYI there. Write that down on the back of your hand.

**Leo:** Yeah. Memorize that, then destroy it. Speaking of MSRT, Corby in Reno, Nevada shares his findings. He says: Steve, I'd almost written to you about a very similar finding that you had with MRT and the Eudora attachments. Like you, I ran the full version of the Microsoft Malicious Software Removal Tool, and it detected some viruses in some very old Eudora attachments that were on my computer. However, MRT was not able to clean them, so I ran the corporate edition of Symantec AV against the same files. SAV said the files were clean. I removed SAV and installed eEye's Blink, scanned the same files. It reported the files were clean. Since these attachments were very old, and they had a file extension I wasn't familiar with, I ended up just deleting them. Also I traded Eudora for Gmail several years ago. I'm pretty sure I didn't need those files. I just thought you might be interested to know that two different AV programs said the files were clean, but Microsoft said they were infected. My guess is MRT was showing a false positive, but I don't know for sure. That happens a lot with viruses, doesn't it.

**Steve:** Well, it certainly can. The problem of course is that, as viruses have become trickier, the scanners have had to become increasingly heuristic. So they're not just matching a rigidly known pattern. They're having to essentially introduce some grey area and say, oh, this - well, they're just saying, oh, this looks like a virus. I got myself off the track here. Because, for example, it happens to GRC's freeware from time to time.

**Leo:** Right.

**Steve:** Some version of AV will suddenly decide that my DCOMbobulator is evil, and we

get a bunch of email from people saying, oh, your DCOMbobulator I downloaded directly from your website, my AV program says it's malicious. And it's like, okay, wait till they update again, and they'll fix it because - and in the meantime please tell them that they're giving a false positive. So that does happen. And so I wanted to share this with our listeners in case other people have this experience. My experience is somewhat different. I do think that, given what I saw, that this thing had found evil stuff in my Eudora attachments folder. But it certainly is the case that false positives occur.

**Leo:** And so what we're saying is we don't know who's false positive. We don't know if it was Microsoft making a mistake, or the other antiviruses not detecting it.

**Steve:** Or if they keep missing it.

**Leo:** Right, both of which happen. False positives and false negatives.

**Steve:** It's also possible that those AV tools at some point, when something gets really old and there's no more incident of it, they may well be removing detection just for the sake of keeping their own pattern updates a modest size. Whereas Microsoft might choose to just let theirs continue. I did look at the MRT.exe, oh, I think as a result of the question we're about to get to. And it's more than 20MB in size.

**Leo:** Wow

**Steve:** It's a monster.

**Leo:** See, you couldn't do that in the old days. I mean, you couldn't silently, without warning, deliver a 20MB file and say, here run this.

**Steve:** Only Microsoft.

**Leo:** I mean, it just shows you how much, I mean, broadband has just changed a lot.

**Steve:** It really has.

**Leo:** Mike Siwinski in Rochester, New York encountered an old copy of Microsoft Malicious Software Removal Tool: Steve, listening to SN-180, thanks a lot. You gave a tip for launching MRT using Start->Run->MRT. The reason this works is that Windows finds MRT in the System32 folder. Note: The copy of MRT on the hard drive is an old copy. This trick does not find the latest copy of MRT and download it. I just tried this, and it launched the December 2008 copy of MRT. I went to Windows Update, and the January '09 MRT was there. If someone's having trouble with an infection, running last month's MRT probably won't help them. Thanks for all the

good work on Security Now!. So then how do you run the Malicious Software Removal Tool?

**Steve:** Well, and this brought up an interesting point because it made me think, oh, what's going on here? And I would recommend our users do this, our listeners do this, too. It's fun to just search your C drive for MRT. That is, anything with MRT in it. You'll find - I found - a bunch of fonts that had MRT embedded in their name. I also found something I didn't know was there, which was interesting, is an MRT.log. And that's very cool. It's under the - in my case it was under the Windows debug directory. And it is a log that the MRT appends to every time it's run. And in this log was an entry for every single month. Actually there were a few earlier months skipped a year or two ago. But then Microsoft got rigorous about publishing a new one every month and running it every month. And so this log shows you every single time that it's been run silently in the background. I mean, and also when you run it manually. But so there's a whole log of it running on my system for quite - for several years, even though I had no idea it was doing that. And the time that I ran it manually, when it found all this stuff, there's a log of everything it found. So the log is also very cool.

But there was just one copy on my system, MRT.exe in the Windows System32 folder. When I ran it, in the title bar it told me that it was the January '09 MRT. So I think what happened in Mike's case is, for whatever reason, his Windows Update did not download, or he doesn't have it configured, but one way or another it's not running the current MRT. So what I wanted to - the point I wanted to raise to our listeners is just put MRT in the Run dialogue under your Start Menu. It'll take a few seconds, because it's 20MB, to load. And that was funny, too, because when I ran it I was thinking, okay, did I type that right? Why is it taking so long to come up? Well, it's a 20MB executable. Takes a while to suck that in off the drive.

**Leo:** And I'd be glad to know that they're not storing 20 different copies of this 20MB executable on the drive.

**Steve:** Exactly. But the point is that it's instantly visible in the menu bar. When you run MRT.exe, it'll tell you what month you've got. And it's worth just doing a double check. Mike sort of did it inadvertently. But I had this month's, the most recent MRT. I imagine a week from now, when we pass over another Patch Tuesday, I'll have February. But I'm going to check. I'm going to just put MRT in after we're talking about it next week and say, okay, yeah, now mine says February '09 rather than January '09, as it does now. If by any chance you don't have the current one, there's probably a reason. Well, there obviously is a reason. But you may want to figure out what that is because it means you're not being updated as you probably want to be.

**Leo:** So what he found was not the January edition, but just a stub or something.

**Steve:** No.

**Leo:** It was there, but it wasn't getting installed.

**Steve:** Yes. He found December '08's copy, which is the only one on his system. And he should have had January's. But he didn't. So...

**Leo:** I'll have to run it on my systems and now check.

**Steve:** Yeah, just...

**Leo:** It'll say. It says in the title bar. You just...

**Steve:** Yup, bang, comes right up. Well, it doesn't come right up. It takes a while to load itself.

**Leo:** Now, we're going to get a new one in a week, so this Tuesday. So, okay.

**Steve:** Exactly. Exactly.

**Leo:** Probably a good idea at the beginning of every month to check that.

**Steve:** It's a neat tip. I like that.

**Leo:** Very good. Moving on to our next question...

**Steve:** Because otherwise you don't know. It's running in the background silently. The log does tell you, so you could check the log. But this is a simple, easy way to know, hey, look, I got a new copy, and presumably it ran. And in fact you could check the log to see if it did.

**Leo:** Derek Robson, UNIX geek, takes issue...

**Steve:** That's what he called himself.

**Leo:** UNIX geek - with YubiKey as a second factor. He says: Steve, for a second week you've spoken of using a YubiKey in static password mode and got it wrong. You talk about having a password and then adding a YubiKey password to it, making a very long password. This is good. I have no problem with the idea. But then you say it's two-factor authentication, something you have and something you know. The problem is, YubiKey in static mode really isn't something you have. It's something you're too lazy to remember. It's no more like something you have than writing your password maybe on a Post-it note. Since it would be very possible to remember a static password if you try, it really isn't a second factor. You don't need to have it. You could have it memorized. And what's more to the point, a keystroke logger will

remember the static password quite well. It doesn't need the YubiKey. Therefore the something you have aspect is valid only when a YubiKey is used in its one-time password mode. As soon as you remove the one-time function, you lose that something you have function. It's just a second password. I know you know this, but got mixed up with the wording. But let's put it right. Love the show, says Derek.

**Steve:** Well, I thought that was interesting. I mean, he's right that it's not something you have to have. It's something you want to have because it's typing out 64 characters in the 256-bit mode, 64 characters of gibberish, I mean, that you probably couldn't even type in correctly. I have enough trouble typing in the Windows product code correctly, let alone 16 characters of really gibberish stuff. So, yeah...

**Leo:** I mean, technically, if it's static, it's no different than having - it's just remembering something for you.

**Steve:** Right. And so I guess it's sort of a question of, a little bit of a question of definitions because he's right that it is static, so the vulnerability is that a keystroke logger could log it and remember it, so you don't have the strength of it being a one-time password. So it's not something you have that's a one-time password that uses the one-timeness to be provably something you have. But due to its nature, it's something that you want to have. So it's like, okay, maybe it's not two-factor. But maybe it's one and a half factors. I'm joking. Maybe it's one and three quarters. It's something you're really glad you have because, if you didn't, then you'd have to type this thing in by hand. So I agree with him pedantically. It's not the same as something that you have no alternative but to have because it's going to generate a one-time password, and you won't know it until it does, and it'll never do it again, so you're thwarting keystroke loggers. So yes, I agree that it's not the same as two-factor authentication where it's two different things that you know.

**Leo:** Right. You'd agree, if I wrote the password down and pasted it on a Post-it note to my screen, that doesn't - a second password doesn't make it two-factor.

**Steve:** Correct. One really good factor.

**Leo:** Well, I use - and actually this is to the point. I use a program that generates a password, a hashed password based on mixing a password I know with the top-level domain name of the site I'm on, and then generates a unique password for that site. But that's not two-factor authentication. Even though it's using two things, it's not two-factor. It's something I know.

**Steve:** Correct.

**Leo:** Paul in Portland, Oregon says, "Secure email can be easy." Hi, Steve. In response to Wes's question in the Q&A episode we did last time about secure email, I've been wondering the same thing myself, which is how do I send an encrypted

email to someone without forcing them to do the whole key dance thing. I'd like the ability to send the occasional encrypted email should I need to send my Social Security number or other sensitive information to someone.

Well, I recently discovered Comodo has a new free product called SecureEmail. The idea is only the sender configures their email client using free certificates provided by Comodo to send encrypted email. If the receiver is not set up for decryption, they're given a one-time session certificate and the option to decrypt it using a web reader service. I'd really like your thoughts on this product. It's http://secure-email.comodo.com/features.html. Thanks, love the show. Oh, this is interesting. But, see, on the face of it, I don't understand how it would work. How would it guarantee that the person asking for decryption is the person you sent it to?

**Steve:** Yeah. And first of all, I went to that link, and there's a Comodo page with a whole bunch of bullet points and all kinds of features and stuff. And I immediately, my eyes went out of focus. It was like, okay, wait a minute. I thought that we wanted to make this easy. So this is certificates on the sending end, and then you send the receiver a certificate. But if they're not set up, then you give the - you get a one-time certificate from Comodo, and then you go to Comodo's website, and you have their server do the decryption for you. So now you're trusting them not to care about what's being decrypted. You've lost...

**Leo:** Oh, that's true, you're giving them the information.

**Steve:** You've lost the TNO, my favorite acronym, Trust No One, because now you're trusting them. And it's like, okay, wait a minute. There was a little, cute, perfect little decryption program that I've talked about before called AxCrypt, A-x-C-r-y-p-t. It's open source. It's free. It's a perfect little - it uses AES long key encryption. The guy is into encryption. It's simple to use. And in fact there's an AxDecrypt which you don't even have to install. So I would say, for somebody who just wants to occasionally send something encrypted, you just encrypt the file and email it and a little AxDecrypt program to a friend, or tell your friend to download AxDecrypt, which is also free. And then what you have to have is some sort of an out-of-band conversation, that is to say, you want to get the secret passphrase to your friend, maybe over the phone, somehow secure. And then it's just an easy matter to encrypt a file, email that, and then your friend uses AxDecrypt to decrypt it using the password. So to me, I call that easy. And that makes sense for someone who only occasionally needs to send something encrypted. And of course you can store files encrypted. You can use AxCrypt for all kinds of purposes like that.

**Leo:** I do wish everybody would just install OpenPGP or GNU Privacy Guard and would just...

**Steve:** Yeah. They will after I start using Windows 7.

**Leo:** I love it. I use GNU Privacy Guard. I install it on every machine. I use a plug-in for Apple Mail. I use Enigmail on Thunderbird.

**Steve:** Boy, are you secure.

**Leo:** Well, it's not, you know, I actually don't encrypt very often. If there is somebody...

**Steve:** [Indiscernible] signatures.

**Leo:** I use it for signatures because people impersonate me. So if you get an email from me that is not signed, then it's not me. And if it's signed, and you're running one of these programs, and GNU Privacy Guard is free, you can verify that it's me. And then I upload my key to the key servers and hope that people who know it's me sign it. And I change - I just changed the key. I've changed the key at the beginning of the year every year. They expire. I learned that because I had about 15 unexpired older keys on the key servers. They're still there. Use the most recent key if you're going to do that. And then if somebody wants to send me encrypted email, they can go to Leoville.com or go to the key server, download my public key, and send me encrypted email.

**Steve:** Yup.

**Leo:** And once we've had an encrypted dialogue, all of our conversations are encrypted automatically from then on. I think it's a very simple system. There are some programs, I play with a program in Windows that I really like called The Bat!. It's a kind of high-end email program. It's from Russia. I don't know if I should trust it. But I love it.

**Steve:** I looked at it a long time ago. I think maybe it was when Eudora was [indiscernible].

**Leo:** It's Eudora-like, yeah, it's very powerful. 35 bucks. But it has built in, and I love - this is one of the reasons I really recommend it, is it has built-in OpenPGP or S/MIME certificate encryption. You choose which you want. It'll generate a certificate for you. That's pretty easy.

**Steve:** Nice.

**Leo:** If Outlook would do that - for instance, why doesn't Microsoft build in certificate, you know, just self-signed certificates, at least?

**Steve:** Right.

**Leo:** Just build that in. If it's built in, then everybody can use it, and it's transparent. All right, I'm sorry. I'm going to get off my high horse.

**Steve:** No, I mean, I think in an environment where high value content is being shared, for example, all the attorneys in a law firm should have their own certificates.

**Leo:** Oh, yeah.

**Steve:** And on their laptops so when they're mailing client confidential contracts and things around, they're just automatically encrypted, like within the firm. And then maybe even set up some of their more important clients the same way. Say look, if we're going to be sharing email, we need to do this in a safe way.

**Leo:** I would really appreciate that. Instead of those silly signatures that say, if you got this by accident, don't read it. Yeah, that'll work. That'll work. Dick - I'm sorry, yeah, Dick Victor in Milwaukee, Wisconsin has some Yubico and YubiKey news. I think this YubiKey thing is the single most popular thing you've ever done, I'm starting to think.

**Steve:** Well, believe me, as I'm - the way I choose questions is I sort of scan through the subjects. And people are just super excited about the YubiKey.

**Leo:** I know you and many listeners are YubiKey fans. So I thought you might be interested to know that Yubico is planning a small change in the firmware of the YubiKey in the next firmware version, so that it can be used - oh, I'm loving this - in static password mode for preboot password entry for a TrueCrypt-encrypted system partition. The present firmware does not provide for the YubiKey to get recognized preboot. And he's got a link in here in the Yubico forums.

http://forum.yubico.com/viewtopic.php?f=2&t=221&p=880&hilit=truecrypt#p880

Seems there's a lot of interest in the static mode, probably because it's something we can use even before there's widespread adoption of YubiKey in its more secure OTP mode, and also because it works offline when there's no authentication server available. And 64 characters of total gibberish with 256 bits of entropy ain't bad, even if they're using that limited mod-hex alphabet. Good point.

**Steve:** Okay. So here's the story. I've had a dialogue with Yubico because I wanted to understand what this change was. And I have some interesting news for our listeners relative to getting their keys updated, which Yubico will do for free, for anyone who really needs it done. They'd rather not have everyone who they ever sold a key to send it back if it's not necessary. But they can do it for some people. The way people have been using their TrueCrypt, I'm sorry, their YubiKeys with TrueCrypt has been post-boot, when TrueCrypt is running, and they'll use the key rather than entering the password into TrueCrypt in Windows to put a partition online or unlock a directory or whatever they're using TrueCrypt for. The reason it has not been possible to do it for preboot is there's a bit in the configuration header of USB devices which specifies whether the device is a boot device or not. That is, does it have any semantic meaning in a boot environment. And that's why people may wonder, like, why some USB drives can be recognized by the BIOS, where others won't be. It was because back in the beginning of USB drives no one was really thinking of them in terms of boot devices for BIOSes. So even some drives don't have that bit set, which means the BIOS which looks at the - a USB boot-enabled

BIOS, a modern BIOS that looks at USB devices will see that this bit is not set, will ignore it. And it's not until Windows or whatever OS you're using is running that that bit is no longer important. So what the Yubico folks have done is in v1.3.3, this firmware update, they are now deliberately setting this bit. I had a dialogue in email with Stina's husband Jakob, who was the engineer on this.

**Leo:** Ha ha. You sold two in the show.

**Steve:** Thank you, Fred. And he explained that he deliberately left that bit clear because he thought, who would want to use the YubiKey before the OS is booted? Because after all, it was at that time only a one-time password device. So you'd have to have networking running in order to contact a remote server in order to do anything with it. Then this static password mode of the YubiKey has become so popular that now there's a non-communications, non-networking application. So v1.3.3 of the firmware has the YubiKey as a boot device, which means it will be seen as a keyboard by a BIOS, and you can use it, when properly configured for static key mode, as your boot-time log-in, boot-time password for TrueCrypt. Which is very cool. And they have said that anyone who wants to do that can send their key back to them, and they will update its firmware and return it for free.

**Leo:** So they don't have a way to do that online without sending it back to them.

**Steve:** Precisely. I'm sure there's, like, something they've got to do where - and I don't know for sure that they're not going to exchange it for a new key.

**Leo:** They may just put a new key, yeah.

**Steve:** They may do that, or they may update the firmware. I don't know whether they're able to write new firmware into the existing key. But it is the case that, if you send them a key that won't work, they will one way or another send you one back that will. And you can send it either to the U.S. or their main offices, and they'll take care of that for you.

**Leo:** Excellent.

**Steve:** So it's very neat.

**Leo:** Excellent. I'm really - the YubiKey is so cool. Although I hate to use it in static key mode. I guess I could get another one. But I just love the idea of having new keys all the time, you know.

**Steve:** That's very cool. I think you're right, the solution is to have two keys. One, for example, that you use for your WiFi WPA password, or you use it to preboot TrueCrypt in order to have TrueCrypt do on-the-fly decryption of your whole drive. And then you've got the other one, which is used for, like, online purposes, where it does make sense. So

you really need two.

**Leo:** Maybe three. The more, the merrier.

**Steve:** Really would be cool if they could have a dual-function single YubiKey that works both ways.

**Leo:** Oh, yeah. Poojan Wagh in Chicago, Illinois suggests a cheaper solution than YubiKey. Another way to do it. Hi, Steve. It pains me to discourage your listeners from buying the YubiKey, since it's a very good technology that is already inexpensive, is only going to get less expensive the more that people use it. However, I wanted to point out a much cheaper alternative to YubiKey for some applications. In Episode 180 you discussed the use of YubiKey's static password. Leo commented he'd like to use that static password as the master password for a password utility. You don't need YubiKey to do this. I use a password utility called KeePass. That's a really good one. That's the open source one. It allows you to use keyfiles in addition to an optional password. Oh. Of course. As a result, I save a keyfile on a USB stick and have it automatically search for keyfiles on removable media. As a result, I get two-factor authentication....

**Steve:** Oh, well, maybe not.

**Leo:** One and a half.

**Steve:** One and three quarter factor.

**Leo:** ...a keyfile on a USB key, and a manual password entry. I've noticed that TrueCrypt also has a similar keyfile capability, with the ability to designate a default keyfile on an external USB stick. I haven't tried it, but I doubt that a keyfile could be used with preboot authentication. These days USB keys could be had for a few dollars. You don't need more than a few kilobytes of space for a good keyfile. Great point. What's even cooler, I store my keyfile on a very small SDHC. That's, of course, the high-capacity - what does the SD stand for? I can't even remember. Smart Digital?

**Steve:** Secure Digital.

**Leo:** Secure Digital, that's right. Secure Digital High Capacity camera storage card that slips into my wallet very easily. Many computers nowadays come with built-in SDHC readers. However, I happen to have one that folds into a USB connector. Very slick. To make things clear, I think YubiKey is still a very good solution for things like preboot authentication. And its one-time password feature is awesome. But not the only way to do it. I should have mentioned that. Of course KeePass will do that.

**Steve:** Well, and we've never really - we've brushed on the idea of a keyfile, but we've

never really talked about it in depth or in detail. And it's certainly an interesting solution. I guess I'm less rah-rah about it because it's always felt to me a little bit like it's security through obscurity, the idea being that the encryption system knows where to find key material in a file. The file's not changing. It's static. It's true that if you make it a removable file, then somebody's completely out of luck without that. And I guess the thing it brings you is absolute proof against a weak password. You would certainly, I think, would always still want to use a passphrase of some kind in addition to the keyfile, obviously to prevent somebody from using that by plugging his HDSC into a laptop, and if that was the only thing that it needed, then it would be able to access his files without him at all. So it's, again, it's certainly stronger than nothing. But a really good passphrase that is sufficiently long is going to provide you with the same security.

It's worth noting that the contents of the keyfile is going to always end up being hashed down to the length of the encryption key, whether it's 128 bits or 256 bits. But as we've seen, only 64 characters, and that's 64 limited characters, is 256 bits. So, and so what, 32 characters of a 16-character alphabet, that's 128 bits, if that is the key length that you're using for decryption. So the notion that you're getting more security from some multi-K file is really not the case. You only need a relatively short phrase in order to get as much security as is available. Anything longer ends up being hashed down.

Now, again, it is true that a bad passphrase that isn't really random gibberish will be inherently, have inherently less entropy than some file. And a big file, by virtue of its size, will end up approaching the maximum entropy that you can get out of 256 bits, or whatever the file is hashed down into. But it's not the case that, like, a big file ends up having, like, that big a key. You end up, there's diminishing returns as the file size increases. So, yes, it is, as we've seen earlier in this episode, it's not a true, full, second factor because it's static, and in that sense it's like a YubiKey running statically. But I would argue, I mean, I would agree that a keyfile is better than not having one, unless you have a really good static passphrase. And, for example, a YubiKey running with the full 64-character static password is going to be good. Oh, and one other benefit of the keyfile is, by not being input through the keyboard, whereas the YubiKey is, by not being input through the keyboard, you are immune to any kind of keylogger of any sort. So that's another benefit of it.

**Leo:** Oh, yeah. But no good for logging in at boot because nothing would know to check that.

**Steve:** Yes. And in fact, even if the SD card were recognized, we know that TrueCrypt's boot sector is probably - I'm sure it doesn't today recognize a keyfile. But it would have to then be modified and made substantially more sophisticated in order to be able to recognize a FAT file system on that SD card and do something proper with it. So it seems a little bit out of reach. But again, it's useful in that it's not - the data from the keyfile is not coming in through the keyboard. And combined with a passphrase, I think it's better security than a passphrase alone.

**Leo:** Jim in Westchester, Pennsylvania is not happy broadcasting his passwords all over the neighborhood. Hi, Steve. Forgive me if you've covered this previously on Security Now!. But what if, for reasons of circumstances, you're temporarily working from someone else's office location? You're not employed there. The only Internet access available is an open WiFi hotspot. No telephone line equals no modem. Huh? Oh, I see. You have to use their Internet. I get it. The owner of the premises tells

you that all the tenants and temps use it without problems or complaints, and it's darn fast.

By the way, that's how we - if you come here, you have - we don't give you access to our internal network. You get access to an open WiFi access point. Everybody else is using a wired system that's on a separate router. But that's - you would be in the same situation if you came here and started to use our WiFi.

So without making it too cumbersome, but some reasonable expense is okay, what would be a good way to reasonably protect one's computer in this situation, without the visiting guest - me - giving the owner and other tenants and temps any grief about running a open WiFi? Thanks, and great job on Security Now!. Regular listener Jim. Jim must have visited the TWiT Cottage. That's how we do it. But not for our business. Just for visitors.

**Steve:** I'm glad to know that. Not for your financial banking.

**Leo:** Nothing. We don't use the WiFi for anything. Any of our - it's all wired. But we have an open access point as a convenience for people who come to visit us.

**Steve:** Well, to answer...

**Leo:** Actually, it's not open. We give them a password. Never mind.

**Steve:** Oh, good.

**Leo:** Yeah, it's WPA2. Of course, what am I thinking?

**Steve:** Okay, yay. That's better.

**Leo:** Yeah.

**Steve:** Well, first of all, this is one of the main reasons that I've got CryptoLink in my future is it's for exactly this kind of application. If Jim had a machine running at home, then he could robustly, and with a high chance of succeeding, access his machine at home from anywhere he was on the planet, and then surf or use the Internet back out through his home connection, exactly as if he were at home, not needing to trust anything between where he is and home.

Now, there are other VPN solutions, but traditionally extremely difficult to configure. I mean, remember that I started doing an OpenVPN configuration guide. And, I mean, I use it. But you really need to have your propeller spinning pretty much 24/7. And, due to some quirks of it, you cannot guarantee a connection. For example, if you happen to be in a local network whose IP address range is the same as the network at the other end,

then routing doesn't work because OpenVPN is routing based. So there are all kinds of little gotchas that make it much less robust than, well, than I believe a VPN could be and should be. Which is why that's GRC's next product.

But there are some commercial VPN solutions. There are some free ones that make me a little nervous because you wonder what their economic model is. How and why are they free? But there's also one that we've talked about, and you and I have both used, Leo, called HotSpotVPN.

**Leo:** Yes.

**Steve:** And I jumped over to see what the pricing model was. Now, Jim said it didn't have to be free, but he wanted it to be reasonable. Well, HotSpotVPN 2, which is their SSL-based, and it's OpenVPN-based SSL, that's $10.88 per month. And you can buy it for one month, so it's a little less than $11.00. And I think in a temporary office mode where you're otherwise being forced to use open WiFi, it's a perfect solution. You download their little installer that basically installs OpenVPN, does all the configuration and sets things up. I mean, it's very easy to use and set up. And then you simply fire that up.

Because they're out on the Internet, you know that you're with a high likelihood able to access them. They use maybe port 80 and 443, both HTTP and HTTPS? It's been a while since I used them. Or maybe it was FTP and HTTP. Anyway, there were a number of ports that you were able to use to maximize your chance of being able to connect to them. And they make a lot of sense. They have a less expensive version, HotSpotVPN 1, which is traditional PPTP VPN. Now, that's the VPN technology that Windows has built in. So I like that from the standpoint of you not needing to install anything on your machine, even temporarily. And it's less expensive. That's $8.88 a month. And they even offer it in one, three, and seven-day packages for 3.88, 5.88, and 6.88. So 6.88 for a week, for example. But because it's PPTP, you're not quite so sure that you're going to be able to access. You could have an ISP that's blocking that traditional VPN port, or the local network could be blocking it, although in Jim's case, with an owner that's boneheaded enough to be running open WiFi for his whole company and employees and temporaries, I doubt that they're blocking anything.

So for as little as 8.88 a month, you could use the HotSpotVPN 1 version, which doesn't require that you install anything, and they help you get set up and configured in order to be able to use their VPN. That solution, of course, fails my TNO, my Trust No One goal, because you are trusting them. But they're a commercial outfit. You're trusting them because all of your traffic goes through them and then emerges unencrypted onto the internet at their location. So they're also someone where, if our U.S. government wanted to be snoopy, they would tend to be looking at traffic at those sorts of aggregation points because a lot of people who for some reason feel that they have something to hide, are going to be using this kind of a service. So I like the idea of staying a little bit further under the radar by using your own existing, for example, residential Internet connection for your own traffic. But that's not available yet. It will be as soon as I can get to it.

**Leo:** There's one out that a lot of people have been telling me about lately called Hotspot Shield.

**Steve:** Yup, that's the free one.

**Leo:** That's free. What do you think of that? Have you looked at that?

**Steve:** I haven't looked at it closely.

**Leo:** It's by a company called AnchorFree. Same idea as HotSpotVPN. HotspotShield.com. I like the idea of paying somebody because I figure they're going to have faster servers. They're going to be around.

**Steve:** Yes, I do, too. I mean, and 10.88 a month, I mean, that's $10.88 for one whole month of use. And you and I both use HotSpot, and they do have multiple locations and servers and really good performance.

**Leo:** Yeah. And I like SSL, I mean, that's really great. That makes it a lot - that makes it so easy. Moving right along, Dixon in San Francisco wonders about YubiKey and keystroke loggers. In Episode 180 of Security Now! you discussed knowing what tools are supposed to combat what threat. I know YubiKey's function is to prevent dictionary attacks. Can you clarify whether YubiKey has any meaning against keystroke loggers? In other words, do keyloggers work before the full OS is booted? If I use a YubiKey to log onto Windows and boot up, would a keylogger be able to see that? How about after the full OS loads? I notice that Windows Vista and 7 no longer require Ctrl-Alt-Del to get to the login screen. My understanding was that little requirement was supposed to thwart keyloggers. Is that true? Thank you. Would Ctrl-Alt-Del thwart keyloggers?

**Steve:** Well, actually yes. From the minute NT was created, and they were talking about how it had the S3 security certification stuff, which it never really had, by the way, because you cannot be on a network and get that certification. So the moment you put yourself on a network...

**Leo:** Oh, well, then, never mind.

**Steve:** ...the computer loses the ability to have S3 government certification for security. It's like, uh, sorry. You plugged this into something else, so we don't trust you anymore. Okay. So it is conceivable that you could have a boot virus keylogger that could co-reside with YubiKey. We know, for example, that Adobe's DRM is able to, thanks to - I'm sorry. The keylogger could co-reside with TrueCrypt. And we know that Adobe's DRM forced the TrueCrypt guys to reduce the size of their footprint down in Track 0 and create redundant copies so that, if Adobe's DRM stomped on one of them, you'd still be able to access your computer.

So it's conceivable that a keylogger could install itself in Track 0, co-reside with TrueCrypt, and get control before TrueCrypt, hook the BIOS keyboard interrupt, which is how it would read keystrokes, feed those to TrueCrypt. Maybe TrueCrypt wouldn't notice that. I don't know whether TrueCrypt checks for that happening, although it's possible that it could. On the other hand, if it did, the keylogger could also neuter that check in TrueCrypt before TrueCrypt gets running. So, I mean, it's theoretically possible for preboot authentication to log what you type when you're logging yourself in for whole

system decryption. I mean, I could write something that would do that, which means other people could, too. So it's not the case that you could - that it's absolutely impossible for a keystroke logger to watch you do preboot authentication. So that's a possibility.

It is the case that this whole login screen was deliberately designed by Microsoft to thwart any sort of keystroke logging. That Ctrl-Alt-Del changes sessions, it raises security, it's really supposed to, like, put you into a whole - there's a whole desktop technology. It moves you to a different desktop. And I don't know now in this day and age if that's been bypassed. I do know that Microsoft went to some lengths to make that Ctrl-Alt-Del and the password screen really mean something from a security standpoint. And so you do wonder if they've backed off on that, if they've managed to maintain the login security with the same strength as they had before. And I don't know one way or the other.

**Leo:** Okay.

**Steve:** So YubiKey and keyloggers, this is the problem with static keys. I mean, this has come up several times in this one hour, is that YubiKey is very convenient to use in a static key mode, but it doesn't really represent a full 'nother factor of authentication. And because it's the same, it is prone to being recorded. So, you know?

**Leo:** So there.

**Steve:** There.

**Leo:** Alex B, lurking somewhere in Minnesota, wants a reality check. He says: Hi, Steve and Leo. I'm guessing, hoping actually, that others have already alerted you to this. But if not, here goes. Oh, first things first. I love the podcast. It makes my commute so much more enjoyable. On page 77 of the January issue of PC World, a writer had a small article entitled "Stop Your Neighbors From Stealing Your Wi-Fi Bandwidth." Quoting from the last paragraph of the article: "You could just turn on your router's built-in WPA encryption, but that won't do you much good if your kids blab the family's WiFi password to everyone on the block. Instead, turn on MAC address filtering in your router's security settings. You'll have to spend a few minutes entering the MAC hardware addresses for all your devices. But after that you won't need to use any additional security at all." Oh, my god. "Only known" - I added the ohmygod. I don't think it was in the article. "Only known devices will be allowed to connect, so a password's not required."

Alex goes on: To say that I was stunned after reading this is an understatement. Who in the tech world really thinks it's okay to disable encryption for any reason, let alone in favor of MAC address filtering? MAC address spoofing, as we Security Now! listeners all know, is trivial. Not only that, but simply preventing someone from joining your network doesn't mean they can't sniff all your unencrypted packets floating around the neighborhood. What do you think? Thanks again, and keep up the good work. Wow.

**Steve:** Yeah. He was actually even more upset than that. He named the writer, and I

took the writer's name out of this because I didn't want to lambaste anyone. It's, well, everyone listening to this podcast knows that Alex is right, that MAC address filtering is no protection against somebody who maliciously wants to get onto your network because the MAC addresses are on the unencrypted front of all the packets traveling on your network, so they're easily copied and spoofed. You simply clone the MAC address, and then the router that's got MAC address filtering thinks it's you. We do know that MAC address filtering is convenient for preventing inadvertent use of the network. So it does, if for some reason you had to have your router open, that is, nonencrypted, then you could at least use MAC address filtering to prevent somebody, a neighbor, from mistakenly using your network because their MAC wouldn't match, and your router would not acknowledge their broadcast for access.

I would say a couple things. First of all, you should not have a WPA passphrase that is easily stated. That is, we've talked about using the YubiKey, for example, as a beautiful way of quickly entering your WPA key into visiting computers, rather than having to type something long and laborious in. So one solution is for the family's router to have a really nasty, gnarly passphrase which, you know, where you've got to have a piece of paper, and where it's written down and you type it in. So all you need to do is configure the younger member of the family's laptops once, not giving them the paper, but typing it in for them. That's not then something that they can give to their friends because there's no way that they're going to know it or memorize it.

The alternative is to use both. That is, because there's nothing to prevent you from using MAC address filtering and WPA encryption at the same time. That has the advantage, if you wanted to use a passphrase that was memorable, it has the advantage of being easily entered by somebody who wants to add a machine to the network or if a machine loses its password or becomes disconfigured. But then you'd still need to log into the router and manually add the machine's, the new machine's MAC address into the permitted list for communications. So I would say use both as opposed to either one in this situation. And it really is unfortunate that a writer in this day and age is saying, is recommending to turn off encryption and use MAC address filtering because obviously, as Alex points out, and as all listeners of this podcast know, those are not the same at all.

**Leo:** Yeah. Use WPA. It's all you need, and it works, and it's simple, and it just works.

**Steve:** Yup.

**Leo:** And I'm seeing another article on PC World where the guy says use SSID hiding. I wonder if they've got editors who know what the hell they're talking about. I mean, how is this stuff getting through? It's very frustrating to me because of course people read this, and then I have to explain it on the radio.

**Steve:** Right.

**Leo:** But they said so in PC World.

**Steve:** Yeah, who's right, Leo?

**Leo:** PC World's a magazine. They must know what they're talking about. Please. Geez, Louise. Okay. Now let's go to our PayPal questions here, starting with Brian in Raleigh, North Carolina, who has discovered that PayPal's security key is worthless when faced with social engineering.\: I recently lost my PayPal security key, but I needed to log onto my account. So I tried to log onto PayPal.com. I selected the "I don't have a key with me." Then I selected "I lost my key." The website said call customer service because my identity couldn't be verified. All right. Good so far. When I called customer service, though, I discovered all I needed was the last four digits of my credit card, and my name. Then they would deactivate the security key, even let me reset my password. This, of course, terrified me. With the information available on any restaurant credit card receipt - because that's what they put on there, isn't it, the four digits of your credit card.

**Steve:** Yes.

**Leo:** Or a little dumpster diving plus some basic social engineering to get the logon email address, you could have full access to anyone's PayPal account. Yikes.

**Steve:** Yeah.

**Leo:** This is a serious security flaw that shocks me. They should at least ask for the full credit card number, if not some security questions.

**Steve:** Or maybe the second group, the second to the last group of four. I mean, it's so common for everyone to show the last four digits in order to identify which card among multiple cards. So that means that that's now public knowledge. The idea of asking two public knowledge questions, the last four digits of your credit card and your name, I mean, and then, okay, fine, and that's the entire barrier for resetting the security on your PayPal account. That's just nuts.

**Leo:** Wow. I guess there's nothing we can do about it except to say, PayPal, fix it.

**Steve:** Oh, but wait. There's more.

**Leo:** Oh, wait, there's more. Robert in San Francisco with another PayPal screw-up. All right. Get this. I had two PayPal security keys, the footballs, one for home, one for office, and I lost one of the two keys. Now, PayPal has a page where you can report the key is lost. After reporting, it shows as lost. The other key shows as active. Then I received an email from PayPal stating that my key had been reported as lost, and it would no longer be required for login. So get this. When I went to log in again, it accepted the password alone and did not prompt me for my remaining, still active key. The non-lost key still shows up in my profile as active. Now what? So it just says, okay, fine, you don't need it anymore.

**Steve:** So you have multiple keys protecting your account. And you can use any one of

them to log in. You lose one of those keys and report it as lost. Now your account, even though you still have other keys, no longer requires them. No longer gives you the option of using them.

**Leo:** And you can't turn it back on?

**Steve:** How would you? They're already shown as active, but the system just doesn't need them. I mean, it's like, come on.

**Leo:** If there were only some other choice.

**Steve:** I know, like I said, there has never been a company that needs competition more desperately than PayPal.

**Leo:** Well, I'm of the opinion eBay is about to go under anyway, so maybe the whole thing will collapse, and we can go somewhere else.

**Steve:** You think so?

**Leo:** You and I totally rely on PayPal.

**Steve:** Yeah.

**Leo:** Well, I just think eBay is not doing well.

**Steve:** Are they really not?

**Leo:** Yeah, I think people have started to realize that it's just not a safe place to do business. And those lax practices...

**Steve:** [Indiscernible] me like just too many scams.

**Leo:** Yeah. And those lax practices are spreading to its subsidiary.

**Steve:** In fact, there were several times in the last couple weeks where I bought a couple things from a single eBay seller. And I said hey, you know, eBay seems to really misjudge shipping costs at the high end. It's like, wait a minute, this cannot cost $50 to ship this from Raleigh, North Carolina. So I said - I wrote to one guy in particular, I said, hey, you know, I bought these two things. Could you put them together, combine the shipping, and send me a request for payment that has them combined? And apparently

they used to do that, but there was some scam that purchasers were perpetrating where they would do that, and then say that - I guess tell eBay that...

**Leo:** They only got one of the two.

**Steve:** Yes, one of the two, and the cheaper of the two, and then get a credit for the other one or something. It's like, oh, goodness, okay, fine. So what are you going to do?

**Leo:** I just, you know, I don't know what to say. It's got to get better. It's got to get better.

**Steve:** It's a great concept. I mean, I love the idea.

**Leo:** I do, too. And if it weren't for all these scammers out there...

**Steve:** Yup.

**Leo:** But they're just out there. I guess we have to live with them. Watch out. Zombies are on the way, folks. Run.

**Steve:** Head for colder climates.

**Leo:** Head for colder...

**Steve:** [Indiscernible] warm climate.

**Leo:** Oh, zombies, do they not like colder climates?

**Steve:** I don't know. I didn't think zombies were really temperature sensitive.

**Leo:** I didn't think so either.

**Steve:** No.

**Leo:** They go where the brains are. Steve, it's great talking to you. Thank you so much for being here.

**Steve:** Always, my friend.

[Talking simultaneously]

**Leo:** Go ahead.

**Steve:** I'll remind our listeners one more time, KatMouse, K-a-t-M-o-u-s-e. It will change your life if you like the scroll wheel on your mouse and you're a Windows user. Oh, my god, it's just wonderful.

**Leo:** I'm putting it on all my Windows machines.

**Steve:** And believe me, I mean, you'll just, like, oh, it just - and not to have to click in the window first in order to get its attention. It's wherever the mouse is hovering, that gets scrolled. It's tremendous.

**Leo:** Steve's at GRC.com. That's his website. You can find 16KB versions of this show. You can find transcripts, show notes, all that information. We also have now very complete show notes, thanks to our listeners to the live stream on the wiki, at wiki.TWiT.tv. When you go to GRC, don't forget to get a copy of SpinRite. Everybody should have that. Everybody needs...

**Steve:** Yabba-dabba-do.

**Leo:** Yabba-dabba-do, SpinRite, the ultimate file, I'm sorry, disk maintenance and recovery utility. And of course lots of great free programs there, as well. GRC, Gibson Research Corporation, dotcom. Thank you, Steve.

**Steve:** Leo, talk to you next week.