SECURITY NOW!

Transcript of Episode #180

Listener Feedback Q&A #58

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-180.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-180-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 180 for January 22, 2009: Listener Feedback #58. 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!, the show where we talk about security, privacy, protecting yourself online and off, with Mr. Steve Gibson of GRC.com. Hi, Steve.

Steve Gibson: Yay. Hi, Leo. Great to be back with you, as always.

Leo: Have you still got the bunting up from yesterday, from the inaugural?

Steve: Yeah, I'm doing better now. This morning was rough. I was - I was a little hung over, actually. Probably for the same reason that Barack was; right? He had to go to 10 balls and wasn't due to finish until 3:00 in the morning. And then he had a 7:00 a.m. security briefing. So...

Leo: Amazing. I was watching him today on a press conference. We record this show, we should mention, the day before, on Wednesday.

Steve: Right.

Leo: I was watching him in a press conference today, and he seemed like he was awake. Joe Biden wasn't, was saying, what do we do? Didn't I swear them in? What do I do now? But, you know, it's kind of funny to watch, it's been a long time, I've forgotten, you know, these people, they don't know what they're doing. It's kind of funny to watch. Do I - now what do I do?

Steve: Right, right, right, because it's not all a routine for them, yeah.

Leo: No, yeah, not yet. Well, Mr. Gibson, what are we doing today? We're back on track with our mod 2 questions; right?

Steve: Yes. Where Episode 180 is a Q&A. I think it's our 58th Q&A. Lots of good feedback from people, good questions, some fun questions. For some reason they tended to be biased toward login and YubiKey and passwords and that kind of stuff. That just happened to be what people were asking about. So we got those.

Leo: We answer the questions you ask.

Steve: Yeah.

Leo: Coming up also, some errata, fixes, changes, updates from last week. Before we do that, I do want to mention...

Steve: [Indiscernible], yeah, go ahead.

Leo: No, no, no, what?

Steve: No, no. I was just going to say no security news. There is news about some GoDaddy problem. But it just happened, or just came to my attention. So if it's interesting, I'll talk about it next week.

Leo: Good. Steverino.

Steve: Hey.

Leo: We're going to get to our questions in just a sec. Oh, thanks. Hey, could you put some soy milk in that? Just take the bag out? Thanks. Getting a little tea from Dane. I've got a good life, don't I.

Steve: Yeah, you do. Well, you've built...

Leo: Do you have somebody bringing you coffee?

Steve: You've built a good life.

Leo: I have built a - surrounded myself with wonderful people who really help me get this stuff done. And you're one of them, by the way, Steve. This is - you're one of the originals. You've been doing this longer than almost anybody.

Steve: Glad to be.

Leo: Thank you. So no security news except maybe that GoDaddy story, which we will look into.

Steve: We'll find out what's going on. During my detailed explanation of security certificates, I properly said what I intended most of the time. But there was one place where I meant - where I said "public," but I meant "private," where I talked about - many times I mentioned that the certificate authority was signing certificates using their private key, which of course is correct, because it's been verified by somebody with their public key. Once I said "public key," that is, they sign with their public key. And a whole bunch of people said, whoa, you know. Our listeners are really paying attention. So I wanted to acknowledge everybody who caught me in that slip-up and affirm that, yes, I of course know that certificates are signed with private keys. That's the whole point.

The only other little bit of news I have is just a little update for people about the PDP-8 kit project. We had a bunch of listeners who were interested, who joined the SpareTimeGizmos list and have signed up for kits. They've all - the single boards, which is sort of the base of the kit, have all been mailed out as of today for U.S. customers and domestic, I mean, for, yeah, for U.S domestic customers. And the foreigners are - Bob is filling out the customs forms.

Leo: That's right. You've got to - and that's pretty complicated on something like that. Looks like a bomb kit.

Steve: Oh, yeah. And then the front panel is being brought back to life and is happening. So that's - he's just waiting basically on the parts arriving for the front panel kits. So people will be able to build little PDP-8s, which is going to be very cool. And I'll have them at one point behind me blinking away, after I've assembled mine. So that'll be fun.

Leo: Very cool. That's exciting. That's really neat.

Steve: And I do have...

Leo: Did he get enough people signing up to do the front panel?

Steve: Yeah. He didn't need a hundred. He talked to the front panel fab people. I mean, this thing, the front panel sounds like it's just going to be gorgeous because it's laser cut. It's laminated, multiple sheets of something clear plastic-y, like Lucite or Lexan or something. Five different colors silk-screened on the back and then laminated; and, I mean, it's quite - it's a very detailed assembly process. But you end up with something, I mean, you know, commercial grade, really.

And of course Bob's put a lot of code into the ROMs that go along with it to build in a debugger and lots of utility stuff. And it has an IDE interface, so you can put a, like a compact flash card or an IDE drive on it, if you wanted to. And it emulates the proper DEC hardware. And he's got drivers, even, for it. So you can run the original DEC operating systems on this thing. And they see the IDE drive as being something that they recognize, thanks to the drivers, which are part of the firmware. So, yeah, I mean, there's a lot in it. And I'm looking forward to playing with it.

I had an interesting, while I was going through the Q&A, I found a fun - oh, I didn't - I forgot to mute.

Leo: Did it go "Yabba dabba do"? What did it...

Steve: That's - someone just bought a copy of SpinRite. Speak of the devil.

Leo: I don't think you should mute it. I like hearing that. So again, for people who are new, and I know most of you know this, but Steve has a whole bunch of sounds that happen when events happen on his network. And the best one is, when a credit card payment goes through, Fred Flintstone goes "Yabba dabba do."

Steve: Yup. It's always a little crazy around here.

Leo: Now, do you get a few of those a day, a hundred a day? I mean, is it going on all the time?

Steve: Yeah. Well, I do mute it at night. I used to, when it was brand new, I would leave it on. And I'd be sort of like half asleep, and I would hear "Yabba dabba do" out in the front of the house. It's like, so I just sort of smiled to myself. But that gets a little old.

Leo: It would give me a nice, cozy, warm feeling.

Steve: Yeah.

Leo: I should set that up so every time we get a PayPal donation to TWiT I get a

"Yabba dabba do." But people are so generous, I think it would keep me at night.

Steve: Well, I wrote a custom UDP client and server system. So where I am here in my office at home, every two seconds the client sends a UDP packet out to the server, which is at Level 3, which is where our network and servers are. And that - essentially, sending a packet out creates a reverse path through all of the NAT and other defenses that I've got protecting me here. And that allows then the server to send a custom UDP packet back which has a chance of getting to me. And what it does is it basically takes a current status of the server, incoming and outgoing bandwidth, SpinRite sales information, a whole bunch of statistics, and sends it back to me here. And then the code that I wrote compares that with what it had before. And if it notices that there's been a change in the number of SpinRites sold from previously, it triggers Fred to say "Yabba dabba do." So, yeah, it's just fun.

Leo: That is really neat. That is really...

Steve: So anyway, a listener of ours, Jason Hedges, his subject line, "SpinRite Saved My Rear," caught my eye when I was looking through our mailbag for Q&A. And he says, "Hi, Steve and Leo. I've listened to every episode of SpinRite, sometimes two or three times so I can understand what you're talking about, and have loved every one of them. I always like hearing your SpinRite stories, and now I have one of my own. I work as the IT director for a small chain of retail cell phone stores. Our stores use a proprietary Point of Sale (POS) system, running on Windows XP.

"Occasionally for advertising purposes we'll host live radio personalities, which usually dramatically increases traffic to the store. Last week we were to host one of these radio remotes beginning at 4:00 p.m. on Thursday. At about 12:15 in the early afternoon, one of the store's employees called to tell me that one of the POS machines had crashed and wouldn't reboot."

Leo: Ugh.

Steve: Ugh. "I keep a current Drive Snapshot image of every machine in the company on an external USB drive. I have a BartPE bootable Windows XP disk with the Drive Snapshot executable on it. And when needed, I boot from the CD and restore the image from the USB drive. Works slick. Usually.

"Unfortunately, when I tried to access the USB drive from the ailing machine, the drive wouldn't mount. That is, the USB drive wouldn't mount. Almost in a panic, I grabbed my trusty SpinRite disk and ran it on the ailing Point of Sale system. SpinRite did its thing, and the POS booted back into Windows, literally five minutes before the radio remote began. The remote drove traffic to the store, and there would have been no way the clerks could have handled the volume on just one POS system. All I can say is thanks. I also removed the drive from the USB case, ran SpinRite on it, and was then able to recover all the disk images."

Leo: Wow. Wow. That's...

Steve: That's sort of a nice double-header success story.

Leo: Yeah. And next time make image backups. I mean, really, a Point of Sale system, that's a mission-critical...

Steve: No, he did make image backups, and he - but unfortunately...

Leo: Oh, they were on a USB drive, that's right.

Steve: And that drive had a problem.

Leo: Oh, so it was like a double whammy.

Steve: It was a double whammy.

Leo: Make two, make two images.

Steve: Yeah.

Leo: You know, though, I'm in plenty of situations where I only have - I only have one image of the TriCaster, so maybe I'd better make another one. I do have SpinRite, though. That's the most important thing.

Steve: Well, and he was able to run SpinRite. First of all, rather than reimaging the system, he ran SpinRite to fix it. And then he ran SpinRite on his image drive to fix it. So everything got fixed.

Leo: Right. I wonder if he backed up a bad image or - hmm. That's a scary, scary thought.

Steve: No, it's not that he backed up a bad image because he never restored the image to the original system. He couldn't mount the drive containing all the images.

Leo: Right, right, right.

Steve: So instead of putting the image back on the system, he ran SpinRite on it to fix it that way, and didn't use his image because at that point he couldn't. So anyway.

Leo: Steve, are you ready?

Steve: Let's do it.

Leo: Do you put a thinking cap on when you do these? By the way, I'm looking now at the GoDaddy thing. And there is a lot to say about that. But we'll - we don't like to go off half cocked. Steve likes to do the research.

Steve: That never comes out well.

Leo: We're always sorry when we do. Starting with Mat Ludlam in Weybridge, London, he wants more of #177. Hey, guys. Loved the show, as always, but particularly enjoyed the off-topic stuff that we did about the PDP-8s and the UltraCapacitors. Made me wonder if you have enough material to do a different podcast, say monthly, on a specific technology subject - solar cells, wind energy, wave energy, your first PC, latest sci-fi releases, whatever. Here's a fan. What do you think? Keep up the great work.

Steve: [Sighing] I wanted to - I put this question in because we got so much positive feedback from that episode. I was a little nervous about taking us off topic because, I mean, it was off of strict security. We've never done that before. But I got a lot of really positive feedback about it. So I wanted to acknowledge all the people that said hey, you know, that was really refreshing. I mean, it was nice. And while I don't, I mean, I just don't have the resources here to spin off another podcast, I will acknowledge that, from time to time, if there's something that really seems worthy of pausing Security Now!'s flow to talk about, we'll do so, because so many people really enjoyed the little bit of a change.

Leo: Well, you know, we also do - you know Ray Maxwell. He's a big fan of yours. And we also do a show every Thursday with Ray Maxwell where we dig into a subject. So, and he was, by the way, he was thrilled with the UltraCapacitor stuff. He talked a lot about that. And there's, you know, fusion, cold fusion experiments in his neck of the woods. And he also talked about the PDPs, thought that was so cool. So there's cross-pollination. And we certainly on the network will cover these subjects. But anytime you want to, everybody loves it. And so you're more than welcome to. We also do a hardware show with Ryan Shrout.

Steve: Right.

Leo: I mean, we've broadened the network. And I don't want to announce anything till it's done. We're going to do a hard science show with somebody who is very well known in his field. And we'll take a single topic and really dig deep into it.

Steve: Wow.

Leo: So I know people love this stuff. And it's not - don't feel like the burden's on you to do it. It's important that we have a security show. But anytime you want to do anything, I think everybody is very open to that.

Steve: Well, I didn't have a single complaint that I ran across.

Leo: That's good.

Steve: Only people saying, hey, this was really fun to do a little walk down memory lane. Lots of people could relate to their first mini computer contact and experience. And the whole UltraCapacitor thing, I mean, it generated a ton of interesting dialogue and some controversy from people. I mean, and we've shared some of those, the ones that I ran across, people saying, oh - well, in fact we've got one in here later on. So...

Leo: Good.

Steve: ...good stuff.

Leo: Well, you'll get no complaints from me, either. And like you, I got nobody saying no. So thank you, Mat, for the encouragement.

Tom in Vancouver, Washington revealed something amazing. He says: Hi, Steve and Leo. I've been a listener since show one. I'm also a SpinRite owner. And I want to leave some feedback about Microsoft's MSRT, the Malicious Software Removal Tool. We've talked about that a couple of times. You can run this program on demand without downloading anything particular from Microsoft's website. Just right-click on the desktop, select New, Shortcut, type MRT into the edit field, and hit Enter twice. This will create an icon for the MRT tool that you can run whenever you want with no hassles and no reboots. Keep up the good work with Security Now!. I guess you could also click Start, Run, and type - here, let me do that right now.

Steve: I thought, there's no way that that's going to work, hit MRT with no extension. And that's, like, in the shortcut, and you hit Enter twice? So I did it. And it works.

Leo: Well, there you go.

Steve: And does Start/Run work for you?

Leo: It does not work on Windows - but I wonder if I have to do uppercase. He says uppercase MRT. Did you have to do uppercase? I don't think Windows is case sensitive, is it?

Steve: Oh, it does, I did just put MRT into the Run box.

Leo: And it works.

Steve: Bang.

Leo: Okay, it doesn't work on Windows 7, but it works on Vista. Well, you're using XP.

Steve: I'm on XP. Okay, so.

Leo: All right. Well, let me try, let me try it on Vista just real quick.

Steve: What's very cool, and the reason I wanted to share this with our listeners, is you get - it's got a complete UI. And...

Leo: It does work on Vista, by the way.

Steve: It does?

Leo: Yeah. So it was just Windows 7 it didn't work on.

Steve: It's got a complete UI. I didn't download anything. One of the things that's there is a "View a list of malicious software that this tool detects and removes." And it gives you this huge scrolling list box of all this gunk that it will deal with. And then you click Next, and it says, oh, you want to do a quick scan, a full scan, or a customized scan? I mean, so it's got a complete UI that we've never seen before because normally it's just running, presumably it's running in the background doing, I guess, a quick scan. Anyway, I said a full scan. And so I set it off, and it's got a progress bar, and it shows you how many files it's scanning, and it was cranking away. I think it was almost done after about three hours. So it was thrashing around in my system for quite a while.

And I don't remember now what interrupted me. But I went off somewhere and came back, and it was done. And to my great surprise, I was met with the dialogue "Infected files found." And it says, "Files on your computer have been modified by malicious software. To help repair these files, select the following checkbox and click Next. Note that some data loss is possible during this process and that the tool may not be able to restore some files to the original pre-infection state. To view the infected files and choose which ones to repair, click on the View Details link." So of course I did.

And to my relief, what I saw was it had found seven things, but they were all in my mail attachments folder. So they were nothing that had gotten out into my system. But they were things that email had brought in. And I'm using Eudora, I never click on links, so none of them ever ran, so there was no infection loose in my system. But what's really interesting, and I haven't been able to perform the experiment yet, because I've worked out a system where I, like John now, I get no spam, I mean, literally nothing unsolicited, I'm very curious to backtrack and find out which things people who I know sent me that I didn't click on, but they were sending me infections. So it was, you know, really interesting.

So I wanted to encourage - now, again, I'm not running any AV. So presumably, if I were, those things would have been found and spotted on the way in through something that was doing scanning of my system, either on the actual communications channels or on the hard drive. But this was - it was fun to run this MSRT that's just sitting there in everyone's Windows machine, presumably being run monthly when Microsoft sends us an update. Although it's also curious that it took a full scan of my system to find these. That is, these are sitting here, and the MSRT running by itself isn't presumably doing a full scan. It's performing some sort of quick scan in order to be time efficient. It took me running it in full depth mode to find these seven files.

Leo: So you probably recommend people do that from time to time.

Steve: Absolutely. Why not? You just - you create a shortcut MSRT or just open your Start menu, as you discovered, and type MRT into the Run dialogue, hit Enter, it pops up, and let it go.

Leo: Microsoft's moving away from this, you know, on the XP where you hit Command, and you open a Command window, and then you do it, or you type Run. They're really moving away from that in Vista and Windows 7. You just have this line, and you type something, and it'll either search or it'll launch something. So it's very convenient to Start, Run, MRT, on Vista anyway. And it does indeed work on Vista. Now, they - and we should underscore this. They say this is not an antivirus. This doesn't replace your regular security software.

Steve: Right.

Leo: This is just for, I guess, additional - you know, this is another story that we talked about on TWiT. And not to go back to the security news section, but it kind of blew my mind that the folks who do F-Protect - who I think are pretty credible people, right, I mean, they're not, you know, these were some of the top security researchers, they're from Finland - they announced last week, Toni Koivunen from F-Secure announced last week that there was a worm, Downadup, that they now...

Steve: [Indiscernible].

Leo: You know about it; right?

Steve: Oh, yeah.

Leo: They now estimate it, it's on nine million computers in just two weeks.

Steve: Yup. Actually, as I understand it, it's not on nine million, it has infected a total of nine million. Because I don't think...

Leo: What's the difference?

Steve: Well, because MSRT is removing it.

Leo: Oh, yeah. Well, and that's the good news. The January MSRT finds it.

Steve: Right.

Leo: But the problem is, the reason it's infecting people's computers, this was the patch that came out in October.

Steve: This was the out-of-cycle serious patch that Microsoft fixed. And clearly this many machines are not being patched.

Leo: Right. Which means it's very likely they don't have MSRT updated, either.

Steve: Right.

Leo: Because that's an update.

Steve: Right.

Leo: So it probably is nine million machines that just, boy, I don't know what you say about it. It just underscores the fact that people are not running updates, and they really ought to be. Okay. MSRT. We like it. We like it.

Bill Everson in Green Bay, Wisconsin, he says: I can't wait to be frightened. Regarding the EEStor capacitor energy storage system - that's the UltraCapacitor that we were talking about a couple of episodes ago, the one that was not about security but everybody loved. Hey, we just like - we're just geeks. He says: Given all the technical hurdles that have to be overcome to make a battery like this work, it's unlikely that we'll see it in a commercially available vehicle for a few years. There's one aspect of a capacitor this large you haven't mentioned. What happens if the capacitor fails or is damaged in an accident? All that stored energy has to go somewhere. [Gasping] Ooh.

Steve: It's true.

Leo: Since a capacitor doesn't have any internal resistance like a battery, the energy will be instantly converted to heat. What we're describing here is a large bomb. Before such a device would be allowed into the hands of the public, it needs to be made safe. This will probably take the form of blast shielding that will greatly increase the size and weight of the unit. Also non-replaceable internal fuses will be required to limit the fault current leaving the enclosure. With that said, if this technology ever does make it into a car in a reasonably safe form, I will be among the first in line to buy it. Well, couldn't they put a big old ground, maybe make, you know, attach it to some big old ground or something? I mean, they don't have to - the capacitor doesn't have to be barebones, standalone capacitor; right?

Steve: Well, the way they build this thing, which is made very clear in the patent, which I read with great fascination many weeks ago before I decided, okay, I've just got to talk about this, is it's hierarchical inside. So it's - basically they're making a huge - it's a huge array of very small capacitors that are all tied together through a series of aluminum bars in part of this manufacturing technique. So I'm sure what they're doing is, I mean, I would be very surprised if it weren't internally fused all over the place. So, I mean, basically all kinds of deliberate fusing inside.

And also I saw an analysis which indicated that, if you followed and did all the math on the volume and the weight of the final battery, that is, a battery of capacitors, a whole bunch of individual capacitor cells, that what they were talking about as the final weight of the whole thing was much larger and heavier than just the sum of the capacitors would imply. So it sounds like they've already done this, that this is a blast shield, there is a serious weight and space that they've devoted to maybe shock-mounting it and who knows what. But, I mean, Bill's point is certainly right. If you imagine that energy is energy and that this capacitor is going to have the same amount of energy, for example, as a tank of gas, well, imagine igniting...

Leo: That's a good point, yeah.

Steve: ...a tank of gas. I mean, you're going to...

Leo: Yeah. You're already carrying a bomb around.

Steve: You are. And, see, the advantage of gasoline is, unlike other technologies - there was a Ben Rosen who was a major venture capitalist. He was behind Compaq, and I can't remember if he's behind Google. But he was an old-school venture capitalist. He created a flywheel-based power train where they were - a very cool technology. They were magnetically levitating a flywheel in a vacuum container and spinning this flywheel up as the energy storage technology. The problem was, I mean, this is literally a whirling dervish. You do not want to be in an accident where this flywheel, again, I mean, one way or the other you're having to store a huge amount of energy. So you don't want to be in an accident where this flywheel breaks loose from its containment and just goes spinning off down the highway because, I mean, it would just chew up anything in its path.

Leo: Yeah. So, look, I guess this is inherent in the nature of an automobile. You [indiscernible] a lot of energy to move a two-ton vehicle for hundreds of miles.

Steve: Exactly. And gasoline has the very nice property of not tending to explode all at once if you're in an accident. People are getting in car accidents all the time. And you see, in an accident where you see leaking gasoline coming out of the car, it's like, oh, that's - we don't want to let that get ignited because then you can have a big problem. But fundamentally, as you say, Leo, the need to propel a car, to accelerate and decelerate reasonably and travel a long distance, one way or the other you've got to carry a lot of energy with you.

Leo: Now, when I talked to Ray about the UltraCapacitor, he was a little more skeptical. He said, you know, this stuff's been - people have been trying to make this. In fact, I got a lot of email from people saying [indiscernible], this is another putting water in your gas tank kind of thing.

Steve: Hey, it's always that way until it's not.

Leo: Until it's not.

Steve: I completely agree. I just want it to be true. I also want there to be aliens and warp drives. So, you know, and teleportation. I'm not getting those anytime soon. I'm just hoping I'm going to get an ultracapacitor. I mean, I would just buy one just to have one. It's just such a cool thing.

Leo: We'd keep one here in the cottage. Look. Look what I got. Don't let it explode.

Steve: Well, and you could do neat things, like charging it up when electricity is cheap at night, and then dumping it back...

Leo: I think you'd see them everywhere.

Steve: Yeah.

Leo: Especially if they were relatively cheap to make. I think you'd see them everywhere.

Steve: Yeah, well, and again, you know, you can have small ones that replace small NiCads in consumer products. So I'm, again, I want it to be true. I want there to be aliens and warp drives. And maybe this will come true in my lifetime. That, you know, I think that'd be great.

Leo: ericDuckMan says, "I'm still waiting for my flying car. They've been promising us that for…." I just saw an article, somebody said we made a flying car. What was the - was it a Heinlein novel where they were getting energy from the air with little wavy antenna on - it was like magic? Do you remember that? It was a - what was the name of that book? It was a classic, science fiction classic, and I just - it escapes me. It was the - I think it was Heinlein because I remember there were Waldos also in that. Was that "Stranger in a Strange Land"?

Steve: That was what I was thinking. I just bought a hardback copy of "Stranger in a Strange Land," not more than a month ago, because it had been so long since I've read it. And I think actually I was too young at the time when it first came out to really appreciate it. I thought, oh, read that again.

Leo: I need to reread it again, and it's on Audible. I'm going to download it. Moving on to another question. We're going to get ready - get ready for the YubiKey onslaught. Matt in Walla Walla wants to use YubiKey's static passwords. He says: Steve, I really appreciate all your hard work with both the show and your software. Looking forward to CryptoLink. I'm very interested in using the YubiKey in the static password role as you described. After the key is set up with the utility, is that the only password that key can ever provide? In other words, is it kind of one fixed password? Or can you run the utility again, get another password, and so on? I'm hoping that losing that one password, though unlikely, doesn't render the YubiKey useless. Thanks again. Matt. How does it work?

Steve: It's completely reconfigurable anytime you want. If people messed around with the personalization tool from Yubico's website earlier, as I did, you want to go back because they've updated it. I think it's at 1.0.3 or something. Anyway, it is vastly easier to use than it was before. The first one surfaced a highly technical interface to the guts of the way that the API essentially works to the key. And you'd just look at and go, oh my goodness, I don't have time to figure this out. They fixed all that. Now there's a very nice interface. You basically put in a couple of your own passwords, select some obvious and easy-to-understand checkboxes, and then say Store or Update, and it updates the key. And you can go back and forth. You can turn it from a one-time password into a static password and back to a one-time password.

The only thing you cannot do is return it to the original state, where Yubico's servers can be used to authenticate the one-time passwordness. So if you switch it to static, you are then never able again to use Yubico's servers. You would be able, for example, to use the authentication that I will build into CryptoLink because you'll be able to tell it what the AES password was that you gave it. And so CryptoLink will know what the sequence is that it's generating. But you won't be able to do that with Yubico.

And in static mode you are able to change it as much as you want to. You give them sort of a passphrase, and then they turn it into something which generates a given static key. And if you ever [indiscernible] the same passphrase, you get the same static key. So you're even able to have multiple of those and switch it around if you wanted to. If you had some reason, for example, for it to be generating one long static passphrase today, a different one tomorrow, and then go back to what it was today, you're able to do that using this little, simple, easy-to-use tool. I was messing around with it this morning to make sure I had a comprehensive response to Matt's question. And it works beautifully.

Leo: Wow. Very cool. I have to - I haven't used it much. And I've really got to get going on this. I feel bad. I've got this YubiKey they sent me.

Steve: Well, and a ton of our listeners are all Yubikized.

Leo: I think I want to use it with - that's the problem, is I have so many ways I can use it. I think I want to use it with a password manager, to provide the password for the password manager.

Steve: You're right, provide some very secure way of unlocking your own password safe.

Leo: And then the password safe generates safe, secure keys.

Steve: Right.

Leo: So it would be a good kind of combination. Number five, Wes in Boise, Idaho wonders why so little email is secured. Oh, boy. Don't get me started. Hey, guys. I know you can explain this one for me. Companies rely so heavily on email now. The data is very often confidential. In fact, you see that all the time in signatures now: If you got this by accident, erase it immediately, it's confidential. Like that's going to make a difference. Ideally this stuff would be encrypted. Many companies have workaround methods via a secure website with just a link transmitted by email. Well, now, okay. My question is why is it so difficult to move to a universal secure method to transmit between email servers? You know, some sort of standard? I'm constantly amazed that there is no massive movement to push toward secure email by corporations of the world. What's the deal, Steve?

Steve: The other thing that I love in email that I receive is when, down at the bottom, and this is sent in the clear, it says: This email was checked by such-and-such virus scanner. It's like, oh, thank you. Okay. Seems to me that's a good thing for a virus to tag on the end of the email as it infects it.

Leo: Yeah, that's really...

Steve: Don't worry, this has been checked. It's like...

Leo: Well, you know what that really is. That's just an ad. The free antiviruses all do that. It's just a way to, you know, it's an ad. They're putting an ad in the bottom, really. You're right, it has nothing to do with security. Anybody can say that.

Steve: And to answer Wes's question, I mean, I don't know why more email isn't secured. I mean, I know that if I send something - and I don't often. But if I need to send something through email securely, I will encrypt a document and attach it to wherever it's going. And so it travels as an encrypted document. I think really what's the problem is there hasn't been a huge demand, and we don't have easy-to-use standards that allows us to easily, and without a lot of mess, send encryption from point to point. And mostly email isn't confidential by nature, it's just random conversation. I mean, I almost never need encryption. When I do, I use a workaround, as I said, by encrypting something and then attaching it. But when I think about it, all of my email is just random dialogue with people, and I don't need confidentiality. But certainly in a corporate environment I can see a much greater need for that.

Leo: Well, I think interoper- what happens is people default to interoperability. And so if you're going to use a standard, everybody has to - it needs to be a standard, in other words. I mean, I could, you know, you could say we're going to sign everything with PGP from now on, and we're going to encrypt it. But then everybody's not using PGP, it's nothing. I always sign my emails with the GNU Privacy Guard, GPG. And I often get emails from people saying I got an attachment .sig. What is that? What am I supposed to do with that?

Steve: Right. So it just creates more pain.

Leo: Right. I suppose I should put in my signature, "The .sig is an email signature to verify the email. And if you have GPG it'll work. If you don't, forget it, you don't need it." But it's just because there's no standard. You know, and you could use Hushmail. You could say corporately we're only going to use Hushmail, which is always encrypted. But then when you have to send a message to a client, it ain't gonna work.

Steve: Yup.

Leo: So I don't - I think there's really - that's the real issue is we need to commun- but who's going to enforce something like this? It's an anarchy. Microsoft tried.

Steve: Yes. Well, and for example, the beauty of something like HTTPS SSL connections is that it was able - it was added later. But it was, because of the nature of a web client and a server, it could be added completely transparently. It didn't impinge on the user's experience at all. Somebody might say, oh, what's this "S" in the HTTP? Well, don't worry about that, that "S" means secure. So it is. It's like, oh, okay, good. But we have all this - a large variety of email clients now. And as you said, we're lacking a single standard that everything is able to understand. And I would argue we're lacking the pressure. There isn't the pressure for it. Otherwise we would have solved this problem already. It's just most people are just gabbing in email, not sending secure things. And those who do need to send secure things have come up with a proprietary solution of one form or another.

Leo: Right. Well, one day maybe this will be solved. It just seems unlikely to me, just because it's - that's the nature...

Steve: Because I don't think there's the need, frankly. I mean, if there was a need, we would have solved it.

Leo: Right. It's the same issue that President Obama is going to face now, which is - I guess they've figured it out. I'd love for you to find out how is he using his Blackberry? What are they doing?

Steve: There are secure Blackberries available. There are - there is the technology, and it's NSA approved. It's a bulkier thing, based on a Palm Pilot. But there are secure solutions that will allow him to, with full approval of the NSA, to do wireless email.

Leo: Ah, interesting. And that probably just puts a bunch of encryption on top of it.

Steve: Yeah.

Leo: Jim in Washington, D.C., he wants to use the YubiKey, too. Me, too. Me, too. I want to use the YubiKey. But, he says: Hi, Steve and Leo. I'm fairly new to the show. I'm an IBM software engineer working out of D.C. I'm currently making my way back through your back catalog of Security Now!. Okay, 179 shows. That's a lot of listening. I love the show. I wanted to say this show has certainly made me much more security aware. Yay. Thank you for a very entertaining and informative show.

I've come to love your Perfect Passwords application. I secure my router at home with it. I'm currently storing passwords in an encrypted text file. I thought it would be very cool to have a physical token that would allow quicker authentication using the static password feature of YubiKey. My question has to do with YubiKey password complexity. After looking at the YubiKey static password site, the how-to, the PDF guide there on the Yubico website, I noticed that the password examples they were generating were only using a to z in lower case. I'm wondering, does a YubiKey - can it do the whole ASCII character set? After listening to the security - or is it, given that you're IBM, EBCDIC? After listening to the Security Now! discussion about the YubiKey I was very excited, but reluctant to purchase one when I see that it's only a through z because that really decreases the complexity of the password. We always say use punctuation, upper and lowercase. What are your thoughts on this?

Also kudos to your listener with the idea of using a concatenation of the static YubiKey in addition to a memorized password. That would add an extra layer of protection in case you were to lose your key. Thanks again for the great show. And I certainly would do that if I were going to use a YubiKey with my passwords vault, have my password plus the YubiKey.

Steve: Yes, exactly.

Leo: Something you know and something you have.

Steve: Exactly. You've got multifactor authentication.

Leo: Right.

Steve: Okay, now, the situation is even worse than Jim thinks.

Leo: Whoa.

Steve: Because what looks like lowercase a to z is actually only 16 characters.

Leo: So it can't - oh.

Steve: It's, yeah, it's a particular 16-character set.

Leo: Oh, that's not good.

Steve: Meaning that they're only encoding - well, hold on. They're only encoding four bits per character. So the reason they chose that, and this is part of what they have in their patent, and it's sort of clever, is that various keyboards in different languages, through the internationalization, map to different scan codes. And what happens at the USB interface is scan codes are transmitted, not ASCII characters, or EBCDIC or anything else.

So what they had to find was, they had to find a subset of the alphabet that, independent of language, would always have the same scan code. And so there is - and I remember we - in the newsgroups at GRC when I was doing the Perfect Paper Passwords, there was a whole issue of whose keyboards had which characters because it'd be a problem if you printed out something that wasn't on your keyboard. You'd have a hard time typing it. And the same is true with the YubiKey. So what they did is they came out with a reduced size alphabet, four bits per character. The static password that the YubiKey can generate is 44 characters long. So 44 characters at four bits per character gives you a total of 176 bits. Now...

Leo: Well, that's enough.

Steve: That's a ton. I mean...

Leo: I mean, we talk about 128-bit being really secure.

Steve: Exactly. Exactly. So it's 176 bits. Which, if you do the math, is just shy of 10^53. So that's 53 zeroes after a one. So, I mean, that is a huge number of possibilities.

Now, whatever it is that you provide, for example, if you were using this as a WPA key, that ends up being hashed using the algorithm that was created to turn passphrases into a final hashed key, which is actually used. So that key, the WPA key, ends up resolving to 256 bits for that security. But we're talking about the YubiKey being able to generate an absolutely random 176-bit equivalent string, which, while, yes, it's not upper and lowercase and using the full alphabet, you have the advantage that it's going to be universal on whatever device you plug it into, thanks to the work that Yubico did. And it's 176 random bits. Which the only thing you can do is brute-force it. So that's 10^53 different possibilities.

Leo: I think that's sufficient.

Steve: Yeah.

Leo: And Jim, since you work at IBM, I know that you can understand that math. Boop. Right over my head. Boop.

Steve: And I'll mention that when you tag on your own passphrase...

Leo: There you go.

Steve: ...that's all in addition to that 156 bits. So it's - 176, rather. 176 bits from Yubico plus whatever you add in your own passphrase.

Leo: I've been using 1Password on the Mac and RoboForm on the PC. They're both commercial products. But somebody's been telling me about an open source product. These are the password vaults that I want to use?

Steve: Right.

Leo: There's an open source free product I think works on both. That would be awesome. That would be the way to go. I hate having to have two different password stores. And then I have the YubiKey, and I'll be great.

Steve: There you go.

Leo: Jon in Duluth, Georgia wonders how secure that PayPal football really is: Hi, Steve. I was thinking the PayPal footballs suffers from a similar vulnerability to that of CAPTCHAs and of Bank of America's SiteKey, you know, click the picture of your teddy bear, which drives me crazy, authentication. Someone could create - which, by the way, have we not agreed that SiteKey, that idea of having a unique picture and a unique phrase that you know is - absolutely no way protects you against phishing? We agree on that; right?

Steve: Correct.

Leo: Okay. It's just a pain. Someone could create a fake PayPal website or a fake storefront that sends people to the fake PayPal website. The fake PayPal - actually he's going to describe right now why SiteKey doesn't work. The fake PayPal site would prompt the user for his username, password, and football token. That's the fake site. Now, for this to work you'd have to be fooled by the URL. But okay. Next, the website could turn around, take the username, password, and football token, log onto the real PayPal site. Once logged onto the real PayPal site the fake PayPal site could do whatever it wants. The football is supposed to be a one-time password, but it doesn't prevent a malicious program from using it that one time. It seems this would need to be a malicious program instead of a malicious user in order to be able to log in before the token expires. Right, it has to do it right away. Is this a vulnerability? You think there's a way to protect against it? I love the show. I've been listening since Episode 1. Keep up the good work. It's kind of a man-in-the-middle thing.

Steve: Well, that's exactly right. And the reason I thought this was a great question from Jon, and one for us to discuss, is that it brings up the question of what is it, what problem is it we're trying to solve with a given security device? Because the problem we're trying to solve, if stated correctly, makes it clear that there are problems that we're not trying to solve, and that we don't solve. So, for example, what any kind of a one-time password system is trying to do is to prevent a replay attack. It's trying to prevent somebody from logging your keystrokes and sending them off to some bad people who then use your username and password as logged to impersonate you. So that's what the PayPal football or the VeriSign one-time token credit card solution offers is that prevents a replay attack.

None of that, however, prevents a man-in-the-middle attack, which is exactly what Jon has described, where you're going to a phishing site that presents you with a copy of the real site's pages, prompts you to enter the information, and because it is intercepted, your attempt to go there, it then turns around and logs in as you, impersonating you. So he's absolutely right that, similarly, the PayPal football, like a one-time password system, will not prevent a man-in-the-middle attack. And you mentioned that you'd have...

Leo: Nothing will. I mean, that's a tough...

Steve: Well, the only thing that will is secure authentication. And secure authentication is possible, but unfortunately it's still on the user to verify that. I mean, I notice, whenever I'm - you know I'm a heavy PayPal user. I've been getting into the antique computer business a little bit lately. So I've been...

Leo: You bought more?

Steve: I've been poking around, oh, yeah, I've been poking around in eBay. And any time I get, for example, an email, somebody will - I'll buy a couple things, and I'll go, hey, can you combine these for me into a single purchase. So then I receive a piece of email that's got an updated price with combined shipping. And I click the link, and it looks like I'm going to PayPal. It's like, okay, wait a minute, is this really where I've gone? I mean, certainly our listeners understand that this is the kind of vulnerability that we have. And so I will go to the trouble of making sure that I've got a valid certificate chain, that I'm secure in HTTPS as I enter it and so forth. So the problem is not all of that is done for the user. And it requires a trained user to go through that. And for example, you mentioned that, if you didn't notice that the URL were wrong, well, we still have 25 percent of the Internet's DNS servers are spoofable. And what Dan Kaminsky's revelation about spoofing the cache does is allow you to put in www.paypal.com and go to a malicious site where the URL is correct because you've gone to the wrong IP. And if the site, then, if you don't notice that you're not on a secure page, then everything looks just fine as you enter your information in. So...

Leo: And that's the key, I mean, users have to be trained, I guess. You know?

Steve: Well, yes. And it's - one of the reasons that I do think that this extended validation certificate is a nice thing, I mean, it is a good thing...

Leo: To see the green bar, anyway, yeah.

Steve: Yes, to have it come up and say - for your browser to take responsibility for the only way I'm going to show you this green bar is if everything matches and makes sense. And so, I mean, it's more obvious than having to check for the little padlock being closed.

Leo: Yeah, but you do a poll of users. I mean, lookit.

Steve: I know.

Leo: Nine million, one third of all users haven't updated since October. That's why this Downadup's everywhere. I mean, you do a poll and say what does the green thing mean, nobody...

Steve: Yes.

Leo: I was explaining to Jennifer, who is - actually Jennifer is a good test, my wife is a good test for me because she's smart, but she's a novice user. And I had to explain to her, this is why you want to hand - I said open the browser, she doesn't even know what I'm talking about. I said, you know, the Internet, open the Internet. And I have to explain to her why you want to hand enter URLs and not click links. And it's not obvious for those users. And, I mean, we want more and more people to use computers. But on the other hand, they're having a hard time, frankly.

Steve: Yeah.

Leo: You have to be a security wiz.

Steve: Yeah. We've not made it easy.

Leo: No. I don't know what the solution is. Angus Scott-Fleming, Tucson, Arizona, brings up a good point about WPA laptop keys. He says: Leo and Steve, I've been listening to Security Now! since Episode 1. Another Episode 1-er. Good stuff. It's my first-choice podcast when I have time to listen. And I always go back and catch up when I get a few weeks behind. I've owned SpinRite since SpinRite 2. I didn't even know there was - SpinRite 2? Was I born then? And use it often. With respect to your enthusiasm for the secrecy of wireless WPA passwords, when you use your YubiKey to "type in" the WPA passwords in visitors' computers, you really should be aware that nothing in a Windows computer is really secret. For instance, NirSoft makes a freeware utility - they make good stuff, actually.

Steve: Yeah, they do.

Leo: ...called WirelessKeyView that instantly shows the WEP/WPA keys stored by Windows' Wireless Zero Configuration Service. Oh, that's nice.

Steve: Yeah.

Leo: They're not - they aren't even hashing it. It's just stored right in there. I carry this around in my USB toolkit. The only time I haven't been able to recover a wireless key using this utility is when the laptop isn't using Windows to manage its WiFi keys. Ah, that's interesting. You know, that's actually a compelling reason to use a third-party software. IBM/Lenovo, he gives an example of the IBM/Lenovo laptops, have a very good wireless profile manager that I always use on them. But if you're using the standard Windows tool for your WPA passwords, anybody can see them with a tool. So that means it's not encrypted?

Steve: No. This is a little bit confusing. What Windows does is it's going to be...

Leo: It has to store it. I understand it has to store it.

Steve: Right. And it can't store a hash of it because it needs to use it in order - in the same way that the access point needs to use it.

Leo: Right.

Steve: What it does is it does the same thing the access point does. It does the same thing that the WPA protocol requires. There's a funky acronym, PBKDF2.

Leo: Which is just a little close to PEBKAP.

Steve: It is a PKCS standard, public key standard. Stands for Password-Based Key Derivation Function, PBKDF2. And it's the second one because the first one didn't allow for arbitrary length output. We need 256 bits to feed into WPA's 256-bit key for WPA2's AES encryption. So what Windows does is it runs that algorithm which involves 4,096 passes of hashing, which mixes in the SSID for the access point and basically performs the same function. And it results in a 256-bit value. That's what it stores. So this view wireless key, it's not able to show you the original passphrase, but you don't need it because Windows allows you to either supply the passphrase or the hex for the actual key. And that's what Windows stores. So someone cannot get your passphrase, but they can get essentially the digested equivalent, which is enough to get you on the network.

So this was an important point I wanted to make to our listeners is that, again, we want to be sure what it is that - what we are securing and what we think we're securing. If we give - if we use the YubiKey, for example, or just give a visitor, or we type it in for them because we don't want them to know it, our passphrase, well, their computer has it. And if they were to run this utility, they could capture the hex of the literally digested passphrase...

Leo: Of course, yeah.

Steve: ...and get back on our network in the future.

Leo: Of course. And now then that means it's not Windows. It would happen on any operating system if you had the appropriate tool to do it.

Steve: Correct. And...

Leo: And with the Lenovo tool, software would, too. It's just that the NirSoft stuff is designed for Windows, not Lenovo software.

Steve: Correct. Exactly that, Leo. So all we're really getting is a little bit of security through obscurity by not using the Windows Wireless Profile Manager and using something else.

Leo: And for all we know there's some other utility that's widely used that does it with any other store. So it can't. So that's the point, is it can't. It can't encrypt it. It can't hash it.

Gustin Johnson in Calgary, Canada offers Firefox thoughts and a plug-in suggestion. I'm not sure why it only just occurred to me now, but isn't Leo exactly the sort of person that should be using NoScript? Oh, boy. No. It seems to me, since he's viewing a large number of sites, his attack surface is much larger. I agree with you. Yes, that's true. I know for me I don't try to add sites to the whitelist since I knew that even if they're safe today, they may not be safe tomorrow. Also true.

On a related topic, I have a couple of Firefox plug-in suggestions. Jsview: This plug-in allows you to view the source of all JavaScript and CSS code sent to your browser. Oh, that's cool. ShowIP: This plug-in displays the IP address of the web server your browser downloaded the current page from. In addition there are two menus full of options, one accessed by a left click; the other right. Things like DNS and WhoIs information, Netcraft lookups and more. Oh, that'd be very handy. Firebug: I do know about this one. This plug-in's a great way to explore how a site is put together. The Inspect option is quite handy for tracking down errors in your own site. It is additionally handy for inspecting suspicious elements of websites or their login methods. Keep up the great work, guys.

So, all right, let me defend myself. Yeah, you're right, I have a big attack surface. But on the other hand, I need to - and this is what I mentioned before. I need to look at sites as you will see them. So if I have - and I've run into problems with NoScript running, I forget it's running, I'm not seeing the full site, and I say, well, this site would be better if it had a login page. And then people say, well, it does. What are you, on crack? So I can't - this is why I can't. I'm risking myself for you. That's why.

Steve: And Leo, we all appreciate it. I wanted to take this opportunity to give everybody an update just on my own experiences with NoScript and to further promote it. Having disabled the annoying notification, I'm completely happy with NoScript. When I go to a site, and it's, like, kind of funky, doesn't seem to be working right, but I don't think I'm ever going to go there again, then I just - I use the "temporarily allow" so that I'm not building up just a huge long list of sites that I've allowed scripting for. But I have relatively little trouble with it, relative to the security that I know I'm getting by not allowing scripting, which is significant security.

I would - the only solution that would work for you that I can imagine would be a Typhoid Mary computer, you know, one where it's completely separate, and this is the one you don't - that you have configured for minimal security so that you're going to see everything that the websites provide, but you don't allow - and if it got infected, some way you've arranged to sequester it from the rest of your network. And then again, that's where practicality falls down because it's just not practical to do that.

Leo: I'm just going to have to live with it. I haven't gotten burned. You know, we had an interesting question, I meant to raise this with you, on the radio show this weekend. It was fascinating. Guy called in, and he said I'm, you know, I'm a photographer. And I have a website. When you go, when you go, when you type into the browser the address of my website, it pulls it up just fine. But then do a Google search for me - it was Joseph Orsillo, Joseph Orsillo - and click the link. Whenever a search comes in from Google or Yahoo!, instead of getting my site, you get Antivirus 2009. You get a popup that says you may have viruses. Click this link to get scanned. You never get to his site. And I said wow. But that only happens through a Google and Yahoo! search. Let me think about that. And actually one of our chatroom guys, [Ben Fransky ph], who has a lot of server experience, says, you know, that sounds like maybe a modified HT access or maybe a modified web server configuration that's looking at the referrer.

Steve: Right.

Leo: And that makes sense. And in fact we looked into it, and there's a host, a very big host, iPower, who either their configura- I've heard two stories. I've seen this happen to other people on iPower. And it may be that their file permissions aren't well set. Or it may be that their users, because they have a lot of inexperienced users, aren't using good passwords. But for whatever reason, their .ht access file is being modified to do this redirection. So, now, if you have NoScript - it didn't harm me because I was on a Mac. And it made me, wanted me to download this EXE file. And I know perfectly well it's Antivirus 2009. It's spyware. But I imagine a lot of people get bit by this. And I imagine a lot of websites that think they're fine, they're being - they've been modified.

Steve: Right.

Leo: To run this little script.

Steve: Right.

Leo: It was a shocker. And by the way, it took him several days to get this fixed. But finally iPower said, well, we've just changed the password on your control panel. Which I don't think was sufficient.

Steve: Well, I did want to share - I know that we've got listeners who would love to know about these tools, these additional...

Leo: Oh, yeah, the Firefox plug-ins, yeah.

Steve: So it's Jsview and ShowIP and Firebug that really do look like they're useful for further drilling down in sites and keeping an eye on what's going on.

Leo: We have a new show notes mechanism that's been really great. We have a TWiT Wiki, wiki.TWiT.tv. It's a little slow right now. It turns out that wiki - it's running MediaWiki, which is the Wikipedia stuff. It's killing our server. So we're doing a lot of caching. And Bear, who's our sysadmin, is really working hard to get memcache and some other stuff working on it to speed it up. But people are keeping show notes while we're talking, Steve.

Steve: Wow.

Leo: And they're doing a great job. So we now have very thorough show notes on all the shows at wiki.TWiT.tv. And we'll make sure that those plug-ins, all three of them are linked there. And I know you'll put them on your page at GRC.com, too.

Kerry, Santa Cruz, California, my old stomping grounds. Go Banana Slugs. That's the UC Santa Cruz mascot. Did you know that?

Steve: Santa Cruz was your stomping grounds?

Leo: Oh, yeah, went to high school. My dad taught at UC Santa Cruz. I went to Santa Cruz High.

Steve: Cool.

Leo: We were the Cardinal. Wonders about needing to trust anyone. He says: I recently obtained a Thawte personal email certificate. I'm wondering how secure these really are. I realize it's safe enough to protect me from a man-in-the-middle attack. However, is it as secure as a "trust no one" technology? In other words, does Thawte or any other certificate provider keep a copy of the private key? I hope you can answer this. I can't seem to find any information about it on Google. I've tried using PGP. But as you know, it isn't free, and it isn't easy for many users to set up. I also wanted to thank you for the show. When I discovered it last winter, I downloaded every edition and listened to them all over again within a couple of months. I now stay caught up every week. I use GNU Privacy Guard, which is an open source free PGP clone, by the way. And that is free and freely available. And very effective.

Steve: Well, to answer Kerry's question, the issue is how was the certificate generated? As we talked about last week, one of the beauties of the way the public key system operates is it is definitely not necessary for you to give somebody your private key in order to get them to sign a certificate for you. The idea is that you use - that you generate your certificate request, having had your system produce the public and private key pair. That is, you do it at your end. Then you sign the request with your private key and provide the request and your public key to the entity who you're asking to sign, that is to say verify, this information. They are able to verify that you are in possession of the private key that matches the public key which you gave them by decrypting the signature that you encrypted with your private key, decrypting it with the public key that you provided. Only if you have a key pair that are matched will that succeed.

So if the Thawte email certificate generation is wholly on their site, that is, for example, if it's a web-based system where you click a few buttons and they say, oh, here's your certificate, well, in that case absolutely yes, they have your private key. We don't - because they perform all the work for you, and part of that had to involve generating a public and private key pair. They would be providing you with the private key along with the resulting certificate. But the fact that they have provided it to you means that they had it. I don't know whether they kept it. We hope they don't. I would presume they don't. But you are trusting them not to keep it.

The safer, better approach is clearly for you to generate that private and public key pair yourself. Or, for example, them to provide an application so that you're able to do it on your machine. Or maybe, for example, it could be an ActiveX control or an applet or a plug-in, for example, that one way or another generates it on your system so that they never get the private key half of that pair. So it's possible to do it in a "trust no one" mode. It's also possible that you do need to trust them, based on how the certificate is actually manufactured.

Leo: All right. Very cool. Moving along to Sean - by the way, the certificate thing is mostly for Outlook users because Outlook likes a certificate. But other email programs you don't have to use certificates. You can use S/MIME or PGP, and it works fine. Or GPG. In which case you generate your own codes. You don't have to use a certificate.

Steve: Well, I'm a little bit partial to S/MIME, only because it is built in, and it is a standard that's all there.

Leo: Right. S/MIME's what I use, but that's where you get that weird - sometimes you get that weird attachment that baffles people.

Steve: Right, right.

Leo: So there is this kind of, you know, PGP and GPG offer this kind of bulletproof, it works for everybody, but it's a little confusing where you actually - there's actually a hash at the bottom of every message. But then people go, what is that? What is that? But in both cases you're keeping the key to yourself. Nobody knows your key.

Steve: Correct.

Leo: You publish your public key so that people can send you encrypted email. But your private key is yours.

Steve: Right.

Leo: Scott Pritchett in Kidderminster, U.K. provides some additional PayPal info. He says: Searching for "plug-in" on PayPal.com gives "PayPal Plug-in. Shop securely online. We're sorry, but the PayPal plug-in is currently only available in the United States and is not offered in any other country at this time. More information: Clicking the "More Information" link gives an out-of-date error. Nice job, PayPal.

Steve: Yeah.

Leo: I think this proves it's U.S. only, and that by extension one-time cards must be, too. And that would make sense because the credit card system is a national system. I mean, what they do in Britain is, it may say Visa, but it's really different.

Steve: Right, right. Anyway, I just wanted to share this because there's been a lot of interest among our listeners about the availability of this one-time credit card system in PayPal. And this information from Scott really strongly implies that this is just U.S., and that it's not available, no matter whether you download the plug-in first in order to get the menu option on the UI or not.

Leo: All right, Steve, our last, our final question from Dan in the U.S. of A., and no further information is provided, and you'll see why.

Steve: Yeah.

Leo: Steve, on Security Now! 179 you mentioned better security questions a user had submitted. It was a blog post. It was a very funny post. One in particular perked my attention as a very bad security question: What was your score on the civil service exam? As a civil servant myself, I can tell you this is not a good idea because in many states, including mine, civil service results are posted online and fall under public information. All someone would need - ooh, yeah. All someone would need is a name, address, and SSN, a Social Security number - of course if they have that you're in trouble anyway - and they can get the results of not only that person's score, but scores from everyone else who took the same test. Oh. That's a problem.

Granted, the question could be referencing a score from many years ago. But there could be a chance the information is preserved. God only knows how far identity thieves will go. The odds are they have some of this information already on hand. Civil servants are subject to a bit of public scrutiny, and therefore the public can get a lot of info from the state, including start dates, years of employment, salary, job title, and so on. Basing any security question on any employment info, bad idea. And that's a good point. That's a really good point. Anyway, just thought I should give you and the listeners a heads up. Love the show and love my SpinRite. I think, you know, these were comedy questions.

Steve: They were. And it's funny, too, because somebody else made a comment similar to this, a little less extensive, who said, you know, I don't think that the security question, "Who did your grandfather vote for in the 1943 presidential election?" is a very good one because how many choices are there?

Leo: There's only two.

Steve: Uh, yeah.

Leo: That's a very good point. And I think everybody in '43 probably voted for Roosevelt anyway. So it's a pretty good bet.

Steve: It was, you know, we did intend those just to be humorous. And I thought there were some that were pretty funny, so.

Leo: It would have been '42.

Steve: I just wanted to make sure that people understood that we were not serious about those. We were not proposing those as useful security for anybody.

Leo: It was comedy. However, I think that there is a good point, which is the best thing to do is to either make up your own question and lie about the answer and remember your lie; or, if you can't make up your own question, just lie and make up, you know, what grade school did you go to, Mortimer Snerdly High, and make it up.

Steve: Right.

Leo: And then nobody's going to guess it. It's not going to be on record anywhere. It's only in your mind. It's just like another password. But I guess the point of security questions is they're easy to remember the answer to, which of course makes them inherently insecure.

Steve: Which defeats the security, yeah.

Leo: That's the problem. Security, convenience, never the twain shall meet.

Steve: Indeed. They are not friends of each other.

Leo: I'll tell you one place you should go, GRC.com. That's your friend online for security information; those great programs like ShieldsUP!, Shoot The Messenger, DCOMbobulator, the wonderful Wizmo - which again I recommended on the radio show this weekend because somebody wanted a quick way to - was it to shut down? Oh, no, I know what it was, reveal his desktop. And he lost the reveal the desktop icon. I said, I bet you Wizmo can do that. Wizmo can do everything. Anyway, it's all there. It's free. And of course when you're there, don't forget, it's not free, but it's a must-have, SpinRite, the world's finest disk maintenance and recovery utility. Really the only one that does what it does. GRC.com. Also have show notes there, including Elaine's great transcriptions - hi, Elaine. Does she have to write that when I say that?

Steve: Yeah, she does. She's very faithful about this.

Leo: Hi, Elaine. [Hey, Leo.] Elaine's really great. [Awwww.] She does a great job with the transcriptions. We also have 16KB versions for the bandwidth-impaired. It's all at GRC.com. And if you want to ask a question next time in Episode 182, two episodes hence, SecurityNow.com - I'm sorry, GRC.com/feedback.

Steve: Exactly.

Leo: That's the place to go. Well, Steve, go to bed. Take a nap. You were up late partying, celebrating. We will talk to you again in a week. And by then you'll have recovered.

Steve: Yes, and we'll have another great episode, I am sure. I have no idea what it'll be about, but it'll be good.

Leo: There's always something to talk about on Security Now!. We'll see you next week.