



Listener Feedback Q&A #57

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-178.mp3>

Quarter size (16 kbps) mp3 audio file URL: <http://media.GRC.com/sn/sn-178-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 178 for January 8, 2009: Listener Feedback #57. 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! #178 in a continuing series...

Steve Gibson: And counting, yeah.

Leo: Yes, Steve Gibson is here, the security guru. Hi, Steve.

Steve: Hey, Leo. It's great to be with you. I'm feeling a little bit less like a guru than usual because I said something completely wrong last week that just really pissed me off.

Leo: I know you hate it when you do that.

Steve: Oh, I really do. And, you know, there's no excuse for it. I was feeling rushed. I was worried that we were going to have a show that was too long. As it was, it was our

longest ever. It was two hours.

Leo: Have you had any complaints? Because I haven't.

Steve: No. Actually I was gratified - I was also a little worried that it was a non-security show...

Leo: Right.

Steve: ...largely. And I got a ton of positive feedback from it. Some people said they thought it was the best podcast we'd ever done. Which, you know, I don't want to worry people, we're not going to go wander off the reservation and no longer do security. But anyway, what I said that was wrong, that just really annoys me, was that I was talking about, in this whole SSL cracked deal - which I'm going to cover clearly and carefully in detail next week because it's a big issue. In looking carefully at what the researchers did, they did some really clever, fun, and interesting things. And we've never really talked about certificate chains. I've referred to them sort of in passing, but we've never done, you know, really explained what that's all about. And there were a bunch of questions that were raised that I saw in preparing the Q&A questions for this week. So that's our topic for next week.

But what I said that was wrong was that it was the signature of the root certificate that was the problem. And, I mean, I knew immediately when it was brought to my attention that I had said that, that I had misspoken. It's the hashing algorithm of the certificates signed by the root authority that is weak if it's MD5. So it's like, oh. Now, it is the case that root certificates that have chosen to sign themselves with MD5 are probably also signing the ones they issue with MD5. So there's that chance. But that's really not the nature of the vulnerability. And also there were people who were arguing that it's only certificates signed from now on that are the problem, not any that already exist. And that's actually not true. It's the nature of cryptographic weaknesses that they grow over time.

Anyway, I'm going to cover this. It's the topic of next week's show. We're going to go, like, in true to form, no rush, cover it from front to back so that everybody who is listening is going to completely understand this whole chain of trust and certificates and signing and all of that. But in the meantime there has been an immediate reaction from somebody who is creating Firefox extensions. There's an outfit called - the URL is CodeFromThe70s.org.

Leo: I like that.

Steve: If you just put in "code from the 70s" into Google, it's the first link that comes up. There's a Firefox add-in called SSL Blacklist. And it's now, as of New Year's Eve, at v4.0. What he just added in v4.0 is a check for whether MD5, the weakened, no longer really very secure hashing algorithm, whether MD5 is in use during the visit to a secure page. And you'll be notified if it is. That, of course, doesn't mean that this is a problem. But it means that, you know, that the known exploit could be employed because the known exploit uses MD5. So apparently about 14 percent of issued SSL certificates out on the Internet today are signed with MD5.

Leo: 40 percent?

Steve: 14 percent.

Leo: Oh, 14. Oh, good. Whew. You scared me.

Steve: VeriSign has responded that - they own the RapidSSL guides that were the target of this particular problem. They have responded that they will replace anyone's certificate free of charge that was signed using MD5. So essentially what it means is that, if you wanted to sort of help clean up the Internet, you could install this SSL Blacklist 4.0 into Firefox from CodeFromThe70s.org. And if you visited sites where you got a notice, what you could do is just notify the webmaster, hey, just thought you should know, you're probably going to be hearing this from more people in the future. You can fix your certificate. Go ask the people who issued your SSL certificate for an update signed with SHA-1. And then you're not going to get anybody else bugging you, saying hey, you know, misunderstanding what this really means about whether their site is secure or not.

Leo: So to clarify, it's not the root certificates that are the issue. It's the certificates assigned to websites by root authorities that are using MD5 as their hash.

Steve: Correct. Correct. So, for example, the root certificate could be signed by SHA-1, yet they could be signing the certificates they issue with MD5, or vice versa.

Leo: Although, as you point out, if somebody's using MD5 as a root certifier, they're probably also using MD5 for everything else.

Steve: Yes, yes. And so, you know, if people had deleted those certificates, then they would be, like, way safe in the case that the same certificate algorithm was being used for the root and for the certificates being issued, which is likely the case. But anyway, I'm annoyed that I got that wrong. So for the record, we're fixed, and we're going to do a whole show on it next week to really explain and clarify what all this is about.

Leo: Excellent. Excellent.

Steve: Sandboxie I have mentioned was in beta with the right-dropping feature. It's now in public release. So anybody who is using Sandboxie may want to upgrade, I would think you would, to 3.34. It just went public a day or two ago. And Ronen has added the DropMyRights feature so that anything you sandbox has its rights stripped, even a little bit more thoroughly - I'm really impressed with what Ronen has done - than DropMyRights does. So it's a really nice addition to Sandboxie so that, for example, if you're running email or your web browser, it has even fewer rights than Sandboxie had already removed from it. He was stripping some, but he wasn't taking away admin group membership, as he is now, and doing the things that dropping the rights does. So it's a nice update. Many people commented to me about the YouTube video showing drive latency increase...

Leo: Oh, yeah.

Steve: ...when you shout at the drives.

Leo: That is the strangest thing ever.

Steve: Oh, my goodness, yes. So I just wanted to acknowledge all the email that we received. We've sort of referred to this before. I've talked about how track density has grown so high in current drives that the drives are doing everything they can to stay on track using embedded servo technology, which provides constant feedback as to the position of the head. And so it literally follows the tracks around.

Leo: So you don't think that - you're saying this is true, that shouting at the drives really does increase latency?

Steve: Oh, absolutely it's true.

Leo: It's not a scam? It's not a joke.

Steve: No, no, no.

Leo: Like the popping of popcorn with a cell phone video?

Steve: No, no. It's, you know, it's low-frequency, high-energy acoustics that hits the drive and that tends to knock the head off track. And so, I mean, it makes sense. I can't guarantee you that - I haven't tried shouting at a drive myself.

Leo: You could conceive of a mechanism where this really would work.

Steve: Oh, absolutely. In fact, a very good friend of mine discovered that the fans in their servers, the vibration from the fans were causing the data rate from their drive to drop, from hard drives to drop, just because of the particular nature of the mechanics. So what is happening when you shout at your drive, which I do not recommend anyone do at home...

Leo: I shout at it all the time. Well, I shout at the computer. There's a drive in there.

Steve: Yeah, okay, right.

Leo: If you want to shout, you want to use a high voice or a low voice?

Steve: A low voice will have more acoustic energy.

Leo: So sound like this.

Steve: And it will interact at the right frequency with the rotation rate of the drive. So anyway, the idea is that, when you're shouting at it, you are vibrating the drive and causing the head to have trouble staying on track. The reason the latency increases is that the head misses looking for the beginning of the sector or goes off sector while it's trying to read. And so the drive aborts that transfer, loses a revolution, and then tries to do it again when that sector comes back around. So, I mean, it absolutely makes sense that shouting at your drive could cause its latency to increase, which is to say its data rate to decrease.

Leo: It's not scared, it's just trembling.

Steve: So don't do that.

Leo: Okay.

Steve: Also someone pointed out, and I love this, that one of my very, very favorite antique sci-fi movies of all time, "This Island Earth," don't know if you know the movie...

Leo: I don't know that one, no.

Steve: I've seen it, I mean, I watch it every few years because it's just so good. But what they pointed out was that it was a supercapacitor that was the original hook in the beginning of the plot. And I had, you know, the moment I read this it's like, oh, my god, of course, because I know the plot really well. But in this plot there's this scientist, Cal Meacham, who is a high-tech aerospace scientist guy. And they get some parts from a supplier. And they order really what they expect to be a huge capacitor. I don't remember now what the specs - a thousand microfarads at 200 volts. And what they receive is this little tiny bead with two connections on it. And they're like, well, this can't be right. But they test it, and it is what the specification calls for. It's a supercapacitor that's, like, way smaller than it should be. And they stick it on this machine and crank the voltage up to see at what point it breaks down. So anyway, I got a kick out of that. And this is, like, 1950-something. I don't remember, like '52 or '57 or something. I mean, it was way old. But that was the example that they chose for demonstrating advanced alien technology.

Leo: But that shows that the idea of the consummate supercapacitor is not anything new.

Steve: Correct. Correct.

Leo: In other words, we've hypothesized about these. This is the first we've been able to make, is that it?

Steve: Well, there are a lot of people who are working on them. It's the high-voltage claim of EESstor that is the most controversial because that's the most tantalizing. As we know, the energy storage goes up with the square of the voltage. So every time, if you can double the voltage, you quadruple the energy storage. And so ultracapacitors have existed for a long time. Normally they have been called supercapacitors because they're big. And, for example, they're used in consumer electronics to, like, keep CMOS memory alive over time.

Leo: Oh, okay. Sure, okay.

Steve: I did want to mention that we are one week from January 15th, which is when the orders for the PDP-8 system that I mentioned last week, the single-board PDP-8 computer, are sort of informally closing. At that point Bob's going to add them up and begin placing his orders to fulfill the kits. So I just wanted to let our users know that, I mean our listeners know that, by the time they hear us again, which will be actually on the 15th, it'll sort of be too late. So...

Leo: What's the website again?

Steve: That was, boy, SpareTimeGizmos.com.

Leo: Very good.

Steve: And extensive notes in last week's episode with links and things. So the show notes for Episode 177. Remember I also created a tiny URL, or a SnipURL, snipurl.com/sn177.

Leo: Yeah. And we apologize for not getting those in the show notes when we put it out. But from now on we'll make sure that we give links to your show notes every time we put out our show notes. And I'm keeping more elaborate show notes as we talk. So we'll have better links in future. I apologize. That's one of the things we really want to work on is getting more - you're done a very good job of getting textual versions of the audio content out there. And I think that's really important.

Steve: I know that people really love it. In fact, I've forgotten to update the Security Now! page with the links to Elaine's transcripts for a couple days. And people said, hey, where are the transcripts? It's like, oh, I just forgot to update the page. So then I just copied my copy to the server, and it was all live again. So I know that people really do like them and rely on them. And about three or four thousand copies are downloaded every week.

Leo: It's kind of ironic. I have for a long time been giving out, in speeches and stuff, saying if you do a blog, you should also do audio, you should also do video, you should do every medium. And particularly if you do podcasts and video because Google can't search audio. So it's really important to have textual matter that people can use, not only to get the links, but to follow along, that can be searched by Google and all that stuff. And you've always done a good job. I have to follow your model into our other shows because it's really the right way to go.

Steve: Well, it's not inexpensive. But I'm happy to pay for Elaine's quality because, I mean, she really is a stickler for details, which I really appreciate.

Leo: Yeah, we may have to call Elaine and say, how many shows can you do? She might have a new career. The podcast transcriber.

Steve: She would love it. She would love it.

Leo: Yeah, yeah. She's really good.

Steve: And I have what is perhaps one of the oddest SpinRite stories in a hundred and...

Leo: Oh, come on. You've had some pretty odd ones.

Steve: I've had some pretty odd ones. But this one may still - it's definitely up there.

Leo: Really.

Steve: This is from Mike Roberts, whose subject looked rather benign. The subject was "SpinRite recovers from burned hard drive."

Leo: Okay.

Steve: So he says, "Hello. I recently had one of my older computers fail to boot. When attempting to start up, the motherboard would only issue a series of beeps. I figured the first thing would be to replace each part piece by piece to determine which part was causing the problem. But replacing each piece failed to solve the problem. Next, I decided to move the jumper on my motherboard to clear the CMOS. Reasonable. As I was turning the machine back on, I accidentally dropped a screwdriver into it, and it began emitting sparks, and parts began to catch on fire. Within seconds my power was shorted, and the entire house lost power. Without even thinking, I grabbed a nearby can of Mountain Dew." He probably had been drinking too much of that. Don't know if anyone knows, that's seriously caffeine loaded. He says, "Without even thinking I grabbed a nearby can of Mountain Dew and splashed it on the burning computer."

Leo: Oh, my god.

Steve: "I realize now that this was an electrical fire, and pouring this on earlier, before the power went out, would have been disastrous. After turning the power back on from the basement, I went to assess the damage. Needless to say, pretty much everything was destroyed beyond repair. Even if it wasn't all burned and/or melted..."

Leo: It was covered with sugar.

Steve: "...it was now covered in Mountain Dew. The files on my hard drive were not critically important, but I wanted them. I took the hard drive, pulled the melted plastic off, and wiped the stickiness and black burn marks off. I connected the hard drive to a clip that I had pulled off an external hard drive and tried to connect it to my computers. Neither my Windows, Mac, or Linux machines could find the drive. So I decided to try one more thing. I connected the drive to a computer and started up SpinRite."

Leo: Oh, man.

Steve: "To my utter disbelief, SpinRite found the drive, and I ran it at level 2 for data recovery. After SpinRite was finished, the drive was recognized by my computers, and I recovered every single file. Thank you. P.S.: I love the show. Keep it up."

Leo: P.P.S.: I'm going to stop drinking so much Mountain Dew.

Steve: Oh, goodness.

Leo: And don't drop a screwdriver into your computer. It's a bad idea.

Steve: Bad idea.

Leo: Wow. What a great - that is a hoot. What a great story.

Steve: Thought [indiscernible] a kick out of that.

Leo: Yeah, yeah. The first question of the day, Mr. Steve, and it comes from someone who wishes to remain anonymous. He's in the business of vehicular travel, wants to comment on what we talked about last week, the UltraCapacitor from EESstor: Dear Steve and Leo, first I want to tell you Security Now! has kept me company and awake on many a long business trip. I hope the show continues for many more episodes. With Steve's "crack the whip" attitude about recording every week, I'm sure it will. He says: Regarding EESstor - which, by the way, is

EESstor.com. Not that you'll find anything there, but there is at least a website.

Steve: Yeah. Actually they didn't have a website up last. They were saying once they finally got it done, then they would have something to talk about. But in the meantime they're just sort of keeping their head down and...

Leo: Oh, they don't even have a site.

Steve: Yeah.

Leo: Oh, well, if you Google EESstor, you'll find many sites talking about them.

Steve: Yes, exactly.

Leo: Now, this guy knows what he's talking about: I'm heavily involved in energy storage research with one of the major companies producing hybrid-electric drive trains. You correctly pointed out in your show that energy storage is the key technology to making hybrids or pure electric cars a commercial success. We were visited by EESstor's principles eight or nine years ago.

Steve: Yeah.

Leo: The credentials of the people that started the company were very impressive. Their product claims were fantastic, although their general method sounded plausible - first red flag, fantastic claims without any accompanying samples or test data. We said, let us test a sample of any kind, even just a single cell, and we'd love to talk more. They were to have something within a year. Since that time there have been only fleeting press releases or news stories every couple of years. I've never seen any evidence of samples or example systems. I've discussed their claims with ultracapacitor and battery experts at a number of conferences. Most experts have doubts about the physics associated with their claims.

There's another issue, even if they're able to produce their ultracapacitor as claimed. You pointed out the magic of V^2 as it relates to the amount of energy stored in a capacitor. EESstor's remarkable energy density is achieved by operating it over 3,000 volts. There are plenty of power electronics devices that operate at these voltages used by electric utilities for transmission and distribution of power. The trouble is, these devices are very large and very expensive. There would be huge challenges with building a power controller small enough and cheap enough that still would safely operate at these voltages in a passenger vehicle or even a large truck.

So I hate to rain on the parade, but I don't have high hopes that EESstor is going to be a game-changing solution anytime soon. But I do have high hopes for ultracapacitors in general. There are a number of good products out there from companies like Maxwell, NessCap, Nippon, and others. We've used ultracaps as the

only energy storage in a number of hybrid vehicles with great results. They don't have enough energy for electric-only vehicles, but they do have nearly limitless life, as you mentioned. Keep up the good work. Note: Please don't use my name or company name on the air if you use any of this in one of your programs. My company has rather strict communications policies.

Steve: Not that he really said anything very controversial. I don't disagree with any of that. I'm just hopeful. The patent looked like it was about as authentic as could be. The fact that they've got this contract with the government, I mean, I don't know what it means. Maybe that is a good thing with military aerospace applications. And certainly the Zenn car folks in Canada are reportedly gearing up to use this. So one presumes that these problems have been solved, and somehow they've worked out how they can deal with the 3,500 volts. I mean, it is a challenge to - you need to step up the voltage, for example, of your charging source, which might just be 110- or 220-volt line power, up to 3,500 volts in order to get the pressure, essentially to pressurize the capacitor at that voltage. And then you do need to be able to step it down and meter it in order to use it for your drive train. And if you're going to use regenerative braking, which everyone wants to, you need to be able to have that step-up capability in the car also, not just in a standalone external charging station. But if you're going to hit the brakes you want to put the momentum from the car back into the capacitor.

So anyway, I just - it looked like a great and interesting piece of work that we saw patented, and we'll keep tracking it. If anything happens with it, I will let our listeners know. Because there was a lot of interest in this also from our talking about it last week.

Leo: Yeah. I'm glad we raised the subject, anyway. And maybe somebody else is also - I know many others are also working on this. Maybe somebody else will come to the forefront, as well.

Steve: Yeah, I saw one piece of email from someone who thought I had just absolutely lost my mind, falling into the "peak oil mythology," as he called it. And it's like, well, okay, I mean, I don't mean to get political. I've read a bunch about it. It makes sense to me that at some point in the not-too-distant future the world's increasing hunger, which is growing constantly, we're going to have a hard time meeting demand. And that's all I was saying, was that at some point prices are going to start really going up because the world's going to want more than producers are going to be able to produce. The question is, is that accurate or not? And again, we should know in a few years.

Leo: Well, it's not like they're making any more oil.

Steve: No. I mean, no one doubts that ultimately we're going to drain the Earth of it. No one apparently doubts that there's about two trillion barrels total, of which we've used one trillion. The question is, are we in trouble in 200 years, or are we in trouble in five years? So...

Leo: Well, either way I think we should be starting to think about it.

Steve: Well, and see...

Leo: I don't want to leave this problem to my grandkids.

Steve: From an economic standpoint, unfortunately, it's going to take energy costs increasing to make these alternative solutions economically viable. So nothing is, as long as oil is as inexpensive as it is now.

Leo: Right. Daniel Farrell, a researcher at the Imperial College in London, knows a thing or two about solar cells: Hi, Steve. I really enjoyed your discussion of supercapacitors when listening to the latest Security Now! episode. You also touched on solar cells. This happens to be my area of research, and I'd be happy to discuss with you the most recent developments and concepts in the field. Some of the current buzzwords and phrases that I hope will get you interested are: down and up conversion of photons; multijunction, multiband, and hot carrier solar cells; and molecular and organic-based concepts. I have just finished my Ph.D. I now work as a solar energy researcher at Imperial College in London. Love the show, have been listening since 2005. You know, Ray Maxwell also got very excited about what you were talking about. And he talked a little bit about a fusion project that's up there in Vancouver. You know, fusion is another one of those holy grails of energy.

Steve: Yeah. In fact, during my recent interest in alternative energy stuff, I took a look at the state of fusion. There's something called, I think it's the National Ignition Lab.

Leo: Not aptly named, I might add. I think probably they should consider a new name for that.

Steve: The National Ignition Lab is out of JPL, up in Northern California. And it's fascinating to look at it. But it also gives you a sense for how far away we are from having this stuff able to come online. I'm not hopeful, unfortunately, about fusion. The reason I wanted to add Daniel's notion, or his dialogue about solar cells, is just to have an opportunity to mention that I'm extremely hopeful about solar cell technology in the future. It feels to me like it's sort of where digital cameras were when digital cameras first began to happen. I remember people, as they began to happen, people were saying, gee, you think I ought to get a digital camera? And my advice was, I said, well, if you can really use it and really need it right now, then yes. But you need to be prepared for being really upset a year from now...

Leo: When something better comes along, yeah.

Steve: Right. I mean, remember the dramatic, I mean, look at the dramatic cost and performance curve that digital cameras went through over the last 10 years. I mean, they just got incredibly inexpensive. The battery life shot up, resolution shot up, I mean, it's just transformative. As opposed to, for example, a mature technology like existing chemical SLR photography, which is just - it was done. My sense is that we are sort of in the same place with solar cell technology, that once we really bear down on this, we're going to see costs drop and efficiencies increase, which will be really significant for the

alternative energy future.

Leo: Yeah, yeah. Look, this is all-important stuff, and it's something that's going to be on people's minds and in the newspapers and the news for the next many years, I think. So it's good that people like Daniel are out there studying it, doing what they can.

James Ortega, in Kokomo, Indiana, needs some YubiKey router configuration clarification: Steve, you mentioned in your show, Episode 177, that you use the YubiKey to secure your router. I've contacted their technical support for instruction on how to do this. Still no response from them so far. Can you demonstrate on your show how to perform the password generation and authentication of the passwords with the router? Thanks.

Steve: Well, there has been a lot of interest in this notion that I mentioned that Stina has shared with me of the ability to switch the YubiKey from its normal mode, which is a one-time password system based on a secret AES key buried in the YubiKey. The personalization tool, which is available for free download from Yubico's site, it's able to change the key so that, instead of giving a different password every time, based on a secure cryptographic algorithm, it spits out a fixed, random-looking and certainly randomly generated or pseudorandomly generated once, a fixed long character string. The beauty of that is that it allows a simple little hardware token to produce a string of gibberish that you just can't memorize when you look at it. I mean, you can't even type it in, probably, unless you really tried. And so that can be used anywhere, at any time, in place of a shorter password that might be vulnerable to dictionary attack or guessing or somebody glancing at it and writing it down and so forth.

So the one way that I mentioned of using it where it is in use now is that it could be used as the preboot authentication password by TrueCrypt. So you have this on your keychain, and you type that in, you use the YubiKey to enter that into TrueCrypt in order to authenticate that, you know, something you have, one type of authentication, as you log into and start up a TrueCrypt whole-drive encryption volume. Or even to use it as the password inside Windows if you want to mount a TrueCrypt volume.

Well, another way it can be used that we talked about is as a WiFi AES encryption key for WPA2, as it's called. But it's actually, you know, the AES cipher. In that case, and this is what James is asking about, it's not that you're using the YubiKey to secure your router, but rather your router's WiFi radio. And so the idea would be you convert the YubiKey, first using Yubico's personalization tool, into this fixed static random gibberish. You then use that when your router is - when you're setting up WiFi, and it asks you for your WPA key, you would put the cursor in the field, touch the YubiKey button, and it would type that into the router. Then it would ask for you again, so you type it in again. Now you've set up your router with its WPA key from your YubiKey. Then you go to your various machines and enter those. And the advantage, of course, is that it's - you don't have to do any typing. It's incredibly difficult to reproduce or manage. And if a friend came over and wants to get on your WiFi, you can just stick the key in, touch the button when their Windows is prompting them for the WiFi key, and it's entered. So it's a neat solution.

Leo: Very cool.

Steve: And a lot of people love the idea. So there was a strong response that I saw in

feedback responses from talking about that, too. I think that it makes a lot of sense to a lot of people just to have something that they can touch, and it zaps out a really long pseudorandom string which is the same every time.

Leo: And we'll see an even better idea in just a little bit.

Steve: Yup.

Leo: Coming up. Mack, I'm sorry, Mike Gillmore in Cedar Rapids, Iowa has a question about Microsoft's Malicious Software Removal Tool: Hey, guys. As I was listening to my show, the show 177 last week, something you said took me by surprise. You reported that the MSRT ran only at startup. For some reason I thought it ran actively, like an antivirus. This makes it sound like perhaps I should be booting each of my eight machines every day. Is that right? Nope, not a business, I'm just a really big geek. Eight machines. Thanks for SpinRite, ShieldsUP!, Wizmo, and other great tools. Mike.

Steve: Actually it's a little worse than that. The MSRT runs once a month, when you restart your system after Microsoft has given you a new version.

Leo: So it only runs when there's an update.

Steve: Right. Well, exactly. And the idea is that, monthly, Microsoft is maturing the tool to add awareness and removability of new malware. The one that they just released added two new programs. And on the MSRT site they've got a list, for example, of all the stuff that it knows about and is able to remove. So what Microsoft is doing is essentially they're adding awareness of new problems that they encounter to this tool, and then running it once just to remove any that may be on the system, or that your system may have acquired in the intervening month. So they're not trying to be running all the time like an antivirus system. There is a tool that you can run on demand, a version of this that you can get from Microsoft from the MSRT region of their site. And so that is an option that Mike has if he really wants to run this all the time. But my sense is that AVG, which is updating themselves all the time and which is running constantly, is probably doing the job for him just as well.

Leo: Okay. Yeah, so I guess Microsoft didn't want to add to the complexity of machines by having it running all the time as an antivirus does.

Steve: And I think they probably don't want to stomp on the AV industry, either.

Leo: Right, right. It's not - in other words, it's not an antivirus, folks. It's just every once in a while we're going to check and see if there's anything really disgusting going on.

Steve: Microsoft's site does say that they explicitly update this monthly. So I think we

can assume we're going to get a new one every month.

Leo: And the only issue is you may be getting, in between the updates, you may be getting some spyware on your system. Right?

Steve: Exactly.

Leo: It ain't going to find it any sooner. So that's just another reason to have some other antimalware software on there.

Elliott Kopp in St. Louis is worried about why Steve dislikes AT&T. I didn't know you disliked AT&T. Steve and Leo, I was listening to 175 the other day; I'm a little behind. You mentioned you didn't like AT&T. I use them as my landline and Internet provider because they're the cheapest in my area. I'm not aware of them doing anything wrong, traffic filtering or logging or so on. I'd love to hear your thoughts as to why you don't like them. If they're doing something naughty, I will switch immediately. Well, I'm an AT&T - I have my home service is AT&T. I don't - that's the local carrier.

Steve: Right. I thought that I ought to clarify this because I have spoken ill of AT&T. But it's only that their broadband technology was not up to speed as soon as Verizon and Sprint's was. They were using Edge technology for broadband; whereas EVDO, which was available over with Verizon and Sprint, was much faster by, like, more than a factor...

Leo: Oh, I see. So you're talking about the 3G, the wireless speeds.

Steve: Exactly. That's all it is. Nothing to do with their behavior or traffic filtering or logging or anything else. It's just that, in fact, I was over on Cingular, which of course AT&T acquired. And I deliberately left Cingular and moved to Verizon because I wanted the EVDO broadband speed.

Leo: Right, right. I think Sprint and Verizon are still the fastest. AT&T's new HSDPA is okay. It's not as fast, I don't think. And it's not in as many markets. But if you're using an iPhone, as I do, you don't have any choice.

Steve: I was going to say. And it's one of the reasons that the iPhone has been criticized is that its wireless, its broadband is just not as fast as you can get over on Verizon and Sprint.

Leo: The story was Apple approached Verizon and got turned down.

Steve: Ugh.

Leo: So there you go. And Verizon is probably going "ugh," too, because the iPhone has sold a few. They've sold a few.

Steve: Yeah. Yeah.

Leo: Burt in Redford, Michigan keeps wanting to install the ill-fated Windows Service Pack 3. This is for Windows XP. Thank you for supplying a venue that allows the common Joe - Joe the hacker - to get an answer to a question no one else seems to have an answer for. I brag about you all the time. Question: What is going on with Windows XP SP3? Like you, I have attempted to install it, in my case on different systems. They both bombed. I had to back out of the update. Can you mention what Microsoft is or is not doing to make this usable, even if no news is available? I feel like my systems are vulnerable without this update, but I'm helpless. I can't do anything about it.

Steve: Yes. I've looked around. I can't find any indication from Microsoft that they're going to address this. This is the last service pack for XP. There's not going to be a Service Pack 4, unless maybe they do one to fix the problem with Service Pack 3. But I'm in the same condition that Burt is. There are several machines I have where I cannot put SP3 on. The good news is that you really don't need it. You can keep current with the patches. All SP3 was sort of a catch-up, an omnibus package that did all of the prior updates bundled in one.

Leo: Yeah. I wonder what's going on. I've been able to install Service Pack 3 on all my machines. Well, I only have one XP machine, but - no, two. I have two XP machines, and both are running SP3. But I do get this call a lot on the radio show. And there's no - doesn't seem to be any answer. It's just...

Steve: And Microsoft never, like, fixes broken service packs. They just sort of limp along and then replace it ultimately. But this one, as far as I know, is not going to be replaced.

Leo: Remember Service Pack 2 was even worse. At least it seems in most cases with Service Pack 3 it doesn't - Service Pack 2 would just give you a Blue Screen of Death, permanent Blue Screen of Death. You'd be out of luck. At least with Service Pack 3 you can roll back. But he's right, he needs the update for security reasons; right?

Steve: Well, no. I mean, Microsoft has moved forward. And so you need to say no, I do not want SP3. But then there's still...

Leo: Oh, and then - okay.

Steve: Yeah, you don't need Service Pack 3. You can still install all the other incremental updates moving forward.

Leo: I get it. Okay. So you'll be as secure.

Steve: Yes, you will.

Leo: Okay. I wanted to mention, I should have mentioned it in the security news, but it's relevant that Twitter - I don't know if you know this - Twitter got hacked. In fact, Twitter's been the subject of a series of attacks lately. There was a phishing attack where somebody's account got hacked, and they were sending out direct messages to everybody they knew saying, hey, have you seen this funny site about you? And when you click the link, you get a login page that looks just like a request for your regular Twitter credentials.

Steve: Uh-oh.

Leo: And then people of course don't look at the URL and get phished. I didn't fall for that. I did get the direct message, but I didn't fall for that. I know better than that. I look at the URL. And then but there was a much more serious hack a couple of days ago, and I got - I did get bit by that. A kid on the East Coast, he's 18 years old, he admits it - in fact there was an interview today with Wired magazine, or Wired News - used a brute force attack on an admin account. He had written his little tool that goes to the dictionary and tries every dictionary word as a password. An administrator at Twitter, Crystal, her password was "happiness."

Steve: Oh, goodness.

Leo: Kid went to bed. He didn't really know what Twitter was. He went to bed, woke up in the morning, he had access to Crystal's account. Now, he said I don't know what to do with it, so he went to a hacker forum and said, hey, anybody who wants access to Twitter and wants to change some passwords, go ahead, send me a note. Well, whose account would you like? Barack Obama was the first, of course. Fox News. Rick Sanchez from CNN. Britney Spears. So he gave these - he gave the credentials to these people. They logged in as Britney Spears, for instance, and put a lewd message up. Obama, everybody. Twitter caught onto it pretty quickly and deleted the bad messages and has reset the passwords. I lost access to my account, but I don't think anybody posted on it. I guess I was one of the people that the kids on the forum wanted access to, but they didn't - thank you for not putting anything stupid up there. And it wasn't till later in the day that I was able to get a hold of Twitter. And Crystal actually said sorry about that, here's a new password for you. But it just shows you, there were two things that they did wrong. One was that they had an admin who had a bad password, that dictionary word password. The other was they didn't have a timeout. You could continue to enter passwords until you got in. So his brute force tool had no barriers to continuing to hit at it. Terrible. I hope they pay a little more attention to security in the future.

Steve: Well, it's the sort of thing, too, that, I mean, Twitter began life not being that big a deal, and look what's happened. I mean, it's become a really big deal.

Leo: Right. And I think that's what happened is the kid who broke in said I didn't really know what it was. I never heard of Twitter. I just - I got in, I thought, oh, well, no big deal. What are they going to - who is, you know - he had no idea what a big deal it was.

Steve: Right.

Leo: Apparently the Obama campaign did contact the Twitter management quite rapidly, saying, uh, guys?

Steve: We've got to fix this now, yeah.

Leo: Yeah. And you have to wonder if somebody like Obama will be on a site like Twitter again, given the risk inherent.

Guillermo Garcia in Santiago, Chile doesn't want to give up and reformat. He says: Hi, I'm a long-time listener and a fan of the netcast. Currently I'm standing up a date, to date with past episodes. I'm sorry. Currently I'm getting up to date with past episodes. I just listened to Episode 172 about Sandboxie. That made me wonder if there really is anything to do when you get malware on your computer. Sandboxie prevented this, but what about systems that are already compromised?

I was listening to Leo on another one of his shows some weeks ago talking about how difficult it is to clean a system after it gets infected. I agree. I'm an IT person. I've been working with computers since my first 8088 many years back. I have some tools that I normally use when my informal clients, family and friends, get in trouble. But after all you've said I get the impression it's futile. Maybe Steve could comment on his tools and procedures for an effective cleanup. I mean, apart from the obvious but normally painful completely system format and reload, is there anything else I could do? Thanks for the excellent show. Please keep it coming. I'm glad he asked this. I want to ask this because...

Steve: Yeah. And the answer is no.

Leo: I got a call on the radio show last weekend from a guy who says I fix computers all the time, and I have tools. He's recommended a website with some tools. And he says I'm always able to get rid of everything.

Steve: He really did say that, huh.

Leo: He thought he was. I think it's a kind of arrogance or cockiness on his part, to be honest with you.

Steve: Yeah, I think so, too. I mean, as we've talked about this, I wanted to sort of reiterate. It's why I chose Guillermo's question is I've heard you, Leo, on the radio show,

tell people what I tell people, what I believe, is that it is becoming really increasingly difficult to get rid of these things. They are - there is so much technology now that is being brought to bear to make these tools impossible to find and impossible to root out, that there just isn't any sort of like a blanket solution.

Leo: Well, one of the things these guys do, they attach themselves to system files. So if you were to remove it, you're now deleting the system file. So now you have to make sure to repair the system file. If you can. It's just - it seems to me that there's two reasons. One is you'll spend - you could spend a lot of time trying to find everything, more time than it would take to just start over. Two...

Steve: And you'd never know.

Leo: You can never be sure, exactly.

Steve: You could never be sure. What I tell people is pull all your documents and files off, and then start again. And then put them all back on.

Leo: This has an advantage. It takes time, but it has an advantage. You've got a good backup.

Steve: Yes. And you also end up with a happier system. I mean, we all know that Windows systems sort of get corrupted over time. They just kind of get old. And so anytime you can start over and start fresh, you're not installing software that you installed once, but you never ended up using. It's sort of a chance to do some housecleaning. I mean, you might not choose to have spent your time that way. But I know of really nothing else you can do to be sure. I mean, these things now are so pernicious that they're just - there isn't a way to know that you got rid of everything. And so often we see examples of them popping back, that they appear after a few weeks of sort of going silent.

Leo: Plus I think that you are impacting the stability of your system long term because you've pulled things out, you've torn things out. You don't know what kind of impact that's going to have. And I just feel like your system's going to run better. You're going to be sure you got rid of everything. You're going to have a good backup. It's just healthful to do this.

Steve: Well, and I've also heard you talking about various imaging tools. We like Drive Snapshot.

Leo: Yeah, really great.

Steve: And to make a snapshot, then you've got your system in an easily recoverable mode that you can restore, and then do backups from that. So, I mean, there are now tools. And it's not like a second hard drive is that expensive any longer.

Leo: Right, right. Yeah, every time I install Windows in a new machine I make an image with Drive Snapshot. Then I make an image of all the applications that are installed. I get all the drivers, all the updates, so it's just nice. And that can be restored in 10 minutes.

Steve: Exactly.

Leo: Then you just restore your data. I mean, that's not a big deal. As long as you keep that snapshot up to date, I think that that's not a big deal.

Steve: Yup.

Leo: Jason's driving to Dallas. He's listening to our show, typing from an iPhone. This guy had to get this question in. He says: I'm listening to your latest Security Now! about SSL and MD5 being broken. It brought up a few questions. I thought, oh, no, as I'm currently using TrueCrypt on my laptop. I'm pretty sure I chose AES, but I'm not so sure. What does this mean for my whole drive encryption? Even if I chose AES, does TrueCrypt use an MD5 hash to help encrypt my drive? Do I need to reencrypt my drive? Is this vulnerability going to impact TrueCrypt?

Steve: No.

Leo: Yay.

Steve: Yay. Yes. AES is completely separate from MD5 and SSL and SHA-1 and all that. TrueCrypt just uses, I mean, TrueCrypt may in fact be using hashing internally to verify integrity of things. I wouldn't be at all surprised. But in no way does this mean you have a vulnerability because AES is so far completely unscathed in all of this sort of security research.

Leo: So it's related somehow? So that - is that why he was concerned?

Steve: No, I think it's just because he was - I think probably Jason is, when he's not typing on his iPhone driving to work, he's using TrueCrypt, and that's sort of his interaction with crypto stuff is through TrueCrypt. And so he was just wondering is there any impact on...

Leo: Other crypto.

Steve: ...his TrueCrypt encryption and anything else. And there is none.

Leo: Yeah. Jared Burford in Australia can't locate PayPal's one-time credit cards. I had that same problem, Jared. It was hard to find. But there may be another reason. He says: Hi, guys. I like the idea of using PayPal's one-time credit card number, but I'm not sure if it's worldwide. I checked at PayPal.com.au, but I couldn't find it. Is it only available in the U.S. and Canada? I currently have my savings set up for PayPal payments because I hate giving my credit card details to anyone, let alone to PayPal. But the use of this one-time pass might change my mind. Maybe I'm missing something. I had a hard time finding it.

Steve: Yes. And I think that's a problem. Unfortunately, it's sequestered under the main menu as "Plug-in." And so it's - they don't have, I mean, it's really dumb. I don't know why, but that's where it is. It's because it's sort of related to their plug-in, their browser plug-in.

Leo: But [indiscernible].

Steve: Yeah. So on the main menu you go to "Plug-in," and then you don't need the plug-in. You don't need to use or install the plug-in or anything because that's where then you can use the browser interface to create a one-time credit card number. So I wanted to let everyone know that's where they've hidden it. And it's unfortunate that they've hidden it because it's a super nice and useful feature. I don't know whether it's available worldwide. I assume it is. I can't imagine why it wouldn't be. But that's where it is located, Jared. So try taking a look under "Plug-in," and I'll bet you do find it.

Leo: Yeah. I mean, these are the kinds of things that maybe there are different features in the world. For instance, that football's not available worldwide, so...

Steve: Exactly.

Leo: Michael Kean, in Black Mountain, Australia - also from Australia - echoes the Hamachi death cries of many [simulating Hamachi death cry]: Hi, Steve. For the last three weeks, up until two days ago, Hamachi's mediation logon servers have seemed to be more down than up. They got sold to a company called LogMeIn.

Steve: Right.

Leo: Making it extremely frustrating and mildly embarrassing to use. See their forums for more. I thought I'd stumbled onto a good thing with Wippien, another similar program. Turns out to be particularly unstable. I could never work out why. Even four PCs on my own LAN would pop in and out for a smoke whenever they felt like it before hanging with 100 percent CPU two days later. So please keep thinking about CryptoLink. The world needs it almost like they needed SpinRite.

Steve: Well, I just - I'm absolutely - CryptoLink is the next thing I'm going to do, once I get caught up with my current little backlog of projects. And I did want to mention that,

because we did such a job of putting Hamachi on the map, unfortunately we may have been indirectly responsible for Hamachi's demise because Alex, who wrote Hamachi, sold it to LogMeIn. And unfortunately it's been having increasing problems ever since. They've changed the drivers, they've destabilized it, they've broken things. The server Hamachi depends upon tends to be unreliable. My own tech support guy, Greg, used to use Hamachi all the time and loved it, but began having more and more problems with it and has begun giving up on it. So for what it's worth, CryptoLink will be designed not to need any sort of third-party support like this, specifically for this reason. Because robustness and the ability to really get a connection all the time is one of my main focuses. So I'm definitely going to move forward on CryptoLink posthaste.

Leo: I'm happy for Alex. I'm glad he made some money off of it. But it's too bad that LogMeIn just can't seem to keep it going. Hamachi, we should explain, is kind of a virtual networking solution. But it does require a third-party, well, you can set up a Hamachi server of your own; right? Or does it need that intermediate third-party server?

Steve: I don't remember now. Of course it came up, but I think that Alex had not made it public at the time. And I don't think so now.

Leo: Oh, okay. So you have to use this third-party server to use Hamachi so the two machines could talk together. And if that server is down, you don't get a connection.

Steve: Right.

Leo: Ben Franklin - I'm sorry. Brian Franklin - Ben's brother - in Mesa, Arizona brings us this week's Brilliantly Obvious in Retrospect Idea of the Week. It's another YubiKey idea. Hi, Steve. On Security Now! Episode 176 you mentioned how the YubiKey can now be configured to spit out a static password for use with TrueCrypt - or as we mentioned earlier, with a WPA key, for instance.

Steve: Right.

Leo: However, if you only used the YubiKey's password, this would essentially be single-factor authentication. In this case, something you have, the YubiKey; right? It'd probably be worth noting you should use the YubiKey's static password as a supplement to your own password. For example, type your own memorized password. Then use the YubiKey to append to what you already have. Oh, that way you've typed - just like the PayPal.

Steve: Isn't that perfect?

Leo: That's a great idea. So on PayPal I enter my text password, and then I append to it the six-digit code that comes off the football. You could do the same with the YubiKey. This way you both get something you know, as well as something you

have, which would be next to impossible to know. I've been listening since Episode 1. Keep up the great work. I look forward to the release of your VPN and DNS utilities. And actually, if you're doing it for a router, you're already doing that because to get into the router's administration interface you have to know a password, and then you would use the YubiKey. So that's two factor on a router.

Steve: Correct. Correct. But in an instance, for example, like TrueCrypt, where they simply want a passphrase...

Leo: Right, much better...

Steve: ...the idea of adding your own stuff, either before or after you touch the YubiKey, I mean, that's perfect. It gives you two-factor authentication. That way somebody who gets your keys doesn't have access to your computer. Otherwise they would because they'd get everything they need to from your YubiKey. But this way you type your own little secret phrase, which no longer has to be incredibly long and complex because you're able to rely on the YubiKey to repeat the incredibly long and complex gibberish every single time.

Leo: Right. I just love that. I use - I told you my bank does that, Bank of America does that. They send a key to my cell phone, so I need my password and that key. I just love that. If Twitter had used something like that, none of this would have happened.

Steve: Right.

Leo: [Groaning] Everybody should get Yubico. And here's another YubiKey from Sean M. Taffert in Montreal. He has a lot of love to go around, apparently. He offers the PayPal Solution of the Week: Steve, let me start by saying thank you for just being you. I love Security Now!. I've been computing for 25-plus years. I'm always eager to listen to your podcasts every Thursday and to glean that little morsel of techno cool from every episode. I can't thank you enough for telling me about the YubiKey. Not only is it a great security gadget, they have to be the bestest tech support team ever. I had a small issue. They responded immediately, proposed a good solution, even gave me something to offset the trouble I was having. They were polite, to the point, and did I say this already, they have real people. I love Yubico. It's because they're Swedes. right? I just think they're nice people.

This all leads me to my actual point. I believe I've found a solution to the PayPal "I don't have my football" login security issue. We talked about this the other day. As you pointed out on one of your shows, the silly questions they ask are really not a great way to go around the fact you don't have your security token. In fact, they really open a big security hole. They eliminate really the value that you've gained from the token, I think.

Steve: Yes.

Leo: So I devised a scheme where you can select any of the lame-o questions they have listed. But instead of using correct answers or even incorrect answers, I use my YubiKey static password. This way nobody will ever guess the answer, and I can always change it once I get my football back from where I left it. Of course, if you lose your YubiKey, then you're really in trouble. Please pass this on to all of your listeners as a little extra secure way to use PayPal. And tell Leo I love him, too, but not in that way. Not in the way he loves you, apparently.

Steve: So I thought that was another good idea.

Leo: Yeah.

Steve: If they want to know your mother's maiden name, just have Yubico tell them, and god help them guessing that.

Leo: It really is - I love this YubiKey thing. It's just really cool.

Steve: Yup.

Leo: Really, really cool. Steve, we've come to the end of a great 12 questions. Boy, we have listeners that just - I love doing a show where the people who listen are thinking while they're listening. I mean, they really are thinking hard.

Steve: While they're driving and typing with one hand.

Leo: Yeah, whether it's to catch us out or to understand it better. I just think that's so cool.

Steve: Yup. I want to encourage people and remind people, I really do, we really do need and love their feedback, which they can provide at GRC.com/feedback.

Leo: Yes. Yes, absolutely. We also encourage you to go to GRC.com in general because of course that's the place where you get SpinRite, the world's best hard drive maintenance and recovery utility, a must-have for anybody. If you've got a hard drive, you ought to have SpinRite, as well. And by the way, than you for sending a key along, was it to Ryan Shrou? Who was it needed a key?

Steve: No, I sent a copy of SpinRite to Paul because he was having a problem.

Leo: Paul Thurrott, that's right.

Steve: Yeah.

Leo: Very kind of you. That's really nice.

Steve: Happy to.

Leo: I'm sure Paul appreciates it. We'll talk about it tomorrow.

Steve: Yeah.

Leo: Also there you'll find the show, the show notes, the transcriptions, the 16KB versions of the show, all of that stuff, GRC.com/securitynow. And when you're there, browse around Steve's free stuff. There's ShieldsUP! to test your router. There's Wizmo, that little gadget. I started recommending that on the radio show, Steve, because we get a lot of callers who say I can't get Windows to shut down.

Steve: Yes.

Leo: And that question we had a couple weeks ago, where the guy said, well, Wizmo did it, not only with the "shut down, dang it" command, but it fixed it permanently. I thought that was great.

Steve: Yeah.

Leo: So that's a great tool to have. And a lot of good security stuff.

Steve: I'm working right now on a DNS benchmark. I developed it actually back in '02, back when I was doing that experimentation with DNS. And it never went public. It was called DNSRU, DNS Research Utility I called it. And it's been like the secret favorite of a whole bunch of people in our newsgroups ever since. I mean, they, like, they keep using it even though it expired, and you have to hold both shift keys down when you start it in order to get around my little not-ready-for-primetime expiration timeout. Anyway, as part of this final DNS work that I've been doing, I decided we need to bring that back to life because so many people like it. So I should have another new utility here before long.

Leo: Well, thank you. I think it would be great to have a page of people submitting their - we'll do it in the forums - submitting their benchmarks for different DNS servers. We recommend OpenDNS. But compare it to your Internet service provider's DNS because, I mean, having a fast DNS server really speeds up your browsing. It's a good thing to have.

Steve: It really makes a difference. And so for example we've been talking about

OpenDNS. The question is, based on where you're located, are your ISP servers providing you results faster than OpenDNS? And I developed a bunch of technology where, for example, I'm able to independently show the cached versus uncached performance of DNS servers by server.

Leo: Wow.

Steve: And as far as I know, no one's ever really done a benchmark. So this'll be a cool little bit, new, a piece of new freeware from GRC.

Leo: Very neat.

Steve: Yeah. Next week we are going to have a great, I promise a fantastic episode, delving into the intricacies and exactly how this whole certificate chain system operates, so that if people listen, they will come away really getting it and finally not being more confused than when they started.

Leo: That I want to hear. But I guess I will. Because I never miss an episode. Steve Gibson, thanks for joining us. Great to see you. We'll see you next week on Security Now!.

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

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