Listener Feedback #156

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-381.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-381-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. He's going to explain that new, that breaking story about how it's easier than ever to crack passwords. Oh, my goodness. We'll also answer questions from our viewers and talk a little bit about an update on the Portable Bark Killer, or the Hush Puppy, as it is now known. It's all ahead with Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 381, recorded December 5th, 2012: Your questions, Steve's answers, #156.

It's time for Security Now!, the show that explains, helps you understand, and in fact helps you preserve your privacy and security online. And there has never been a better time to do that than right now, in fact. Fortunately, we've got our Explainer in Chief right here, Mr. Steve Gibson.

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

Leo: Good to have you. Here we are, another Wednesday. And, yes, yet another security flaw. It just never ends, does it.

Steve: Yes, we never run out of material. And I have to say that I'm getting feedback from our listeners who are, I would say, overwhelmingly, not without exception, but overwhelmingly do enjoy our divergences from the topic. We're not going to turn this into the Portable Dog Whistle Show or the TV Sci-Fi Review Show or anything. But I think people enjoy hearing what you and I think about things, sometimes when it's not about security. So I'm seeing the feedback from people. The response to the dog whistle project being brought back to life has been phenomenal. So we'll give it a little bit of

time. We'll keep the show focused on what it is. But I wanted to recognize that our listeners are enjoying us.

Leo: Well, of course. But of course, Mr. G. All right. Steve, I guess we should start with this. I saw it in Ars Technica. It was kind of the headline in Ars Technica today.

Steve: Yeah, it got a lot of attention. There has been for the last couple days in Oslo, Norway, a conference called Passwords^12. And during that conference there were a couple presentations from researchers that have upped the ante on brute-force password-cracking technology once again. One researcher, Jeremy Gosney - and if his name's familiar, it's because we've talked about him before. He's the guy who processed the 6.4 million LinkedIn password hashes that had leaked. He ran them against the most common password list. And, for example, that's where "monkey" was No. 14 or something.

Leo: It's my password. Ohhhhh.

Steve: It's bizarre that everyone was using "monkey." So, and I can't remember, there was some strange number that was also...

Leo: 123456789 is very popular because...

Steve: Yeah, this was a little odd that so many people would have independently chosen it. But very much like "monkey." But anyway, he demonstrated a "rig," as he called it, which leverages the Open Computing Language, which is OpenCL, framework. And a technology that he found after VMware disappointed him because he wasn't able to do sort of cloud-based sort of community computing with VMware, but an older project that had been around for a long time called Virtual OpenCL. It allowed him to essentially associate multiple 4U servers, equipped each with 25 AMD Radeon GPUs, which were communicating at 10Gb across an Infiniband switched fabric. Which is to say that he needed a large number of GPUs, graphics processing units, custom programmed for hashing. But the key, aside from having that many, was getting them to communicate, that is, bringing down the communication barrier so that they could coordinate their work. So he was able to do that using this Virtual OpenCL fabric. As a consequence, he was able to demonstrate far more potent brute-force password cracking than we've seen before.

So, for example, the maximum character length Windows XP password - he chose Windows XP as an example because it uses the older LanMan-style hash, where it has a 14-character maximum. And it's not very secure. That's the point of this. It converts lowercase to uppercase to at most 14 characters. And it actually, for some weird reason, splits them into two seven-character strings before hashing. So that reduces the amount of work that needs to be done. So only 69^7 hashes need to be performed. As a consequence of that, knowing what the algorithm is, it is now possible for this system and things of that scale to brute-force crack any Windows XP password in six minutes.

Leo: Any Windows XP password in six minutes. Do they have to have physical

access, I guess they would, to the machine...

Steve: Yes, so again, this is - to be clear, this is a so-called "offline" attack. So, for example...

Leo: You have to have a database or something.

Steve: Exactly. So if someone got your machine and got the hash, this reverses the hash, by doing a brute-force forward-going simulation of the weak LM, the LanMan, which is old, algorithm. So it turns out that, as a consequence, he's able to do the algorithm at 20 gigahashes, that is, giga attempts per second, and so it takes six minutes to try all of them. So, for example, if there was ever a database of LanMan hashes that got loose, in the same way that we see other hashes getting loose all the time, they're just toast. So there's one benchmark.

Another is the more recent NTLM, and that's an update on the algorithm. That's able to run at 348 giga attempts per second. So an NTLM hash takes about 5.5 hours to crack an eight-character password. So this really moves things forward. And SHA-1, he can crack those at 63 giga attempts per second. And MD5 at 180 giga attempts per second. So what we're seeing here, now, okay, these are old, weak algorithms. And so, for example, when we apply state-of-the-art password-based key derivation that we've talked about, for example, a thousand iterations of even something like SHA-1, well, now, we go from 5.5 hours to 5.5 thousand hours. So state-of-the-art approaches, if they're used, still provide us with substantial strength. So what we're seeing is we're seeing the core level of speed jump forward, almost sort of following Moore's Law, which is the famous law talking about the rate at which chips get small and processing power increases and so forth that Intel put forth years ago, and it's bizarre how well we've been following this curve of performance increase. Even when we keep thinking that we're hitting a dead end, we find a way around it. So anyway, that was one of the presentations.

The second one was from the developer of HashCat, which we've talked about before. That's the software that does very, very fast brute-force password cracking. The developer, who's Jens Steube, maybe it's Steube, he also demonstrated yesterday in Oslo a very clever optimization that he had designed for brute-forcing SHA-1 hashing. He's been staring at this, as the developer of HashCat he's looking at this, how can we make this faster? So what he realized was, looking carefully at the way SHA-1 works, in any situation where you are going to be running many closely related inputs through SHA-1, there's a lot of it, if you were to do them independently, which is being duplicated in the algorithm.

So he realized that, by taking sets of input brute-force tests and looking at the way they run the hash the same, he could do a precalculation one time to cover that group en masse and produce a 21 percent improvement in performance. So he shaves 21 percent off the time required to crack large numbers of passwords, essentially. So this is just - this is, again, this reminds us of Bruce Schneier's comment that attacks never get worse, they only get better. Or maybe that is worse. Anyway, they only get faster.

Leo: They only get better faster, yeah.

Steve: So, yeah. So again, this is nothing to run around and worry about except for any sites that are still using old strategies. For example, the Windows XP operating system itself is by definition using a very old strategy since it's so old. But websites that are just doing, for example, one SHA-1 hash, and also allowing those hashes to leak out onto the 'Net, well, they're just toast now. I mean, that's just like not - it's a no-brainer. If anybody who wants to grabs a database of SHA-1 hashes, they can be brute-forced so that, I mean, it's just like cutting through air. It's not a problem. So it really does take - now, this does say it's increasingly important for people to do password-based key derivation, that is, thousands of iterations on this. And we know that iOS does now. We know that LastPass has been now for some time. Although, if you're an older LastPass user, they haven't changed that for you. So you do need to go in and turn that on, which is a transparent change, and that's, again, for this sort of reason, definitely worth doing.

And you and I mentioned briefly this note that you had encountered before we began recording. But I thought this was important for our listeners to hear. An Australian man, William Weber, was recently arrested for running a TOR - that is, TOR is the acronym for The Onion Router - a TOR exit node. The police raided his home, where he had seven TOR exit node servers running that were piping terabytes of data back and forth daily. They were seized, and he was arrested for trafficking in child pornography. So what had happened was that users of TOR were leveraging the anonymity which TOR, by design, creates. And remember that TOR was designed by the U.S. military. It was a U.S. Naval Research...

Leo: Oh, I didn't know that.

Steve: Yeah. It was the U.S. Naval Research Lab that designed this. And for listeners who don't know about TOR, that is, people who have come in in the last few years, we have a podcast where we very carefully explain the technology, and it is way cool. It's called an "onion router" because it was named after onions that are made of layers of, you know, onion. And we've all heard the expression "peeling the onion," "peeling the layers off the onion."

So the idea is that, as traffic moves through a cloud of TOR nodes, from one TOR node to another, as the traffic - you plot the path that you're going to take before you send traffic into the TOR cloud. So you say, we're going to go to this server, this server, this server, this server, this server. You then get the public keys of each of those servers, and you prepare a packet by successively encrypting your data in the sequence, actually in the reverse sequence that you're going to be traversing. And each layer only knows about the next jump it's going to make.

You then put this packet into the first TOR node. That server has - it's only able to decrypt its layer of the onion because it has its private key that matches the public key which it advertises. So it takes that layer off, and then it looks at the next layer, which instructs it where to send this somewhat smaller onion module, and it sends it to that node. That node - oh, and by the way, this server cannot decrypt what's in the onion because it doesn't have the next node's private key. All it can do is forward it. Anyway, if you want more, check out the podcast we did on TOR, on The Onion Router [SN-070].

Leo: But I guess the point is it's designed to preserve anonymity, not security. It doesn't replace a VPN. But it anonymizes incoming and outgoing traffic.

Steve: No, it replaces a VPN even better than a VPN does.

Leo: Okay, okay. But it's encrypted traffic.

Steve: Yes. And so the point is that people...

Leo: Is it encrypted to the TOR?

Steve: It's encrypted, and its path is encrypted. And so the whole idea is that there is no way to find out who's at the other end. So what happened in this case is that authorities saw child porn images going through the Internet, and they saw where they were headed. They were headed to William Weber's living room, or wherever he has his seven TOR nodes. And so they said, oh, this guy is trafficking in child pornography. Well, he's not. The so-called "exit node" is, at the end of all this jumping around inside the TOR network, at some point it needs to emerge onto the Internet, after having jumped around enough to confuse everybody so they can't figure out where it actually came from. And that's the point. This really, really does work in hiding who is actually behind the requests which emerge from the exit node. So somewhere back at the beginning of that traffic was somebody who actually was trafficking in child pornography, or going to servers that made the stuff available, but they were using TOR to hide behind, to hide their identify. And it works. It does that.

But the point is that at some point it needs to emerge onto the Internet in order to go, I mean, whatever. It's certainly useful for many other things. I mean, you know, for free speech advocates. This was designed by our government, the U.S. government, because they wanted to hide their own footprints and be able to poke around on the Internet, and having there be no way for it to be traced back to them. So, I mean, this is - it is world-class strength anonymity. But as always is the case, it can also be abused.

And so there were criminal abusers using TOR to hide. But the authorities didn't understand what was going on. In fact, Mr. Weber said he was - he said after the raid he was interviewed by police who, he said, became, quote, "more friendly," unquote, after he explained how TOR worked, and that he was not responsible for what people did via the TOR anonymizing system. And he said he had kept no log files. Well, frankly, log files don't help. I mean, nothing helps. This system really does work for hiding the identity of the people making the requests. This is interesting, of course, for us because it does demonstrate something that I've always been concerned about, which is exit nodes are potentially vulnerable to, if nothing else, to misunderstanding of this sort, but also to this kind of unfortunate exploitation of the anonymity. I mean, because the anonymity TOR provides is, I mean, absolute. It really does work.

Leo: So is he off the hook?

Steve: No. In fact, he's appealing now for donations to help fund his legal defense and establish a legal precedent which would help protect other operators of TOR exit nodes from similar police attention. And he faces a lengthy prison sentence if found guilty of distributing images of child sex abuse.

Leo: Hmm, interesting.

Steve: So, I mean, he's in trouble.

Leo: Yeah.

Steve: Yeah, this sounds like the kind of thing where the EFF will step up and say, okay, we agree, you're not a bad guy, and we'll help explain this to the judge.

Leo: Well, if not, nobody will ever want to run a TOR node again.

Steve: Well, and, now, you mentioned VPNs. Because, as you know, they're similar. This has been a concern, I mean, this should be a concern of anyone who offers a VPN service because a VPN does, it's much less exotic, but very much the same thing. When you use a VPN, your traffic is encrypted. It goes to the VPN server, that is, the other endpoint of the VPN, which then decrypts the traffic traveling through that tunnel and typically releases it onto the Internet. So you would use a VPN, for example, at a Starbucks that has unencrypted WiFi in order to prevent your traffic from being sniffable until it got to wherever the VPN server was. Then it would decrypt it, and off it goes.

So again, if you were doing something illegal or questionable, or if you were thinking this was giving you anonymity, a VPN actually doesn't give you much anonymity because it's very easy to watch the VPN server and get the IP of where the encrypted traffic is going. That's specifically why TOR was created, and this so-called onion approach of multiple hops through the network, which, by the way, does slow the traffic down a lot. I mean, it's not for real-time sorts of things. It's just way slow. But what you get in return is anonymity. But again, a VPN server runs the same kind of risk because it's the IP that the authorities would see on the public Internet for all of its customers that are using it.

So again, at this point it's a problem for the law to understand the kind of things that William Weber is trying now to explain to the police, in that he's offering a service. And you can imagine, I mean, they're saying, well, why? Are you making money? And he says no, I believe in freedom of speech on the Internet. And they think, yeah, uh-huh, and child porn is moving through your living room as a consequence. And he says, well, freedom of speech can be abused, but it's also a power for good.

Meanwhile, following our interesting trail of John McAfee, something that - I just love the irony of this. John's location leaked a couple days ago. And I saw some people commenting that it was just due to pure ego. But a magazine called Vice.com, their headline was "We are with John McAfee right now, suckers." Meaning they were, like, poking at the authorities that were unable to find John. And they're saying, "We're with him right now."

Leo: Yeah, because he granted them an interview.

Steve: Yes, he granted them an interview. So they take a picture of John standing next to the reporter in a setting where his location is not obvious. So from the image in the

photo, you can't tell where he is. Then they post this photo on their website with great fanfare. And a hacker says, huh.

Leo: This is so stupid. I can't even believe how stupid this is. Okay.

Steve: I know. Grabs the photo file off the server and takes a look at the metadata containing the GPS time and position...

Leo: How stupid.

Steve: ...of exactly where and when the photo was taken.

Leo: Stupid.

Steve: So, I mean, you would imagine John, who's tech savvy...

Leo: I think he's moved by now.

Steve: Well, yeah.

Leo: He's in Guatemala now, is the latest.

Steve: He initially obfuscated when this first arose, the idea that he had been outed by the photo which was taken of him. Then the next day, after I'm sure he had relocated, he said, well, yes, that did happen. And it wasn't his camera phone, it was the photographer, who had "track me and post my location into the metadata of everything I do." It's like, whoopsie. So, yeah. I thought that was sort of interesting.

And, wow. Really interesting news about flash memory. A Taiwanese company appears to, I mean, seriously appears to have solved the "where" problem of flash memory. We've talked about this often, that, I mean, it is what's been holding flash back, so to speak, is that it only can be written to about 10,000 times. Now, that's fine for a little thumb drive that you carry around with your files on it, if you actually do the math, how many days that would last for 10,000 rewrites. And when you also then consider that the flash memory, as a consequence of the fact that it tends to wear out, has all this so-called "wear leveling logic." That is to say that the problem of flash wearing out has been dogging it forever.

It turns out that it's been known that the process of so-called "annealing" - that is, annealing is heating up the memory - annealing cures the wear problem, but that requires hearing it up. It's been believed that that would prevent it from being used practically. But it turns out that these guys at Macronix, which is the Taiwanese company, they took some tricks from a different type of technology which has not yet made it to the world called "phase change" technology, where phase change actually changes the structure of a type of glass. It does that by producing spot heating,

essentially. They took that concept, and they designed an architecture of a flash memory that allows milliseconds of local heating to about 800 degrees C. Now, this is not the whole chip. This is a microscopic little region of the chip is resistively heated in order to remove any problem with memory.

And we've talked before that the problem is essentially the way flash works is you have an insulator, and you use high voltage to drive electrons through the insulation. Essentially you break down the insulation by using a voltage. And we know that voltage is pressure. Essentially you just pressure the electrons to squirt through the insulator, and you strand them out on a little island. And then the way field effect transistors work, that's the field that they're being affected by is the charge on this little stranded island. And that's how the memory works.

So the problem is, in the process of squirting these electrons through an insulator whose job is to resist that, the insulation begins to break down. And after about 10,000 - and that's why there's a problem with write endurance. There's no problem reading because reading is nondestructive. No electrons have to pass through the insulator. It's when you are charging or discharging that little floating gate that you're doing so by deliberately breaking down the insulation. Well, it turns out that briefly reheating it fixes it. And, I mean, fixes it completely. So whereas a normal flash cell has about a 10,000-cycle life, they haven't found any deterioration after 100 million cycles.

Leo: Wow. So, what, do you have to put a little heater coil in the NAND?

Steve: No, it's actually - you distribute these little heaters, you actually integrate them right onto the chip.

Leo: How weird.

Steve: So there's millions of those spread around the chip. And the idea is, while it does take energy, this would be done, for example, while our smartphones are plugged in and with energy available charging the battery, or when our laptops are plugged in and having their battery recharged.

Leo: Is it destructive to the content of the cell?

Steve: I don't know. But they can certainly copy that region...

Leo: Oh, they can copy - just what you do with SpinRite, in a way, yeah. Yeah.

Steve: So it goes from 10^4 to 10^8. So 10,000 10,000, essentially. And that's not like where it ends. They're saying that they've gone a hundred million cycles, and they have found no change. So this thing, this may be a revolution in non-volatile, non-spinning memory technology. So it's very exciting. It's funny...

Leo: That's exciting. That's great.

Steve: ...because I tweeted the link to the story this morning, and one of our listeners, or at least a follower of mine, @barsteward - his description on Twitter says "lapsed physicist, coder, dad, standup comedy junkie, inappropriate sense of humor (according to my boss)," he says. So he wrote: "@SGgrc Heating redistributes the imperfections that allow stress-induced leakage current through Fowler-Nordheim quantum tunneling."

Leo: There you go.

Steve: And I thought, well, obviously.

Leo: You're sealing off the tunnel. Wow.

Steve: Yeah.

Leo: So it's re-chaosing the substrate.

Steve: Yeah. And, I mean, it makes absolute sense.

Leo: That's what I'm going to call it.

Steve: Leo refers to it as "re-chaosing." That's good. Yeah. But, I mean, this is huge. It'll take a few years, probably, for this thing to hit. Maybe not even that because, I mean, the flash memory technology is mature. They have to then print a layer of heater on top. But this is good news.

Leo: That's really interesting. Wow.

Steve: Yeah. Also a listener of ours, Andrew, who has the site AndrewTechHelp.com, he posted a nice - or sent me a tweet about a page he had put together about how much easier it can be to disable Java in IE8, 9, and 10. And that's just by using the built-in add-ons panel. Remember that I think it was Brian who posted - we referred to Brian Krebs' page where he had instructions, and we commented that, oh, my god, almost the entire page was taken up in registry changes...

Leo: All for Windows.

Steve: Yes. And so it's obvious in retrospect that you can just change the add-on settings in IE to turn off Java. So anyone who's interested can find - you can probably look at AndrewTechHelp.com, and I imagine you'll find his blog post. Or look at my

Twitter feed because I just tweeted it for everyone who's interested, which of course is Twitter.com/SGgrc. And I got a kick - I got a piece of feedback from Kyle Cronin, who said: "@SGgrc Best method of securing Java: Control Panel > Uninstall Programs > Java > Uninstall." It's like, okay, yeah, right.

Leo: So that is true.

Steve: But then someone said, hey, how do I know if it worked? And I realized, I have at GRC an absolutely safe Java applet that anyone could try. I have a Big Number Calculator which I use for doing work on big crypto numbers. It's just under "Other," I think, off the main menu at GRC, and then you'll see Big Number Calculator, or it's also GRC.com/big-number-calculator.htm. And that's a little, I mean, that's a nice, well-behaved Java, not JavaScript, Java applet. And if it doesn't work, that's good because that means you don't have Java available to your browser, which is the problem. It's fine to have it installed in your computer. It's just you don't want web pages to be able to get to it unless you know that they need to. And of course NoScript prevents this from happening unless you give web pages permission, as well. So that's also a solution.

Leo: Great. Great, great, great.

Steve: A couple bits of miscellanea. I tweeted a really neat link to a YouTube video. This was a recent production by BBC News. The WITCH computer from Bletchley Park, which was one of the very early sort of electromechanical computers, was found in a warehouse, and it has been - all the pieces put back together. It's been restored and is now working. And so there's...

Leo: Now, explain what this computer did. Bletchley Park was where Enigma was solved; right?

Steve: Yes. And this was apparently around atom bomb R&D time.

Leo: Ah, interesting.

Steve: So there was code breaking. And that's what Alan Turing was so involved in, was machines for automating the process of breaking German codes. But so I'm not sure which aspect of what Bletchley Park was doing the WITCH computer was used for. But anyway, it's fascinating. They have these bizarre things called "dekatron tubes." This was a decimal computer rather than a binary computer. So these dekatron tubes - and you can look up "dekatron" on Wikipedia - they're actually decade, that is, 10 counting units. And so you could feed pulses in, and they would move, like, a neon glow around the tube and then send a pulse out when it went back to zero. So it's just like a decade counter. And so this thing operated by very rapidly shooting thousands of pulses in, and this would accumulate them and allow them to be read out and function as memory. Anyway, this YouTube video, I also tweeted that, or you can, I imagine, find it on YouTube. And I ran across this thanks to Nathan Ramsey, who had this in our feedback email that I saw.

And I just did want to mention, Leo, I had here a note to tell you, yet again, how amazed

I am by "Homeland," the series on Showtime.

Leo: I told you first.

Steve: You told me first, yes.

Leo: I am really - now, I've finished the first season. I know the second season is already almost done, actually.

Steve: We have two episodes left in the second season.

Leo: So it's a Showtime series. So if you don't get Showtime, you're out of luck. But it is - Claire Danes is fantastic in it. And what's the other guy, Damian...

Steve: I don't know, but he's equally good.

Leo: Is it Williams? What is his name now?

Steve: Oh, wait. You would have seen the interrogation scene.

Leo: Now, don't - no spoilers.

Steve: No, no, I won't. But you did; right?

Leo: Yeah. Yeah. Damian Lewis, that's his name. Thank you, Punchy. Yeah. Very good. Very good, yeah. And you know who actually doesn't get as much credit as I think he deserves is Mandy Patinkin, who is in it, as well. He's the guy who has said, "My name is Inigo Montoya. You killed my father. Now prepare to die." Not in that show. In another show. Another movie. Another movie. But he's a - what's funny, he's a - "Princess Bride." He's a Broadway singer, you know, performer, who is really best known as a singer, who's just a great dramatic role. He's playing Saul.

Steve: Oh, Saul. Oh, my god, yes.

Leo: Saul's great.

Steve: Yes, fantastic role.

Leo: Yeah, yeah, love that.

Steve: And I also did want to mention that I saw the news that another series I've been enjoying, and I know that our listeners have a strong following there, and that's "Fringe" on Fox. It's had a really interesting run. But they're not going to let it go forever. And in fact the last episode is rapidly approaching. On January 18th of next year, so not many more, will be Episode 100, and the end.

Leo: A hundred episodes. Wow.

Steve: Yeah.

Leo: So that's been going on for some time. That's, like, eight years.

Steve: Yeah. Oh, and, god, Walter and, I mean, just - it's, again, I've really, really enjoyed the series. It's strongly character driven. And of course we know that Leonard Nimoy is one of the sometimes-seen characters. They kind of brought him back, dusted him off, in order to show him. Oh, and speaking of which, there's a trailer for the next Star Trek movie is apparently going to be out, I think Thursday it comes out. So...

Leo: Is he in it?

Steve: No. I don't - oh, I don't know.

Leo: But is this going to be another...

Steve: It's following from the new cast...

Leo: The reboot.

Steve: ...that we, exactly, that we just...

Leo: I really enjoyed the reboot.

Steve: It was great.

Leo: Yeah.

Steve: Yeah. And, finally, the dog whistle project, also know as the PDK, although I cringe every time I think...

Leo: No, no dogs are killed. You know, we decided you should call it the Portable Bark Killer because that's really the point of it, is not to hurt the dog, but just to stop the barking.

Steve: Yeah, I mean, even the original device was - it was meant to be a trainer so that this rabid creature in the neighborhood when I was 15 would stop attacking people who were walking past.

Leo: Bothers the dog less than a swat with a newspaper or a yank on the choke chain. In fact, it's really no different than yelling at the dog in a surprising way.

Steve: Yes, exactly. So I did want to mention that the project is moving forward rapidly. I've posted the schematic for the amplifier on the 'Net. This is actually the entire electronics package I'm holding up to the camera. But for those who don't have video, I've got links in the Google Group, which is just, if you Google "Portable Sound Blaster," which is what I named the group a year ago last summer, you'll find the group. I'm really unhappy with Google Groups, by the way, Leo. It just is - you can't edit posts.

Leo: It's abandoned, I think. I don't think they're using it anymore.

Steve: I'm very disappointed. We need to organize a community somewhere else because it's just not - it's just annoying. But so I've got the amplifier built. The schematic is done. I will have one in hand, like, almost, I'm just, like, hours away from the first handheld prototype. An amazing number of people have expressed an interest. So I want for everyone to rest assured that as soon as I can...

Leo: I like this. Now, the bottom of the schematic there's a name that I really like.

Steve: Yeah, I do, too.

Leo: Have you trademarked that yet? Well, I guess somebody else has the trademark.

Steve: It's not - actually it's Hush Puppies is trademarked. The singular have all expired.

Leo: Hush Puppy. Wouldn't that be a good name for it?

Steve: It's a great name for it. So I'm just calling it...

Leo: The Hush Puppy.

Steve: The Hush Puppy Electronic Dog Whistle. So I wanted everyone to know, one way or another, your needs will be met. I will do it. Everything's going to be open for the project - the software, the schematic, the parts list. It looks like it costs about $10, so it's not an expensive thing. The design...

Leo: That's not including speakers, though. That's just the board.

Steve: Nope. Speakers $2.

Leo: Really. Doesn't take much to hush that puppy.

Steve: They're $2. You can a pair of them for four bucks with free shipping on Amazon.

Leo: Oh, man.

Steve: Yeah. So it's...

Leo: Maybe we should do a know-how on this, and you could be our special guest. I'm going to talk to Iyaz. Because, you know, we do a show, half-hour show on exactly this kind of stuff, building stuff and...

Steve: Well, you know, and I heard him mention the Arduino.

Leo: Yeah, we just did an Arduino.

Steve: And anything that produces a square wave can drive the little power amplifier that I designed. This power amplifier, it turned out to be sort of amazing. It's five components. It takes a 6v DC from four AA cells or AAA cells and turns it into an 80v near sine wave across the tweeter. And it's almost a hundred percent efficient. So it's turned out really well. But what I wanted to say was, for people who can build things, everything will be provided for you to be able to build one. I expect that there will be enough people who really have a need who are not construction people that they'll say, I've got a barking dog, my neighbor has a barking dog, I really, really want to try this. What I want is feedback about how well it works so we can see if it's useful. And so I'm willing to build some number of these and provide them for free in return for feedback. So...

Leo: And pictures of dogs with their tails between their legs.

Steve: Videos, I would love videos of dogs' reactions. So anyway, so I'm just - I'm doing this as quickly as I can. I'll get the pages up. There will be one of our standard sort of feedback-style pages where everybody can explain who they are and what they want. I'll get a sense for the size of the audience, and we'll move accordingly. So anyway, it's all

happening. And, oh, I should also mention that - I mentioned that this was based on the Texas Instruments MSP430. There's a development kit called the LaunchPad which TI sells for $4.30. Several of the people have posted over in the Google Group that they ordered a couple, and they came, like, the next day. One guy said he ordered it on November 30th, and it came on December 1st. So that would be next day; right? Because November only has 30 days?

Leo: Yeah. 30 days, yeah.

Steve: And it came FedEx Express. So, like, the shipping clearly cost more than he even paid. So they really are $4.30.

Leo: That's great.

Steve: And I'll have a design using those chips that are included in the LaunchPad to drive this amplifier. So anyway, right now everything is over on this Google Group, which I am not liking. I will be moving all - I'll have the whole deal laid out on GRC.com as soon as I can get there.

Leo: Good. Good, good, good.

Steve: Oh, and I almost forgot, while I was going through the mailbag I found a note from November 26th from a Shawn Milochik, who's a listener of ours. He's in Reading, Pennsylvania.

Leo: Reading.

Steve: Reading, oh. And the subject line caught my attention. He said, "SpinRite fixed my drive, and nobody cares."

Leo: That's true.

Steve: And I thought, well, I care.

Leo: Oh, yeah. Steve cares.

Steve: I care. So I thought, okay, what? And I opened the note, and he says, "I came back from my Thanksgiving vacation to find a boot desk error on my work computer. The computer booted properly from my old hard drive, and the bad drive mounted fine as a secondary drive. So I ran SpinRite on Level 2. I canceled it 10 percent of the way through, assuming that something causing a boot error would be near the beginning of the drive. Sure enough, now I'm back to work, and nobody really noticed or cared. That's how recovery should be. Thanks for SpinRite. Licensee since 2006 and Security Now!

listener since the beginning."

Leo: Aw, that's great.

Steve: So Shawn, thank you very much for sharing your story. And we all care.

Leo: So, let's do a Q&A. What do you say?

Steve: Oh, what - is that why we're here? Oh.

Leo: Well, it's not why we're here. No one knows why we're here. But...

Steve: All of our listeners keep telling me, don't ever stop. No matter what you do, do not stop.

Leo: It's fun. Oh, no. In fact, I was talking to Iyaz yesterday. He was a little toasted, so I don't know if he meant it. But he said that...

Steve: Merry Christmas. Must be the company Christmas...

Leo: He said, "Leo, I love doing Security Now!. I love it." He enjoys it. He says sometimes, though, it's a little hard to understand. I said, oh, don't think I understand everything Steve's saying. You've got to listen carefully and do your best.

Steve: Well, now we have Tom moving to L.A., I have a feeling that Iyaz will be inheriting the role.

Leo: More of Iyaz, yes.

Steve: Hanging out when you're off in - where are you going, to Greece for half a year or something?

Leo: That's not till September. And I wish it were for half a year. I wouldn't mind that.

Steve: You'd be here no time.

Leo: I'll be there three weeks. September, I think, 17th we leave, and we come back

in October. But I decided to start planning early this time because this way...

Steve: Planning is good.

Leo: Yeah, this way everybody will know why we're not here. All right. I'm looking for your questions. I think you sent me two copies of the notes.

Steve: Uh-oh. I don't think so. The title is very similar-looking.

Leo: They are. I got it. I got it. I got it. I got it. Eight great questions and answers, starting with Sao Paulo, Brazil.

Steve: Oh, actually it's 10, but I forgot to change the number at the top.

Leo: Eight, 10, whatever.

Steve: Okay. We'll go until we run out of time.

Leo: Michael wants to know: First of all, I'd like to thank you for the amazing show. I've been listening for over four years. I've learned a lot. Do you have any updates on Cloudberry? This was a new cloud service that you mentioned a couple of episodes ago. Should I keep using Jungle Disk? Or is it time to move to Cloudberry?

Steve: So my feeling is that, if you're a Jungle Disk user, and it works for you, then why not keep using it? Cloudberry has additional advantages. My vetting of the security came out as full TNO, so it passes all of the Trust No One tests. They are encrypting things absolutely correctly. I mean, maybe a little overkill, but that's, as we know in security, that's a good thing. I was a Jungle Disk user so long ago that I got, like, the lifetime for free deal. And I remember that they then terminated that. And so Cloudberry is a pay only once, and it does also support the super inexpensive Amazon archival bury-it-in-ice technology, Glacier.

So I could see a switch making sense and, like, leaving Jungle Disk behind if Jungle Disk are themselves charging you periodically for the privilege. Cloudberry charges you one time, which is, I think, the right model for this. And then using Glacier you can really, really save on your data storage. And Cloudberry is also multi-cloud. Glacier is only one of a huge number of cloud services that it supports. So I haven't yet switched myself over. But I'm going to do that, just for what it's worth. I think it's the right solution. So, yes, Michael, it probably does make sense.

Leo: Cloudberry. I love the name. Tom Callahan, Cincinnati, Ohio, settled the issue once and for all, darn it: Steve, I know you have a problem - I don't know if it's you. A lot of people have a problem with using the term "reading" when listening to an

audiobook. I get messages all the time because I always say "reading" when I'm doing the Audible ad because I feel like it's reading a book. And I had one guy say in the chatroom, "You know, those of us who are neuroscientists really are irritated." And I thought, you're not a neuroscientist. But anyway.

Steve: Well, Tom, I think for everybody listening to this, Tom may have...

Leo: He's going to flatten it?

Steve: I think he is.

Leo: All right. But if reading is only something you do when looking at a book, then what is it blind people are doing when they "read" a book in Braille?

Steve: Hmm.

Leo: Hmm. They're feeling the book. Touching the book.

Steve: Well, the point is, what we're saying, clearly somebody using Braille...

Leo: Is reading.

Steve: I would agree they are reading the book with touch. Which says that it's not which sense you use for input that matters.

Leo: Right. Exactly.

Steve: You use your eyes for input when you are reading visually. You use your fingers for input when you are reading Braille. And you use your ears for input when you are reading an audiobook. So I can't argue that.

Leo: Now, if I look to Wikipedia - and as you know, I always do - it says, "Reading is a complex cognitive process of decoding symbols" - so this would apply both to reading with your eyes and your fingers - "in order to construct or derive meaning."

Steve: But audio symbols, those are symbols, too.

Leo: Are those symbols?

Steve: Yeah, they really are.

Leo: I think it's like pre-chewed food.

Steve: Well, here's the problem. Somebody read the book in order to read it to you.

Leo: Yes.

Steve: So somehow it's been read twice.

Leo: That's what I'm saying, it's pre-chewed. This is interesting. This actually is a good article. It's clearly about kind of the neuroscience of reading. "Other types of reading are not speech-based writing systems such as music notation or pictograms." Yeah. I don't know. I mean, I think the Braille example is a good example.

Steve: Yeah. I just thought, oh...

Leo: Depends on how you define "reading," obviously.

Steve: Well, yeah.

Leo: See, I don't define "reading" as a "complex cognitive process of decoding symbols in order to construct a derived meaning." I say it's the process of ingesting writing. And you ingest writing. You can ingest it...

Steve: And under that definition, Leo, I think we all agree.

Leo: Yeah. I'm ingesting a book somehow. Adi Khajuria...

Steve: And more importantly, Henry is, too. And so that's...

Leo: Yeah, he likes audio books because he has ADD, as I think all of us now in the tech industry have acquired ADD, or AADD.

Steve: Wait a minute, something just came in my Twitter feed. Hold on.

Leo: Acquired attention deficit disorder. But he says after a page I lose interest and start staring out the window. But audio books I can absorb. And he listens intently.

Steve: Well, he can stare out the window and read the audio book.

Leo: Well, and it's obviously some mechanical thing in the brain where the process of reading is hard to hold his attention, but he can listen to something. He's like me. I'm an auditory learner, as well.

Steve: Well, and I have to say also, there was a server at a restaurant where I was having breakfast a year ago who attempted to read out loud something which I was reading, but then it was time to eat my breakfast. And so he picked it up and continued to read it. And it was clear that I read effortlessly something that is written, and he was not an effortless reader. It was still work for him to turn that printed word into something that meant something. Whereas listening to it really drops the barrier. Obviously, you're a good reader. But you use audible reading for convenience. You can do it while you drive, and they won't arrest you.

Leo: Right. And, you know, somebody said, what about music? If you read music and play it, and then the person listens to it, you're not both reading the music. There's somebody reading it, and there's somebody listening. I guess that's true with an audio book. There's somebody reading the book. And I am an audio book listener. So I don't know. I understand the issue. I do.

Steve: And now we've completely done nothing with the topic.

Leo: It's way too much, yeah, way too much. Way too much.

Steve: We've made no progress.

Leo: There's no point of so much effort on this simple topic. But, you know, that's why we're geeks. Geeks obsess. Adi Khajuria in London, U.K., wonders about TNO web browsing: Steve and Leo, I've decided enough is enough, and I want to go TNO - trust no one - with my web browsing by using a VPN. I'm going to - we got acronym crazy here - virtual private network. With that being said, are there any free VPNs that are reputable and TNO? I know that TOR is TNO. TOR is the onion router we talked about earlier, is trust no one. I know it's not a VPN, but it is TNO nonetheless. I was wondering if there are any others out there. I'm on a Mac running Mountain Lion. RAWR. He actually writes RAWR.

Steve: He did.

Leo: Yeah. I also have a Windows laptop which I use on rare occasions using XP. [Indistinguishable sound] I put that in there. Kind regards, Adi. Hmm.

Steve: So, okay. I'm not sure from what he wrote what he wants. He says, "I've decided that enough is enough and wanted to go TNO with my web browsing by using a VPN." Now, okay. A VPN, as we did discuss earlier, it encrypts your link from Point A, where

you are, to Point B, where the VPN server is. So it's the transit between those two endpoints which is encrypted. But once it arrives at the other end, it is decrypted coming out of the so-called "tunnel," the encrypted tunnel, and then it either comes to you, or it goes out to the Internet. So a VPN can be used to hide your location, that is, people out on the Internet will see the IP of the traffic as that of the VPN server, where it goes into the server to be encrypted, and then come to you. But as we just saw by talking in depth about the onion router, that really doesn't provide identity or location protection, whereas the onion router does because it's easy to see. It's easy, once you get to the VPN server, to see where its incoming traffic is being routed to.

And so he says "enough is enough" and wants to "go TNO with my web browsing." So I'm also thinking maybe what he's really thinking is identity being tracked and followed and so forth. And of course that's about the storage of information, of state information, typically about his computer or about his browser so that, when he appears at other websites, he can be reidentified as somebody who was also somewhere else earlier. So that's generically called "tracking," where as he bounces around the 'Net his location is tracked because there's some sort of identifying tag on him, on the events that he puts out onto the Internet, that allow him to be tracked down.

So neither - I don't know. I'm sure the onion router must do anonymizing of your traffic, although it's mostly meant for making you untraceable. It probably does header stripping and things. Frankly, it's been so long since I looked at it. But I'm sure that we discussed it in our onion router podcast that we did previously in detail. So anyway, I just wanted to sort of explain what Adi was asking from the context of, well, I'm not quite sure what it is he's trying to achieve, but simply VPN doesn't do it. And I don't think there are free ones. There are free trials.

Leo: Oh, there are free VPNs, yeah. They're not very good.

Steve: Yeah, I was just going to say, that's the problem is that you get what you pay for.

Leo: Yeah. They don't put any bandwidth behind it or hardware behind it.

Steve: Yeah. And normally they're like, here, try this for free. And if you want better service, then pay us. There's one, like, HotSpotVPN...

Leo: That's the one I use, and I love that. Now, for a hundred bucks, you get Hotspot, a year of HotSpotVPN, and they give you a free little device, it's really awesome, that's a WiFi receiver firewall that has HotSpotVPN built into it. So you put it on the Velcro on the back of your laptop. It goes by Ethernet into your laptop. It picks up the WiFi signal.

Steve: Wherever you are.

Leo: Wherever you are. Blocks, does the firewalling, but also then connects you, without any - you don't have to do any configuration or software on your computer -

connects you to your account at HotSpotVPN. So I really like that little - it's not too big, either.

Steve: Not free, but I think it's $8.88 a month is what they quote.

Leo: Yeah, right. But I would highly recommend doing the $99 a year deal, if you think you're going to do this, because you get the hardware and HotSpotVPN, makes it very, very easy.

Steve: Right.

Leo: What was the one everybody was using during the Olympics? The chatroom will remember. Because I think that one was free. I want to say, like, something like Torrent Buffalo or...

Steve: You mean they were, like, using it over in China in order to...

Leo: No, they were using it in the U.S. so that they could watch the BBC for the Olympics because NBC was so terrible. TunnelBear. I knew it was something like that. Now, is TunnelBear free?

Steve: That's cute. Never heard of it.

Leo: Yeah, TunnelBear. But you're right, it depends on what he wants, doesn't it.

Steve: Yeah.

Leo: Yeah. Single, yeah, this looks pretty good. This says, "Simple, private, free access to the global Internet you 'heart.'" Now, they do - I see "free," and then there's "pricing." So I would guess that the free gives you a hearty helping of 550MB every month. If you want more, then it's five bucks a month for unlimited tunneling, and then you can buy $50 for a year. So TunnelBear, that's actually smart of them. You can get your first 500MB for free, so that's not too bad. Anyway, enough of that. Moving on.

Ian Smith, near Grenoble, France - speaking of the Olympics, Winter Olympics were there some years ago - wonders about a six-digit password: [Accent] Steve, my French bank has just changed their online banking, so I am now...

Steve: I think that's kind of an Irish accent.

Leo: I don't know. It's Steve Martin doing a bad French - so I am now limited to my six digits for password. Six digits? Six digits? I need to enter it in an onscreen widget thingy. Previously the limit on password length was longer. Mine was 12 characters, and I could have letters and digits. They move the order of the 09 buttons each time to make things more interesting, but I still believe this is a backward step, security-wise. So my podcast question is whether the onscreen keyboard is more or less secure than a standard password entry field, and why. For info, Citibank used to do this, but they switched back to standard keyboard entry, which allows me to use LastPass. That's the other problem with this little PIN thing is LastPass won't support it. Thanks for the podcast and for Vitamin D. Ian Smith, a SpinRite user for many years.

Steve: So this is not as bad as it sounds on the surface.

Leo: Oh. It sounds horrible.

Steve: It does. But consider that our one-time passwords, like our little famous football for eBay and PayPal and VIP and so forth, those are all six characters. And the idea is that obviously they change constantly. Well, rather than the password changing constantly, the position of the numerals is changing every time. So you use the same fixed six-digit password, which you remember. But the location of those is different every time and provided by the website.

Leo: Ah. So the password is actually where you're touching. Ah.

Steve: Yes. Yes. And that changes every time. So...

Leo: Oh, that's a one-time password, in other words.

Steve: Effectively it is. What they're trying to do is they're trying to prevent something which is scraping the screen, watching where you're clicking...

Leo: Or a keystroke logger.

Steve: Or a keystroke logger. So it thwarts keystroke logging.

Leo: Interesting.

Steve: Notice that it thwarts LastPass.

Leo: Yeah, which is not good.

Steve: Which is not what you want. On the other hand, the fact that it does gives you some sense for some of the benefit. And by rearranging things every time, even if you wrote something custom for noting the coordinates where you clicked, they mean something different each time. So if we also assume that there is good security behind this, that is, for example, you can't just sit there and guess and guess and guess, that is, you get three strikes, and then you've got to talk to customer service, presumably there is also some retry limit, and then you're elevated to some other level of needing to authenticate. I think this is pretty good.

Leo: You know, it's funny. Now that you explain it, it sounds good. I just didn't understand it. Now, do you want me to do Question 5 as a video question? Or should I read the question, then play the video?

Steve: Read the question. I'll talk and explain, and then...

Leo: And then you can tell me when...

Steve: ...I think it would be fun to play the video, yeah.

Leo: So this comes from Juan Cabrio in the U.K. He shares a revelation and a question. Why? Why, Steve, why? As you are the world-renowned super guru, Mr. Gibson, of a great many things including spinning disks and especially those that don't "SpinRite," I thought I'd tell you a tale of great calamity.

We had our gas fire suppression released over the weekend in our data center. Our gas fire suppression released over the weekend. Oh, that's like - I don't know what that is. What we've found is an alarming number of disk failures at the second the gas was released. Some entire arrays have been wiped out. What I believe at this point is that the noise, the noise from the 2200PSI gas release is what killed the drives. That sounds crazy. How could noise kill the drives? I read the link below which has me maybe convinced this is the issue. I don't see the link here, but we'll let you explain that.

Steve: Oh, yeah.

Leo: The fire suppression vendor has advised the dBs from the release in a relatively confined space is extreme.

Steve: Oh, so the sound, as in decibels.

Leo: The sound decibel level. Extreme. Well, I'm glad you weren't in there. You'd be deaf. The gas we use is completely inert, not harmful to anything - human, hardware, or otherwise. Can a man of your great wisdom advise one way or the other? I should note there wasn't actually a fire. There was a fault in the system. Thanks from a long-term listener. So they had a fire suppression system which

triggered.

Steve: Yes. Remember, like, halon gas is released. And apparently, because data centers are large, it is necessary to release the gas fast. That is, you want to get it out into, you want to fill the air very quickly. So the releasing - the gas is under tremendous pressure. It is released through nozzles that are doing their best. But apparently the releasing is loud, and it's accompanied with alarm bells that are somewhere north of about 120dB in strength. So you want to get people out of there because you're about to fill this with a gas that's not oxygen. So there's a YouTube video which is really fun. And you might play the beginning of it, at least. I tweeted the link in my Twitter feed for anyone who's interested. And it shows the reduction in hard drive throughput when you shout at a drive.

Leo: What?

Steve: Yes.

Leo: So drives are sensitive to sound.

Steve: Yes. And it's funny because I had two instances. A buddy of mine who I worked with years ago asked for a copy of SpinRite to see whether he could detect - he could use it to measure data transfer rate because they were having some problems with servers. And they'd noticed that, like, just doing something like pushing their hand down on the case made the thing perform better. And it turned out that the vibration from the fans in the server case was enough that it was throwing the drives' heads off track, and so they were - the data throughput dropped because they were going off track and having to go around another revolution in order to try to get back on track and find the data.

Leo: Oh, that makes sense.

Steve: And so in this YouTube video, which is just funny, it's a guy who's got some data throughput measuring instrumentation and shows the graphs. And he goes over and screams at an array, he calls them JBODs, Just a Bunch of Disks, or Just a Bunch of Drives. He screams at them, and then you can - you see graphically the drop in throughput just from him yelling at his drives.

Leo: Let's take a look at the video.

[Video clip: www.youtube.com/watch?v=tDacjrSCeq4]

Leo: He's shouting at it. And look, look at the latency spike. Another latency spike. Well, I think that, unless it's a hoax, I think that's pretty convincing. I mean, it could be a hoax, I guess, but...

Steve: No. Well, see, this is what's happened is that hard drives have become incredibly sensitive to vibration as a side effect of the insane densities that we are demanding from drive manufacturers, or they're demanding from themselves and their own engineers to be competitive.

Leo: The packing of the bits is so tight that you can't have any variation or you won't be able to read it.

Steve: Right. The good news is you have inertia that keeps the drive spinning at a close enough speed. So that's one dimension. But the off-track problem, that is, vibration of the drive, the head is trying to maintain itself exactly over the track, which has year after year after year become thinner and thinner and thinner. The track density has gone up so high that staying on track almost requires a zero vibration environment. So much so that anything that disturbs the environment, like that guy yelling at his drives, I mean, it creates a demonstratable problem.

Now, if you're just reading, that's not a huge problem because the drive will realize it could not read the sector. It just waits for it to come around again. If you happen to be writing, though, that's a problem. In fact, that's one of the things that SpinRite is about fixing because, if you're writing during vibration, you're actually going off the trail, and you can't tell that you're not on track because the head is busy writing. And it's written then permanently off track. So you've got to essentially go back to where it wasn't supposed to be in order to get the data, which is something that SpinRite does. But this demonstrates something; I just loved how graphical it was. I mean, it's very clear. So anyone who wants to see that, look at Twitter.com/SGgrc. I recently tweeted "Do not shout at your drives" and the link. So it's amazing.

Leo: Wild. By the way, do not point your Portable Dog Killer at the drives, either, I would imagine; right? Even if those are inaudible, still that's high-frequency vibrations.

Steve: Yup.

Leo: That's really great. It makes sense. John Pfaff in Pittsburgh, PA shares his thoughts about "Daemon." That's our favorite, one of our favorite novels by Daniel Suarez. I heard you talking about "Daemon" and "FreedomTM" by Daniel Suarez for some time, and I've always wanted to pick it up but just didn't get around to it. Then I was walking through the airport, and I saw it there in hardcover for $7.99. I couldn't pass up that deal. So I bought it. I couldn't put it down. Usually when I read I all asleep within an hour or so. Not with this. I had to force myself to stop so I wouldn't stay up all night. This book scared the crap out of me more than any psycho thriller I could find. I don't see a black sedan or silver BMW without looking to see if there's a driver. I want to go live with the Amish. Wow.

When I came back through the airport, I looked for "FreedomTM," but they didn't have it. They were out of "Daemon," too. I'm buying "FreedomTM" today for the Kindle - you have to because it's a second part, basically, it's a two-parter - so I can read it on my iPad and smartphone, as well. Thanks for a great podcast. I swear I get as much out of the ancillary stuff as I do out of the computer security stuff. I've

been a SpinRite user for a couple of years, and it did save me once, but not in a story-worthy way. Security Now! and TWiT are the only two netcasts I listen to religiously. Keep up the great work.

Steve: So I loved his writing. I just wanted to remind our listeners that that's another great book. I really did enjoy it.

Leo: Love it.

Steve: It's really well done.

Leo: And, you know, as we get more and more deeper into the weeds with these drones, "Kill Decision," which is Daniel Suarez's latest, and it's all about unmanned drones and the illicit use thereof, sounds more and more like fact, not fiction.

Steve: Yup, especially those new little quadricopter gizmos that actually exist.

Leo: [Humming]

Steve: Uh-huh.

Leo: [Humming] It's part of the story in "Homeland" Season 1, as a matter of fact. Jon Engle, Fredericksburg, Virginia wonders about one-way Ethernet transfer. Steve and Leo, thanks for providing such an interesting podcast. I find both your products and services to be extremely useful, especially SpinRite. I use SpinRite about once every six to eight months or so on my home server in order to prevent any disk failures. So far, so good.

Steve: Cool.

Leo: Anyway, in your recent podcast 379 you spoke about a company called Owl Computing Technologies. They specialize in one-way transfer-type hardware. Did a little research online and found some resources that discuss how to create a transmit-only Ethernet cable. Could one use something like this in conjunction with a protocol like UDP for purposes of enforcing a hardware solution? Would this be a practical home solution to make sure an attacker could not modify logs, files, notifications, et cetera? If this is possible, why would Owl Computing need to create a new protocol? Well, yeah, you just take out the receive pin; right?

Steve: Well, the way Ethernet 10Base-T and 100Base-T works, not 1000Base-T, but up to 100Gb, I mean 100Mb per second, is that even though the cables are always RJ-45 connectors, which means eight pins, Ethernet actually only uses four wires. That is, they use them as two twisted pairs, one in each direction. So one pair of wires is always

transmitting, and the other pair is always receiving. And in fact that's why you have to have - sometimes you had to have, like, a null cable or sometimes a crossover coupler or a crossover cable. It was because in some topologies you'd try to - you'd be plugging a cable in where it was confused about who was receiving and who was transmitting. Newer switches that you plug into, they have automatic recognition of that. But some of the older ones didn't.

Leo: Yeah. Most new computers do, too, yeah.

Steve: Right. So if you were to cut the two wires in one particular direction, you would get an Ethernet cable that could only receive or only transmit. Or actually, better stated, it would only transfer data in one direction between two endpoints. Now, why does that not work? That doesn't work because Ethernet is not just about UDP. It's true that UDP is a, as we've discussed often, is a one-direction protocol. That is, you simply send a packet off, and with no handshake required. TCP, by definition, requires a multiple packet interchange to get going. Not so with UDP.

But UDP is layered on top of other underlying protocols, like IP. IP has things like ICMP, Internet Control Message Protocol, where things like traceroute and ping and things that manage the IP layer live. And then below that is the Ethernet protocol itself. And, for example, Ethernet has protocols like ARP that we've discussed, Address Resolution Protocol, which must be two-direction. They're bidirectional protocols. When an endpoint is getting on the 'Net, it sends out an ARP broadcast to the gateway, but it doesn't know the IP of the gateway. So it sends it out - that's why it's called a "broadcast" - to every device on that local link and says, hey, I'm looking for who's got IP whatever. And then the endpoint with that IP responds, saying, hey, heard your request. Here's my MAC address and my IP. And then this thing knows how to address traffic to that IP by using its Ethernet MAC address.

The point is that, even though the higher level protocol like UDP may work in only one direction, none of the other protocols that UDP relies on are unidirectional protocols just because it's, like, never been a need. So it would take more than just cutting a couple wires in an Ethernet cable to get a working architecture. You could do things like hardwire the ARP table. There are ways to do that. So you pre-train your system that this IP is in that direction. But my sense is it's not as easy as just cutting the two wires. You could probably shoehorn a one-directional operation. But it would be a little - there's a little more to it than just cutting a couple wires and saying, hey, why does this not work? It's because the underlying protocols all assume bidirectional traffic. It's probably easier just to use a firewall. Although then you don't have hardware enforcement of that.

Leo: Somebody in the chatroom says that ATM, which is a media transport, high-speed media transport, can be configured for one way. The point of this is what? So that, like if you had a secure power plant, to have...

Steve: Yeah. And in fact you and I talked about it last week. This Owl Computing Company, they actually use optical fiber where there is only a transmitter on one fiber and only a receiver at the other end of that. So by physics the information can only go in one direction. And so to do that, they have to sort of like terminate the protocol at each end. So they satisfy everybody on the transmitting end themselves that their message has been received. Then they blindly transmit it through the fiber optic cable to the other end, and without any acknowledgment that the other end has received it because they

can't, by definition, they can't get any acknowledgment back. So this was a neat technology for, like, protecting nuclear power plants from intrusion where they wanted to extrude information for monitoring purposes but not allow that to be hacked in some way to get control.

Leo: Question 8 from John Bell in Northern Virginia, or NOVA. He's been made curious about full disk encryption: Steve, in the last episode of Security Now!, you and Tom - I guess more than the last couple episodes back - you and Tom were discussing full disk encryption, and specifically the use of cascading encryption. I have a comment and a question.

Comment: I think you might have missed a big advantage of cascading encryption. In a previous episode you talked about how a brute-force attack can know that it has found the key because it checks the decrypted data against a dictionary to see if the text produces recognizable words. In cascade encryption, the brute-force application may get the outer key correctly, but it won't know because the resulting decryption is still random data and not recognizable words. Thus the only way for the brute-force app to produce results is to create a nested loop of outer key and inner key decryptions until it hits recognizable words. The amount of time needed for that, as you might imagine, is pretty big.

So, question: At the end of that segment, Tom boldly stated that all hard drives should have full disk encryption. I don't have a lot of personal data on my hard drive, just some account passwords. I don't see too much that I need to protect. Aside from protecting personal information, is there a compelling reason to encrypt my hard drive that would be worth the performance hit? He's using OS X.

Steve: So, okay. First of all, about his comment. Essentially, chaining encryption like that, using a cascade of encryption, it's exactly identical to increasing the key length. So if you had a cipher like AES, which has a 256-bit key, and a different cipher like Twofish, and I forget how large the key is or can be on Twofish, but say that it was 256. Well, so what you have essentially is a composite 512-bit key. So this is really no different than using a very strong cipher with a 512-bit key. The question is, does that buy you anything? Because it's going to be slower.

So we've already seen, I mean, it's easy for us to underappreciate what key length means. 128 bits in reality is really all you need. We're talking 256 for new applications just because why not? As we talked about at the top of the podcast, cracking is always getting faster. Let's stay way ahead of it. And 256-bits is way ahead of it because every single bit we add doubles the difficulty. So we start at 128 bits. And now we're going to double the difficulty 128 more times. Double it 128 times. It's ridiculous. So that really the only advantage for cascading is, as I said originally, if either of the ciphers turned out to be vulnerable, you would still have the protection of the other one. That's why it's useful.

But really it doesn't help you from a brute-force attack except that it does give you a longer effective key than a single cipher would. AES maximum key size is 256 bits. If for some reason you want more key than that, well, yeah, you could cascade a cipher, and then you'd be concatenating the keys, effectively. But, as I said, whoa, 256 bits is really enough. The weakness would be in your choosing a password that was as good as your key length.

Leo: Oh, that's a good point. Excellent point.

Steve: And Tom's comment about whole disk encryption? Here's the test. He mentioned, okay, I only have some account and passwords. Well, do you mind if those are public? I mean, because that's the test is, yes, it's a tradeoff. So you're saying, apparently there's some resistance to encrypting your whole drive. Okay. There really isn't a performance hit that we've been able to measure. When I was testing the performance of the latest TrueCrypt, I couldn't see anything being slower using TrueCrypt. There's a little bit of overhead of having to manually put in a password every single time you turn on your computer. But that's necessary because the bad guys have to also. If you don't have to, they don't have to.

And so you just need to say, okay, if somebody got my computer - and say that it was password protected, but they can briefly remove your drive and mount it as a secondary drive on a computer that did boot up. Well, then they would have access to your drive. There's zero protection. So that's the thing to keep in mind. Ask yourself what if, and see how the answer comes back.

Leo: Question 9, Rob Alexander in Boston. He's wondering about SSL Interception and LastPass: Steve, great podcast. Been a listener for a while. I'll skip to the chase and give you my question so I don't have to say "blah blah blah."

Steve: But he did anyway.

Leo: Blah blah blah. I am at a company that was recently acquired and have been forced to migrate to a new IT infrastructure. They are forcing us to use Windows 7 and have installed various monitoring and controlling pieces of software. One of the things they claim they can do is intercept SSL traffic so they can decrypt it and inspect what's inside. The claim for this is they have to prevent malware or filter outbound connections to malicious websites.

First, how can I tell if SSL interception is occurring? Will the Firefox plug-in Cert Patrol reveal this if my company is installing a new root CA in Windows that is used by their SSL proxy to generate new certificates for real websites? Secondly, will LastPass's encryption of my vault still prevent them from seeing my passwords contained in the vault, even if the SSL transport can't protect the download of the vault from LastPass's servers? My suspicion is yes, but I was curious if there are any other considerations for data leakage or exposure of sensitive data that I have.

Steve: So we've covered the first part many times. I do realize, though, that we're continually getting new listeners. And this is an often-asked question, that is, how do I know if my company or my school or my organization or whatever can be seeing my encrypted traffic? And the answer is pretty simple: Go to a site that uses SSL. For example, go to just Google, https://www.google.com, and verify that the browser says you've established an SSL connection. That's important because your organization could be removing your attempt to bring up an SSL connection. That would be a horrible thing for them to do. But it's possible.

So make sure the address bar turns green or blue or whatever color it's supposed to

when you've got a secure connection. Then right-click on the page and choose "View Certificate," which is what most browsers allow you to do, and inspect the so-called certificate chain. It's typically a sort of a hierarchy of links up to some final authority which is typically VeriSign or maybe GoDaddy, some certificate provider who provided the authority for the certificate to Google. And I guess we could look and see who Google's CA is. But the point is you need that chain to terminate there at that authority, not at something like it's got your company name in it or, like, anything that looks fishy. If it looks fishy, then it probably is.

Leo: And it can't say the name of the actual website, like Google.com, unless it's legitimately Google.com; right? They can't have a certificate that spoofs the actual name.

Steve: Yeah, right. And it would be that...

Leo: Even if it's self-signed.

Steve: Yes, because your browser would then not accept that. Your browser needs to get a certificate from Google saying I am Google, and here's my credentials. So but the problem is, if your company were intercepting, they would be building fake Google certificates on the fly so that you'd still have a certificate that looked like it was coming from Google, but it would not be signed by Google's certificate authority. It would be signed by your company acting as a certificate authority, which your browser would have been fooled into trusting because a certificate would have been installed on it. So you want to make sure that the highest level of authority in that chain is a legitimate certificate authority, a public authority, not something local and private to your company.

Leo: And you could tell that.

Steve: Yeah.

Leo: I mean, it's pretty obvious.

Steve: And so the second part of the question was a little bit more interesting, and that is, if the company was completely violating the security of your secure connections, what about LastPass's vault? And that's the beauty is LastPass never relies on any link-level encryption. None. That is, so it is secure if SSL didn't exist at all. And that's the beauty of what LastPass has done is they use, as Rob expected, they use local encryption in the browser so that when the user's LastPass database, their vault, is being sent up to LastPass, it is preencrypted. It's full TNO, Trust No One. It is preencrypted in the browser and sent as an opaque blob. So not only can your company not decrypt it, neither can LastPass. And that's what's so elegant about their solution is nobody can see into that blob except you, you who have the master key that never leaves your control, even if your company is watching you.

Leo: Yes.

Steve: So Rob, you're safe.

Leo: Right on. Right on, right on. Last question from "Morthawt" in the U.K. Actually it's a comment, really, about the Hush Puppy, the Portable Bark Killer. He says - and you wanted to set that, you were planning on setting it at 15KHz. He says that's not high enough. Children and adults that have good hearing can hear it. Dog devices like your PDK are way higher at 1820KHz. And I would hope you increase the frequency to at least 19. By the way, I'm 28 years old, and I still hear frequencies up to 16K easily.

Steve: Okay. So I have set it at 15. And the components that I have chosen pretty much lock it at 15. That is, one of the ways I reduce the component count and the cost to a few dollars, which is truly what this thing ends up costing, is that the amplifier is tuned, the amplifier itself is tuned to resonate at 15KHz. So if you try to use 14 or 16, you get a much lower amplitude output. It peaks at 15. And in fact even that will be tunable a little bit shortly, just so you can actually find the exact center of that tuned spot. Since component tolerances vary, it may be that the actual sweet spot, well, you could guarantee that a sweet spot is going to be slightly different from one to another. Although I've arranged for it not to be too peaky.

I chose 15 for a reason. I, too, can hear it. And I decided, first of all, canine hearing is acute at 15. But it, too, begins to fall off at higher frequencies. So even though dog hearing is very good, at 20KHz it's beginning to be less sensitive. And we definitely want, the whole point is for something that is loud and startling to a dog that's barking and is completely unfamiliar in its experience of life. It's like, I've never had that happen before. So we want something that gets its attention. So consequently we want it to perceive it as loud. But the other problem is the mechanics, the tweeters. Tweeters have a difficult time going a lot higher. They say, oh, they go to 20KHz. But they're already beginning to fall off before that. So I also didn't want, again for the goal of getting the maximum output power, I didn't want to go too high.

But lastly, I want people to be able to hear this. I don't want something which makes no perceptible sound because people might be inclined to aim this thing in their ear and pull the trigger. And this thing generates substantial acoustic energy. That's the point. But we need to think of it, I mean, this is not a toy. A knife is obviously not a toy. We intuitively understand that it's pointy and sharp. And a gun is not a toy. We understand from our real-world experience, you don't aim, you don't point that at anybody, any person. So I wanted something where you could perceive that this thing was not something you wanted to aim at anybody, like, put it right up to them, anyone that you care about.

And also, I mean, you'll need to use it judiciously. In fact, if you try to use it for too long, the sound volume decreases because we're putting so much power into this tweeter that the piezo electric ceramic heats up and becomes less efficient. So for the first second it's the loudest, and then it begins to get quieter, which is - I think that's fine, design-wise, because this is meant to be used in short bursts to get a dog's attention and cause it to react, rather than to do harm to anybody.

So I'm happy. I absolutely hear it. I mean, I keep this thing pointed down at the table when I'm using it because I don't want it aimed at me. And I think it's important that this

thing be treated with respect. And I'm going to print up and do the design for some warning labels which I would advise people to put on these things when they make them because it's not a toy. So that's why I set it at 15.

Leo: I think that's a really good point. You don't want it to be completely invisible.

Steve: No. It's like an X-ray machine. There's a reason that your dental tech leaves the room every time you're getting X-rays, and why your gonads are draped with a lead apron, is that this stuff is dangerous. But if we don't perceive it, it's very difficult to act responsibly. It's a little bit like getting a sunburn at the beach. It's like, well, one good sunburn, and that teaches you a lesson, that even though you can't see something happening, it is. So I didn't want to have this be completely imperceptible. And believe me, it's not. I'd be surprised if anyone can't hear it because it really pumps out some power. So I thought, let's just help people to treat this thing with respect.

Leo: Steve, you know what, you have my respect. That's who's got respect. Steve Gibson is the man behind this show; GRC.com; SpinRite, the world's best hard drive maintenance utility. Lots of freebies at GRC.com. If you want a 16Kb version of the show, we've got it, or Steve's got it at GRC.com. He also has text transcriptions done by human beings, so they're accurate.

Steve: One human being in particular.

Leo: Elaine.

Steve: And actually Elaine wants one because she's got a problem when she's riding her horse of dogs want to nip at the heels of the horse. So she's going to make sure first that it doesn't spook the horse. I imagine the horse could probably get used to it. But she would like to see if it would allow her to zap the dogs and convince them that chasing this horse is not a good thing to do.

Leo: That's interesting.

Steve: All kinds of uses.

Leo: Yeah. Wow. We do the show Wednesdays at 11:00 a.m. Pacific, 2:00 p.m. Eastern time. That's 1800 - 1900? - UTC.

Steve: It keeps jumping around.

Leo: If you want to watch live. Yeah, because it's this stupid Ben Franklin. I blame Ben Franklin. But we do have audio and video after the fact. Steve's got the bandwidth-constrained version, and we have the video and the audio at TWiT.tv and

wherever better podcasts are offered. Just look for Security Now!.

Steve: Hey, they're all here. They're all at TWiT.tv, Leo, where all the best podcasts are to be found.

Leo: They're all here. Yeah, we won last night. I have an award from Stitcher, which is a great little podcast app, for the best tech show. And that was audience voted, so thank you, everybody in the audience. It wasn't for Security Now!, it was for TWiT. But next year, now that I know they do these awards, we're going to make sure that Security Now! gets a nomination.

Steve: All we have to do is tell our faithful listeners, and they will do the rest.

Leo: Absolutely.

Steve: They've done so in the past.

Leo: When it comes down to an audience-voted award, I think there's nothing we can't win. But that's a nice award. That's a prestigious award. We're also nominated, and I will be at the awards show in Vegas for the - there's two big award shows. There's the Podcast Awards. I don't know if we're nominated in those or not. I'm hosting that, though.

Steve: Ah, cool.

Leo: And there's the International Academy for Web Television that has an award every - actually this is the second annual at CES. And we are nominated for several awards at that.

Steve: Very cool. And you are pumping out video, so that would explain it.

Leo: Yeah. We are web television. So I'm excited about that. And people, if they want to go, if you're a member, you can vote. Vote for us. And if you want to go, you can go to IAWTVAwards.org. If you're going to be in Vegas for CES, go a day early, I think it's Tuesday night, and you can see the awards. And I will be there, so it'll be a lot of fun.

Steve: Is it in February this year? Or next year?

Leo: January...

Steve: Oh, January.

Leo: ...8th, something like that. I think the awards are January 7th, I guess.

Steve: Cool.

Leo: Yeah. It'll be fun. Steve, thanks so much.

Steve: Thanks, Leo.

Leo: See you next week on Security Now!.