Listener Feedback #23

Description: Steve and Leo 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 they have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-108.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-108-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 for September 6, 2007.

It's time for Security Now!, and we're in September already. Steve Gibson, the year is waning, fall is on its way, and the bugs are out of your house.

Steve Gibson: I'm back in the house and hopefully breathing pure air. I'm not really sure. They say they mixed the - the problem is that this Vikane, which is the commercial name of the gas, I think Dow produces it...

Leo: Well, they have a spotless track record, so I think you should...

Steve: Yeah.

Leo: Nothing to worry about.

Steve: Nothing to worry about in terms of pesticides. It's odorless and colorless. So you wouldn't know if you were breathing a potent neurotoxin.

Leo: That's nice.

Steve: But they deliberately mix in tear gas, which you certainly do know if you're breathing.

Leo: Oh, that's smart.

Steve: Yeah. And that way, if you happen to walk into a house, I mean, it's not easy to walk into a house that's got notices posted all over the walls, and it's under a tent. But you would immediately know that something was wrong.

Leo: That's what they do with LNG, right, it's odorless.

Steve: Exactly.

Leo: Well, that's encouraging, anyway.

Steve: Yeah. So we have no more bugs here. So I haven't seen any, as a matter of fact. In fact, this area geographically has a serious spider problem. And so I don't know that I had any termites, but boy do I know that I had spiders. And they're not moving around anymore, so.

Leo: How do they clear out - so that's interesting. Because I thought they were using poisons that - this has now become the bug report. But I thought there were poisons that had a short half-life. But I'm sure tear gas does not. So I wonder - they must clear it out heavy-duty; right?

Steve: Well, yeah. In fact, it's a three-day process. You exit your home in the morning. They put the tent over and then fill it with this gas. It spends 24 hours in that condition. Then they remove the tent, open all the windows...

Leo: Oh, that's good. Vent it right out into the environment.

Steve: Exactly. In fact, it's funny because it's heavier than air. That is, the Vikane is - it settles to the ground. So they also put some fans in your home to keep your air stirring around. And one of the homeowners during one of these prep meetings were saying, well, you know, what about if I'm, like, living in a home below one that's been fumigated, and then you take the tent off, and all the Vikane pours down the hill into my home? And, you know, the poor Terminix guys roll their eyes and say, well, lady, you know, just exhale.

Leo: They live with it. I wonder...

Steve: Oh, as a matter of fact, that's one thing that I felt good about was these poor guys, I mean, they're in this Vikane environment all the time. So I'm figuring, well, if they're clearing it out - and they do go in with sniffers, they say, to make sure that they get no readings. And the original label said it had to be as low as five parts per million. And now they've changed it to one part per million. And then the guy said, oh, yeah, but we always get zero. And I'm thinking, I think that heater's working.

Leo: Zero.

Steve: How do you get zero?

Leo: How do you get zero anything?

Steve: Maybe it's just stuck on zero, yeah.

Leo: Let's get to security.

Steve: Oh, why don't we.

Leo: Enough of pesticides, although I find this fascinating. But we probably should talk about security. First of all, any errata, addenda?

Steve: Oh, I've got a ton of things, Leo. Okay. First of all, top of this episode I wanted to suggest a change in our format from now on. During my reading of email, incoming email, I ran across sort of a grumbly note, actually it was grumbly phrased, from one of our listeners saying, essentially, or actually pretty much, why don't you guys drop this artificial distinction between the Q&A and the Mailbag episodes and just call the even episodes - oh, and he was grumbling about mod 4 and still didn't like our equations. Just call the even episodes Listener Feedback, whether they're questions or they're comments.

Leo: That makes sense.

Steve: And, well, I actually liked it because I have been having trouble, like, sorting out questions and comments. And so, for example, many of these that we're going to start our show with this week I actually found two weeks ago when I was only looking for comments and not questions. So it hasn't really functioned well at my end. And frankly, also, so many people have written saying they love the Q&A episodes, I think we really end up with a nice mix because the Q&A episodes allow us to spend an hour talking about all kinds of different things, whereas the odd episodes are generally single topic or a low number of topics, at least, where we're focusing in more depth. So I really like that. And if it turns out that we tackle some big issue that needs multiple parts, well, we'll just drop a feedback for that one if we need to do several hours in a row. So we'll give ourselves some freedom. But from now on, no more distinction, Mr. Grumbly, between the Q&As and the Listener Feedback, the so-called Mailbag. They're just all Listener Feedback episodes. And we're doing No. 23 today.

Leo: Well, we thank you, Mr. Grumbly, for a good suggestion.

Steve: Mr. Grumbly evolved Security Now!. Okay. Big correction to what I assumed incorrectly, and have since verified, last week. I assumed that the fact that VeriSign would sell you three of their tokens, fob dongles, whatever we call them, deals, meant that you could simultaneously register multiples. And you can't.

Leo: Oh. Well, why do they sell you three, then?

Steve: I don't know. One of our listeners, actually very courteous, a Walter Soldierer I think is how I pronounce his name, he provided me with the name of the guy at VeriSign, and email address, who's in charge of the whole PIP technology program. His name is Gary Krall at VeriSign. I sent Gary a piece of email saying, hey, I was really glad to get your name and email. I'm told you're the guy who would know this. Is it in fact the case that it's possible to register multiple "tokens," is the word Gary uses, although on the site they use the word "credential." And this is the thing that we've been calling, you know, the PayPal fob or dongle or token or whatever. So, and he said, oh, that's an interesting idea, but no.

Leo: No. Nice try.

Steve: I mean, and he referred to many late nights. So I have a feeling that he's, like, really the guy on the front line of the technology. And he explained that it would require a substantial change, like new database format update and things, to, as he put it, to "bind" more than one token at a time to the account. So I wanted to correct - I mean, people were really excited about this, as was I. And Gary did promise to add it to his list of possible updates. But I didn't get the sense that it would be happening anytime soon.

Leo: All right. Good to know.

Steve: So, yes. Also I did mention the combination lock padlock gizmo last week, and that I ordered two. They both came. I was going to crack one open to see what it looked like in terms of how difficult it would be to work around the padlock. I really like the device. However, it is conspicuously larger than - actually larger than I expected it to be from the photos on their site, and certainly larger than a so-called "thumb drive." This is a - I would call this a large middle finger drive.

Leo: Okay. Is that in terms of length?

Steve: Yes. And, you know, when you think about it you really do need - it needs more panel surface in order to be able to host a five-key pad where they put zero and one together and two and three together and so forth. So you have five combination buttons. Then you've got a sort of initiate button that shows a padlock, I mean a key on it. And then other little icons that light up when it's doing different things. So, I mean, this thing, it's big, but I have to say I think it's pretty cool. I mean, if you have an application where, again, you'd like to store either one or two gig of data in a fashion which is not going to be easily read, for example if, you know, it's around the house and you don't want your kids to get it, or a coworker or so forth, I mean, this thing, it's by Corsair, and they call it the Padlock, the Flash Padlock. So it's neat, but it is big. It's not a thumb anymore, it's like I said, more like a long middle finger.

Leo: All right. And these things are getting smaller and smaller. So if size is an issue, there may be some other choices. And they put TruCrypt on it. It's just as secure.

Steve: Right. And speaking of USB dongles, Sony, as you may have heard, Leo, has done it again.

Leo: Oh, no.

Steve: Yes. They've got a USB dongle that has a thumbprint reader or a fingerprint scanner of some form on it. Remember that we talked about SanDisk having one before. Unfortunately, Sony's has software which includes again rootkit.

Leo: They can't stay away from it, can they.

Steve: Ugh.

Leo: You know they're suing the company that did the rootkit, the original rootkit.

Steve: Oh, it's been a big mess, yes, you're right. Sony is suing them because of course they got in a lot of hot water for doing this with their, as we talked about it back in, like, it was '05, the original Sony rootkit scandal. Well, now they've done it again. When you install this software, it installs a subdirectory underneath the main Windows directory which hides all the - it hides itself, that is, the subdirectory itself, and all the files it contains, and executable content. So, and it hides it from the Windows API using rootkit technology so that - and it's confirmed that virus scanners and malware scanners will not find things that are in there.

Leo: So this is their - they keep coming back to this idea that the best way to be secure is to be rootkit.

Steve: Oh, I mean, it is just another - well, we know what a bad idea it is. And remember that last time they did this with the Sony VCD stuff, it took about two weeks for malware to be written that would leverage the Sony rootkit in order to hide itself using that technology. And so it doesn't take much imagination to imagine, although this is, of course, being a USB thumbprint dongle, there's going to be far less market penetration than there was of any audio music CD from Sony.

Leo: Well, and you're buying a secure dongle. So presumably it's a little different than sneaking this onto your system through a CD.

Steve: Like for example on - exactly right, Leo. Any consumer audio CD. So, but again, they apparently have not learned their lesson. And...

Leo: Hard to believe. Hard to believe.

Steve: Just unbelievable.

Leo: And again, part of the reason this was so easily utilized by hackers last time was it really had a big flaw. It was very badly written. Any file of a certain type, filename, was all of a sudden hidden.

Steve: Right.

Leo: Maybe they didn't make the same mistake, but I'm not going to count on it. We don't know exactly how dangerous it would be, I guess.

Steve: And then lastly I wanted to mention that, without reading endless individual emails, so many people agree with us, Leo, about PayPal. I mean, that is to say about the negative aspect of this weird, you've got to register with a checking account in order to become authenticated, then there's no way to - I mean, I got all kinds of email from people saying, yes, yes, yes. And, in fact, some saying that, due to the fact that this is a default that cannot be changed, that is, that PayPal will force you to manually override their deducting from your checking account, one guy did in fact have a fraudulent transfer made and just went through all kinds of hell trying to get his money back. Basically PayPal never was able to do it because it was gone. It was out of his checking account, and they were not ensuring it. But he had a third-party insurer of the transaction that ended up - he ended up being able to get restitution from. But it was a nightmare. So, I mean, I have read a bunch of horror stories and corroborations of, like, why is - this just seems like a bad and dumb thing for PayPal to be doing default-wise.

So, finally, I got - as far as I know this is the first, at least the first one I've seen, a report from a Nerds On Site nerd who used SpinRite. And I didn't really pick up on it at first. He said: Please - his name is Raoul Velez. And Raoul said: Please pass this to the feedback section of SpinRite. So he must have sent email to my office, and they forwarded it to me. So all he said was: My name is Raoul, and I am a nerd. And I thought, well, okay, you know, I am, too. So nice of you to just step up and admit it, Raoul. So he said, I've been a nerd since my retirement from the Navy three years ago. And I thought, okay, well, he's a late nerd bloomer. But so he says, yesterday I received a call from a hotel in the Raleigh area that their server was down. I went in, took a look, and after talking to the manager about what they have done and what they were heading, he wrote, or where they were heading, he says - anyway, he says, I decided that it was time to give SpinRite a chance. The software ran for almost seven hours. At the end, the server rebooted, and voila, it was working again just in time for the morning checkouts. The drive has to be replaced, but we've been able to buy some time and back up critical files that otherwise would have been unavailable and would have had to have been recreated. Needless to say, the front desk people were loving me. It's a great thing we have a site license. And that's when I go, ah...

Leo: That kind of nerd.

Steve: This is a Nerds On Site nerd. So he says, it's a great thing we have a site license for this. By the way, I also own my own personal license of the software.

Leo: Oh, that's neat.

Steve: And this is signed Raoul E. Nerd in Cary, North Carolina. So we had a neat - we had a combination of a SpinRite success and a Nerds On Site story.

Leo: Very nice. Shall we talk - are you ready to go to our questions?

Steve: Absolutely.

Leo: And we do hold 12 fantastic questions.

Steve: Thanks to our fantastic listeners.

Leo: Starting with Justin Teal. He has a way not to use WEP or WPA. We're talking about wireless security here. Wow. He says - yeah, wow. I like the idea. He says rather than use WEP or WPA he just turned off wireless broadcasts. That's what broadcasts the name of the network. And he uses Mac address filtering to only allow his machines. He says: Isn't that sufficient? For someone to get on my network, first they'd have to know it's there. Second, they'd have to spoof my Mac address. I'm assuming it's enough protection because I don't know of any way for someone to get the name of the network or my Mac address. Steve, would you like to enlighten him?

Steve: Well, Justin, okay.

Leo: I'm glad Justin asked this because I'll tell you what, this is a very common - and I still go to places that say we need your Mac address before we'll let you on our network. And I just - I have to laugh at them.

Steve: Yup, yup. Because, you know, well, for example, Leo, following up them saying that, all you would have to do would be to turn on any of the many and multiple available sniffers.

Leo: Ping enable is a good choice.

Steve: Exactly. See any of the Mac addresses which are flying through the air, and go, oh, there's one, and then just...

Leo: I'll use that.

Steve: Well, yeah, exactly, clone that Mac address for your own, and you're automatically given permission to use the network.

Leo: And it's not just the Mac addresses flying through the air. The SSIDs are flying through the air.

Steve: That's exactly right. Even though you're not broadcasting it in beacon mode, you are able to see the SSID as part of the protocol in the wireless packets. So, Justin, I'm afraid to tell you that what you've done has a benefit, but not the benefit you're looking for. The benefit it has is it will prevent people from inadvertently using your wireless network. We see this all the time with, for example, in apartment buildings or in condo complexes or in any situation where you've got, you know, many times people will turn on their Windows and look at the available wireless networks. And you'll see five or six of them at different signal strengths. Well, you sort of choose which one you want to join if they don't have security. The point is that it's often inadvertently the case that somebody would be using yours without your permission and even without their knowledge, just because their system would have said, oh, look, there's open Wi-Fi.

Well, turning off the beacon prevents it from being seen in that mode where it's just looking at all the available networks. And turning on Mac address filtering will certainly prevent their system from inadvertently connecting to your wireless access point. But anybody nefarious who actually still wanted to get onto your network could still do so easily. As we just said, all you have to do is sniff the traffic. The traffic shows the SSID, that is, the name of your access point, and the Mac addresses of all of the devices that are flying through the air. So it's very easy for someone to use an existing Mac address and be authenticated and authorized on your network. So it will prevent people from using it by mistake. But it certainly isn't bulletproof if somebody wanted to get on your network without your knowledge or permission, and they certainly still could. The only way to prevent that is through one of the encryption technologies. And of course WEP still has problems. Now WEP is so badly broken that someone with the latest WEP cracking tools, which are, again, freely downloadable and available on the Internet, it takes them about a minute to crack the WEP key on a WEP-encrypted network. Only WPA is safe. And any version of WPA is safe enough.

Leo: So that's kind of the bottom line. There is one thing that works, WPA, and that's it. And that's pretty easy to remember. David Johnston of Eufaula, Alabama, says: I, like many of your listeners, am the tech guy for my family and friends. He heals many an ill PC. Actually wants to talk about virus scanning and removal. To scan an infected PC drive I have a standalone beige box PC running Windows 2000 and Symantec AV 10 that I'll install the infected drive in as a slave. I then scan the, I'm presuming the master drive, for viruses and spyware. So how effective and safe is this? I've cleaned many drives and never noticed any ill effects on my PC. Oh, I see. He takes the - I get it. No, he takes the infected drive and puts it in as a slave and then scans it.

Steve: Right.

Leo: I'm wondering how likely it is that a virus will migrate from the slave drive to the master drive. Thanks for the help, and keep up the great work. Interesting solution.

Steve: What's interesting about this is that what he's done is he's avoided the possibility of viruses on the slave drive being live. The problem is - if he were booting that drive and then trying to scan it on itself, the problem is you could have things that have antivirus scan technology. But by pulling the drive out of its normal live mode, sticking it in essentially as a data drive, not as a bootable drive, none of the code on that slave drive ever has a chance to run, so nothing malicious has a chance to ever get going. Now, he is assuming that, as he calls it, his beige box, his scanning machine, he's assuming that that is clean and doesn't have anything bad on it. You certainly wouldn't want it to have something bad on it that would then be able to clone itself over and jump onto any drive that was inserted, and certainly historically that's been sort of a propagation strategy for viruses of the past...

Leo: He can't cross-infect from the slave drive, the one he's put in, to the master drive.

Steve: Exactly. Exactly. And that's the key. There is, you know, he needs to be conscious of the fact that it could go the other way, that if something did get infected on his beige box PC that he's using for scanning, that master drive could potentially infect the slave. But his question really was can anything on the slave get over to the master drive? And given what he's talked about, I don't see any way for that to happen. So I think it is, it's a neat idea to scan a drive that is not running so that it doesn't have a chance to protect itself.

Leo: I mean, it's a lot of work because you have to pull the drive and put it in the beige box. A lot of people will do this with a CD. They'll make a boot CD, which can't be reinfected. You know that's clean. The drawback to a boot CD is that it's not always up to date. You have to make it fresh every time to make sure it has all the updates. I think F-PROT, the folks at Frisk have software for making DOS-based boot scanners. And of course there's plenty of Linux scanners, too. But then you have to always update it, which could be a pain.

A listener named Dale has a blast-from-the-past question. Episode 32, a ways back, we talked about bogon space and listed a bunch of IP ranges that are in the bogon space. Is he talking about bogus?

Steve: No, bogon, in fact, yeah, bogon.

Leo: They're nonroutable. So if 5. space is bogus, how come Hamachi, which uses 5., is workable? 5. lives in bogon space.

Steve: Yeah. So, okay, let's back up a little bit and, since this has been a blast from the past, review from the past. The Internet has a bunch of blocks of IPs which have even today still not been used. And in fact there are - it's a surprising number of IPs that are completely unusable. So, for example, the 4. space is in use, but the 5. space, that is to say, any IP that begins with 5. and then its three other components, has never in history been used. So, and there are many other similar so-called "Class A" networks, that is, various numbers at the start of the IP address, so something dot something dot something dot something dot something, that first number has never actually appeared in use. They're called nonroutable because, if you happen to drop a packet onto the Internet at a given location, as we know from talking about how the 'Net routing works in episodes in the past, a router would go, oh, here's a packet that begins with 4. And it would have tables, routing tables that tell it which direction the 4. network is in. And so it would route that packet out of the proper interface toward another router that would have a similar table that would tell it where to forward that packet to. So the packet hops from router to router, heading toward its destination.

Well, if you dropped, for example, a 5. packet onto any router on the Internet, the router would say, huh? It has no instructions about where to send that packet because no 5. IP addresses exist. Somebody owns that network space. I think all of the space is owned by various people, or maybe just never assigned by the main signing authority, but still the point is that there would be no routing table entry telling the router where to send that packet. So Dale's question is, if that's the case, how does Hamachi do this? Well, what Hamachi does - Hamachi of course is a peer-to-peer networking technology that uses VPN-like technology to create sort of ad hoc peer-to-peer networks. What Hamachi is doing is it's actually using the normal routable IPs, that is, the normal IPs that the Internet is currently using and which Hamachi's users currently have assigned. It's using those IPs to actually move the packets from machine to machine as required. But once the packet arrives, it takes the envelope off of that packet, and that's where the 5. addressing is.

So to say this differently, the machine that you are talking to has a packet with a 5. address, which is nonroutable. What Hamachi does is it puts a packet around it, it encapsulates the nonroutable 5. packet in a standard Internet routable packet with the destination IP of the other Hamachi machine where this packet is bound. So that packet it puts on the Internet, which is routed to that target machine. When that machine gets it, it takes that wrapper packet off of the interior packet, which is addressed to the 5. address of that target machine. So essentially the packets that Hamachi is routing are internally using this unroutable 5. space. But externally they're using standard Internet addresses.

Leo: That makes sense. The other unroutable spaces, the bogon space IP addresses are 192.168?

Steve: Well, of course, those are private IP spaces, like 192.168 and then 10. space, of course.

Leo: Are those considered bogon or not?

Steve: Well, they're really not bogon. They're privately, I mean, they're well-known, in-use private networks, as opposed to...

Leo: But they're not routable. They can't be used on the 'Net.

Steve: Publicly, correct.

Leo: Mark Ryan of Agassiz, BC, Canada has a two-factor authentication system he'd like to share with us. First of all he says: Thanks for the work you do to make the Internet a safer place to roam in. I've listened to all the Security Now! podcasts, and the information you provide has helped me keep the computers of mine and my own running with fewer problems for years. He's owned a copy of SpinRite for about five years, and he says: I know it's one of the main reasons my computers have continued to run smoothly for years, one for about seven years with no reformatting. How often do you recommend running SpinRite?

Steve: Well, I would say quarterly is probably often enough. I would say maybe once a year is not often enough. We've run into many instances where people have run SpinRite and it's found lots of uncorrectable errors. It's certainly the case that, had they run it more often, SpinRite would have worked with them to correct those before they became uncorrectable. So, I mean, it absolutely is preventative maintenance. And so quarterly is prob- once every three months or maybe every four months, do it three times a year.

Leo: And it wouldn't take seven hours if you do it all the time.

Steve: No, it zooms right along when it's not stuck on a problem.

Leo: If there's something wrong, that's when it starts to take a while. We often say, oh, it took about - that one they said three months, and I think that scares people off. That's only if there's a problem. That's only if you really need it.

Steve: Right. And in fact, you know, it is interruptible. You can stop it. You're able to start it past the prior problem if you don't care about it fixing something where it's stuck. You're able to kind of nudge it forward and say, okay, let's get on with this. So there's all kinds of options while you're running it.

Leo: Rob Hartvikson writes from Italy...

Steve: Oh, we skipped the second part of that.

Leo: Oh, there's more. Yeah, he mentioned a - I'm sorry. I got so caught up in that, I forgot to mention his two-factor authentication system he uses. His broker has introduced what seems to be a pretty slick system, a card with a unique eight-character ID number and 224 columns on this card containing three random alphanumeric characters. To use the card I have to register it to my account. And then when I log into my broker, I enter my username and password, and then the site gives me two numbers corresponding to the columns on the cards. So you look down the column and along the row, I guess, and enter the two sets of three characters from the matching columns, and now I have access to my account. So how secure do you think that is? It's better than a password alone, but what are the weaknesses?

Steve: Well, it's a neat idea. It combines - it sort of combines something you know and something you have because you're being prompted by the site that wants you to log in for information that only you will have. He talked about the card having a unique eight-character ID. So clearly the card was algorithmically created based on that ID number so that back on the server they know the ID number associated with his account, which is the ID number on his card. That allows them to know what his card contains. So then he's randomly asked to essentially read out part of the data on the card.

We mentioned this kind of approach briefly a couple months ago, and I wanted to bring it up again because I think it is really kind of cool. It has the advantage of being extremely inexpensive. For example, in this case I think his broker set him up with a card. But there are systems where you print your own index. When you're signing up, it gives you a page, you print it, you fold it, you stick it in your wallet. And this thing has essentially a ton of pseudorandom data. It's pseudorandom because it was algorithmically generated, not truly random. Otherwise the server would have to maintain an exact copy of what it was that you were carrying. And of course pseudorandom is no weakness as long as you don't know what the algorithm was to generate it, and as long as no bad guy had the eight-character ID number. And the eight-character ID number is not part of this challenge-response handshake, so that can't be known either. So it's really cool because...

Leo: Is it better, do you think, than the dongle? Or, I mean, is it as good, I should say, as a dongle. Or the fob.

Steve: I think one of the things I like about it is it has no batteries.

Leo: Yeah. You carry it in your wallet. It's cheap.

Steve: Exactly. You can carry it in your wallet, it's cheap, you could Xerox it. Now, you might say, wait a minute, that's a security weakness. If somebody briefly got your wallet and Xeroxed the card, now they've got a copy of it, now if they had your username and password they can log on as you. So that's a problem, unlike the dongles and fobs which are, you know, you can't Xerox those. We don't have teleporters that can do matter duplication at this point. So there's a weakness. But on the flipside, it's inexpensive, and it's going to give you very good security.

So one vulnerability would be that somebody could record one transaction, that is, if they were monitoring through a man-in-the-middle attack of some sort, and we're assuming that this would all be over secure socket layer connection with valid certificates and everything, so that would be ruled out. But if there were something, for example, on your computer, upstream monitoring your screen and keyboard, for example, that was capturing your transaction, there

is the possibility for a replay attack, where something sees you log on, sees the numbers you're being given from the server, sees the alphanumerics that you returned...

Leo: Because it would match every time, wouldn't it.

Steve: Exactly, because the data on the card is static.

Leo: There's the flaw. There's the flaw right there.

Steve: Yeah. The data on the card is static, whereas the dongle is a constantly changing number that never repeats.

Leo: So if you had a man in the middle, all you'd have to do is watch.

Steve: Yup.

Leo: Ah. It's still pretty good.

Steve: But still, absent that, it's less expensive than hardware, and it's really - it is certainly stronger than just a username and password because what you're being asked to provide changes every time.

Leo: Very interesting. Now to Rob Hartvikson, writing from Italy. He's wondering about rotten bits. I just listened to Security Now! 104 and your discussion about bit rot on Windows and using SpinRite to correct it. If I understand correctly, SpinRite will deal with bit rot. Doing a complete drive reformat is not going to give me better performance over just running SpinRite. Oh, that's interesting. What if he's willing to erase and reformat? Is that just as good?

Steve: Well, I wanted to bring it up real quickly because we had a couple questions that were asking similar things. A reformat is, except for the areas of the drive that involve the file system, where the directory and bitmaps and so forth that manage the contents of the file system, a format is only doing a read pass, given that you do a long format and not a quick format. Most people these days just do a quick format because a long format is really a long format. I mean, it'll take a long time to format the drive. All it's doing, though, during that long time is reading all the sectors. Well, that's better than not doing that.

But SpinRite ups the ante one level because SpinRite in its normal mode is reading/writing, reading/writing, and reading the drive. So it's actually flipping all the bits twice, looking for any problems being reported by the drive, and giving the drive then the chance to recognize that there's a trouble sector that it should map out of use. So SpinRite will give you a better result than just reformatting the drive. But reformatting the drive is better than nothing.

Leo: Right, okay, cool. Jeffrey in Columbia, Maryland is ready to defrag: A while back you were talking about some of the free programs you use. One of the programs you pointed out was SpaceMonger. The other was a free hard drive defragging program. What was the

name of that defragging program you recommended? He uses Diskeeper Professional. His license is up, and he wants something free that works just as well. Is there a free one? I don't remember mentioning that.

Steve: No. I wanted to let Jeffrey in Columbia know that it wasn't a free one I mentioned, it was a good one that I mentioned. And actually I now have two favorites. I think I referred to Vopt. Vopt is very nice. It's at Version 8 now. However, I've started using one called PerfectDisk. And I bought it because I was very impressed with it. It will do something that Vopt won't, which is it will defrag the so-called metadata. What I was talking about just a minute ago when I was talking about the bitmaps and the directories and things, nothing is able to move those because those are locked by the system while the volume is in use. PerfectDisk is able to do a preboot defrag of those and, for example, to defrag your swap file, which is another area that cannot be moved around while you're running the swap file, running on the drive with the swap file. So I like PerfectDisk, and I like Vopt. And I also wanted to remind people, we got a bunch of other questions about what was that thing that allows you to see where your drive has gone, or how much space....

Leo: Yeah, SpaceMonger, yeah.

Steve: And that's SpaceMonger. So I wanted to reiterate the name of that for people who were asking that question, as well.

Leo: And there's a free version, and there's a newer version which is no longer free. But we like the free version.

Steve: Oh, SpaceMonger 1.4 is the last free one that Sean wrote, and it's all I use. I mean, his new one does all kinds of wacky things, but much more than SpaceMonger. And for me, SpaceMonger is enough.

Leo: And for the Mac there's a program that does that, as well, I think it's called Drive Space X, that is also free. Is that it? Oh, now, see, every time I do this I forget the name. There is a Mac program, and I've once again forgotten the name. For some reason I think it's Drive Space X. But anyway, good. No free defraggers unless you send us an email and tell us about one.

Steve: Well, of course, you know, Windows has one built in.

Leo: Oh, that's right.

Steve: Under Accessories and System Tools is a defragger.

Leo: Yeah, why not use that?

Steve: And it is, the technology was licensed from Diskeeper. It is a nice defragger. And that may be all you need. What I like is that, well, first of all, PerfectDisk does defrag the so-called metadata areas, which nothing else will do because it does it as a boot-time defrag, like a

preboot defrag. But Vopt and Perfect Disk both do something else, and that is they look at the amount of use you're giving to the data and arrange it for faster booting. So, and again, PerfectDisk does an even better job than Vopt, which is why I bought PerfectDisk even though I owned Vopt already. PerfectDisk looks at all the files that are used at boot time and moves them to the very front of the drive, and also looks at the frequency of use. Files you don't use very often it puts next. Files you modify sometimes it puts in a big block after that. And then files that are being modified all the time it puts right next to the free area. The beauty of that is that it tends to centralize your fragmentation, which minimizes head activity, and it means that subsequent defrags run much more quickly because the files that are changing often are the ones that are getting fragmented, and they're right next to the unused area in the drive, allowing them to be redefragged much more quickly. So it's really my current favorite right now is PerfectDisk.

Leo: Good. Very cool. I have one questions, says Dennis Jones in nearby Carlsbad - nearby to you - Carlsbad, California: One question I had about the PayPal Security Key, which I didn't hear an answer to, is how do security keys stay in sync? Because obviously PayPal has to have something that's generating the numbers at the same time. Generating a new key every 30 seconds requires the key to know what time it is within a second or two forever. Do they have clocks that accurate to put on the key, or is there some clever way of keeping the key and server in sync? That's a good question.

Steve: It's a neat question, and it's cool because the answer is there is some window that the server allows for letting the key's clock and the server's clock be out of sync. So, again, because the key is based on a pseudorandom sequence generator, and the server has the matching serial number for the key, and there's a database at VeriSign or wherever which maps the key's serial number to the cryptographic key which is being used to generate the pseudorandom numbers. That means that the server can tell what the key's number was 30 second ago, 30 seconds before that, 30 seconds before that, and what it will be now, 30 seconds in the future, 30 seconds in the future, and 30 seconds further in the future. So that creates a window which really can be as large as somebody wants to allow it to be based on how long you want the key's current number to be valid in the face of some time drift.

However, as soon as you give a number which is within the window, now the server knows within 30 seconds' range what time your key thinks it is. So with every one of these accounts, not only is it storing the serial number, but it's storing an offset from the most recent use of the key where the key clock believes time is compared to the servers. And so every time you use the key it relocks or resynchronizes the key's clock to the server's master clock to keep them from drifting too far out of sync.

Leo: Very clever.

Steve: It's really clever.

Leo: Yeah. John Pearce posted this one in the GRC Security Now! newsgroup - highly recommended, by the way. He says: My PayPal and eBay accounts have secure passwords, that is, randomly generated using your site. Oh, he's using the first 30 characters, I guess, from your password generator because it's 64 characters; right?

Steve: Yup.

Leo: He says: I have to use my Password Manager to use them since there's no way to remember them. It's a bit of a pain for me. But I do it. Once I receive the PayPal Security Key, will I still need a huge password that's impossible to remember to be secure? Or can I now use a relatively short, easily remembered password, combining that with the key digits? It would seem logic dictates something short and sweet would be fine. However, I don't trust myself to consider all possibilities. He wants your opinion.

Steve: Well, it's a great question. So what he's saying is, before I had the PayPal Security Key, that is to say, given a two-factor authentication so that I have to have this thing in my possession, I was just using my username and password. So now that I've got that, that is, I've got two-factor authentication, doesn't that mean that I'm depending less on the first factor, which used to be all he was depending upon, now I've got two factors. So can I weaken the strength of the first factor because now I've got something even stronger than the first factor ever was, which is this thing that I'm in possession of which is changing every 30 seconds? And I would say absolutely. That is, it is certainly the case that two-factor authentication allows him to weaken the first factor.

Now, consider that he has a burden of he's been relying on an unmemorizable 30-character random text string that he got from GRC's password's page. So what he's asking to do is, couldn't I bring this thing down now to something I can remember so I don't have to use my Password Manager? And I would say absolutely. But here's the threat. The threat is that he loses control of his second factor. It is physical. Somebody could borrow it or make off with it. And then their challenge is, since they've essentially got the second factor, all they now have to crack is the first factor. So you don't want to weaken it so much that it would be possible to guess his username and password through traditional brute-force dictionary attack, any of those reasons that he was using his 30-character nightmare password in the first place because by somebody getting a hold of his second factor, they've taken that completely out of the equation. Now he's only being protected by his first factor, which needs to be strong enough to balance the possibility of him losing control of his security key.

So, I mean, practically, I would say yes. Still you must practice safe single-factor security under the assumption that somebody could get a hold of your second factor, that is, of your security key. But you don't have to go way overboard any longer with a 30-character bizarro password. Just do something that's not in a dictionary, that isn't prone to brute-force attack. So it needs to be long. It needs to combine words, maybe a couple special characters, and something that's not going to be easily guessable. And then I really think you're okay.

Leo: Yeah. I mean, the other issue, of course, is that PayPal allows you to use your password without the dongle, but then you have to go through some additional security questions. So if you weaken the password too much, I don't know. And then they go through the security questions, it seems like that might be another kind of reason to...

Steve: Another way in, good point.

Leo: Michele Thomas in Olney, Maryland needs the URL - I need the URL. I was listening to Episode 106 and heard you guys mention the VeriSign fob/token/key/dongle thing, but you didn't give us a link as to where we can get them. You talked about being able to order multiple ones that could all be tied together. Well, we've destroyed that notion.

Steve: Yes.

Leo: I went to the VeriSign PIP site to sign up for a PIP account. That's nice. It'll come in handy. But I really would like a fob. She already has the PayPal token, which I got after you mentioned it last month. I like the - he or she. I like the VeriSign idea to have multiples so I can keep one in my purse - she - one at work and one at home. Or he.

Steve: Let's not be discriminating here.

Leo: I'm not going to make any exceptions. So first of all we should say that, as Steve mentioned at the beginning of the show, that was an error. You can't get three and have them all be the same account.

Steve: Correct.

Leo: Each token is a separate account; right?

Steve: Now, you know, I hadn't thought this through. I'm doing this on the fly here. But if you had multiple PIP accounts, each single account associated with a different dongle, then we're back in the game, Leo. No one says you can only have one.

Leo: Well, many people have many OpenIDs. That's right.

Steve: Well, exactly. So all you need to do is have - hey, that works. So you [trumpets].

Leo: VeriSign may not like this, but yes.

Steve: Yeah, so you create multiple PIP accounts, and you give them, like, you know, for example, I'm stevegibson.pip.verisignlabs.com. So I would be stevegibson1.pip.verisignlabs.com, stevegibson2.pip.verisignlabs.com, and stevegibson3.pip.verisignlabs.com, each one associated with a different dongle. I then write a 1, 2, and 3 on the back of my three VeriSign dongles, have one at home and one at the office. And when I want to authenticate, instead of having a single authentication URL, now I have one that matches each dongle. But no problem because I just give each of those PIP accounts the same data to authenticate myself. So we're back in the game.

Leo: Okay, good. So, good, yeah.

Steve: We are recording now Episode 108. Michele was listening to 106 where she was unhappy that she had no URLs. In 107 we talk about this explicitly, and the URLs are all in the show notes.

Leo: So go to the show notes for - it's a long URL or we would give it out; right?

Steve: Yes. And there's a bunch of funky ones. Now, here's the other catch is that Michele already knows this, Leo, because she's a loyal listener.

Leo: She's heard it by now.

Steve: Exactly. So she sent in her question, frustrated after listening to 106. And then she found that it was magically answered in Episode 107, even before I read her question for Episode 108, which is what she's listening to now. So everybody's happy.

Leo: Now, we should say that the show notes are on your site, GRC.com/securitynow.

Steve: Yes, under Episode 107.

Leo: And there are show notes for a lot of episodes. Look at it on there. Wow. Starting with "As the Worm Turns" in August 19, 2005, that's Episode 1, all the way up to Episode 107, which will go up - it's not on right now because we're recording this early, but will go up any minute now, I'm sure.

Steve: So just to deconfuse people who have just been crossed by all this...

Leo: It's a time thing.

Steve: At the top of this episode I reported and corrected the mistake of my assumption that because VeriSign would allow you to purchase up to three dongles at once - oh, and by the way, Leo, I have verified that you can get even more because I bought another three.

Leo: Oh, wow.

Steve: Just because I love them. I think they're cool. So now I have six of those.

Leo: Do you give them out as party favors?

Steve: They're just neat. Actually I'm thinking maybe I'll use them with my own employees for some future stuff, too. So it's just very cool. So I corrected my assumption that you could, as the VeriSign guy puts it, bind more than one dongle at a time to a PIP account. But nothing prevents you from having multiple VIP PIP accounts, associating one dongle with each, and just putting in the URL, which you're able to create for yourself, put in the URL with a 1, a 2, or a 3, and write that on the dongle, and then we've solved the problem. You've got multiple dongles. She can have one in her purse, you can have one at home, one at work, wherever you - as many as you want them, and just set up a separate account for each one, and you're good to go.

Leo: That's easier obviously with a PIP account than it would be, say, with a PayPal or eBay account because you only have one. I have one PayPal account.

Steve: Exactly.

Leo: But PIP it doesn't matter, you can have as many as you want.

Steve: Anyway, we did confirm with the PayPal guy that it is only a single dongle for now. And now that we know that they're using VIP, the VeriSign Identity Protection technology for the back end, it probably won't be until they allow multiple token bindings that it would be possible for PayPal to do that, too.

Leo: Of course they would keep their algorithm top secret because it's probably tied to the ID in some way. And so there's no way you could use a dongle for your own purposes because there's no way you could regenerate those tokens programmatically.

Steve: Well, and not only that, but you do get - oh, actually when you - in this case you don't get any documentation. But I also got some SecurID dongles from VeriSign directly that use a different technology. They've got a constantly changing display. A little bar graph on one side has - it decreases to zero height, and then the number changes. And I think it changes every 30 seconds. So it's every five seconds a little square disappears to give you warning of when the number's about to change. So that's simply based on time. But when you get those you also get a CD with a set of XML files giving you the cryptographic key associated with each of those. Now, as far as I know they're still not documenting the technology.

Leo: They couldn't because that would viol- then you'd have something completely insecure.

Steve: Well, no, it's because there's no way of knowing from the outside without that XML file what the key is. So they are providing that to you. Anyway, I'm going to do a little more research on this because, frankly, I would love to be able to use the dongles myself directly and not need to go through the VeriSign back end in order to make the technology go. So that's my next email to our VeriSign friend.

Leo: Yeah, yeah. They can't very - they could show, I guess, the code, well...

Steve: And remember that the back of the key, the back of the fob/dongle/doohickey/gizmo, it's just a serial number. That doesn't give you any information about what the cryptographic key is. There's a database that they have that matches the serial number to the cryptographic key. So even knowing the serial number and knowing the algorithm wouldn't help you guess the next number because you would never know what that key was.

Leo: Which is why I was wrong, you wouldn't want to tie the serial number to your algorithm except internally in some secret way.

Steve: Exactly.

Leo: Jeff Schmidt, traveling somewhere in Northern California, he wants to encrypt his laptop drive. He says you briefly mentioned in 106 the Hitachi Travelstar disks with bulk data encryption. I know you've only got a thousand different subjects or tasks competing for your time, but for what it's worth I vote for hearing more of your thoughts on this.

What do you think? Well, you like it; right?

Steve: I very much like the idea.

Leo: It's strong encryption; right?

Steve: Yes. Well, it is Rijndael AES encryption, which is state of the art, I mean, that is the good crypto technology to use. I should digress a minute. When we were talking about the passwords page, I don't remember whether I mentioned - oh, I think I did. It was the first part of last episode that I talked about having rewritten the algorithm for the passwords page. I submitted 16 megabytes of data to those security researchers who had decided that I didn't have enough entropy in my passwords. Well, they're happy now. I've got something like 7.999989 bits of entropy out of a possible eight, so as much as anybody. But what's very cool is I wrote my own Rijndael algorithm, that is, my own Rijndael cipher, in Assembly language. And then they asked - but just because, you know, that's me. Then they said, how many - how fast is your password generator? Well, it generated, I don't remember the number now, but it was like 81 million bytes of pseudorandom data per second. And on their chart it is the fastest pseudorandom number generator there is.

Leo: Really.

Steve: Yeah. So there's Assembly language for you.

Leo: Wow, really.

Steve: Yeah, the fastest one there is.

Leo: That's cool. That's really cool. He also wants - he says he knows you're a Windows guy, but he wants to know if the Travelstar would work in his MacBook Pro.

Steve: My mission...

Leo: Go ahead.

Steve: My mission is to nail this down. I tried to do some research so that I would have an answer to this question by the time you posed it to me, Leo. And I cannot find any documentation over on the Hitachi site. So I'm going to have to get a hold of someone.

Leo: I'm sure it uses a Windows client to interface with the hardware.

Steve: Well, it can't because the entire drive is encrypted.

Leo: Of course, it's got to be in BIOS.

Steve: Exactly. It's going to have to be something that is done in the BIOS when the drive is initially being booted. And I think that the way they would do it is that they would simply use the standard security technology that is a part of the ATA spec to, you know, where you lock the drive. Rather than locking it, they would now use that, they would take the password you give the drive, hash it into a long key, probably a 256-bit key, which is what the Rijndael AES cipher wants, although it can operate in 128, 192, or 256 bits. But I think I remember seeing that it's a 256-bit key, and that that's what they would use. It's got to be done at the BIOS time. But I'm wondering if there's a recent extension to the ATAPI spec, which is the protocol used to talk to the drive, which supports bulk data encryption. That's what I'm going to see if I can track down, in which case you might need BIOS support in order to get the benefit, rather than being able to swap it in. Anyway, I've got one of these drives. It's on my list. As he says, I've got a long list. But I'm going to see if I can track this down.

Leo: Sounds like something Apple would have to support in its EFI boot stuff.

Steve: Don't know yet.

Leo: Yeah. Interesting. Edward in Fort Collins - because Apple does use, I'm sure, standard ATAPI controllers. So if it is an ATAPI spec, shouldn't be a problem.

Steve: Yes.

Leo: Edward in Fort Collins, Colorado raises a very good question about virtual machine use. He says: My wife is stationed in Korea for a year. Before she left I installed VMware Player with an Ubuntu appliance for her to do her banking on. Oh, that's cool. What a good idea. She asked the question, if she has a keylogger on XP, or some other form of spyware, can the hackers see what she's doing in VMware since it's running with Windows at the same time? Oh.

Steve: That's why it's such a good question, Leo. And the answer is she's probably vulnerable.

Leo: Depends on the keystroke logger, of course.

Steve: Well, exactly. But his point is exactly right, and this is why I wanted to bring the question up because it's very good. What we've talked about using virtual machine technology for is containment. That is, in a VM you're containing something bad from getting out. You're not letting it modify your global machine, your host machine. You're keeping it contained. His question is, what if something - essentially he's inverted that. He's wanting to use the VM to protect what goes on in the VM. The problem is, it's running, it's on Windows, it's hosted on Windows, meaning that anything it does needs to run out through Windows. So, yes, this is not a safe thing to do. We don't know again that a keylogger that exists today could do this. Certainly the VMware system is putting keyboard and drive and network drivers into your system in order to achieve its goals. But there's nothing to prevent something in the kernel from chaining onto that driver and capturing from the VM.

Leo: When the VM window is active, though, does it capture the key scans directly? Does it go through Windows at all? Doesn't the VM window capture it?

Steve: Well, there is no "directly." It's going to be down in the kernel, and there could be drivers in the kernel, and VMware does install drivers. But drivers can be intercepted.

Leo: I'm just wondering, if the window's active, does it bypass - essentially the way keystrokes work is that the scan codes are sent from the keyboard, as you say, to a driver that then interprets them as keystrokes. Is the Windows driver active when the VM window is active?

Steve: Yeah.

Leo: It is.

Steve: Yeah. Oh, yeah.

Leo: There's no way to turn that off. So when you switch the context, you're not switching all the OS context. You're still operating within the OS.

Steve: Exactly. And in fact the installation of VMware's acceleration drivers is optional. So VMware will run without installing any of its own special drivers. Those just make things go better. So without them you're really vulnerable, but even with them you're still in Windows kernel. Windows kernel is hosting this session. And you're needing to run through the kernel and through Windows drivers in order to talk to the hardware. So the real takeaway from this is inverting the model, that is, wanting to do something secure in a VM to keep it from Windows is not at all the same as doing something dangerous in the VM that you want to keep out of modifying Windows. Those are two very different things. One works; the other one really doesn't.

Leo: So the way to do this properly would be make a boot CD...

Steve: Boot CD, exactly.

Leo: Yeah, a Linux LiveCD.

Steve: Yes.

Leo: And if she has to save her banking information, then you'd have to solve that problem separately.

Steve: She could do that maybe with a dongle, for example.

Leo: Right, encrypted drive or whatever. But, yeah, that would be very secure then. Unless there's a hardware keystroke logger.

Steve: Oh, you're right.

Leo: In that case you're out of luck. They've got you. If they got in so deep that they put in - replaced your keyboard or put something in between your keyboard and the computer to log keystrokes, you're out of luck. Which is why, even if you used a boot CD in the library, it's...

Steve: Sounds like maybe she's using a laptop. He says: She's stationed in Korea for a year. Before she left I installed VMware. So...

Leo: A CD would be a way to do this.

Steve: A CD is a great solution, yes.

Leo: Rob Strating in Hudsonville, Michigan has a great question for encrypted hard drive users. Want to know if the decrypted contents of the encrypted information on a sector in your new Hitachi hard drive makes it easier to find the AES key to decrypt the entire thing. Hmm, interesting. I ask because in any Windows installation the boot sector of the hard drive is always a constant. Back in the day, IO.sys and MSDOS.sys were written in known locations of the drive. In modern times it's the NTFS bootloader. Would it not make the encryption infinitely easier to crack for that sector, and then the entire drive?

Steve: That was a really good question.

Leo: Boy, they're asking tough ones today.

Steve: Yeah, we've got great listeners, Leo. As a consequence of the way the encryption is being done, there is really no solution other than brute force. The reason he asked the question, and I assume he's been a listener for a while, is we have talked about many instances where knowing what the so-called "plaintext," that is, the nonencrypted data is, knowing what that is would allow you to attack the key because there are - oh, in fact this was one of the main weaknesses in the original implementation of Wi-Fi encryption, the WEP encryption, was that many of the contents of the packets were not changing. WEP used a pseudorandom sequence generator to generate scrambling data, essentially XORing pseudorandom data with the plaintext. And the problem was, all you had to do was re-OR that, re-XOR that with the plaintext, and you got back the sequence.

AES, that is, the Rijndael cipher, is a symmetric cipher. So, and it's a block cipher that takes 128 bits at a time and maps it using the key, the secret key. It maps that 128 bits to a different pattern of 128 bits. So it's certainly the case that, for example, take the partition sector. If we're encrypting the hard drive, we're encrypting the entire hard drive. So the very first sector on the hard drive is the partition sector. Well, we know a lot of what the contents of the partition sector is in the drive. So essentially you would know what the first 128 bits are, and you would - that is, of the partition sector. And you would know what they mapped to in the encrypted case, that is, what they encrypt to through Rijndael.

However, you quickly get lost because Rijndael uses, and I was referring to this last week, the so-called CBC, the cipher block chaining. When you actually employ symmetric encryption, you don't simply encrypt each block of 128 bits by itself. You take the result of the previous encryption, and you XOR that with the plaintext before the next encryption. And actually I have a diagram of that process down at the bottom of the passwords page now, at GRC.com/passwords, if someone wants to see sort of a schematic of how that looks. In order to make this work, there is what's called the initialization vector that I referred to also last week. And that'll be an additional 128 bits of secret data. And so you have that 128 bits plus the 256-bit key. And essentially it means that you need to do a brute-force attack, even though you know what some part of the plaintext and some part of the encrypted data is. The way this mixes the data together means that immediately as you start encrypting blocks of data, you're reduced to a brute-force attack. And that means you've got, what is it, 256 plus 128 is 384 bits of secret data that you need to brute-force attack and, you know, have a nice day.

Leo: I like that. And I think one of the reasons he asked the question is because in encryption techniques like DVD encryption, CSS, the key has to - same thing with HD-DVDs, AACS, the key has to live on the player. And so maybe that's why he's asking this question is...

Steve: Yes, and that's a very good point. The key has to live on the player, or it's often, as we know, it's discovered in RAM because it's being used on the fly to decrypt the data.

Leo: It has to live somewhere to work.

Steve: Right. And that's one of the things that's different about hard drive encryption is that the drive itself does not have the key. It doesn't know the key. It needs to receive the key when it's booted up and initialized. But it never stores it anywhere on itself. It lives on the drive where you can't get it out. And it's being used to encrypt and decrypt the data on the fly.

Leo: But where's the key? Is it in BIOS?

Steve: The key, well, it depends...

Leo: It's somewhere on the hardware; right?

Steve: Well, and that's where the Trusted Platform Module comes in, because it's going to be in the Trusted Platform Module where, again, you cannot get to it.

Leo: We hope. I would never assume it can't be gotten to. Hackers are very determined. But there's less incentive. I mean, really, frankly, it was one thing to figure out how to crack DVD encryption. It's another thing to figure out how to crack hard drive encryption.

Steve: Well, and also remember that, for example, the user has many modes of operation. They could use their fingerprint scan to unlock the Trusted Platform Module, which then unlocks the key that goes into the hard drive to unlock the drive. Or if they wanted more security, they could not use the Trusted Platform Module and have to type in, manually type in their password every single time they start up or resume the drive. And so they would be typing in the

password. That then gets hashed to generate the long key which the drive uses. So literally you could set up your laptop so that it is not stored anywhere in the hardware.

Leo: Interesting.

Steve: So, I mean, it can be really secure.

Leo: That's pretty darn secure. All right, Steve. We've come to the end of this fascinating episode. Boy, I thank our listeners for sending in such great questions. Fascinating. Tough ones, too.

Steve: Really. And they covered the gamut, I mean, all just, you know, large range of questions.

Leo: They do, indeed. Yeah, the VMware Fusion just came out, and I really am very impressed. In fact, in some benchmarks it's faster than Parallels. So there's another way you can run Windows on your Mac. All right, Steve. We've wrapped this puppy up and tied a bow on it. I think we're done.

Steve: We'll have a podcast for all of our listeners, without fail, next week.

Leo: Yes. I'll see you in Vancouver next week, which is coming right up. Thanks for coming. We'll see you next time on Security Now!.