
# Listener Feedback Q&A #35

**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-132.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-132-lq.mp3

---

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

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

This is Security Now! with Steve Gibson, Episode 132 for February 21, 2008: Listener Feedback #35. This show and the entire TWiT broadcast network is brought to you by donations from listeners like you. Thanks.

It's time for Security Now!, everybody's favorite podcast about protecting yourself against the bad guys on the Internet. Here he is, the good guy, Mr. Steve Gibson. Hey, Steve.

**Steve Gibson:** Hey, Leo. You know, I think this is everyone's favorite podcast.

**Leo:** Well, you're getting a lot of positive mail, is that why you say that?

**Steve:** Really, really, yeah, really do. I just - for these Q&A episodes I get to read through the feedback that we receive. And, you know, one of these days - I don't think I'll ever retire. But I would love to do nothing more than be able to read all of the feedback.

**Leo:** Just read your mail.

**Steve:** Every time I check it there's 600 pieces of email in the Security Now! folder. It's like, oh, god, I can't, I just can't read and reply. But I want everyone to know who writes how much I appreciate the feedback we do receive. And I do try to, like, rush out little quick replies when there's something that I want to reply to, but I don't want to use it on the show. So anyway, I

do what I can, and I really do, really do encourage people and thank them for sending their feedback to GRC.com/feedback.

**Leo:** Yes, indeed. We thank you very much. It's always nice to get so much positive feedback for the stuff we do. So, and I extend that to the entire network. Now, this is a Q&A episode. And we're going to get to - we've got 12 questions; right?

**Steve:** And we do have two fun ones at the end. I think we got the most clever hack and the great observation.

**Leo:** Observation of the Week and the Hack of the Week. Cool Hack of the Week. That sounds good. You want to go right into the questions, Steve? Do you have addenda?

**Steve:** The good news is it has been a relatively quiet week in terms of security disasters.

**Leo:** Good.

**Steve:** And we have a lot to cover, so I don't want to take too much time. But I wanted to mention a couple things that have just sort of been sort of buzz that's in the air. There is increasing thought about requiring encryption on different things, on corporate databases containing personal information. In fact, there's - I remember seeing a blurb somewhere abroad, some country was considering requiring government laptops to all be encrypted. So it's sort of just a general movement in a good direction.

**Leo:** Well, they get lost and stolen so often, for crying out loud, they really out to be encrypting that secret stuff.

**Steve:** Yup. And of course last week's show - and we've got a lot of questions about whole drive encryption because of last week's conversation about the FREE CompuSec product. And next week's show we're going to do TrueCrypt v5. We haven't talked about TrueCrypt since '06. And of course, as many people know, TrueCrypt v5 adds whole drive encryption, so that's very topical.

Another nice bit of news, we had talked about the stories that ISPs were interfering with their customers' actions, whatever they were. One of the large carriers was, for example, interrupting torrent downloads and things. A couple of U.S. Representatives have introduced what they call their Internet Freedom Preservation Act, which is a formal Net Neutrality law, which would be a really good thing because essentially it means that the ISP can't mess around with the data. They've got to treat it all the same. Which is really good.

One other little bizarre bit of news that I ran across I thought our listeners would get a kick out of, and this sort of falls in the category of classic security and obscurity, you know, the old phrase is that you can't rely on obscurity for security. It turns out that a German firm has built a computerized unshredder. This thing is a conveyor belt that can scan up to 10,000 little itty-bitty bits of paper at once and reassembled shredded documents.

**Leo:** Oh, my goodness, even the crosscut ones?

**Steve:** Yes, I mean, little, itty-bitty bits of paper.

**Leo:** Oh, goodness.

**Steve:** And so I've got a crosscut shredder, and I'm diligently aware of issues of identity theft. And so I don't throw things away that have any information about me on them.

**Leo:** You shred them.

**Steve:** I just run them - I stick them in the little slot, and it crumbles around for a minute, and then it turns them into confetti. Well, what a perfect example of nonsecurity, essentially. It is obscuring the document by chopping it up in bits. But clearly, with the right technology, you just dump this whole bin into some shaker that puts the bits out on a treadmill, and a computer scans it and reassembles them.

**Leo:** Now, that's a fairly expensive operation. I doubt it's going to be widespread. But if there's enough money in identity theft, I guess somebody could set it up.

**Steve:** Yeah, well, these things all start being expensive, and then they get cheaper over time. So I wouldn't - I'm not, obviously, I guess that means that after you shred, then you want to separate your documents or your confetti into 10 separate bins and drop them off at different locations or something.

**Leo:** Oh, my goodness. Or burn it.

**Steve:** Yeah. And the other thing I wanted to mention, I've been sort of thinking about your comment, Leo, last week about the closed source nature of FREE CompuSec versus the open source nature of TrueCrypt. And of course I certainly like the fact that TrueCrypt is open source. But my sense was that maybe we came off a little too negative about the closedness of closed security solutions. And what I wanted to comment, I guess, is that it would be a shame if someone didn't use something that was valuable to them for security because it wasn't open source. And I wanted to observe that the vast majority of software we use is - well, Windows uses at least - is closed source. I mean, Windows itself is closed source. All of the firewall, the personal firewall products are closed source. And we rely on them and trust them.

Now, I guess the point is that when something is closed source, you're relying on the reputation of the closer of the source, you know, the author of the product. Whereas, in theory, when something is open source, you're able to examine and look at it. Now, what most people of course do is expect that other people have looked at the open source and examined it. But in the real world we've seen instances where everyone assumes somebody else is vetting the open source code, and no one ends up doing so. Or that is to say that analyses have shown that open source code, in terms of inadvertent vulnerabilities, is not necessarily any more secure than closed source code. So I just sort of wanted to say let's not discard closed source solutions just because they're closed source, recognizing that we are depending upon the reputation of the source of the code to have integrity and the best interests of its users at heart.

**Leo:** And there's a little bit of a difference. If you're using a firewall, you're not trying to

protect against, say, government intrusion necessarily. You're worried about hackers. If you're using encryption, and the encryption was designed without your knowledge by the NSA and sold through CompuSec, that's a very different thing.

**Steve:** Yeah, although CompuSec, for example, is using AES standard Rijndael...

**Leo:** What they say. How do you know?

**Steve:** Right, true.

**Leo:** So my point is that encryption, I never use a closed source encryption product. And I think that - I think it's a little risky to use a closed source encryption product. I mean, I'm going to use a closed source antivirus or a closed source firewall. I don't think that's the same level of issues. And you're right, you have to trust. But on encryption I - there's enough good open source encryption stuff, I don't see a need to use closed source, I guess is my point.

**Steve:** Right. Well, and I have to say, I am so impressed with TrueCrypt.

**Leo:** TrueCrypt, yeah.

**Steve:** I've been, well, I mean, with the whole drive encryption of TrueCrypt.

**Leo:** Well, and that's the issue, yeah. If there were no whole drive encryption in TrueCrypt, or it weren't as good as FREE CompuSec, then I could see that.

**Steve:** Yes. And we'll be talking about it in depth next week. But I have to say we've had a lot of listeners from last week who did jump onto FREE CompuSec and are using it and liking it. And some listening to the end of our show, where we talked about the fact that TrueCrypt had added this, have been working with TrueCrypt, and we'll be reading their postings right now.

**Leo:** Yeah, I'm curious. Yeah, I'll be very curious. One other story, and I'm just going to leave this with you, and I'll send you a link to it. Interesting article, and this is more in your other area of expertise, in ZDNet by a guy named Robin Harris who writes a storage blog called Persistence of Memory. And he's talking about something called "latent disk errors," or actually "latent sector errors," LSE, and how larger drives, which you've always said seemed like a bad idea, larger drives are actually getting some serious data corruption due to LSE, and there's not much you can do about it. Have you heard about this stuff? It's very interesting.

**Steve:** No, I can't imagine what it is. I mean, I'm sure when I read it I'll go, oh, yeah, okay. But, you know...

**Leo:** Oh, I'm sure you will. This was a - it comes from a vendor, okay. But he works at a

network-attached storage vendor, Network Appliance. And so they're studying the reliability of drives. And they published something called an Analysis of Latent Sector Errors in Disk Drives. Interesting study that says 8.5 - they make a distinction between consumer drives and business drives, which they call something kind of odd, like enterprise drives. See, they call them "nearline" drives. I'm not sure what the difference is between that and - I don't know. A nearline drive is a consumer drive. An enterprise drive is a high-end drive. They say 8.5 percent of all the consumer drives developed LSE, including size, age, vendor problems, errors, these all make a difference. And they say this is why desktop RAID or cheap RAID with cheap disks is a bad idea. Anyway, I'm going to send you the link, and I'd love to get your impression on it.

**Steve:** Cool. I will definitely read it, and we'll let our listeners know. Speaking of disk errors, I had a funny little quick anecdote here. This one caught my eye because the subject line was "Damn you, SpinRite!" Eric Gerlach wrote, he says, "Hi, Steve. I picked up a copy of SpinRite a while ago when I first started listening to Security Now!. It's come in handy a few times since then, but never has it frustrated me as much as it did a few months ago." And so I'm reading this, I'm thinking, uh, okay. He says, "One of the computers at work, a point-of-sale terminal, got the dreaded unmountable boot volume error. Given that it was needed desperately that night, I got out SpinRite and did a run. A few hours later the drive was running like new again, and the night went by without a hitch." So I'm still thinking, okay. And he says, "I still had my suspicions about the drive, though," he says, "and as the computer was still under warranty, I decided to call Dell to get a replacement. When I called them the next day, SpinRite had worked too well. I could not convince the Dell representative..."

**Leo:** There was a problem.

**Steve:** "...that the drive had failed in the first place," he says.

**Leo:** This drive's fine.

**Steve:** "Then, after months of waiting, two days ago the drive failed again. Once more, right before a busy night. But this time we called Dell first and got the new drive sent. Then we ran SpinRite, and all was well again. Curse you, Steve, for making a product that works too well." And he says, "Cheers, Eric." And he says, "P.S.: I know that using my personal copy of SpinRite for work was bad form. But I've got a site license in my budget for next..."

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

**Steve:** So, absolutely. And I'm happy to trade a use of SpinRite for a great success story any day.

**Leo:** Well, now, be careful what you...

**Steve:** Okay.

**Leo:** Buy the product, folks. Buy the product. And we should reiterate now, as more and

more drives now, SSD drives are going out, Apple now is selling one with the MacBook Air, which is really expensive. And I see other computers coming out with these solid-state drives that - you do not recommend SpinRite on solid-state drives.

**Steve:** Correct. It is made for, I mean, intimately made for the technology of magnetic recordable media. And so it doesn't make sense on a CD-ROM or a DVD or, I mean, it's about the magnetic domain. That's where SpinRite's technology really does work.

**Leo:** Right, right, right. Okay. Let me see. Anything else? Oh, I sent you the LSE thing. I'll be really curious if SpinRite can work with those. I think the problem with these latent sector errors is that even the system doesn't know about them. They're just...

**Steve:** Well, I don't know what they are. I mean, they've made up a term. I mean, I've never heard the term. So I would have heard it if it...

**Leo:** Yeah, I think you would know about it.

**Steve:** If it was a common term. So they made up something. I'll find out what they're talking about, and I definitely will talk about it again.

**Leo:** They're transient errors, basically. But we've talked about that before where the ECC will fix an error.

**Steve:** Yeah. I mean, the only kind of transient error I could see would be there is checking on the cable, that is, there is a CRC test that the drive performs on the transfer between the drive and the motherboard through the cable. And that can be transient. And CRC is not a super robust test. So it's possible...

**Leo:** ECC is, of course...

**Steve:** ECC is really robust.

**Leo:** This is what they say. This error occurs when a particular disk sector cannot be read or written, or when there's an uncorrectable ECC error. And of course at that point any data previously stored in a sector is lost. But that's what SpinRite does is find those places...

**Steve:** And fixes them.

**Leo:** ...and fixes them, if it can read it. Now, if it can't read it, you are going to lose that data; right?

**Steve:** No, that's one of the cool things that SpinRite does, and this does bear on one of the questions we have today because people were wondering about what about SpinRite and

encrypted hard drives. SpinRite is able, and it's one of its best tricks, to perform a partial sector recovery. So it's - and that's what this whole DynaStat thing is in SpinRite where it kicks in, if it's unable to, after trying all kinds of tricks, to get a perfect read, and it's able to accept as much of the sector as is available, which might mean you lose a few bytes. But, for example, and that's in the middle of a directory, you could still get all of the rest of the branches off the directory and get a huge amount of data recovered. So SpinRite's able to do partial sector reads which is, you know, really handy.

**Leo:** That's good. All right, good. Well, I'm sending you this. And maybe we can talk more about this. It's an interesting subject. But right now we have plenty of questions from you, our viewers.

Glenn Edward in Notting- or listeners, since you really can't see us. Glenn Edward in Nottingham, Maryland is not, I repeat, not patch happy: Dear Steve, I downloaded and tried to apply the latest Microsoft security patches of this month. I have never before had so many failures of such patches. No damage to my system, but at least three of the five patches failed to complete. According to the logs, either some System\CurrentControlSet subdirectory wasn't present, or something (iis_www) wasn't of the proper value. I wonder if this is because I have several Windows XP services turned off for improving security, or because I haven't applied all the patches since SP2, only the ones for correcting security flaws. Are these latest patches expecting a certain state of Win XP that not everyone has? Has Microsoft created them without accounting for more than one configuration of Win XP or Win XP Pro? Should I worry these patches aren't in effect, if there isn't something present for them to patch? I've already checked the Knowledge Base on these patches, and there's nothing mentioned about downloading something to alter or supplement the system before the patches are applied. He gives the patch numbers. I don't think we need to give those out.

**Steve:** No. This is a really good question because it reflects a - well, it reflects my having given up.

**Leo:** Okay.

**Steve:** I mean, the gurus in the PC world who are our listeners will probably relate to sort of the general annoyance that - and I'm sure you will, Leo - that was first met by Microsoft's automatic patching idea. You know, the idea, it was just sort of a bend over and let Microsoft do to your computer whatever it wants to. And those of us who liked to - who actually used to know what every file was on our hard drive said, no, you're not reaching into my machine and doing things. So I well remember when I was sort of making a partial compromise. It's like, well, I'm going to review these. And, I mean, even now I don't use Express, I use Custom, that Custom option, just because I just kind of want to look over the list before it does it to me and make sure that I want all those things. And for, like, for a while I was resisting Silverlight. It's like, no, I do not want Microsoft's attempt to do their own Flash thing. But every time, here, you want Silverlight. Take Silverlight. You need this. And the same is true for many of these things.

I've got a friend of mine, a contemporary. In fact, you've met him, Leo. Bob is an old-world computer guy. And we just talked about this a couple weeks ago. He said - he was grumbling about something about Microsoft's patching. And I said, "Really, Bob, you haven't given up yet?" And he said, "What do you mean?" I said, "Oh, I just let Microsoft do what it wants. I just - it's easier." And frankly, and this is what really bears on Glenn's point, is I do think that this system is becoming more brittle. I've had some machines that are just always think they need a certain patch, and I try to let them have it, and they won't take it, and it just - it's always saying it needs this patch. And I finally got annoyed with it. It was one of my little laptops. And

so I did some research and found that there's a tool that you can get to sort of remove things that are stuck somehow in Windows Update. And...

**Leo:** Oh, that's good. What's the name of that tool? I'd like to get that.

**Steve:** I'll track it down because I still have it on that machine.

**Leo:** I get this call a lot from people who say Windows Update failed. And it's always a different place. I think this guy is assuming that there's something particular about these patches. It's not. It's a general problem. You're exactly right. It's brittle.

**Steve:** Well, yes. And, I mean, frankly, it's a daunting problem. I mean, when you think about - I'm amazed, frankly, that it works as well as it does. When you have all the interacting, overlapping, code replacement, I mean, I don't know how Microsoft manages this, what is fundamentally a disaster in progress. But pretty much they do. So my point is, as I said, I've given up. I just say, look, Microsoft is clearly developing patches, assuming that the machine that it's patching is already patched current, or to some level. And frankly, I can't wait for Service Pack 3, as we've talked about for XP, because it will resolve all of this phenomenal torrent of individual fixing of things which you have to do when you install a new machine and give it Service Pack 2 in order to get up to pre-Service Pack 3 level. So my feeling is, I still go into Custom mode just to sort of survey what they're going to do to me this month. But I think I'm better off just saying, okay, fine, go, and hope for the best. Because that is the code base against which Microsoft is developing this. And as we've agreed, "brittle" is probably the best word for it.

**Leo:** Well, you know, it's funny because I'm on the frontlines of this doing the radio show. I mean, I take callers every week who have problems. And it used to be you could get a tool, you could fix it, you could clean it up, you could - and this is not just patches. It's spyware and viruses and all of this stuff. Increasingly this system is so complex, so brittle, that the only option most users have is to start over. And when Glenn writes about how these three patches are blocked, it's not those three patches. It's not exactly - it's something about your system. And the problem is that Microsoft has to work in this hugely homogenous environment, I mean heterogeneous environment, where every system's unique, hardware and software. Every system's unique. So they can't - the only way to make it not unique is to start over. Format the drive, put your system recovery disks or Windows on there, patch patch patch patch patch, right up to the current patch, and then re-add your software. And I'm afraid that people are doing that more and more.

**Steve:** Yeah, well, they're giving up.

**Leo:** You've got to, though. What is your option?

**Steve:** That's exactly right. Otherwise you're Don Quixote, tilting at windmills and just saying no no no, I'm going to - I want to understand everything that is going to happen. It's like, oh, good luck with that.

**Leo:** Geeks have a tendency in that direction. They're, you know, they are Don Quixotes. I mean, we are, that's what we want to do. But in this case I think if you're going to use

Windows...

**Steve:** You've got to bend over, bend over.

**Leo:** Yeah. Don in Ventura has a quick Kindle question: Steve, in all of your talk about the Kindle I don't recall you addressing its suitability for reference and technical material, whether it's manuals, maybe the latest O'Reilly book. Does it work well for that kind of book? Is searching effective? Could it replace MSDN? Oh, that's an interesting idea.

**Steve:** Yes. The reason I - I saw the question, and I liked it; but it also bore on something I had done recently. I'm, first of all, I'm loving my Kindle. It is my constant companion to Starbucks in the morning when I read the stuff that I subscribe to.

**Leo:** It's great for news, isn't it? Yeah.

**Steve:** Oh, it's fantastic for news. And in fact there was a little kermuffle, is that the word?

**Leo:** Kerfuffle.

**Steve:** Kerfuffle on MSNBC, which I watch every afternoon when I'm on my Stairclimber, that involved, god, I can't remember his name now, David...

**Leo:** Gergen.

**Steve:** No. He's one of their frequent guys. No, it's the guy that Chris Matthews has on that does the...

**Leo:** Shuster.

**Steve:** Dave Shuster. He came on and apologized...

**Leo:** Oh, the Shuster incident, yeah.

**Steve:** Yes. Yes. And for making a comment about Chelsea Clinton and how the Clinton campaign was using her. And based on his apology, I was guessing what he had probably said.

**Leo:** Right.

**Steve:** But anyway, so the point is, the next morning I saw a little blurb about it, and I thought, oh, I felt like I had, like, missed that news event because it was then several days before. So I put "Shuster" into the Kindle's little search deal, and bang, there was every

reference to Shuster and little snippets, I mean, it's exactly what you want.

**Leo:** But, now, you didn't do a web search. You did that...

**Steve:** It was just all the content in Kindle is indexed. And so it indexes everything that comes in. And so that's why I love - basically what's happening is every day - I subscribe to Salon and Slate and Wall Street Journal...

**Leo:** So that's the key is you subscribe to all that stuff.

**Steve:** Yes. And so that's all coming in. It's building this news database which is indexed. So anything that comes along that I think of that I want to know about, I'm able to do a search. It's like having my own little off-the-web news search system. I mean, it's really fantastic.

**Leo:** I have to say, though, in direct response to Don, many of the reference and technical works you want are not available for the Kindle. It's just what Amazon sells. Now, you can convert it, if you've got it in electronic form, if you've got a PDF. Have you tried emailing documents to yourself and...

**Steve:** Yeah. I tried it initially to see if it would work and could work. And it sort of does. The free Mobipocket v4.2 converter, which you can get from Mobipocket, it will convert TXT and DOCs and PDFs and other things into the native Kindle PRC format. And so that's really the way to do it, I think. And then you've got control over it to a great degree.

**Leo:** I found some of them were unreadable. Sometimes a PDF wouldn't convert properly.

**Steve:** Well, and PDFs...

**Leo:** But I didn't use Mobi, so...

**Steve:** Yeah, PDFs are not inherently a text-flowing format. They're a page layout format.

**Leo:** That's exactly what happened. For instance, I had a bunch of documents that I had to review for a meeting, one of which was a letter. They were all PDFs. But apparently for some reason in the PDF that letter was turned into an image. So it couldn't scale the fonts. It was always going to look small.

**Steve:** Very good point. And some PDFs are scanned, they're made from a scanned text. And there you're just stuck.

**Leo:** Right. So it's not - it's less than ideal for reference, I think. You know, you might look at safari.oreilly.com. The Safari online thing is fantastic. All the - it's not just O'Reilly. It's Addison-Wesley, Sams, Prentice Hall, Que - my publisher - Peachpit, New Riders, IBM Press, Macromedia, Adobe Press. They put all of their books online. You pay a fee for this.

Searchable, bookmarkable. If it's textbooks that you want as a reference, and you can get to a browser - and of course the browser in the Kindle's probably not good enough for this. Safari is amazing. It's a really neat thing. But the Kindle's not ready. I know why Don would like that. What if you're working on cars, and you could get all the manuals that you needed in the Kindle? Man, that'd be great.

**Steve:** Yeah.

**Leo:** Be really nice. Derek Rainwater, he says he's in the middle of somewhere in Texas. I don't care where you are, even if you're in the middle of somewhere, expect a visit from Hillary and Barack any day now. Your recent website changes certainly make it more user-friendly. Nicely done. He likes GRC.com. He said he's in the midst of reading Simon Singh's "The Code Book" - that is a great book - which is so relevant to much of what you've discussed during the past few weeks. I'm getting much more detailed background information than you've got time to cover on the podcast. Well, of course, it's a big book. I know Leo made a brief mention of it long ago. You might want to recommend it to your listeners. By the way, I'm one of the many who enjoy hearing you and Leo talk about the books you're reading, as well as the Kindle. Thanks.

**Steve:** I did want to mention, he's one of many people who said, hey, Steve, I love what you've just done to the site. What I've just done is...

**Leo:** What did you do?

**Steve:** I finally made time to put the script-free pure CSS menuing up.

**Leo:** Yay.

**Steve:** Yup. I'm going to do one more change to lock it to the top of the page so that the page scrolls underneath is so you don't have to go all the way back to the top to get the menu. I'm in the middle of doing that at the moment. But I really appreciated people discovering it on their own and saying, hey, you've got a menu on your site.

**Leo:** Yeah. You needed this because it was always hard to figure out where stuff was. This is great.

**Steve:** And people are discovering things they didn't know was there. It's like, hey, I didn't know you had that. How would you know?

**Leo:** Right. Look, under the freeware alone you've got one, two, three, four, five, six - you've got security, you've got utilities, you've got obsolete. I mean, this is great. I didn't notice it either. Just shows you how often - I was at GRC the other day looking at show notes, and...

**Steve:** And you notice there's a search bar there, too. I wasn't sure whether I had read that particular SpinRite story before because it was familiar to me, but I thought, I don't remember.

So I just put in one of the phrases in the story about the drive. I put it in quotes. And it said - it found it in two places, neither of which were Elaine's transcription of that. So it's like, okay, I know I haven't read that before. So we also have site-wide search, too.

**Leo:** It's really great. You did a nice job. Very well done. Thank you. As for "The Code Book," really a good book. There is another one that's a classic called "The Codebreakers." Both of them are available on Amazon. I'm just going to check to see if Audible has the Simon Singh book. That's more accessible, I have to say. He's a good writer, and it's not as technical. "The Codebreakers" is a history of encryption that was actually - it was fairly old. No, unfortunately it's not on the - but it's, like, really thick and heavy. And if you're really into crypto, "The Codebreakers" is an amazing book, amazing book. I'll find out who wrote that.

Bryan Key, Huntsville, Alabama, wonders about the value of obscurity. I think you were talking about this a second ago, security through obscurity. I'm a long-time listener, love the show. My question is this: You're always talking about how hard it is to crack encryption. You say to break RSA would take X number of attempts, cracking an algorithm with 128-bit key would take Y number of attempts, and with a 256-bit key it takes Z number of attempts. But would not a practical crack theoretically take all of these added together?

What I mean is this: If the NSA, the spooks at Fort Meade, grabbed an encrypted piece of data - by the way, we have many listeners who work at the NSA, and just a tip of the hat to them. And I'm not against the NSA, and I just - these are the guys who have the best crypto-breaking, we assume, the best crypto-breaking technology. If the NSA grabbed an encrypted piece of data on the Internet and wanted to break it, would they not have to try - ah, there's the key word - try RSA with 32-bit key, RSA with 64-bit key, RSA with 128-bit key, Blowfish, and on and on and on. Doesn't the fact that they don't know what was used to encrypt it add an even higher level of difficulty, astronomically higher?

I've never heard you mention this. I thought if it were true it would be a good point to make. That being said, I would not think that if one encryption method became the standard, then - or I would think that, if one encryption method became the standard, then not using it would actually make you even more secure. In fact, it would be less secure, wouldn't it, if everybody used the same encryption. Is that true? Can you just look at a file and say, oh, I know how this was encrypted?

**Steve:** No, and that's, I mean, it's a good point, and Bryan's right. I've never touched on that. I mean, pseudorandom data which is just noise is truly that. I mean, it is noise. It is pseudorandom data. There is no way for - and given that anything was properly encrypted, and all these different things we've been talking about are good crypto strength, the result of data coming out of, as we've said many times, out of a cryptographically strong cipher, is pseudorandom data. It is just - it looks like static. It has no meaning. There's nothing in there. So he makes a very good point. And but it highlights sort of an issue of obscurity and security. From my standpoint, and the standpoint of any formal cryptographer or crypto person, we assume that an attacker knows everything about where this came from. And this is standard sort of crypto dogma is we assume, for example, that Rijndael, AES, well, it's open and published. And that's a strength to it because it's allowed it to be really well understood and really well vetted.

By comparison, for example, our friends at the NSA have historically tried to keep their ciphers secret, you know, the old Clipper Chip algorithm was secret. And it was a problem that they had because some things cannot be kept secret. I keep talking about, for example, the problem with cell phone encryption is everyone's got a cell phone. And when we've talked about DRM, the fundamental problem, for example, with a DVD player is that the consumer has to be able to decrypt it in order to watch it. So the decryption stuff is there. Well, someone is going to pry

the lid off that chip and figure out what's going on, if just for curiosity's sake or because they want to. So any kind of security that relies upon, fundamentally relies upon the bad guys not knowing something, other than the key, is important.

And so the point is it's true that all security relies on a secret being kept. But you want to understand what secret you are relying on being kept and which you are not. And so, for example, if data were captured off the 'Net, the example that Bryan gives, well, so this is an SSL link. Well, someone capturing the data knows it's going to port 443 from a client to a server. So they pretty much know it's SSL. And certainly if they watched the whole conversation they would see the SSL session getting set up. Even doing a man-in-the-middle attack they wouldn't be able to determine the key that is being shared for the encryption; but they would know, for example, a lot about that conversation being set up. The beauty, for example, of SSL is that it is safe even in the presence of somebody with perfect knowledge about the protocol, the ciphers, and everything that's happening, and even still no one can crack it within, as far as we know, within a reasonable amount of time. And we know, we understand really well why it's strong, why it's strong security even in the face of that perfect knowledge.

So having pseudorandom data, it's very true. If it was just someone handed you, for example, a blob of ciphered data on a CD, and you knew nothing about it, well, okay, that's Bryan's point is you'd have a much harder time doing something with it than if you knew what cipher it was ciphered in. On the other hand, any cipher worth its salt is going to give you a hard time anyway.

**Leo:** Harder than impossible is still - is not much harder.

**Steve:** Exactly, exactly. After it takes much longer than nine times the length of the life of the universe, it's like, okay, well, does it matter if it's nine or 10 times the life of the universe?

**Leo:** Well, yeah. When you send a PGP-encrypted email, it clearly says begin PGP block and end it. I mean, you know it's PGP encrypted. Doesn't help.

**Steve:** Right.

**Leo:** That's the point. So, yes, it is harder, but you know you don't need it to be harder.

**Steve:** It's already hard enough.

**Leo:** Already hard enough. An anonymous sender from Calgary, Canada, says: Thank you for the site updates. Wanted to let you know how much I appreciate seeing the PPP v3 pages up. That's the Personal Paper Passwords. Perfect Paper Passwords.

**Steve:** And I forgot to mention that last week. I finished all that. For a long time, for several weeks, ever since we talked about it they have been, I'm going to get to that. So I invite our listeners back to GRC.com/ppp. It ended up being very cool. There's a form there where you can put in your own alphabet. You get to put in your own key. You can specify how long you want the passcodes to be. And in fact it's funny, when I posted this I said, hey, try putting in as the alphabet greater than, hyphen, and less than, as those just three symbols. And somebody wrote back in our newsgroup and says, wow, Steve, this is the first-ever cryptographically strong ASCII art generator.

**Leo:** That's neat. So it looks kind of cool, huh?

**Steve:** Yeah, it really is, it really came out nicely. So it's done, and we've got people are, either have upgraded or are upgrading their third-party open source implementations. So that stuff is around. Anyway, I'm sorry to interrupt you, Leo. Go on with your question.

**Leo:** Ah, yes. Well, no, you're not interrupting me, you're responding to that part. Now here's another part. It's also nice to see the new scripting-free, pure CSS menu system in use. I've been coming to this site for the last couple of years and wondered what other educational materials and resources there might be hiding in an obscure link somewhere. The new organization will help a lot.

You know, I have to apologize because I use CSS menus on my site, and I do use a little bit of JavaScript. And it's to determine if you're using Internet Explorer because if you use IE then the CSS, one little CSS thing doesn't work, and you have to modify it. I'm amazed, impressed that you got around it without JavaScript, though. That's pretty good.

**Steve:** Well, I had to use some CSS hacks. There are some things where the CSS parsers in the different browsers are known to interpret things a little differently. So I've got some, for example, I'll have a CSS callout where I've deliberately put a backslash in the word because one browser won't understand it, whereas another one will. So, I mean, sadly we're still not at a point where CSS is a standard implementation across the board, although mostly Microsoft was guilty in the early versions of IE. And the later versions of IE, the most recent one is way better.

**Leo:** Well, get ready.

**Steve:** Okay.

**Leo:** Because it's getting way worse. There's an article by the CEO of Opera. And Opera is a wonderful browser company which has for some time now really tried hard to enforce web standards in the face of Microsoft's absolute indifference about it.

**Steve:** Oh, yeah. IE5 and 6 were just horrible.

**Leo:** Well, he's talking about now IE8 and what Microsoft's talking about doing in there. And once again he's saying, you know, essentially what's happened is because Microsoft's so dominant, has eliminated competition, that they just set the standards, they do their own thing, and everybody has to follow along. And IE8 is no better. And this is my problem with those hacks is it's different every time a new version comes out. You have to update your code because it'll detect IE6, it'll detect IE7, now you've got to detect IE8. It's a lot of work to maintain CSS. It's just terrible.

He also says, he goes on: I might as well also thank you for teaching me so much through your site and podcasts. A couple of years ago I could have appreciated the concept of Perfect Paper Passwords but would have had no confidence in being able to implement a working system. All of your hard work and continued sharing is appreciated and highly valued. OH, that's nice. That's really nice. And true.

Mike Cerminara of Moorestown, New Jersey poses some drive encryption puzzlers. Put on your thinking cap for this one, Steve: Hey, Steve, I have a simple but important question. I've known about CompuSec for a while now - we talked about it last week - was put off by its closed source nature - as we were talking about just a minute ago. I've been waiting for the new version of TrueCrypt, but using it on my laptop is a nonstarter because it doesn't support hibernation. That is a big problem.

**Steve:** And the good news is, it's coming.

**Leo:** Oh, good.

**Steve:** Yep, the TrueCrypt guys understand that that's a limitation that is going to put some people off, and they're going to address it.

**Leo:** So since it was discussed on Security Now!, and you seem pretty pleased with it, I figured I'd finally give CompuSec a shot. There's only one problem. What happens if I need to mount that drive on another system? There's a number of - this is because CompuSec uses the BIOS, right, that's tied to the system. There's a number of reasons I might need to do this, migrating to a larger drive or if Windows gets hosed and I need the rest of my data. Is it possible to mount my CompuSec-encrypted drive on another system? Shall I go on, or do you want to address this?

**Steve:** Okay. If you were to move the CompuSec-encrypted drive to a different system, to a different motherboard, it would be okay because it's the process of booting it. In the case of CompuSec, as with TrueCrypt, all of the data needed to decrypt the drive is on the drive itself. So moving it to a different system would work. But there's no way to mount the CompuSec drive. That is, it needs to be booted in order for its boot-time code to function. The only thing you could do would be to boot it one last time and then, as you're booting, you can hit F2 to get some boot options, one of which is decrypt the drive now. And so that boot-time code can run through the entire drive to decrypt it. Then of course you could do anything with it that you wanted to, stick it as a slave drive of another system, because he was talking about, like, moving to a larger hard drive, where you'd have to have it and a larger drive.

**Leo:** Well, for recovery purposes, too.

**Steve:** Correct.

**Leo:** And by the way, SpinRite would work on that drive because SpinRite doesn't care about the data, it's just looking at what's underlying it; right?

**Steve:** Yes, and we got a question about that coming up.

**Leo:** Oh, good, okay. Now he wants to know if TrueCrypt has that same problem. Can TrueCrypt mount an encrypted system partition just like mounting any other TrueCrypt volume? If TrueCrypt could handle this more gracefully I'd probably be more likely to choose TrueCrypt. Does it do the same - it's the same thing, though; right?

**Steve:** I don't know for sure. So that'll be one of the things, that is a question I will answer for sure for next week's episode, show, on TrueCrypt. I will have an answer to whether you're about to mount a system partition. I sort of think not. But I will know for sure.

**Leo:** Incidentally, "The Codebreakers," the book I was thinking about is by David Kahn. I found it on Amazon, K-a-h-n. And he updated it in '96. So it's a little more up-to-date than it used to be. They also have Bruce Schneier's "Applied Cryptography," which is, if you really want...

**Steve:** That's my bible.

**Leo:** Yeah, if you really...

**Steve:** I mean, that's code.

**Leo:** That's the real stuff. Yeah, I'm talking about the layman's stuff. But if you really want the bible of it, that's the one, yeah.

Sky Moreno in Yorba Linda, California, that's in Orange County, wonders about Amazon's S3 service going down. It's gone down, it went down last week. I forgot to mention that. My name is Sky Moreno. I appreciate all you guys do, and to support you I've purchased a copy of SpinRite and send TWiT a $10 a month donation. Thank you, Sky. That money is much appreciated. Those donations are what keeps the day-to-day operation going. I should explain that, because we have ads. And I think some people, in fact I got an email from somebody saying, you know, I see you taking expensive vacations, I guess I'm not going to send you any more money. Well, I have to explain how this all works.

**Steve:** You're kidding me.

**Leo:** No. I do have real jobs which pay well, a radio job and a TV job.

**Steve:** You've got a family.

**Leo:** And I support them with those real jobs. And frankly, I support TWiT with those real jobs, too. It's not like - now that we're getting advertising it's a little bit better. But essentially I donate my time to TWiT. Thank goodness I have a real job. And your donations go to the infrastructure, the things I have to pay every month - rent, Dane, servers, equipment. That's where the - those donations. And the monthly donations are great because then I know I have a certain budget every month because I know it's going to be consistent. When we get ad revenues then, as Steve knows, TWiT takes a small operating fee, and then we split the rest with the participants. So essentially all the ad revenue but a small part goes to the people who are doing the shows, as it should be, and that's why the ads are important to me because they pay people like Steve, who otherwise do this for free. TWiT for the first two years really was a volunteer operation by me and the hosts, and is only now starting to get on its feet in terms of - and I still don't draw a salary, but that's all right.

**Steve:** Well, and you know, we also have toys to buy, Leo. I mean...

**Leo:** We've got to pay for this stuff. This is...

**Steve:** Yeah, I dislike, for example, trying to get a promo copy of IronKey. I don't...

**Leo:** You just buy it.

**Steve:** I just buy it because I don't want to feel like I owe these people a positive review for giving me something, and I don't want to have to worry about sending it back. So we have a serious toy budget around here, too. So we know what all this stuff is.

**Leo:** And I do the same thing. I don't take loaners in general. I actually do have a loaner, a rare loaner right now, the MacBook Air, but that's mostly because I didn't want to buy it.

**Steve:** And you know I'm not that impressed by it.

**Leo:** It's pretty. It's light.

**Steve:** Yeah, but it's not, I mean, compared to the MacBooks it's like, okay, so it's thinner. Okay, well, thin is good, I guess. I thought, eh, I mean, I didn't have to have one.

**Leo:** No. Me neither. Me neither. And so I could have bought one, but I just thought, you know, I actually didn't, and they called me up and said wouldn't you like a month loaner, and I said okay. But normally, like you, I don't want to be beholden. I want to be able to say this thing's crap. You know? I want to be able to say that. And when they are - it's hard...

**Steve:** Yeah. And I ran my car over it, and now I feel much better.

**Leo:** You might say, oh, you can always say that, they understand. And of course they do. They never say, oh, you just gave us a - well, most of them don't say that, you gave us a bad review. But there's a human thing that, when somebody's very nice, and they say, oh, please try our product, it's hard to say bad things about it. So I don't - that's why I don't even get to know these people. I don't want to know them. I don't want to like them.

**Steve:** Exactly.

**Leo:** Anyway, he says, I hope you and Leo keep up the great work. I own a small network integration company down here near Steve in Orange County. After listening to the netcast on Jungle Disk, which both Steve and I use for backup, I immediately signed up and started sending all my family photos out to Amazon, 5,500 of them. I was surprised about them going offline, wanted your comments on them going dark. Should I and Jungle Disk users like you and Steve worry about this?

**Steve:** Well, this caused a great deal of controversy because Amazon had their much-

ballyhooed...

**Leo:** 99.99 percent up time.

**Steve:** Yeah, and their so-called SLA, their Service Level Agreement is what it's called, and that's a jargon in the industry for 99 - I don't know, what is it, like five nines, 99.99999999? Anyway, they're not supposed to go down. And it's like, oh, we're spread around the country, and we've got fault tolerance and resilience and self-healing mumbo-jumbo. And unfortunately, starting about 5:00 a.m. Pacific time, I think it was Friday, they were gone from the - their West Coast facility was down for as much as four hours, and then kind of came limping back online, and things were slow.

And there were a number of people whose businesses depended on Amazon S3. That is, there were photo-sharing websites that use S3 as their back end. There were greeting card companies and all kinds of things that were like, they were out of business while Amazon was down. And there were several people that said, well, this cost me $5,000. And I could have bought a couple servers for $5,000 and be doing this myself. And so my reaction is, well, this maybe was a good lesson for people about how not to rely on S3 if you're worried about this. I mean, first of all, it was extremely expensive in terms of Amazon's reputation. This hurt them a lot. Which to me means they're going to make sure this doesn't happen a lot. There was, of course, a Blackberry outage not long ago, too.

**Leo:** A couple, yeah.

**Steve:** And I was going to say, and not the first one, that had all the Blackberry people freaked out for a few hours because they couldn't - they weren't - they couldn't jack in directly into their neural system and get their email the moment it came in. And so my feeling is, I'm not worried. And like you and I do, we use it for backup. So it is trickling out of my machines as needed. And Jungle Disk is very robust in the face of my link coming up and down, Amazon coming up and down, my laptop coming up and down. Basically, when it's got a connection and everything is working and happy, it sends what it can up to Amazon. And so I'm not relying on S3 for being able to get access to mission-critical data. And I would say, well, this is perhaps something that people want to consider when you use an outsourcing service. I mean, imagine what would happen if the Internet went down. We know all why it really can't because it's just so phenomenally redundant and was designed for the packets to be able to find a way around. And ISPs, well, there are ISP outages, and of course there are attacks which cause problems. But in general it stays up pretty much and is robust. But when you rely on a service like this, well, you need to think about what happens when it's down.

**Leo:** Yeah. And I, you know, I think they're still going to be pretty reliable. They say it wasn't their servers, it was their authentication got overloaded. Too many people were using it.

**Steve:** Yeah, got to beef that up, then.

**Leo:** Beef that up. Jeffrey, Columbia, Maryland, wonders about whole drive encryption backup and imaging: Steve, I encrypted my entire hard drive with TrueCrypt. I do have a question that comes to mind now - now? - now since I'm using full-disk encryption. Do I have to decrypt my entire drive before I make a backup image of the partition that has my OS on it? I've tried using Acronis True Image on it after I encrypted it. Acronis knew where

the partition was but didn't recognize the file format of the partition. Obviously, this is because it's encrypted, and it's just random data. It would let me make an image still if I wanted to, which I did not. Is this one of the downfalls of full disk encryption? How do you make an image of it? Yeah.

**Steve:** Yeah. Really, really interesting. A couple things. First of all, there's a complete difference between, and we'll discuss this further next week, but I just did want to address the question. I mean, I felt a little up in the air as I was reading through these questions that people had sent because I still want to talk about TrueCrypt. I didn't want to hold these off until the Q&A after TrueCrypt because I figured, okay, we'll put this right in between FREE CompuSec and TrueCrypt so it sort of answers some questions that we'll be dealing with in more detail next week. The real issue is whether you're doing an imaging inside of Windows, or your OS in the case of TrueCrypt, or outside. So, and there is some impact. For example, if you're using an external imager - as I assume Acronis must be. Certainly I know that PowerQuest's Drive Image is.

**Leo:** It's the same. Yeah, it's just - it's software.

**Steve:** And sort of like an external ghosting of the partition. But it runs, for example, it boots itself, or boots...

**Leo:** No, it runs within Windows.

**Steve:** Okay, well, now, this is different, then. If you use an external imager...

**Leo:** I see what you're saying, like Ghost, which you have to boot to.

**Steve:** Ghost, exactly, or Drive Image from PowerQuest that was one I was using for years, years ago, before Symantec sucked them up and killed them. There it's going to see, first of all, several things. It's going to give you no compression. And the imaging that gives you compression is very handy because the imagers often recognize a file system. They know not to bother saving empty sectors. And lord help us on a - if you've got a 500GB drive, hopefully you're not using all of that. So it's a real saving for the imager not to be able to - not to have to image data that's not in the file system, and to be able to compress it. Well, if you're running an external imager, and the drive is compressed, the entire drive just looks like an opaque blob of pseudorandom data. Maybe the external imager won't work at all. PowerQuest is pretty finicky. And I'll bet it would not have worked at all. It wouldn't have even offered to do just a snapshot of whatever this blob...

**Leo:** It could do a bit copy, though; right? I mean, it could go bit by bit, sector copy.

**Steve:** Well, an imager could. But I don't think that PowerQuest Drive Image does because it complains if anything is wrong with the partition. So it's really caring about it. He says that this thing would have been able to make an image, so perhaps that's the case. Now, I've already experimented with my favorite in-Windows imager, which is Drive Snapshot. And because it's running in Windows, it's asking the device driver for the drive image data, which decrypts it on the way to it. So what's interesting is, and this is an important thing for people to recognize, is in the case of Drive Snapshot you still get the compression benefit and the unused space not

being stored benefit. But you end up with a decrypted backup. So your backup is decrypted because it was done by Windows on behalf of the program running in Windows. So again, you would then want to maybe manually encrypt it or maybe run Drive Image into an encrypted file container in TrueCrypt that we'll be talking about next week. That would give you a still-encrypted image. So there are ways around this. But it's definitely the case that imaging changes relative to whole drive encryption.

**Leo:** Yeah. Yeah, very interesting. I actually hadn't even thought of that, so that's good to know. He says should I make - unencrypt, make images, and reencrypt? That sounds like the way to do it, then.

**Steve:** Well, it really depends upon what your tool is.

**Leo:** Of course you don't have an encrypted image, yeah.

**Steve:** Yeah, it really depends upon what your tool is. If you, for example, say that you had to use the old PowerQuest

Drive Image that booted DOS and then ran outside. Then you would have no choice but to decrypt your entire drive, leave Windows, image the drive - whoa. And then again remember, the image is again nonencrypted. So you've made a nonencrypted image. Then you'd have to reencrypt the whole drive to get back in. So it's like that seems like the wrong thing.

I think the solution would be to use something like - maybe Acronis will do it. The question would be, does True Image, you know, how does it work? I'm not familiar with it. It's not the one I use. I use Drive Snapshot. And I know, because I've experimented with it already, that it works beautifully on a TrueCrypted volume, or for that matter on a FREE CompuSec-crypted volume. But it's - and you get the compression benefit, it makes a smaller image, all things which I like. Then you encrypt it, for example, using a TrueCrypt file container, in order to - or just do a standalone encryption of that file so it's safe and it's small. And I think it's much nicer to have much smaller images than to just take a, I mean, literally a sector-by-sector copy of the physical entire drive. That's big.

**Leo:** Jeffrey of Columbia, Maryland, wonders about whole drive encryption backup and imaging. Oh, we already did that one.

**Steve:** You're right, we did.

**Leo:** Number nine. Here we go. Isaac, a proud SpinRite owner, I'm glad to say, in New Orleans, wonders: Hey, Steve, I was just listening to Episode 131, last episode, hearing you explain FREE CompuSec's driver handoff procedure. And I wondered, what happens if Windows doesn't work, and you need to run the Recovery Console to repair it? Oh, that's a good question. Does CompuSec's boot driver support the Windows boot disk repair procedure and third-party SCSI/SATA driver installation? That's when you press that F6 thing and put a disk in. If not, does that mean that the console will find no installed versions of Windows, since it's all just random noise on the drive?

**Steve:** Yeah, this is a great question. And I should say, here we are at the Q&A between the FREE CompuSec episode last week and the TrueCrypt episode next week. And I've got to say I'm very, very impressed with TrueCrypt. I'm going to go into detail about how they compare

and why I'm so impressed with TrueCrypt. But essentially I was doing the FREE CompuSec whole drive encryption research prior to the release of TrueCrypt 5, and I didn't know when that would be happening. So in my opinion, although the FREE CompuSec system has many other features way beyond, you know, we talked about, I mean, it'll basically encrypt and decrypt every channel in and out of your machine, you know, standalone drives, your network connection, just sort of everything. It really locks down a system from an encryption standpoint. Whereas TrueCrypt only deals with what we know is storage encryption/decryption on-the-fly stuff.

My point is, if that's all you need, I really think TrueCrypt is a superior solution, and I'll be explaining exactly why it's superior next week. So I did want to entertain this question about FREE CompuSec since we had talked about it, of course, last week. But in my opinion - well, for example, I've removed FREE CompuSec from that system. It is now running whole drive encryption under TrueCrypt.

**Leo:** Oh, wow.

**Steve:** So absolutely.

**Leo:** You got a lot of listeners who started using CompuSec after last week going, what? Wait a minute. Hold on there.

**Steve:** There are many reasons why TrueCrypt that came along afterwards is superior, and I've switched over to it. But to answer Isaac's question, if you had a problem, and Windows would not boot, there is an option. You hit F2 as FREE CompuSec is booting. That gives you an emergency decryption menu that would then allow it to sit there, unencrypt the drive, put it back to its original condition, and then whatever it is that Windows wants to do, if you need to do, you know, a Recovery Console or anything wacky, it's then decrypted so you can proceed with whatever you want to do.

**Leo:** Interesting. That's a good solution.

**Steve:** Yeah. It's nice, and it's good that they have it. But I'm not using it anymore.

**Leo:** Well, whoa, okay. But we'll find out more about that next week when we talk about TrueCrypt and the TrueCrypt 5 which has this whole disk encryption technique. But in general, Isaac's absolutely right. Because it is random code, you're not going to be able to do the recovery thing unless you decrypt first.

**Steve:** Yeah. It'd be interesting to experiment with the Recovery Console. I didn't because, you know, there is this handoff going on which is how both TrueCrypt and FREE CompuSec work. That is, you're booting, running decryption code, which is - it's probably intercepting Interrupt 13, as I mentioned last week. Interrupt 13 is the BIOS routine which pretty much all software starts using in order to get itself going. And then as the OS boots there's a handoff between Interrupt 13, which is the BIOS's original technology for reading sectors from the disk, and the system's own protected-mode drive, which then takes over. So...

**Leo:** But that driver does not run in Windows. That's a kind of a BIOS-level driver,

effectively.

**Steve:** Well, there's two drivers. There's the external FREE CompuSec/TrueCrypt code which has to intercept the BIOS in order to decrypt the contents on the fly.

**Leo:** And where does that code - does that code live in the boot record? I mean, where does that code live?

**Steve:** Well, now, that's very interesting because there's a question, in fact we're about to, oh, no, wait, where is the question? We didn't have the question. Oh, no, it's one of our last...

**Leo:** Coming up.

**Steve:** It's one of our last two, 11 or 12, which was a really interesting interaction that this guy had in his application, whereas FREE CompuSec would work. FREE CompuSec, because I looked at the first track of the drive, wondering if FREE CompuSec's code was there. And it's not. What they do is, their boot sector, that first sector of the drive that contains the partition table at the end of the boot sector, it references some physical sectors out on the disk in the Windows partition which are locked and prevented from moving. After FREE CompuSec was installed - because I was doing this benchmarking of it, remember, that I determined that it had about a 9 percent performance overhead - I noticed that there was a bunch of regions of the drive that were now locked, that were resistant to any defragging because their physical positions were known to the boot sector. So the FREE CompuSec code itself lives out in the Windows partition. What's different about TrueCrypt is that TrueCrypt puts itself down in that first track. And that can cause some problems.

**Leo:** Oh. That makes sense. So they do have to load before Windows loads, obviously, or they wouldn't be able to load Windows. So if your recovery occurs after they're loaded, then you'd be able to do the recovery stuff.

**Steve:** Except that the system...

**Leo:** Recovery is booting from a CD, though, so you wouldn't be able to do it because a CD doesn't know to load the thing.

**Steve:** Well, and there's also the Recovery Console, or like the various safe-mode boots where you might be - you might not be loading a special driver as part of safe-mode boot.

**Leo:** So it is loading as a Windows driver. It's not loading pre-Windows.

**Steve:** Well, it's both. It's both. And that's the cool thing about this. And this, actually, it's why it's hard to do. It's why there isn't a lot of this being done now is that it's both. You need decryption outside of Windows until Windows gets going, and then you need a preinstalled Windows driver that can take over and continue decrypting as Windows boots and from then on. So there's an outside and an inside portion to all of these solutions.

**Leo:** Got it. So really the answer to his question is, well, depends. Or better, it probably doesn't.

**Steve:** Well, the answer to his question was that there is a solution, which is if Windows was having trouble...

**Leo:** Oh, yeah, I see, you use the boot console, encrypt console, right.

**Steve:** You hit F2 to get in and, like, do the emergency decryption is what FREE CompuSec calls it.

**Leo:** Got it.

**Steve:** And of course TrueCrypt has a whole bunch of options that we'll be talking about next week.

**Leo:** So you better listen. Matthew Simmons in Raleigh, North Carolina wonders about confusing SpinRite: Steve, I don't own a copy of SpinRite, nor do I have a drive encrypted with either FREE CompuSec or TrueCrypt. But both are things I keep thinking about how I should do. My question is, what happens between SpinRite and - oh, yeah, this is the one you were talking about we're going to answer, yeah - between SpinRite and whole drive encryption? Presumably SpinRite can still determine the bad blocks, but can it recover the data if the drive is just filled with what looks like random noise? And how can SpinRite tell what is real data and what is broken data? Doesn't care, I presume. Similarly, how resistant are TrueCrypt and FREE CompuSec to hard drive failures or partial failures through bad blocks?

**Steve:** Yes, this is a really good question. Not necessarily the SpinRite portion, but the question of how resilient are TrueCrypt and FREE CompuSec to hard drive failures or partial failures through bad blocks, as he says. First of all, SpinRite is able to operate on just a blank drive, one you just get open, take it out of its hermetically sealed, electrostatically proof plastic bag and stick it on SpinRite. SpinRite doesn't care what you've got. It'll just show you that you've got a blank drive. If you've got a partition table with partitions, SpinRite will show those to you, and you're able to choose which ones you want to run it on, if you don't want to run it on the whole drive, or you can choose them all.

So we were talking earlier about the one cool thing in SpinRite is its Dynastat data recovery, that is, the ability to recover portions of sectors, that is, to recover all but the unreadable part, essentially. Now, one of the features of whole drive encryption is that they encrypt on a sector level, that is, sector by sector. So each sector is encrypted individually. But they use a technology similar to what we've talked about before, similar to the Cipher Block Chaining, CBC, mode, which means that all of the data that you're encrypting is dependent upon all of the data that you have already encrypted or decrypted. Which means that that does create a subtle weakness in this technology. That is to say, if there were some data early in the sector which was unreadable, then there is no way to decrypt the rest of it. Or that is to say, in SpinRite's case, SpinRite would still do a partial data recovery. But because the entire sector had been encrypted, you'd still lose all of the sector from that point on, rather than being able to recover the rest of it from that point on.

**Leo:** Well, and this is the problem with encryption in general, and full disk encryption especially, is that a failure can be more catastrophic.

**Steve:** But again, I want to - I don't want to scare people off because, remember, it's limited to one sector. And the fact is only SpinRite, of any utility in the world, can recover parts of sectors. So, and this is why the people who are doing whole disk encryption are saying, oh, no, there's no difference because normally an unreadable sector is unreadable. And so you've lost the sector. So the fact that you've created in sort of internal encryption that makes the sector more brittle normally doesn't result in any, you know, in any loss because you've lost the whole sector anyway. Only with SpinRite is that not true because it can perform, and does perform, partial sector recovery. So it's like, well, okay. So there's a slight loss, if you were a SpinRite user, and you could have been - a partial sector recovery would have given you some benefit. Okay. So you can't get that on that one sector if you are using whole drive encryption. It's like, or any of the, I mean, all the encryption is working in small blocks like that. So it's like, okay, so there's some subtle weakness. But I would say it's not significant.

**Leo:** The thing that's good to know is that these encryption, full disk encryption technologies work sector by sector. So a loss of a sector isn't - doesn't mean you lose the whole thing.

**Steve:** Is only a sector.

**Leo:** It's localized.

**Steve:** Yes.

**Leo:** Is there a part of - are there any special sectors that, if you lose those, you're going to have more catastrophic data loss?

**Steve:** Yes. But that's always been the case with a file system, except file systems that are extremely resilient for loss, like maintain redundant indexes and things. The classic is, in the old FAT days, if you lost the first sector of the root directory, you were hosed.

**Leo:** Right. There's no recovering.

**Steve:** I mean, it was just - you had no way to get to anything else. And of course the FAT was important, the File Allocation Table, which is why there were two copies of the FAT because - oh, it's funny, though, because DOS wrote two copies but never used a second copy. It was just...

**Leo:** Oh, I think sometimes in a catastrophic loss some - I remember I think Norton would recover that, from the second FAT.

**Steve:** Yes. And there were certain - and SpinRite was very aware of the second copy of FAT.

**Leo:** Oh, okay, good.

**Steve:** And would automatically fall back to that. But DOS itself never read the second copy of the FAT.

**Leo:** It was for utility purposes, not for...

**Steve:** Even though it maintained it, yes.

**Leo:** Interesting.

**Steve:** And so it is important to note. We had a question pop up in the Security Now! newsgroup in our Usenet forums last week after the FREE CompuSec discussion. One guy wrote that his boss wished he had their laptops encrypted, but he was really afraid to do that because he believed encrypting the drive made a loss of any area much more, like it would spread throughout the drive, or they could lose the whole file system. That is absolutely not the case. So encryption is constrained to individual sectors. And it's done with that boundary. So it's really no more brittle than a nonencrypted drive.

**Leo:** Except for this weird case where you're using SpinRite, and you could have recovered some of it.

**Steve:** Yes.

**Leo:** But that's - yeah. And now, ladies and gentlemen, the Tremendous Observation of the Week. Dane, could you put a little echo behind that? Just, you know, give it that - what it needs there? Little echo? Here we go. This is from Steve Nicholas in the U.K. Hi, Steve. Having heard your recommendation of FREE CompuSec - see, I'm telling you, a lot of people heard that, and they say, ooh.

**Steve:** Yeah, I know.

**Leo:** We gotta try that out. I had a look at their website but found several postings in their forums regarding the fact that it doesn't, does not, create a recovery CD. This prompted me to try TrueCrypt 5.0a - he'd already used TrueCrypt - and I encrypted my entire system disk with no problems. However, after several days of smooth running, I opened Macromedia Dreamweaver for the first time since encrypting the disk. Dreamweaver told me it needed activating, and I had to let it connect to Macromedia again and activate itself, which it did successfully. Everything was fine until I rebooted my PC and then found the TrueCrypt bootloader froze after I entered my password. Ooh, that's scary.

**Steve:** Yes, it is scary.

**Leo:** He repaired it. He repaired it using the TrueCrypt recovery CD. It booted okay again.

I then opened Dreamweaver, and it again wanted to activate itself. And after doing so, couldn't boot again. So it looks to me like Dreamweaver has some copy protection built in that modifies the MBR or something and stops TrueCrypt's bootloader from working. I bet you're right. That's bad behavior on Macromedia's part.

**Steve:** It sure is.

**Leo:** Actually we should say Adobe, which owns it now. Restoring the bootloader must then overwrite this copy protection, and Dreamweaver - it's a loop - wants to be activated again, then the bootloader gets overwritten. I have now unencrypted my disk as I need Dreamweaver for my work. And I'm unsure whether to try FREE CompuSec as, if applications can overwrite the MBR or corrupt a bootloader, and FREE CompuSec doesn't create a recovery CD - thank goodness TrueCrypt does - I'd have to reformat my drive, and I've lost everything. Just letting you know this complication as I'm sure it can't only be Dreamweaver that can cause this problem. I'm sure others. In fact, the chances are good - this is Leo now - that Adobe didn't make this technology, but licenses it, as most piracy measures are, from another company. Which means other companies are probably using it. So it's probably not just Dreamweaver.

**Steve:** Well, what's going on here, and the experience that Steve Nicholas reports makes it very clear, we've got two different systems that are fighting over territory. There is, as I know from reading the TrueCrypt docs so far, TrueCrypt's code puts itself down in that first track. And remember that last week I was explaining that the very first track, the 63 sectors, the first 63 sectors of the drive, the first one is this partition sector and partition table, which is actually executed code. And then the 62 sectors which follow it are normally empty because by - not necessarily by design, but by practice, partitions always start on even track boundaries.

So it starts, so the first partition - since the first track has been ruined, essentially, by that one sector being taken, that partition table sector being taken - the first partition is forced to be bumped to the end of that first track to the beginning of the second track. That leaves the rest of the first track free, which is where TrueCrypt lives. FREE CompuSec does not live there. So it would probably be the case that Steve could use FREE CompuSec if he wanted to.

On the other hand, FREE CompuSec doesn't have nearly the robustness of recovery from disaster, which is one of the reasons I like TrueCrypt so much. I'll be talking about it next week. TrueCrypt gives you no choice but to make a recovery CD. You can't encrypt your drive until you prove to them that you have one. In fact, it was bugging me so much I found an ISO loader so I could fake it out and say, yes, dammit, I made a CD. Here, sniff this CD, and you can see for yourself. Because I was, you know, doing all kinds of testing, and I was burning up CDs. I said, okay, enough of this.

So anyway, I'll give people a pointer to that if they want to be experimenting with this. But what this essentially means is that, as you said, Leo, Dreamweaver - and we talked about this in fact relative to boot sector viruses. Remember that there are some root systems now, some rootkits which are essentially working just like whole drive encryption, inasmuch as they get control before the operating system do. Well, they're able to install themselves because Windows is not protecting the first track of the hard drive, which is the way Dreamweaver is able to reach down outside of the partition and make some changes down there, which is where they're storing their DRM, their activation scheme, whatever. They're just probably tweaking a few bytes. The problem is that now TrueCrypt is living in those bytes. So it's very good that TrueCrypt is being as picky as it is about forcing people to make boot CDs because people might go, oh, I'd really like to do that. And it's like, oh, you really do want to do that.

**Leo:** And I have to say this is probably bad behavior on Dreamweaver's part.

**Steve:** I really don't like it on Dreamweaver's part. I agree. I don't think that they ought to be going down and mucking around with the hard drive because there's going to be all kinds of unintended side effects. And in fact, what they ought to do at the minimum is to see if there's all zeroes in the area that they want to occupy. And if somebody appears to be living there, then they do something else. I don't know what. But I guess my point is there are many - there are obviously many other ways to achieve the same effect because everybody else manages to achieve the same effect without mucking around with the first track of the drive. I hope that this hurts them, and they get their hand slapped for doing this and come up with some alternative because they really ought to.

**Leo:** Well, there you go. And as I said, I bet you others are doing it. It's probably not just Dreamweaver. I understand, because what they want to do is write something where you can't see it, it's not part of the file system, so that you can't, you know, end around it. But now everybody knows it's in the master boot record. So I don't know, this is a dubious fix anyway, a dubious protection anyway.

Peter Burtis in North Conway, New Hampshire wins the Cool Hack of the Week Award. Dear Steve, I thought you and your Security Now! listeners might get a kick out of this. I'm a technology consultant out of New Hampshire. I should probably read it more like: I was very interested when you mentioned TrueCrypt now did boot drive encryption because that's exactly the solution one of my clients is looking for. But I run Macs, whereas my client runs Windows. Not wanting to experiment on my client's systems I thought, well, what the heck, I'll try it in VMware just for fun, knowing it should work in theory - ah, interesting - but also more than half expecting to brick my virtual PC because of the intricacies involved. Long story short, nope, didn't brick the PC, it worked flawlessly. The bootloader comes up on "power on," which is in quotes because of course you're already powered up, it's just mounting the virtual machine.

**Steve:** Starting up the VM, right.

**Leo:** Yeah. Asks for the password, and from then on in you'd never know you weren't running on a stock copy of Vista/VMware. I wonder what they do if they have to write the master boot record. I guess there's still a master boot record on that drive image.

**Steve:** Oh, absolutely. It looks just like a hard drive with a boot sector. You can do multi-bootloaders, everything you want to. I mean, it really is identical.

**Leo:** These guys are so clever. In fact, that's what he says: It's a testament to the great programmers at VMware and TrueCrypt that both of their applications work exactly the way you would hope they work, even under very unusual conditions. I don't really have an application for this beyond goofing around, but I imagine some security-minded person out there might, so I thought I'd share. An interesting bonus, you can inspect the virtual machine's drive file using a hex editor on the host system, which I've done. And from what my layman's eyes can see, compared to a similar nonencrypted Vista VM, it is really, truly encrypted, just as advertised. Random bits. Thanks for such a great podcast. You and Leo are a big part of why I am so successful at what I do. Well, thank you, Peter. P.S.: SpinRite saved my bacon two weeks ago. I won't bore you with the same old story - mother's lap- we can do this now, shorthand. Mother's laptop, never backed up, power failure, worst

possible nanosecond, BSOD on boot, SpinRite saves it. So thanks for that, too. I love that. We need to have, like, a little checkbox. Grandma's laptop, mother's laptop, wife's laptop, your laptop.

**Steve:** Never backed up, desperately needed the data that was on there, blah blah blah.

**Leo:** Yeah, it's always - isn't it always the case that the drive fails on the day you need that drive most.

**Steve:** Right, right.

**Leo:** Well, that's a great letter. Thank you, Peter, for your kind words. And that's a clever solution. And actually not surprising.

**Steve:** Yeah, I thought that was very cool. If someone wanted to play around with TrueCrypt but either didn't have a PC or for whatever reason didn't want to actually do it to their machine, they could see what it's all about by running it in a virtual context, and it works just fine there.

**Leo:** Ta-da.

**Steve:** Next week is TrueCrypt v5.0.

**Leo:** Hey, just out of curiosity, FREE CompuSec would do the same thing with VMware; right?

**Steve:** Yeah, absolutely.

**Leo:** It should work with both. All right, next week - I'm really excited about this - TrueCrypt 5 is out. And not only does it add a lot of features, including full disk encryption, it's Mac compatible and cross-platform compatible. So you can on a Mac read a TrueCrypt disk encrypted on a Windows machine. I understand that at least to be the case. But we'll find out. You'll talk about it.

**Steve:** Yup. And we're going to also talk in more detail about the traveler mode, which is so nice for it being able to encrypt, for example, a USB thumb drive. And the reason we're going to talk about that is that again will straddle into the episode two weeks from then, when we're going to have the founder of IronKey as our special guest on our IronKey podcast. So we'll do of course a Q&A in between. But then the week after that we'll have the IronKey guy. So we will have talked about using TrueCrypt for something similar to what IronKey does in hardware because their big claim to fame is true hardware encryption in the key itself and all kinds of neat, weird effects, like they deliberately pot this thing in solid epoxy so that if by mistake you do run over it in your car or your truck, it will - it's uncrushable because it's filled with solid epoxy. And of course that also makes it a little more tricky for the bad guys to get to it. So that'll be in several weeks. But we will talk about the traveler mode of TrueCrypt specifically next week because it's something that lots of people care about. And in fact my - the little 4GB thumb I keep on my keychain is now TrueCrypted because it really works nicely.

**Leo:** Excellent. Well, folks, if you want to know more, or you want to see Steve's super-duper new CSS menus, go to GRC.com. It makes it a lot easier to find all the things you're looking for, including in the Security Now! section show notes, transcriptions, even 16KB versions of every show, all 132 episodes, so that you can download them quickly on dialup. Of course if you've got broadband you'll want the full quality version, the 64K version. Do you offer the 64K version, as well?

**Steve:** Yup, also, yes.

**Leo:** Both of us. And then do you, you know, I never asked you this. You do link through Podtrac on those, I hope.

**Steve:** Yes, we redirect to you so that they're being counted there.

**Leo:** Because we don't want to miss a single one of you, the reason we do that redirect. For those of you security minded, I probably should mention this, too, because there's security-minded folks saying, wait a minute, what's this site I'm going through here? We redirect through Podtrac, which is our ad agency. And it's a very simple redirect. They just count how many people are downloading the show because that's how we sell it to advertisers. So what happens, it's a simple redirect, goes through Podtrac. They have a very sophisticated system. In fact, they have a data - I didn't know this, Steve, but they have a database of IP addresses so that they can compare to make sure that you are a legitimate IP address. They're not keeping track of you, but they want to make sure that you are a unique IP address coming from a real place.

**Steve:** Oh, to actually improve the quality.

**Leo:** They validate you, yeah.

**Steve:** And improve the quality of their counting.

**Leo:** Well, advertisers want that. In fact, I think it's an advantage that we and the thousands of other podcasters who use Podtrac have is that the numbers you get from Podtrac are dead accurate.

**Steve:** And very conservative.

**Leo:** Yeah. Well, and advertisers like that, too, of course. But they can never say, oh, you're inflating your numbers. We know each and every one of those people is downloading the show. And once, they're counted once and only once. Anyway, long story short, that's why it goes through there. GRC.com. You can get those. You can also - he's now got that menu for all his great utilities.

**Steve:** And site-wide search is there, too.

**Leo:** Site-wide search. Don't forget, of course, ShieldsUP, which is the great firewall tester. And he's got a lot of other cool stuff. And last, but certainly not least, that's the home of SpinRite. And you've heard us talk about that several times today. More than several times. It is the hard drive recovery and maintenance utility. It's just really a useful tool. And I use it, and I know a lot of people do, and I'm very happy. GRC.com. Steve, out of time. Tomorrow, or next week I should say, TrueCrypt.

**Steve:** TrueCrypt 5.0.

**Leo:** 5.0. And we'll see you then.

**Steve:** Talk to you then, Leo.