TrueCrypt v5.0

Description: In this second half of our exploration of whole-drive encryption, Leo and I discuss the detailed operation of the new version 5.0 release of TrueCrypt, which offers whole-drive encryption for Windows.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-133.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-133-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 133 for February 28, 2008: TrueCrypt 5. This show and the entire TWiT broadcast network is brought to you by donations from listeners like you. Thanks.

Time for Security Now! with Steve Gibson, the show wherein which we talk about securing yourself on the Internet, securing your computer, protecting your privacy. Sometimes we talk about protecting your hard drives because that's Steve Gibson's day job. He's the author of SpinRite, the man who coined the term "spyware." And his site, GRC.com, is really a haven for people who are looking for security online. Hi, Steve.

Steve Gibson: Hey, Leo. Great to be back with you. This is the much-anticipated episode about TrueCrypt v5.

Leo: Now, this just came out, what, in January; right? I mean, it's pretty...

Steve: Oh, actually in fact I think it was February 5th was the day that it came out.

Leo: Oh, yeah. And in fact I remember because we were talking about TrueCrypt, and I was bemoaning the lack of a Mac version.

Steve: Right.

Leo: And then I noticed on the web page it said we've got one coming. And, like, two days later I got about a hundred emails. People said it's here, it's here.

Steve: Yeah. I am very, very impressed with everything I've seen. I mean, we loved it when we first talked about it on this podcast back in 2006. And that was a v4 dot something or other, I believe. And, I mean, they had done so many things exactly right. And this whole issue of whole-drive encryption, first of all, it's captured the attention and imagination of our own audience. People who have laptops are thinking, wow, this makes sense. And it's dicier, though, that is, to encrypt your entire system drive because if something goes wrong you're hosed. I mean, it's game over.

And so you're going to love what I have done to test this. I've even created bad sectors and watched how it handles unreadable and uncorrectable damage on the drive. And bottom line is they've nailed this whole aspect. I will use this without hesitation anywhere it would be useful to encrypt the entire system drive. And of course it also provides, as we know from the past, many other features, one of which we're going to talk about because it segues perfectly into the podcast we're going to have in two weeks where we have the founder of IronKey on to talk about his hardware-encrypted USB thumb drive solution. And we'll be able to compare that with this aspect of TrueCrypt.

Leo: Let's see. Anything else you want to deal with from last episode before we get onto TrueCrypt?

Steve: Our listeners don't realize until we tell them that this has been - that we're recording this the day after we recorded last week's podcast, which was a day before it was released on Thursday the 21st.

Leo: Very confusing, I know.

Steve: Because you're, again, up in Vancouver, and I'll be joining you next month up there.

Leo: Oh, good.

Steve: But this month you're on your own. And so we're recording two in a row. Thus there's been no opportunity for a week to pass with any new security problems or anything. But as always, we will catch up and have two weeks' worth of what's been going on in the security world when we record our next podcast.

Leo: Well, let's just knock on wood. Maybe nothing bad will happen all week long.

Steve: It's been quiet so far. I did want to share - I always look for something that hasn't been said before in these SpinRite testimonials that I receive from people. And I got a kick out of this one. It's from a listener of ours. Well, I guess many of them are, of course. Jeff Locke in Portsmouth, Virginia said, "Steve, I am most" - well, the subject was "SpinRite Saved Me," of course. Said, "Steve, I am most happy to be writing to you to thank you for the wonderful product, SpinRite. I'm a regular listener to Security Now! and very much enjoy your products and the show with Leo. A week ago I found my computer completely frozen and could not get it to respond unless I completely cut the power. Upon reboot, Windows reported an error on my

data drive, which holds all my family photos, a wealth of software I've collected, and all the build files for several websites I manage," he says.

Leo: Oh, boy.

Steve: "So Windows said it fixed the drive problem after a CHKDSK. But the system frozen again an hour later, and the problem persisted. So I unplugged my data drive, and the computer ran fine for three days straight. After guessing that the data drive had a problem and was giving Windows a problem, I went straight to GRC. SpinRite spent four hours on the drive, found and recovered what appeared to be a bad sector, and I was back in action. Thanks so much for your work on this product. I would also like to tell you that the SpinRite buying experience was the easiest I've ever been through. The shopping cart you wrote was great. And of course I had no concern about its security. Love the show and SpinRite. Jeff L., Portsmouth, Virginia."

Leo: He raises a couple interesting questions there. One is that a data disk can affect Windows. You'd think it's completely separate.

Steve: Yeah, yeah. I have seen Windows get, well, the Windows drivers, the disk drivers are down in the kernel. So they're down where the real plumbing is going on. And there are places in Windows where there actually is no multitasking. That is, there isn't the ability for the kernel to be, whenever it wants to, be switching around between tasks. And so deep kernel problems can lock up the entire system.

Leo: That explains why sometimes Windows will just get stalled.

Steve: Yes, exactly. Exactly.

Leo: So you're saying if there's bad data on the data disk, it can lock up Windows because it stalled trying to read?

Steve: Exactly, it stalled trying to read or gets itself into, I mean, there are some funky modes that the driver can get into where what it's expecting, the way it's expecting the drive to perform and get back to it doesn't happen. And it just gets itself tangled up. I mean, probably the sort of thing, if you could induce the problem reliably, Microsoft could fix it. But they don't see it often enough, and so it's just sort of like one of those, ah, well, you know, sort of like the blue screen of death, which unfortunately too many of us see too much of the time.

Leo: Yeah. Very interesting. The second thing that came up for me was he used CHKDSK, and it wasn't enough. What happened? I mean, we do all have CHKDSK. Doesn't that do kind of the same thing as SpinRite? Boy, is that a loaded question. A little softball for you, Mr. Gibson. Here you go. I lob it.

Steve: I remember when, I guess it was before DOS 6, maybe it was DOS 5, I'm not sure now which version. But I had dinner with two Microsoft VPs back in the days when I was writing the TechTalk column for InfoWorld. And it was the version of DOS where they introduced ScanDisk for the first time. And this was Brad Silverberg, whom I really liked...

Leo: Oh, yeah, I remember him, yeah.

Steve: ...and Brad Chase, who I had less affection for, but that's another story. But Silverberg was just a super guy. And they were self-conscious about the fact that they were about to introduce a disk-scanning thing into DOS because I had had SpinRite for many years. And I remember over dinner them saying, now, Steve, you know, this isn't going to affect sales of SpinRite at all. You know, so ScanDisk doesn't do anything like what SpinRite does. And of course for the entire balance of my life I was trying to explain to customers why SpinRite was different than ScanDisk.

Leo: Because we assume, hey, it's a disk checker.

Steve: It scans a disk, so isn't that the same thing?

Leo: Same thing; right?

Steve: Uh, no.

Leo: You're doing a much lower level. You're working a lot harder. And CHKDSK really is just looking for some very simple errors in the file system. It's not even looking at sector reads; right?

Steve: Well, one way to put it might be that ScanDisk or CHKDSK are sort of - they want the drive to have a problem so that they have something to do. SpinRite doesn't - when SpinRite's done, it doesn't want the drive to have a problem. That is, SpinRite is about repairing things. ScanDisk and CHKDSK are sort of about finding file system problems. And so it's the reason, for example, you run them before doing something else. You want to make sure the file system is okay. And, you know, they basically say, oh, look, we found some lost clusters. Well, we moved them over into a file, here you go. But they're not about - they're much more about the higher level file system than the low level. And if they run across a low-level problem, they don't do anything to fix it. They just say, ow. We can't finish. We can't complete.

In fact, it's funny, when they added their own partition compression to DOS, which was - I'll never forget that version. That was DOS 6, which caused me to kill SpinRite 3 just as I was getting ready to release it because it didn't support that natively. And it's like, oh, no. I mean, so I couldn't be releasing a new version of SpinRite, which I don't do very often, and not have it support the drive compression built into - that was then going to be built into DOS. So that's why...

Leo: Oh, I remember that, yeah. This was DriveSpace.

Steve: DriveSpace, exactly.

Leo: Oh, what a nightmare that was.

Steve: And one of the things that DriveSpace would not do is compress your drive if there was

a single problem on it. And back then many people did have problems on their drives. And so we actually sold a lot of copies of SpinRite because it would fix the drives, which would then allow DriveSpace to perform its compression operation. And actually the same was true with the FAT32 converter. Remember when FAT32 support first came out, and then you were able to convert your non-FAT32, your 32-bit FAT, into a 32-bit one, which everyone wanted because it had lots of, you know, better features, upper and lowercase text support and other things. And again, if there was any problem on your drive, that would fail. And so we sold copies of SpinRite to people who, you know, wanted to be able to convert to FAT32 but they couldn't without having SpinRite fix the problem.

Leo: Now, watch this amazing segue. You know the same problem they have with DriveSpace, if you have a little error with DriveSpace, the whole thing's messed up. Seems like the same kind of problem you'd have with whole-drive encryption. In fact, I think they're very - in a way they're very similar. You're taking the drive and turning it into one big file in DriveSpace. Does TrueCrypt do the same thing with whole-drive encryption, make a big encrypted blob?

Steve: No, no.

Leo: Because that was a real flaw, I think, in DriveSpace.

Steve: Well, TrueCrypt runs in a number of different modes. The way it ran prior to v5, where they added this notion of preboot authentication and the ability to have your system partition encrypted, that's what's new in 5. So the various modes it can run is you can give it a file, so, for example, you could just have a file on your hard drive, on any hard drive or, for example, on a USB thumb drive, and TrueCrypt is able to mount that as a drive letter and, in the process, perform on-the-fly encryption/decryption of any data coming and going from that drive, which is actually just a file somewhere. So it can do that itself. So those are the three modes it's always been able to run in.

And then what was added, which really has brought it to a lot of people's attention, is they added the ability to encrypt the actual system drive, which you couldn't do before. And the reason that's tricky - and this is what we've been talking about really for the last two weeks, first in the context of the FREE CompuSec program, and then we talked about it a lot during last week's Q&A. And the idea is that if your system volume, your system partition, your C: drive, if it's completely encrypted, then Windows, the Windows files, the Windows code, the registry, I mean, everything you need in order to do anything is encrypted. So you need something on the outside which will decrypt the Windows operating system files itself until they get going. And then you need something on the inside, that is in Windows, which will seamlessly hand off that encryption task, so that when Windows takes over control from the external booting process, it also is able to transparently handle encryption and decryption of itself, essentially. So it requires these two components. And I've been extremely impressed with the way this was implemented.

When you install TrueCrypt - and it's still a very small, easily downloadable EXE, and as we've said now for the last couple weeks it is all open source, the source is available, so everything they've done is there, and the documentation documents what they've done. So you don't have to go in and read all the code. I mean, they lay out the format of the headers, which is the preamble before, for example, an encrypted partition. It's like, this is how this data is. And so they're not relying on obscurity at any level for the security of the system. And they've really gone security happy with this thing.

So to give you a sense for how committed to the safety of this process they are - and this goes way beyond what FREE CompuSec did, and it's one of the reasons that I've completely switched

over to TrueCrypt for this solution. When you want to compress your system drive, you run TrueCrypt in Windows in that drive. And you select Encrypt System Drive. And I'm paraphrasing here, but it's easy to see from the UI. That brings up a menu or a list of you want to encrypt - oh, is this drive a single boot or a multiboot? And in my case I'm just booting just the standard OS. I don't have anything else there. It does support multiple OSes. It supports of course Linux and Mac, although not, as I understand it, not yet in this full-drive encryption. But you are able to essentially still boot unencrypted operating systems if you have - if you're using Windows multiboot loader. They only support Windows multiboot loader. Or there is a way that you're able to use the Linux multiboot. I can't...

Leo: LILO or GRUB or...

Steve: GRUB. You're able to - and they give GRUB as an example. You can't have GRUB on the boot sector. But apparently it's possible to move GRUB to a partition.

Leo: Yeah. Both GRUB and LILO, in fact I think any bootloader in Linux can live on the boot partition, not on the master boot record.

Steve: Ah, and that's exactly it.

Leo: If you took over the master boot record, this whole thing would fall apart.

Steve: Well, and in fact - okay. So let me go back to this procedure because we'll see how safe they have made this. So you say, okay, yes, I want to encrypt my system partition. So the first thing you do is, as we've seen in prior versions of TrueCrypt, they start generating random stuff. And they show you a little window of hex randomness and tell you to move your mouse around, you know, and the more erratic and randomly you move it, the better your randomness is going to be. It's like, oh, okay. I mean, this is, like, so overkill. But it's typical of these guys. I mean, they don't tell you that they're also taking all kinds of random stuff from your system, from the clock, from various serial numbers, from globally unique IDs, I mean, they're starting with something where, I mean, you could unplug your mouse and this thing would still be massively random.

Leo: And this is designed because the pseudorandom number generators of computers, if you know where they begin generating numbers, you can predict what the next number will be. So this way they use these seeds, these completely chaotic seeds, to seed it; right?

Steve: Well, yeah, except that, for example, in the case of a static pseudorandom number, that wouldn't matter. What you're talking about was important, for example, for the keys being used dynamically for generating SSL connections.

Leo: Right, right.

Steve: Where you could make some guesses about what the next key would be of the next SSL connection because Windows doesn't have a very good pool of entropy that it works from.

Leo: So why do they go to all this trouble, then, I would ask.

Steve: Oh, it's just feel-good. I just wanted...

Leo: Extra, this is extra.

Steve: Yeah. I wanted to bring this up because I don't want our users to sit here messing with their mouse for an hour, just sitting there scrubbing it and scrambling it and bouncing it on their desk and spinning it around by its tail, thinking that that's going to give them a better key. I mean, literally, it's already really good. It's not possible. And that's one of the things I like about these guys is they've really, really concerned themselves about the security. It's not possible to have TrueCrypt give you a bad key. Before it even touches you it's already got a fantastically random key. So, but okay, fine, I like that they've done this. But I just want our users to know they don't have to sit here and worry about how long they need to scrub their mouse before...

Leo: I've seen other things do that. I thing PGP, some other programs do that when they're...

Steve: Yeah, it's...

Leo: It's a feel-good measure.

Steve: Okay. So now you generate all this pool of randomness, and from that it generates your master keys. Then, unlike again FREE CompuSec, that has none of this, it builds for you an ISO file which you have to burn to a CD. This is your recovery disk. And at first I thought, yeah, yeah, yeah, yeah, this is just a scrap machine, I've been using it for the last couple months, and recently with FREE CompuSec, I've got images, I can reimage it, I don't care about it. So I tried to say Next. And it said, wait a minute, you didn't do it. And it's like, whoa. What? It's like you have to make an ISO, you have to burn a CD or DVD and prove it to us. And it's like, oh, come on. So I have all these coasters lying around here now because for a while I was doing that. Then I found something that would allow me to fake it out. But these guys are really serious about protecting you from yourself.

Leo: And you're saying that you did this because it was a test machine, you didn't care if you hosed it. But you should make this disk if you're going to do this.

Steve: You don't have a choice. You have to...

Leo: They're right to require it.

Steve: Yes. You have to really work to fake it out. So...

Leo: And don't. Don't fake it out is what I'm saying.

Steve: So don't work to fake it out.

Leo: Yeah.

Steve: So you burn a little - and I have mini CDs, so they're small coasters that don't take - and it's a very small ISO, takes no time to do it. Then you have to put it back in the drive if your CD-burning software spit the disk out as mine does, put it back in the drive, then hit Next and let TrueCrypt sniff the disk. Oh, and the other thing it's doing is it is reverifying the image it made and that it's able to properly read. So again, it's verifying that you got a good burn of your CD. So it's useful for that, too. So now it's made you make an emergency recovery CD. And we'll talk about what that contains in a second.

Then it's like, okay, you've made your CD. Now, hold on a second. Now we've just put our bootloader on your hard drive. Now we're going to - we're not doing any encryption yet. We're going to make sure that it works. So we're going to shut down and reboot. See you in a minute. And so it pops up a dialogue, you say yes, fine, shut down now. So now you reboot, and you're taken to TrueCrypt's boot screen, where you have no choice but to enter your password. Now, again, in trying to really push the limits here I said Escape. Well, Escape bypasses its bootloader. And since I had not encrypted Windows, Windows came up. And TrueCrypt says no, good try. You cheated. Go back and try again.

Leo: It really nannies you on this.

Steve: Oh, it does.

Leo: This is funny.

Steve: We are not going to get faked out here. We are not going to encrypt your system unless you prove to us you can enter the password. And again, that's good. So it's like, okay, fine, reboot. So now I'm at TrueCrypt's screen again, and I type in my passphrase. Oh, and mine is, it's like...

Leo: You're going to tell us your passphrase?

Steve: No no no. I was just trying to count the characters. It's 18 characters long. I was using my fingers to count right there. Okay, that's not long enough for it. So when I give this gnarly 18, I mean, it looks like the keyboard broke, right, and no one could ever duplicate this - no. Passwords less than 20 characters long are not considered safe. If you make us go forward, we will. But we're going to grumble. It's like, yes, I want to use my 18-character impossible-to-repeat passphrase. And so but again it's like saying, you know, that may not be long enough. Okay, it's long enough for me. Besides, this whole thing is going to last about an hour before I scrub it off and do something else with it. So I give it my passphrase. Then it goes back into Windows and says, okay, so what we've proven now is, we've proven we've got a recovery CD. We've proven that the bootloader we put on the first track of the hard drive successfully worked. That is, you know, it was recorded, it worked, and you properly typed in the passphrase which, baby, you are really going to need from now on. So it's like...

Leo: Don't forget it.

Steve: ...now we will encrypt your hard drive. Okay, finally. So this thing does a beautiful job. It brings up a dialogue. It shows you what percentage with three decimal digits of accuracy. It estimates how much time is remaining or how much it's spent, I don't remember. But it shows you time passing in one way or the other. And you're in Windows. So you can use Windows. Now, it is sluggish. I mean, it's got the hard drive saturated. The drive light is on solid. And while Windows is still functioning, I wouldn't go and try to do any 3D rendering or play a game or do anything that requires much of the system. You could probably answer your email, but that's about it because, I mean, it is seriously working the system and just saturating the drive. It runs on a slower, older machine with a 40GB Maxtor ATA. It ran about two minutes per gig. So that 40GB drive took 80 minutes to compress.

Leo: Whoa, that's a long time.

Steve: On a newer machine with an SATA, a SATA drive, it was 1GB per minute. And Leo, here we're going oh, how many gigs do you have? This is billions of bytes.

Leo: Oh, yeah, I understand, yeah.

Steve: So people are very cavalier about the size of their drives. And of course they grumble about SpinRite. Oh, it took, you know, two days. It's like, yes, because we're moving an incredible amount of data. So it's literally, it is reading, in the case of TrueCrypt, it is reading every sector. It is in some block. It is encrypting them all, then it's writing them back. And it's making a note of where it is because remember, in order to do this on the fly while Windows is working, that encryption...

Leo: Oh, that's amazing. That's a good point. Windows, you're still using Windows.

Steve: Yes. And so imagine, here's your drive in front of you, this veil of encryption is being pushed from the front of the drive through the entire partition, encrypting files on the fly. So at some point a chunk of the beginning of the drive is encrypted, the rest of it is not because we're moving along, taking...

Leo: So you have to watch Windows, and when it asks for a sector, you have to unencrypt it and give it to us.

Steve: If it's a sector that you've already encrypted.

Leo: If you've already done it.

Steve: And not if it's one you haven't gotten to.

Leo: Now, does it do - is it file-aware when it's doing this whole-disk encryption? Or is it really just going sector by sector?

Steve: No, no, it is sector by sector. And again, you want that because...

Leo: So it would have to, yeah, because it would just get slack space and so forth.

Steve: Exactly. Deleted files and your...

Leo: Swap file and all that stuff. But if you didn't encrypt that it'd be a problem. But I guess you could encrypt those things. But if you're going to grow the file or whatever, you really want the whole thing encrypted. But I could see now why it's taking a long time because it's even doing empty space.

Steve: Well, yes. But conceptually, Leo, it's important that we understand conceptually, this is entirely different, I mean, this is entirely different from anything TrueCrypt has done before. In the past there was this notion of turning a file into a drive and, you know, having a container file that contains a drive. You know, this is every physical sector of the drive. And of course the reason people would do this is they want maximum security from any, I mean, any possibility that any of their data on their drive can get loose. So for laptop users this makes so much sense because unless you enter your passphrase, which is mixed with the master key, which essentially creates the master key to do this decryption, that entire drive looks like random noise. It looks like static. And one of the cool things is you never have to worry about wiping the drive to decommission it. This is a wipe-in-progress, essentially as it moves through this.

So eventually this process finishes, and then you get your computer back. It's no longer super busy any longer. And it works exactly as it did before. Now, if you then reboot, for example, and you come up to TrueCrypt's loader, you hit Escape, nothing happens. You've said bypass the decrypting bootloader phase, and nothing happens. I know, for example, that it's actually trying to boot Windows because at one point when I was messing around with how imaging, drive imaging affects this, I just restored a saved image of the whole system without changing that bootloader. So it was still there. And so it comes up and says, you know, what's your password? Well, okay. That's not going to work because I've just restored an unencrypted version of the Windows file system, the Windows drive, right on top of what was previously encrypted. So I thought, huh. Now what? Well, I hit Escape, and Windows booted because it was no longer encrypted because I had restored an unencrypted drive sort of in place, right over what I had before. So this thing, it holds your hand, it verifies what it's doing, it is incredibly safe.

So I decided, okay, I'm going to really stress this thing. So I went into the NTFS file system. Oh, and I restored - I think maybe I decrypted it first, or I had restored the image. I think maybe I did that because it was a lot faster. And I found early on the drive, about 18MB into the drive, I found a free cluster. And it happened to be sector number 37299. Sector 37299 was not in use by the file system. So using some tools that I have that are proprietary tools of mine that I use for developing SpinRite, I damaged that sector. I have the ability to create bad sectors.

Leo: Not physical damage, but soft damage.

Steve: No. Physical - well, I'm not bouncing the head. But I can deliberately create a bad sector that ECC cannot recover, that the drive will refuse to read and refuse to relocate. So nothing will fix it. It is just sitting there and absolutely uncorrectable and unreadable, unwriteable, I mean, it's just dead.

Leo: You'd better not let that tool get in the hands of...

Steve: No. As I said, this is...

Leo: That's a good tool. I like that.

Steve: This is stuff I have that I use for SpinRite development and testing. So I created an absolutely bad sector because I wanted to find out what would happen if I was encrypting this drive, and it hit a sector it could not read. I mean, early in the process. I didn't want to wait an hour for it to get to a sector toward the end. So I fired up TrueCrypt. I said, oh, I went through all the hoops again and, you know, burned the CD because I thought, well, maybe I'm going to really need this, depending upon how badly this hoses things, and started up the process. Almost immediately it stopped. And it said, you have a CRC - cyclic redundancy check - error on your drive. You have a problem with your hardware. This is not a TrueCrypt problem. And it's funny because it said, don't call us.

Leo: It's not our problem.

Steve: Don't send us anything. Don't complain in the forums. This is, you know, go call your computer vendor. There's something wrong with your drive, your cabling, or your motherboard. And we can't do anything. Okay, but I'm thinking, well, yeah, but you just did 18MB of something which, you know is - because I'm defragging and putting all the Windows files at the front of the drive so that they boot faster. So it's like, you know, Windows is in that first 18MB. So now what? So I'm thinking, well, but everything was still working. So it's like, okay, let's reboot. So I rebooted, and it asked me for my passphrase. I put in my passphrase. Windows came back up. It's like...

Leo: Because TrueCrypt hadn't done anything.

Steve: No, it had encrypted the first 18MB of the drive. Well, I wasn't sure at that point, okay, because I got there pretty quickly.

Leo: Right.

Steve: So then I went in - oh, and I got a dialogue box when I came back in. And it said there was an encryption process interrupted. Would you like to continue? And it's like, oh, well, thank you very much, I would. So I said yes. And immediately, bang, you have a problem, you know, same message again. So it knew where it failed, and it tried again, right on that sector. And so I was unable to proceed.

Leo: So if you have a bad sector like that, it will not do the drive encryption.

Steve: Well, yes, exactly. It stops, and it will not proceed. Now...

Leo: Is that how it should do? Shouldn't it just map that sector out or...

Steve: Well, no. I don't mean to tell you that you need to buy SpinRite, but SpinRite would fix that for you. But it would be nice, I guess, if it could say, do you want to proceed past this

problem. But these guys are being beyond careful.

Leo: Yeah, well, that makes sense. They don't want you to continue to do it if there'd be any problem down the road. They just say, look, we're not going there.

Steve: Exactly. I mean, I know exactly what the problem was because I manually created it on the drive. But somebody else - okay. So two different - there's two different courses of action now. You cannot proceed. So I thought, okay, let me choose the Permanently Decrypt Volume option in the menu. So I did that, and it went zip. I mean, it took, like, no time. And it said, okay. And it's like, oh, okay. So then I rebooted Windows, and it asked me for my passphrase. But I knew that it wasn't - the volume wasn't encrypted. So I hit Escape, bypassing the decryption boot. And Windows booted. So everything was back to normal. It had decrypted that first 18MB that I had assumed had been encrypted because, I mean, it did, it went zip and did something.

So then, okay, let's try this whole thing again. So this time I did the same thing, got up to that 18MB point, sector 37299, bang, stops. Okay. This time I rebooted, and I hit Escape - no. I hit something, I think it's maybe F2 for options. There are some options when you're booting. One of them was Decrypt This Partition. So it's like, oh, okay, so it knows it's encrypted, or at least partially. So it made me put in my passphrase again, of course, because you can't let anyone come along and just decrypt your partition, or what would be the whole point? Then I was so pleased, I saw it go 18, 17, 16, 15, 14, 13, it counted down rapidly from 18MB, knowing how - now, this is outside of Windows. So this is the bootloader portion was able all by itself to decrypt that only as much of Windows as had been encrypted before I hit this error. I'm just - I'm completely impressed with the way this thing works.

Leo: Wow. So it sounds like they did everything right.

Steve: Okay, well, I got a killer one for you. Now, remember that I was benchmarking FREE CompuSec? And I thought, okay, we've got to find out what kind of overhead we have here.

Leo: So just to recap, you get what, about, I think you said a 5 to 10 percent hit with FREE CompuSec?

Steve: It was 9 percent overhead. Okay. Well, I haven't computed the overhead here.

Leo: Why not?

Steve: Because it's faster with encryption.

Leo: Now, that's not right.

Steve: I am not kidding you.

Leo: You have a divide-by-zero error here.

Steve: I don't know. It's like, okay. So I wrote a little batch file using that EndTimer tool and the Windows defrag and Vopt and Windows defrag. I ran those three in sequence. With no encryption, Windows defrag took 8 minutes and 35.765 seconds. Vopt took 4 minutes and 31.046 seconds. And then a final Windows defrag took 1 minute, 54.765 seconds. Okay, so just look at the first number, 8 minutes and 35 seconds. I did it; I did it again. That is, I restored the image, ran the script again, and it was 9 minutes and 1 second. So, you know, about 8 minutes and 45 seconds on average. And the difference are just we're doing a lot of head-seeking. And so where the disk's rotation happens to be is going to affect timing a little bit.

Leo: Oh, yeah. Okay, that makes sense, yeah.

Steve: Okay. So it's like, okay. So I'm seeing, like, 8.5 to 9 minutes to do the first defrag of a very well-fragged image. And this is the image where I went from Service Pack 2 and applied those 95 patches and rebooted a whole bunch of times. So, I mean, it mangled up the drive, so it was nicely fragged. Okay, then I restored that image, the superfragged image. And I encrypted it. Then I ran the defragger in the encrypted system. The first time it took 6 minutes and 13.531 seconds, down from 8.5 or 9.

Leo: Down a lot.

Steve: Yes.

Leo: I mean, that's a significant difference.

Steve: I know. It makes Windows much faster.

Leo: This can't be true.

Steve: I'm not - okay. The second - and I thought, what, you know, I can't have a smaller number with encryption. So I did the whole thing again - restored the image, reencrypted it, 6 minutes and 21.765 seconds. So twice it was 8.35 and then 9.01 unencrypted. Then with encryption it was 6 minutes, 31 seconds - I'm sorry, 6 minutes and 13 seconds, 6 minutes and 21 seconds. Okay. So then I'm thinking, what is going on? So I went back to no encryption, final sanity check, back to the original, back up to 8 minutes and 21 seconds.

Leo: So do you have a theory for why this is doing that?

Steve: Well, they say on their web page that they've got 100 percent pipelining of some sort. Apparently once upon a time it was too slow, and boy did they fix it.

Leo: So it sounds like they've kind of written new drive read routines. They'd have to, I guess.

Steve: Well, they ought to send them to Microsoft because it runs...

Leo: No kidding. This is a typical open source [sound] take that, Microsoft. That's so funny.

Steve: It runs faster under TrueCrypt than it does without.

Leo: That's just amazing. And great. I love it.

Steve: So there's, like, so there's - overhead is not a problem. That won't be causing anyone any headaches.

Leo: Wow. Now, this is something that they used to say about DriveSpace, too, was when you compressed it you would get a faster read because you could read the data in faster, which would...

Steve: That's not the case here though because this is changing - it's not changing the size at all, exactly, it's just doing an in-place symmetric cipher. In fact, it uses AES - oh, that's another thing where overkill, you know, you're able to chain together multiple ciphers. So you could do AES followed by Blowfish or Twofish or, you know, it's like, come on, folks, no one needs any more.

Leo: There's severe paranoia going on here. But, you know, the people who use TrueCrypt are very paranoid; right?

Steve: And again, I don't want to promote that in this case because AES 256-bit key is absolutely fine. It's all anyone needs. So maybe before we had that, when your option was like triple DES, they also had some 64-bit ciphers, that is, a cipher with a 64-bit block size. And again, what I love about these guys is they're like, okay, that's no longer safe. We will still support that on volumes that have been encrypted by older versions of TrueCrypt, and the person shows a 64-bit cipher. But we will refuse - even though we have those ciphers inside of us, because we have to in order to be backward compatible - we're not going to build any volumes under any circumstances with a cipher that isn't at least 128 bits wide, has 128-bit block length. So it's...

Leo: Actually, that's great.

Steve: It is. It really is. So the other thing, to wrap up this issue of full drive encryption because then I want to cover the traveler mode briefly, the other thing I really like about this is for a person like me that is a tweaker and really wants a minimal environment, I wanted to see whether I needed TrueCrypt EXE and all of its, well, not that there's a lot of files. But, like, do I need it running at startup? Do I need it sitting there in my tray all the time? Say that all I want is whole-drive encryption. All I want - and this is like, you know, for an office computer, where the only thing you want is, when you boot it up, they have to type in their passphrase. That way if someone steals the drive in the middle of the night they get nothing. You know, that was what originally brought me in to looking at FREE CompuSec.

And the answer is you need nothing. There's a TrueCrypt.sys drive which you of course have to have. That's the key for being able to perform on-the-fly decryption. But you can completely remove the rest of TrueCrypt, take it out of startup, not have it running. You need none of that in order for your drive to be encrypted. You can't - oh, and of course thanks to the bootloader

having the ability to decrypt you, you could even take yourself back out without ever needing TrueCrypt again. So a minimal configuration would use TrueCrypt to perform the encryption, and then you can take it out, not have it start up, not have it always there in the tray because you only need that for, like, mounting and unmounting other volumes and doing other things with TrueCrypt than doing whole-drive encryption. I mean, it is just beautiful.

Leo: That's neat.

Steve: I really, really, really like it. Now, I should talk a little bit about the recovery CD. The only thing you can do when you boot the hard drive is you're able to bypass it completely, or you're able to enter your passphrase. If you enter your passphrase, you can go into Windows, that is, boot the encrypted partition, or you are able to say I want to remove encryption from this drive right now, sort of like a emergency decryption. You can also, as I did, do it in Windows, where you're able to kind of use Windows at the same time, although the system is really busy. But again, you're able to, from the bootloader, bring your system back to nonencrypted status. Okay. You can do more things with the recovery CD, which is one of the reasons they make you create this and don't give you any choice about it at all. And let me find my notes here because there was a whole bunch of things.

Leo: Have you found more things in your list?

Steve: Yes, and I'm glad I had a chance to browse through my notes here a little bit because there are a couple of really important things.

Leo: It's a lot of stuff.

Steve: Well, there's a couple of really important things we haven't covered, either. So remember one of our questioners in last week's Q&A told us about the collision he discovered between Dreamweaver, Macromedia's Dreamweaver's DRM or activation or whatever you want to call it, and the bootloader. Well, were it not for that CD, he would have lost his entire system because, when he activated Dreamweaver, it overwrote something in the first track of the drive, which I guess we said last week is a bad thing for some software, some random application software to ever do, you know, step outside of the partition. It's just a bad idea. But it did.

Fortunately he had his rescue CD. So if the bootloader becomes damaged in any way, the rescue CD is able to restore the original bootloader code to repair that first track. If the passphrase, if you were typing in your passphrase correctly, but the system said it's wrong, that would be caused by something having messed up the master key and some other critical management data for the decryption. So again, the CD is able to restore that if anything mangles it. Or if the bootloader area were to become infected by malware, such as, for example, the track zero rootkits we've been talking about. The point is, it would be running at boot time. And you certainly wouldn't want to have a rootkit. You'd be forced to boot from the hard drive in order to get decryption, yet in the process you'd be allowing the rootkit to run.

So the CD can itself provide the booting code, staying completely off of track zero. And the CD will hook interrupt 13, load itself, get Windows going. So you're able to still boot Windows with full use, not touching track zero at all. And finally, if Windows is, for example, itself damaged and refuses to start, then you could either use, as we said, the boot code in track zero, or also the CD has a copy of that, and it's able to independently permanently encrypt the drive. And finally, if when you first install TrueCrypt, whatever you originally had on track zero, it gets largely overwritten by all this TrueCrypt code. A copy of that is on the CD. So you're able to

restore the original track zero to its original condition. And TrueCrypt is essentially completely removed then from the low area of the drive.

Leo: Another reason to make that CD.

Steve: Oh, yeah. Well, you have no choice. And again, encrypting one's whole drive is a scary thing. But these guys have nailed it. I mean, they have made it so safe and so bulletproof against anything that might happen.

Now, one thing we talked about, I think in both of the last two episodes, I want to remind people of is that at this point in time the one thing that is not encrypted is the hibernation file. And we know that it's possible for a whole system encryption to do that because that's the one thing that FREE CompuSec does do at the moment, and they're proud of it. So it must be that it's kind of tricky. You can imagine how it could be because it must be that the hibernation file, since it's not being encrypted, it's either not able to be decrypted at boot time, or it's not able to be encrypted when it's being written.

Essentially the hibernation file is a copy of your RAM and various hardware registers and the dynamic state of the system. And so it's just copied, however much RAM you have is essentially copied to this hibernation file. And it's after Windows is in, like, most of Windows is shut down so that everything is static, yet Windows isn't quite gone. And so its last gasp is to write this file to the drive, and the reverse process. But top of their list of, that is, the TrueCrypt guys understand this is a problem. It's the first thing they list as the next thing that they're going to be working on.

So this would not be a problem in any system that isn't typically using hibernation. For example, the desktop application that I have, like the corporate desktop, where you just want to make sure that, if someone spirits the system away in the night, you're not losing any corporate secrets, those systems typically don't use hibernation. They're just shut down. And what TrueCrypt does, again, in its super, make sure there's no way you can hurt yourself mode, is it completely disables hibernation if you do the full system encryption. Hibernation is just no longer available to you as an option. And so they protect you that way.

Also it's worth noting that there is nowhere, not even on your emergency rescue CD, is there any password recovery. And, I mean, that's really what you want because password recovery is dangerous. If the CD, for example, had the ability to forgive you for forgetting your passphrase, then that would be a huge security vulnerability. But it won't remember it for you. So whatever it is you choose, it is entirely incumbent upon you never to forget it.

Leo: Do they put anywhere on the website, don't call us if you forget your password? We don't know it, and we never...

Steve: And now the last two things are interesting, sort of edge cases of whole-system encryption. And that is the wear leveling, which exists now in the higher end solid state media, and hard drive sector sparing. We've talked about before many times about how if a hard drive sector starts becoming marginal, so that the hard drive is seeing that it has to apply more on-the-fly error correction than it's comfortable with, then it will read the sector and correct it one last time, then swap it out of use, essentially stop using that physical sector and use a good sector in its place. The problem is, whatever data was in that sector at the time is still there. So although you can't access it through the normal API, there are manufacturer-level means for doing so. That is, that sector, you really cannot get to it from the outside. But it's physically there on the drive. And remember, it's only 512 bytes, but over time they tend to accumulate.

So the point is that if you then TrueCrypt your drive, you are TrueCrypting all the sectors currently in use, none which were once in use. Those are gone. They're not available. But they have whatever data they had in them at the time. And wear leveling on a solid state drive is similar. As we know, the technology, the actual chemistry, tends to wear out in a given spot. And so high-performance, good solid state drives, even if you're trying to rewrite the same spot, for example, well, you would never want to run Windows swap file on one of these. I remember telling our listeners that Mark Thompson, my buddy at AnalogX did, and burned out a drive in a couple hours by doing so.

But the point is, in wear leveling, even though you think you're writing to the same spot, you can actually be writing to a physically different location, which means that, again, whatever was in the previous location has not been overwritten. And these solid state drives also have extra sectors just for the possibility that one becomes damaged. So similarly, you could encrypt your thumb drive, and TrueCrypt, in rewriting, it would read what it thinks is a physical sector and encrypt it and write it back. But it might be writing it back to a different location, meaning that the original contents of that sector didn't get overwritten by the encrypted data as normally is the case on a hard drive.

So both of these say, I mean, these are, again, they're edge cases. They're probably really not a huge concern. But to their credit, again, the TrueCrypt site addresses this - actually it addresses wear leveling. I don't think I saw it talk about sector sparing, but I understand that that's a problem. So if someone was really concerned, the solution is get a new device, get a brand new solid-state drive, a brand new thumb drive or a brand new hard drive, and the first thing you do is encrypt it. That is, you put it under TrueCrypt management.

Leo: Interesting.

Steve: And if you do that, it will never be the case that unencrypted data is ever written to that, ever.

Leo: And you might have some data integrity protection because of this wear leveling.

Steve: Sure.

Leo: I think it would it kind of help you with that.

Steve: Well, wear leveling is certainly a good thing. And it does extend the life of our little thumb drives.

Leo: Especially for flash drives, yeah.

Steve: Yeah. And then that's exactly what we're talking about.

Leo: So encrypt to improve your flash drive life, among other things. That's interesting.

Steve: Well, the wear leveling is something that happens continuously in the background, where it's always trying to sort of even out the amount of exposure...

Leo: Oh, the drive does that automatically.

Steve: Exactly.

Leo: Oh, I'm sorry. I thought TrueCrypt was doing that. It's just aware of it. I get it, I get it.

Steve: Yeah, it's just underneath. Well, actually it's not aware of it. And it's not aware of it, and it can't do anything about it because it's happening at a level underneath - it's literally at the hardware level this remapping is going on, typically in large blocks, just to kind of keep things evenly written to across the entire surface of the drive. But it does mean that you don't really know when you've encrypted something that you wrote back over the old stuff. Not that you can read. I mean, when you read what you wrote, you get back what you wrote. But technically, electronically, there's still that data there. It's not accessible from the outside. But it could be accessible by, you know, NSA sorts of people, I mean, people who really, really know this stuff and want to see what was there. So if you were really concerned, you just wanted to start fresh, TrueCrypt something before you ever start using it, and you never have to worry that anything of yours was ever there before.

Leo: It's a beautiful thing.

Steve: And finally, this traveler mode is just spectacular. It allows you essentially to carry TrueCrypt EXE and the TrueCrypt SYS. And there is support for 64-bit version, or 64-bit OS. It allows you to carry them on the media that is encrypted. So, for example, you could create a traveler disk from a USB thumb drive. And there's a nice little wizard that walks you through the process of doing so. And you end up with an autorun INF file such that, when you plug this in to any computer, it runs TrueCrypt EXE that's on the unencrypted portion of this thumb drive. And that has to be unencrypted so it's able to run it before it starts doing the encryption, the on-the-fly encryption. Then it prompts you for the password that contains the data on the rest of the drive. You enter that, and then it creates - you will already have a drive letter for sort of the outside container. Then it creates another drive letter for what's encrypted and protected on the inside. So you get a second drive letter, and that's your inner sanctum contents.

Now, it's worth noting that you have to have admin privileges because it needs to load the TrueCrypt.sys device drive, and non-admins are unable to load device drivers. So what I've done is, rather than - I have, like, a 4GB thumb drive. But I don't really have that much super secret stuff. I have a lot of random freeware and utilities that I don't care about having them encrypted. But I also, for example, have my master WiFi keys and other things that I really do care about. So because you're creating a file that lives on this thumb drive, you can make it any size you want. And the advantage of that, for example, is that you do not need admin privileges to read all the unencrypted area, only to get to your super secret inner sanctum, which is actually what I call the file, innersanctum.tc, on the thumb.

So the point is, I would say, if that makes sense to people, you know, if you had, like, a 4GB thumb drive, maybe make it half a gig. 512MB is the inner sanctum, and the other three and a half is just there, open and in the free, so that you can still get to most of the data without ever needing admin privileges. And if you ever need to get to your really protected TrueCrypted stuff, then for that you would need admin privileges because you're not sure what control you're going to have over the computer that you might want to be plugging this into.

Leo: Right. Very cool. And it's free from TrueCrypt.org.

Steve: It's all free. And, Leo, it's open source.

Leo: Thank you. Another victory.

Steve: I know what that means to you.

Leo: For the open source community. No, it's really - but it shows you that, you know, sometimes people say, oh, how could you, how could open source write good software? How could it compete with commercial software? I don't think there's any question it can.

Steve: This is better than anything I've seen commercially, Leo. I mean, it is a fantastic - I can recommend this without hesitation. The only caveat I would have is it's very new. It's February 5th. It's a few weeks ago. It already went from 5.0 to 5.0a. And in doing so they made their bootloader - they reduced the size of their bootloader so that it was less greedy about how much space it needed on track zero. And that allowed it to accommodate other things that might also want to share track zero with it. So I would say maybe give it a few months, depending on how cautious people are feeling. I mean, it's hard to imagine that with all the testing it's had, I mean, if you look at the download counts on their site, this thing is being heavily downloaded.

Leo: I'm not surprised, yeah.

Steve: Lots of people have jumped on it. I have never had a single bad experience with this. And I love the idea that I can create a minimal system where TrueCrypt is almost not even present, where you only see it when you have to type in your passphrase, and it's not running in your tray, it's not running in the system, it's just a device driver that is allowing, advantaging the encryption of the whole thing. And it's faster than before you installed it.

Leo: And that's the amazing thing. You know what is also good for your system? SpinRite, all the free utilities, ShieldsUP, all the stuff Steve does at GRC.com, including 16KB versions of this show, transcripts, show notes, it's all there. And now, thanks to the new menuing system, easy to find. GRC.com. And we come back every Thursday to bring you more security news. Next week your questions and Steve's answers, so make sure you go to the feedback form there at GRC.com and submit your questions for our next episode.

Steve: It's GRC.com/feedback. And I will be checking in before we do the Q&A that listeners will hear next week. It's actually going to be two weeks for us in real time. So people will have a week to listen to this, play with maybe TrueCrypt, and let me know what they think. And we'll be sharing it in our next episode.

Leo: Good. Thank you, Steve.

Steve: My pleasure, Leo. Great to talk to you.

Leo: See you next time on Security Now!.