SECURITY NOW!

Transcript of Episode #131

FREE CompuSec

Description: In this first of their two-part exploration of the world of whole-drive encryption, Steve and Leo begin by discussing the various options and alternatives, then focus upon one excellent, completely free, and comprehensive security solution known as "FREE CompuSec."

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-131.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-131-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 131 for February 14, 2008: Free CompuSec. 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!. I know you've been waiting all week with bated breath and unprotected systems to hear what Steve Gibson has to say about security. Hi, Steve.

Steve Gibson: Hey, Leo. Great to be back with you.

Leo: Good to talk to you. And today we have a new program we're going to talk about in just a little bit that will protect us all. But before we get into that, do you have any updates that...

Steve: Well, it was a busy week in security news. Of course this is the podcast after the second Tuesday of the month, that is, of February...

Leo: The first Thursday after the second Tuesday.

Steve: The first Thursday after the second Tuesday. Now, of course the first Tuesday of the month was the Presidential Primary Super Tuesday. I'm inclined to call this last Tuesday the PC Industry, or I should say the Microsoft Super Tuesday. They released 12 security updates. Any of them are important. I'm not going to go through them in painful detail because, you know, it gets sort of redundant at some point. But Windows and Office and VBScript and Jscript and, I mean, it was a big - oh, and a big new IE update, as well, to catch IE up. There were just a whole bunch of problems, many of them rated critical, meaning that it's a remote code execution exploit sort of thing. So standard practice is just - I wanted just to remind our listeners that it's important, if they don't already have their machines updated, to recognize that we just crossed the second Tuesday of the month, and there was a whole bunch of stuff.

Leo: Yeah, it's funny, it sometimes takes a couple of days. I came in today, this morning, and my system said I rebooted last night after installing patches. Because I have it set to, you know, automatically install, download and install any patches that come out, critical patches. Which I think is probably the sensible thing to do. Maybe not necessarily automatically install, but certainly to automatically download and notify you.

Steve: Yeah, that's what I do, too. Of course Apple had - well, I don't mean to say "of course Apple had." But Apple also had a substantial update. In terms of hugeness, apparently it's about 180MB, or twice that if you've got an Intel-based platform. I record our Skype sessions, I use a little Mac Mini that's PowerPC based. And it had - I watched it - 180MB update to the OS. And apparently...

Leo: Oh, really. Was it that big?

Steve: Yeah. And apparently, oh, and there were a couple other little updates. But this was a biggie. And apparently Intel-based machines can be as large as 360MB. So it takes a while.

Leo: I don't think mine was that big. It must be depending on what you've got installed and so forth.

Steve: That's probably the case.

Leo: Although, you know, they break it up. They say there's this, and there's that. And mine did reboot two times, then wanted to install more and rebooted more. So it was a - whatever went on, a lot of - some of it was cosmetic. Some of it was not security. We talked about this on MacBreak Weekly. They fixed some cosmetic things in Leopard that people didn't like at all.

Steve: Interesting. Well, also we talked last week or the week before, we mentioned an Adobe Acrobat problem that Acrobat had updated recently but hadn't really talked publicly about what was being fixed. Well, that didn't stop the bad guys from figuring it out. And the most recent Acrobat flaw is now being actively exploited to install a trojan called the ZoneBac Trojan, which disables AV, alters search results and banner ads, and is just another one of these bad things you don't want to get on your machine. And it works by taking advantage of a flaw essentially in Acrobat that allows a bad PDF to install this trojan on your machine. So if you - and my Acrobats recognized that there was a new version, and they've updated themselves. So if users haven't launched Acrobat for a while, it's probably worth doing and having it check for updates because there's definitely something you want to get fixed before you go further. Firefox had also an important update that for me, again, was automatic. I had Firefox open for a while, I think it was maybe two days ago. And it notified me that it needed to restart itself, having downloaded and fixed itself. So it's like, okay, uh, go ahead.

Leo: Now, of course beta 3 came out of Firefox 3. But you're running 2.

Steve: I'm running 2. I'm not, yeah, I'm not running in betaland yet.

Leo: 3 is actually, I hate to say it, but 3's more stable than 2 is. But anyway.

Steve: Well, that's probably where everyone's attention has been. They're all focused on 3. It's like, that old version 2. And there was a - over on the Windows platform, Skype has been having a series of problems involving various scripting exploits. It was caused by the fact that Skype was invoking the Internet Explorer display control for some of its purposes. So it's like having IE, unfortunately, hooked into an instant messaging system, which is really asking for trouble. And so they were incrementally fixing them, one after the other, as they were occurring. And then they finally figured out, that is, the Skype guys did, that this was dumb, that they ought to just do an architectural fix. And the problem was that they were invoking this IE control under the local zone which had too liberal security. And so now with this latest final update to Skype, they've architecturally improved it so that it's opening the IE control in the Internet zone that is inherently, by default, much more tightly bolted down. So that hopefully will fix, well, basically it would have fixed all the problems they've been having. And this way it's looking like it'll fix things that are coming up in the future. So...

Leo: It's a little worrisome, though, that a program can decide what zone to install itself into.

Steve: Yes.

Leo: Because that means it could install itself, as it did, into a lower security zone. If you're a bad guy installing malware on a system, you would do that.

Steve: Well, yeah.

Leo: It shouldn't be able to choose.

Steve: It makes sense for software to be able to specify a zone more secure than the default. But the default would be the local zone. I mean, you'd expect, like, an application running on your system to be safe. But then you're depending upon the thing you're installing to be safe. And to suggest that Internet Explorer is safe, well, you know, few people would do that. Also we talked a couple weeks ago about Yahoo's music jukebox ActiveX control that had some problems. There's now malware actively exploiting that, installing backdoors on PCs. No fix is available from Yahoo!. So the only thing you can do, in fact, is to enable the so-called "kill bit" to prevent the ActiveX control from functioning, but of course that shuts down the music jukebox, which is not safe to use. And in fact there have been so many ActiveX problems that finally the U.S. CERT agency, the U.S. Computer Emergency Readiness Team has just thrown up their hands and recommended that people disable all their ActiveX controls.

Leo: Really.

Steve: Because, yes, because it turns out that there are new ActiveX controls which are being supported by Facebook and MySpace, the whole little new widget thing. And so it's a typical case of non-security-aware people being in a big hurry to come out with new Facebook and MySpace widgets, which are operating on web pages. And we've talked about ActiveX controls a lot in the past. It was a really, really bad idea for Microsoft to allow IE to basically - it's like a DLL, it's actual code. It's not even sandboxable in the way that JavaScript or VBScript are. It's a DLL essentially that you are downloading and running in someone's machine. And it's like, oh, isn't this nice, look at this new little widget that I have on my MySpace page. But if it's not carefully written it's going to be, I mean, it's open to exploitation. And so these ActiveX controls are causing all kinds of problems. So one thing any IE user can do to disable ActiveX controls is set their browser's security level to high, that is, the highest available. And the good news is, that tells ActiveX controls, no thank you. Or...

Leo: And if you don't use Internet Explorer, you don't have to worry about it at all.

Steve: I was just going to say, yes, exactly. Or if you're using Firefox, and you were not using the ActiveX control extension that allows Firefox to invoke ActiveX controls, by default Firefox doesn't load and run ActiveX controls. You'd be safe with Firefox.

Leo: Yeah. One way Yahoo! dealt with this is of course to go out of the music business entirely. I don't know if this is related. They killed their music business. So the jukebox won't be around much longer anyway.

Steve: Well, that's going to be good news for a lot of people.

Leo: But, you know, it's important to remember that a lot of these programs that use the Internet for content are really just ActiveX controls or versions of IE or using IE's engine. And so they're just as vulnerable as IE is.

Steve: Yes, exactly. Exactly.

Leo: That's the easiest way to program it. And on the Mac side, I have to say, the same thing happens. WebKit, which is basically Safari, is used for a lot of Internet access in a lot of programs. So when there's a WebKit vulnerability, just as when there's an IE vulnerability, it propagates to all these other programs.

Well, before we get on, I'm sure you have a SpinRite letter, and I'd love to...

Steve: Oh, I got a great one, actually.

Leo: Let's do it now. Then I'll talk about Astaro.

Steve: Okay. Now, this individual who wrote to me has asked for anonymity because he doesn't want to get fired.

Leo: Uh-oh. That's always a good way to start.

Steve: The subject was, "Wow, SpinRite Really Works." And he says, "Hey, Steve. First, let me start off by saying that I listen to Security Now! every week and haven't missed a single episode. Okay, now onto my story. I am a Geek Squad agent at Best Buy, and as such I'm constantly seeing failed hard drives coming in. It's sad because I know that many of them would be back to normal with just a few hours of SpinRite working its magic. One customer named...." Okay, now, I've changed the name here. We'll call him John. Although I had his real name in the original note. "One customer named John came in with a look of desperation, as do most customers who come into the Geek Squad Precinct."

He says, "John stated that his five-year-old Dell laptop kept on bluescreening with the error message 'Unmountable boot disk.' I immediately thought of SpinRite. Best Buy, sadly, does not have a SpinRite enterprise license, or any license at all, for that matter. So the 'agents are not allowed to use it.'" He says, "I have emailed corporate about this, and they said they will see if the budget allows them to purchase one. I explained the profit Best Buy will generate with all the backups customers come in for, but we turn away because their file system and drive are too corrupted." He says, "I had two options. I could send out his hard drive to Best Buy's service center for a fee of $1,712.32."

Leo: What?

Steve: $1,712.32. And he says in parens, "tax included." He said, "Or I could tell him about SpinRite, surely risking my job, as this would be cutting revenue from Best Buy's bottom line. But I couldn't let him spend the $1,700+ knowing SpinRite would probably would work for literally 25 times less. So I did it. I told him about SpinRite, where to get it, and how to use it. Needless to say, you took a panicking radio personality and turned him into one happy man."

Leo: Not me.

Steve: Not you. He says, "Here is a quote from the email he sent me. Quote, 'My computer had finished with SpinRite when I got home from work today. Everything you said would happen, did. My computer is now operational again.'" He says - so this author says, "Thanks, Steve and the GRC team, for making an amazing product and making my job a lot easier. I will continue recommending SpinRite for the rest of my life." Then he says, "P.S.: If you share this testimonial, please either change my name or blank it out. I do not want to get fired."

Leo: Yeah, because he was supposed to send it in for that $1,700 repair. You're costing us money, kid.

Steve: Yeah, well, and it's funny, too, because an enterprise license is 10 copies of SpinRite. So that's $890. So it's less than half the cost of one of those $1,712.32 Geek Squad fixes. So it's like, well, you know, they could certainly have an enterprise license with no problem.

Leo: I might even know who that personality was. But I'll ask you off the air. I have my suspicions about just who that might be. But it wasn't me. Say that right now because I have a copy of SpinRite. That's the first thing I try. And it did work for me just, you remember, about a year ago it was that we lost a hard drive. I'm still using it, by the way, so it did fix it.

Let me also mention a couple of things before we go much farther. One is, oh, I forgot what it was. It was really - it was a security thing, and I thought you would want to know this, and I forgot it. Where is - oh, Service Pack 1, what am I thinking, of Vista. Microsoft is moving that schedule up, and they've just announced that they're going to have it for MSDN users by the end of this week, on the 16th. So we're getting very close to Service Pack 1 for Vista. Which will be, I'm sure, an improvement. It certainly will roll up all those patches into one big file.

Steve: So Vista has a whole bunch, as well? I don't use Vista, so...

Leo: Well, their service - yeah, I know, you're back in Windows 2000. So for those of you in the 21st century, let me just...

Steve: No, but even XP, I mean, I'm...

Leo: XP has Service Pack 3, yeah.

Steve: Yes, and I'm excited about that one.

Leo: Paul and I talked about it quite a bit on Windows Weekly. But so I'm going off of what he tells me. But Service Pack 3 on XP is really just a rollup of all the patches to date. But you need it because, of course, after you install Service Pack 2, you spend 10 hours rebooting and reinstalling the rest of the patches. So...

Steve: So how is Service Pack 1 different on Vista?

Leo: It changes some of the way Vista behaves. And there's some question, some debate about whether it's faster or not. A lot of people have been trying it, but it's not official code. The official code will go out on MSDN this weekend. They say sometime in March it will start getting pushed out to end-users. But I don't know, you know, I only know what - Paul wrote a little bit of an FAQ, if you want to read more about it at the SuperSite for Windows, WinSuperSite.com. And of course we'll talk about it tomorrow on Windows Weekly.

Steve: And I did hear that it was RTM, so...

Leo: It is RTM. And as I said, it's going to go out to tech and MSDN folks today or tomorrow. By the end of this week, they said.

So we've talked about TrueCrypt at great length in the past. Free, open source.

Steve: And actually a prior version. The way I got into today's topic, today's topic is - I referred to it a week or two ago. It's a very interesting and very impressive system that I found which is called FREE CompuSec. The problem was I was doing some, have been doing some sort of just free consulting for a friend. She's in the process of setting up a little office and some computers and a network. And she's in the human resources field and is very security conscious, which I'm glad for. I didn't have to do any preaching to her about the problems of security. In fact, she was the motivation for my checking out and coming up to speed on

Windows SteadyState because one of the problems she has had in previous entrepreneurial ventures is employees coming in and just installing their own crap on company computers, which is really a problem. So SteadyState was the solution for preventing that kind of employee abuse of corporate resources.

But she has this - the other real concern is, since she's an HR company, and she reads the Wall Street Journal, and she hears all the horror stories about people getting laptops stolen or computers stolen, where hard drives have really confidential information on them. So she said, you know, Steve, what do I do about protecting our workstations from someone breaking in and stealing them and discovering all of this potentially very confidential data on them? Well, so that means, okay, it means one way or another we need to prevent the hard drive from being readable without authorization.

Now, we've talked about drive passwords in the past. And, for example, my laptops have a fingerprint reader on them; and I use TPM, the Trusted Platform Module built into the motherboard that contains the code for essentially unlocking my hard drive. I don't have the whole drive encrypted, but I'm using the drive password facility that's been available on little hard drives, especially laptop drives, for years now. The idea being that only if I swipe my finger when I power up or restart the machine will the BIOS give the hard drive the password that it's been registered with to essentially enable the hard drive. Without that, if someone got my machine and took the drive out of it, the only thing they can possibly do is low-level reformat the drive in order to get access to it. That is, it would wipe it to zeroes in order to cause it to unlock.

Now, that's not secure against governmental agency-scale attack, that is, if I had a hard drive on my laptop and it was absolutely imperative that the data be recovered. Because it's not actually encrypted on the magnetic surface, it would certainly be possible to go back to Hitachi or Seagate or wherever, and with enough inducement I'm sure they're able to unlock the drive. So government subpoena sort of scale access is still possible. But I'm not worried about that. I'm worried about losing control of my drive and having it fall into bad guys' hands because certainly a drive password is sufficient to protect the information at that level. And I don't really have anything super confidential on my system that, I mean, again, I don't want to lose control of it, but the drive password is just fine.

Now, the next level up is native hard drive encryption, which is, as we've also said in the past, beginning to be available. It was an option that I just decided not to pursue when I purchased my most recent ThinkPads, is for an additional X amount of dollars it seemed like more than I needed to spend for that. The drive itself uses the AES, the Rijndael cipher. And so the BIOS, in a similar fashion to unlocking it, but the BIOS is actually giving it a passphrase, which the drive does not store on itself anywhere, but that passphrase is used to perform on-the-fly encryption and decryption.

So inside the drive, everything that I write to the drive runs through AES encryption on the way down to the magnetic surface, and runs back through it on the way out. So there's no overhead in time at all. That is, you get 100 percent performance that way. And what's on the drive is always encrypted. That is, the swap file, the hibernation file, all the contents, I mean, your deleted files, I mean everything. And so without that, without giving the drive the passphrase that it's looking for, there's just - there's no way anybody - and again, not even under governmental-level subpoena strength, I mean, it is pseudorandom data on the drive which can only be decrypted by giving it the proper passphrase.

Now, as we know, brute-force attack is possible so you want a really good passphrase, something that couldn't be brute-forced. But that's the only vulnerability that would be available would be asking the drive, here, take this as a passphrase, now give me the first sector, does this look like the boot sector or not. And until you gave it the right passphrase, you wouldn't. On the other hand, it would be reading this thing from the drive constantly, so you couldn't brute-force fast. It would take a long time to brute-force a hard drive's magnetic media like that. So either password-protecting the drive or native hard drive encryption are those first two options.

Now, in the case of the workstations that my friend had, she had no TPM on the - it was like the bottom-of-the-line Dell workstation. Did not have any security built in. There was not the ability in the BIOS to set a hard drive password. So I couldn't even lock her drive if the drive had that option. And certainly there was no native hard drive encryption. So what I needed...

Leo: You know what's funny, I just - I don't mean to interrupt, but I wanted to ask you about this. There is hard drive locking built into the IDE spec; right?

Steve: Yes, it's been built into the ATAPI, the so-called ATAPI, which is...

Leo: Try to get that acronym. It's okay.

Steve: I'm blanking it. ATAPI.

Leo: It doesn't matter. The reason that just came up is somebody mentioned that - called the TV show and said my hard drive's locked, you know, it's an old machine. And I did some research and found out about this ATAPI locking. But that's not encryption, is it?

Steve: It's ATA, which is - the ATA spec is the original spec, and PI is Packet Interface. ATA Packet Interface. I'm sorry, and I was so busy trying to remember the acronym I didn't hear what you said.

Leo: So the question is, is this encryption, or is it just locking? In other words, many machines will have it because it's such an old - it's part of the old ATAPI spec. But does this...

Steve: Oh, yes. Almost every drive anyone has been able to purchase for the last...

Leo: You can do it, right, yeah.

Steve: ...10 years can be locked, but not encrypted. Encrypted is only in the last six months or so.

Leo: Does locking keep people off of it, though? I mean, you can't get into it if it's locked; right?

Steve: Absolutely. You cannot get into it if it's locked. And the system is very mature. And so if people have BIOSes where the BIOS gives you the ability to create a hard drive password - and now, see, this is something that's been available on laptops for a much longer period of time than it's been available on desktops.

Leo: That's why I bring it up.

Steve: Right. And so that's very good encryption. It's all I - oh, I'm sorry. It's very good protection.

Leo: Protection, right.

Steve: It's not encryption. It's very good protection because the hard drive will refuse to be a hard drive until the BIOS gives it the unlock password. But because the data is not actually encrypted, under government subpoena I'm sure that Seagate or Hitachi or whomever could say, okay, we've removed the lock from the drive, grand jury. Now you can - you're able to see what's there. So here I was faced with the problem of...

Leo: So she wouldn't use something like that. That would be insufficient.

Steve: Well, she can't because it's not available in her BIOS.

Leo: Ah. It has to be supported in the BIOS as well as on the drive. I get it. You have to have an interface to it, for obvious reasons, yeah.

Steve: Well, yeah. You have to have code which will use the ATAPI spec at power-up time to give the hard drive the unlocking password that it's looking for before you can even read sector one on the drive. I mean, you can't get to the partition sector without that. So I was faced with, okay, a desktop system like most of us have that doesn't offer you a hard drive password option. And it was absolutely critical that, if the machine got stolen, the data would be protected. So I dug around, and this was a couple months ago, and came up with this system, it's out of Singapore, called FREE CompuSec. And if any of our listeners just put "free compusec" into Google, it's the first link that comes up. And it's...

Leo: Now, I'm confused because it's from CE-Infosys, yes?

Steve: Correct.

Leo: That's a German company.

Steve: Yes. In fact, they have three different offices around the globe. So I don't know what the lineage of this is. But I know that some of the stuff ends up coming out of Singapore; and you're right, CE-Infosys is German.

Leo: Thank you.

Steve: So I have to say I am very impressed with the system. I've looked at it very carefully. I had to really understand it before I was going to trust it and stick it on these workstations. Let me explain how this works. It's called preboot authentication, and it's significant, not only for this, but also for the most recent version of TrueCrypt. TrueCrypt 5.0 just came out of beta like a week and a half ago. In fact, it was on February 5th it came out of beta. They tweaked it a week later, just two days ago, in fact, on February 12th of 2008 they tweaked it and fixed a problem which was interesting to me because it's a problem that FREE CompuSec doesn't have because of the way they implemented their system.

But here's the idea. We want to encrypt the entire drive. And that's the only way to keep - if the BIOS won't support unlocking the drive, then we need to do something as the system starts to boot. So the drive is not locked because the BIOS won't do that for us. So it turns out that - and I mentioned this in passing recently. The so-called boot sector, or the partition sector of a hard drive, is actually executable code. The BIOS loads it into low memory and jumps to the front of it. It actually runs the partition sector, which has just enough code - a sector on a hard drive is 512 bytes. It has just enough code to interpret the table at the end of that sector, which is the so-called partition table. It's got four entries in it. And it'll read that table, which tells that code where to find the beginning of the bootable partition, which it then loads into memory and runs. So it's because the partition table, that is, the partition sector is actually executable that a number of tricky things have been possible over time. I believe we've talked about BootIt NG, which is one of my favorite, is my favorite multi-OS booting tool, where...

Leo: I don't know if we have mentioned that.

Steve: It's actually OS independent. It's not free, but it's very good, and it's not very inexpensive. BootIt NG is - you install it on a hard drive. And it installs itself in the first track of the drive. Now, an interesting quirk of hard drive history is that partitions always start on an even track boundary. So if you've got the partition sector on the first sector of the drive, which is where it is - literally it's on the very physical first sector, that's where every BIOS knows to find the partition sector. Well, it's being there essentially ruins the rest of the track. You can't have partition data on the rest of the track.

Once upon a time that was no big deal. We had 17-sector MFM drives. And so the 18th sector was the beginning of the partition. Then we went to RLL, that had 26 sectors. Now we've got drives that have many, many, many more physical sectors. But for other historical reasons, the maximum number of sectors you can have on a track, logical sectors, is 63. And you'd think, well, it ought to be 64 because that's a power of 2, except that sectors are numbered from 1, so there is no 0 with sector. The first sector is number 1, then you go up to 63. So my point is that you always have the first 63 sectors of a hard drive almost uncommitted because that first sector is the partition table, and the partition table sector. And the beginning of the first partition will start on the second - I'm getting myself confused - the first sector of the second head of the drive. So that is to say the second track of the drive. So you've got almost 64 sectors. You've got 63 sectors, each 512 bytes long. So a little less than 32K bytes of space where clever people can tuck a program.

So, for example, BootIt NG creates a custom boot sector that displays a simple text menu on the screen, allowing you to choose which OS you want to boot. And in fact I do remember, Leo, on The Screensavers many, many moons ago, some guy wanted to see how many bootable OSes they could have on one drive. Do you remember that episode of The Screensavers?

Leo: He had hundreds; right? It was just crazy.

Steve: It was insane.

Leo: I don't even know how he found that many operating systems.

Steve: So anyway, a custom bootloader will take advantage of the fact that a partition sector is actually executable code. Another class of application that has used this fact, there were some - it used to be that BIOSes did not know how to handle the advent of really big drives. And so when you would buy a copy, for example, of - buy a copy. You'd buy a very big hard drive, like a big Maxtor drive. They would come with a little CD or a little diskette that had a sort of a BIOS patching utility...

Leo: Right, I remember that.

Steve: ...that would allow - it would allow an older machine to recognize a drive's full size. Well, that worked in the same fashion. It altered the partition sector to add some code that would essentially replace the BIOS's table that just didn't understand how to deal with drives of that size with a much bigger table. So there were - and of course now all contemporary BIOSes are up to speed, and they know how to ask the drive how big it is, and so they sort of adapt themselves dynamically rather than having a fixed table of drive sizes.

Well, the final really interesting possibility here for what to do with the fact that a partition sector is executed code is preboot authentication. That is, you could have an entire drive encrypted, except just the first track, just this chunk of data that is behind the partition sector. That could be executable code which is enough to get the system booted, that is, it would prompt you, it would put up some sort of a screen and prompt you for a passphrase or a username and passphrase or whatever they want for your authenticating to the system.

That code would then proceed to read in the beginning of the bootable partition, decrypting it on the fly. That is, it would read the physical sectors, decrypting those sectors as it loads them into memory. And it would stay in control. Essentially it would be - there's an old interrupt I know really well as the author of SpinRite called "Interrupt 13," which is the way the BIOS does its data reading and writing. So Interrupt 13 and the BIOS code is what gets Windows going until Windows' own driver takes over, takes over control from the BIOS and runs from there. So you could have this preboot authentication technology, which would - it would hook the Interrupt 13 BIOS, that is, it would - essentially it would intercept Interrupt 13 on the fly, performing on-the-fly decryption, until Windows took over. And then a companion Windows driver would know how to continue decrypting the drive in order to allow Windows to run and the entire drive to appear decrypted to Windows because there would be a seamless handoff between the decryption that happens to get Windows going and then a new Windows driver that's provided by the same decryption system that would pick it up and continue.

And so what this allows is it allows the entire drive to be encrypted, I mean, really, really strong encryption. It uses 256-bit AES Rijndael encryption. No force on earth could cause this data to be decrypted unless you provided it with the authentication information at boot-up. And once going, Windows just sees it as a regular drive. It sees it as, you know, it has full access to it, and it's able to use it. But if anything happened, for example the drive got stolen or the system got stolen, which was what I was concerned about preventing, there's no, absolutely no vulnerability of the data on the system.

Leo: Can I be a turd in the punchbowl here?

Steve: Sure.

Leo: It's not an open source encryption program, is it.

Steve: No, it's not. It's free, but not open source.

Leo: And here's why I raise that issue is, I mean, I don't know this company. I don't know what backdoors there are. It's not even a U.S. company, not that I would trust it more if it were a U.S. company. But this is why I stick with things like TrueCrypt. I don't know what's in there. I don't know if there's a backdoor in there.

Steve: Well, that's a very good point. More to my concern was that, as I was getting to know this system, I had some questions about specifically how things were done. That is, you know, exactly how...

Leo: Right. You can't tell how they've implemented it because you can't see the source.

Steve: That's very true. That's very true. Now, I have to say this hasn't put me off of it at all.

Leo: Yeah, because you're a closed source guy.

Steve: Well, because...

Leo: You are using Windows. I mean, I guess you're already in that environment.

Steve: Well, yeah. I mean, there's certainly far more danger from the user of Windows and Internet Explorer than there is from this whole-drive encryption system. Now, one of the things that I was concerned about was what is the overhead of doing this, because we've got a software driver that has essentially imposed itself between Windows and the hardware, that is, Windows and the drive. And those drives are not super speedy, we know, anyway. And it's not like it's software encryption/decryption that is sitting there between Windows and RAM or something, where there would be tremendous overhead.

So what I did was I made a drive - I used Drive Snapshot to create an image of the system. And I actually had an image that I had made of the system from, I don't know, like a year before. So needless to say there were many Windows updates, many security updates since that image. So what I did was - and anyone who's ever used Windows Update knows that that just drags a hard drive horribly because you've got all of these files that are being replaced and old ones deleted and so forth. So what this allowed me to do was this allowed me to create an environment where I was able to benchmark the performance of this FREE CompuSec whole-drive encryption before and after.

So I returned the system to an old image. I then - oh, and I also set up Vopt. Vopt is able to run from a command line. And I found a command line timer program, it was part of a Windows Resource Kit called EndTimer, that allowed me to time the execution of Vopt running from a command line to defrag this very fragmented system. So I went to the image. I updated it with Windows Update to bring it current, which just fragmented it to pieces. Then I timed the defrag operation without FREE CompuSec installed. Then I restored the image, reupdated it so that it was again fragged in exactly the same fashion, this time with FREE CompuSec installed. The defrag without any encryption took five minutes and 23 seconds in order to bring the drive back to a known defrag state. Five minutes and 23 seconds. With FREE CompuSec installed, it was five minutes and 54 seconds.

Leo: That's not bad.

Steve: So it was really not bad. It was less than 10 percent overhead. It was 9.74 percent overhead, which is unnoticeable in any sort of regular usage scenario. So, okay. So that's just one of the things. That is, this whole-drive encryption is just one of the things that FREE CompuSec does. It also - and again, this is a - I have to say, I am very impressed with the system. It creates log files for itself. It installs itself carefully. You're able to encrypt the whole drive from outside of Windows or from inside of Windows. If you do it from inside, I mean, it's sort of freaky, but you can literally be encrypting it while you're using Windows because it's moving from the front of the drive uniformly forward. It knows where it is, that is, how far it's gotten. And that's just a simple sector number. I'm now on sector number this. Now I'm on sector number this. And so the driver, the Windows driver is being informed in a synchronous fashion whether or not to decrypt based on whether it's accessing earlier on the drive that is already encrypted, so it needs to be decrypted on the fly and reencrypted before any writes, or whether we haven't gotten that far yet, in which case the data is still in the clear. You're able even to shut down Windows and then restart it, and it will pick up where it left off and continue the encryption process.

So they have this whole-drive encryption as part of the FREE CompuSec suite. Also CD encryption. You can create encrypted CDs and DVDs which are burned with any of a number of keys that it will make. And again, the result is a CD or a DVD that is just noise. It is pseudorandom meaningless noise unless you have the matching key. And this all uses AES 256-bit and Rijndael cipher. It will also handle removable media encryption - diskettes, any removable drives or USB drives. You're able to specify for any drives that the system has whether you want them to be encrypted or in the clear. And so it will do on-the-fly encryption to and from reading and writing from those drives. It will do individual file encryption using Diffie-Hellman public key crypto, so you're able - it'll create a pair of keys, a public and a private key, as we've discussed many times in the past, so that you're able to...

Leo: Why would you have public/private key encryption for a drive?

Steve: Oh, no, for individual files.

Leo: Oh, I see, for files. So you could send somebody the file, or they could send you a file, better yet, yeah.

Steve: Exactly. Yeah, you would be able to publicly post your public key, and then they would use this to encrypt a file that they send you, and you know that it was encrypted using that key, and you're the only one who's able to decrypt it. They even have what they call SafeLan is on-the-fly LAN encryption that allows you to create folders and directories on a remote server which are fully encrypted over the LAN. So any data that is being transacted through Windows filesharing to any file in a folder, with a nice, hierarchical, I think it's six or seven levels of key hierarchy, where you're able to specify, with a lot of granularity, who is able to access which files on the LAN. So, for example, you could have multiple systems all sharing files on a common server, and have good control over who is able to access and essentially see which files that are being shared on the server.

And finally, secure VoIP is part of this. Now, all of this is also available for Linux, except the VoIP is Windows only. So if there were an application, for example, within your corporation, where for whatever reason you need point-to-point, absolutely secure audio link, audio conversation, voice over IP, this system has it through a system called ClosedTalk, which uses the same crypto technology, builds the whole infrastructure for a VoIP system where everything going over the link, again, is just pseudorandom noise, absolutely indecipherable unless you have the key. And they've got all of the technology and a really nice presentation, I have to say. I'm very impressed with this package. Now, the only thing I know that competes with this is TrueCrypt 5, which is just out, as I said, updated two days ago.

It was interesting, one of the update notes for TrueCrypt mentioned that they had reduced the size of the decompressor, or of the preauthentication stuff, by 18K, which would solve a problem that apparently many people had been having since its release of TrueCrypt saying that it was out of space. What that meant is that, remember we talked about how there are literally 62 sectors of space behind the partition sector, which is probably where TrueCrypt was storing its data. The FREE CompuSec system works differently because I did, even though I've never been able to get a hold of these guys, their sector, their partition sector references areas on the main C drive and is able to load those. And those are locked in place.

I'm very sure, although I haven't done an extensive analysis of TrueCrypt, we're going to address TrueCrypt 5 in an episode here within the next few weeks because I want to essentially wrap up the whole question of preboot authentication and whole-volume, whole-drive decryption. TrueCrypt it looks to me like allows you to encrypt one partition, whereas FREE CompuSec encrypts the entire physical hard drive. There is no provision for only encrypting one partition of the hard drive. So it does the entire thing. Which, you know, may or may not be a problem.

One thing that FREE CompuSec does that TrueCrypt does not do, and they make a point about this, so it must be something that's difficult to do, is support for hibernation. FREE CompuSec will encrypt the hibernation file, which is a snapshot of the system RAM at the time the system was hibernated. TrueCrypt cannot, and so it disables hibernation mode completely when you are using a TrueCrypt volume.

Leo: Because it was a security vulnerability because that hibernate file would be unencrypted.

Steve: Yes, it is unencrypted; and it shows, you know, it's like a snapshot of RAM. It'll have your various keys, it'll have the files that are open, everything you're doing at the time of hibernation. Now, the problem is, I mean, I'm an avid user of hibernation. I boot my laptops very rarely because hibernating is just, I mean, in the original days hibernation was kind of flaky. Sometimes the system wouldn't come back from hibernation. Your VGA screen wouldn't work again or whatever, or sometimes USB wasn't functioning right. Well, that's all been worked out. And Microsoft has put a lot of time into power state management in Windows. So I come in and out of hibernation constantly with my laptop.

Again, I don't know how concerned I would be if my hibernation file were not encrypted. But it's definitely something to be aware of, that it is something that TrueCrypt specifically does not do, and they disable hibernation if you encrypt your entire drive because they want to make sure you understand that this is no longer safe. Whereas FREE CompuSec does manage to encrypt the drive. So it is at least one difference between them. So I just want to say that I'm, despite the fact that, as you say, Leo, it's not open source, I've spent a lot of time with this thing. I'm very impressed with the technology. And I wouldn't hesitate to use it, even though it's not entirely scrutinizable from an open source standpoint.

Leo: I'm just a paranoid. I just figure, oh, some government has created this. Particularly the VoIP. That's, you know, it's one thing, okay, so I encrypt my hard drive. They don't want my hard drive, and who cares if they have a backdoor to my hard drive, whoever "they" is. But VoIP might be the kind of thing, you know, if I were a government I'd encourage people to use our, quote, "encrypted voice over Internet" so I could snoop on them. So that makes me nervous.

Steve: Sure. I mean, it's definitely a possibility.

Leo: Yeah. Generally when it comes to encryption I like to stick to open source stuff just because at least it could be verified by - not by me, certainly. Maybe by you, maybe by somebody who knows what they're doing. But I just presume that it has been, and I don't even know who these guys - had you heard of this company, CE-Infosys, before? I hadn't.

Steve: No. Although I did pick up a pointer from one of our listeners who said they've got a very good reputation.

Leo: Yeah. They've been around for 27 years, it says on their website. So, yeah. If you're encrypting your company's laptops, you don't really care if some government has a backdoor to them. That's not the issue. The bad guys you're worried about. It is CE-Infosys.com. You know, I'm going to bring this up in a second. There's a couple of interesting recent court cases about encrypted drives.

Steve: Yes, as a matter of fact I was going to talk about a Washington Post story. But go ahead.

Leo: So I guess this was a fella coming across the border into Canada from the U.S.

Steve: Yes, you and I have the same story.

Leo: Yeah. He had on his hard drive some pretty nasty titled files. I mean, really, I wouldn't even want to say them out loud, they were so nasty.

Steve: No. I was planning not even to mention the content that this guy had. I mean, ugh.

Leo: Doesn't sound good. But it's just a filename. They were encrypted. He admitted that he downloads porn and occasionally comes across child porn, which he immediately deletes. Canadian officials arrested him - or I guess it was U.S. officials, I think he was coming in from Canada - arrested him and prosecuted, saying you've got to give us the password. You have to unencrypt this. They couldn't do it themselves. I don't know what he was using, but they couldn't unencrypt them without the password. So he obviously was using strong encryption. He refused. A judge has ruled that he has the right to avoid self-incrimination.

Steve: Yes, exactly. It was essentially the judge says that he has a Fifth Amendment right not to incriminate himself.

Leo: Fascinating. Very controversial. I mean, let's say - let's not say - the child porn thing makes it kind of as a macguffin. It makes it more controversial. But let's say he had on there a file saying a plot to blow up the Pentagon. So then it's, I mean, that's still pretty bad. But you get the idea. It doesn't - do police officials have the right to demand passwords? Judge says no. And in fact this isn't the first case. In another case a few years ago a judge said it would be equivalent to demanding to look into somebody's mind. You have a right to privacy. So that's kind of interesting. It means, at least in this country, it's not true in many other countries including England, but in this country the courts seem to protect your right to encrypt stuff and keep it encrypted.

Steve: Well, yeah. And the reason I found this really interesting was that it does speak to the question that people have asked. It's like, okay, well, if I really want to keep my private data private from everyone, and I have the technology to do it - and, I mean, this is the problem that the FBI and Justice Department face now is that they make the point that more and more people are using state-of-the-art encryption technology for their own privacy, and that it completely thwarts them because, I mean, there aren't backdoors to this kind of technology. When it's implemented correctly, there is nothing they can do. And so it's extremely frustrating for them because here they're got bad guys that are hiding evidence of their wrongdoing behind the technology, and using the technology. And so we've argued, and we've talked about this several times, Leo, the morality and the ethics of this, we've argued that it's not the technology's fault that it's that good that it's a tool both for protecting free speech and privacy, but unfortunately there's a dark side. It protects the bad guys who are able to use it.

Leo: I was frankly stunned. The court decision surprised me. I would not have expected that.

Steve: Yeah. It says on November 29, Judge Jerome J. Niedermeier ruled that compelling Sebastien Boucher, a 30-year-old drywall installer who lives in Vermont, to enter his password into - so compelling him to enter his password into his laptop would violate his Fifth Amendment right against self-incrimination. The judge said, quote, "If Boucher does know the password, he would be faced with the forbidden trilemma of either incriminating himself, lying under oath, or finding himself in contempt of court."

Leo: And so they had him in jail because he wouldn't give them the password.

Steve: Yeah. And so the judge said he is protected by the U.S. Constitution against being forced to give up the password.

Leo: Now, you know, I've spoken to the Secret Service and law enforcement officials, and I've asked them this question. This was some years ago, and they said, you know, we usually just ask the guy, and they give it to us. A lot of crooks don't make a big deal about not giving up the password. They're intimidated or whatever, and they do give up the password as part of, you know, and I'm sure they get read the Miranda rights. But as part of the interrogation this is something that they willingly give up. Also, you know, that's one of the things about TrueCrypt is this - I don't know if CompuSec has it. But TrueCrypt has this, quote, "plausible deniability" where you can't tell - the flaw in this Boucher's problem was that you could read the filename. If he had used TrueCrypt, you wouldn't even know there was any data there. Wouldn't look like a file at all.

Steve: Correct. In TrueCrypt you're able to essentially use a space at the end of the container, the container file you create, to create an additional sort of hidden place. And the way TrueCrypt builds its container, when you set up a TrueCrypt container it fills it all with pseudorandom data that looks just like...

Leo: Noise.

Steve: ...pseudorandom data. That's what it is. So there's no way to forensically analyze a TrueCrypt container and determine what's in it or whether there's anything else in it. So you're able to give up, for example, your external password and go, oh, look, here's what I've got in my TrueCrypt container. Well, the fact is you could still have another one, but there's no way for them to know or ever prove that you actually had another one that unlocked this essentially sort of a hidden compartment inside the container. So it's very clever. And no, FREE CompuSec doesn't have anything like that because it doesn't work in file containers. It encrypts the entire hard drive.

Leo: And it would be immediately apparent that the drive is encrypted. There's also, I don't know if it's TrueCrypt, I think it is TrueCrypt, there's some program that has this capability of having a pseudo key which you give the law enforcement people, and it unlocks something completely benign, and you're off the hook, and the stuff that you're really trying to hide - now, I'm not supporting all this because, I mean, I think about a terrorist. But fortunately terrorists don't seem to be technologically very savvy. But I think about a terrorist, how they could use this. Look, it's a picture of Mickey Mouse. And instead it's, you know, blueprints of the Rocky Mountain missile silos. So I'm of mixed feelings about this, you know?

Steve: Well, the one thing I want to mention relative to hard drive encryption, that is, whole-drive encryption, and this applies to native hard drive encryption where it's being done in the drive's hardware, and also to FREE CompuSec or the whole-drive encryption offered by TrueCrypt that we'll be covering extensively once I've brought myself up to speed on it completely, is it completely solves the problem of discarding your hard drive.

Leo: Oh, yes, that's right.

Steve: That is, you take one of these drives out, and you can just, I mean, you can hand it to anybody you want to. There's nothing on the drive that is meaningful or forensically recoverable if you have encrypted the entire drive. So you don't have the Darik's Boot and Nuke sort of problem, or the need to worry about having securely deleted things. It is just pseudorandom data on the entire drive. So you can sell it on eBay and not worry that anybody is going to be able to get anything else from it ever.

Leo: It's amazing. It's a very interesting philosophical discussion, I find. All right. We've got links to that program in our show notes, so you can find out more. You can of course go to GRC.com. That's where Steve not only puts his show notes, but also 16KB versions of this show. So if you know somebody who doesn't have a lot of bandwidth but still wants to listen, they can listen to that lower quality version, and it's a much smaller file, it's one quarter the size. You can also get transcripts there. And I think a lot of times people find it very nice to be able to read along, even highlighting and underlining information that they want to keep track of.

Those are all available from Steve's site, GRC.com, not to mention all the free stuff he gives away there, great programs like Wizmo for configuring your system or ShieldsUP for testing your router, all at GRC.com. And of course that's also the home of SpinRite, the finest, the best, the one-and-only hard drive maintenance and recovery utility, used for decades by geeks everywhere. We need to come up with a slogan like that for you. Saving the world one hard drive at a time.

Steve: I actually do have a slogan.

Leo: Oh, what is it?

Steve: It works.

Leo: Typical Steve. Simple, to the point, no frills. It works. That's all you need to know. Hey, Steve. Great to talk to you.

Steve: Likewise, Leo.

Leo: Have a great week. We'll talk again next week on Security Now!.