Listener Feedback Q&A #36

Description: Steve and Leo discuss the week's major security events and discuss questions and comments from listeners of previous episodes. They tie up loose ends, explore a wide range of topics that are too small to fill their own episode, clarify any confusion from previous installments, and present real world 'application notes' for any of the security technologies and issues we have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-134.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-134-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 134 for March 6, 2008: Listener Feedback #36. 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!. And it feels like more than a week since we've done the show, and actually it is because Steve and I prerecorded our last episode. I was about to go up to Canada. And now we have a lot of catching up to do. Hello, Steve Gibson.

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

Leo: Security guru extraordinaire.

Steve: Well, it was a busy, busy, busy week and a half, I guess it's been. It's funny, you know, this is a Q&A episode. And I literally had a difficult time sorting through all of the feedback that we've received from listeners because of something major that happened that bears directly on the recent topics of whole-drive encryption. You know, bizarrely enough, some guys at Princeton did some research where they really - this is an issue that's been known for a long time but never really received any focus. They did some quantification of a weird phenomenon with dynamic RAM where they learned and showed exactly how long data will persist in dynamic RAM after it's been turned off. The presumption was, you know, milliseconds. It turns out, well, no, it's more like seconds. And these guys did a ton of work to demonstrate how, for example, whole-drive encryption keys could be recovered from RAM before it had had a chance to decay far enough. And, I mean, they've done some really clever things that I'm going to talk

about in, I mean, extensively. We're going to give it a whole episode of its own. And there are other things that have all sort of happened all at the same time because it turns out that Firewire represents a vulnerability, and then USB dongles could be used to recapture RAM that hasn't been zeroed from, for example, after a cold boot. So...

Leo: We were all excited about the fact that we'd found this great full-disk encryption, and it all fell apart two days after we recorded the show.

Steve: Well, now, just - okay. Because I want to give this whole treatment, we're not going to be able to get to it for a couple weeks because next week we've got the founder of IronKey is going to be our guest on the show to talk about IronKey and their hardware encryption stuff. We've got today's Q&A, and we have a Q&A after that. So it won't be till the episode after that...

Leo: So we won't address this at all?

Steve: Well, there's just no need to. I mean, I want to give it - there's so much to talk about, I don't want to give it partial treatment. But what I did want to say was, for anyone who's worried, the bottom line is, if you wait 10 seconds, you're fine. That is...

Leo: So shut down and wait 10 seconds.

Steve: Exactly.

Leo: Before you walk off.

Steve: Well, maybe 20 to be really safe. Now, I mean, the fact is, it would be very difficult for someone to probably grab your laptop away from you and employ some sort of a hijack of the RAM without you knowing it. So my point is, the length of time we're talking about data staying in RAM, it was believed to be insignificant. It turns out, well, it can be significant, especially if you spray it with Freon, which can then actually cause the RAM to - the data in the RAM to last a lot longer. Anyway, I wanted to let all of our listeners know that I was well aware of this. Please...

Leo: We know. Stop emailing.

Steve: Please, when I updated my Security Now! mailbag, there were 745 pieces of mail. Most of them were about this. So...

Leo: First of all, we welcome people letting us know about this stuff. And really the fault is mine. I'm going to take full responsibility because we had to prerecord that show because of my monthly trip to Vancouver. And so as a result we did a show on TrueCrypt full-drive encryption several days after that news came out. And people thought, oh, well, they obviously hadn't paid attention. So it's just because we had to prerecord it. And that's not going to happen again. I've rearranged my schedule. I'm not going to be making those trips to Vancouver. So I will be able to make sure that we do this stuff the day, or the day

before, usually, we air it. So it's not going to be out of date. So that'll help.

Steve: Yep, that'll be neat. Also I wanted to mention that many people have subscribed to the ChangeDetection service. I've got a button on the Security Now! page, and there's one at the bottom of GRC's home page. And something like 8,000 people have subscribed over the years. And every time I make a change to Security Now!'s page, I deliberately send out an update. And the same thing is true with our web page. Well, the ChangeDetection people upgraded their system and broke the ability for me to say to their bot, do not look at this page except where I tell you to because all of GRC's pages have stuff that's changing on them, like download counts and page, you know, how many days since the page was last updated. And so I've deliberately over time constrained the ChangeDetection bot so that it only launches when I tell it it's okay to send the following message.

Well, they broke that. And so for, I don't know, for weeks people, like these 8,500 people were all getting mail saying, oh, this page has changed, this page has changed, when it hadn't. So I wanted to let everyone know, I wanted to apologize for that. It's out of my control because there was no way I had of telling their bot not to do the pages. And it was impossible to get a hold of them. I had to track them down by their DNS registration and then sent email that had a long response cycle. Finally I got somebody. And then it wasn't until I showed him a snapshot of all the mail they were sending out. Because I was getting a response from their bot saying, hey, we just notified 8,500 people of the change in your page. It's like, argh. So they finally fixed it.

Also our feedback form broke. Normally when you submit feedback, and you say, okay, here's my note to Steve about Security Now!, and you press the button to send it, it says thank you for your feedback, it's been sent to Steve. End of story. Well, what happened was, when I made some sitewide changes to add the GRC menuing that we talked about last time, I broke inadvertently that page. So people were concerned that maybe their feedback hadn't been received, so they would hit the back button and send it again, hit the back button and send it again. So I got lots of copies of everyone's feedback. The moment I saw that that problem was happening I fixed it. And so that's fixed also.

Leo: Sounds like it was a perfect storm of a week.

Steve: It was quite crazy. Also I did want to mention that the script-free menuing is up on the site. And we've got a search feature, sitewide search, courtesy of Google. And also if you get a search that is too wide, there's a link at the top that allows you to narrow it down to just Security Now!. So there's some nice Security Now!-oriented search that will allow people to find past episodes based on the transcripts that Elaine is doing.

Leo: Yeah. Great. That's very handy.

Steve: And then my last note is that there were three critical security vulnerabilities in the Opera browser that were recently addressed. My copy doesn't notice and look for updates by itself. I had to tell it to look for updates. I caught the little security blurb go by. So I just wanted Opera users to know that they do want to do a little manual check for updates because there were a couple important changes that were made. So they'll want to update Opera.

Leo: Okay. Very good. Steve, anything else before I read you - we've got so many questions for you.

Steve: I did have one little bit of errata that I wanted to share. We got a report from one of our listeners, Brian Dent, who reported that he was really glad that TrueCrypt made him produce an emergency rescue CD.

Leo: Oh, yeah.

Steve: It turns out that another Adobe utility - I don't know what it is with Adobe and track 0. But it turns out that he's learned that their acrotray.exe utility, which is some sort of something that lives down in the tray of Windows, is also writing into track 0 and wiped out TrueCrypt. He rebooted, and he typed in his password. Nothing happened. And he said he saw his life pass before his eyes. Then he realized, wait a minute, I've got that CD. So he booted from the CD. It was able to, of course, restore that track and the boot track, and he was able to get back into Windows. And again, by juggling back and forth a little bit, he figured out what it was that was causing the problem. And so this is two different things now from Adobe relative to, I guess to Macromedia. Or I think Macromedia was the other one. And so it's something DRMish that Adobe is doing is really causing problems. And he did do some browsing around and confirmed that lots of other people are having the same problem with Adobe's software and its collision with the TrueCrypt bootloader.

Leo: Oh, that's too bad.

Steve: So I just wanted to make sure our listeners knew.

Leo: That's too bad. That's too bad.

Steve: Eh, they'll have to fix it. I mean, nobody else is doing DRM that way. They certainly don't need to do it that way. Someone just said, oh, this'll be clever. And unfortunately that's an area that really needs to be reserved for non-OS or pre-OS things, and not used by software running in the OS.

Leo: But that is why they do it there, because then you can't - it's harder for you to hack it, basically.

Steve: Well, it's really not. Now that you know it's there, I would imagine you could just copy it to another drive and say, oh, look, you know, it's probably easy to fool after it's been exposed like this. I think they were thinking, oh, this'll be off the radar.

Leo: Yeah, nobody'll see it there, yeah.

Steve: Exactly. It's off the radar. Now it's really right in the middle of your radar because it's keeping your system from booting.

Leo: Yeah. Do you have any SpinRite tales to tell?

Steve: I have one little short notice. It's something that we haven't really focused on before. It turns out that most people who write testimonials do so because, first of all, they're Security

Now! listeners, and they run across some serious problem with their system. This is actually not from a Security Now! listener. I don't have his real name. His handle is Mgomgo. So, you know, yeah. Anyway, so he says, "I haven't used SpinRite very often (every couple of years or so). But one of my important USB drives got really goofy on me last night. None of the usual fixes worked, not even the XP repair utility on the install CD. So I finally remembered SpinRite. And in three hours a completely unreachable USB drive was restored to happiness. Just thought you would appreciate a positive feedback note."

Leo: Always.

Steve: So here's someone who doesn't know we get positive feedback notes pretty much all the time from our Security Now! listeners.

Leo: Now, don't say that. We welcome them. It's always good to get them.

Steve: Absolutely. Someone wrote the other day, well, I know you must get tired of these. And I'm thinking, no, no, no, no, I never get tired of hearing news of SpinRite saving somebody. I love that.

Leo: Yeah. Well, that's very nice. And of course if you want to get a copy of SpinRite it's easy enough. You just go to Steve's site, GRC.com. It is really the best hard drive maintenance and often recovery utility. Not always. Depends on what's wrong with the hard drive. If it's a file system error it's not going to fix that. But if it's a hard drive error it will. More than anything else I know. Are you ready for Q&A?

Steve: Let's plow in, Leo.

Leo: Mr. G. This is from Keion, I guess. Age 19, he's at Monroe College in the Bronx. He writes: Steve, I'm majoring in information technology. I'm a new lis- no, he doesn't talk like that. I'm a new listener to the Security Now! podcast. Welcome, Keion. Must say it's very interesting. You made me encrypt my - you made me. You made me encrypt my whole hard disk with TrueCrypt. But one important question. Even though a user may have encrypted his or her hard disk with TrueCrypt, can't the password still be retrieved if the user uses rainbow tables or the LOphtCrack live CD? Thank you. Now, explain what these are.

Steve: Yep. We've never talked about rainbow tables. It's even funny, the heritage of the name "rainbow tables." It comes from one of the early very popular DRM anti-piracy dongles that was from a company called Rainbow. And rainbow tables - so anyway, that's the name that these tables got. They are nothing however, other than precomputation hash tables. That is to say, the idea being that you could take all kinds of common dictionary-based words.

We've talked about how hashing works, how hashing is a one-way function. And oftentimes, for example, a passphrase will be hashed in order to turn it into a fixed-length blob which, for example, might be used as a key for symmetric encryption or for some other purpose. And so the idea being is hashing takes time. It takes time to put something from a dictionary through the hashing algorithm in order to get the hashed output. So since many different programs, for example, might use in the old days, for example, an MD5 hash, you could precompute the hashes, and that's what rainbow tables are. Rainbow tables are all kinds of phrases and dictionary words and combinations of words that have painfully, in terms of compute time, been

hashed once.

But rather than redoing all that work when you want to crack somebody's password, if you knew, for example, that the password was going to be run through an MD5 based on the OS, for example it might be a version of Linux or UNIX where they use an MD5 hash for the person's passwords, instead you would - somebody, some, like, bunch of people would do all of this work finding out, determining the MD5 hashes for a huge number of common phrases and passwords, and they'd save them. So the result is these rainbow tables. And then it's much faster to simply run through the table trying all of those at very high speed. You no longer need to do the hashing of each of these things because they've already been hashed. So essentially they are prehashing a large number of possible common passwords and phrases. Well, so that's what rainbow tables are.

To answer his question, it's certainly the case that precomputation attacks like this are possible. But they only work if you're starting off with a bad password. So if you've got, you know, if you've used Scott, for example, as your passphrase, well, that's very bad because it's going to be in a dictionary. It's going to likely be in a precomputation table. And so, sure, it would certainly be possible for a system if you had a very, very weak passphrase and somebody specifically modeled the TrueCrypt technique going from your passphrase through the building of the decryption key for your drive. Then, yes, potentially it would be better to do that than it would be to manually put in every possible phrase.

So again, the takeaway is you absolutely want to have a nonguessable passphrase, which is not going to be in a dictionary. You know, something that looks really random. Come up with some algorithm for typing on the keyboard, skewing the letters, scrambling things, add in some noise characters, you know, all the things we've talked about in the very, very early episodes of Security Now! for how to get good passwords. If you use good passwords, then you're not going to be subject to any kind of a precomputation hash attack because yours won't be in that table of possible hashes.

Leo: Right, right. So as far as LOphtCrack, that's just a brute-force crack; right?

Steve: Exactly.

Leo: And so same issue.

Steve: Exactly. Same issue, the idea being that you don't want whatever - you don't want your passphrase to be in anybody else's dictionary or crack library in any way.

Leo: But if it's a totally random password, the likelihood - with enough characters - the likelihood of them getting it by a brute force shrinks to nothing.

Steve: Well, yeah, exactly, because they're inherently going to try more likely passphrases, and yours just won't be among them.

Leo: Yeah. There you go, Keion. Thanks for writing, and welcome to the show. We hope you listen from now on to every episode. Benton Greene of Austin, Texas wonders about data recovery on encrypted drives: Hi, Steve. I was listening to Security Now! 132 and heard you talking about how SpinRite doesn't care if a drive is encrypted or not since it only looks at the bits and whether or not it can read them. It's trying to make sense of

them or its file structure. That got me thinking. I remember you talking about how SpinRite will read the data off a bad sector, write it to a good sector. But if the drive is encrypted, everything on the drive is pseudorandom noise. So how does SpinRite know not to write over any pseudorandom noise it might find on a good sector?

Steve: This was a great point because it highlights some confusion about the way drives handle bad sectors, and also how it is that data recovery can still function even on an encrypted drive. I mean, you know, if a lot of people are going to be encrypting their laptops, and for example they were able to successfully use SpinRite in the past to get them out of a jam, they'd like to know that SpinRite or appropriate data recovery technology could still be used.

So back in the old days of the FAT file system and when I first wrote SpinRite, it was aware of the file system structure and operation. And it had to be because SpinRite needed to manually spare out sectors and move clusters around as it was moving valuable data out of regions that it had found to be defective. So in those days drives were not dealing with their own defective sectors. They were relying on the operating system and the file system to mark clusters bad, saying this is a region where it is not safe to save data.

When drives became intelligent, that all changed. Drives then became responsible for the data stored in their own sectors and responsible for relocating those sectors themselves. So what SpinRite developed into was technology which would work with the drive to show the drive that it had a problem. That relieves SpinRite of the responsibility of understanding the file system and made SpinRite file system independent, which is the way it's able to work on Macs or TiVos or unformatted drives even, just anything. Or drives that have been completely encrypted. So again, SpinRite doesn't need to understand what is there. It's able to show the drive, hey, I've got a sector that I've managed to recover the data from. Give me somewhere safe to put it. And the drive will then perform that relocation underneath, sort of underneath the level where the operating system and SpinRite interact with the drive.

Essentially sectors are all numbered. They're numbered zero through some really big number with lots of digits. And that's how many gigabytes of data you've got. And so literally sector number 32627, for example, will go bad. Well, what happens is, the drive takes that physical sector that was 32627 and makes it inaccessible. And it takes a spare sector that it has and numbers it, literally gives it the same number, 32627. And then SpinRite puts the data back from the recovered sector that it's been holding in RAM into this new sector which has the same number but is a physically different sector. So essentially the operating system doesn't know anything happened, yet the data was recovered from a bad sector, put into a good sector, and that sector's number is the same. So the operating system accesses it just like it was the bad sector, although now it's good.

Leo: Interesting. Interesting. So really the file system keeps track of this stuff, not SpinRite.

Steve: Well, SpinRite doesn't. And the file system no longer needs to because the drive keeps track.

Leo: Oh, the drive, I see, at the lower level, yeah.

Steve: Exactly. Underneath all this the drive says...

Leo: But there is a file system, isn't there? I mean, even when you're encrypted there has to, I mean, doesn't - there has to be a file system to know where the file is.

Steve: Sure. But that's on the other side of the encryption/decryption.

Leo: That's encrypted. So that's garbage data, as well.

Steve: Exactly.

Leo: Invisible, yeah.

Steve: So all the drive - the drive doesn't care what you store in its sectors. And now neither does SpinRite. So SpinRite works with the drive. Neither SpinRite nor the drive care about the specific data you're storing because working together they're able to make sure that whatever it is you store is stored correctly, regardless of what it is. Whether it's pseudorandom noise or normal, nonencrypted file system data.

Leo: That's actually quite clever.

Steve: It's very cool.

Leo: So does it do that even on unencrypted drives? I guess it would.

Steve: Yep, it does them on all drives.

Leo: That's how drives work.

Steve: Yep.

Leo: It's good to have Steve around because he understands how drives work in ways that I think most people do not. I mean, you have to to work - to do SpinRite.

Steve: To write it, yeah.

Leo: Ryan listening in Florida was thinking about latent unencrypted data. I don't know what it means, but I like the phrase. Steve, after hearing your review and your concerns with full-drive encryption I've been wondering something. You mentioned before that even if a hard drive is zeroed out, depending on how many times a sector is written to, it will still contain bits from previous data. Please forgive me if I misunderstood what you were saying. But if this were the case, couldn't the original unencrypted data still be read from a drive even if the drive was fully encrypted? Would the best possible scenario be DBANing the drive - that's that program we recommend, Darik's Boot and Nuke - for a clean install

of the system, then immediately encrypt the drive before any sensitive data is put on the drive? That's a very good point. Just want to confirm my suspicions and inform your listeners of potential security risks involved even when using full-drive encryption.

Steve: We sort of touched on this during our discussion of full-drive encryption, but it's a very good point, as you mentioned, Leo. And I wanted to sort of highlight it. And that is that we've talked about secure deletion of data from drives, that is to say that if you simply write zeroes over a data sector, when you read that data back, you are certainly going to get zeroes. I mean, that's how drives work. They're going to give you back what you last wrote. But in fact when you write zeroes, it's an additive process. That is, you're adding magnetic flux reversals on top of the ones that were there before. You're doing it strongly, that is, you are suppressing the prior ones. But you're not completely eliminating all of their influence. So there is a sort of a latent image of the data that was stored before, underneath what you've just written.

Now, it's very weak. And it's weak enough that it won't confuse the drive when the drive reads that data back. It'll read back zeroes if that's what you wrote. But if you had very sensitive equipment - and this definitely exists, such sensitive equipment exists - and that equipment, for example, read back that you had zeroes, and then it said, okay, I know that he's written zeroes, so I'm going to subtract the zeroes out of the actual magnetic flux data that's there. What that would do is that would have the effect of subtracting out what had most recently been written, leaving behind what was there before. So it's literally a way of, like, peeling a layer of history off of the hard drive, allowing you to get to what was there before. Which means if you simply ran one encryption pass over your drive, you are writing - you're turning every sector of unencrypted data into pseudorandom noise, as we know, and writing it right back on top. But that latent unencrypted data is still there.

So it's exactly like we were talking about the problem of securely erasing a drive. In order to securely erase a drive, the best way to securely erase a drive is to record multiple passes of really, truly random data. Well, we know how virtually impossible, not completely impossible, but really hard it is for computers to create truly random data. So really good pseudorandom data is good enough. The point is, you want to - there are, for example, there are secure erasure programs which write well-known patterns on the drive. Well, that's not what you want because if the well-known pattern is written, then somebody who's trying to peel these layers off to get back into the history of what was written, they know what those well-known patterns are. They know what to successively subtract from the existing data in order to peel back each layer.

So what you really want, the optimal erasure is just several erasures, several overwrites with pseudorandom data. That way they don't know what they're peeling off layer by layer because it was just pseudorandom. So, and the state-of-the-art secure erasing utilities do typically now have a pseudorandom options. And a few passes of that is absolutely all you need. But we did also mention, and here would be like the ultimate solution, and that is, get a brand new drive that has none of your data on it. TrueCrypt it first, then do all your work. That is to say, you have to have Windows on it. So you would take a brand new drive, you would install Windows, then before doing anything to it, before customizing it, putting any data on it at all, give it full-drive encryption. That way everything you ever store of yours is always encrypted by full-drive encryption, and it never exists on the drive in unencrypted form.

Leo: So let me just ask you, this is actually a topic that goes beyond whole-drive encryption, but the issue of fully securely erasing a drive. And let me ask you a couple of questions. If you - obviously the chance of recovering it if you do it a few passes is going to get tougher and tougher.

Steve: Yes. Essentially what happens is you are pushing the signal into the noise. There's a

signal, and there's noise, the so-called signal-to-noise ratio. So every time you're writing on top of it you're obscuring the signal, pushing it into the noise. And at some point, after a couple passes, there's just no way that anybody, no matter how sensitive their equipment is, is going to be able to find a signal that is several writes into history. At that point the actual physics of the signal being recovered from the drive will prevent you from finding the signal amid the noise.

Leo: Right. Now, practically speaking, who has machinery that even can read it if it's overwritten once?

Steve: Oh, we're not talking some guy in his garage. We're at the NSA sort of level.

Leo: But you are sure such a thing exists?

Steve: Oh, absolutely. It absolutely does.

Leo: Okay.

Steve: Yes. Yes. I mean, it sounds like science fiction. But nobody would have believed a couple weeks ago that you could turn a computer off and capture its RAM half an hour later if you quickly froze the memory chip. So, yes, I mean, this kind of stuff, it absolutely does exist.

Leo: How many passes do you think you need to do to make it impractical to do this?

Steve: With pseudorandom data, three or four would absolutely be enough.

Leo: Not ones and zeroes, but pseudorandom data.

Steve: Yes. You absolutely need a pattern that is not known by the people who are trying to recover it.

Leo: Ah. If they know it's a one they can subtract that one.

Steve: They can subtract that one, exactly.

Leo: Oh, interesting. So you need to cover it - one pass with pseudorandom data, would that be enough?

Steve: Eh, it's enough for me. I mean, maybe two.

Leo: It'd be pretty hard to do, I mean, one pass even, since you don't know what's been

written over there, it'd be pretty hard to reconstruct that, I would think.

Steve: Correct. Well, okay. Think about it this way. If you did two passes, you always know what was last written. Because that's, I mean, that's screaming at you, one, zero, one one, zero zero.

Leo: Oh, because the file system tells it, that's right, of course.

Steve: Yeah, I mean, that's the data the sector has.

Leo: That's retrievable, right, right, right. Two passes is what you need, then.

Steve: Yes. And, I mean, there are people that have, like, do 30. It's like, okay, well, how much time do you have? You could throw the drive away and go to Fry's in the time, I mean, in fact, you could earn enough money to buy a new drive in the time it would take to do that 30 times. So...

Leo: What I am surprised is to see the number of supposed drive shredders that do ones and zeroes. That seems to be the most common.

Steve: Yes. It is a misnomer that writing known patterns is useful. It's absolutely not what you want to write. You want to write noise. Because no one then will know what it is they're trying to subtract after a couple layers.

Leo: Now, I'm looking at Apple's secure erase options. They have zero-out data, which writes zeroes over the data once. Not good enough.

Steve: Not good enough.

Leo: They do have a seven-pass erase using DOD 5220-22M. It erases the information and writes over the data seven times. Doesn't say what it writes it with. But it's going to take seven times longer. And then there is a 35-pass array.

Steve: I know.

Leo: I don't know why it would include that. It doesn't specify random. But I'm figuring, if you're going to write, you might as well write random if you understand what you're doing.

Steve: Right.

Leo: Which I didn't, but now I do. Thanks to you, as usual, we've learned something today. Matt, tuning in from Melbourne, Australia, has connectivity troubles. I'm sorry, Matt.

I have a Netgear wireless router WPN824 RangeMax that I'm now using with a hardwired Ethernet connection on my PC. That's a terrible accent, I apologize. Also with a wireless connection to our other home PC. My whole LAN was wireless until I got fed up with having to reboot/repair the connection due to signal loss, or what I thought was signal loss. I installed the Ethernet connection - it's amazing, all the questioners actually sound like me, don't they. I installed the Ethernet connection to my PC and left the other PC to continue using the wireless connection on the router. However, even now with a direct wired link to my router my connection is having the same continuous issues. I get these kinds of questions on the radio show all the time. I'm so glad you're getting them. What can I do? Since I download approximately 50GB a month - what's he doing?

Steve: Uh-huh. I think his ISP has got his number, too.

Leo: I think so. I need a reliable connection that won't keep dropping out, et cetera. Is it dropping out, or may I have a setting wrong somewhere? Also, how can I give my connection to the router priority over the wireless connection without interrupting performance for either one?

Steve: Okay. There are a couple things going on. First of all, if Matt is downloading from Melbourne 50GB a month...

Leo: That's a lot.

Steve: ...it may very well be that his appetite for downloads has come to the attention of his ISP. We do know that ISPs are now doing so-called "bandwidth throttling," not being 'Net neutral, and have the ability to interrupt connections. So we know that's going on. We don't know that that's what's happening for Matt. He's having this problem over his non-wireless connection, that is, over his physical, electrically wired Ethernet connection.

Now, I have seen that some switches and routers are more finicky about the quality of the cable that is being used. And most people are now running at 100MG, if not a gig, between their equipment. The equipment on each end has to be a gig, so you have to have a gig Ethernet adapter. But, for example, most laptops, new laptops now have it because it's like, oh, yeah, well, why not? This is a phenomenal amount of signal to squeeze over a cable that's wandering around the living room and looping around the dining room table a few times and going lord knows, probably runs behind the toaster on the kitchen sink. I mean, it's amazing this works at all. So I would absolutely pay attention to the quality of the cable and the connections.

The Ethernet connection, the RJ45 connector was beautifully designed with gold contacts. It was designed so that, as you plug it in, it's creating a wiping contact in order to continually sort of self-clean and get any oxide off of the wires that may be there. But I know that I've solved problems sometimes just by jiggling it in and out a little bit to sort of rewipe the contacts. So that's worth doing. Now, many people also have problems with wireless disconnections. And it turns out...

Leo: That's very common.

Steve: Yes. It turns out, believe it or not, that this is by design, and it's Microsoft's fault.

Leo: Oh, great. Just empirically I have this experience because whenever we do Skype with people on wireless I ask them to go wired because of dropouts.

Steve: Yes.

Leo: Usually brief, but nevertheless apparent.

Steve: Well, and believe it or not, even deliberate. What happens is, Microsoft came up with this wonderful technology in XP called Wireless Zero Configuration. And what it literally does is it deliberately disconnects you periodically in order to see if it can find a better access point for you to be connected to. Now...

Leo: I call that promiscuous.

Steve: Who knows what they were thinking. The common wisdom is that they were thinking, well, people are just web surfing. And so you click a link, and you get some stuff, and then you read the page, and you click a link. So they really won't even notice if we just disconnect them...

Leo: And it's true, you don't.

Steve: ...as long as we reconnect them quickly enough.

Leo: Yes, it's true.

Steve: The problem is that many people are not in that model anymore. Many people, like you were just saying, Leo, create static connections for instant messaging or Skype or remotely connecting across a VPN to some other system. I mean, the model for many people, especially as ubiquitous as WiFi has become, no longer tolerates brief disconnections. So I made, in response to this, the first update to Wizmo in six years.

Leo: Oh, that's great.

Steve: Wizmo has a new command called wanlock. So you say "wizmo wanlock." And following the Wizmo model of creating a shortcut, basically it allows you to put a little shortcut on your desktop or down in your quick launch tray where, after you've got a connection that you like, you just click that, and it stops the Wireless Zero Configuration service. It turns out that just stopping the service stops this from happening, and you no longer lose your wireless connection.

Leo: I do recommend people just disable that service because there's no real reason for it.

Steve: Well, as long as you don't need it in order to get your connection going initially. So I also have wanopen, which does the reverse of wanlock. And so that just starts the service up

again, in case somebody needed it. Now, normally the service is set for autostart, so it'll automatically start when you boot. So the idea would be, you boot up and get connected. Then you can just do the little Wizmo wanlock. Or, I mean, you don't have to do that. If you don't want to use Wizmo, just stop the Wireless Zero Configuration service. You could also open a DOS prompt and type "net stop wzcsvc" and hit enter. That'll do the same thing. But that's all I did. Wanlock just stops the Wireless Zero Configuration service. And I think you'll find, given that you've got a strong enough signal, that these dropouts go away.

Leo: Didn't we also talk about a fix that Microsoft pushed but never told - actually didn't push, released but never pushed, never told anybody about, that improves Wireless Zero Config or fixes these problems?

Steve: I know that we did. And I don't know...

Leo: Fixes this problem.

Steve: I'm not sure now what it was that it was doing. The problem is, some people who are network-savvy believe they're making things better - or, that is, more secure - by turning off their access point's SSID broadcast.

Leo: Yeah, right.

Steve: That's another problem is it's better to have that on. For one thing, it provides you no security. Remember...

Leo: It's in every packet.

Steve: Yes.

Leo: It's actually transmitted. So...

Steve: Yes. It's got to be - it's in the packet. Anybody sniffing anyway can see what your network's SSID is. The only thing...

Leo: And it slows things down considerably because your system's going who are you, what are you doing here?

Steve: Yup, it ends up being a bad thing for WiFi performance. So I have a friend who, sort of tongue in cheek, he changed it to something like NORAD Central Command or something. And he actually lives not far from a major military base. And so you could imagine people who, like, networks - networks within range comes up. And it says NORAD Central Command. It's like, ooh, crap, I'd better not touch that one.

Leo: Or more likely, let's attack. Let's get in that one.

Steve: Oh, he uses a WPA key from GRC, so believe me, they're not going to figure that one out.

Leo: Yeah, I get calls all the time about connectivity issues. And wireless especially is a constant dropout. Why he would get a wired dropout, I think you're hitting the nail on the head. If he's downloading 50GB a month, his ISP is kind of nudging him a little bit.

Steve: I think they're doing a little throttling, yeah.

Leo: Do you really need all that bandwidth? He's probably doing BitTorrent, and they probably are throttling those. Deric Merino in San Diego, California needs his file to be touched. Touch me. Hi, guys. Before going into my issue let me say I'm looking through the documentation, and I haven't found anything to help me yet. Good, we like it when you read the manual first. He says: I've been using TrueCrypt for some time and recently started using Jungle Disk. Which we both love. Steve and I use that. I just love it. I'm running into a situation where Jungle Disk is not backing up TrueCrypt archives and would like to run my scenario by you. Let me explain.

I have a TrueCrypt archive - actually I have a few, but let's just use one for example - created Jan. 1, 2008, given a size of 200MG. So the initial timestamp says 01/01/08. The file size will not change as I add/delete files because of the way TrueCrypt chunks HDD space. It's always a 200MB file.

Steve: Right, it's a container file.

Leo: Yes, container. I've configured my Jungle Disk auto backup to run periodically, grabbing some specific folders as well as this specific archive file. Jungle Disk pulls them all up to S3, no problem. Now, let's say that today, February 25 - in this case March 6 - I add or delete or modify some file in the archive through TrueCrypt. When I'm done, I unmount all the TrueCrypt dives, then manually kick off the backup process. Jungle Disk does not see that the archive file has changed. Therefore it doesn't reupload it to S3. Looking at the archive through Windows Explorer I see the initial timestamp hasn't changed from 01/01/08. To me this is strange. Shouldn't the timestamp or at least the hash of the archive change when I modify the internal content? If it does not change, I'm not sure how to get Jungle Disk to reupload. Any thoughts? I don't think it's using date. It's probably using a CRC or something that...

Steve: Well, that would take a long time to compute.

Leo: Oh, would it. Oh, okay.

Steve: Yeah. My guess would be, for example, that at first that Jungle Disk first looks at the date, assuming that that's going to change if the file is written to. And then maybe then it does some sort of a hash, or it has some logic for deciding whether the date reflects an actual change. I sort of smiled because this sounds to me like the TrueCrypt guys doing their job, which I think they do very well, of further obscuring what's going on.

Leo: Nothing's changed here. Go somewhere else.

Steve: Exactly. I'll bet that they are deliberately keeping the timestamp constant, just to say, oh, yeah, you've not accessed this strange file. We don't know what this is. It was created back at the beginning of the year, and no one's done anything with it since. I just think that's very cool, and I would bet that's what they're doing. However, that has a problem which Deric has discovered, and that is that Jungle Disk, or for that matter any other backup tool which is based on - which is using timestamps on files to determine whether they've changed, would not see a change. Which is why I mentioned at the top that his file needs to be touched.

Many old computer guys may be aware of the "touch" command, which is probably originally a UNIX command, which allows you to essentially manually change a file's time and date to the current one. It was used by developers a lot because there's a process known as "make," that uses a make file, which sort of automatically compiles changes and sort of builds - it's used for rebuilding programs. Sometimes you have a need for telling something in your system, very much like this, to take a look at this file, it needs some attention of some sort, needs to be recompiled or something, where that process may not be automatic. So you would have a touch command. You would touch the file to set its time and date to the current one.

It turns out that the UNIX utilities have been recompiled and ported over to Windows. And on today's show notes for this show, Episode 134, I've got a link to a set of open source versions of many of the standard UNIX commands, among which is touch. It's very small. I've got one of them on my machine which I use for various purposes. So anyway, I wanted to aim Deric at that link where he could find the touch program to manually tweak his TrueCrypt archives so that Jungle Disk would then see them. And it looks, I mean, this is a manual process. But he's already unmounting his archives and manually launching Jungle Disk. So I would imagine that adding one little command to a batch file, if that's what he's using for unmounting them, would be trivial. And then this would work for him.

Leo: There's another possibility, and I'll run it by you. Jungle Disk's backup by default does not back up in-use files. Would it be seen as in use if TrueCrypt had that file open and was saving stuff to it?

Steve: No, because in the scenario that Deric mentioned he is unmounting those.

Leo: Oh, okay.

Steve: And that would be closing them.

Leo: There is a switch in Jungle Disk that you could say backup, locked, or in use, or files that are in use by other applications. So that might be worth a try. But, yeah, if he's unmounting it, I guess it wouldn't be seen as in use. The other thing is there are other programs like rsync that do in fact do a checksum. I don't know what Jungle Disk is doing for its backup, how it's determining it. If it's just looking at the date, yeah, that's obviously what's confusing it. But rsync does a rolling checksum. I mean, it actually looks at if the file's been changed. And that will work with Jungle Disk, as well. Moving on, another question.

Steve: And for what it's worth I think rsync is part of that package also that I mentioned.

Leo: Oh, yeah, rsync is a universal UNIX program. Just it's odd that Jungle Disk would only look at the file date. That's not a great way to do that. I guess it's faster, though, isn't it,

yeah. Andrew Dalton, lurking somewhere in Connecticut, was wondering: Steve, a question came up amongst my coworkers. I thought you'd be the guy that ultimately could answer the question. We are thinking of using an eraser utility to securely delete sensitive files, overwriting them seven times. A question came up on what kind of threat or vulnerability - we're circling back.

Steve: Yeah, we sort of are.

Leo: What kind of threat or vulnerability does that protect against? Does an attacker need physical possession of the drive to retrieve files that were deleted by conventional methods? Or could an attacker retrieve these files by hacking in over a network, if they could get past the firewall and the security measures? They'd need physical access, wouldn't they?

Steve: Yeah. This was interesting because it puts a nice little bit of frosting on the discussion we were just having. In order to read the data underneath what's been written before, you need, I mean, serious, serious, technology. Maybe you could use the drive's normal heads with a high-precision analog-to-digital converter to digitize to a much greater degree and with much greater accuracy than the drive normally did, the analog signal that the drive's heads retrieve. But it may very well be necessary to take the drive apart and give the platter extra special care and extra kinds of equipment.

So the answer is, to do anything like this, to get underneath the data that has been overwritten on a drive, I mean, it is way beyond anything you could do at the API, that is, the electrical interface to the drive. That's always, by definition, going to just give you what was most recently written to the sector, which of course is the drive's whole point. It never wants you to see what was there before because something was written on top of it, and that's the data that you want to get back when you read it. So no way could you do it with anything other than really fancy equipment, replacing probably the little motherboard of the drive, or maybe even needing to take the drive physically apart and have access to the platters themselves. So by no means could it be done remotely or from outside the computer.

Leo: Let's just say it. Only the NSA could do this.

Steve: Right. It's not something to worry about.

Leo: If anybody can, it would be the NSA. And they would have to come to your house, take your computer, take it back to Fort Meade - it's not going to happen.

Steve: Well, but this is the kind of stuff that was done, for example, after 9/11, if terrorists' hard drives and laptops were found.

Leo: It was, you're right, yeah.

Steve: I mean, believe me, they were going to find out what was written there.

Leo: Yeah. You know, I wonder, I mean, how sophisticated are terrorists? Are they smart enough to use encryption?

Steve: Unfortunately they're all using it now.

Leo: Rob Pontes of Toronto, Ontario, in Canada, of course, worries that maybe Steve wasn't paying attention. Steve, pay attention.

Steve: I'm trying.

Leo: You need another quinti venti latte.

Steve: You've got my attention, Leo.

Leo: Hi, Steve. I listened to your podcast on TrueCrypt 5 and was confused by your finding that system performance was increased. You mentioned that you were restoring your system from an image, though. So my question is this: Wouldn't the act of restoring a drive not place the data more closely together than the initially imaged drive? In other words, optimize it? Defragment it? Could that account for the performance increase?

Steve: I was paying attention. And that certainly did occur to me. So I verified that the imaging tool I was using, which was Drive Snapshot, I verified that a restored snapshot was restoring the individual sectors in their highly fragmented, lots of holes and spaces left on the drive, position, which in fact it was. So Rob is completely correct. If I did, for example, a file-by-file backup and then did a file-by-file restore, it would just put them all right back in the file system, packing them one after the other, and I would lose the fragmentation that I had deliberately created by giving Windows all those security updates on an old version of Windows specifically for the purpose of fragmenting the drive pieces. So I did make sure that this was going on.

I should mention that this was by no means a super extensive, thorough benchmark. I just did it quickly because, when I was using the FREE CompuSec utility, I did see a 9 percent overhead of just doing this defrag operation. And as we know, for whatever reason I got a negative percent overhead with TrueCrypt. I have to imagine that it was some caching and buffering they're doing that happened to favor the fact that I was doing sort of random reads and writes to the drive. The good news is, though, it is not slowing systems down appreciably. That much we know. But I wouldn't want to sell my little quickie benchmark of just seeing how long it takes to defrag a drive as being extensive, real-world performance. That was just something to give me an idea whether this thing was going to be slow. And it sure is not.

Leo: Well, for one thing, it's much heavier disk access than most programs would ever do. But that's what you wanted to find out is how it impacts...

Steve: Exactly, exactly.

Leo: Clement listening in Melbourne, Australia - another Melbournite - found scripts on

GRC. No. For shame. Mr. Anti-Script? Hi, Steve. I'm a long-time listener of Security Now!. I used the Firefox no-script plug-in to disable scripting while browsing the 'Net. I noticed as I am surfing your 'Net that three to four scripts are currently forbidden from GRC.com and GRCtech.com. I'm curious about this. I thought your website was script-free. Could it be some malware hijacking your site? What's the matter, mate?

Steve: Not to worry, Clement. I have to say, though, I've slipped a little bit into the dark side.

Leo: Oh, Steve.

Steve: It was a consequence of adding that Google search technology to the site.

Leo: That's a JavaScript piece.

Steve: Well, it is JavaScript, and it uses JavaScript in order to return the results. However, while I was over there in Google Land, they sort of said, hey, you know, if you like search, how about our web analytics technology? And Mark Thompson, my buddy at AnalogX, had been raving about...

Leo: I use it. I love it, yeah.

Steve: Yes, the amazing amount of information that a webmaster is able to obtain about where people are coming from, what searches they're using, what search tools they're using, how long people are staying, how many people apparently go there and immediately leave, blah blah blah blah blah. So I thought, well, let me just sort of try this. And to do web analytics requires that you put this little, actually two little JavaScript instances at the bottom of each of your pages. So that's what's going on.

I don't think I'm going to keep it because I can live without it. And I do still sort of feel like this is kind of icky, especially to be, like, exactly as Clement has seen, to be throwing up warnings because he's using no-script all the time. I don't like that. And here I went to all the trouble of doing an absolutely 100 percent script-free CSS-based menuing system. So, yeah, I think that's just temporary. I'm going to give it a few more - maybe another week or two. And, I mean, I looked at it today, I look at it every couple of days and go, okay, that's interesting. But it's like, I don't really care. So it'll be leaving soon.

Leo: You know, it just really underscores how difficult it is to use a script-free web.

Steve: Yes, Leo, we're losing the battle.

Leo: Both for users and for webmasters. I use Google Analytics. And while I don't have the same fear of scripts that you do - well, they're just everywhere. I mean, you're probably one site in literally a million that doesn't use them. So everybody does. And, yeah, if you don't like them, no-script is a really good Firefox plug-in that just alerts you and will disable scripts whenever you say I don't trust this site. On the other hand, you're probably going to enable them in most cases. Certainly if you use TWiT.tv there's scripts for the

Flash, there's scripts for analytics, there's all sorts of scripts on there, all benign.

Now, there is a larger issue with Google Analytics, which I think is worth addressing, which is you're sending Google information about every single person who visits your site, including the things that any log keeps track of, like IP address, browser used and so forth. I'm not sure we want to share that information with Google. And certainly we're not telling our users we're doing that.

Steve: Good point.

Leo: So that's - I think that's an even larger issue. And I use Google Analytics because it's free. It's really excellent analytics. They bought Urchin. If you are willing to spend money, you can host it locally. And there are certainly many stats packages you can host locally that don't, in fact, put any JavaScript on the page, they just analyze the log. And that's probably, you know, you won't get heat maps and things like that. For that you need JavaScript. So I...

Steve: And they've got some just...

Leo: Oh, it's great.

Steve: Oh, have you seen that deal where you can do the overlay, where you...

Leo: Yeah, that's the heat map, yeah.

Steve: You hover your mouse over your own links on your own page, and it shows you - oh, my goodness.

Leo: You can see where people click, where they linger, what they're looking at. And that's really useful for understanding how people use your site, what they like, what they don't like, what they never use. But that requires JavaScript because something has to follow their mouse around. And that's the problem. That you cannot get out of the logs. You can only get what page they're on and for how long. You know, the referrers, things like that.

Steve: And I don't even have logging on most of the time.

Leo: Your server is not logging?

Steve: No.

Leo: Really.

Steve: No.

Leo: See, that's good. I think that's great. I mean, that really is, you know, 99 - again, you're one in a million. Almost everybody, I mean, if you just run Apache out of the box or IIS out of the box, it logs every visitor. That's just normal. I mean, I don't pay attention to the log. But if there's a problem you can go back and say, well, what was going on?

Steve: Yep, in fact on our privacy page I mention that I do not have logging because I feel it's part of what I want, the privacy I want GRC's visitors to have, and that if during like weird times I may turn it on for forensic purposes briefly to find out if something's wrong or what's going on. But in general - and then I delete them afterwards. But in general, I mean, I don't have logging on right now. I never do.

Leo: Excellent. You're a rare man, Mr. Steve Gibson. But we knew that for a long time. Colman Burke in San Francisco reminds us of the Heise Security Offline Update: Almost 10 episodes back, #124, your Fantastic Tip of the Week went to someone who clued you in to the Heise stuff, which I tried and found to be a godsend. Since that episode, though, you and Leo have several times referred to the pain of doing a Windows reinstall, in particular the repeated patching and rebooting that entails. Have you forgotten about Heise or found some reason not to use after praising it so highly? I've done a couple of XP reinstalls on various machines since learning about Heise and found it avoided the headaches you guys continue to grouse about, except for one trivial Windows update for the most recent patches that Heise didn't include. In my defense, I haven't done a reinstall since we've talked about it. But I definitely had forgotten about it. I probably wouldn't use it just because I forgot.

Steve: And Leo, I think mostly we just enjoy grousing about the 90-plus patches that XP now needs, even after Service Pack 2, and wondering where Service Pack 3 is. I did want to affirm for everyone that it is a really good system. What happens for me is, I'm not installing XP often enough, and normally I'm never really planning to do it, that it's worth going through all the trouble. Also, I've got so many machines around here, I'm never doing it on, like, my main machine. So I don't mind really if it just sits over there and sucks things down and grinds along and does whatever it's going to do and does reboots and things. So for somebody who is in the XP reinstall business, oh my goodness, this thing really makes sense.

And again I'll remind people, you can find it just by Googling the phrase "offline-update." If you Google "offline-update," the first few links that come up, definitely the first link at the moment, will be the page that will take you to these guys. And, I mean, it is absolutely terrific. And I wanted to bring this up again to say that I've had a bunch of positive feedback from people who we turned onto this 10 episodes ago and who are saying, oh, this thing really works. I mean, they've looked at the scripts, the way it builds these ISOs, and they've been very, very impressed with it. So I wanted to remind people about it. It will be less critical once SP3 comes out for Windows XP. Speaking of which, Leo, I just saw something today earlier about Microsoft getting ready to end XP.

Leo: Well, they have said for a long time that June 30th they would stop selling it.

Steve: Oh, okay.

Leo: And there's been quite a bit of protesting about that. I don't know what the latest is. I'll have to look real quickly and see. But they've been planning on phasing that out. And they don't - they want you to buy Vista. And you know, to be honest, it makes sense to

buy Vista. It's just - if it's on a new machine it makes sense. I guess...

Steve: It doesn't make sense yet, Leo. It needs another three or four years. They just broke it with Service Pack 1. Just the Service Pack 1 broke a whole bunch of things. It's like, oh, this is really not ready yet.

Leo: Well, you know, I try to stay away from Windows whenever I can. And frankly, that's one of the reasons. It's old, and it's showing its age.

Steve: You know that I run Skype on my little Mac. And I turn it on once a week to talk with you. And I was doing it today, and I was sort of browsing. I thought, oh, I haven't updated Skype for a while, so I checked, and oh, I was way behind, so I updated Skype. And I just sort of felt peaceful. Like oh, this is just sort of peaceful to use a Mac. You're not, like, holding onto the edge of your desk thinking, oh, what could happen.

Leo: Oh, my God. Windows 2000 was like that. It was a peaceful operating system.

Steve: I'm looking at Windows 2000 right now, Leo.

Leo: It just works and works and works. I think really, if I could say anything to Microsoft, I would say just keep something like - probably Windows 2000 would be the best choice. Just keep that around. Offer it for 100 bucks, 50 bucks. Just say we'll keep it up to date, we'll keep it patched, it's not going to be high priority, you're not going to see any new features. But just for people who want a solid, non-changing, and secure operating system, we'd like to just give you that. Kind of Windows Light or something, or Windows Business or something. I don't know why they don't do that.

Steve: Well, because, as you say, ultimately - okay. In fairness to them, Windows has got so many problems that keeping it current is a full-time job. I mean, you know, somebody...

Leo: You would say, look, this isn't going to run anything past 2000. It's for those of you who are still running all your old software and are not planning to upgrade. But the problem is they no longer ship patches.

Steve: Well, exactly. And unfortunately it still needs them because they've got so much legacy code that they're still finding problems in that they would have to - and again, in fairness to Microsoft, having that many versions all in different states, I mean, I don't know how they do it as it is. I mean, it is such a huge task that they have. But it's a problem that they brought on themselves, of course, by needing all those patches.

Leo: It's difficult. That's why I think in the long run for a lot of users a UNIX system is probably a very good idea. But it's not good for novice users. But then is Windows good for novice users anymore? I don't know.

Steve: Well, and Mac, I guess Apple really took some heat for this most recent Mac OS upgrade. A lot of people thinking I don't know what I paid my money for.

Leo: As with I guess anybody, they're moving away from simplicity. And the idea of a - that's what I'm saying is we need a simple kind of no-frills operating system for people who just want to surf, get email. And the Mac has got, you know, as always happens with age, it accretes more and more features, more bells and whistles, and that means more bugs. And the only reason Windows is worse right now is because it's older. OS X in 10 years is going to be the same creaky machine Windows is and will need to - at some point you have to cut it off and say we're going to start completely from scratch. Let's see, Martin in Calgary, Alberta, Canada needs the magic password.

Steve: Oh, you're not going to believe this one, Leo.

Leo: What is the one - what's Pee-wee's magic password? He says: Hi, Steve. I recently bought a new Toshiba laptop. It came with a 200GB Toshiba hard drive. During last weekend my kids played with the laptop, created a system and a hard drive password using the BIOS. They can't remember it. In order to reset the BIOS password, I knew how to do it, so I removed the battery from the motherboard and put it back. Bingo. Well, that's good he can get his BIOS. However, the hard drive password, still there. In order to use the new laptop I pulled the 20GB hard drive from my fried Xbox 360, put it into the laptop. The partitions were a little weird, but it worked. Now, how can I reset the password on the hard drive? There's no jumper or nothin'. He's got one of those new hardware encryption drives; right?

Steve: Well, no. He probably - it may just be...

Leo: Or used that IDE lock?

Steve: Yeah. I mean, the ATAPI spec has had a password facility which many laptops BIOSes know about. This is the so-called hard drive password. It's not encrypted, it's just locked. And here's the bad news. There's no way to unlock it. There is no...

Leo: Really?

Steve: No. There's no jumper. Now, the only thing you could do is if you had, literally, a subpoena, or you were the NSA or government clearance or something, Toshiba certainly has the ability at the factory to remove the password because it's just a password that the drive has on it that you would need somehow to remove. The problem is, the spec, the ATA password management spec does have a way to remove the password from the drive. The only way it will agree to do so is if it first wipes the drive. So you are able to force the removal of the password at the cost of all the drive's data. Which really makes sense. I mean, that's a secure solution. So it doesn't - you're not just having to throw the drive out the window and say, well, my kids put a password on the drive that they no longer - you've got to keep your kids away from the BIOS, I think, in your laptop in the future. But so you are able to prevent completely scrapping the drive. But you'd have to have a utility - perhaps Toshiba makes it, I'm not even aware of one that's wandering around - that gives you the option of doing this, of removing the password at the cost of wiping the drive. But all drives will unlock themselves under command after they have successfully wiped their entire contents clean. But there is no jumper.

Leo: At least you can use your computer again. And he says he just bought it, so maybe

he doesn't have a lot of data on it.

Steve: That sounds likely. Although I don't know where I would tell him to go get such a utility. I mean, I could write one, but I never have. It must be out there somewhere.

Leo: What if it were one of those new hardware-encrypted drives? Would there be any recourse?

Steve: No, because the drive would not have the password. But I'm sure you could do the same thing. There is the same facility of saying unlock the drive, just wipe yourself first.

Leo: Rene Knigge - which sounds like a Peter Sellers name - is at NATO HQ in the Netherlands, so I'm not going to make fun of him anymore, has solved the unshredding problem: I heard you guys mention the deal with shredders and scanners plus computers being able to put Humpty-Dumpty back together again. We talked about the fact that there are machines that will reassemble crosscut-shredded documents automatically. At NATO HQ here in the Netherlands our papers get shredded, as well. But in the same machine, water is added - oh, what a good idea.

Steve: Isn't that neat?

Leo: Creating, yeah, an irreversible and definitely unscannable pulp. Just add water, you should be good. And then you can make papier-mch animals afterwards.

Steve: So I just loved that. It's like, okay, the shredder machines have been upgraded to compensate for this problem. They now have a water reservoir. And so you shred the paper, and it turns it into pulp.

Leo: Wow.

Steve: Like this big goo pile at the bottom of the...

Leo: Magical. That's very cool. All right. You ready for the last question?

Steve: Or the segue question.

Leo: Brian W. in Montreal: Computer World Magazine just published a lengthy article reviewing several "secure" USB drives from major vendors. Most of what they said has already been covered better on your podcast. But some of the security features and hoops these drives use are pretty funny in a sad sort of way, like this nugget: "Kingston refused to say what encryption mode the device runs in, citing that it was proprietary information." In the end, they came to the same conclusion as you and recommended IronKey, although they failed to point out you could do better than almost all of these devices just by using any old USB key and a free copy of TrueCrypt.

Steve: Right. It's funny, I took my car in for its, like, major service last week. And I literally have, I have a little 4GB - I actually think it is Kingston. Kingston has a cool little super-mini USB gizmo. It's got a little weird sort of slider on the outside. And immediately I thought, well, this isn't going to last long. And the detents wore down in about four days because of course I couldn't keep from sliding it back and forth.

Leo: You keep sliding it, don't you. I knew it. I have the same one on my keychain. It just gets...

Steve: Yeah, I know, it's just too fun to play with, you know? Anyway, so, and then the little slider cracked in half, and it's gone, leaving just a sort of a little exposed USB UI electrical interface on the front. But it doesn't matter, wasn't being hidden very well anyway by that thing. But the point is that I had to leave my keys with the service folks to have the car for the day. And I thought, wow, I mean, now I'm really glad that there is nothing on this in the clear. There is TrueCrypt.exe and TrueCrypt.sys and a file, can't remember what I called it, blob, I think, dot ct. And so there was no danger from turning my keys with this little USB dongle over to the techs. Because, you know, you have to think what a tasty thing for anyone to see is like a USB dongle on someone's keychain. It's like, wow, I can just plug it into my little laptop here and see if he's got any good files I need. So, you know, you definitely want that encrypted.

Leo: Absolutely, yeah.

Steve: And next week we will have the founder of IronKey as our guest to talk about his hardware's encryption solution and what makes it, he thinks, the best there is.

Leo: Well, that'll be fun. We'll talk about IronKey and how it works and why it's a good idea, or not, on Security Now!. Steve, everybody knows that the place to go for great free software is GRC.com, including your new, updated Wizmo with a special turn off zero wireless config feature.

Steve: Yep, the new wanlock command.

Leo: Wanlock. You're good at naming stuff. Wanlock. You could have worked in advertising. SpinRite, wanlock, Wizmo.

Steve: DCOMbobulator.

Leo: DCOMbobulator, Shoot the Messenger, Unplug n' Pray, they're all there for free. And of course SpinRite, which is the world's greatest must-have disk maintenance and recovery utility, GRC.com. We also put 16KB versions of the show there. Steve gets transcripts made, which is really handy for people who want to follow along as they listen or want to share the information with others because we've heard you do that, as well. GRC.com. Now with the new script-free menuing system. Google Analytics included without charge.

Steve: I'm in the process of nailing down some loose ends from some research that I had done, actually it was the summer of '06. The menuing system was one. There's another new feature coming to GRC shortly which is going to be a blockbuster. I'm very excited about it, and it's going to be right up the alley of our Security Now! listeners. So we will certainly be doing an

episode about some major revelations that have been uncovered as a consequence of this research. And it'll be a new, basically a new feature, not unlike ShieldsUP!, which will greet people who come to GRC. So we'll be talking about it within a few weeks.

Leo: Excellent. Thank you, Steve Gibson.

Steve: Talk to you soon, Leo.

Leo: Bye bye.