SECURITY NOW!

Transcript of Episode #41

TrueCrypt

Description: This week Steve and Leo explain why they love "TrueCrypt," a fabulous, free, open source, on-the-fly storage encryption tool that is fast, flexible, super-well-engineered, feature packed, and able to provide advanced state-of-the-art encryption services for many applications.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-041.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-041-lq.mp3

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

This is Security Now! with Steve Gibson, Episode #41 for May 25, 2006: TrueCrypt. Security Now! is brought to you by Astaro, makers of the Astaro Security Gateway, on the web at www.astaro.com.

Steve seems to have hidden today. In fact, there's some plausible deniability that he was ever here. Ladies and gentlemen, it's time for Security Now! with Steve Gibson. And I'm making a joke because today we're going to cover our favorite encryption program.

Steve Gibson: It really is. It's like a bunch of guys over a long period of time who were not in a big hurry just worked out the most perfectly feature-packed, like, right set of things with no agenda. They were not trying to force anything on anyone. It's just, I mean, as I browse the manual, as I was doing this morning, preparing to sit down and sort of, like, fresh myself up on the whole thing, I just had this wonderful feeling, like, okay, this is what open source and the whole open source community can produce when it really works well.

Leo: So this is a traditional open source – we're talking about TrueCrypt. This is a traditional open source project.

Steve: Yes. It is...

Leo: There's not just one guy. It's a bunch of people working on it?

Steve: It's clearly a bunch of people. And you can feel the influence of a team, which is really what you want in an open source mode where, you know, people were using it and someone said, hey, what about this, and now it’s a feature.

Leo: Yeah, yeah.

Steve: And, I mean, it just – TrueCrypt is spelled T-r-u–e-C-r-y-p-t, and the site is www.truecrypt.org. It is now running on Windows 2000 and XP. The very old version, only 1.0, ran on the 95/98/ME group of machines. And a lot of things have been fixed in it since then. So you really shouldn’t be using it on a really old machine. But it runs on the newer Windows platforms. It’s now running on the 64-bit platforms under Windows. And they ’ve got it running under Linux. In fact, all of the recent work has been in adding features to it over on the Linux side, although Windows has also benefited in some ways. And their plans are to also move it to OS X.

Leo: Wow. That’s great. Great news. Now, when you’re talking about encryption software, it seems to me – and I’d like you to let me know what you think – that open source is really the only way to go. It’s the only way to be sure there’s no backdoor, that it works as advertised, that it actually uses those algorithms properly. You almost have to go open source, don’t you?

Steve: I agree. I mean, for this kind of project, the last thing you would want to do would be to download something from whitehouse.gov.

Leo: Or nsa.com.

Steve: Or NSA. Trust us.

Leo: But of course now we know they have a huge influence with private industry, as well, so SBC or Verizon.

Steve: Exactly.

Leo: I mean, frankly, I think it’s safe to assume that any commercial enterprise in the United States, large commercial enterprise in the United States, any encryption it offers may well have a backdoor.

Steve: Well, and the beauty is, there is nothing this is missing. Not only is it all open source, but I guess the point is that there’s no reason that you need anything more than this. This is open source. This is using well-proven, academically-pounded-on encryption algorithms, exactly like the stuff we were talking about in our crypto series. I mean, here’s just a beautiful application of those concepts that, I mean, there wouldn’t be – I can’t imagine a reason to go buy something from Symantec or – not that they have anything like this. But, I mean, this is like – this is done now. This problem has been...

Leo: This gets the job done.

Steve: This has been solved.

Leo: So tell me a little bit about how it works and what you can do with it.

Steve: Yeah, let's talk about what TrueCrypt is. The idea is, it is for storing powerfully encrypted data on computer media. Typically, for example – this came up in last week's Q&A. We had – one person asked – I think the name was Kim. I don't know if that was him or her. But Kim asked – he or she had a corporate laptop and was worried about the laptop being stolen and was wondering what about BIOS passwords and hard drive locking and so forth. The problem is that even a locked hard drive can be unlocked by the drive's manufacturer. The drive's contents, even when the drive is locked, is not encrypted. You know, the Xbox was, I think, the first commercial place, other than the IBM ThinkPads, that we saw drives being locked and the fact that it's possible to get around that in various ways. So what you really want is the data that you care to protect to be powerfully encrypted.

What TrueCrypt is, and what makes it special, is that it's an on-the-fly disk encryption system. It installs a device driver into your OS which basically creates a virtual drive out of either a source file or a source partition. So, for example, you then have a drive where anything you write to the drive, as it goes into the drive through this TrueCrypt device driver, uses state-of-the-art, symmetric, very fast encryption to turn that data into noise. It is never not encrypted when it's on the drive. So there's no way that anything can, like, catch it part way done or not finished or, you know, like where you walk away from your computer and you forgot to encrypt whatever it was you just did. Everything ever written to a TrueCrypt volume is always encrypted. And then, of course, this process is reversed in the other direction. Anything you read from it is, again, symmetrically decrypted and returned back into the clear. So from your computer's standpoint, you're just looking at a drive letter. And you can't tell that it's an encrypted volume. It's just, you know, it looks to your computer like any other drive.

And, in fact, I'll give you an example of how I myself use this. I created a TrueCrypt volume that is a little bit smaller than a CD. So, for example – or a CD-R. A CD-R can store 700MB. So my TrueCrypt volume is 680MB. So what I have is I have a file on my system which is a TrueCrypt volume. And I actually have it, you know, in my Windows directory. It could be anywhere.

Leo: It's a visible file.

Steve: It's a visible file. And whenever I start my system, there's all kinds of autorun and autostart things. You're able to, like, permanently mount volumes to require passwords, to make them optional, to make them required the first time but then TrueCrypt can be asked to cache them so when you try to remount the volume, it'll try mounting the volume with all the passwords it's seen. And in case any of them work, then it mounts. I mean, again, it's got so many features that sort of just give you this feeling that this is a really mature solution. This is, you know, a lot of the stuff that you find on SourceForge and is open source is just kind of like, it's still at v0.0296 or something, you know, and it feels like they're not ready yet to call it 1.0. Well, this is currently v4.1 And, I mean, it feels that way.

So anyway, in my application I've created sort of a virtual CD volume, that is, I've created – I have a file which is 680MB in size. TrueCrypt mounts it as a drive letter. Anytime I want to store stuff archivally that I want, like, an extra copy of, I just store it on that drive. Well, over time, of course, it fills up. The stuff I'm storing is not big. I'm not needing to archive, you know, huge stuff. Mostly it's source code. So what I'm doing is I'm maintaining a source code archive of the things I work on, the projects I have that I absolutely want to make sure I don't lose, but I also don't want to lose control of that code.

So finally this thing fills up. And from time to time I'm checking to see how full it is. Well, what I end up with is a TrueCrypt volume, where that file which is living on my main drive, on my C drive, is seen by TrueCrypt as a drive letter. It's actually still just a file, but it's a file of noise. I mean, because it is encrypted there is no value to it unless you know what the password is that decrypts it. So what I do is, I then burn that to a couple CD-Rs. And I send one to my attorney, and I send one home to Mom.

Leo: It's half and half. Is it the same file on two, or is it...

Steve: No, they are redundant copies.

Leo: Oh, okay.

Steve: Because...

Leo: I thought you might be splitting it in half and making it really hard to figure out.

Steve: No. Well, because I wouldn't want anything – so the idea is that...

Leo: You have multiple copies. Yeah.

Steve: I have multiple copies.

Leo: Yeah.

Steve: They're in geographically different locations.

Leo: Right.

Steve: And I don't have to worry about, you know, Mom sticking it in her CD player by mistake or leaving it on the coffee table or...

Leo: Because your attorney has a copy.

Steve: Well, because it is a TrueCrypt volume burned on a CD, it is absolutely useless...

Leo: It's noise.

Steve: It is noise. I mean, as we know from...

Leo: Now, here's a question.

Steve: ...our talking about cryptography.

Leo: Do you give the attorney and your mom the passkey or not?

Steve: No.

Leo: They can't use it. They can't look at it.

Steve: It's of no use to them. From their standpoint it's just an opaque disk that they're saving for me...

Leo: That's nice.

Steve: ...in case I ever need, for whatever reason, to come and get it from them or ask them to send it back to me. So it's remote, it is absolutely secure, and I don't have to at all worry about anyone getting their hands on it. It's only of value to me when I then apply my password.

So let's talk a little bit more about TrueCrypt and some of the features. First of all, one of the nicest ways, sort of convenient ways, is to create a file container, that is, a file of a certain size which contains the volume. It's just nice because you can create them on the fly. You can create ad hoc TrueCrypt volumes out of files, store stuff in there, and do whatever you want to with them. The other reason that's nice is that it supports its use on a USB key. So, for example, you would create a USB key. You would create probably one large file that is not using the entire key because you want to leave room for TrueCrypt itself. The TrueCrypt EXE is not super big. You're able to specify what features you want to include. And then the balance of the USB key is this one big file. Well, the advantage of that is that gives you portability, which TrueCrypt specifically supports in what they call "traveller mode," where all the various settings are kept on an XML file.

And here's another example of them doing things right. TrueCrypt never keeps any of its own settings in the registry. It deliberately keeps all of its settings in an XML file which is inherently portable and will be version compatible. So again, they've just done things right. They don't want to leave anything in the registry. They want you to have – throughout the design of this is this notion of plausible deniability that we'll talk about a little bit more in a second. But in traveller mode, you move the TrueCrypt program to a USB key, fill the rest with a large file which you then format as a TrueCrypt volume. Now you've got the ability to carry a USB dongle around with you which you can stick into any machine you want. And, in fact, the traveller mode creates an autorun.inf file on the root of that. And it'll also do the same thing for a self-running CD if you want to use CDs in this way. So that you stick this in. It'll run TrueCrypt; mount your TrueCrypt volume as a drive letter; and then, of course, prompt you for your secret password, which you need to supply in order to unlock it, presuming – and I imagine you would – want to require human intervention. But again, all of these things are user configurable.

Leo: Sometimes for convenience people make it so that it automatically logs in when they log into Windows, kind of like the Windows encryption. But that does seem a little bit less secure. It is certainly more convenient. So you'd recommend having it ask for a password, a separate passphrase each time.

Steve: Well, again, I think it's really a function of how you're using it and what you're doing this for. But I think most people would require that. And here again we come back to our discussion of passwords because a strong password is required. TrueCrypt, in standard, you know, good crypto mode, allows you to use completely random gibberish of up to 64 characters. So, for example, going to my passwords page at GRC is a perfect way to get a super strong password that you would use and store somewhere.

Now, I mean, again, there's so much to talk about here because, for example, not only does TrueCrypt base your password on what you give it, but you can even use other files as password material. That is...

Leo: Oh.

Steve: For example, you might have an MP3 sitting in your media directory of Windows. Well, TrueCrypt knows that that's a file which is providing keying material.

Leo: Wow.

Steve: And so it uses – basically it creates a fingerprint of the file. It hashes the file to create some password material, which it then merges with what you provide. So it's not even just like – oh, and this can be multiple files in whatever order you want. It never writes to them; it only reads to them. There is no way for anyone who analyzes your volume to determine what it is that you're using as seed material. So even if someone had a password, unless they knew which files you also had tied the decryption to, even then the password would be useless to them.

Leo: But don't lose those files. You could be in trouble.

Steve: Oh, absolutely. You would be in serious trouble.

Leo: There's no way of reversing this in any way. So there's no backdoor. If you lose the password, you lose the files. You've lost the data.

Steve: That's exactly right. Now, there are some things they've done. The way to think of these TrueCrypt volumes is that there's a master key which encrypts the entire volume. That master key is stored in a header, but at no point does anything look anything different from noise. That is, these guys have gone nuts in terms of plausible deniability, so that there's nothing stored in a TrueCrypt volume file or a TrueCrypt partition that doesn't look like purely random data. There's, like, no – you know how most file headers will talk about what type of file they are, and you can tell by looking at the header what the rest of it is. There's nothing like that here. And in fact...

Leo: Would you want to not use a – I mean, a file's kind of a flag that here's some secret stuff. If you used the partition, it could look like an empty partition, right, just an unused partition?

Steve: Yes, it would look like an unused partition. Although, you know, you could bury the file somewhere and name it something that looks – I mean, you could name your TrueCrypt volume BestofSecurityNow.mp3.

Leo: Yeah, but if somebody looked at it and realized it wasn't, they might then – the reason I ask is because – and we talked about this on TWiT. The British government is now proposing that, if they demand of a criminal or a suspect in a criminal investigation that he decrypt it or give you the password, and if he doesn't, you go to jail, They're proposing that that be implemented in Britain. And I imagine the U.S. and other countries will try such a thing. If they know it's – they say, well, look, here's some data, it must be secret. But if they look at a partition, and it just looks like an empty partition, they're not even going to know to ask for a password; right?

Steve: Well, believe it or not, the TrueCrypt guys even have that covered.

Leo: I'm not surprised.

Steve: Yeah, I mean, it's just so well done. What they have is they have the notion of a hidden partition within a TrueCrypt volume. So you're able to take a TrueCrypt volume and only use half of it.

Leo: And maybe put some real data in the half, you know, just like your grocery list.

Steve: No, you would want to have something that looked like stuff you wouldn't want someone to have.

Leo: Ah, yes.

Steve: Thus the reason...

Leo: Why it's encrypted.

Steve: ...for looking like you had encrypted it.

Leo: Right.

Steve: But the fact is, you're able to have another encrypted volume using the unused space of the main one. And once again, there is no way to prove that the unused space does contain another encrypted volume because TrueCrypt always fills the entire volume with random data when it formats it. So the...

Leo: So clever. That is so clever.

Steve: Oh, it's just, I mean, just from one end to the other, these guys have thought of everything. So your entire TrueCrypt volume is filled with random data. And as we know, strongly encrypted data is indecipherable – which is probably the wrong choice of words in this case – from random data. It looks exactly the same as random data. So if someone came to you and said, you know, we know you have encrypted data on this computer, we demand you give us your key – so you hem and haw and, you know, put up a good fight and then give it to them. What they get when they decrypt it is something that makes them think, oh, well, maybe we got the wrong guy here. Or, I mean, I don't want to sound like we're encrypting criminal...

Leo: Would not encourage criminals, but the whole...

Steve: No.

Leo: ...point of this is, if you are a freedom fighter, if you're not a criminal, but let's say the government decides it doesn't like you for whatever reason, by refusing to decrypt whatever that data is, they can throw you in jail. And so...

Steve: Or maybe your ex-wife's attorneys don't like you that much.

Leo: So this way you have more than plausible deniability. You can be cooperative and say...

Steve: Exactly.

Leo: ...oh, yes, it's all my Social Security numbers in there, and please, feel free.

Steve: You know, I'm a fanatic about keeping my phone bills, you know, just like the NSA. So I keep mine...

Leo: Well, you have to forgive us for being a little bit paranoid. But there is perhaps cause for paranoia. And, you know, if you talk about the right to bear arms, I think there should be a right to bear encryption. And it's part of the right to privacy, and that's all we're talking about.

Steve: And so the beauty of this approach is you're able to divulge the information, let the authorities have the data, yet still within that same container have a secondary encrypted volume that uses a different password and is, again, completely secure.

Leo: Wow. I mean, that's really amazing.

Steve: They really did a great job. Now, with the newest version you don't have to pre-assign the maximum size of a file-based volume. It is able to grow dynamically using something that the NTFS file system calls "sparse files," where you're able to sort of like pre-allocate a large container, but it doesn't actually use space on your disk until you actually require it, which is a new feature that TrueCrypt is now supporting. I ought to mention, though, that if anyone wants to, like, try the CD archiving approach, which I love, you do need to use a FAT 32 container, not an NTFS container, because if you ever wanted to mount one of those CDs, Windows will not mount an NTFS file on read-only media. It'll only mount a FAT 32 file on read-only media. But of course, since the thing's only going to be 680MB anyway, FAT 32 is fine for that.
And then...

Leo: Right. And there's no limit for sizes on drives. It's just the limit would be on CDs.

Steve: Exactly, if you were wanting to spool it out there. And you could also instead go to DVD format instead of CD, I mean, if you really wanted to store, you know, 4.7GB per disk of encrypted stuff and you had that much that you really needed to encrypt. And there again you need to use the UDF format when you burn this to DVD because you'll end up with a 2GB file size limit otherwise. So that's something to keep in mind.

But in terms of features, you might be concerned, okay, I've got my TrueCrypt volume mounted, and I'm using my computer. And for whatever reason, somebody approaches me in a coffee shop, you know, the boss at work, your kids, I mean, who knows, whatever the situation is. The presumption is that you want to be able to close that quickly. All the technology is there to do that. If you don't use it for a certain amount of time, it will auto-dismount the drive so that it is then – it typically would require a password in order to regain access. So, for example, you could just, if it's something you wanted to make sure stayed secure, you could just say, I only want this to remain available for two minutes. Which, of course, would be an inconvenience if it were something you were using all the time. But it would be a lifesaving thing or a crypto-saving thing if it were something you just needed access to from time to time, but you worried you might forget to dismount it.

Leo: Mm-hmm.

Steve: Similarly, when you log out, you can have TrueCrypt dismount the volumes. When your screensaver kicks in, so that, you know, you're at work, and you get up from your desk, screensaver kicks in. Or, for example, you could use my little Wizmo utility to start the screensaver on a single button click, and that automatically dismounts any TrueCrypt volumes that you have said you want dismounted at that time.

Leo: This is a particularly good idea, I think, for those of us who use laptops, to TrueCrypt our data drives on the laptop, because laptops get stolen.

Steve: Well, that was exactly the advice that I gave to our questioner last week...

Leo: Oh, yeah, that's right, yeah.

Steve: ...was, for example, set up a laptop – now, one thing TrueCrypt cannot do is it cannot encrypt an existing partition. There actually are very good security reasons for it refusing to do so. Because having a snapshot of the partition before encryption and after encryption could give a crypto analyst a lot of material. So TrueCrypt refuses to encrypt an existing partition. If you wanted to do this, for example, you would have to back up the partition to some other drive, basically move that data off of your laptop. You'd want to make sure you really had it safely off, you know, maybe burn a couple copies of DVD, or just move it to another drive and make sure you've got it safe. Then you would create from that existing partition, like your D partition – D for data – you would create a TrueCrypt volume in that which inherently, as we said, fills it with random data. Now it is ready to receive its contents.

So now you simply restore that backed up drive, that backed up content, over into the D drive, which is a TrueCrypt partition, and now you're good to go. You've got your C, which is, you know, a minimal size Windows, just enough to hold your apps and to boot. And then all the precious stuff that you care about – oh, and you are able to run applications from a TrueCrypt drive. It looks just like any other Windows drive. So you could install apps over there if you wanted to, or run things from there that you didn't want, for security reasons, to put over on your C drive. And it all works correctly.

Leo: You know, Windows XP Professional has similar kind of hard drive encryption built into it. Is there a reason to use TrueCrypt over XP Professional's built-in encryption?

Steve: I just feel more comfortable with this. I mean, I know what it is, the source code is there, it has features coming out its ears, the ability to, for example, put CD volumes and USB volumes. And for my way of thinking, you know, this is a nice multiplatform solution. Oh, and the volumes are transportable across OS versions.

Leo: Oh.

Steve: So, for example, so this is one thing, for example...

Leo: That's a good reason, yeah.

Steve: ...if you ever needed to move or to view something created under Windows, under OS X, once TrueCrypt supports OS X, or under Linux, you have that. And you don't have to worry about, you know, forward compatibility. They've just got that nailed.

Leo: There's another issue with Windows encryption that I come across a lot helping people. The way it works is it stores certificates into the encrypted directory, which people sometimes forget to copy. It's not enough merely to have the passphrase. You also need the certificate. It's kind of like that file hash system that TrueCrypt uses. And if you don't have the certificates, even if you know the password, you will not be able to decrypt that volume. And I think people frequently lose their data in Windows because they don't know about these certificates they have to copy, as well.

Steve: Well, yes. And you've just demonstrated that there is no plausible deniability...

Leo: Right, there's a certificate.

Steve: ...using Windows crypto in that sort of mode. You know, the world knows, anyone who cares to look at your machine, knows you've got an encrypted volume. You're not able to say, oh, no, that's just a bunch of junk...

Leo: No.

Steve: ...or it used to hold data, but now it doesn't anymore.

Leo: Right. Those certificates, I misspoke, are not stored in the encrypted volume but stored in the Windows directory, so...

Steve: Oh, okay.

Leo: Yeah, all you'd have to do is look in their Windows directory, and they can see the certificates and say, oh, hmm, I guess he's got something he's hiding.

Steve: Right.

Leo: Let's go see.

Steve: Right. So anyway, I encourage anyone who has, you know, a need for storing data, either on their own machine, in a laptop environment where there's a chance it could get stolen, and where you've got any kind of sensitive data, TrueCrypt – oh, it's got a – the EXE that you download has a beautiful user's manual. They have got – their manual is in web page form online. And I wasn't able to find a PDF on their site. But when you download the EXE and install TrueCrypt, it does bring with it a nice PDF. You know, print it out, sit down, read through the manual once. You'll end up with a really secure, really useful tool for, you know, just any kind of application where – I mean, for example, you could even create a small TrueCrypt file, put a bunch of files in it, and mail them to someone. I mean, and again, you'd need to give them the password over a secure channel. But you could also use it for secure file transport or temporary storage on an FTP server or on a web server or wherever. I mean, you know, really it's so flexible. And again, that's one of the reasons I like it better than the solutions tied to Windows XP is that anything you can think of in the application space, you can apply TrueCrypt on.

Leo: Although I'd say because it's not public key crypto, it's not public/private key, it's probably not as good as, say, PGP for encrypting and emailing things or encrypting emails. But it's, you know, I mean, it's really for a different purpose.

Steve: Right. It's not something that is as convenient for, like, on-the-fly crypto. But if you wanted some way to store or archive or, again, even to send data, it's possible.

Now, one last thing I'll mention is that there is a header that I started to talk about in any TrueCrypt volume – although the header is not like we think of, as I was saying before, it's not something that you can see is a header. But think of it as private TrueCrypt header data. That contains the master key for the rest of the volume. And that's what you are decrypting when you provide the raw material files or your password.

Leo: Clever. So you only decrypt the header, and then the header decrypts the rest.

Steve: Exactly. And in fact, what's really cool is you're able to choose among many different algorithms. I mean, it's just a whole pile of hashing and crypto algorithms. And for people who are super security conscious, you can even chain algorithms, so use Blowfish followed by AES followed by Twofish or something. I mean, it's just, if you really wanted to go overboard, which is what I think that would be, you're able to do that.

Leo: I presume the defaults are acceptable.

Steve: I really think they are.

Leo: Yeah, okay.

Steve: I mean, which is – would just be to use AES. And it's also going to be faster that way. Again, there's going to be a speed versus overkill crypto tradeoff. But what's cool is that the system doesn't know what crypto format you chose. And one of the – I loved it. One of the questions in the FAQ is, why can't I choose whatever sequence of crypto I want? Why do I have to choose from among the list they provide? Well, the reason is, the way TrueCrypt determines the algorithm is by trying them all because it doesn't know. Nowhere does it – because if it stored it in the file, then you lose plausible deniability.

Leo: Right.

Steve: If it's stored anywhere. So what it does is, it takes the files you've provided it, if you used file-based keying or just your password. And it tries – it uses your password against all of the various flavors that it offers until one of them works.

Leo: I love it.

Steve: It's just beautiful. And finally, in a corporate mode, say for example – the question was asked last week about, you know, the sense I got was this person had lots of employees who needed by their job to store sensitive corporate data or client data on their laptops. There's a problem if corporate IT set up the D drive, you know, the encrypted partition or drive, with an existing set of keys, and then the employee were to change the key and forget it, because there is no backdoor. There is no way – if you lose this key, you are seriously hosed. So anyway, what's very cool is even that's been considered. Once you set up a partition, you're able to back up the header. That is, you can separately store – it's like about a 1K file. You back up the header and store it somewhere safe. Then the employee could come along and change their password...

Leo: Oh, this is great.

Steve: ...but you are never able to change the master key or the crypto used because once that's been laid down the entire partition is encrypted that way.

Leo: So it's almost like having a PKI. You now have a second key that will always work.

Steve: Exactly. If the employee forgot their key after changing it from what corporate IT set up...

Leo: I love this.

Steve: And of course, as we know, prudent security policy says you should change your keys from time to time. Or maybe, for example, you were at a client site, and they may have seen you enter your key to unlock your drive. In that case you certainly would want to change it afterwards. So the point is the user, separate from IT department, could be free to change it all the time. And if they ever forgot it, IT is able to restore the original header, which brings back with it the original password.

Leo: You've got a key storer, that's great.

Steve: And then you could hand it back to the employee and say, okay, now, don't forget it next time.

Leo: It's really impressive. I mean, this is really exactly what's needed. I'm thinking probably a good thing for me to do, even though I don't have any application for it right now, would be to take one of my many USB keys and make it a TrueCrypt volume and just have it lying around in case I ever needed to put something on there.

Steve: Yeah. I mean, for people who are security conscious, this problem is solved. I mean, many people wonder about how to carry dongles, you know, USB keys around that are going to be secure. What if someone, you know, if they left it behind or forgot it? TrueCrypt's traveller mode does that. For any kind of long-term archiving, which is what I use it for, you know, I absolutely want to keep long-term archives. I need them to be physically removed, you know, in case my office burned down or I was burglared or something happened. So I need to physically move them somewhere, yet I don't want to lose control of the security of that. TrueCrypt does this for you. I mean, what I like about it is that it's a toolkit that you can apply in just all kinds of different ways.

Leo: Very slick. Very slick. Speaking of great toolkits, I want to thank Astaro for supporting the show and providing a great security toolkit for people who have to protect themselves online, the Astaro Security Gateway, Astaro.com. Really useful. Free distribution for home users, and for corporate there's hardware, as well. It's a really great way to protect yourself.

I also want to say that the gateway offers easy migration for Novell BorderManager users. Lot of folks still using it, particularly, I think, in universities. ASG v6.2 features a new single sign-on capability for eDirectory clients, an eDirectory browser, and a generic proxy server. So you're not stuck. Check out Astaro's BorderManager migration Wiki at Astaro.com/bordermanager.

And of course, if you have hard drive problems, there's no better place to go than GRC.com for SpinRite. SpinRite's the ultimate disk maintenance and recovery utility. You want to see some testimonials, SpinRite.info is a great place to go, SpinRite.info. I think everybody who has hard drives ought to have SpinRite. Just my personal feeling.

Steve: It helps. It helps so many people constantly, Leo.

Leo: Yeah.

Steve: I'm just glad to do it.

Leo: Yeah. Makes Steve feel good, too. And of course, if you head to GRC.com/securitynow.htm, you'll find transcripts of each and every show, thanks to Elaine; and a 16KB version for the bandwidth impaired; and show notes, as well. That's

GRC.com/securitynow.htm.

What are we going to talk about next week? Have we run out of topics?

Steve: Oh, no. Next week – you know, last week, in answering Q&A, we talked about Skype several times, and we were talking about that relay node and about how NAT routers sometimes need help to find each other. Next week we're going to talk about what it means to be peer-to-peer friendly, what is a peer-to-peer friendly NAT router, and what is the technology that allows two people, both behind NAT routers, to create a connection. Because traditionally that's been impossible. But that problem has been solved.

Leo: And not with Universal Plug and Play, I might add.

Steve: Not by opening ports, exactly.

Leo: No, a safe way to do it. That's next week. Every Thursday, another great episode of Security Now! with Steve Gibson. We're glad you joined us this week, and we'll see you next time on Security Now!.