RUNAS RADIO

http://www.runasradio.com

RunAs Radio is a weekly Internet Audio Talk Show for IT Professionals working with Microsoft products. The full range of IT topics is covered from a Microsoft-centric viewpoint.

Text Transcript of Show #009
(Transcription services provided by PWOP Productions)

Eric Marvets Talks TrueCrypt
June 5, 2007

[Music Playing]

Carl Franklin: From runasradio.com, you're listening to RunAs Radio - The weekly Internet talk show for IT professionals with Richard Campbell and Greg Hughes. This is Carl Franklin, introducing Show #9, with guest Eric Marvets, recorded Friday June 1st, 2007. RunAs Radio is produced each week by Pwop Productions - Offering professional media and Podcasting services, online at pwop.com.

Richard Campbell: Hi, you are listening to RunAs Radio and this is Richard Campbell and with me as usual, Greg Hughes.

Greg Hughes: Hello Richard, how are you doing?

Richard Campbell: I am enjoying the fine technology of radio, because right now, we are at TechEd.

Greg Hughes: That's right.

Richard Campbell: In fact, we have been working with Pwop with Carl Franklin and all the other guys at Pwop to put together quite a show at TechEd. We are working with the Virtual TechEd folks, and at the Virtual TechEd stage, down in the main hall. So, that's us, we are there all the time, we have been doing all sorts of things, putting together some panels, we have even been shooting some video. Of course, I am talking about stuff I haven't actually done yet.

Greg Hughes: Because we recorded this a little bit ahead of time, but I am confident that it's beautiful sunny Orlando, Florida, and that we are doing what everybody does when they go to Orlando.

Richard Campbell: Staying inside.

Greg Hughes: Go to a great big building with air conditioning.

Richard Campbell: That's right, we are staying inside, it's hot out there, stay inside. If you are at TechEd, please come down to the Virtual TechEd stage, come and visit us, we'd love to talk to you.

Greg Hughes: Yeah, it would be great to see you and find out what you think and just geek out for a little while and have a little bit of fun. It's a fun time, TechEd is always a great show and looking forward to seeing people down there at the Virtual TechEd booth.

Richard Campbell: All right Greg, I got an email.

Greg Hughes: Yes.

Richard Campbell: This one says, "Hi Richard and Greg, I just finished listening to show #8, with Brian Komar, which I found very interesting."

Greg Hughes: Yes, it was.

Richard Campbell: It was a lot of fun, Brian is a gas. "I can't believe how much you can fit into a half hour show and yet I can only imagine how much more there is to cover on this subject. Once again a brilliant show".

Greg Hughes: Well, thanks for thinking so. I am always surprised at how much we fit into half an hour as well.

Richard Campbell: But I always feel like I've left two or three shows on the floor at the end of every show.

Greg Hughes: That's a good thing, because it gives us the reason to call people back and to say, "Hey, let's come back and talk about this again."

Richard Campbell: I did not expect Public Key Infrastructure to be quite as interesting as you guys made it, and I say you guys meaning, Greg and Brian, because I was faking it through that show.

Greg Hughes: Well, we each have our own little areas of interest and focus, don't we?

Richard Campbell: Yeah, two security professionals walk into a room, fill in gag line here. Let me read the rest of this email.

Greg Hughes: Sure.

Richard Campbell: "At the start of the show, you mentioned 'Backup to disk', which brought a smile to my face", and that was another email of somebody else saying, "Talk about Backup to Disk some more."

Greg Hughes: That's right.

Richard Campbell: "I'd really like to hear some experts talk about this subject." Do you hear, a theme here Greg? How many times have we been asked to do 'Backup to Disk' as a show?

Greg Hughes: You know it's a low cost -- I mean, they say disk space is cheap.

Richard Campbell: It is.

Greg Hughes: In the grand scheme of things, there's two things that tend an application

environment to be cheap, sorry to interrupt your email here, but you know one of those is disk and the other one is Ram. If you have got performance problems, RAM is cheap insurance, disk is cheap insurance.

Richard Campbell: Absolutely.

Greg Hughes: You know, the reason it's really popular and there's so much interest, reliability, the fact of the matter is that the old school way of doing tapes, it just don't cut it, so much no more.

Richard Campbell: I find tapes unreliable, but you know the biggest thing is, I have got a drive, doesn't matter what computer I walk up to, I can plug it in. I have a tape, I found tapes where they didn't work between the same model drive, because they had different Firmware on it.

Greg Hughes: Well, I can tell you one thing, and that is you're absolutely right, and I can tell you another thing and that is that when it really works really, really well, and when you can truly take a drive and plug it into any machine, then well, you have to start thinking about, "Wow, that's awfully easy access to the data, what do I need to do to protect it?"

Richard Campbell: Right, yeah you are going the other way. And gee, isn't that this week's show?

Greg Hughes: Actually, I think it is.

Richard Campbell: Yes, it is, but a nice setup you did there Greg.

Greg Hughes: I did not mean to.

Richard Campbell: Let me finish this email, "I work for a small company of seven people where I am the IT team". It has happened to me too man, don't worry about it.

(00:04:56)

Greg Hughes: Yeah, that's our target audience -- it's a tough, tough job, there is a lot of heroes out there that make amazing things happen and really work magic and kudos to all of you. I have been there and done that before, and it's hard work.

Richard Campbell: Look at the list of things this guy has to do, "I look after the network, Microsoft SQL, Microsoft Exchange" here is a life terror right there, "and user account management. I also do development of the company website and all of the internal desktop applications. The programming side of things is the major part of my job, but all the other ones are just as important."

Greg Hughes: Well, it sounds like they need to buy some more software for that guy to use.

Richard Campbell: He is obviously not managing enough equipment yet.

Greg Hughes: Yeah that sounds like quite the workload and it also sounds like, it's probably an awful lot of fun.

Richard Campbell: Yeah, I hope so. "When it comes to backup, we are using tapes, but I would much rather move to something like an external disk for nightly backups. I would also like the ability of taking the backups offsite, even when it is just the weekly one. At this stage, I backup about 10 to 15 gigabytes of data, easily fitting on a single tape, so I do a full backup each night. I would love to hear some suggestions for my kind of scenario, keep the great shows coming, regards, Philip."

Greg Hughes: Yeah, that's terrific. Philip, I think that we really intend to address more backup options in the future shows. The only thing that I would caution people against is taking their backups home and sticking them in their garage or even worse, leaving them in the car.

Richard Campbell: Yeah, don't leave it in the car.

Greg Hughes: When it comes to doing offsite backups, there is a real security risk associated with doing that. So, the companies that I have worked for, we utilize a professional offsite Vault and organization that does that for us with armored cars and there is a reason that we do that, especially in our financial services business and banking, is that the sensitivity of that data can be very, very critical, but even where it's employee records and stuff from your QuickBooks or other accounting system that you are running for the small business, if you have that data on a laptop or on a backup drive or whatever, you leave it sitting in the car or you leave it sitting in your house, that kind of thing, just keep in mind that there is risks associated with that.

Richard Campbell: Yeah, I think it's well worth paying for a service for that, it just takes that issue off the table.

Greg Hughes: There is a probably a size of business and a size of revenue, that makes that more possible than otherwise, but one thing that I found is a lot of small businesses don't really look into it enough to find out how inexpensive it can

be, to leverage an offside tape or other media, they will even do CD's and paper for you, if you ask them to. Type of a company that can really give you an awful lot of peace of mind, we talk about cheap insurance, there are ways to do that using these companies and it's probably worth looking into.

Richard Campbell: Way less money than your premium for your errors and omissions insurance, I am sure of that.

Greg Hughes: Considerably less I think in most cases, and you know what, that's a good segway as you mentioned into our topic for the show today.

Richard Campbell: All right Greg, let's introduce our guest. Eric Marvets is a Developer Security MVP and the consulting services manager with Mark Dunn's group, DUNN Training and Consulting. Of course, Mark Dunn -- definitely a friend of the show, and his specialty is encryption. Eric is passionate about spreading best practices to the developer community, he can often be found delivering user group talks on security related subjects throughout the Southeast. He also maintains a blog and I shrinksterized the blog, so you go to shrinkster.com and type in pko, so shrinkster.com/pko will take you right to the Security Samurai blog, Eric's blog. So, welcome Eric.

Eric Marvets: Hi

Richard Campbell: So, here we are and I know we started out our conversation via email about laptop security and it sort of morphed into this external storage security in general, whether it be the hard drives in a laptop or just the loose hard drives that are USB or FireWire things like that and that kind of let us down the path of TrueCrypt, am I going in the right direction here?

Eric Marvets: Yeah, it's good for any type of mobile based computing where you have a laptop or you have a Thumb Stick that you carry between office and home. Anytime you have data that's going to be in a vulnerable or compromised state where an attacker could possibly get their hands on it, this will be good. It's not really designed for servers in the backroom, or anything of that nature.

Richard Campbell: Now, I am imagining they are not focused on performance near as much as reasonable security.

Eric Marvets: But they do have some performance options in there, which make it actually a little bit more configurable than GFS or BitLocker. You are right, it is not designed for performance, it's more for usability.

Richard Campbell: Alright so, what are we talking about when we talk about TrueCrypt, where does it come from and what does it do?

(00:09:57)

Eric Marvets: TrueCrypt has actually been around for a while, it used to be 'Encryption for the Masses' and then I think back in 2000 it was changed over, the developer of 'Encryption for the Masses,' he went to work for a private company and a new group took over and they named it TrueCrypt. It's quite interesting, because it works on both Windows and Linux and they are also working on a Mac version that hopefully will come out in the near future. It truly is portable, you can take a USB thumb stick with a TrueCrypt partition and use it in either a Windows or a Linux environment.

Richard Campbell: So, when you said partitioned, is it just a particular partition type then?

Eric Marvets: Well, there is two different types of volumes, TrueCrypt volumes, they both function the same, they have a volume header which will have the encryption key and every file in the volume will be encrypted with that single encryption key. So, if you look at other hard drive encryption utilities, they often use a single key per file, or just one key for all files, which really makes it quite interesting in the encryption mode, which I will talk about in just a second. You can have either an entire partition or a file. It looks and acts just like any other file that you would have on your hard drive, but it's actually a volume that can be mounted. TrueCrypt acts as a driver in the operating system and does the encryption on the fly, when you read or write to it. So, you would load up the TrueCrypt application, point to the file and say, "Mount this drive L," and you are off and running.

Greg Hughes: So, it's a mountable volume, can it grow in size dynamically, or you fixed a certain size, how does that work?

Eric Marvets: It does have a dynamic option, where you have to give it a maximum size limit, and as you add files to it, it will grow, it won't shrink and there is a couple of different problems with it, it's very poor as far performance goes and it also leaks information. For example, which sectors in the volume are in use, things like other volume options, like a fixed size or a partition would not do, so it's not the best way about doing things. It would be better to say, "I want to have a

file that's four gig in size, and mount it as a four gig drive. "

Richard Campbell: Now, I am thinking about things like, "Wow, I've got 32 gig Compact Flash Cards and things like that, that could have data on it. So, I want these things encrypted as well. All of that works, I just mount it as a volume on that drive?

Eric Marvets: Oh yeah, personally my laptop, I have a laptop which is ultra-portable. It's a little 3 pounds ThinkPad, I love it to death. As far as doing developer work, and stuff like that, I have a personal machine that's at home. My entire profile is on that, an 8 gig Flash Voyager GT drive. So, that entire drive is an encrypted TrueCrypt partition, when I get home, I plug it into my workstation, when I am on the road, I plug it into the laptop.

Richard Campbell: It's just a mountable volume. So, is it actually possible to build a bootable drive like this?

Eric Marvets: Yes it is, and I am not sure if you can do it on Windows, you can definitely load Linux, half of it. I don't think there is any way to do that with Windows.

Richard Campbell: So, the idea here is you are not trying to encrypt everything, you are not trying to encrypt the OS, you are just trying to encrypt the data, so put My Documents on a volume that is encrypted.

Eric Marvets: Right, so I mean if somebody were to take my laptop, I have a very -- I am not really worried about the strength of my password for the laptop, there is no data on the physical drive. This machine, I have an image of it at home, stored on another TrueCrypt partition, where if I suspect anything is going wrong with it, I wipe that hard drive in a second, and I know there is no files on there that I am going to be missing. Everything that is of any importance is on my Flash drive, which is securely protected.

Richard Campbell: I am getting at the idea here that what we are trying to resist is the relatively intelligent data feed, who isn't even going to try to start up your laptop after he steals it, he is just going to yank the drive out of it and plug it into something else and try and pump data out of it.

Eric Marvets: Yes, one of those mistakes people make with encryption I see a lot is that they think they have something valuable, so they want to protect it with encryption. You really have to start to think about what are my attack vectors, how is somebody going to get at me? For example, there are multiple different algorithms that you can use with TrueCrypt. AES Rijndael which uses a 256 bit key is by far the strongest, it's the one that the government uses, it's the DLB standard.

(00:15:00)

That works great, but if you want some more speed then you can use Serpent, Twofish, a couple of different other ones and TrueCrypt actually makes it very easy from a user standpoint, because it will show you how fast, your read and write times will be to the drive, what it thinks it will be, and you can push the test button and it will actually try to work with the drives, a Flash drive is going to be a lot slower than the SATA drive in your machine, but it will tell you, so you can get an idea of the performance.

Richard Campbell: And what the consequences of using 256-bit AES actually is.

Eric Marvets: Yes, if you are trying to protect it from the government or a computing corporation, then you'll probably going to go the AES route, if you are trying to protect your financial data from a identity theft, then you can use Twofish and be just fine.

Richard Campbell: Probably any one of those encryptions is going to do.

Eric Marvets: Yeah.

Richard Campbell: It's sort of more of a, what am I thinking of, I always used to sync the description of the club. Right, the thing you put in your car, doesn't make your car impossible to steal, it just makes it awkward enough to steal, they will steal somebody else's.

Eric Marvets: Exactly, It's a thousand times more secure than a shredder, you got to think what the attacker is going to -- how valuable is that data? Who the potential attackers are, and what do I need to use to prevent a particular threat from being realized? I do a lot of security projects, I deal a lot with people's Social Security numbers, I deal with you know -- I first got started working in the financial industry, I had access to just about everybody who lives in the US, who is social, that had a credit card. That type of information, I am definitely using the highest encryption standard I can.

Richard Campbell: You are willing to sacrifice performance, because the consequences of losing the data are so high.

Eric Marvets: Exactly, but I'll tell you one thing, trying to run Outlook when it starts filling it's indexing, on your data files, you are going to see

a little bit of a performance hit on a three pound ThinkPad.

Richard Campbell: A little bit huh?

Eric Marvets: A little bit, it's manageable, I have no…

Richard Campbell: So, it wasn't unusable, it was just noticeably slower.

Eric Marvets: Yeah, it's noticeably slower, you will be able to tell if something is running in the background, it's no less severe than an anti-virus program doing a full search of your hard disk systems, it's definitely no worse than that.

Greg Hughes: So, thinking about this from the stand point of the IT guy who's running or working in the IT department, recognizing that their data, security and preventing data leakage is really, really important. What does TrueCrypt offer the IT department and the IT worker in terms of managing this on behalf of their users, and what do you see as some of the low hanging fruit, where would a typical business IT department deploy this in order to solve the biggest problems?

Eric Marvets: The design of TrueCrypt makes it extremely advantageous over EFS or BitLocker or any other technology that's out there. First off is the fact that they can use a thumb drive or they can use -- thumb drives have bad filing systems, EFS doesn't work good, or they can use a file on the hard drive or if they have a partition, they can use a partition that's not being used on the hard drive. So, being able to select where that data is going to be, it is the first thing that makes it very advantageous. The second thing is, the volume header contains the encryption key that's used to encrypt all the files on the drive.

What detects that can do is when they setup the TrueCrypt partition, is they can use a single key for all users, install the partition and then backup the header, let the user use their own password and then they can go out and if they have put in a strong password, and if they lose their password, their data is not lost. They can bring it back in, the IT guy can restore the header over the previous one, which it overwrites 32 times, so the old header is really gone, that is one of the things, it doesn't have a secure delete, because it's encrypted data anyway, but it would overwrite a header to make sure that the old one is gone.

They use the same password they used to initially create the partition and they are up and running. The users do not have to be administrators to mount a drive, you have to be an administrator to install TrueCrypt, and you have to be an administrator to create a partition, but to mount it with a password, any user will have the ability to do that.

(00:20:00)

Greg Hughes: So, walk me through as a user, I have TrueCrypt, my IT department or I set it up on my system. What's the mechanism that I use to gain access to the data on my volume? Is it different for different volume types or is it safe to assume that if I log on to Windows or Linux, then I just click on a drive through a command line, just access a drive and it's magically there, or do I need to do some other things before I can do that?

Eric Marvets: The administrator, because TrueCrypt has command line arguments, you can create a batch file which will automatically mount the drives, and it will prompt the user to enter the passwords. So, as soon as somebody logs in to their machine, it will be able to load up, ask them for the password and boom, by time the operating system has finished welcoming the user to the experience, it's already going to be in their File Explorer. Which is really handy, because if you forget – I go to load Outlook and my data files are not there, and it will yell at me three or four times before it finally quits and says, "Okay, you don't have your L drive installed right now."

Richard Campbell: So, as far as Outlook is concerned, it's just a drive, it doesn't know anything about TrueCrypt.

Eric Marvets: Yes. The operating system and anything that runs on it has no idea that this is anything other than a normal drive, there is no hint it has, that anything else is going on.

Greg Hughes: What about password complexity requirements? Of course, a lot of -- especially with all the compliance requirements that a lot of IT organizations are forced to take into consideration these days in a good way, what does TrueCrypt offer? What can it do for me in terms of enforcing complexity requirements and making sure that I don't have a toothpick holding my Vault door shut?

Eric Marvets: There is a good part and bad part to that answer. The first thing is, there is no requirement. There is stern warning if you don't use a password, I think it's 96 bits of entropy, but you are talking a 20 character upper case, lower case -- you are talking about a very, very strong password.

Greg Hughes: Sure.

Eric Marvets: If you don't use something like that, it will give you a fairly strong warning. I personally feel like 76-bits of entropy, I don't know if you guys use Password Minder. Password Minder does a much better job of showing you how strong your password is going to be, this doesn't do as good of a job, it has a very black and white line.

Richard Campbell: And not really any level of enforcement per se.

Eric Marvets: Right.

Richard Campbell: The guy can ultimately click past these warnings and put in whatever password he wants.

Eric Marvets: It's been my experience that people don't quite understand password strength, and tools would do a good job to get them a little bit up the way there as far as saying you must have upper case, lower case in a particular length, but when they are using a phrase, they are using something that's easy to remember. You are not making it that much stronger, because dictionary attacks do use every possible – they'll take a common phrase and they use every possible combinations, upper case or lower case, substituting exclamation points for the letter I and that sort of thing. So, what I always tell users to do, get a good password, make it random, use something to generate your password for you, and then write it down and keep it in your wallet. If your wallet is stolen, then you know you need to change your password on your computer. If your computer is stolen, then your password is safely in your wallet. You don't store the two together, you don't put your wallet in your laptop bag and then leave that in the car.

Richard Campbell: Sticky notes stuck to the laptop with the password on it, not a good idea.

Eric Marvets: People think that writing the password down is bad, writing the password down and storing it with the other thing that it could be used with is bad. As long as you keep the two separated and you would be aware when one is missing versus the other, then you are not in that terrible of a spot.

Greg Hughes: Right, or writing it down on a posted note that you stick into your wallet, that says, "My TrueCrypt password for this laptop is blah," obviously. We can probably write it down on the piece of paper and know that that's what it's for, right?

Eric Marvets: I usually try and go, just to share my secret with the world, I usually try and go somewhere that I have been to on occasion and I might go to, I can always get back to a static surrounding, and I will use things from the environment there to randomly come up with a password. So, I will go down the hall to a friend of mine's office, I will walk in, I will look at his books on the bookshelf, and I will come up with a password, I will just pick a password out of those books, completely random. I could have walked into anybody's office, I am not using words, I am pulling pieces of text that I see in his room and putting it together in a password, plus how am I typing it enough times I will remember, if he adds another book to the bookshelf in six months, I am fine.

(00:25:02)

Richard Campbell: This is not about you remembering the password, it's about you creating a very random password.

Eric Marvets: Yes, and TrueCrypt also has another great thing which is the keyfile. You can use not only a password, but additionally a keyfile. So, let's say your TrueCrypt partition is on a hard drive, you can take and create a password, take a thumb stick with a file on it, and now you have three things that must come together for an attacker to decrypt your data.

Richard Campbell: So, what's in the keyfile?

Eric Marvets: The keyfile is any file you want, TrueCrypt will generate a keyfile for you, you can use a file from your hard drive, you can use a picture, you can use a Word document, you can use any file, and it will use it for everything.

Greg Hughes: So, kind of the multifactor approach, the something I know with the password, and the something I have with a keyfile.

Eric Marvets: Yes, and they would need all three at that point, the hard drive, the password and your keyfile in order to breach your security.

Richard Campbell: And obviously, it's in your best interest not to store the keyfile on the hard drive.

Eric Marvets: Yes, well you know, if you have got a 2000 song library and it's not going to say, "You are using a keyfile." It's going to ask you what your password is, you can plug in the password, you can plug in a keyfile. The attacker won't know per se that you are using a key file, so if I have a 2000 -- I've got quite a few more

than that, but if I've got an MP3 collection and only I know the song, then I can pull it up, it can just as very easily be a picture, it could just as easily be any number of things. The system that's going to take the password in the keyfile and try and generate the encryption key for the volume header, if it's unable to, it's going to say, "You know, I don't know what you are doing. What you gave me does not correspond with what I have."

Greg Hughes: So, when we are talking about putting in a password, we are talking about typing. So, again for the end user, what's the actual mechanism? What does the process look like in terms of providing that keyfile? Is it a browse button and then they go find out a file system or how does that work?

Eric Marvets: Yes, that's it. You say, "Add keyfile", and it opens up File Explorer, pick out the file or files, you can use multiple keyfiles, you can use an entire directory.

Greg Hughes: Got you.

Eric Marvets: That will all be used. Now, when picking a keyfile, you want to make sure that you are using something that's going to have a lot of randomness in the data. Text, when you are looking at text in a particular byte, over half of the available bits are not being used. So, what you want me to use is a compressed file like an MP3, like a RAR file or WinZip. You want to use something that's compressed, so that all the available bits in a byte have the potential to be used.

Richard Campbell: JPEG would qualify nicely there too, it's dense.

Eric Marvets: JPEG, yes absolutely.

Greg Hughes: So, you have to ability to use just a password or a password plus, a keyfile, is it even an option to use just the keyfile?

Eric Marvets: I am not sure if there is an option to use just the keyfile, I have never tried that. I've always done either just the password. For example, whenever I setup my TrueCrypt drives, all of them, I use just the password and securely store the backup and then I will use a password and a keyfile going forward in day to day life. I have never tried to use just a keyfile.

Greg Hughes: Well, there you go, it gives our listeners a reason to download and check it out, and they can find out for themselves.

Eric Marvets: Which this is all available at truecrypt.org, it's a sourceforge open source project. General public -- I think, GP3, and General Public License is available on this.

Richard Campbell: So, you can't argue with the price anyway.

Eric Marvets: No, definitely can't argue with the price and really this is -- it's such uniquely designed. They've taken everything into account. So, I don't know if you guys have seen the new Mercedes that has the Biometric thumb print scanner.

Richard Campbell: Yes.

Eric Marvets: How you start the car? Well, as soon as they came out with that car, no less than a few months later, somebody lost a thumb in a carjack.

Richard Campbell: No.

Eric Marvets: An attacker followed that car, it required the thumb to start and he took the thumb, and you saw that on 24, season 8 where they chop up the Air force pilot's finger, so they can get into the building. That is not a good scheme, alright.

Richard Campbell: I've never thought that the thumb scanners on the laptops is a good idea, after all your thumbs are all over the laptop.

Eric Marvets: Yeah, and there is actually -- you can go online and find the recipe for how to overcome the biometric scanners with a gummy bear, some translucent papers like we used to have in school with the little overhead projectors.

Richard Campbell: Right.

(00:30:01)

Eric Marvets: Make a copy on it, you can actually copy a fingerprint on there and it will be raised to the point that you can use a gummy bear and get past those biometric scanners.

Richard Campbell: Lovely.

Eric Marvets: Yeah, it doesn't take much skill at all.

Greg Hughes: It's pretty clear that there is no one silver bullet for everything security in the world and biometrics are not. It certainly raises it to a new level, above and beyond as to username and password, but I think your point is that there is really no one way to solve every problem, so it's a question of raising the bar.

Eric Marvets: Right, the major problem with biometrics and that will always be to biometrics is that, it's supposed to be based on a secret. If somebody finds out your password, you can change your password, if somebody lends your fingerprint or your retina, you cannot go get another fingerprint or retina.

Greg Hughes: Yeah, at least not yet.

Eric Marvets: That is why biometrics will always be a failure in the security industry.

Greg Hughes: Absolutely, yeah.

Richard Campbell: It's an interesting statement guys, and probably not an obvious one for those who haven't worked in that space near as much, you know I am looking at the TrueCrypt site and there is a line right in the middle of it that says, "Plausible Deniability." Now, where does that fit into this equation?

Eric Marvets: That's where it's run with the old old -- setup on the fingerprint on, exactly. If an attacker were to get you, your hard drives in the same room and say, "Alright, you are going to give me your password." One of the cool things is, inside of a TrueCrypt volume, you can have another volume, and it is impossible to detect. One of those is, when you create a TrueCrypt volume, it formats that volume by writing random bits of data to the entire drive. So, you setup a 500 gig TrueCrypt partition, you are going to come back tomorrow, and it will be finished. I had actually thought, "Only takes about an hour and a half," but it's going to write random data through the entire thing, so that you can take -- and you have one half of the drive that is the outer volume and the other half which is an inner. What TrueCrypt does is when you put in a password, it will look at the beginning of the drive and try and decrypt the header. If that fails, it jumps to the end of the drive and tries to decrypt the last few bits to see if you were looking for an inner partition.

Now, the one problem here is that if you are using the inner partition, you could overwrite data on the outer. If you are using the outer partition, you could overwrite data on the inner, because unless you have them both mounted at the same time, TrueCrypt is not going to know what belongs to what.

Richard Campbell: So, in normal use, you have to mount them both, so you don't mess things up.

Eric Marvets: You have to either mount them both, or there is an option when you load it, say, "Load as read only." So, you can load it read only, so there is no possibility of changing data, so you don't overwrite data on the other one, or you can mount with hidden drive protection. As you click that option, it's going to ask you for two passwords, it's going to ask you for the password for the outer and the inner. Once it's loaded, the file explorer is only going to show one drive, but it will know which sector does the hard drive belong to, which line and it will not overwrite it. So, even if an attacker walked in at that moment in time, I think there is a slight difference in one of the icons, but other than that, you will not be able to tell that there is two volumes loaded at the same time, and there is no way that they could tell when it's offline.

So, that is one thing that's very cool, so if you are worried about that type of – if you are talking some serious Corporate Espionage, or live gang factions or -- something where somebody is going to use force to get you to give up your data, you would always want to have dummy data in your outer volume and the real data in your inner volume.

Richard Campbell: Yeah, I think that's probably pushing the envelope for the average corporate environment, but it's certainly out of the realms of protecting yourself from identity thieves. But the fact that somebody is thinking about this is probably pretty clear proof that somewhere there is a requirement.

Eric Marvets: Somewhere there is a requirement and somewhere it has happened before.

Richard Campbell: Yeah, since this probably is not the first time that has happened.

Greg Hughes: I think another area where TrueCrypt can provide real value is, it's not always the case that a portable storage device is staying with one person, it's also -- I mean working in financial services industry and dealing with very large volumes of data, which as you mentioned Eric, can be quite sensitive at times, is the ability to do strong encryption, so that as you are safely couriing a 500 gig hard drive across the country to ensure that it's properly protected, there is a real value in that as well.

(00:35:01)

Eric Marvets: Right.

Richard Campbell: I can see that three part protection being great for that. That I would have a separate package of the drive, the thumb drive and the password.

Greg Hughes: Exactly.

Richard Campbell: So that, you need all three of those things to put it together.

Eric Marvets: Exactly, and that was one of the things I was saying in the beginning. TrueCrypt, the design of it is such that you can protect yourself to a very minimum level or to extreme. So, you just have to look at what adversary you think you are going to be facing. If you are trying to hide certain bills or certain financial records from a spouse, you don't need the same level of protection as you would from a foreign intelligence agent. There is quite a bit of difference in what you need to do. That's where TrueCrypt really excels, easy to use, they have a beginner's module which will take you through all of the things that I have talked about, and have you up and running with the TrueCrypt volume in the matter of an hour.

Greg Hughes: I think also, one of the other things that I recall seeing in TrueCrypt is just some of the usability preferences and some of it's even security related preferences, the ability to -- if there is no activity on a volume for a certain number of minutes, then automatically dismount volumes. Also, decide whether or not to cache passwords in memory, and if I do, then how do I scrub them and when? So, in the backend and from the configuration standpoint, there is some pretty valuable tweaks and tools that you can use.

Eric Marvets: Yeah exactly, if you were to Hibernate a laptop, then everything that's in memory gets stored on the hard drive. Now, TrueCrypt, when it reads data from the drive and loads it up to the memory, it decrypts it as it loads it up. So, if you are using a paging file, then TrueCrypt will lock the memory for the driver, which is still going to guarantee, but once it sends data over to Microsoft Word, Word is going to end up in a paging file, especially a large document. So, if it does have the documentation that goes along with it, which is only -- it's not that long to read, maybe 50 pages. It tells you things like, if you are dealing with this, if you are in this set of circumstances, you may want to turn off your paging file. You may want to have it automatically disconnect the drive when you go into hibernation or sleep. It covers those things that you may not think about, and good detail and the documentation goes along with it. Especially for XP and Vista, not that they did a better job for XP and Vista, it's just XP and Vista give you more options than say Windows 2000, where you can't really control that paging file.

Greg Hughes: It also gives the option to set hot keys for use of TrueCrypt, so I could for example instead of I don't know, control, alt, w if I wanted to wipe my volumes out and dismount all the volumes or what have you. So, for the keyboard user, a wide variety of different configuration and usability options.

Eric Marvets: This is a mature product, it's been around for a while, it's been used by quite a few people that are very security conscious. They have a website where you can suggest features and also what they are working on right now, you can see, you can take a look at all of that, but it's definitely a mature product.

Richard Campbell: Alright gentlemen, I think we are about out of time, so the product is TrueCrypt, and you can find it at truecrypt.org. Eric, thanks very much, any last words?

Eric Marvets: Oh, it's been fun guys, thanks.

Greg Hughes: Thanks a bunch, Eric.

Richard Campbell: Thanks a lot and we'll see you next week on RunAs Radio.

Total Duration: 39 Minutes.