

Forum:[Hack Forums](#)

Thread: [\[BHCPU\] How to setup Bitlocker now that truecrypt is insecure](#)

-Hyperion - May 29, 2014, 6:47 am

Hey guys it's -Hyperion ?

As you may or may not have heard Truecrypt has probably been compromised and it is no longer advisable from the creators even to use it. I will be walking you through today using another option that is built into windows called BitLocker and using it to encrypt the entire drive. Performance impact is minimal less then 5 MBps.

But first what is BitLocker? Bitlocker is a full drive disk encrytion program that uses the AES encryption algorithm in CBC mode with a 128-bit or 256-bit key, combined with the "Elephant" diffuser for additional disk encryption-specific security not provided by AES. In my opinion is it even more secure then truecrypt. You can read about it [Here](#)

To use BitLocker you will need:Ultimate and Enterprise editions of Microsoft's Windows Vista

Windows 7 Ultimate

Windows 8 Pro or Enterprise

A computer with Trusted Platform Module (TPM), which is a special microchip in some newer computers that supports advanced security features. If your computer was manufactured with TPM version 1.2 or higher, BitLocker will store its key in the TPM.

A removable USB memory device, such as a USB flash drive. If your computer doesn't have TPM version 1.2 or higher, BitLocker will store its key on the flash drive.

If you have one of the supported systems just go to the drive you want to encrypt and right click on it then hit turn on BitLocker.

Spoiler [\(Click to View\)](#)

Next choose a strong password that will be used to unlock the drive and click next.

Spoiler [\(Click to View\)](#)

You will then be prompted to save the recover key if you lose your password.

WARNING DO NOT LOSE THIS KEY OR STORE IT ON THE ENCRYPTED DRIVE
if you lose this recovery key after forgetting your password you will have to re-install windows and all data will be unrecoverable.

Spoiler [\(Click to View\)](#)

Then click that you want the drive to encrypt and let it run. That's it you're done. Now any time you want to access that drive you will have to enter your password.

If your computer does not have TPM you can still enable and use Bitlocker. To keep this tutorial short I will direct you [Here](#) which is an excellent guide on enabling Bitlocker on a system without TPM.

King Cin - May 29, 2014, 6:48 am

(May 29, 2014 06:47 AM)-Hyperion Wrote: [\[CITE\]](#) Hey guys it's -Hyperion ?
Orly?

Nice guide though. Nice of you to write it up for the people inexperienced in this field.

Aura - May 29, 2014, 6:51 am

This feg is using my signature introduction but modified ?
Add more images and fix that broken MyBB code.

-Hyperion - May 29, 2014, 6:53 am

(May 29, 2014 06:51 AM)Aur? Wrote: [\[CITE\]](#) This feg is using my signature introduction but modified ?
Add more images and fix that broken MyBB code.
learn from the best steal like the rest eh :P

?lixir - May 29, 2014, 6:55 am

Why would we use bitlocker? It's like using Internet Explorer as a secure browser.

King Cin - May 29, 2014, 6:55 am

(May 29, 2014 06:55 AM)Dr. Caspers Wrote: [\[CITE\]](#) Why would we use bitlocker? It's like using Internet Explorer as a secure browser.
Internet Explorer was the most secure browser on Windows 8 not so long ago, lol.

Aura - May 29, 2014, 7:03 am

(May 29, 2014 06:55 AM)Unknown † Wrote: [\[CITE\]](#) Internet Explorer was the most secure browser on Windows 8 not so long ago, lol.
This, lol.
Also, people seems to forget that IE is the most used browser in compagnies/entreprises running Microsoft technologies, lol.

-Hyperion - May 29, 2014, 7:07 am

(May 29, 2014 06:55 AM)Dr. Caspers Wrote: [\[CITE\]](#) Why would we use bitlocker? It's like using Internet Explorer as a secure browser.
Because I would rather use BitLocker then some shitty 3rd party app that someone made that not been tested or could be from the NSA. Look what happened to Truecrypt now.

immortalwon - May 29, 2014, 7:08 am

(May 29, 2014 07:07 AM)-Hyperion Wrote: [\[CITE\]](#) Because I would rather use BitLocker then some shitty 3rd party app that someone made that not been tested or could be from the NSA. Look what happened to Truecrypt now.
And you think microsoft bitlocker isnt sponsored by the NSA? LOL

-Hyperion - May 29, 2014, 7:12 am

(May 29, 2014 07:08 AM)immortalwon Wrote: [\[CITE\]](#) And you think microsoft bitlocker isnt sponsored

by the NSA? LOL

Are you under the impression they do not already have everything? BitLocker will keep unauthorized users from accessing the data and as far as we know law enforcement to. Truecrypt is now up for grabs so why use it? Microsoft has already said several agencies have requested a BD and been turned down. I would like to believe we can have some trust in them.

?lixir - May 29, 2014, 7:18 am

(May 29, 2014 07:03 AM)Aur? Wrote: [\[CITE\]](#) This, lol.

Also, people seems to forget that IE is the most used browser in compagnies/entreprises running Microsoft technologies, lol.

When companies use software they purchased, it leaves a paper trail so if something goes wrong, they can yell at them. If companies use free and open-source software then it is always the IT's fault. I prefer open-source over closed source for security any day.

zombiehacker - May 29, 2014, 7:19 am

I wouldn't trust bitlocker with anything since it's made by microsoft.

-Hyperion - May 29, 2014, 7:21 am

(May 29, 2014 07:19 AM)zombiehacker Wrote: [\[CITE\]](#) I wouldn't trust bitlocker with anything since it's made by microsoft.

Shouldn't you be in the linux section then ?

Aura - May 29, 2014, 8:28 am

(May 29, 2014 07:18 AM)Dr. Caspers Wrote: [\[CITE\]](#) When companies use software they purchased, it leaves a paper trail so if something goes wrong, they can yell at them. If companies use free and open-source software then it is always the IT's fault. I prefer open-source over closed source for security any day.

Wrong. It's always the IT Department's fault, no matter what. Trust me, I get shit at everyday for things that aren't even under my control.

?lixir - May 29, 2014, 8:58 am

(May 29, 2014 08:28 AM)Aur? Wrote: [\[CITE\]](#) Wrong. It's always the IT Department's fault, no matter what. Trust me, I get shit at everyday for things that aren't even under my control.

Show them the paper trail. Or check your logs to find the blame.

Aura - May 29, 2014, 9:30 am

(May 29, 2014 08:58 AM)Dr. Caspers Wrote: [\[CITE\]](#) Show them the paper trail. Or check your logs to find the blame.

Even there, lol. And I'm part of the technical support department. When you sign for this job, you sign to get shit at everyday, lol.

?lixir - May 29, 2014, 11:32 am

(May 29, 2014 09:30 AM)Aur? Wrote: [\[CITE\]](#) Even there, lol. And I'm part of the technical support department. When you sign for this job, you sign to get shit at everyday, lol.

Oh I'm a network admin/technician so I can see how its different for you.

Aura - May 29, 2014, 11:36 am

(May 29, 2014 11:32 AM)Dr. Caspers Wrote: [\[CITE\]](#) Oh I'm a network admin/technician so I can see how its different for you.

Here, Network Admins are my tier 3 (I'm tier 2, I'm just an intern too) and the ones I go seek help from when a problem is beyond my level of authorization/action ?

?lixir - May 29, 2014, 11:43 am

I could never do what you do mate. Respect lol. I can only relate to machines.

Madison Ivy - May 29, 2014, 11:49 am

Hello. I installed truecrypt couple days ago and crypted some files. Should I switch to bitlocker? I don't know why but it feels kinda weird "truecrypt is not safe but we won't tell you why now you have to use microsoft's service"

Aura - May 29, 2014, 11:51 am

(May 29, 2014 11:49 AM)zgooglez Wrote: [\[CITE\]](#) Hello. I installed truecrypt couple days ago and crypted some files. Should I switch to bitlocker? I don't know why but it feels kinda weird "truecrypt is not safe but we won't tell you why now you have to use microsoft's service"

What are you keeping encrypted with TrueCrypt ?

XXX - May 29, 2014, 11:52 am

As if bitlocker is secure... brb using something made by microsoft.

Ryxa - May 29, 2014, 11:53 am

Why not just use an older version of Truecrypt? Just because their site and keys got compromised doesn't suddenly mean the previous versions of TC suddenly has backdoors...

The amount of misinformation is extremely high.

Madison Ivy - May 29, 2014, 11:54 am

(May 29, 2014 11:51 AM)Aur? Wrote: [\[CITE\]](#) What are you keeping encrypted with TrueCrypt ? Just some files that I'd like to keep safe. Nothing super illegal though.

Aura - May 29, 2014, 11:58 am

(May 29, 2014 11:54 AM)zgooglez Wrote: [\[CITE\]](#) Just some files that I'd like to keep safe. Nothing super illegal though.

Well then it's not that bad. If it's porn or something who cares. Who knows if there's EVEN an exploit for it too. Also, it would require that someone access your computer and use that exploit on TrueCrypt, which will most likely not happen via one of your friend or else except if you're RAT'd.

Enough with the bitching about Microsoft. If you're not happy with it, don't use Windows or any other Microsoft products. If you think you're a l33t h4x0r or any other Black Hat Hacker that can get in trouble, use open-source tools and GNU/Linux distros and stop bitching. God it's annoying.

Null Byte - May 29, 2014, 4:13 pm

Fuck that shit I'm sticking to LUKS or dm-crypt, bitlocker is backdoored anyways.

Also read this: https://en.wikipedia.org/wiki/Warrant_canary

The TC developers would never recommend switching to bitlocker. Definitely a low-key sign that something has gone wrong.

Fuck the Patriot Act

Loki123 - May 30, 2014, 6:52 pm

CBC mode ?

<http://hackvalue.de/files/padding.pdf>

http://en.wikipedia.org/wiki/Padding_oracle_attack

No.

