Notes on BitLocker and the TPM and the pre-boot password or PIN

devblogs.microsoft.com/oldnewthing/20220412-00

April 12, 2022

Raymond Chen

I had an older system that had BitLocker configured with a pre-boot password because it didn't have a Trusted Platform Module (TPM). I later discovered that the system did indeed have a TPM, but it was disabled by default, which is why BitLocker couldn't find it.

Here's how I converted the system from a pre-boot password to TPM-managed protection.

Step 1: Enable the TPM chip in the BIOS.

This will vary from manufacturer to manufacturer. The tricky part is that some BIOS menus don't refer to the TPM as a TPM. They call it an "Embedded Security Device" or a "Security Chip". You want to Enable the TPM / Embedded Security Device.

You also want to enable *OS Management of Embedded Security Device* if you have that option.

This web site walks you through the BIOS of many major manufacturers.

Step 2: Let Windows take control of the TPM.

From an elevated command prompt, type `tpm.msc` to run the TPM console snap-in. Over on the right-hand side, there will be an option called "Prepare TPM for use". If prompted, reboot the system back into the BIOS, so that the BIOS can verify that you really want to let Windows use the TPM.

After convincing the BIOS to let Windows manage the TPM, you can switch over to letting the TPM manage your BitLocker volume.

Step 3: Enable TPM management of BitLocker.

From an elevated command prompt:

```
manage-bde -protectors -add C: -tpm
```

This tells BitLocker to allow the TPM to protect access to the volume.

Doing this might regenerate the recovery key, so do a

```
manage-bde -protectors -get C:
```

to get the new Numerical Password. The ID is a bunch of letters, digits, and dashes inside curly braces. This lets you remember which volume the password is for. The password is the sequence of six-digit blocks separated by dashes. Save both the ID and password in a safe place.

Step 4: Remove the old password.

```
manage-bde -protectors -delete C: -t Password
```

This last step is what stymied me. I had set up the TPM to unlock the volume, but I still kept getting prompted for the password. That's because the password protector was still there, and the system insisted on using it.

Delete the password protector, leaving just the TPM protector. That lets the TPM take over as the source of unlocking the system volume at boot.

As an extra check, run

```
manage-bde -protectors -get C:
```

and look for interactive protectors like Password, TPMAndPIN, or TPMAndPinAndStartupKey. If present, delete them. (But don't delete TPM or Numeric Password!)

Bonus chatter: Sometimes, the TPM doesn't play friendly, and I have to enter my 48-digit BitLocker key (ugh). I don't know why this happens.

Raymond Chen

Follow