June 2022

METHOD OF ENCRYPTING DISK ON LINUX CLIENTS AND PROTECTING DISK ENCRYPTION KEY WITH TPM 2.0 DEVICE

HP INC

Method of encrypting disk on Linux clients and protecting disk encryption key with TPM 2.0 device

Disk encryption with TPM 2.0 on Linux clients

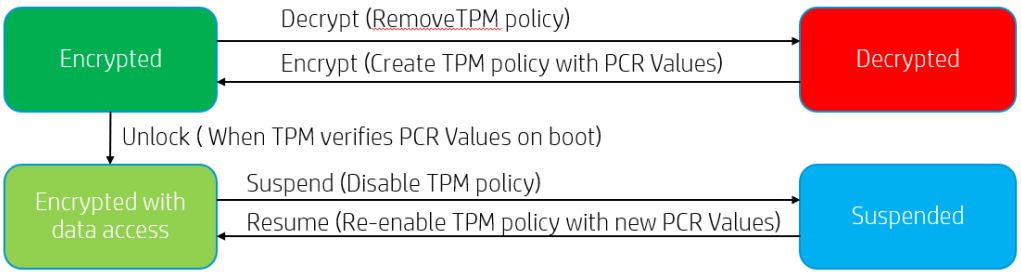
ABSTRACT

Disk Encryption is a common way of protecting data on Operating Systems nowadays. It becomes mandatory on some modern Operating Systems, e.g., Operating Systems on a wide variety of mobile phones. TPM (Trusted Platform Module) is a hardware module on modern PCs to improve the security of PCs. This publication demonstrates a solution to encrypt disk and protect the disk encryption key with TPM 2.0 on Linux clients.

DESCRIPTION

Encryption is a common way of protecting data, and disk encryption are one of the approaches, but disk encryption is not turned on by default on most modern Linux distributions. Even when disk encryption is turned on, the disk encryption key is not protected by default, the end users must enter the disk encryption key to unlock the encrypted disk. Described is a method that encrypts the data on the disk of a Linux client by encrypting the whole disk and protects the disk encryption key by TPM device 2.0 if there is one present on the Linux client.

There are four disk encryption states defined in this article: Encrypted, Decrypted, Suspended and Encrypted with data access. And there are five operations which allow user to transition between states. The disk encryption states are very self-explanatory, and five operations will be covered in next session.



Encryption

This method consists of two major parts, one is disk encryption, the other is the use of TPM 2.0 device to protect disk encryption key. Below are how both parts work together to get the disk encrypted while getting disk encryption key protected on a Linux client.

Step 1: When a user turns on disk encryption on a running Linux client, the Linux client reboots into a mini-Linux operating system and kicks off disk encryption.

Step 2: A random disk encryption key is generated and then the disk starts being encrypted by using the key with strong encryption algorithm, which usually takes a few minutes, the duration of encrypting the disk depends on the size of the disk.

Step 3: Once the disk encryption is completed successfully, the disk encryption key is stored into TPM storage, and the Linux client's boot process is also re-configured so that the encrypted disk will be unlocked automatically on boot.

Step 4: The Linux client reboots back to standard Linux operating system. During the first reboot after encrypting the full disk, TPM cryptographically measures platform software running on the platform and configuration data used by the platform software. The measurement action is like taking a snapshot of the status of the platform software. TPM PCR (Platform Configuration Register) records these values. TPM uses selected PCR values to create a TPM's authorization policy to lock down disk encryption key. And encryption is now turned on.

Unlocking

Normal Unlocking

After disk is encrypted, these selected PCR values are re-measured on every boot and used to compare with the recorded PCR values in the TPM's authorization policy. If these values do not match the recorded ones, the platform is not in a trusted or authorized state, therefore, the disk encryption key cannot be retrieved from TPM storage. If these values match the recorded ones, the disk encryption key can be retrieved from TPM storage, and the encrypted disk is unlocked, and user can access the data on the disk.

Recovery Unlocking

If the encrypted disk cannot be unlocked as expected, user must go through recovery process to unlock the encrypted disk. User can try to re-enable TPM policy with new PCR values.

Decryption

Decrypting the disk is more or less a reverse operation of encrypting the disk, the Linux client with encrypted disk boots into the mini-Linux operating system and starts decrypting the disk. After disk decryption is completed successfully, boot process will be re-configured and TPM's authorization policy will be removed.

Suspension and Resuming

Since PCR Values are recorded by measuring the platform software, system changes to platform software make PCR values change too, like changes in BIOS and BIOS configuration, changes in boot loader and kernel/kernel modules. But system changes take place quite often, e.g., system maintenance tasks as BIOS update, OS upgrade and etc. Disk encryption suspension is introduced to resolve this issue. Before deploying any potential system changes that may cause changes in PCR values, user can suspend disk encryption and let user complete the system changes, and then resume disk encryption to transition back to

"Encrypted with data access" state. Suspending disk encryption disables the TPM's authorization policy and resuming disk encryption re-enables the TPM's authorization policy with new recorded PCR values on next boot. Suspending disk encryption is intentionally started before any system changes and resuming disk encryption is designed to start automatically and bring back protection to disk encryption key as early as possible. Developers can also provide some tools to detect possible system changes and suspend disk encryption automatically to avoid bricking the Linux client. Once a Linux client is bricked, it can only be recovered by recovery options.

Recovery

Recovery is needed but not limited to the following scenarios,
- Hardware or TPM failure
- System failure
- Admin wants to move disk to a new machine
- Admin forgot to suspend disk before system changes

Recovery password is generated to unlock the encrypted disk. There are a few options to recover.
1. manually input recovery password to unlock
2. store recovery password in USB drive and read the recovery password in USB drive when failing to unlock encrypted disk on boot

2. Recovery password management is considered
- Allow admin to retrieve recovery password when operating system is not compromised
- Allow admin to back up recovery password to USB drive when operating system is not compromised
- Allow admin to back up recovery password to central management tool when operating system is not compromised

Disclosed by Qin Wan, Zhiwei Yu and Michael J Frick, HP Inc.