Contribution ID: **83** Type: **not specified**

Inline Encryption Support

Monday, September 9, 2019 5:00 PM (45 minutes)

Storage hardware with built-in "inline"encryption support is becoming increasingly common, especially on mobile SoCs running Android; it's also now part of the UFS and eMMC standards. These devices en/decrypt data between the application processor and disk without generating disk latency or cpu overhead. Inline encryption hardware can be programmed to hold multiple encryption keys simultaneously and can be dynamically reprogrammed to use any of these programmed encryption keys to en/decrypt a particular request. This makes this new class of storage ideal for supporting fscrypt (file-based encryption). Unfortunately, there isn't currently a unified approach for supporting inline encryption hardware in the Linux kernel.

We've sent out an RFC patchset to add support for inline encryption to the block subsystem, UFS driver, f2fs, and fscrypt
(https://www.spinics.net/lists/linux-block/msg40330.html).
We'll discuss our approach including:

- How the filesystem communicates an encryption key to inline encryption hardware for each struct bio it submits.
- How to add support for inline encryption to storage drivers.
- Support for layered devices like device mapper.
- A software crypto fallback.
- How this work can make future encryption tasks cleaner - like metadata encryption, file-based encryption on removable storage and the possibility of unifying how fscrypt, dm-crypt, and eCryptfs implement encryption.

I agree to abide by the anti-harassment policy

Yes

I confirm that I am already registered for LPC 2019

Primary author: TANGIRALA, Satya

Presenter: TANGIRALA, Satya

Session Classification: Kernel Summit Track

Track Classification: Kernel Summit talk