



Whamcloud

Community Lustre Security

05/2019

sbuisson@whamcloud.com



Community Lustre security

- ▶ Encryption at Lustre client level
- ▶ Security related code reviews in the Community

Encryption at Lustre client level

► Requirements

- encrypt file content
- encrypt file name
- have a master key for encryption
 - per-file encryption key derived from master key
- lock files when master key is removed
- work in “batch scheduler” mode

Encryption at Lustre client level

► Proposal

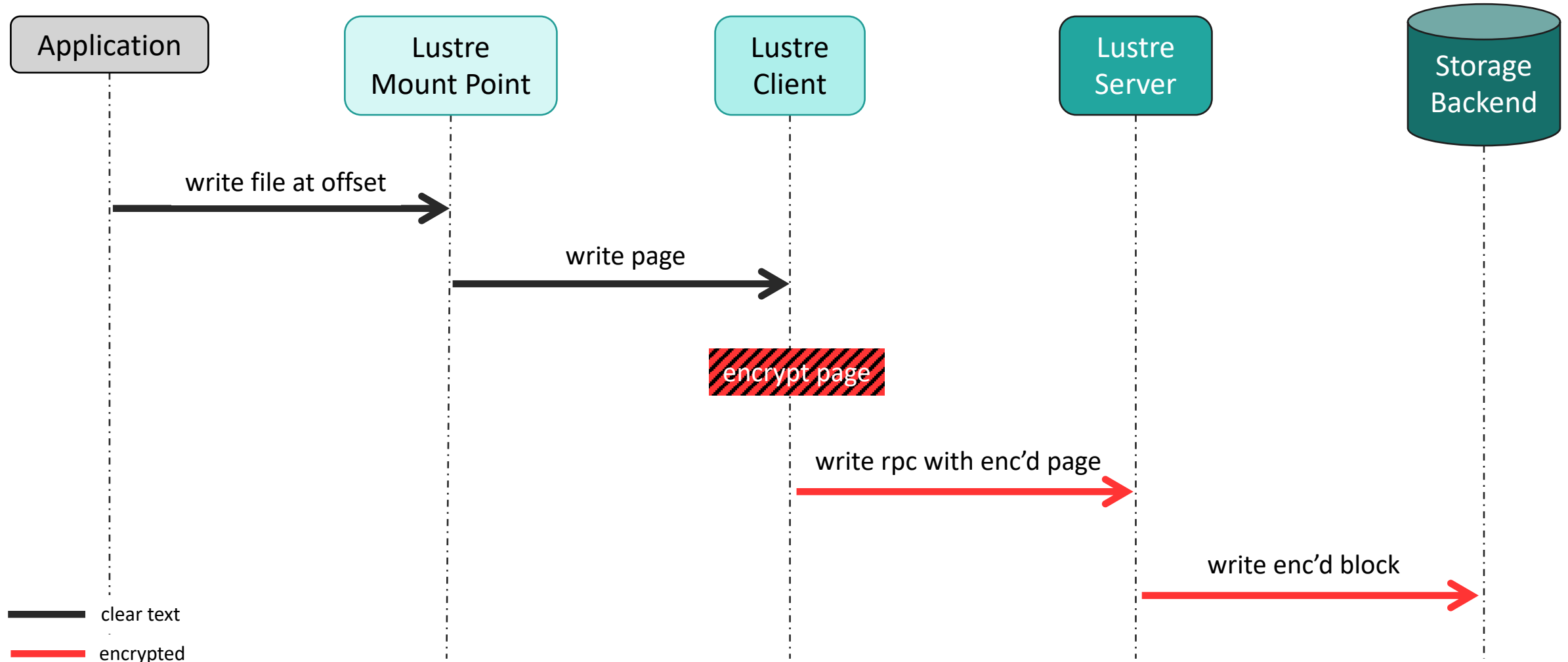
- conform to fscrypt kernel API
 - current users are ext4, F2FS, and UBIFS
 - need to use newly pushed policy v2
- rely on ext4 encryption principles
 - file system block size = system page size
 - each filesystem block is encrypted independently in a separate block
 - pages in the page cache always contain clear text data
- mutualize code infrastructure with compression work
 - same kind of operations, at same code locations

Encryption at Lustre client level

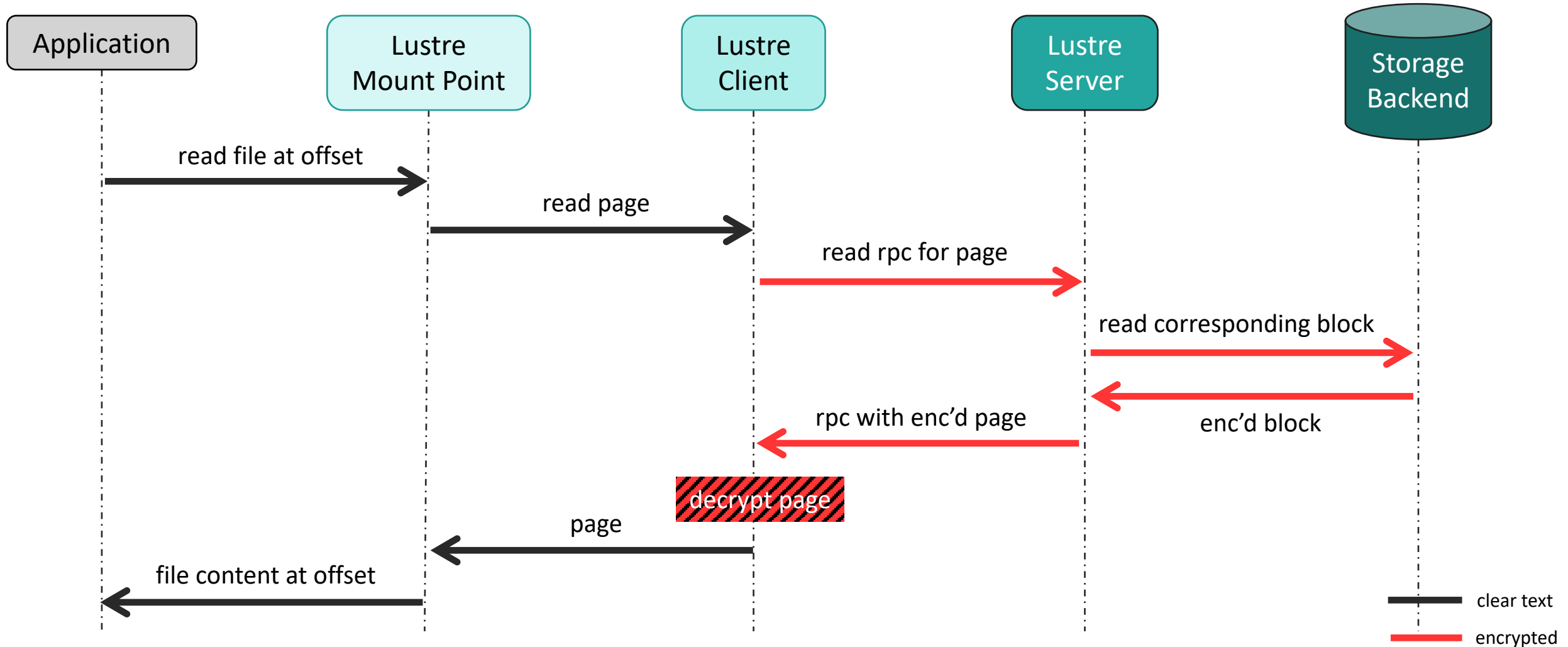
► Workflow

- applications see clear text
- data is encrypted before being sent to servers
 - then remain untouched
- data is decrypted upon receipt from servers
 - untouched before that
- servers only see encrypted data
 - but do not need to be aware of it
- only client nodes have access to encryption keys

Encryption at Lustre client level – write case



Encryption at Lustre client level – read case



Security related code reviews in the Community

- ▶ Security features have impact on various Lustre components
 - maintainers for these components are affected...
 - but reviews also need a security sensitivity!
- ▶ Looking for people willing to participate in security oriented patch reviews
 - knowledge of
 - authentication
 - encryption
 - SELinux
 - implementation experience with other software, best practice, ...



Whamcloud

Thank you!

sbuisson@whamcloud.com

