Two-factor LUKS Decryption using YubiKey

Sree Harsha Totakura
sreeharsha@totakura.in

28. Dezember 2014

About me

I . . .

1. use Full Disk Encryption with LUKS, always.
2. paranoid about entering passwords, especially for FDE.
3. Wish for a two-factor decryption for LUKS.

Two-Factor Decryption; How?

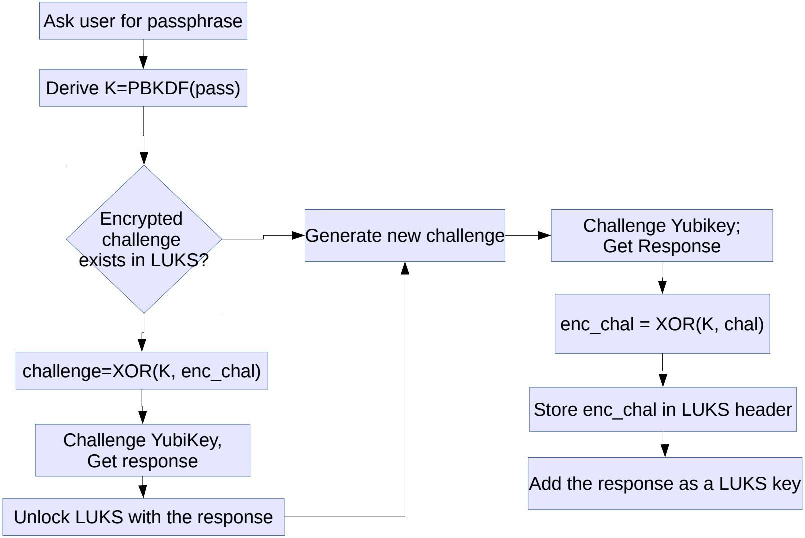
1. Use a keyfile from a USB media to decrypt LUKS; USB media needs a password to unlock.
2. Use a PGP smartcard to decrypt a keyfile; smartcard needs a PIN
3. Use a YubiKey

Yubikey

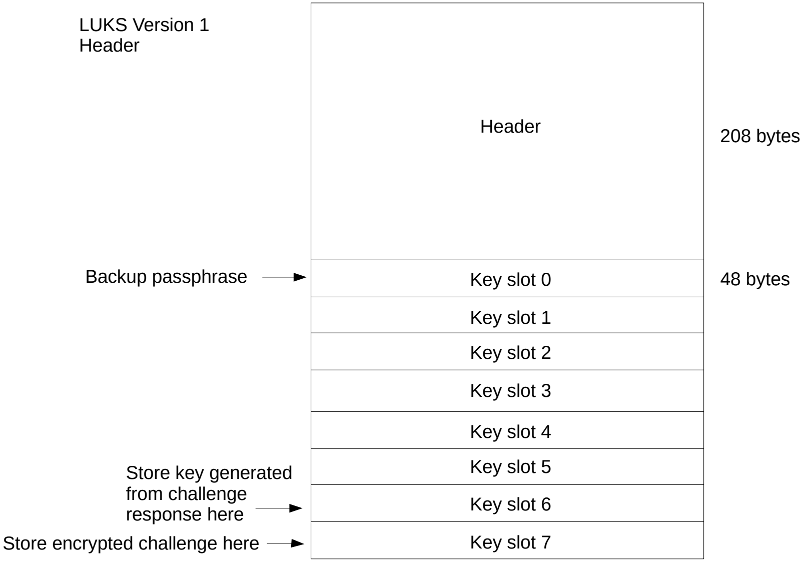
A USB device used to Authentication which generates OTPs. It . . .

1. can store AES keys
2. generates OTP tokens using these keys
3. can also do challenge response with these keys
4. keys are only written, but never read. (really? Hmm, need to check on that.)

ykluks – This is how it works


Ask user for passphrase
Derive K=PBKDF(pass)
Encrypted challenge exists in LUKS?
Generate new challenge
Challenge Yubikey; Get Response
enc_chal = XOR(K, chal)
Store enc_chal in LUKS header
Add the response as a LUKS key
challenge=XOR(K, enc_chal)
Challenge YubiKey, Get response
Unlock LUKS with the response

Dirty bits



LUKS Version 1
Header

Header — 208 bytes

Backup passphrase → Key slot 0 — 48 bytes

Key slot 1

Key slot 2

Key slot 3

Key slot 4

Key slot 5

Store key generated from challenge response here → Key slot 6

Store encrypted challenge here → Key slot 7

Statutory Warning

Backup your LUKS header before using this.

References

1. https://github.com/lfasnacht/ykluks
2. https://github.com/totakura/ykluks (with 2 factor auth; not merged into 1 yet)
3. https://github.com/cornelinux/yubikey-luks/blob/master/key-script

Thank you