Cryptsetup-javacard

A JavaCard key manager for LUKS

Ondrej Mosnáček, Manoja Kumar Das,
Mmabatho Idah Masemene

PV204 - Security Technologies

May 5, 2015

https://github.com/W0nder93/cryptsetup-javacard

Use case

- disk encryption on Linux (via Cryptsetup[1])
- the card stores the encryption keys, protected by a master password
- user actions:
  - **change master password**
  - **create an encrypted partition** (card generates and stores the key)
  - **unlock an encrypted partition** (encryption key is loaded from card, decrypted contents are mapped to a new block device)
  - **erase an encrypted partition** (encryption key removed from card, partition header is erased)

[1] `https://gitlab.com/cryptsetup/cryptsetup`

Components

- **JavaCard applet – KeyStorageApplet**
- **Host application – JCKeyStorage**
  - written in Java
  - command-line interface for communicating with the applet
- **User interface**
  - a set of shell scripts
  - a “bridge” between JCKeyStorage and Cryptsetup
  - simple commands corresponding to the use cases
  - includes applet install/delete scripts
  - example:

```
$ ./luks_erase.sh card-pk.ber ’ACS ACR1281 1S Dual Reader 00 00’ /dev/loop0
Deleting key of partition 68ae5cd9-5614-49fd-a089-8e6e22208930...
Enter master password:
Erasing the partition header...
Successfully erased keys for device ’/dev/loop0’!
```

Secure channel

- Priniciple:
  1. ECDH key exchange used to derive session keys
  2. communication encrypted with AES-CBC and integrity-protected using HMAC-SHA256
- the card-to-host part of the ECDH key exchange is signed using card's RSA key (to prevent MitM attack)
- card's public RSA key must be downloaded from the card in a secure environment and stored on the host
- user(host)-to-card authentication done by sending the master password over the secure channel

Bug in JCardSim

- during development, we discovered a bug in JCardSim's javacard.security.KeyAgreement implementation
- about 50 % of the time the key exchange would produce different keys than the real card
- pull request coming soon…