Transparent Encryption of Data with Embedded Peripheral Hardware

S T U
F I I T

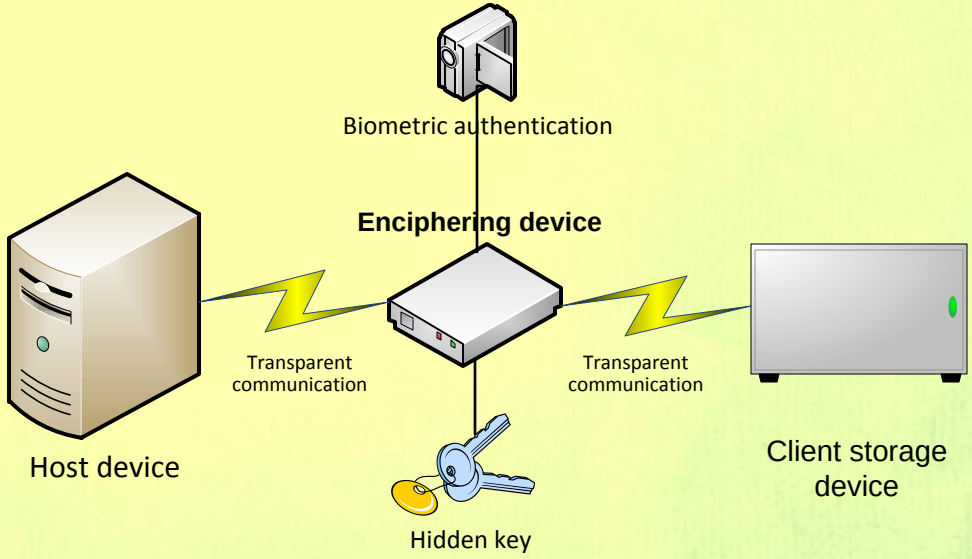
Author: Ondrej Perešíni, supervisor: Ing. Mária Pohronská
Faculty of Informatics and Information Technologies
Slovak University of Technology in Bratislava, Slovakia, 2011

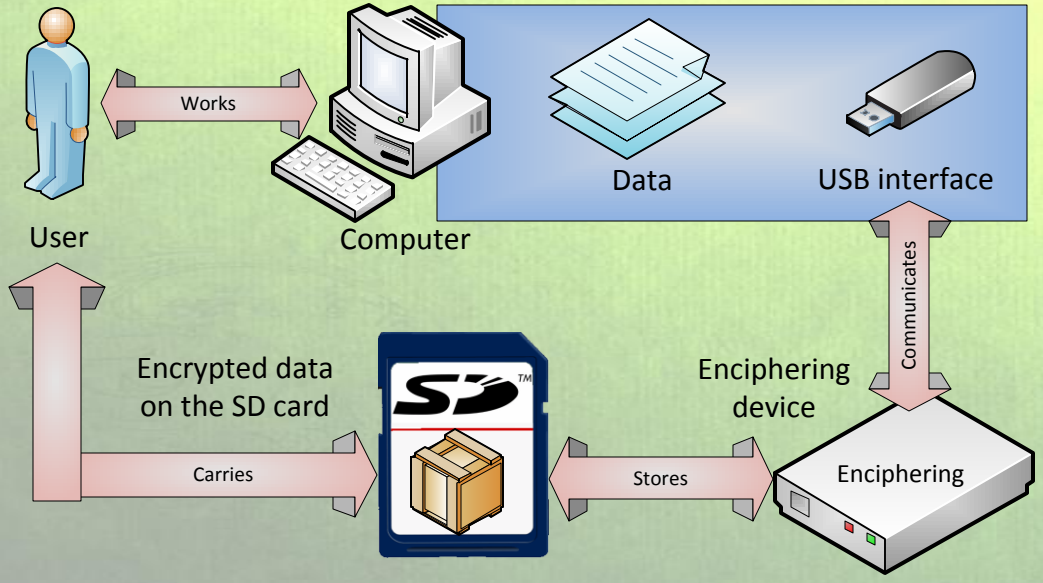
ACM SPY

- Today, data encryption is used on everyday basis
- Weak encryption algorithms can be broken in matter of minutes
- Need for fast, secure and reliable enciphering device for everyday usage

Block scheme of proposed solution

- Independent from host operating system and client storage device
- Both way transparent communication with possibility of storage device change
- Optional biometric authentication within enciphering device for better security (no need for host contribution)
- Enciphering key is hidden inside protected FLASH memory





Working diagram

- Useable with any device compatible with USB Mass Storage Device class
- USB interface is wide-spread and provides sufficient communication speed
- SD memory cards are fast with low price and ease of implementation

Benefits of encryption device

- User can carry small SD card without carrying the whole enciphering device
- Proof of cheap design concept with sufficient security and speed
- 128 bit XTEA encryption algorithm with dynamic enciphering key shifting and SD card filesystem encryption for brute force attacks resistance
- USB bus powered with universal ARM microprocessor
- Ready for future improvement of speed and security