



μDS

www.fixme.hu/uds

Mátó Péter

<mato.peter@andrews.hu>

Ez az előadás egy mókás
ötlettről és annak
megvalósításáról szól.

Meg arról, hogy a Linux elég
rugalmas volt, és hagyta.

Minek?

- elterjedtek a notebookok
- egy notebook – egy merevlemez
- a merevlemezek meg tönkremennek
- vagy ellopják a notebookot, az adat elvész, a titkok kiderülnek
- de mi biztonságban akarjuk tudni az adatainkat

Rész megoldások

- rendszeres mentés
 - a kutya se csinálja meg
 - a mentés is elveszhet, így a bizalmas adatok kiderülnek
- rendszeres mentés, titkosítva
 - a kutya se csinálja meg, szintén
 - a kulcs elveszhet, így a bizalmas adatok örökre elvesznek (pl. csipkártya vagy USB token használata feloldásra)

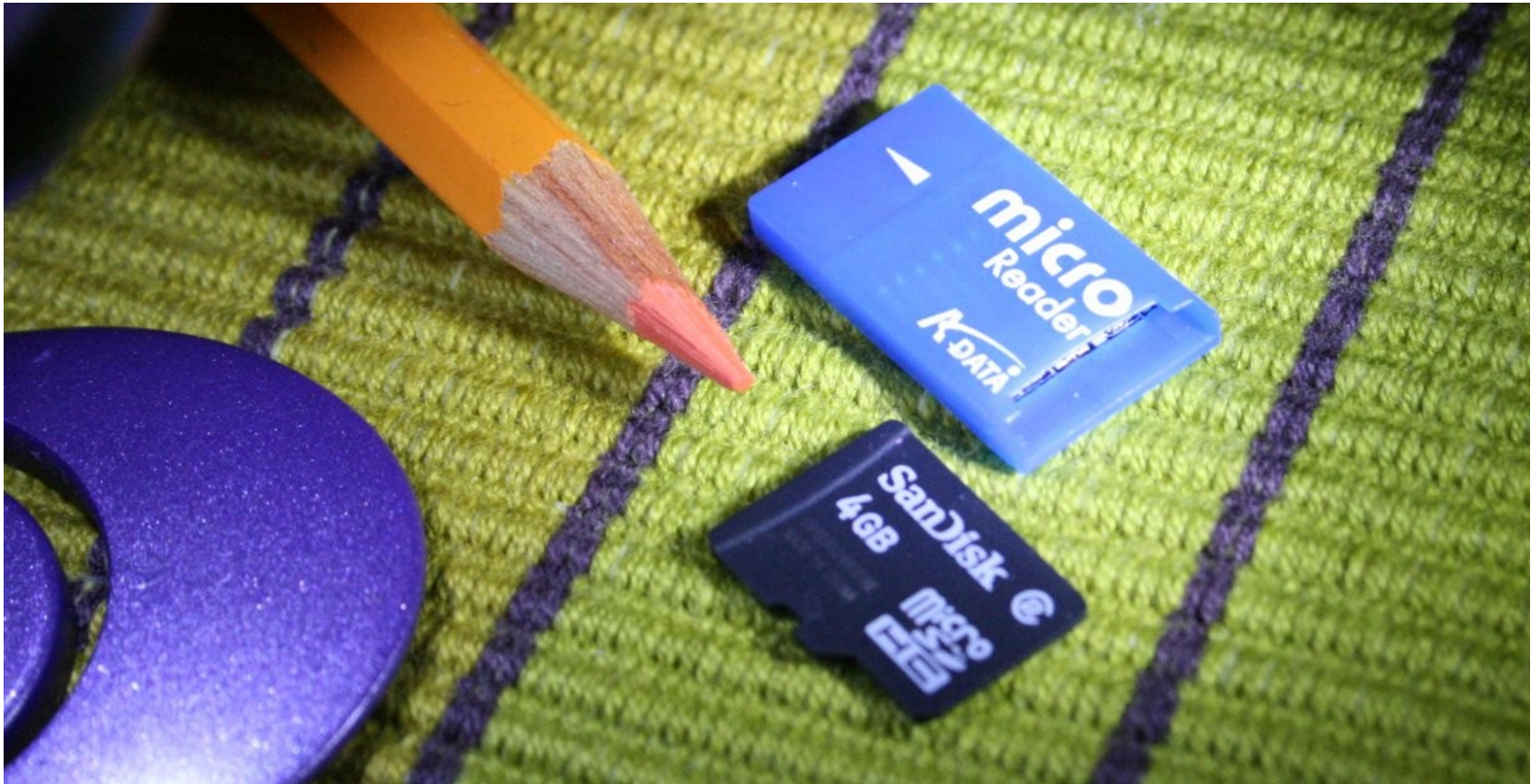
Részmegoldások még

- titkosított partíció vagy diszk
 - tönkremehet a diszk
 - ha a jelszót elfelejtjük, akkor ecet
- RAID1
 - nem lehet több diszk egy notebookban
- USB diszk használata
 - ha elveszik, a bizalmas adatoknak annyi

Az ötlet

- 2005 körül szokás szerint, újfent elszállt a diszk
- Lilo javasolta, hogy csináljak pendrive-okból RAID tömböt. Nyilván viccnek szánta (szinte mindent annak szán :P).
- Akkoriban volt egy 64 megás pendrive-om. Nagy volt, lassú és ronda.
- De az ötlet szöveget ütött a fejembe, és lassan...

Valami megváltozott



μ DS

www.fixme.hu/uds

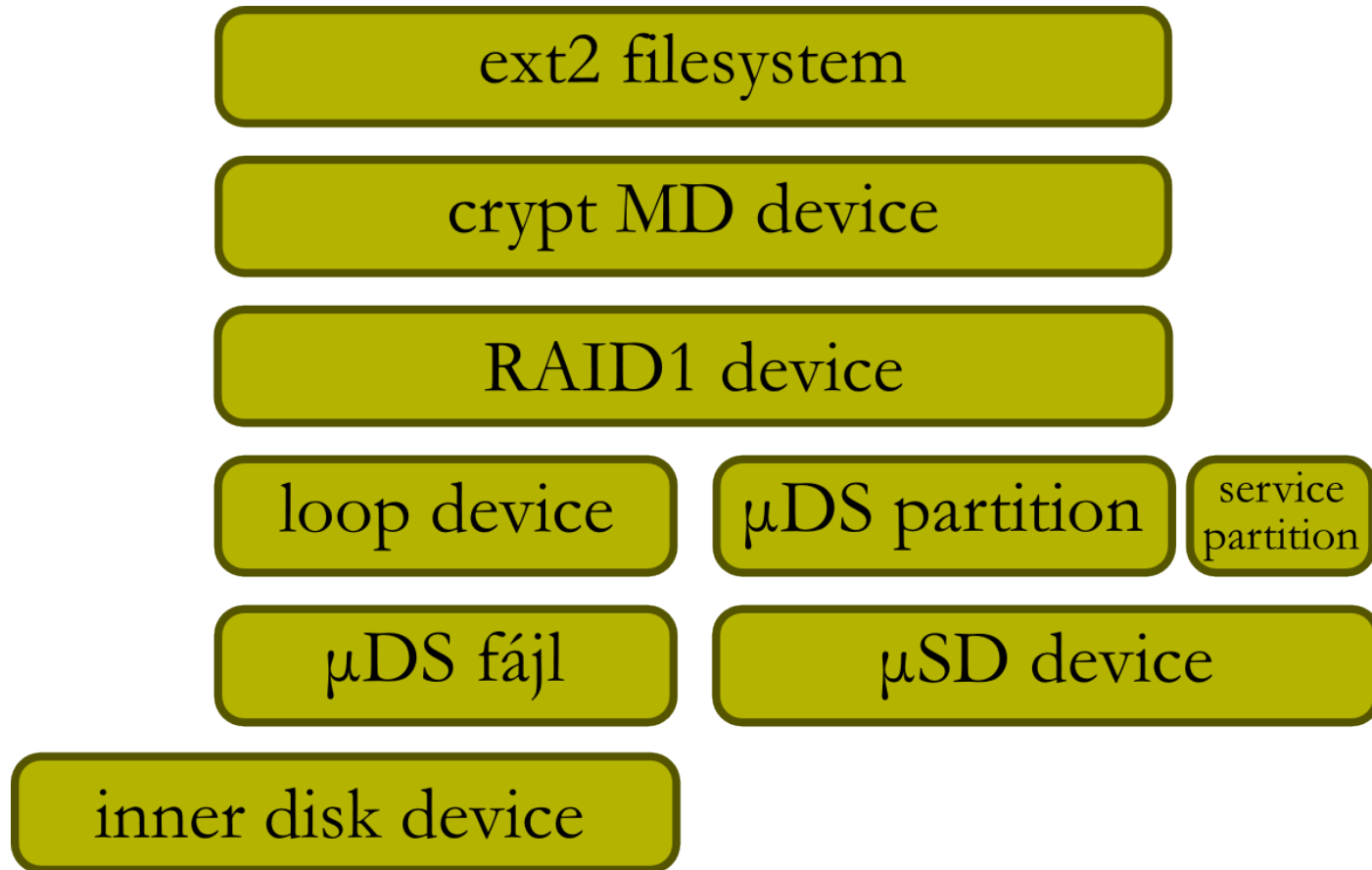
Mátó Péter

<mato.peter@andrews.hu>

A megoldás

- A Linuxban minden fájl. És majdnem minden blokkeszköz.
- Van benne RAID és titkosítás-támogatás is.
- Diszk csak egy van, de az elég is. Jó lesz másodiknak egy külső USB- μ SD.
- Nosza rajta, csináljuk meg.

Teljes működés



Felmerülő problémák

- ne legyen szükség a diszk újraparticionálására
 - loop device használata
- lehetőleg legyen gyors
 - a RAID tömb tagjaira beállítható a write-mostly és a write-behind flag
- legyen könnyen archiválható
 - a 4G méret pont jó, egy DVD-re le lehet archiválni

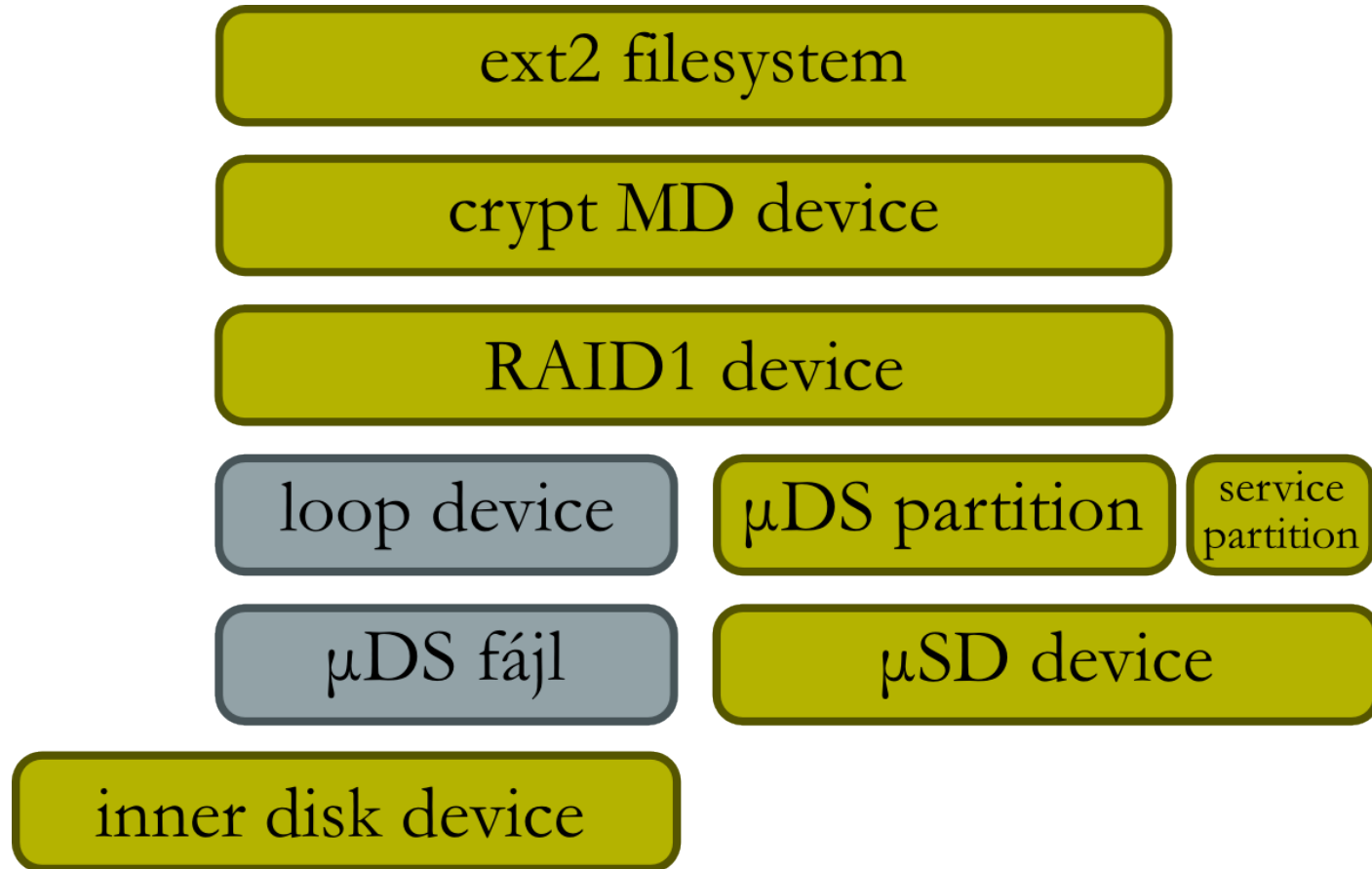
Felmerülő problémák még1

- nem Lugosi Bélával egyidős rejtjelezési módszerek (DES, ne már! AES.)
- adjon lehetőséget gyors kulcscserére
- a titkosításnál lehessen több kulcsot beállítani
- legyen mód más rendszereken is használni (nyílt tárolási formátum, szoftverek más rendszereken)
 - LUKS (Linux Unified Key Setup)

Felmerülő problémák még2

- milyen fájlrendszert használjunk
 - ne naplózót, mert a naplófájl nagyon gyakran frissül
 - vannak flash-re optimalizált fájlrendszerek (pl. JFFS2), de nem túlzottan támogatott (Linux és eCos)
 - legyen akkor ext2 és relatime (majd: ext4 w/o journal)
- legyen mód másik számítógépen is használni
 - részleges RAID működés, resync

Részleges működés



Felmerülő problémák még3

- legyen resync
 - a Linux RAID alapból tud ilyen
- gyors legyen a resync
 - felkészíthető egy „write-intent bitmap” segítségével
- az SD a sok írástól tönkremegy
 - relatime, havi vagy gyakrabban mentés külső diszkre
 - négyhavonta teljes μ SD csere (a levedlett archív lesz)

Merre tovább?

- automatikus async érzékelés, resync
- kulcscsere és szerviz kulcs használatának beépítése
- grafikus felület és csatlakoztatás után automatikus indítás noob-oknak
- dokumentáció, más nyelvű verziók
- fittség, világuralom



μDS

www.fixme.hu/uds

Mátó Péter

<mato.peter@andrews.hu>