Baslug - Basilicata Linux Users Group - www.baslug.org

Se mi lasci ti cancello:
Cancellazione sicura asincrona su ext3

Donato Capitella

scorpio2002@baslug.org

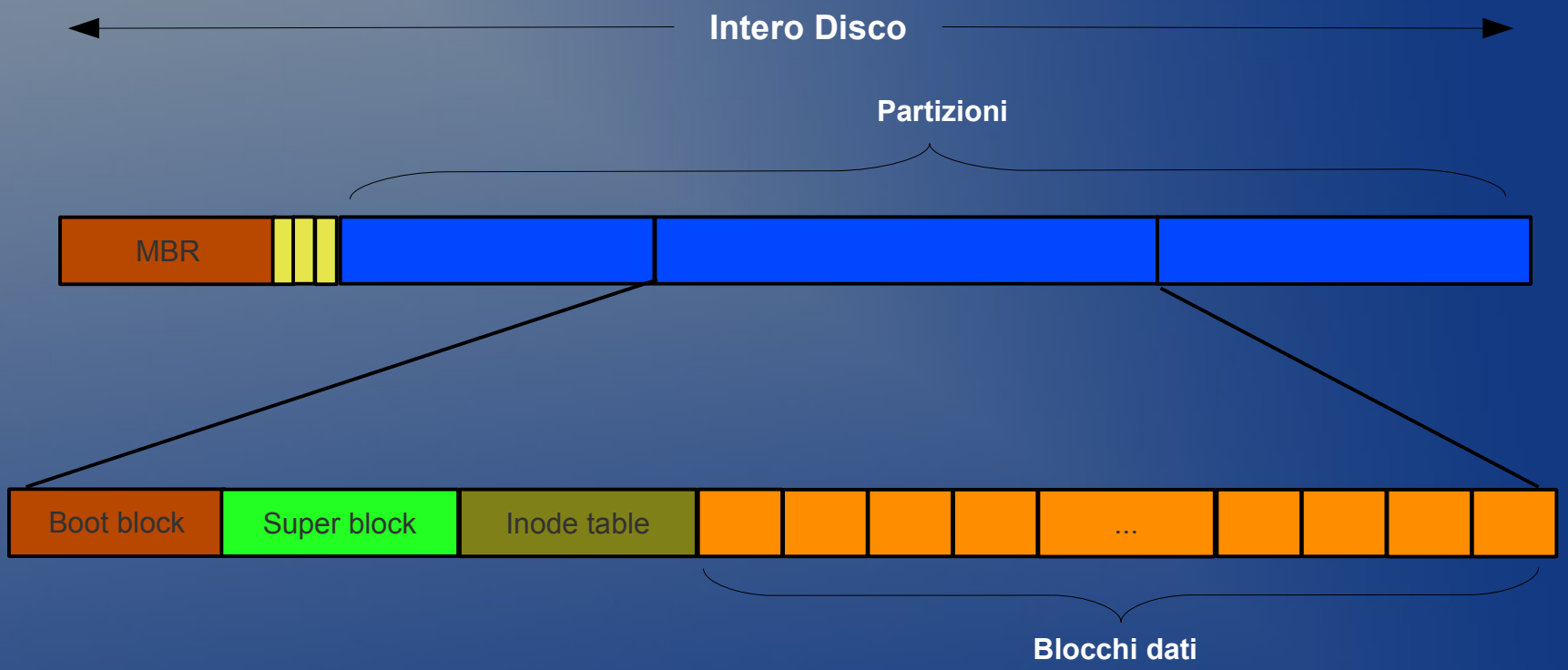
Linux Day 2009 - Giornata nazionale dedicata al Software Libero e GNU/Linux

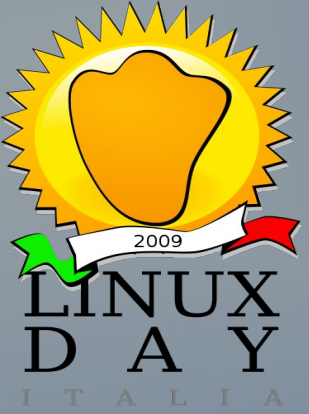
Se mi lasci, ti cancello

Sommario

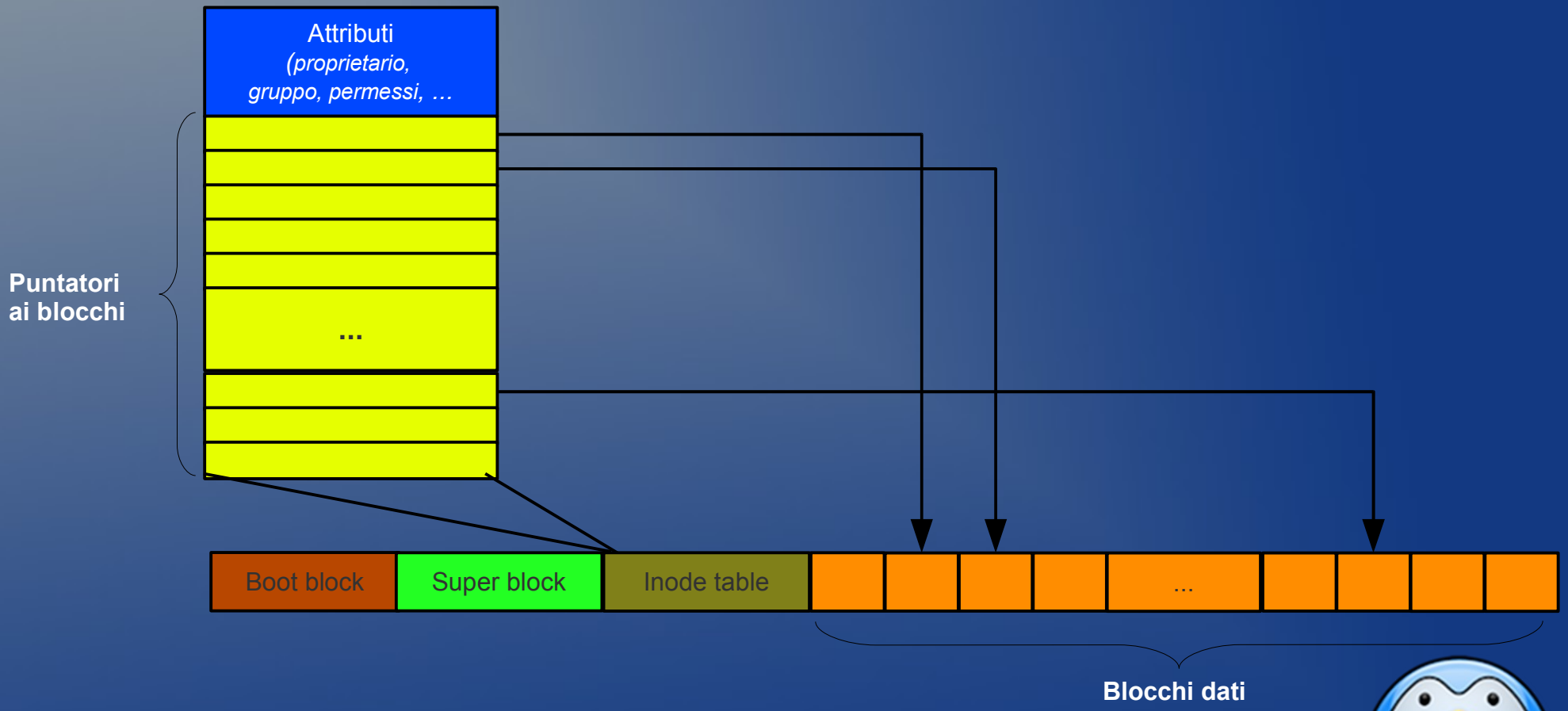
- Struttura di un file-system
- Cancellazione logica vs cancellazione sicura
- ext3secdel

Struttura FS



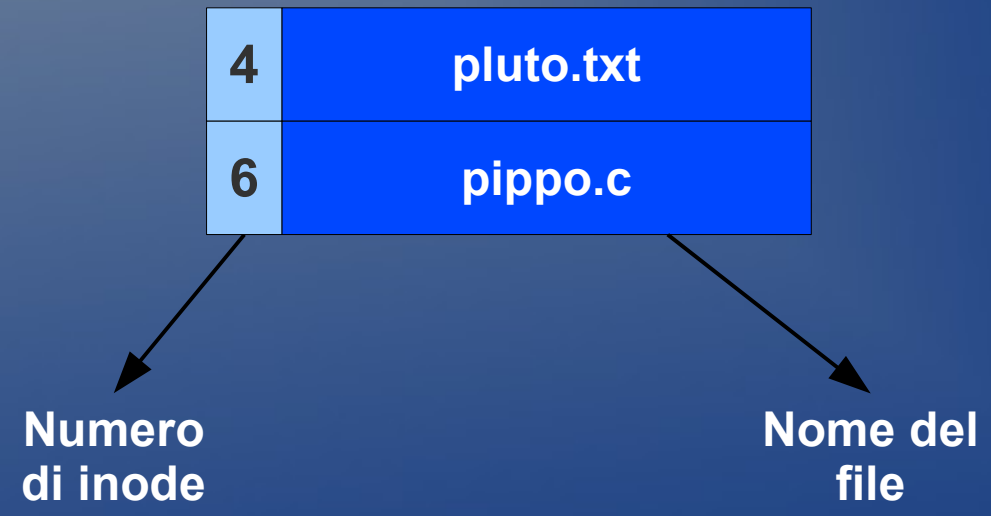

2009
LINUX
D A Y
I T A L I A

Inode


Attributi
(proprietario,
gruppo, permessi, ...
Puntatori
ai blocchi
...
Boot block
Super block
Inode table
...
Blocchi dati

Directory Entry

- Una directory è un file che contiene record chiamati directory entry:



Cancellazione logica

- Quando si cancella un file, il SO modifica solo il **minimo indispensabile** delle sue strutture per ragioni di efficenza
- Vale a dire:
  - Elimina la **directory entry** (il file non è più raggiungibile dall'utente tramite un nome)
  - Marca l'inode e i blocchi come liberi

Conseguenze

- I blocchi dati non sono stati toccati e il loro contenuto è ipoteticamente (e praticamente) ancora accessibile
- Questa situazione permane finchè quei blocchi non vengono assegnati ad un nuovo file e quindi sovrascritti con i dati di questo nuovo file

Cancellazione sicura

Cancellare un file in modo che il suo contenuto non possa essere più recuperato

Sovrascrivere i blocchi dati al momento della cancellazione

Cancellazione sicura

- Problema
  - Come sovrascrivere i blocchi in modo sicuro?
- Ossia
  - Con che valori sovrascrivere i blocchi? (zero?)
  - Quante volte deve essere sovrascritto un blocco?

Cancellazione sicura

- **NIST** (National Institute of Standard and Technology)
  - I dischi magnetici devono essere sovrascritti almeno 3 volte
- **NISPOM** (National Industrial Security Program Operating Manual)
  - Espone alcuni pattern di sovrascrittura >>

Alcuni metodi di sovrascrittura

- Sovrascrivere tutte le locazioni con un carattere
- Sovrascrivere tutte le locazioni con un carattere e il suo complemento
- Sovrascrivere tutte le locazioni con un carattere, il suo complemento, e poi un carattere random

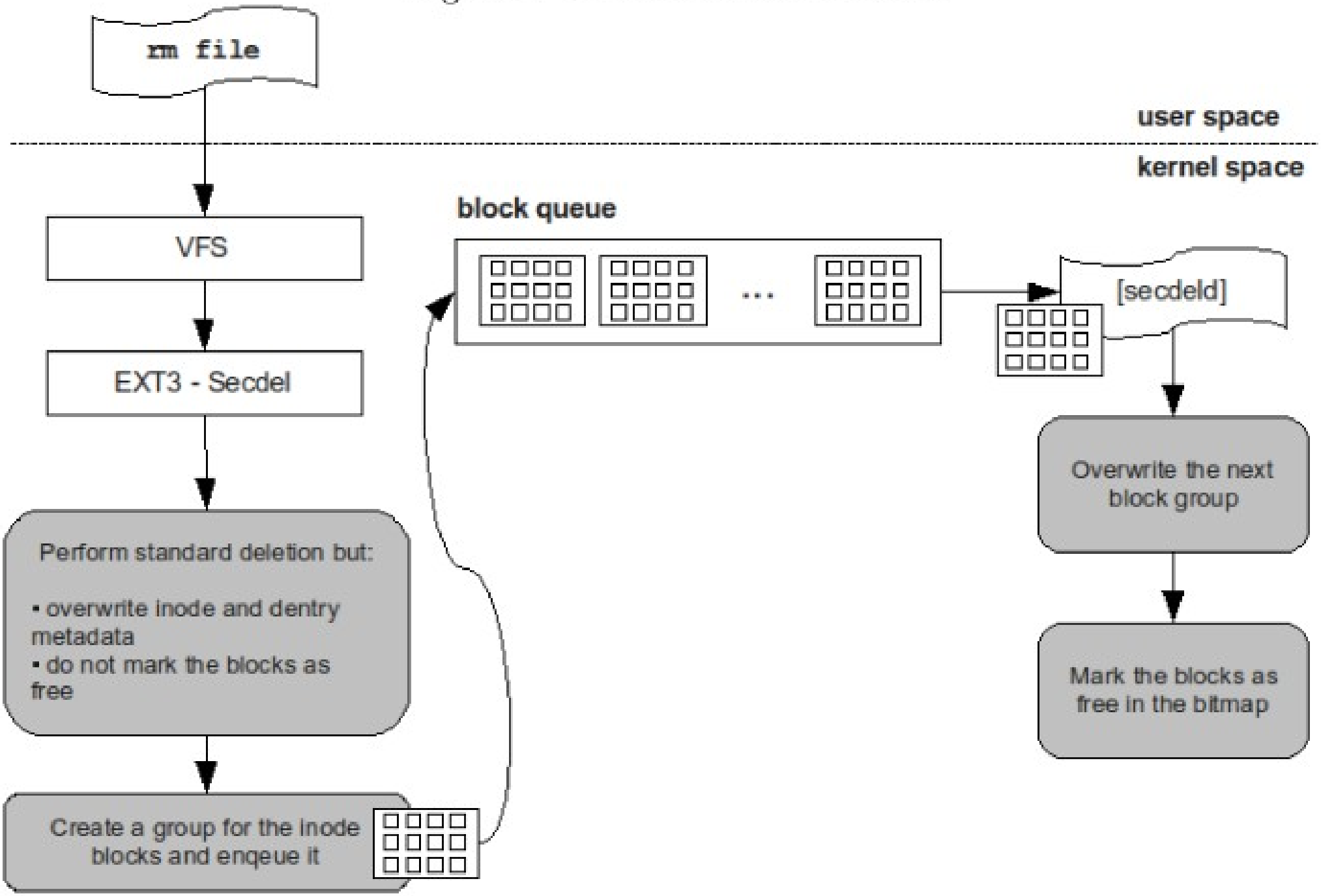
ext3secdel

- Patch *sperimentale* per ext3 che implementa la **cancellazione sicura asincrona** a livello di file-system
  - http://sourceforge.net/projects/ext3secdel/
- Sviluppata nell'ambito di un progetto universitario
- Testata sulla versione di ext3 distribuita col **kernel 2.6.29**

Architettura

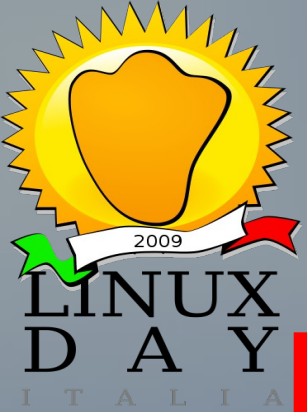
- La sovrascrittura dei blocchi non viene effettuata all'atto della cancellazione del file
- Un kernel thread, **secdeld**, si occupa di portare a termine la sovrascrittura dei blocchi in background
  - piccolo impatto sulle prestazioni globali

Figure 1: Ext3Secdel Architecture



Passi per la sperimentazione

- Al momento, non è consigliabile utilizzare ext3secdel col filesystem di root
- Inoltre, è necessario che ext3secdel sia compilato come modulo
- Passi:
  - Applicare la patch al kernel 2.6.29
  - Preparare il filesystem
  - Montare il filesystem con l'opzione secdel

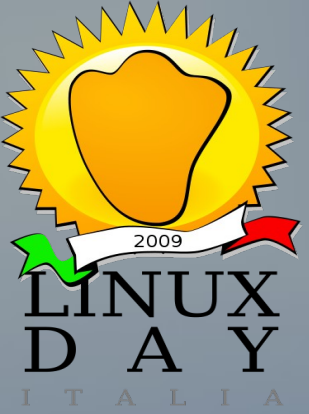


Preparazione del filesystem

- Prima di montare un filesystem ext3 con ext3secdel, è necessario eseguire il comando fsck.secdel che preparerà opportunamente il filesystem creando le strutture per contenere il journal di secdel:
-
```
# fsck.secdel /dev/sda3
Reserved inode not initialized, initializing
it...
```

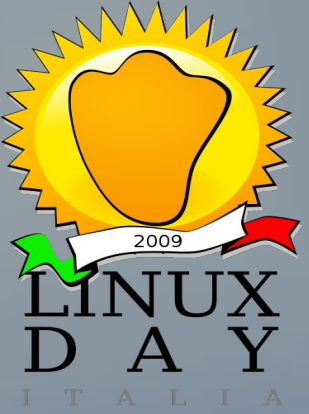

Abilitare la patch

- La patch può essere abilitata a tempo di montaggio passando l'opzione **secdel**:
  - `# mount -t ext3 -o secdel=205 /dev/sdb1 /mnt/secure`
- 205 indica la modalità di sovrascittura
- E' possibile modificare la modalità di sovrascrittura ricorrendo al comando **ext3_secdel_mode**



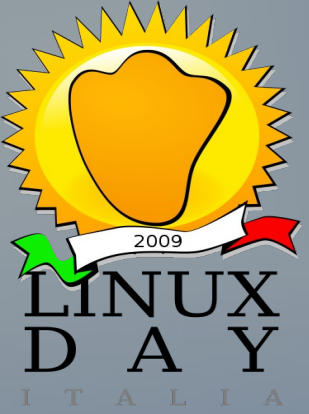
Modalità di sovrascrittura

- Numero di 3 cifre (oppure 0, se si desidera disabilitare la patch)
- La prima indica il pattern di sovrascrittura:
  - **1**: Zero
  - **2**: Zero-Uno
  - **3**: Zero-Uno-Random
- Le altre due il numero di passate (1-99)



ext3_secdel_mode

```
# ext3_secdel_mode sdb1 status
status Secure deletion on, zero-one
overwrite, 5 passes.
Pending operations:  0.
```



ext3_secdel_mode

```
# ext3_secdel_mode sdb1 on
Please select the overwrite mode:
   1) Zero
   2) Zero-One
   3) Zero-One-Rand
Please select one of the above(1-3): 3
Please specify the number of passes: 35
```

chattr +s

- Per marcare un file per la cancellazione sicura:
  - **$ chattr +s nome_file**
- Il comando lsattr, duale di chattr, mostra gli attributi dei file

Smontaggio

- Prima di smontare il filesystem, è necessario assicurarsi che non ci siano operazioni di cancellazione sicura ancora in corso, pena il crash di secdeld
- E' possibile controllare la presenza di operazioni pending col comando ext3_secdel_mode

Ext3secdel journal

- La patch ext3secdel mantiene un **journal** parallelo dedicato alla cancellazione sicura
- Se il sistema crasha, al prossimo riavvio, eseguendo il comando fsck.secdel prima dell'fsck.ext3 è possibile riprendere le cancellazioni sicure non completate

Call for developers

- Testing
- Realizzazione di ext3secdel come modulo indipendente da ext3
- Reingegnerizzazione (portare secdeld fuori dallo spazio kernel)

Baslug.org

Basilicata Linux Users Group

Presentato da: Donato Capitella
scorpio2002@baslug.org

Per Info e contatti: http://www.baslug.org