File Triggers

Nikhil Bobb, Scott Brandt, Carlos Maltzahn, Ethan Miller
MRAM Group
University of California, Santa Cruz

UC Santa Cruz

Storage Systems Research Center

Quick Triggers Review From Yesterday

- File Trigger: A small procedure that executes on a pre-designated filesystem call.
- Part of the LiFS (linking filesystem)
- Per file easy to use extensibility

Architecture

- File Trigger infrastructure composed of four parts:
  - File System Hooks
  - Trigger Controller
  - Behavior Interface
  - Behavior Module
    - a group of triggers which works together towards a specific end
    - stored in a dynamically loaded library.
- Example
  - Encryption
    - Read and write calls to file system encrypt and decrypt while reading and writing.

Behaviors

- Implemented
  - Snapshots (~120 lines of written C code)
- Possible
  - Intrusion Detection
  - Encryption
  - Mirroring, Backup
  - File level digital rights management
  - Indexing and Crawling
- Misuses
  - File level virus

Conclusions

- Lots more work to do
  - Protection
  - Composition
  - Performance