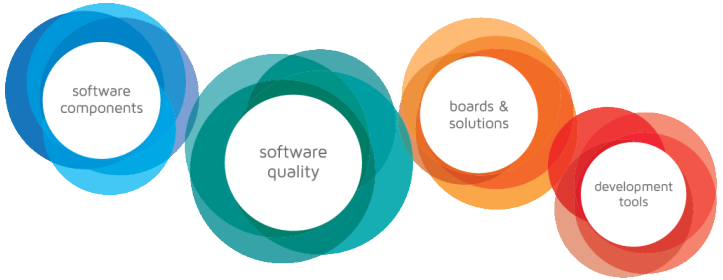
Securely erasing data in flash media

Tom Dohmen, Product Manager Reliable File Systems
Logic Technology

LOGIC TECHNOLOGY
There's always a Logic Solution!

Logic Technology

our mission: "to enable devlopers to create great products"



- Embedded specialist supplying the innovative European high-tech industry for more than 20 years.
- Our focus is on consulting and supplying, efficient and top quality embedded software, development- and test -tools, accompanied by customer centric service.

LOGIC TECHNOLOGY
There's always a Logic Solution!

People just don't understand that when you 'delete' something it is not necessarily 'erased'

Paul Henry - security & computer forensic expert

Survey

state of data security for embedded developers

- More complex – More data – More security
- Need for protection of critical/secure data will continue to grow
- Loss or corruption of data due to e.g. power loss
- Exposure of personal data while at rest or in flight

LOGIC TECHNOLOGY
There's always a Logic Solution!

Security Requirements

today's privacy and confidential requirements demand security

- Major Multi-Function Printer vendors defined a Protection Profile
- Concern for data exposed, remote or physical
- MFP vendors support a subset of IEEE2600-2008 which defines security requirements for HCD/MFP
  - 1.4 Offline salvage of deleted or stored user document data

LOGIC TECHNOLOGY
There's always a Logic Solution!

Topics

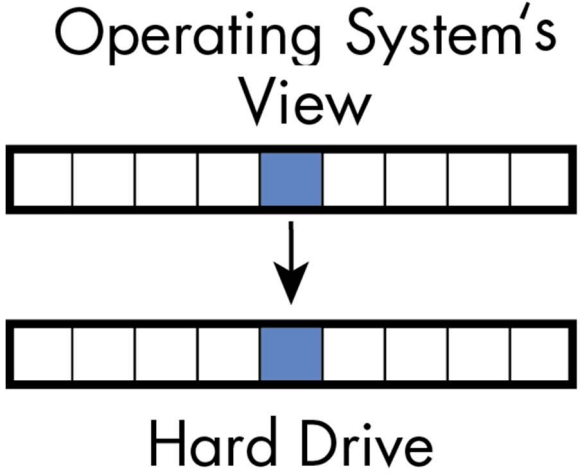
covered during this presentation:

- Erasing data on HDD
- Fundamentels of flash data storage
- Reliably erasing data on flash
- Secure operations available for eMMC
- Influence of the file system
- Performance impact of secure operations

Sanitization

erasing data so that it is difficult or impossible to recover

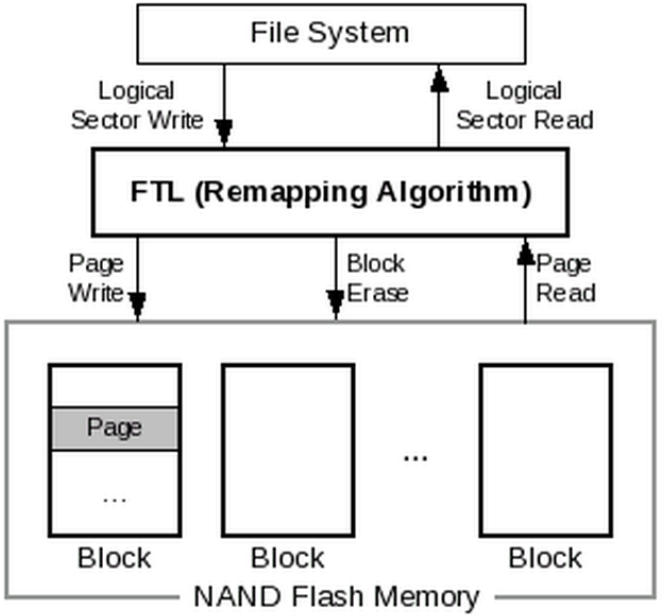
- Knowledge from years of research on hard drive
- Different sanitizing techniques for HHDs
- Flash is a different story



Flash memory

the next generation storage

- Non-volatile memory
- Flash media controller
- Flash Translation Layer (FTL)
- Most common



Erasing

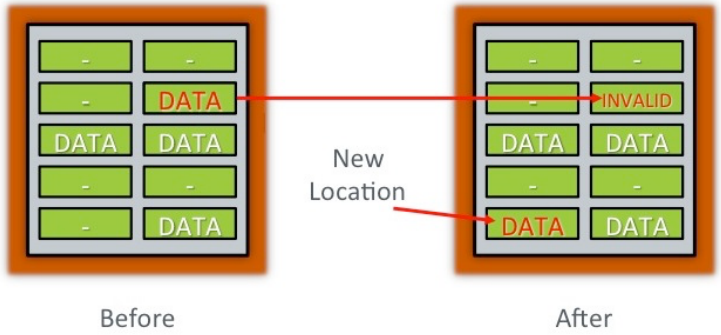
NAND flash memory

- Erase in large blocks
- Queued
- Discarded blocks

Writing

NAND flash memory

- Page write
- Only be written once
- Wear-leveling

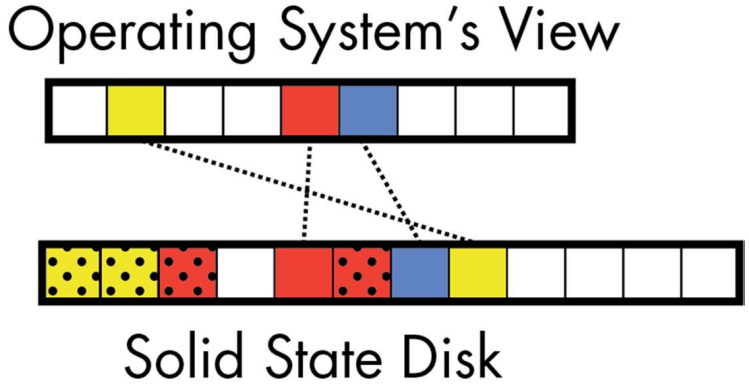


LOGIC TECHNOLOGY
There's always a Logic Solution!

Problem

older version of user data
Retained

- Logical view vs. Physical view
- Data intended to be secure



Retain data

on NAND flash

- Studies how NAND flash retains data
- Conclusions refer to SSD, but also apply to eMMC
- Test techniques and commands to securely remove data

CMRR
Center for Magnetic Recording Research

NVSL
Non-volatile Systems Laboratory

First conclusion

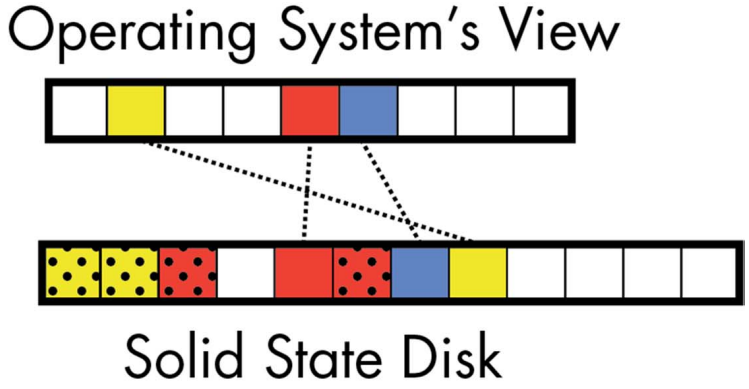
standard ATA secure erase methods are useless

- Overwrite with random data
- Useless for flash memory

Second conclusion

Flash Translation Layer required to be involved

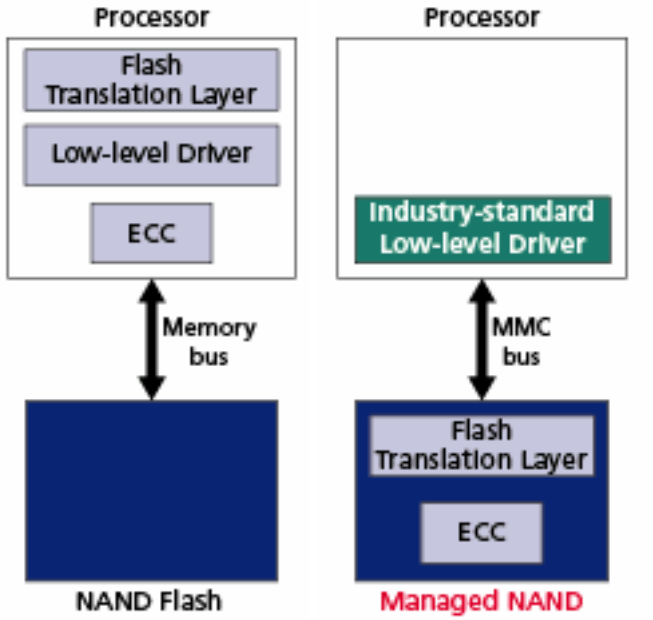
- Earlier copies stored
- Modifying FTL raw-flash
- Intelligent interfacing for managed-flash



eMMC

embedded multi media card

- JEDEC specification
- Managed NAND flash
- Growing in popularity



First option

for secure removal

- Secure Erase and Secure Trim
- Differ from basic commands
- Erase operation when command is issued

Second option

for secure removal

- Sanitize
- Erase / Trim commands
- Physically data removed that is no longer required
- Process can be slow

Secure Removal Type

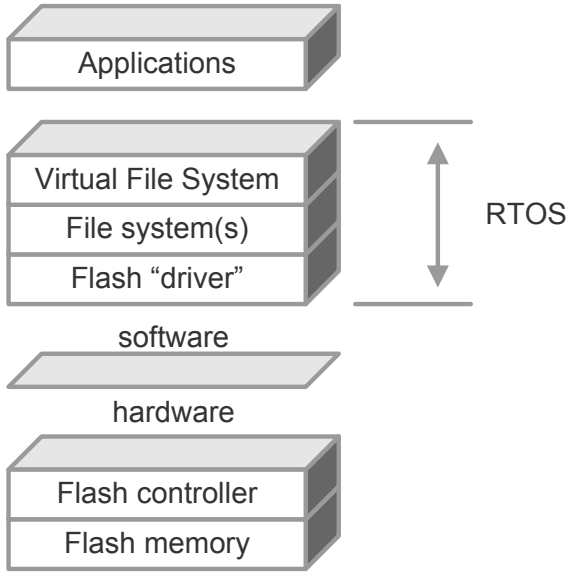
most recent revision of eMMC specification

- eMMC firmware allowed to decide
  - erase of physical memory
  - overwriting addressed location with a character, followed by an erase
  - overwriting addressed location with a character, its complement, and another random character
  - using a vendor-defined procedure

Application

knows which data is "secure"

- Rely on the file system
- Secondary copies of the data

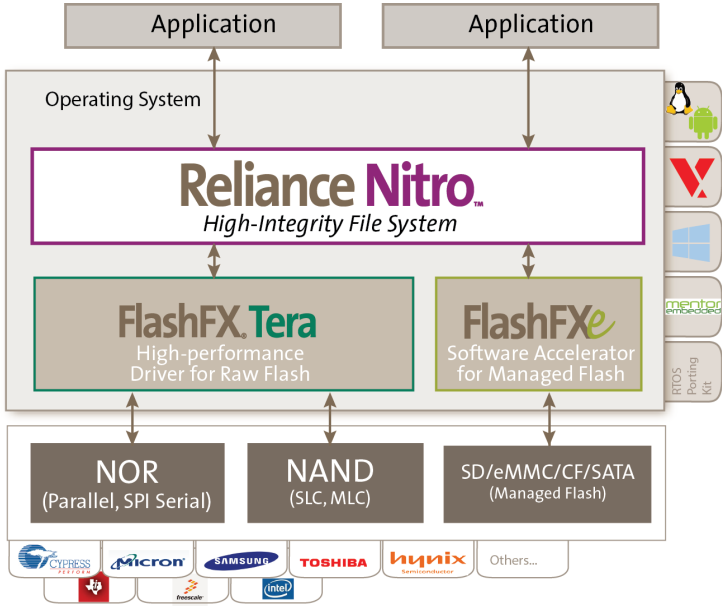


LOGIC TECHNOLOGY
There's always a Logic Solution!

Critical data

can be marked secure
by the file system

- Notify FTL to direct use of secure operations
- Datalight's Reliance Nitro
- Vendor MFP testing Reliance Nitro for IEEE2600



Measuring

time required to perform
Various secure operations

- Utilizing eMMC media on an i.MX6

Platform	MCIMX66Q-SDB (Freescale SABRE Board for Smart Devices)
Processor	i.MX6
Operating System	Windows Embedded Compact 2013
Software	Flash Command Tool from Datalight Common Libraries v3.8
Flash Media	Sandisk 8GB eMMC, Part #SDIN5C2-8G

Charts

- individual secure operations take longer than standard operations
- sanitize command took longer when performing more operations

Operation	Time
Discard	0.3 ms
Secure Trim	2.7 ms

Sectors Trimmed	Time
10	4 ms
13107	739 ms
477395	1124 ms

Understand

the use case for the device

- Control all media operations
- Other threads writing
- Superior solution to use individual secure operations

Secure operations

are designed to remove data from
the physical device immediately

- Security is a necessary component
- Full controlled use case -> sanitize and secure operations provide security on eMMC
- General use case -> utilize a file system controlling Secure Erase and Trim for best performance
- Datalight's Reliance Nitro provides control

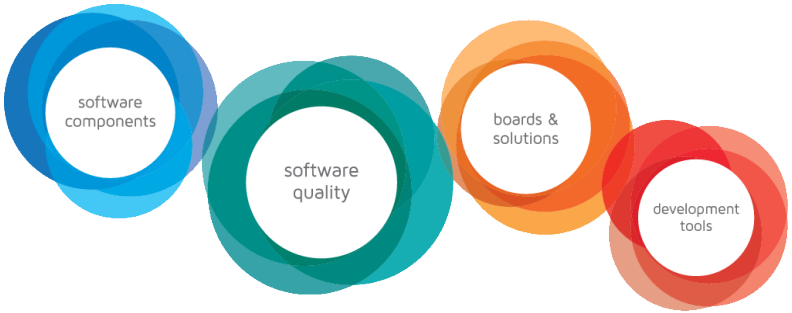
Datalight

keeping data reliable in over 300 million units across the embedded industry

- Offer flash memory drivers and file systems to improve the user's experience by boosting throughput, cutting file seek time, shortening boot time, and eliminating data corruption.
- Best-in-class, award winning customer support
- European partner Logic Technology

Questions?

LOGIC TECHNOLOGY
There's always a Logic Solution!



For more information and questions, visit www.logic.nl, contact me via t.dohmen@logic.nl, or just visit our booth!