

Seven Myths About SED

Dmitry Obukhov, SandForce Inc.

- Introduction
 - ▶ Evolution of self-encrypting drives
 - ▶ Architecture of self-encrypting drive
- Myths to be busted
 1. Drives are using weak algorithms
 2. Software-base disk encryption on SSD
 3. ATA Security is good enough
 4. Hardware encryption adds a lot of latency
 5. Opal is only for Windows
 6. TCG is all about TPM and DRM
 7. Vendors have backdoors in their products
- Conclusion

Evolution of self-encrypting drives

1st generation:

- Proprietary control mechanisms and protocols
- Proprietary encryption algorithms
- External crypto hardware (bridges), performance loss

2nd generation:

- Control mechanisms are based on standards (T13, T10, TCG)
- NIST-approved encryption algorithms (AES, SHA, HMAC, etc)
- Built-in encryption hardware, no performance loss

Samples available for OEMs

Products are on market

1st TCG Plugfest

2003

2004

2005

2006

2007

2008

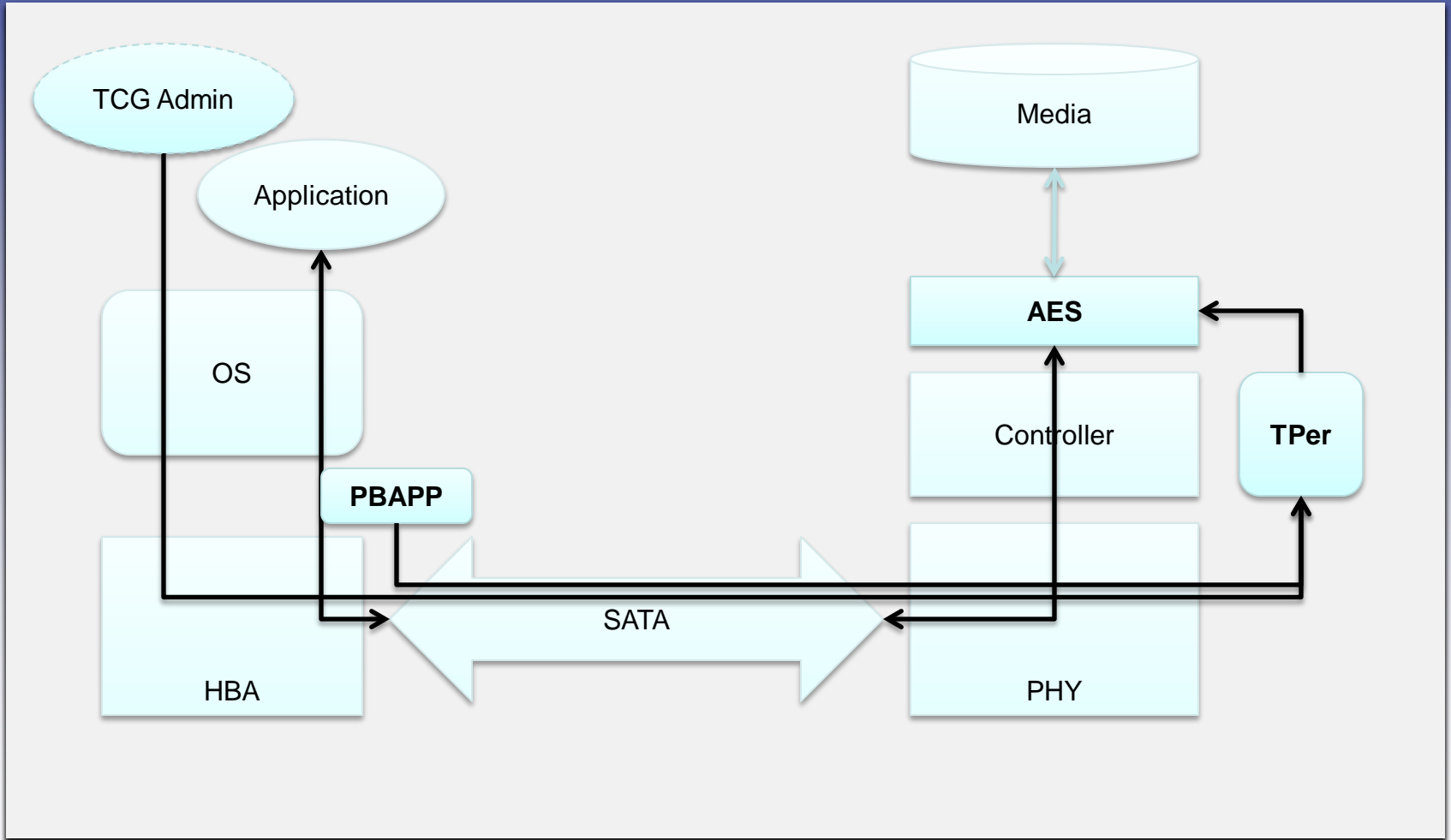
2009

2010

2011

2012

Architecture of SED



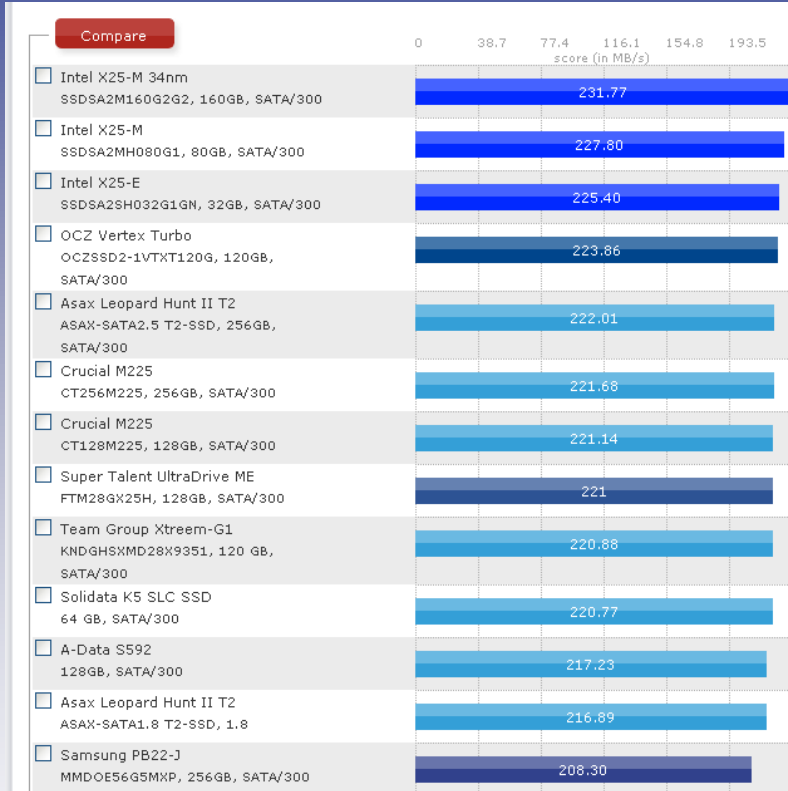
Myth 1: SED is using weak algorithms

- This is true statement for the 1st generation
 - ▶ External solutions (disk enclosures, bridging, etc)
 - ▶ In best cases matching USB speed
 - ▶ “Childhood disease”
- 2nd generation is using AES 128 or 256
 - ▶ AES hardware is simple
 - ▶ AES is very efficient
 - ▶ Required for FIPS certifications

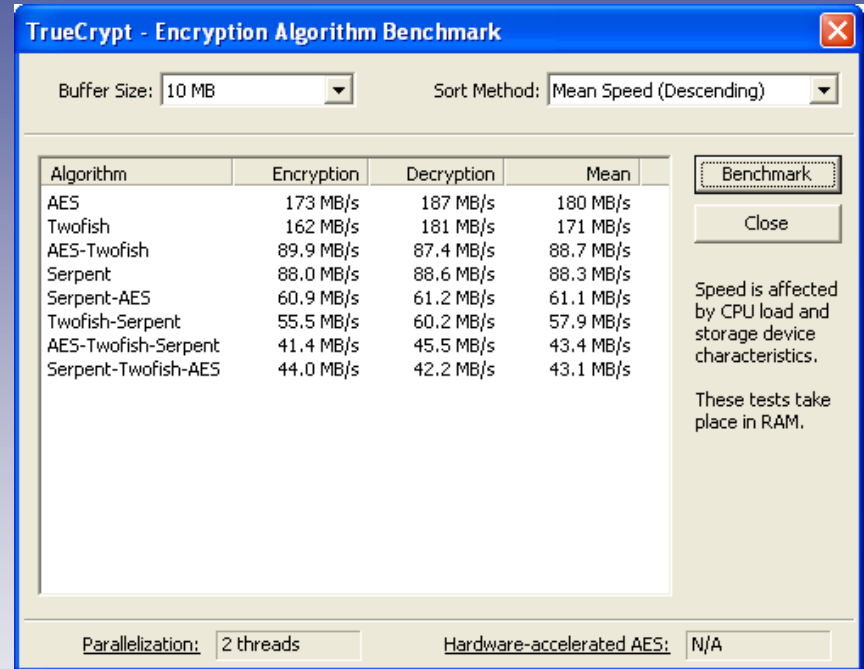
Myth 2: ATA security is enough

- ATA Security is no more than a sign.
 - ▶ There is no encryption in classical ATA security
 - ▶ “Master” passwords leaked on Internet
 - ▶ Data can be recovered by many data rescue companies
- Class 0 = ATA Security + Encryption
 - ▶ This might be enough for simple use cases
 - ▶ Inherited problems from ATA security
 - ▶ Not fully compatible with ATA specifications
 - ▶ Can be disabled by user (compliance problems)
- Not suitable for more complicated security use cases
 - ▶ No multiple users
 - ▶ No access right configuration
 - ▶ No security log
 - ▶ Notepad VS. Word

Myth 3: Software Encryption works better on SSD



231 MB/s [2]

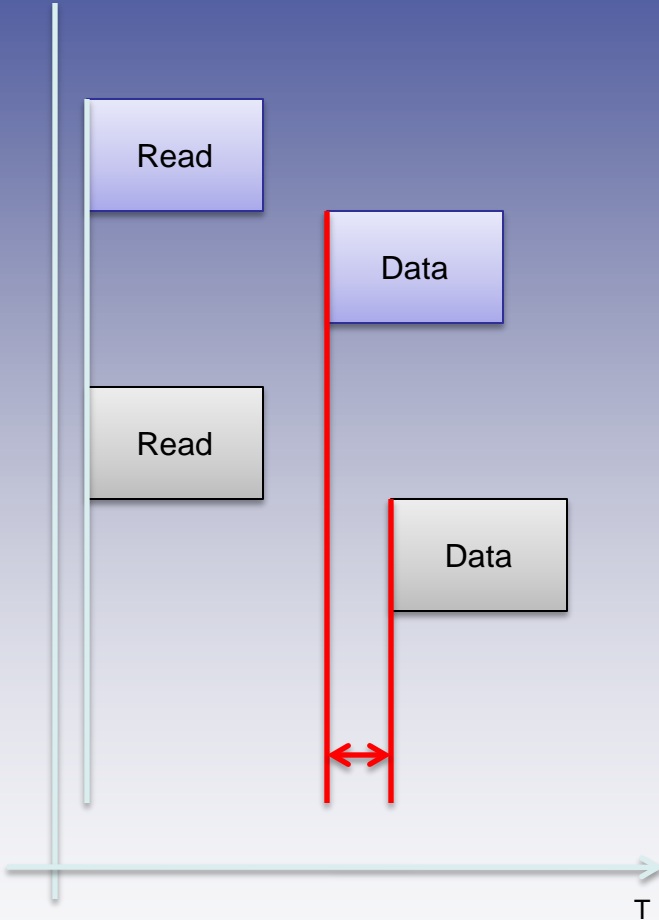


187 MB/s

Myth 3: Software encryption for SSD

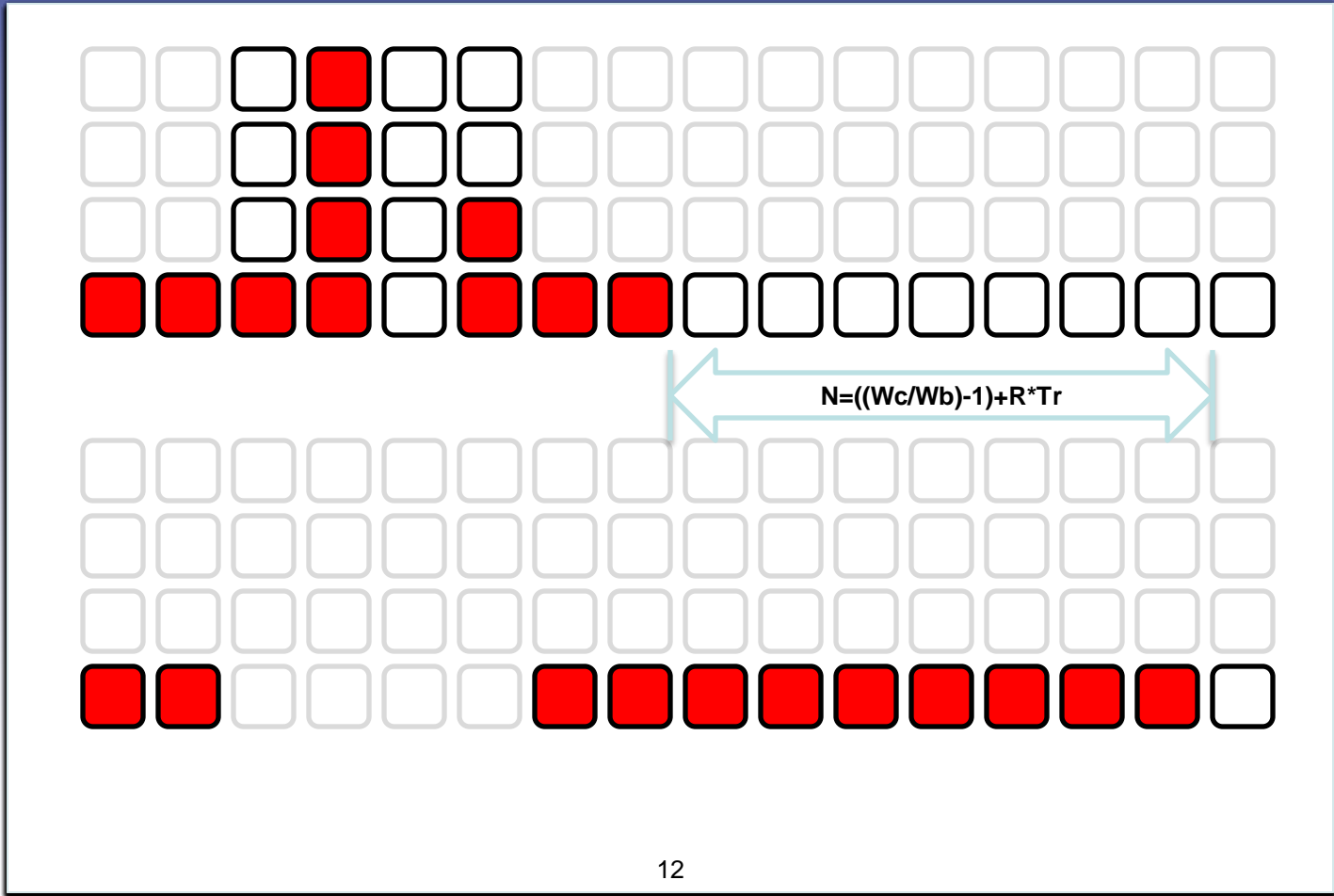
- Software encryption cost
 - AES: 21 clock/byte (Pentium, 512 byte/block)
 - Throughput: 231 MB/s
 - 5,083 MIPS for throughput encryption
- Comparable to overall power of mobile CPU
 - Netbooks: Atom 3,300 MIPS [3]
 - Easily can eat half of notebook CPU
- Hardware encryption
 - Zero CPU consumption
 - Scalable with throughput

Myth 4: Latency of SED



- There were a lot of speculations about latency
- Write latency – impossible to measure on host side
- Read latency – delta in response to read command

M4: Latency mechanism



M4: down to numbers

- Clock tick
 - ▶ 3Gb/S = 2.4Gb/S after 10 to 8 decoding
 - ▶ 0.4 nS per bit
 - ▶ 13 nS per 32-bit word
- Latency in clock cycles
 - ▶ 128 bit of AES block / 32 bit bus = 3 clocks
 - ▶ 14 rounds of AES 256
 - ▶ 17 clocks total
- Good news: **~221 nS** of total latency added
 - ▶ ~0.1-0.2% for SSD
 - ▶ 15K RPM HDD ~ 66 uS to position a sector
- Even better news: latency is scalable with interface speed
 - ▶ For 6G 1 clock is 6.5 nS, 17 clocks = 111 nS

Myth 5: TPM/DRM

- TPM might be used for DRM protection
- Many users don't like DRM

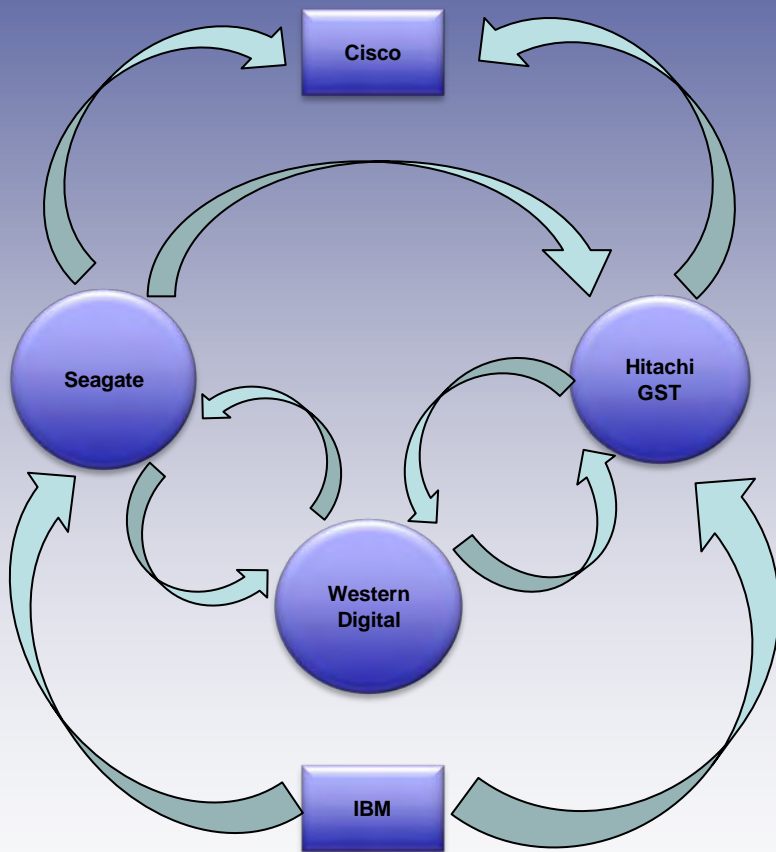
- But the fact is:
- **THERE IS NO TPM or DRM in TCG SPEC**

- TPM is a host security device
- Take a moment and read these specs

Myth 6: Opal is only for Windows

- There are 3 software components in security system:
 - ▶ Firmware – host independent
 - ▶ Pre-boot application – platform-specific (PC/Mac)
 - ▶ Configuration software – OS specific
- Configuration software
 - ▶ Supported OS: Windows XP, Vista, 7, Mac OS
 - ▶ Potential support: GRUB, Truecrypt, LUKS, CryptoFS
- Linux community is more than welcome to develop support for TCG drives
 - ▶ Protocols are free
 - ▶ Specifications are open and free
 - ▶ TCG Storage Workgroup will support this initiative

Myth 7: Backdoors and conspiracy theories



- There is no pressure to make backdoors from government agencies
- Failure analysis people are most interested in “debug features”
- There is no vendor that can afford such dirty secret as backdoor
 - Problems with FIPS certifications
 - Workforce dynamics (LinkedIn research)

1. AES Performance Comparisons, Bruce Schneier
2. <http://www.tomshardware.com/charts/2009-flash-ssd-charts/Read-Throughput-h2benchw-3.12,906.html>
3. http://en.wikipedia.org/wiki/Intel_Atom