Self-Encrypting Drives for Data Protection: The Industry’s First Forecast with Thoughts on Usage

Brian Berger, Director, Trusted Computing Group
Tom Coughlin, President, Coughlin Associates
Welcome and Introduction

- Self-encrypting hard disk drives were initially introduced in 2007. These initial products were called Full Disk Encryption (FDE) drives. FDE drives were introduced by Seagate in advance of a SED standard from the Trusted Computing Group (TCG), a consortium of HDD, SDD, electronics, OEM, software and other interested companies whose Storage Work Group was tasked with creating universal standards for storage devices with internal hardware based encryption—often called Hardware (HW) Encryption. Storage devices with HW encryption, where the encryption key never leaves the storage devices and where encryption and decryption of data are handled by the storage device electronics independently of the host, are called Self-Encrypting Drives or Devices (SEDs).

- Hardware encryption is contrasted with Software (SW) encryption which runs the encryption software and accesses the encryption keys off of the storage devices. HW encryption runs entirely on the digital storage device and the encryption key never leaves the storage device.

- All sorts of storage devices can be SEDs. The Trusted Computing Group has standards for internal encryption of hard disk drives, optical disc storage, as well as NAND flash storage devices such as Solid-State Drives (SSDs).

- In July and August 2011, in cooperation with members of the Trusted Computing Group and its Storage Work Group, Coughlin Associates conducted a survey of a number of interested parties to the use of encryption to provide security in various types of electronic equipment that use storage devices. Those interviewed included storage device suppliers (hard disk drives and solid state drives), systems OEMs, security software companies, storage controller suppliers and others.
Webcast Logistics

No Sound?
Check to be sure that you have dialed into the audio portion:
Participant Passcode: 2402551
Press *0 to reach an operator if still experiencing difficulties

Questions?
Pose a written question to our speaker or moderator throughout the webcast:
Select the question mark icon (??) on the primary navigation bar
Type your question
Watch and/or listen for a response

Webcast Archive Availability?
Webcast to be available for viewing within 5-7 business days at:
http://www.trustedcomputinggroup.org/resources/selfencrypting_drive_market_and_technology_report
Tom Coughlin, President, Coughlin Associates is a widely respected storage analyst and consultant. He has over 30 years in the data storage industry with multiple engineering and management positions at high profile companies.

Dr. Coughlin has many publications and six patents to his credit. Tom is also the author of Digital Storage in Consumer Electronics: The Essential Guide, which was published by Newnes Press. Coughlin Associates provides market and technology analysis (including reports on several digital storage technologies and applications and a newsletter) as well as Data Storage Technical Consulting services. Tom is publishes a Digital Storage in Consumer Electronics Report, a Media and Entertainment Storage Report, and a Capital Equipment and Technology Report for the Hard Disk Drive Industry.

Tom is active with SMPTE, SNIA, IDEMA, the IEEE Magnetics Society, IEEE CE Society, and other professional organizations. Tom is the founder and organizer of the Annual Storage Visions Conference (www.storagevisions.com), a partner to the International Consumer Electronics Show, as well as the Creative Storage Conference (www.creativestorage.org). He is also a Senior member of the IEEE, Leader in the Gerson Lehrman Group Councils of Advisors and a member of the Consultants Network of Silicon Valley (CNSV). For more information on Tom Coughlin and his publications. go to www.tomcoughlin.com.
SELF-ENCRYPTING DRIVES FOR DATA PROTECTION: THE INDUSTRY’S FIRST FORECAST WITH THOUGHTS ON USAGE

Tom Coughlin, President, Coughlin Associates
www.tomcoughlin.com
Outline

- Factors that led to slow market adoption of SEDs
- Factors favoring future growth of SEDs
- Comparison of SW and HW (SED) encryption
- Market Projection Methodology
- HDD SED Projections
- SSD SED Projections
- Conclusions
- References and Sources
Factors That Led to Slow Market Adoption of Self-Encrypted Storage Devices

• Higher costs/prices for initial SEDs,
• Slow corporate IT spending due to economic disruptions and uncertainty in the last few years,
• Lack of knowledge about the difference between HW based encrypted SEDs and SW encrypted solutions,
• Lack of training of OEMs and integrators on the use and advantages of SEDs,
• Issues limiting the use of encrypted drives in some countries,
• A limited initial market mainly driven by government mandates and,
• Until recently, a lack of common standards and a continuing lack of product certification.
Factors Favoring Future Growth of Self-Encrypted Storage Devices

- The approach to cost parity of SEDs to non-self-encrypting storage devices will make it easier to get these products adopted universally.
- SEDs have no discernable encryption time (unlike SW encryption).
- SEDs don’t have the performance overhead that SW encryption running on the host has, leading to better overall system performance.
- SEDs may have a somewhat longer useful life than drives used in a software encrypted system (more reads and writes with SW encryption).
- Because the encryption key is stored on the storage device, it cannot be accessed through host hacking, like SW encryption can.
- SEDs allow simpler storage array encryption solutions.
- Government mandates and regulations increase the requirements for privacy and favor the use of SEDs, (esp. with FIPS 140 certification).
- Crypto-erase is the only effective way to make data on a SSD inaccessible.
HDD Encryption Throughput Test Results
(extracted from 2010 Trusted Strategies Report)

<table>
<thead>
<tr>
<th></th>
<th>No Encryption</th>
<th>Seagate SED HDD</th>
<th>SW Encryption Avg.</th>
<th>SW Encryption 1</th>
<th>SW Encryption 2</th>
<th>SW Encryption 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start-up Throughput (MB/s)</td>
<td>7.9</td>
<td>8.0</td>
<td>7.7</td>
<td>7.9</td>
<td>7.8</td>
<td>7.5</td>
</tr>
<tr>
<td>Application Loading (MB/s)</td>
<td>5.9</td>
<td>5.7</td>
<td>5.5</td>
<td>5.6</td>
<td>5.5</td>
<td>5.4</td>
</tr>
<tr>
<td>Modest Size File Test (MB/s)</td>
<td>5.4</td>
<td>5.3</td>
<td>5.1</td>
<td>5.1</td>
<td>5.2</td>
<td>5.1</td>
</tr>
<tr>
<td>Extensive Data Read (MB/s)</td>
<td>80.2</td>
<td>82.8</td>
<td>38.6</td>
<td>46.3</td>
<td>35.6</td>
<td>33.8</td>
</tr>
<tr>
<td>Extensive Data Write (MB/s)</td>
<td>50.7</td>
<td>50.3</td>
<td>35.2</td>
<td>39.1</td>
<td>31.4</td>
<td>34.9</td>
</tr>
</tbody>
</table>

- The software packages that were tested and compared to the Seagate SED were McAfee Endpoint Encryption for PC, version 5.2.3; PGP Whole Disk Encryption for Windows, corporate desktop version, release 9.12; and Microsoft Bitlocker, Windows Vista Ultimate, SP2.

- HW and SW encryption was tested using PCMark Vantage Professional edition mostly using the hard disk drive test suite. Identical 32 bit Dell Latitude E6400 laptops running Microsoft Windows Vista Ultimate, service pack 2, with Intel Core 2 Duo Processors and 2 GB of RAM were used for the comparison testing.
SSD Encryption Throughput Test Results (extracted from 2010 Trusted Strategies Report)

<table>
<thead>
<tr>
<th></th>
<th>Samsung SSD, No Encryption</th>
<th>Samsung SSD with SW Encryption</th>
<th>Samsung SED SSD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start-up Throughput (MB/s)</td>
<td>82.50</td>
<td>47.90</td>
<td>95.33</td>
</tr>
<tr>
<td>Application Loading (MB/s)</td>
<td>48.33</td>
<td>30.77</td>
<td>60.37</td>
</tr>
<tr>
<td>Modest Size File Test (MB/s)</td>
<td>41.13</td>
<td>26.77</td>
<td>50.40</td>
</tr>
<tr>
<td>Large Scale Data Read (MB/s)</td>
<td>178.00</td>
<td>70.23</td>
<td>169.33</td>
</tr>
<tr>
<td>Large Scale D Write (MB/s)</td>
<td>170.80</td>
<td>63.60</td>
<td>164.50</td>
</tr>
<tr>
<td>Random R/W (MB/s)</td>
<td>54.77</td>
<td>29.57</td>
<td>54.50</td>
</tr>
</tbody>
</table>

- There was no observable performance penalty for the SEDs, in fact they performed faster than the non-encrypted drives (for some reason).
- SED drives (as well as the non encrypted drives) had significantly higher performance than the SW encrypted SSDs.
Encryption Throughput Test Results and Other Consequences

• The SED gave a 115% higher read throughput than the average of the SW encryption products and 43% higher write throughput.

• SEDs allow a quicker implement of an encrypted data solution than SW encryption. The lower performance overhead (and thus improved system performance) as well as elimination of any encryption time for a new storage device can offer considerable ROI advantages for SEDs (HW encryption) over SW encryption.

• These advantages would also scale from individual host systems to virtualization environments, making SEDs better storage devices for use in cloud storage environments where data security is important.

• In my interviews with OEMs and suppliers, it was mentioned that a 10-15% loss in effective life of storage devices may be a result of SW encryption vs. SED HW encryption.
Market Projection Assumptions (1)

• Two types of projections for given market segments and for HDDs and SSDs as a whole.
  - The first projection will be for the growth of SED- encryption-based security adoption in terms of drive units.
  - The second projection will be for the implementation of SED capability in drives for that market segment in terms of drive units.
  - We call these two projections Security Adoption and SED Capability respectively.

• The actual modeling methodology will assume that Security adoption (the use of SED drives for encryption based security) will follow an S-shaped adoption curve. Because of some intrinsic adoption issues for encryption-based security in some geographic regions, the maximum security adoption will not be 100% of all the drives produced.
Market Projection Assumptions (2)

- In February 2011, Seagate announced that it had shipped more than 1 M self-encrypting HDDs into the laptop and enterprise markets.
- Seagate introduced their laptop SEDs in 2007 and their enterprise SEDs in 2009.
- Other companies that have shipped SEDs include Hitachi (announced in 2007) and Fujitsu (announced in 2008, note that Fujitsu ‘s hard disk division is now part of Toshiba).
- Hitachi also announced 3.5-inch SED HDDs for desktop PCs in 2008. Toshiba announced an SED HDD in 2011.
- Samsung announced an SED SSD in 2011. Micron also announced an SED SSD in 2011.
- Western Digital has not announced shipping SED drives as of the date of this report.
- By the end of 2010, we estimate that a total of about 1.2 M SED HDDs shipped, mostly for laptop and some for desktop and enterprise applications.
We use an equation for the cumulative fraction of adopters at time $t$, $F(t)$, where $p$ is the so-called innovation factor and $q$ is the imitation factor.

$$F(t) = \frac{1 - e^{-(p+q)t}}{1 + \left(\frac{q}{p}\right)e^{-(p+q)t}}$$
Banded Hard Drive Volume Projections
Security Adoption for Laptop HDDs

- High Security Laptops
- Mean Security Laptops
- Low Security Laptops

Million Units Shipped

Security Adoption for Enterprise HDDs

Million Units Shipped

- High Security Enterprise
- Mean Security Enterprise
- Low Security Enterprise

Security Adoption for Desktop HDDs

Million Units Shipped

- High Security Desktop
- Mean Security Desktop
- Low Security Desktop

Security Adoption for CE HDDs

- High Security CE
- Mean Security CE
- Low Security CE

Million Units Shipped

Median Security Adoption for all HDDs Market Segments

- CE
- Desktop
- Enterprise
- Laptop

Million Units Shipped

Security Adoption SED HDD Estimates (high, median and low)

Million Units Shipped

- High
- Median
- Low

HDD SED Conclusions

• **It is likely that by about 2017 all HDDs will shift to SED capable units, although estimated security adoption units by 2016 (SED capable HDDs actually used or intended for data security) are about 25% of all HDDs shipped.**

• Factors that could accelerate *security adoption* and SED capability in HDDs:
  - if HDD controller makers move to incorporate SED capability into standard HDDs the shift to SED capable units could happen much quicker than this. If this happened it would also be part of a significant cost reduction for SEDs and would probably accelerate *security adoption* with SEDs as well.
  - increased publicity to susceptible mid-market users, especially with increasing amounts of government privacy regulation could increase *security adoption*. 
SSD SED Considerations

- SSDs by their very architecture do not know if there is unerased content in the device, unlike HDDs. Providing encrypted data on the SSD where the key is within the device allows erasing the encryption key and making the data unavailable to others—a crypto-erase. This feature will be popular for many users even if they don’t use the SED features on a day to day basis, since drives can be reused without fear that the data is available to a new user after the internal encryption key is erased.
SSD Annual Shipped Unit Projections

<table>
<thead>
<tr>
<th>Year</th>
<th>Financial and POS</th>
<th>Servers</th>
<th>Notebook PC</th>
<th>Cellular Base Station</th>
<th>Set Top Box</th>
<th>Desktop PC</th>
<th>Switch &amp; Rounter</th>
<th>Test &amp; Measurement</th>
<th>Process Control</th>
<th>Military &amp; Aerospace</th>
<th>NAS and SAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Millions of Units

High/median/low SSD Estimates

- High
- Median
- Low

Year:
- 2009
- 2010
- 2011
- 2012
- 2013
- 2014
- 2015
- 2016

Values:
- 0
- 20
- 40
- 60
- 80
- 100
- 120
- 140
- 160
We project that within 2 years (by 2013) SED capability will be in over 80% of SSDs and likely in almost all SSDs within 3 years (2014).
Conclusions

• It is likely that by about 2017 all HDDs will shift to SED capable units, although estimated security adoption units by 2016 (SED capable HDDs actually used or intended for data security) are only 25% of all HDDs shipped.

• By 2016 the high, median and low estimates for security adoption for SED HDDs are 411M, 315M and 122M units.

• We project that within 2 years (by 2013) SED capability will be in over 80% of SSDs and likely in almost all SSDs within 3 years (2014).

• Although actual SSD SED feature implementation in 2016 is likely to be about 122M SSDs, the projected actual SSDs from that year used for security and data protection purposes is estimated at less than 18M units.
Sources and References

- Trusted Platform Module (TPM) Adoption Dynamics, IDC, 2006
- Trusted Computing is Real and it’s Here, Endpoint Technologies Associates, 2007
- Perceptions about Self-Encrypting Drives: A Study of IT Partitioners, Ponemon Institute, 2011.
- Reliably Erasing data from Flash-Based Solid State Drives, M. Wei et. al, Presented at Fast 2011
- Based upon discussions with encryption and SED experts during the course of this research
- Solid State Drives: Outlook 2010, Objective Analysis, 2010
Questions?

Trusted Computing Group
www.trustedcomputinggroup.org
Tel: 503.619.0562
3855 SW 153rd Drive Beaverton, OR 97006
admin@trustedcomputinggroup.org

Coughlin Associates
www.tomcoughlin.com
Tel: 408.978.8184
9460 Carmel Road Atascadero, CA 93422
info@tomcoughlin.com
More Information

- For a copy of the full report, Self-Encrypting Drive Market & Technology Report, please visit:

- For more information on Self-encrypting Drives and the work of the Trusted Computing Group, please visit:
  - Executive Summary – Self-Encrypting Drive Market & Technology Report: [www.trustedcomputinggroup.org/resources/selfencrypting_drive_market_and_technology_report](http://www.trustedcomputinggroup.org/resources/selfencrypting_drive_market_and_technology_report)
  - Data Protection/SED Solutions: [www.trustedcomputinggroup.org/solutions/data_protection](http://www.trustedcomputinggroup.org/solutions/data_protection)