Solid Security: The Rise of Self-Encrypting Solid State Drives

Thomas Coughlin

Marketing Chair, SNIA Solid State Storage Initiative
President, Coughlin Associates

About the Presenter

Tom Coughlin, Marketing Chair, SNIA Solid State Storage Initiative, and 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. In addition to consulting, Dr. Coughlin publishes reports and a newsletter and organizes several conferences.

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). For more information on Tom Coughlin and his publications. go to www.tomcoughlin.com.

Outline

- Why Do we Need Self Encrypting Solid State Drives?
- TCG Market Report on SEDs
- 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 (Summary)
- SSD SED Projections
- Conclusions
- References and Sources

Why Do We Need Self Encrypting Drives (1)

- Data security is the biggest reason for self-encrypting drives (SEDs)
- Data security can be compromised by lost or stolen desktop and laptop computers and external storage devices that are not properly protected—a password on a computer is not enough!
- Data security can be compromised by poorly protected storage devices that are given away or sold to others—deleting files is not enough and erasure techniques may not be done properly
- Software-based encryption methods have additional overhead that impacts overall storage system performance

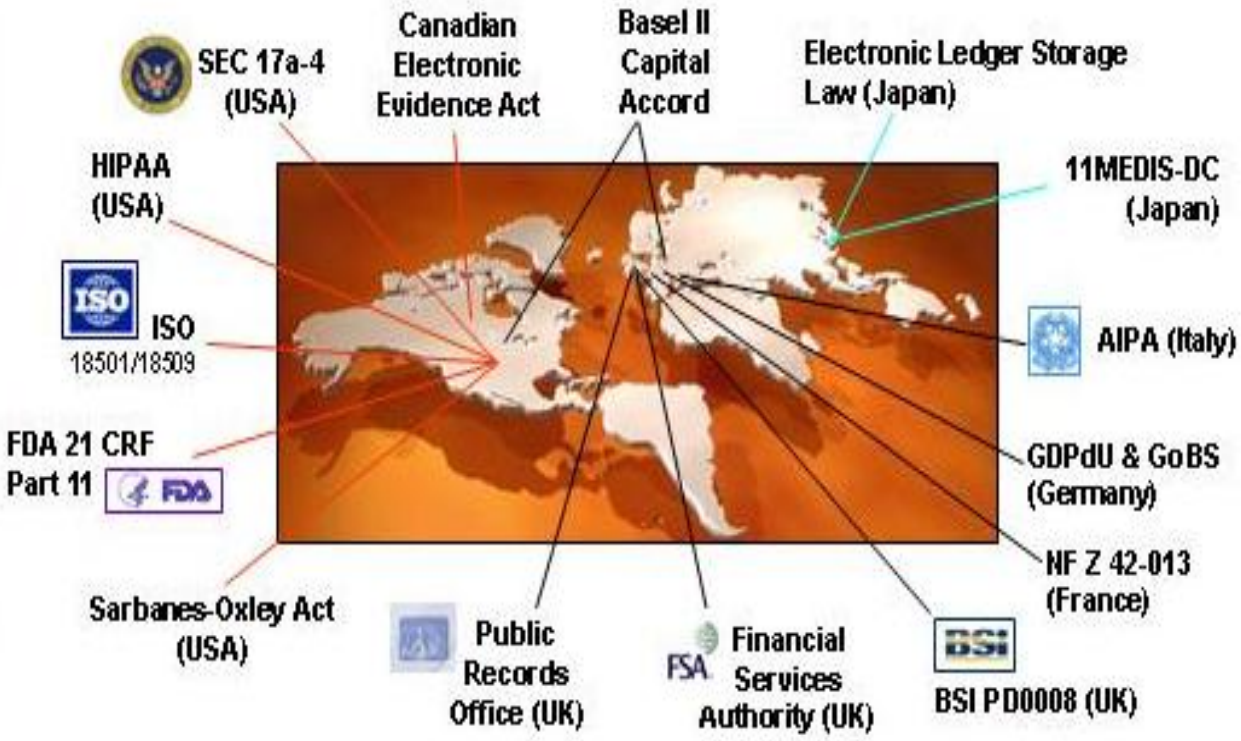
Why Do We Need Self Encrypting Drives (2)

SNIA
Advancing storage & information technology

Some statistics:

- Since 2005, well over 345 M records containing sensitive personal information have been involved in security breaches
- In 2008, the average cost of a data breach was $6.65 million per affected corporation ($202 per record)
- 50,000 drives leave data centers daily
- 90% of retired drives are still readable (IBM study)

Why Do We Need Self Encrypting Drives (3)



Worldwide regulations for data protection and privacy compliance are creating significant legal and financial incentives to encrypt data stored on storage devices and data centers

- 46+ states have data privacy laws with encryption "safe harbors" which exempt encrypted data from breach notification

TCG Market Report on Self-Encrypted Drives (SEDs)

SNIA
Advancing storage & information technology

- In July and August 2011, in cooperation with members of the Trusted Computing Group storage working 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.
- Based upon input from the interviews we created a list of drivers for the use of self-encrypting drives (SEDs) as well as factors that limit their use in the market, both historically as well as in the near future.
- In this report we examine each of these positive and negative factors and look at their historical impact on the SED market and the implications of these factors in the future growth of SEDs, both HDDs and SSDs.

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 limits their growth
- 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
- With SEDs there is no discernable encryption time like there is with 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, due to increased reads and writes with SW encryption

Factors Favoring Future Growth of Self-Encrypted Storage Devices (2)

- Because the encryption key is stored on the storage device, it cannot be accessed through host hacking, like SW encryption can
- SEDs are less complex to implement in storage array encryption solutions
- Government mandates and regulations are increasing the requirements for privacy and favor the use of SEDs, particularly those with FIPS 140 certification
- Crypto-erase is the only effective way to make data on a SSD inaccessible

Encryption Throughput Test Results

- 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.

Encryption Throughput Test Results (2)

- 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 SSDs as a whole.
  - The first projection will be for the growth of SED- encryption-based security in terms of drive units.
  - The second projection will be for the adoption of SED capability in drives for that market segment in terms of drive units.
  - We call these two projections **Security** and **SED adoption** 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)

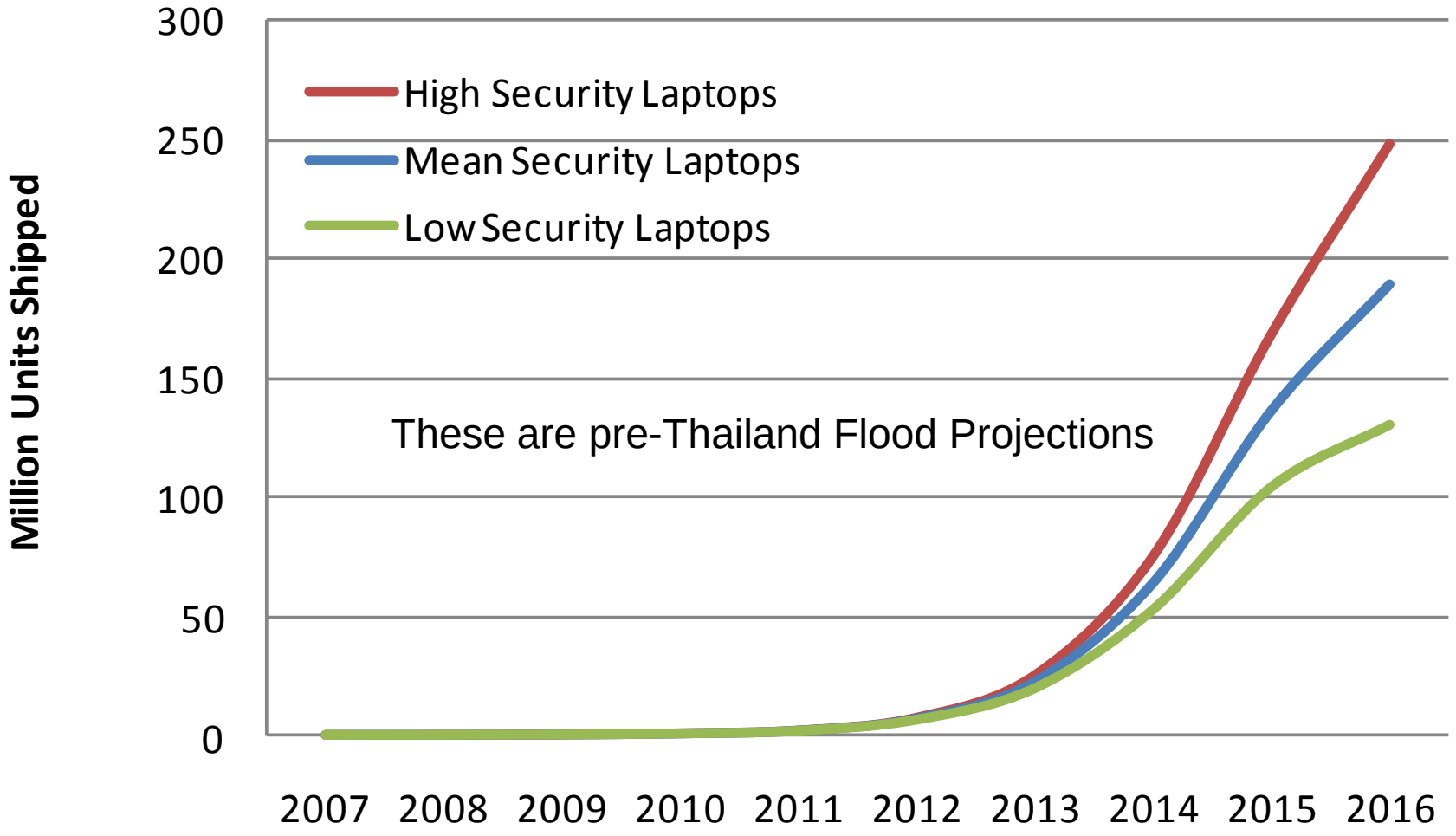
- In February 2011, Seagate announced that it had shipped more than 1 M self-encrypting HDDs into the laptop and enterprise markets.
- Seagate introduced their laptop SEDs in 2007 and their enterprise SEDs in 2009.
- Other companies that have shipped SEDs include Hitachi (announced in 2007) and Fujitsu(announced 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 and Samsung announced an SED SSD respectively 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

Simplification of Bass Diffusion Model

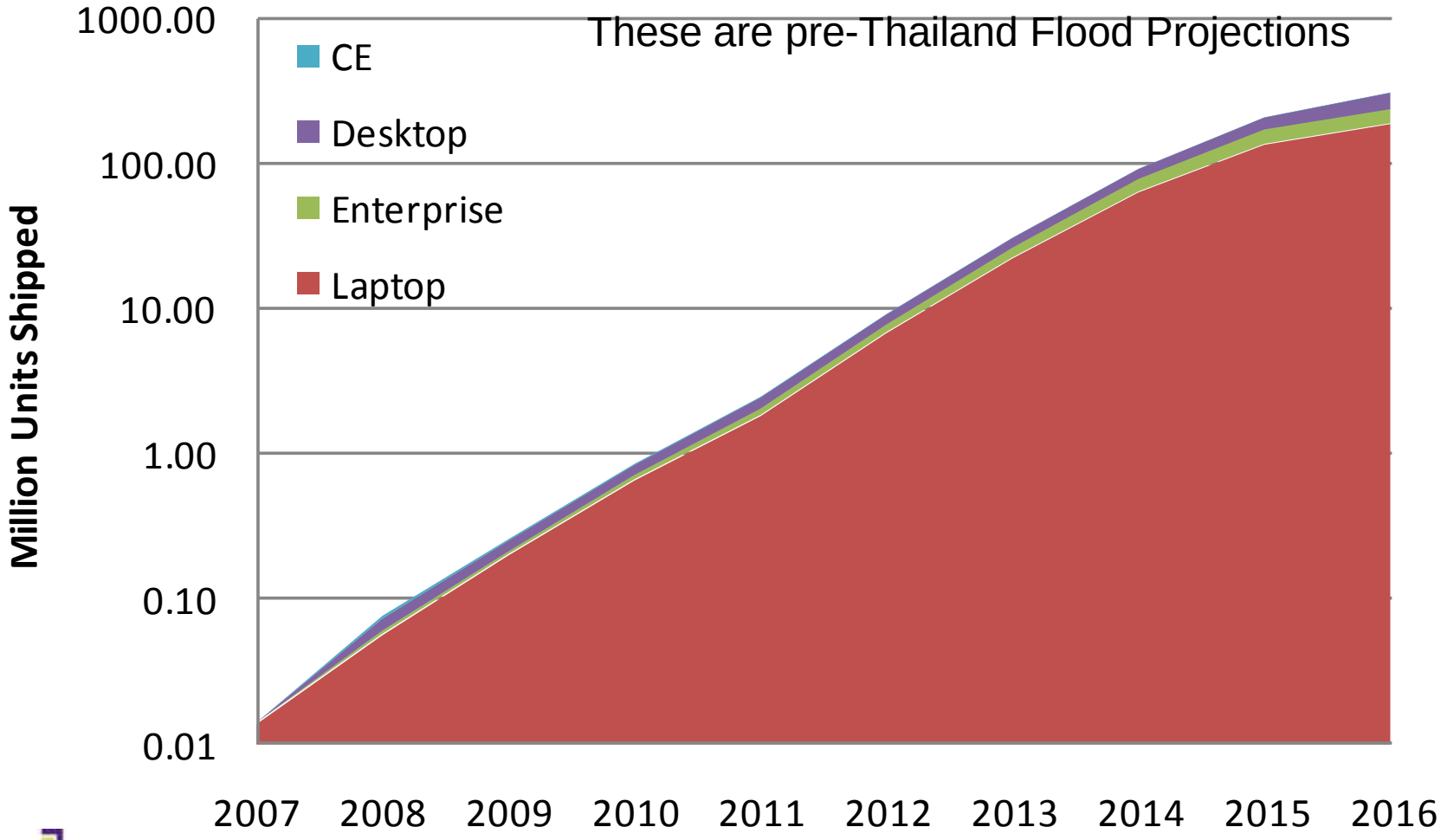
$$F(t) = \frac{1 - e^{-(p+q)t}}{1 + \left(\frac{q}{p}\right) e^{-(p+q)t}}$$

- 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.

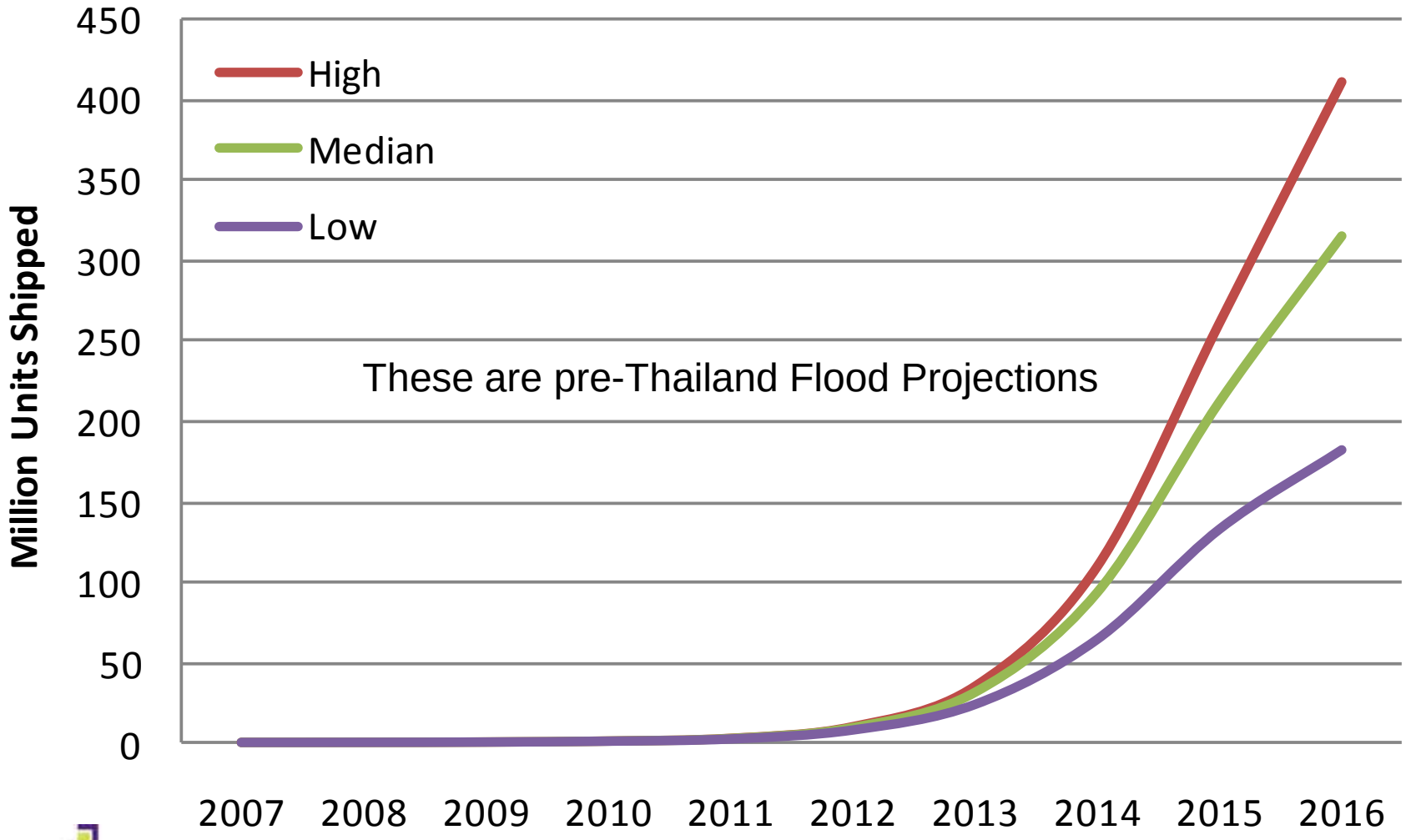
Security Adoption for Laptop HDDs



Median Security Adoption for all HDDs Market Segments



Security Adoption SED HDD Estimates (High, Median and Low)



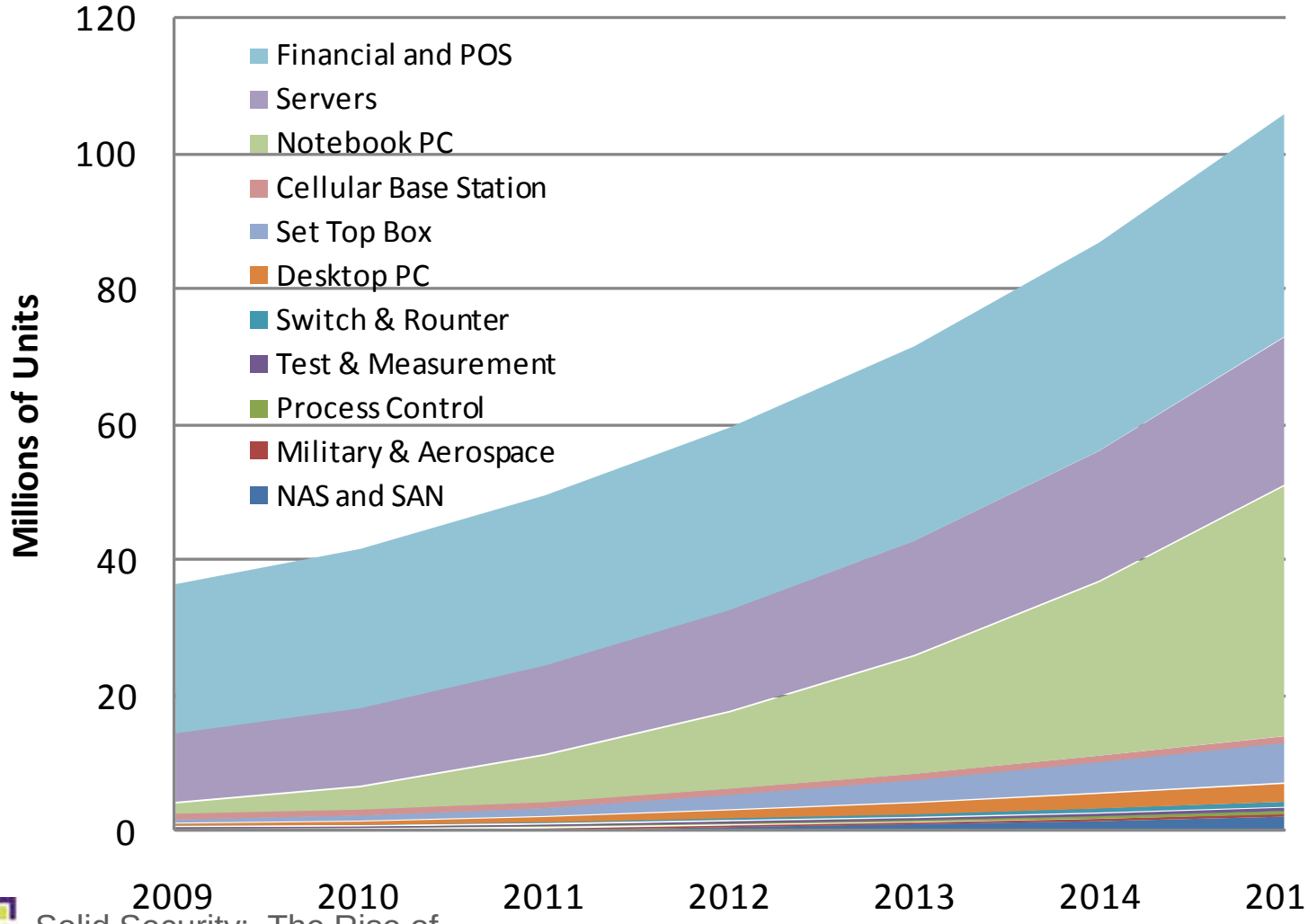
HDD SED Conclusions

- ***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 only 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

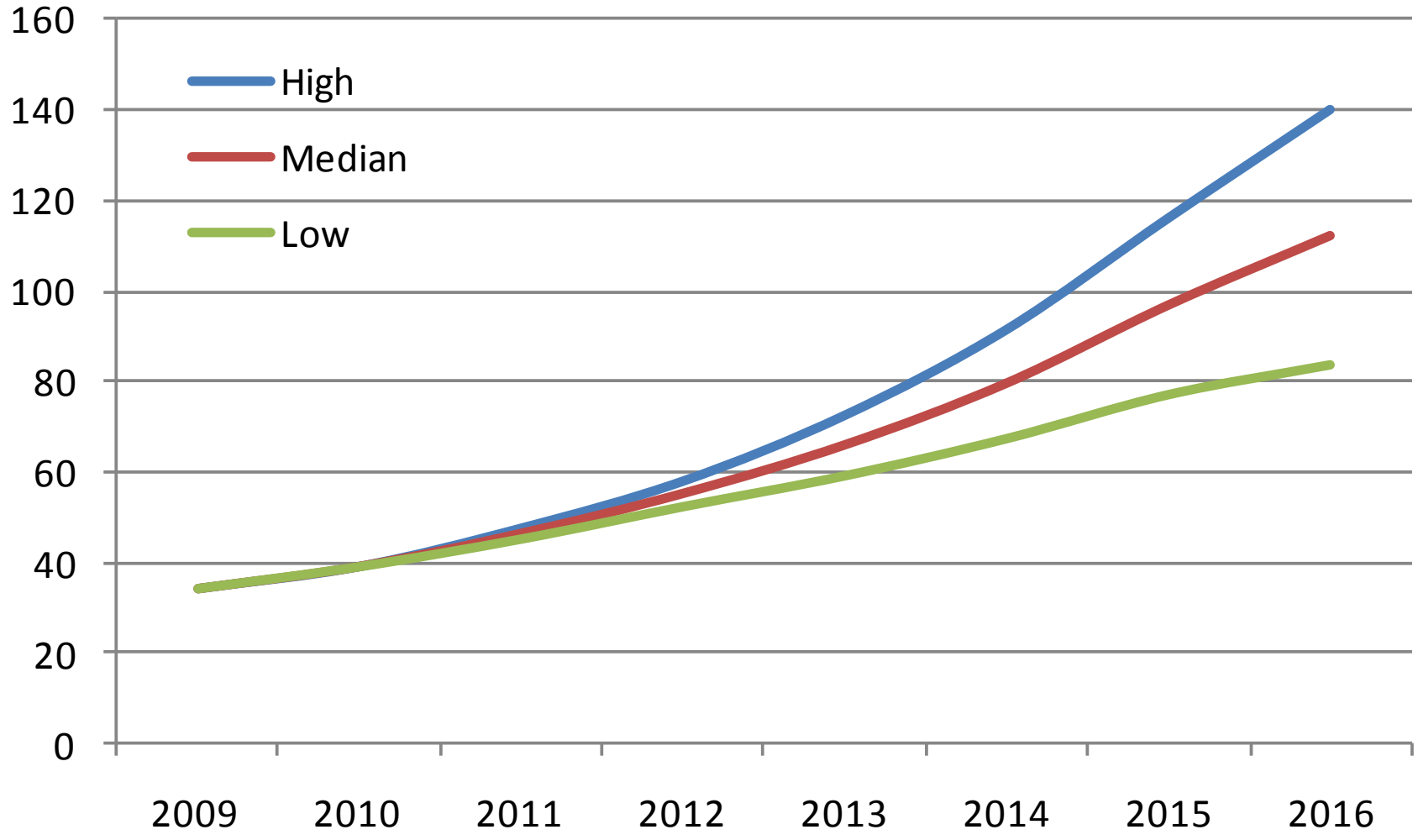
- Erasing all the memory cells in an SSD can take many seconds and most SSD controllers don't support easy access to all the cells .
- Providing encrypted data on the SSD where the key is within the device allows erasing the encryption key within milliseconds and making the data unavailable to others—a 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

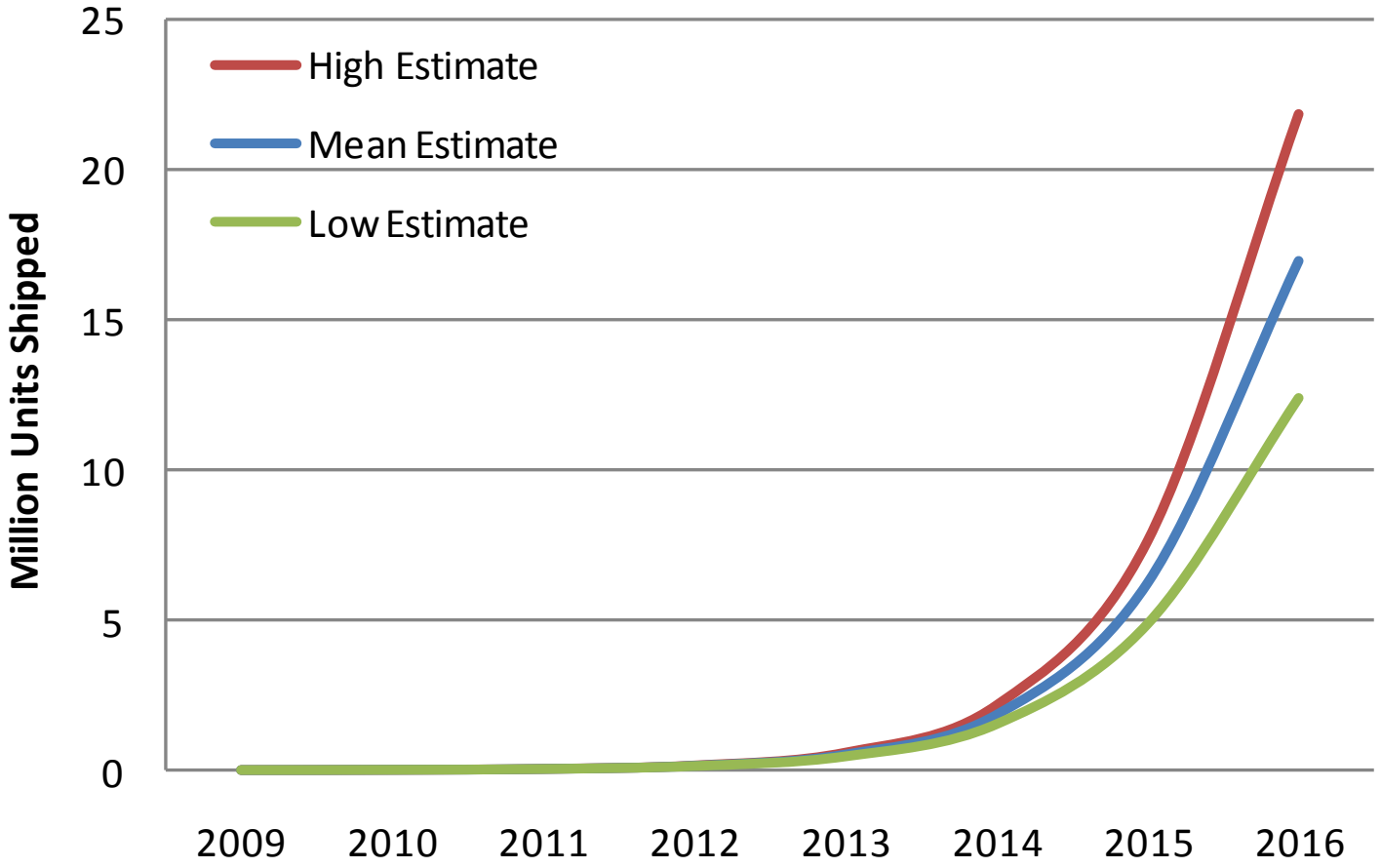


Source: Objective Analysis

High/Median/Low SSD Estimates



SSD Security Adoption Projections



- ***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 411 M, 315 M and 122 M 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 100% in about 122 M SSDs, the projected actual SSDs from that year used for security and data protection purposes is estimated at less than 18 M units***

Sources and References

- **FDE Performance Comparison: Hardware vs. Software Full Drive Encryption**, Trusted Strategies, February 9, 2010.
- **Full Drive Encryption with Samsung Solid State Drives**, Trusted Strategies, November 2010.
- **New Product Diffusion Models in Marketing: A Review and Direction for Research**, V. Mahajan, E. Muller and F.M. Bass, Journal of Marketing, Vol. 54 (January 1990), pp 1-26.
- **Managing technology and innovation for competitive advantage**, V. K. Narayanan, 2001, Prentice Hall.
- **Digital Storage Technology Newsletter**, Coughlin Associates, July 2011.
- **Implementing Stored-Data Encryption**, Michael Willett, Samsung, SNW 2011.
- **Solid State Drives: Outlook 2010**, Objective Analysis, 2010