IDF15
INTEL DEVELOPER FORUM

The Future of Storage Security

Adrian Pearson
Storage Security Architect, Non-Volatile Memory Solutions Group, Intel Corporation

SSDS004

intel
experience
what's inside™

Agenda

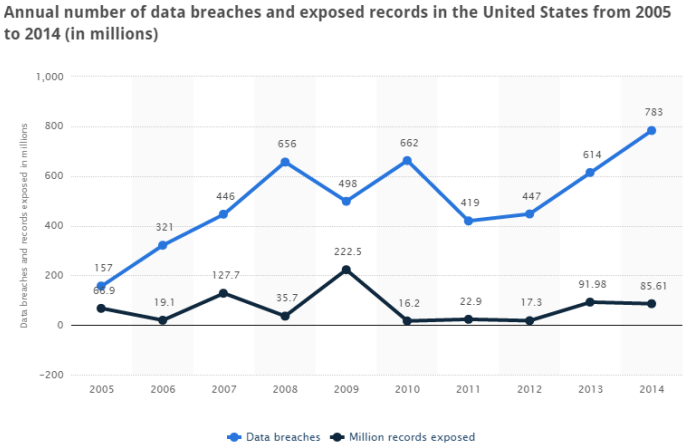
- A Brief History of Storage Encryption and Options Available
- Inherent Benefits of Self Encrypting Drives (SED)
- Comparison:
  Self Encrypting Drives vs. Software Full Disk Encryption (SW FDE)
- Storage Interface Transition from SATA* to PCI Express®/NVM Express™ and Emergence of Opal
- Benefits of Opal Over Previous Storage Security Standards
- Opal/SED Enhancements Needed to Maintain Parity with Software FDE
- Proposed Solutions and Standardization Efforts
- Summary/Call to Action

Agenda

- A Brief History of Storage Encryption and Options Available
- Inherent Benefits of Self Encrypting Drives (SED)
- Comparison:
  Self Encrypting Drives vs. Software Full Disk Encryption (SW FDE)
- Storage Interface Transition from SATA* to PCI Express®/NVM Express™ and Emergence of Opal
- Benefits of Opal Over Previous Storage Security Standards
- Opal/SED Enhancements Needed to Maintain Parity with Software FDE
- Proposed Solutions and Standardization Efforts
- Summary/Call to Action

A Brief History of Storage Encryption

- (2002) First law enacted requiring protections on corporate data (SOX)
- (2003) First State law enacted (CA) requiring breach disclosure on unencrypted data (S.B. 1386)
- (2005) Tracking begins on significant data breaches
- (2007) Seagate* introduces first SED (DriveTrust*)
- (2008) Intel IT mandates encryption of all data stored on managed machines
- (2010) Intel releases Intel® Advanced Encryption Standard New Instructions instruction set
- (2011) Intel introduces its first SED SSD
  - (Intel® SSD 320 Series)



Global study at a glance

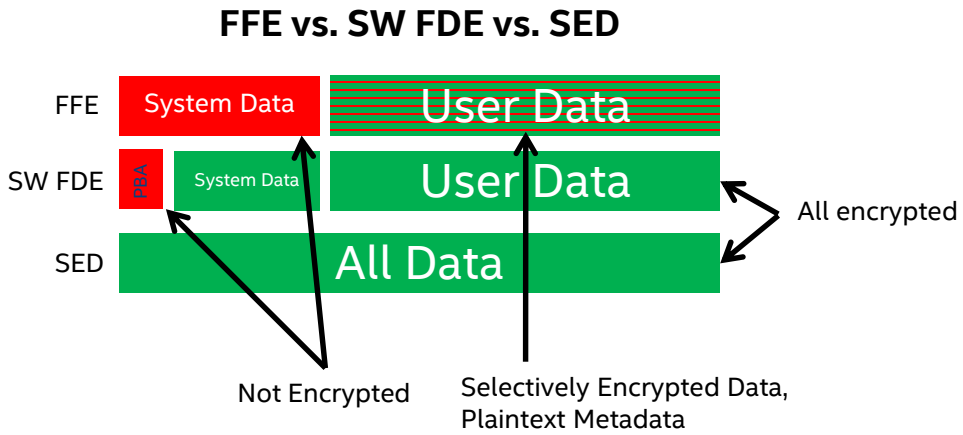
- 350 companies in 11 countries
- $3.79 million is the average total cost of data breach
- 23% increase in total cost of data breach since 2013
- $154 is the average cost per lost or stolen record
- 12% percent increase in per capita cost since 2013

Ponemon Institute May 2015: 2015 Cost of Data Breach Study: Global Analysis

Data Breach Cost and Frequency will continue to increase.
Storage Encryption provides a significant part of the solution!

Storage Encryption Solutions

- File and Folder Encryption (FFE)
  - Selective encryption of user files
  - Typically Enterprise Rights Management based
- Software based Full Disk Encryption (SW FDE)
  - Encryption applied by storage driver on most data
- Self Encrypting Drives (SED)
  - Encrypt all user data all the time



Only SED's Offer Complete User Data Encryption ALL the Time

Agenda

- A Brief History of Storage Encryption and Options Available
- Inherent Benefits of Self Encrypting Drives (SED)
- Comparison:
  Self Encrypting Drives vs. Software Full Disk Encryption (SW FDE)
- Storage Interface Transition from SATA* to PCI Express®/NVM Express™ and Emergence of Opal
- Benefits of Opal Over Previous Storage Security Standards
- Opal/SED Enhancements Needed to Maintain Parity with Software FDE
- Proposed Solutions and Standardization Efforts
- Summary/Call to Action

Inherent Properties of Self Encrypting Drives

- SEDs encrypt ALL user data ALL the time
- SEDs typically perform encryption that meets/exceeds interface bandwidth
- SEDs integrate encryption, media, and media management into a single device
- Intel® SSDs are designed to execute only signed firmware
- Storage Device Interfaces have a smaller software attack surface than Operating System Interfaces

SEDs Provide a Solid Foundation for Secure Storage

Resultant Benefits of Self Encrypting Drives

- SEDs provide higher assurance that ALL user data is encrypted
  - SW FDE is applied at the storage device driver level which has a larger attack surface than firmware inside a self encrypting drive
- SEDs provide higher assurance that data has been cryptographically erased
  - SW FDE AND File Level Encryption must perform I/O to the storage device to overwrite data for erasure. For SSDs, this issue is exacerbated due to wear leveling.
  - From NIST SP800-88 (Guidelines for Media Sanitization):

2.6 Use of Cryptography and Cryptographic Erase

Many storage manufacturers have released storage devices with integrated encryption and access control capabilities, also known as Self-Encrypting Drives (SEDs). SEDs feature always-on encryption that substantially reduces the likelihood that unencrypted data is inadvertently retained on the device. The end user cannot turn off the encryption capabilitieswhich ensures that all data in the designated areas are encrypted. A significant additional benefit of SEDs is the opportunity to tightly couple the controller and storage media so that the device can directly address the location where any cryptographic keys are stored, whereas solutions that depend only on the abstracted user access interface through software may not be able to directly address those areas.

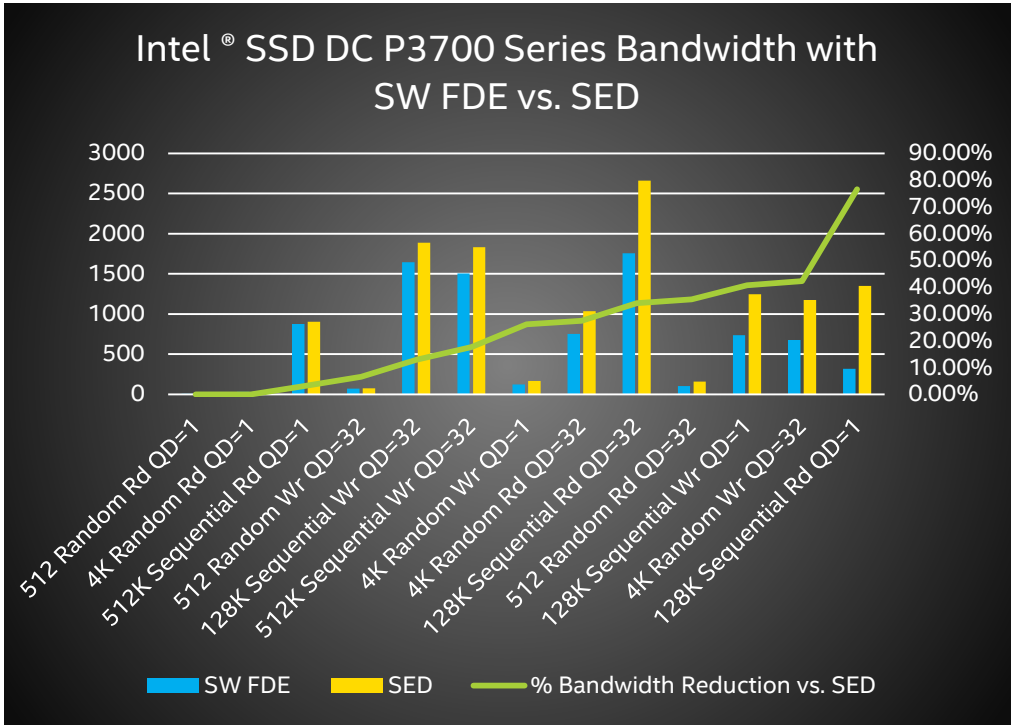
Resultant Benefits of Self Encrypting Drives

- SED key generation/management is less complicated/more secure
  - Currently, SW FDE exposes media encryption keys to other SW/DRAM
- SEDs provide near instant provisioning/setup time
  - SW FDE must perform read/encrypt/write to all user data during initial setup
    - Consumes hours, increases wear
- FIPS certification
  - SEDs are able to achieve higher levels of FIPS certification more easily than SW FDE

2089	**HGST, Inc.** 5601 Great Oaks Parkway	**HGST Ultrastar SSD800/1000/1600 TCG Enterprise SSDs**	Hardware	02/25/2014; 04/03/2014;	***Overall Level:* 2**
1601	**McAfee, Inc.** 27201 Puerta Real, Suite	**McAfee Endpoint Encryption for PCs** (Software Version: 5.2.6)	Software	09/08/2011; 10/04/2011	***Overall Level:* 1**

Resultant Benefits of Self Encrypting Drives

- Performance
  - Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) is a giant leap forward allowing near full bandwidth crypto for SW FDE
    - uArch performance optimizations continue
    - Software overhead remains, adding extra latency
  - SED AES performance provides low latency and bandwidth at interface speeds



With SW FDE, Consumers Don't Fully Realize the Performance Gains from their Awesome SSD!

Source: Intel. System Configuration: Asus Z97 PRO, Intel® Core™ i5-4670T CPU @2.3 GHz, DRAM 4GB, Intel DC P3700 800GB SSD, Microsoft Windows® 8.1 x64 with and without McAfee EEPC Endpoint Encryption
Results have been estimated based on internal Intel analysis and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance.

Agenda

- A Brief History of Storage Encryption and Options Available
- Inherent Benefits of Self Encrypting Drives (SED)
- Comparison:
  Self Encrypting Drives vs. Software Full Disk Encryption (SW FDE)
- Storage Interface Transition from SATA* to PCI Express®/NVM Express™ and Emergence of Opal
- Benefits of Opal Over Previous Storage Security Standards
- Opal/SED Enhancements Needed to Maintain Parity with Software FDE
- Proposed Solutions and Standardization Efforts
- Summary/Call to Action

Comparison: Self Encrypting Drives vs. Software Full Disk Encryption†

Category/Feature	Self Encrypting Drive	Software Full Disk Encryption
Run-time Performance	Best	Good
High Assurance that All User Data is Encrypted	Best	Good
High Assurance of Cryptographic Erase	Best	Good
Ease of Regulatory Compliance	Best	Good
Ease of Maintenance	Good	Best
Compatibility	Good	Best
Susceptibility to Attacks (Hot Swap/Password Sniffers)	More Susceptible	Less Susceptible

†Represents Intel's opinion regarding disk encryption features based on a review of publicly available data. For informational purposes only.

Comparison: Self Encrypting Drives vs. Software Full Disk Encryption†

Category/Feature	Self Encrypting Drive	Software Full Disk Encryption
Run-time Performance	Best	Good
High Assurance that All User Data is Encrypted	Best	Good
High Assurance of Cryptographic Erase	Best	Good
Ease of Regulatory Compliance	Best	Good
Ease of Maintenance	Good	Best
Compatibility	Good	Best
Susceptibility to Attacks (Hot Swap/Password Sniffers)	More Susceptible	Less Susceptible

Industry focus Needed to address Compatibility Issues and Add Enhancements to Security Model

†Represents Intel's opinion regarding disk encryption features based on a review of publicly available data. For informational purposes only.

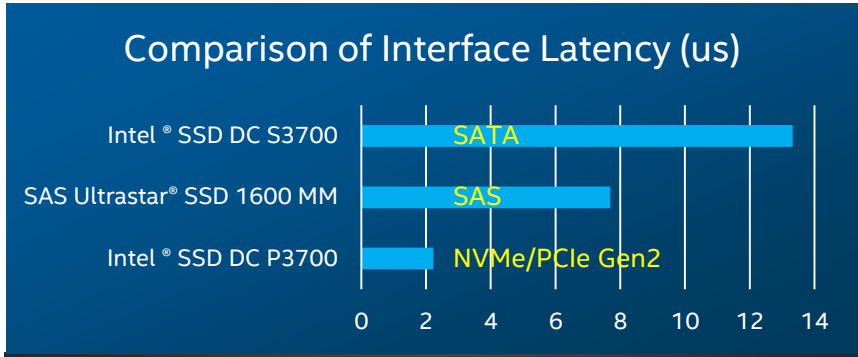
Agenda

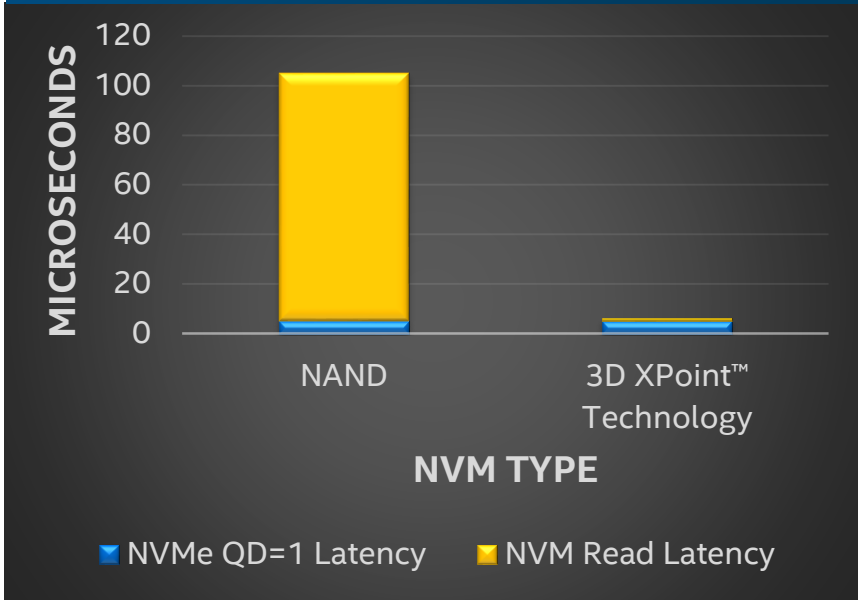
- A Brief History of Storage Encryption and Options Available
- Inherent Benefits of Self Encrypting Drives (SED)
- Comparison:
  Self Encrypting Drives vs. Software Full Disk Encryption (SW FDE)
- Storage Interface Transition from SATA* to PCI Express®/NVM Express™ and Emergence of Opal
- Benefits of Opal Over Previous Storage Security Standards
- Opal/SED Enhancements Needed to Maintain Parity with Software FDE
- Proposed Solutions and Standardization Efforts
- Summary/Call to Action

Storage Interface Transition

- Transition occurring from SAS/SATA* to PCIe®/NVMe™
  - Increased bandwidth and reduced latency
  - Multiple hardware and software optimizations merging
- 3D XPoint™ Technology further reduces latencies (>1000x lower latency than NAND)

Technology claims are based on comparisons of latency, density and write cycling metrics amongst memory technologies recorded on published specifications of in-market memory products against internal



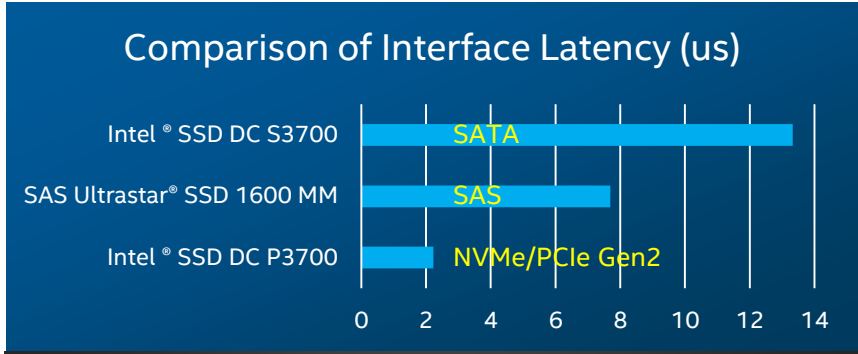


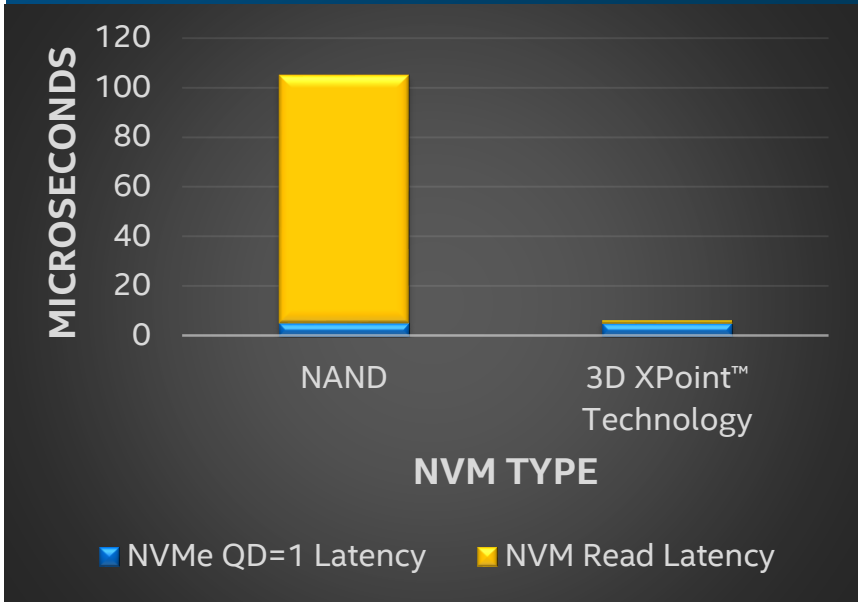
Storage Interface Transition

- Transition occurring from SAS/SATA* to PCIe®/NVMe™
  - Increased bandwidth and reduced latency
  - Multiple hardware and software optimizations merging
- 3D XPoint™ Technology further reduces latencies (>1000x lower latency than NAND)
- Software Full Disk Encryption adds latency and reduces bandwidth

Why increase performance and reduce latency only to give it back with SW FDE?

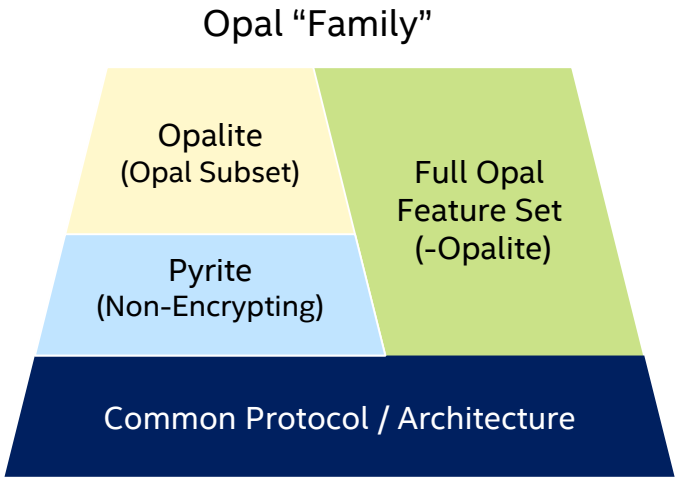
Technology claims are based on comparisons of latency, density and write cycling metrics amongst memory technologies recorded on published specifications of in-market memory products against internal





NVM Express™ and Opal

- NVMe™ is leveraging the security expertise of the Trusted Computing Group* (TCG)
- TCG has developed a “family” of specifications to scale across the needs of NVMe in different Client and Enterprise solutions
- SKL Reference BIOS slated to support simple password management via Opal over NVMe



Consumers, enterprise client users, and data centers are able to take advantage of encryption via Opal on NVMe using the same, standardized interface

Agenda

- A Brief History of Storage Encryption and Options Available
- Inherent Benefits of Self Encrypting Drives (SED)
- Comparison:
  Self Encrypting Drives vs. Software Full Disk Encryption (SW FDE)
- Storage Interface Transition from SATA* to PCI Express®/NVM Express™ and Emergence of Opal
- Benefits of Opal Over Previous Storage Security Standards
- Opal/SED Enhancements Needed to Maintain Parity with Software FDE
- Proposed Solutions and Standardization Efforts
- Summary/Call to Action

Benefits of TCG Opal over Previous Storage Security Standards

- TCG Opal is the only industry standard for storage security that scales to all storage interfaces and usage models
- TCG Opal is actively being developed by an architecture community with focus and knowledge in storage security

Capability	ATA Security	Opal
Guaranteed industry grade AES cipher for data-at-rest protection	✗	✓
Remote management	✗	✓
Interface agnostic	✗	✓
Extensibility to other security usage models	✗	✓
Specified support for Crypto Erase	✗	✓
“Purge” level erase	✗	✓

TCG Opal is the Storage Security Management Interface of the Future

Agenda

- A Brief History of Storage Encryption and Options Available
- Inherent Benefits of Self Encrypting Drives (SED)
- Comparison:
  Self Encrypting Drives vs. Software Full Disk Encryption (SW FDE)
- Storage Interface Transition from SATA* to PCI Express®/NVM Express™ and Emergence of Opal
- Benefits of Opal Over Previous Storage Security Standards
- Opal/SED Enhancements Needed to Maintain Parity with Software FDE
- Proposed Solutions and Standardization Efforts
- Summary/Call to Action

Opal/SED Enhancements Needed to Maintain Parity with Software FDE: Security

- Classic conflict between User Experience (UX) and Security exists with SEDs
- Unfortunately, platforms containing SEDs are vulnerable when the SED is unlocked and the user is not present
  - I.e. Stolen laptop in S3 state
- This is due to End User Experience (UX) Expectations:
  - Ease of data access (passwords - ugh!)
  - Fast responsiveness (S3 Resume)
- Which led to Tradeoffs: Auto-Unlock SED during…
  - S3 resume (open lid) & Connected Standby/Always on Always Connected
  - S4/S5 resume still requires user password

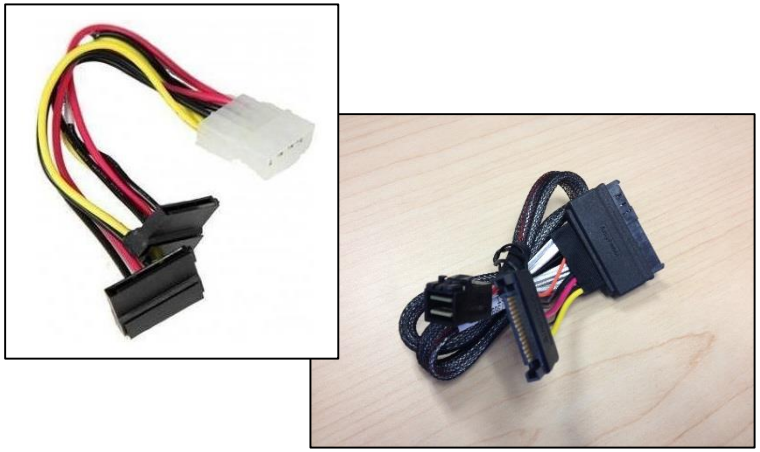
User Experience Favored over Platform Security

Attacks on Self Encrypting Drives

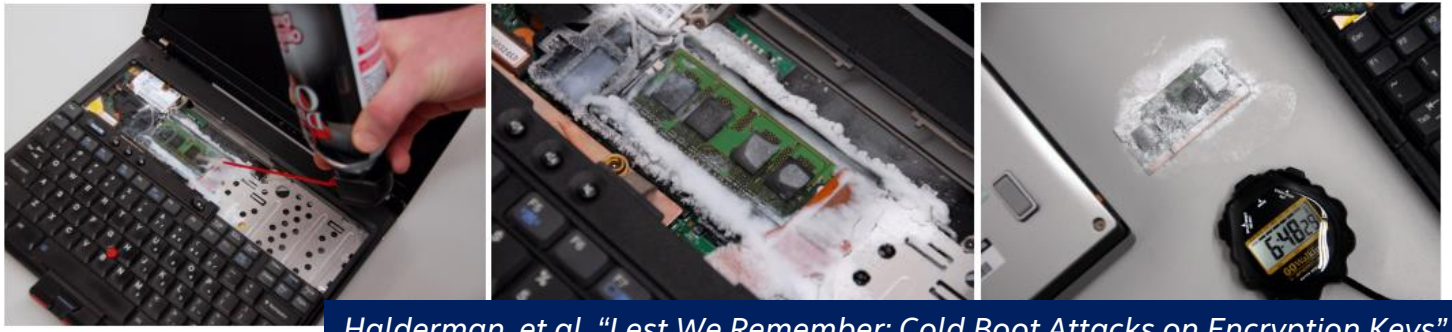
Hot Swap Attack

Overall, only a few SED-based systems withstood more attacks than equivalent software-based FDE systems. The majority of machines is equally vulnerable in both scenarios, and some machines are arguably more vulnerable when using SEDs.

Muller, et al. "Self-Encrypting Disks pose Self-Decrypting Risks"



Cold BootAttack



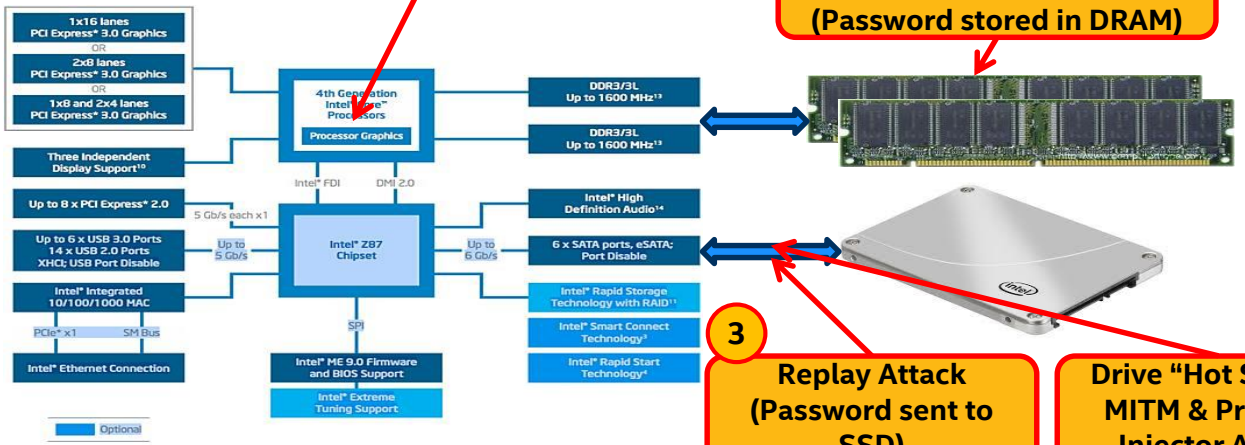
Halderman, et al. "Lest We Remember: Cold Boot Attacks on Encryption Keys"

Exposed Security Gaps

Note: Password is Handled in clear txt

2 Malware Sniff & Ransom Ware Attack on Password (Password used for Auto-Unlock by Host)

1 Cold & Warm Boot Attacks on Password (Password stored in DRAM)



3 Replay Attack (Password sent to SSD)

4 Drive "Hot Swap" / MITM & Protocol Injector Attack

Auto-Unlock Provides UX Benefits, but Opens Data Access Security Gaps!

Agenda

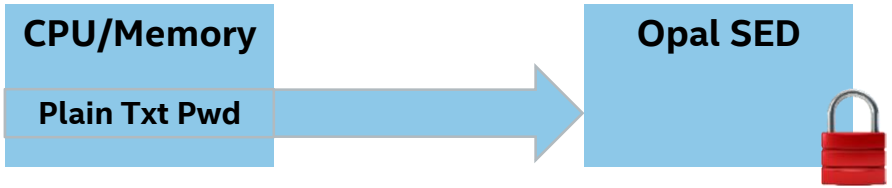
- A Brief History of Storage Encryption and Options Available
- Inherent Benefits of Self Encrypting Drives (SED)
- Comparison:
  Self Encrypting Drives vs. Software Full Disk Encryption (SW FDE)
- Storage Interface Transition from SATA* to PCI Express®/NVM Express™ and Emergence of Opal
- Benefits of Opal Over Previous Storage Security Standards
- Opal/SED Enhancements Needed to Maintain Parity with Software FDE
- Proposed Solutions and Standardization Efforts
- Summary/Call to Action

Proposed Solution: Challenge Response Authentication Method (CRAM)

- CRAM introduces a random element into the authentication process
- Prevents sniff/replay of the authentication credential to the drive
- Removes the need to store the password in DRAM
- Signing key can be held securely in a TEE such as Intel® Management Engine (Intel® ME)/Intel® Trusted Platform Module (Intel® TPM)

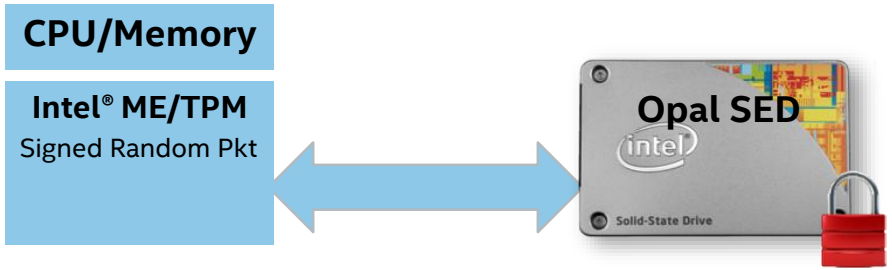
No CRAM

Resume from S3 Auto-Unlock



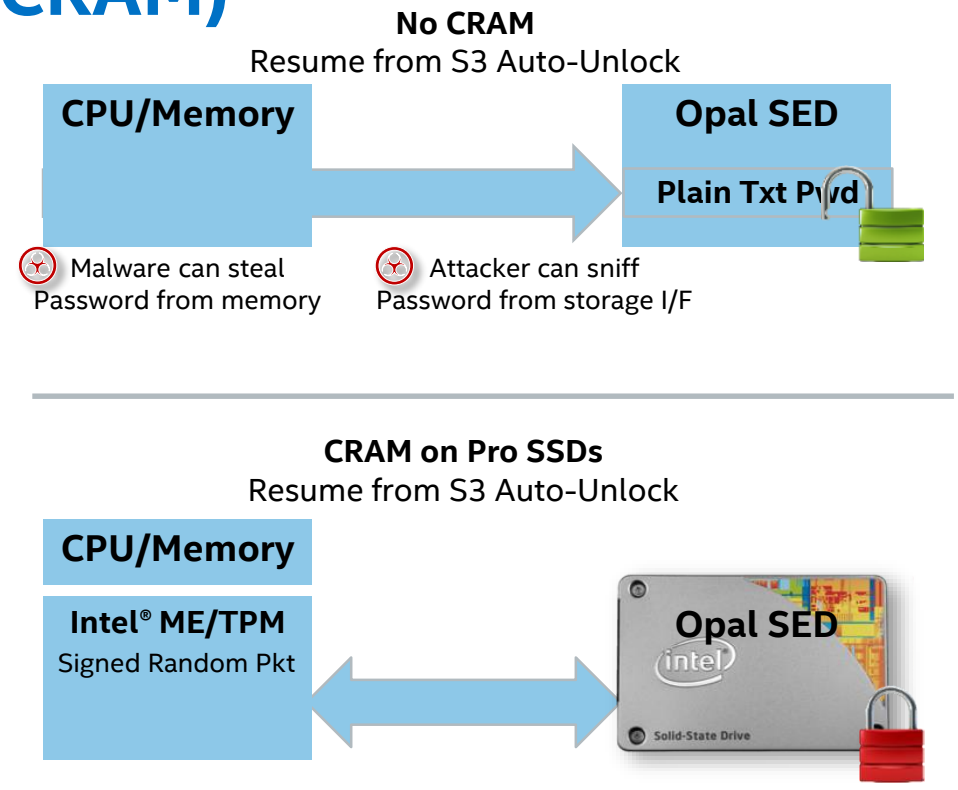
CRAM on Pro SSDs

Resume from S3 Auto-Unlock



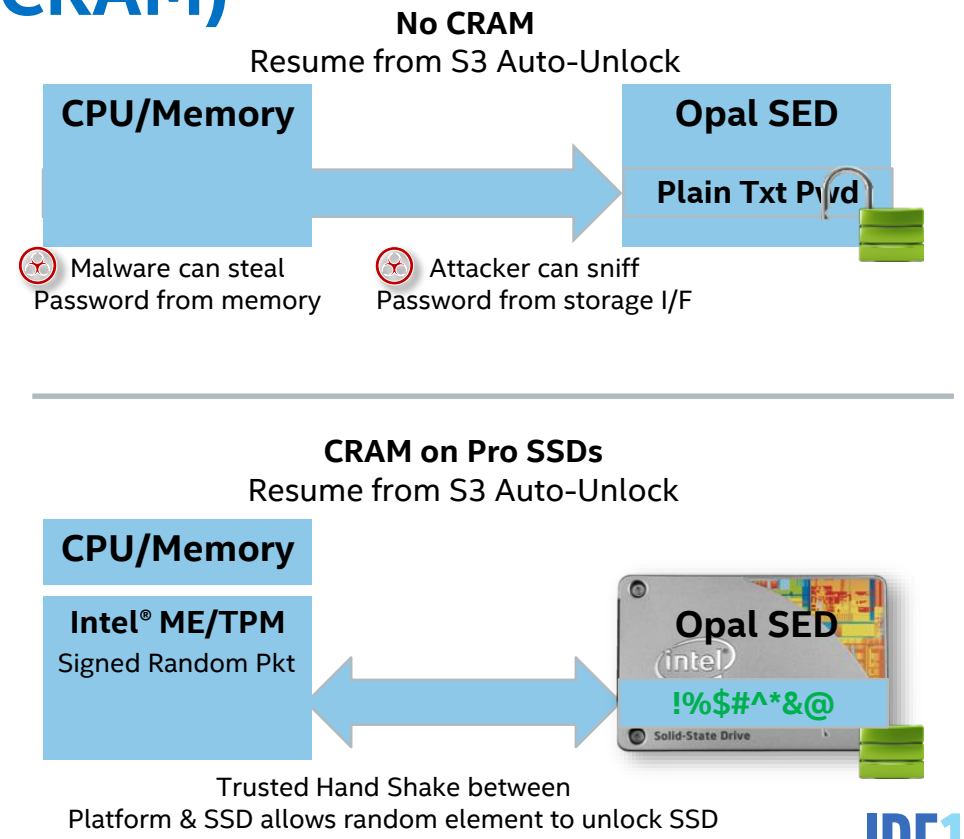
Proposed Solution: Challenge Response Authentication Method (CRAM)

- CRAM introduces a random element into the authentication process
- Prevents sniff/replay of the authentication credential to the drive
- Removes the need to store the password in DRAM
- Signing key can be held securely in a TEE such as Intel® Management Engine (Intel® ME)/Intel® Trusted Platform Module (Intel® TPM)



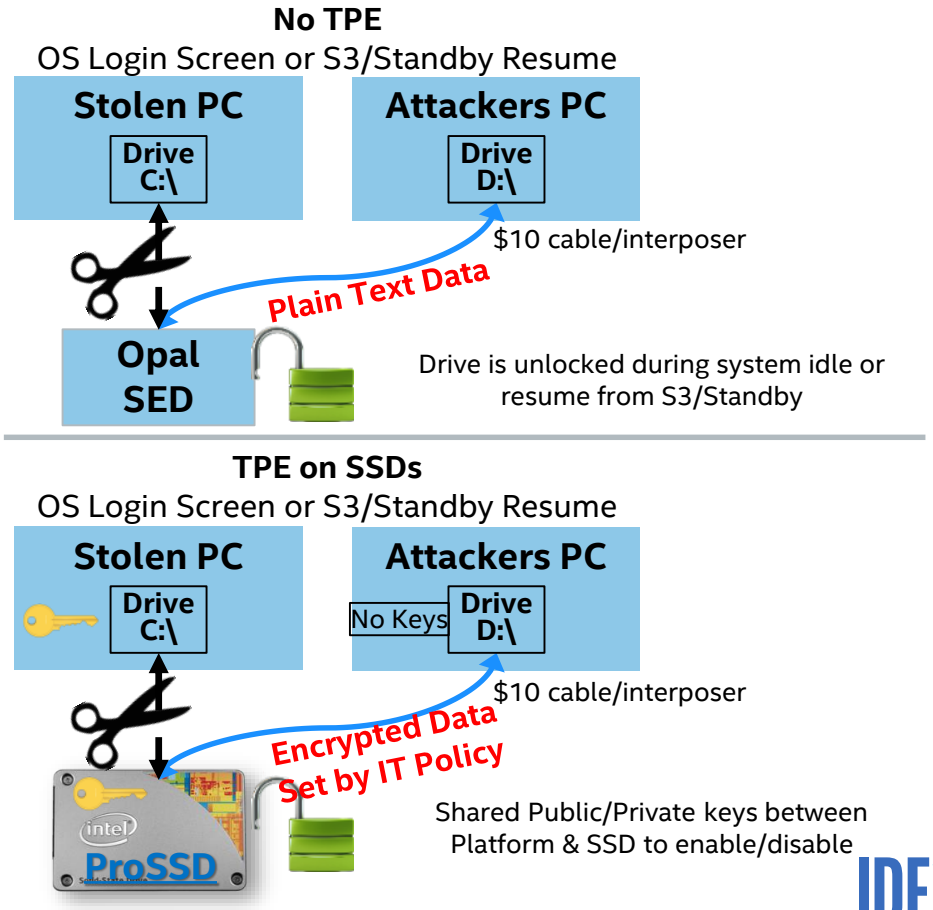
Proposed Solution: Challenge Response Authentication Method (CRAM)

- CRAM introduces a random element into the authentication process
- Prevents sniff/replay of the authentication credential to the drive
- Removes the need to store the password in DRAM
- Signing key can be held securely in a TEE such as Intel® Management Engine (Intel® ME)/Intel® Trusted Platform Module (Intel® TPM)

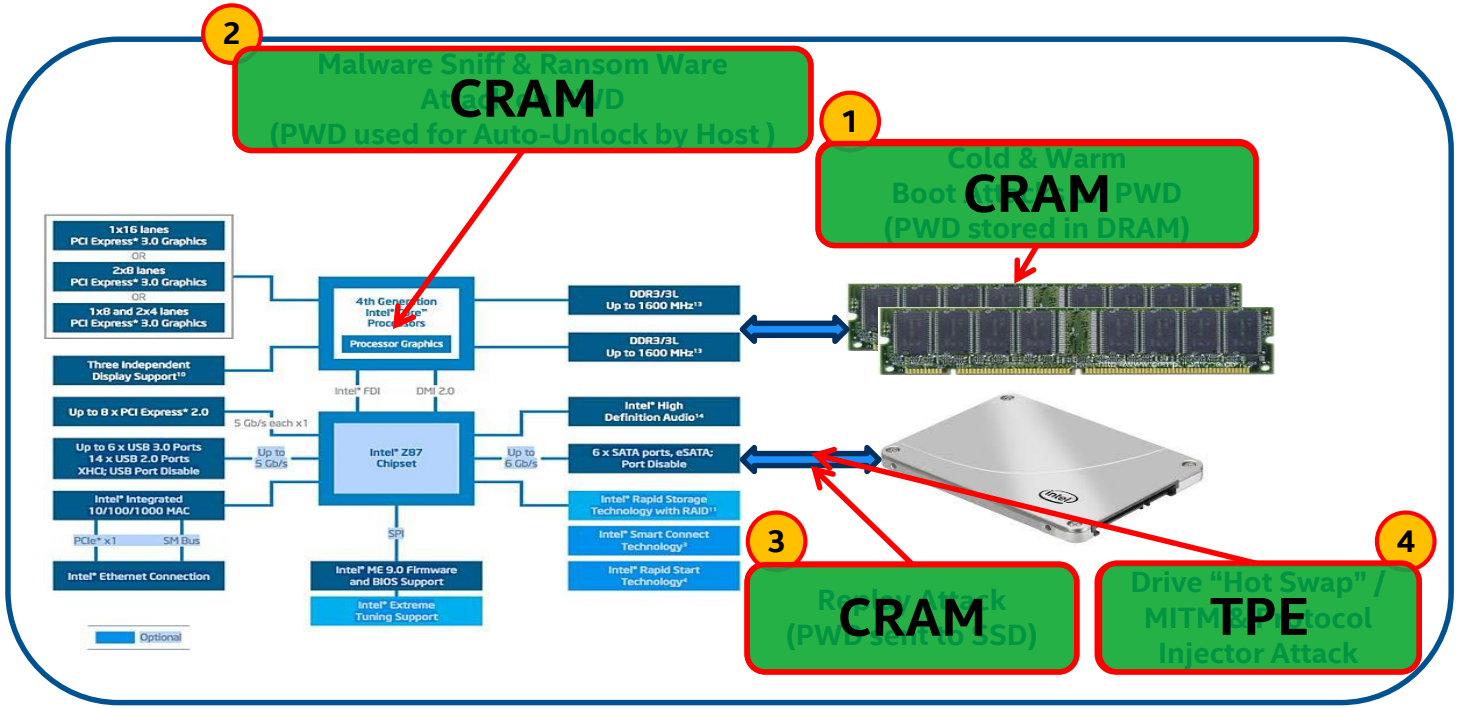


Proposed Solution: Transport Encryption (TPE)

- TPE encrypts all data over the interface in platform “vulnerable states”
- Enable/Disable of TPE requires cryptographic authentication
- Encryption disabled while user is logged in to the OS (maintains performance)
- Encryption enabled at OS lock screen



Gaps Closed!



Proposed Solutions Solve Security Gaps While Introducing Minimal Platform Performance Degradation

Agenda

- A Brief History of Storage Encryption and Options Available
- Inherent Benefits of Self Encrypting Drives (SED)
- Comparison:
  Self Encrypting Drives vs. Software Full Disk Encryption (SW FDE)
- Storage Interface Transition from SATA* to PCI Express®/NVM Express™ and Emergence of Opal
- Benefits of Opal Over Previous Storage Security Standards
- Opal/SED Enhancements Needed to Maintain Parity with Software FDE
- Proposed Solutions and Standardization Efforts
- Summary/Call to Action

Summary/Call to Action

- Opal SEDs maintain storage performance while providing comprehensive data at rest protection
  - Standards based enhancements are needed to address SED security gaps
- Corporate Consumer?
  - Demand an Opal SED on your next system! (Intel® SSD Preferably)
- Platform or Storage Security Oriented?
  - Join the Trusted Computing Group* (TCG) Storage Workgroup and assist in defining the future of Storage Security through Self Encrypting Drives

The Success of Opal SEDs depends on Consumer Demand and Increased Contributions to SED ecosystem through TCG Opal

Additional Sources of Information

- A PDF of this presentation is available from our Technical Session Catalog: www.intel.com/idfsessionsSF. This URL is also printed on the top of Session Agenda Pages in the Pocket Guide.

- Additional info in the storage security community – https://www.trustedcomputinggroup.org/developers/storage

Legal Notices and Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at intel.com, or from the OEM or retailer.

No computer system can be absolutely secure.

Tests document performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. Consult other sources of information to evaluate performance as you consider your purchase. For more complete information about performance and benchmark results, visit http://www.intel.com/performance.

Cost reduction scenarios described are intended as examples of how a given Intel-based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest forecast, schedule, specifications and roadmaps.

Statements in this document that refer to Intel's plans and expectations for the quarter, the year, and the future, are forward-looking statements that involve a number of risks and uncertainties. A detailed discussion of the factors that could affect Intel's results and plans is included in Intel's SEC filings, including the annual report on Form 10-K.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel does not control or audit third-party benchmark data or the web sites referenced in this document. You should visit the referenced web site and confirm whether referenced data are accurate.

Intel, Core, 3D XPoint, and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.

Risk Factors

The above statements and any others in this document that refer to plans and expectations for the second quarter, the year and the future are forward-looking statements that involve a number of risks and uncertainties. Words such as "anticipates," "expects," "intends," "plans," "believes," "seeks," "estimates," "may," "will," "should" and their variations identify forward-looking statements. Statements that refer to or are based on projections, uncertain events or assumptions also identify forward-looking statements. Many factors could affect Intel's actual results, and variances from Intel's current expectations regarding such factors could cause actual results to differ materially from those expressed in these forward-looking statements. Intel presently considers the following to be important factors that could cause actual results to differ materially from the company's expectations. Demand for Intel's products is highly variable and could differ from expectations due to factors including changes in business and economic conditions; consumer confidence or income levels; the introduction, availability and market acceptance of Intel's products, products used together with Intel products and competitors' products; competitive and pricing pressures, including actions taken by competitors; supply constraints and other disruptions affecting customers; changes in customer order patterns including order cancellations; and changes in the level of inventory at customers. Intel's gross margin percentage could vary significantly from expectations based on capacity utilization; variations in inventory valuation, including variations related to the timing of qualifying products for sale; changes in revenue levels; segment product mix; the timing and execution of the manufacturing ramp and associated costs; excess or obsolete inventory; changes in unit costs; defects or disruptions in the supply of materials or resources; and product manufacturing quality/yields. Variations in gross margin may also be caused by the timing of Intel product introductions and related expenses, including marketing expenses, and Intel's ability to respond quickly to technological developments and to introduce new products or incorporate new features into existing products, which may result in restructuring and asset impairment charges. Intel's results could be affected by adverse economic, social, political and physical/infrastructure conditions in countries where Intel, its customers or its suppliers operate, including military conflict and other security risks, natural disasters, infrastructure disruptions, health concerns and fluctuations in currency exchange rates. Results may also be affected by the formal or informal imposition by countries of new or revised export and/or import and doing-business regulations, which could be changed without prior notice. Intel operates in highly competitive industries and its operations have high costs that are either fixed or difficult to reduce in the short term. The amount, timing and execution of Intel's stock repurchase program could be affected by changes in Intel's priorities for the use of cash, such as operational spending, capital spending, acquisitions, and as a result of changes to Intel's cash flows or changes in tax laws. Product defects or errata (deviations from published specifications) may adversely impact our expenses, revenues and reputation. Intel's results could be affected by litigation or regulatory matters involving intellectual property, stockholder, consumer, antitrust, disclosure and other issues. An unfavorable ruling could include monetary damages or an injunction prohibiting Intel from manufacturing or selling one or more products, precluding particular business practices, impacting Intel's ability to design its products, or requiring other remedies such as compulsory licensing of intellectual property. Intel's results may be affected by the timing of closing of acquisitions, divestitures and other significant transactions. A detailed discussion of these and other factors that could affect Intel's results is included in Intel's SEC filings, including the company's most recent reports on Form 10-Q, Form 10-K and earnings release.

Rev. 4/14/15