
COMPUTERWORLD
SNIA
SNW
OCTOBER
11-14
2010
The Gaylord Texan, Dallas, Texas

Industry Perspective: Compliance and Self-Encrypting Drives

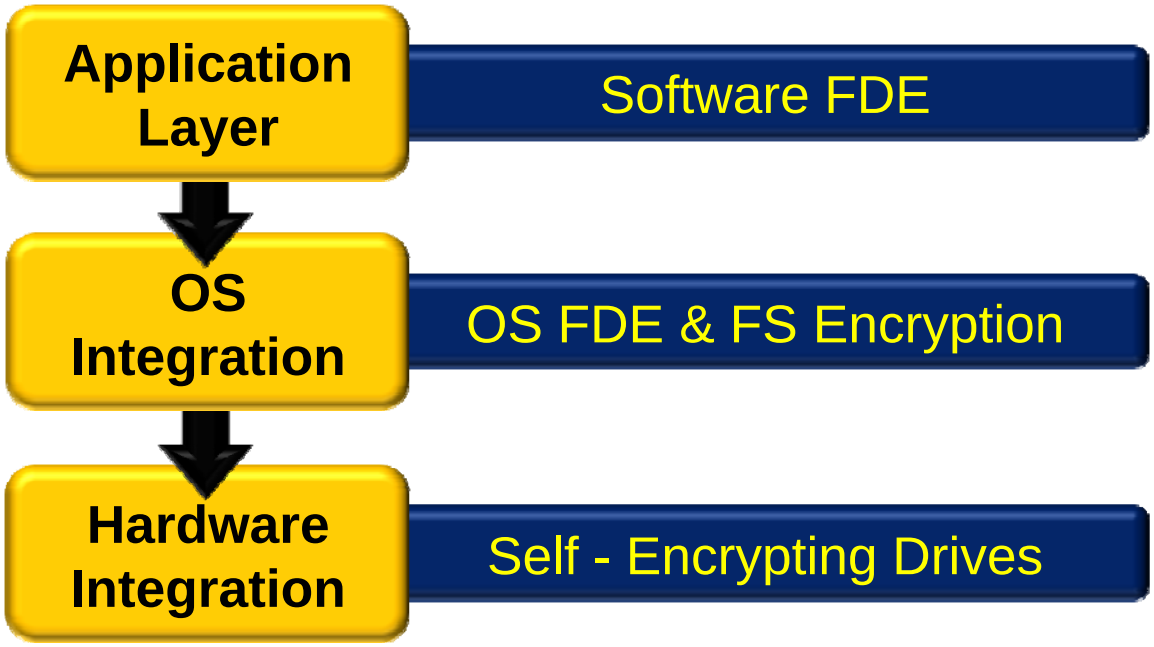
Robert Thibadeau, Ph.D.
Senior Vice President and Chief Scientist
Wave Systems, Inc.

Agenda

- Self-encrypting drives
  - Characteristics
  - Market Drivers
- TCG
- Shadow MBR and Self Healing Demo
- Controller SP and Intel's CPU Conversion

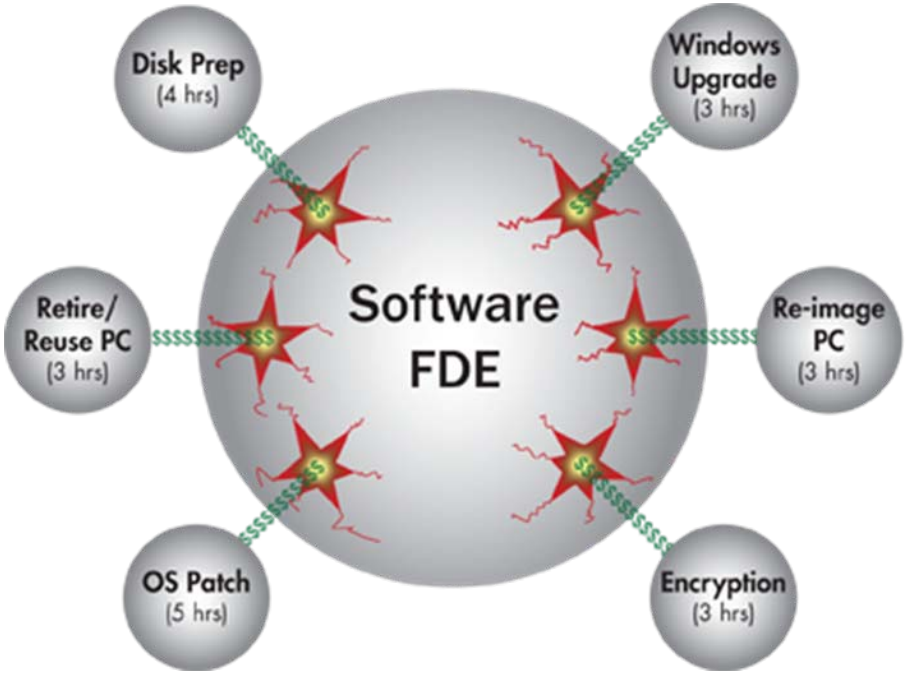
Self-Encrypting Drives

Evolution of Data Protection Solutions
Migration to Hardware



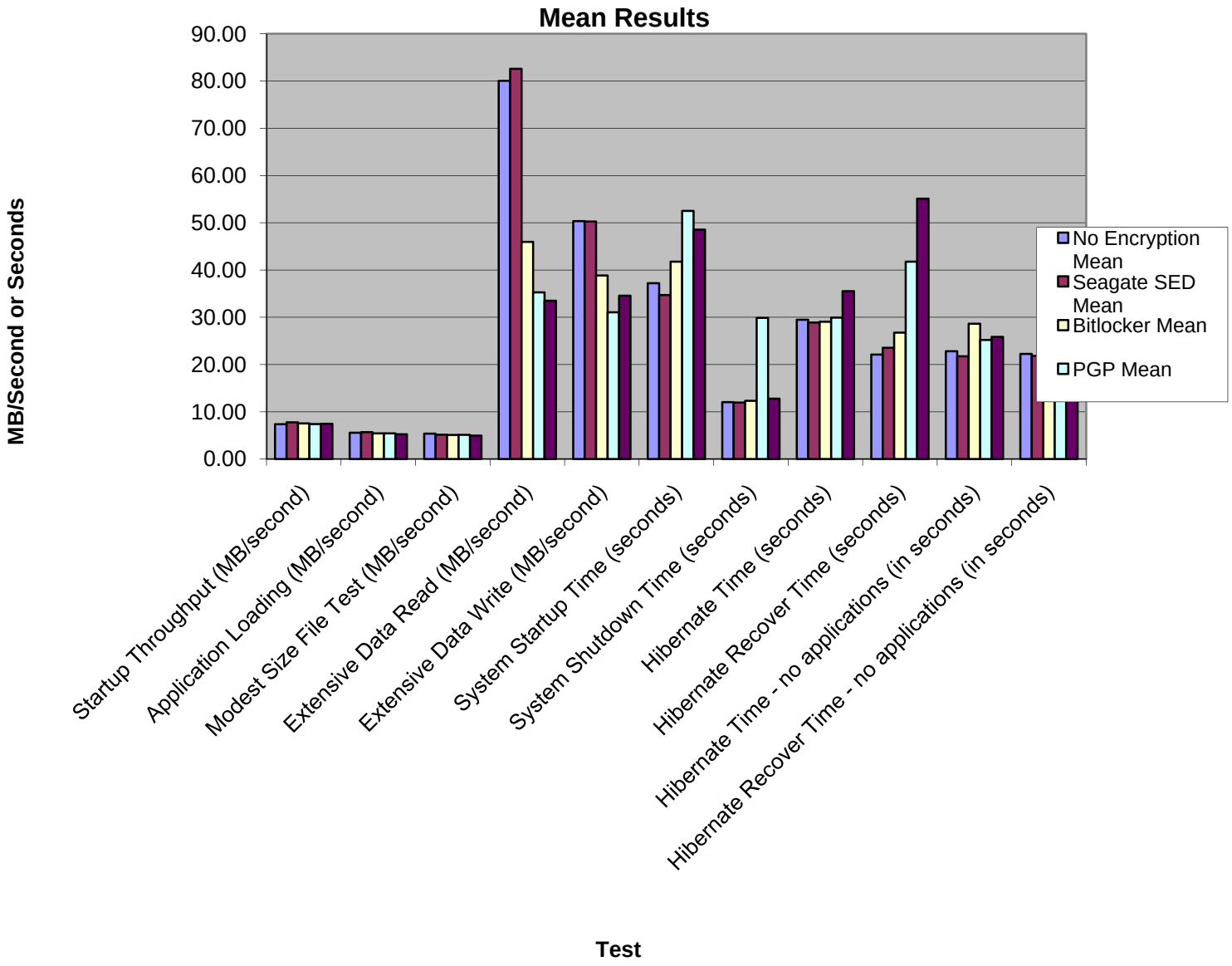
Faster, Simpler, Lower Cost!

FDE Deployment Considerations



Set it ...
Self-Encrypting Drive
... and forget it

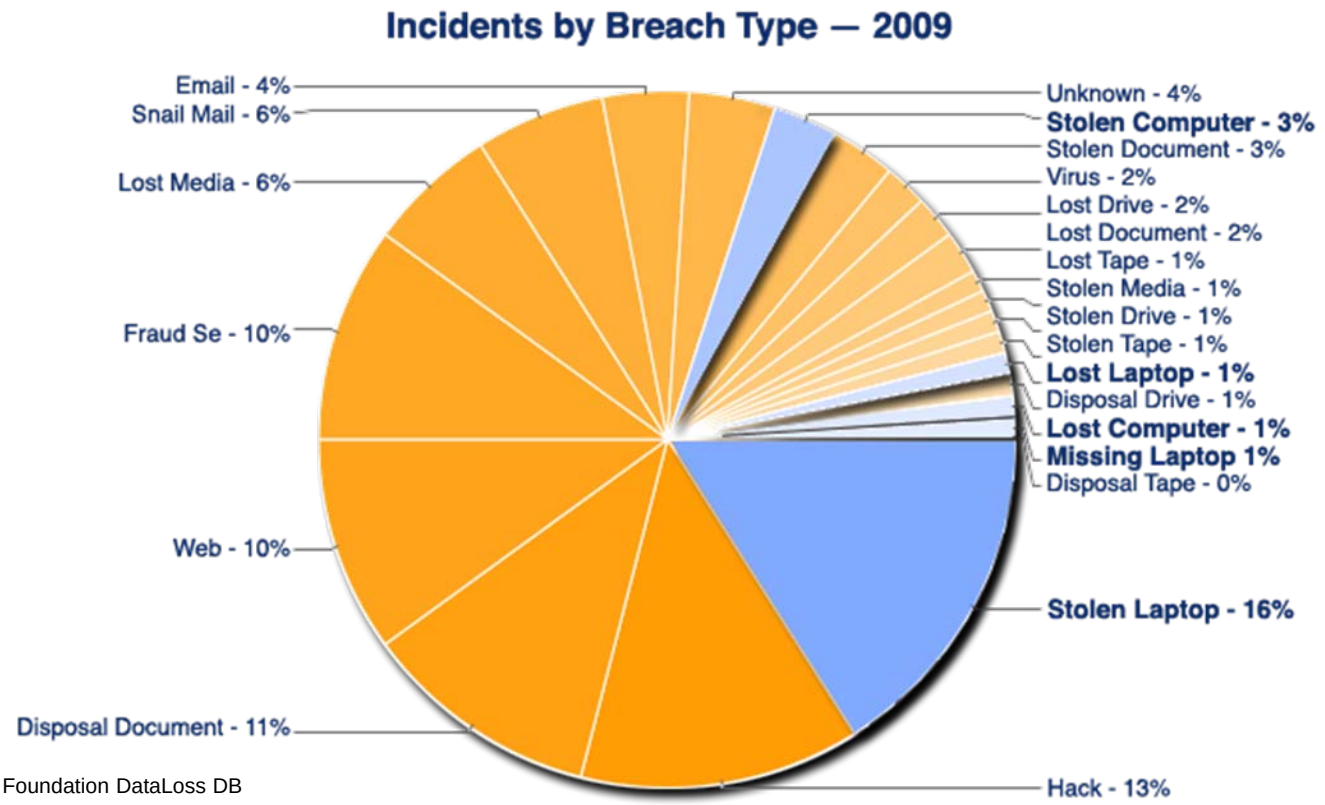
SED vs. SW FDE


Mean Results
MB/Second or Seconds
90.00
80.00
70.00
60.00
50.00
40.00
30.00
20.00
10.00
0.00
Startup Throughput (MB/second)
Application Loading (MB/second)
Modest Size File Test (MB/second)
Extensive Data Read (MB/second)
Extensive Data Write (MB/second)
System Startup Time (seconds)
System Shutdown Time (seconds)
Hibernate Time (seconds)
Hibernate Recover Time (seconds)
Hibernate Time - no applications (in seconds)
Hibernate Recover Time - no applications (in seconds)
No Encryption Mean
Seagate SED Mean
Bitlocker Mean
PGP Mean
Test

Data Breach Headlines

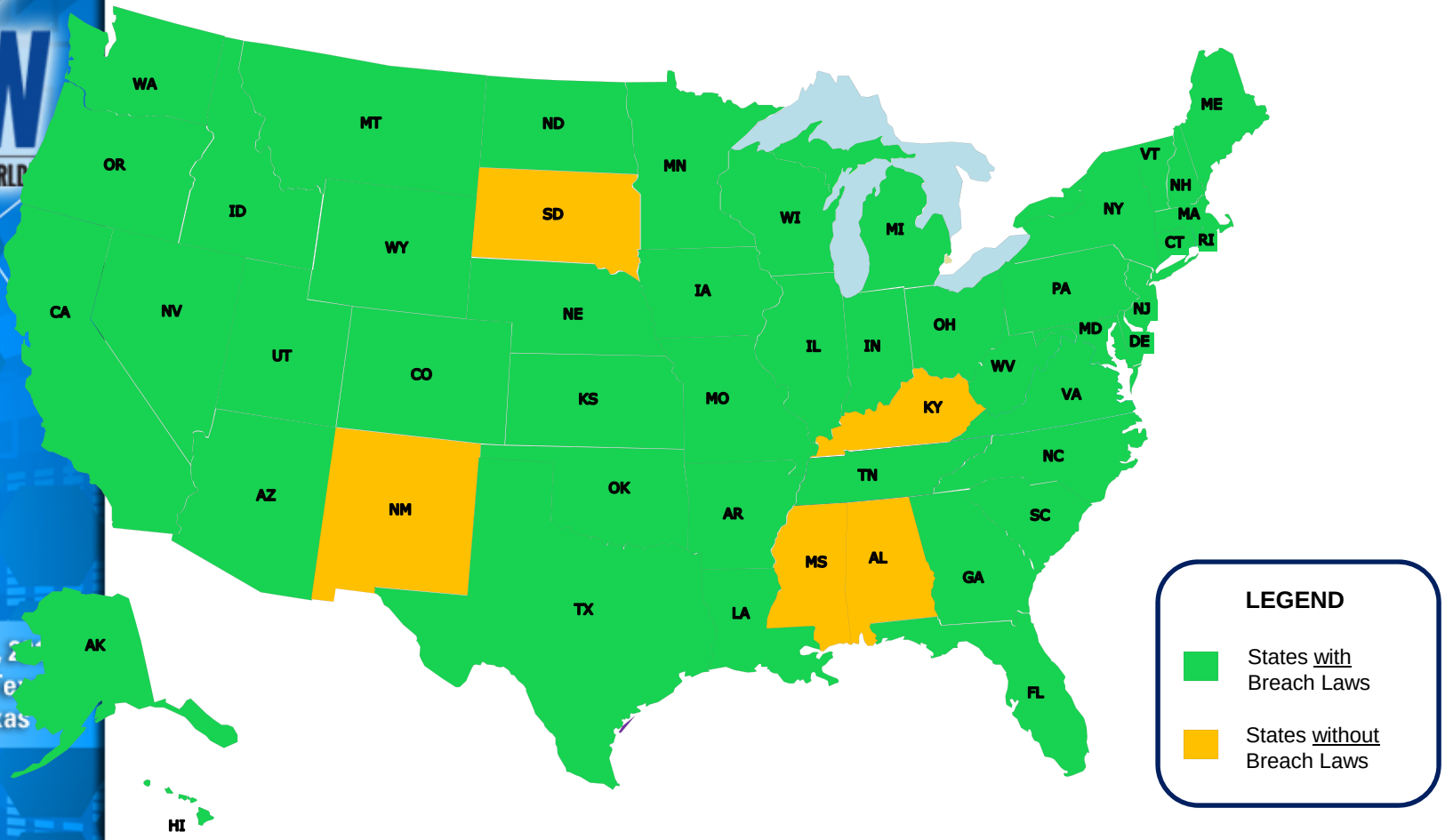
- Organization: Blue Cross Blue Shield
- Breach Type: Stolen Laptop
- No of Records: 850,000
- Date: October 6, 2009

Stolen or Lost Computers are The #1 Cause of Data Breaches



Source: Open Security Foundation DataLoss DB

45 States and the District of Columbia Have Notice of Breach Laws



HITECH

- Safe Harbor for Data Breach Notification Laws
- Amendment to HIPAA Effective Law Feb 17, 2010
- Requires NIST 800-111 for Data At Rest
  - Requires IT Managed Full Disk Encryption Solutions

Feb 17, 2010 : Safe Harbor

- Must Meet NIST SP 800-111

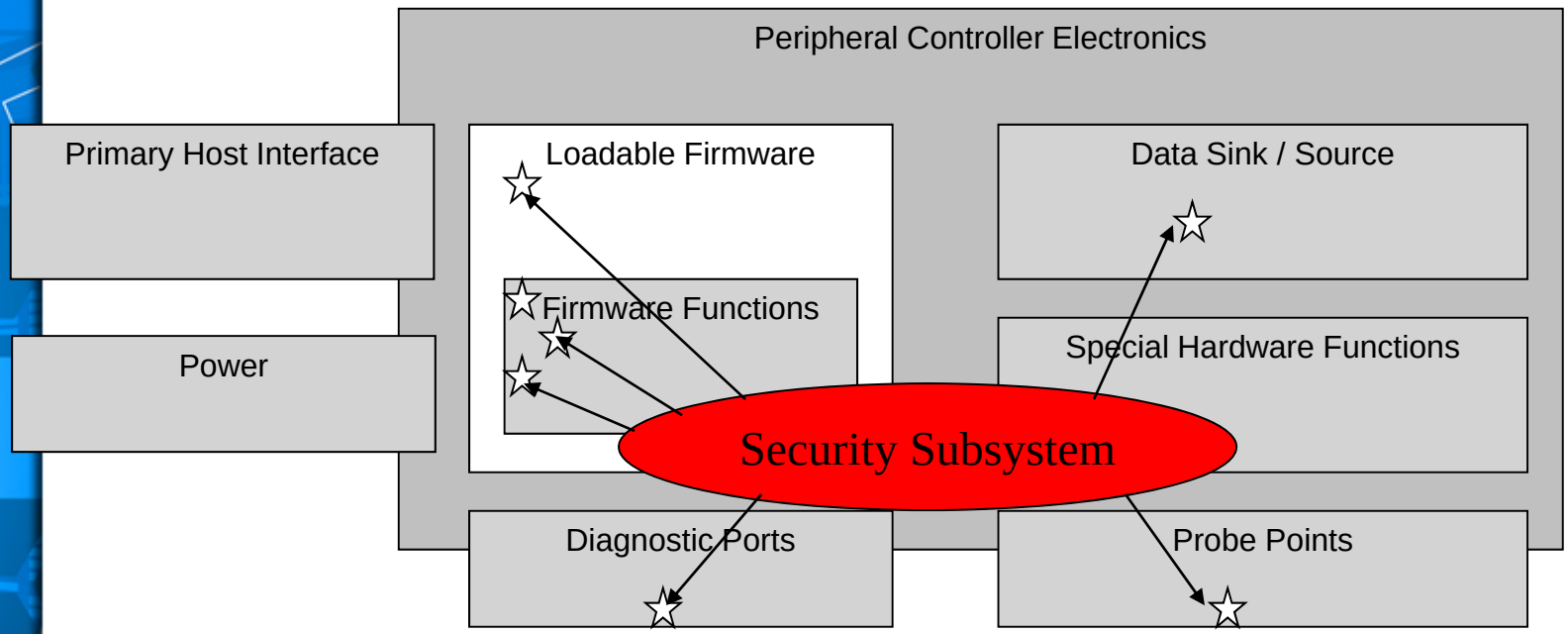
- June 2010 : Now even if a contractor loses PII, you are blamed unless he meets SP 800-111

Completing the Data-at-Rest Security Puzzle

- 800-111 Access control, centralized mgmt and reporting are required

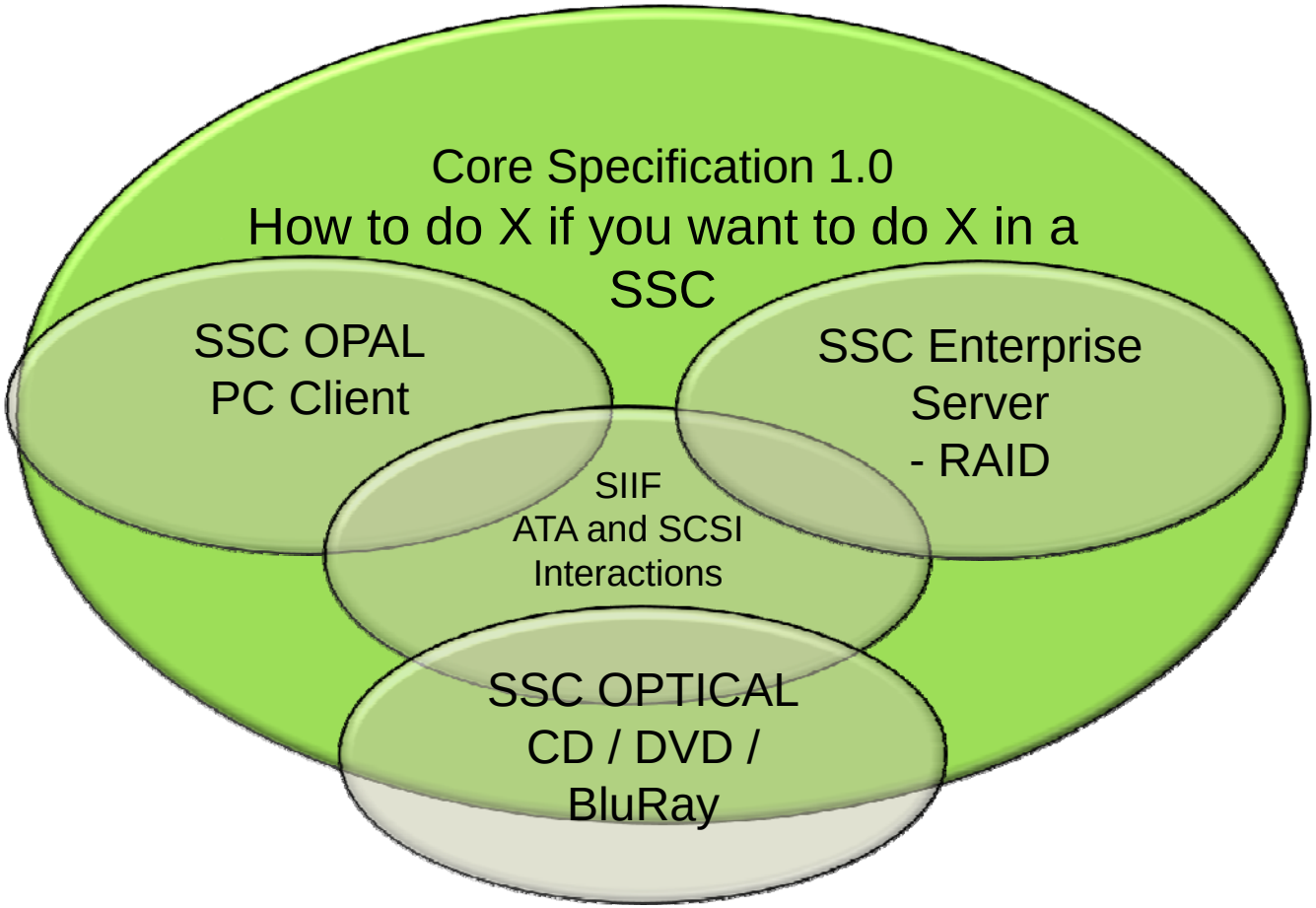
Storage Devices are full scale computers (CPU(s), RAM, ROM, Flash, and lots of secured NV Memory) that are SLAVEs with limited commands.

- Only two ATA and SCSI command sets, TCG adds security subsystem commands that tunnel through ATA and SCSI.



Spec Organization – VENN Diagram

SSC = Security Subsystem Class



How do they work

- KEK not MEK
- Opal and Enterprise: Multiple Bands (Match FS Partitions)
- Opal: Shadow MBR and Preboot
  - Self-Healing MBR & Hypervisor Demo

SED is Secure for Data at Rest

BOOT HYPERVISOR / OS

Kleissner Return from Hibernate Attack

- Hiberfil.sys for rapid ‘winresume’ restart of Windows
  - Changes everytime – not great for TPM measurement!
  - Winresume cannot and does not check programs frozen in hiberfil.sys
  - Hack hiberfil.sys and you can load unsigned code into Windows in returning from hibernation.

- Write malicious MBR to disk via normal application using raw sector access
- Modify hiberfil.sys with MBR record and now the user will unknowingly inject malicious unsigned code into Windows (or, similarly, any OS/hypervisor)

the attack

Kleissner Return from Hibernate Attack

Foiled by measuring MBR in preboot

Problem: Do you stop booting?

Need a Self-Healing Solution to the Kleissner Attack

Demo: Why SED can Provide MBR Boot Integrity

RESUME HYPERVISOR/OS

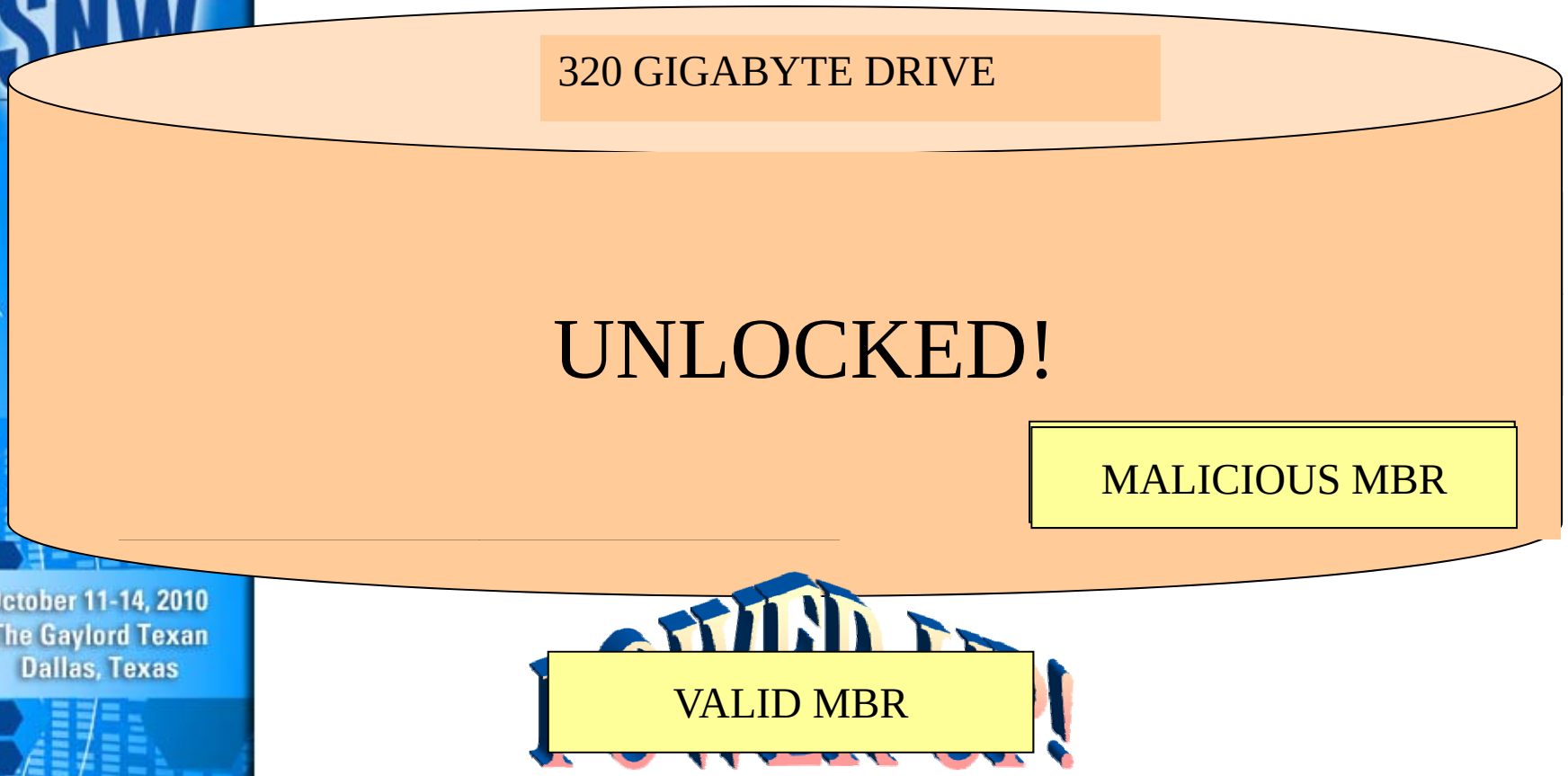


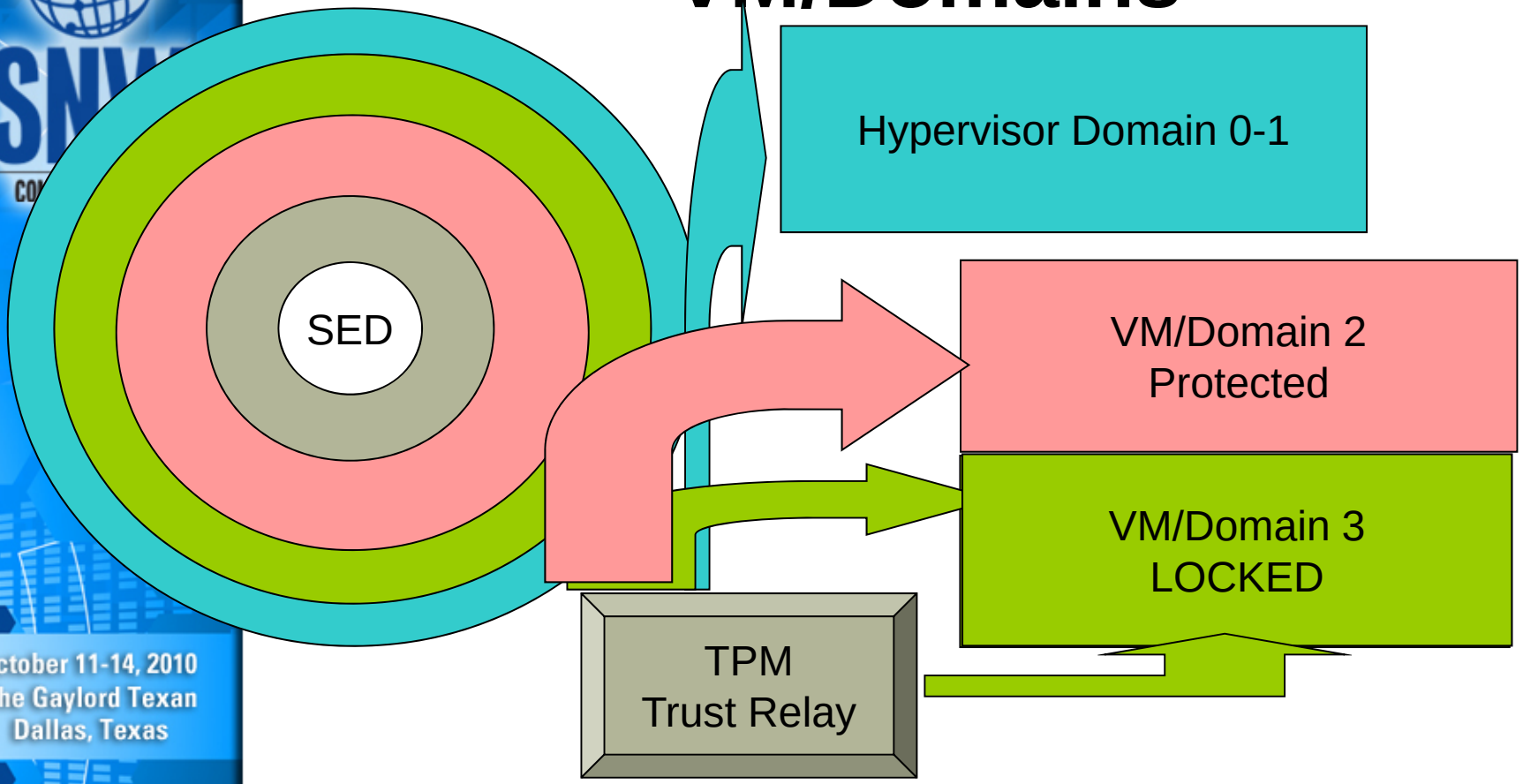
Table 223 LockingInfo Table Description

Column Number	Column Name	IsUnique	Column Type
0x00	UID		uid
0x01	Name		name
0x02	Version		uinteger_4
0x03	EncryptSupport		enc_supported
0x04	MaxRanges		uinteger_4
0x05	MaxReEncryptions		uinteger_4
0x06	KeysAvailableCfg		keys_avail_conds

Table 224 Locking Table Description

Column Number	Column Name	IsUnique	Column Type
0x00	UID		uid
0x01	Name		name
0x02	CommonName		name
0x03	RangeStart		uinteger_8
0x04	RangeLength		uinteger_8
0x05	ReadLockEnabled		boolean
0x06	WriteLockEnabled		boolean
0x07	ReadLocked		boolean
0x08	WriteLocked		boolean
0x09	LockOnReset		reset_types
0x0A	ActiveKey		mediakey_object_uidref
0x0B	NextKey		mediakey_object_uidref
0x0C	ReEncryptState		reencrypt_state
0x0D	ReEncryptRequest		reencrypt_request
0x0E	AdvKeyMode		adv_key_mode
0x0F	VerifyMode		verify_mode
0x10	ContOnReset		reset_types
0x11	LastReEncryptLBA		uinteger_8
0x12	LastReEncStat		last_reenc_stat
0x13	GeneralStatus		gen_status

Multi-band and HAP VM/Domains



TCG Opal is minimum of 4 bands

Controller SP

- Recent announcement of post sales CPU performance upgrade
- Controller SP – Methods for configuring drive personalities under cryptographically strong activation / deactivation.

Thanks!

See Technical Article Steven Teppler on Current Compliance Laws