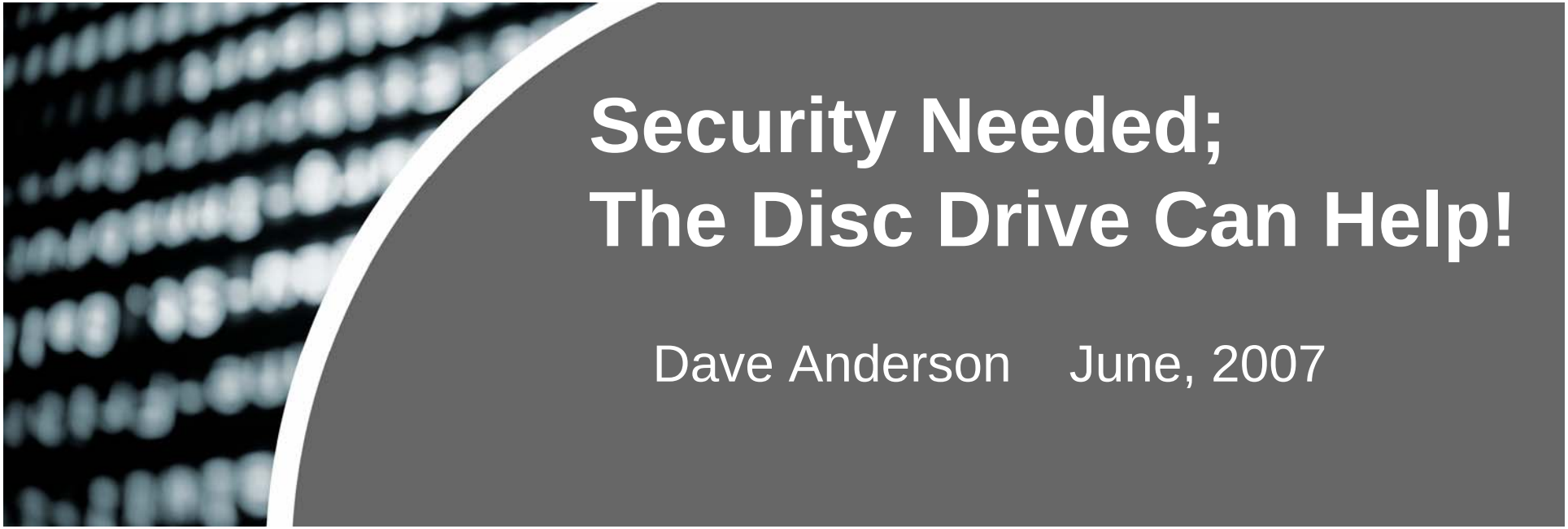


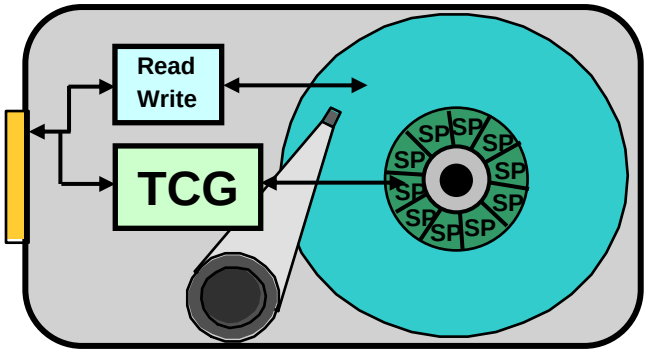
Security Needed; The Disc Drive Can Help!

Dave Anderson June, 2007

TCG: A New Identity for Hard Drives

Traditional: HDDs store & retrieve data

New: HDD-resident security functions



Components:

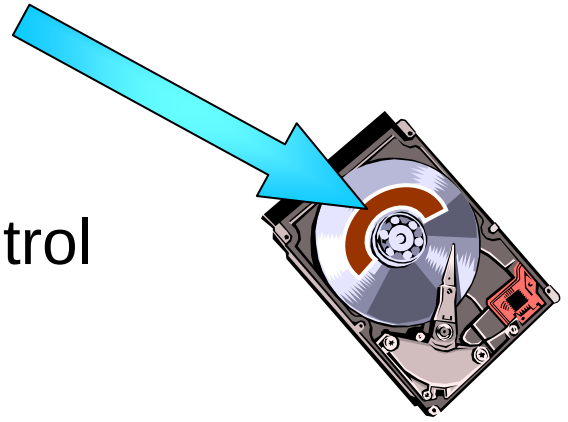
Secret storage (SP's, or Service Providers)

- Inaccessible to standard Read/Write
- Multiple, separate spaces, each hidden from each other & secure
- Impervious to reformat, OS load, virus attack
- Securely issued, access controlled by owner

Operations (Methods)

- Create, manage, deactivate SP's
- Create, store, retrieve information in SP's
- Perform cryptographic operations – encrypt, decrypt, sign, hash, etc
- Provide services: logging, secure clock, RNG
- All with access control – permit only authorized operations

Why Security in the HDD



Storage for secrets with strong access control

- Inaccessible using traditional storage access
- Arbitrarily large
- Uncircumventable gate to access

Unobservable cryptographic processing of secrets

- Processing unit united to storage
- Secrets can be cryptographically processed in secret

Custom logic for faster, more secure operations

- Inexpensive implementation of modern cryptographic functions
- Makes feasible complex security operations

Typical Cryptography

Asymmetric encryption

- RSA 1024 and 2048
- EC under consideration

Symmetric encryption

- 3DES (current product)
- AES-128 => AES-256

Hashing

- SHA-1, SHA-256

Random number generation

- High quality RNG

TCG SP's: "Secret Playgrounds"

Secure allocation of disk space

Exclusively controlled by owner

Owner creates tables of data & defines methods

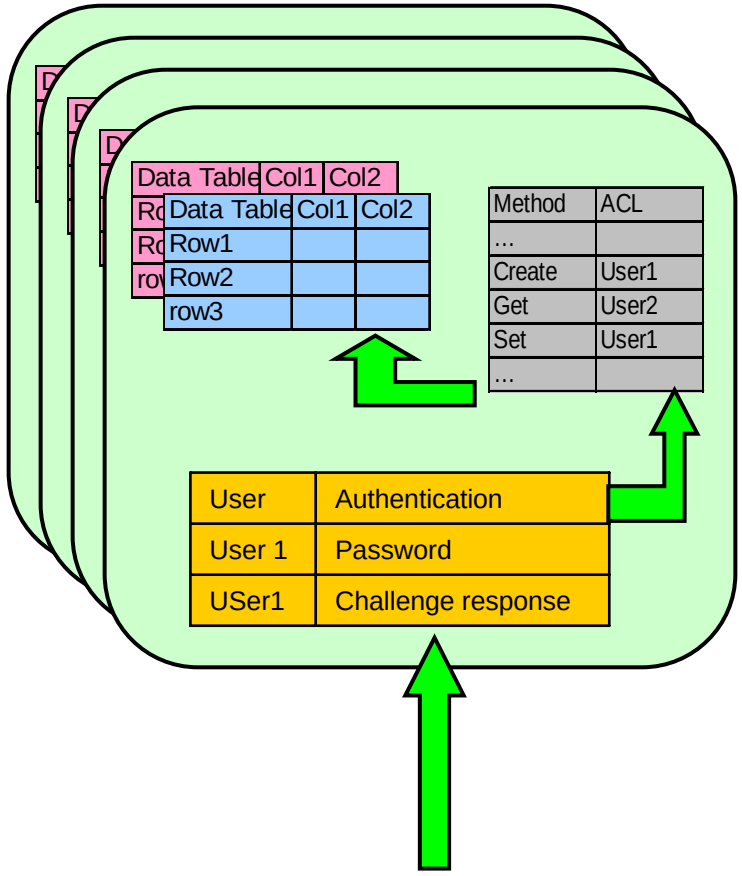
Each method has related access control

Owner can assign subset of uses to another

Some SP's are predefined for specific use

Each SP consists of several tables:

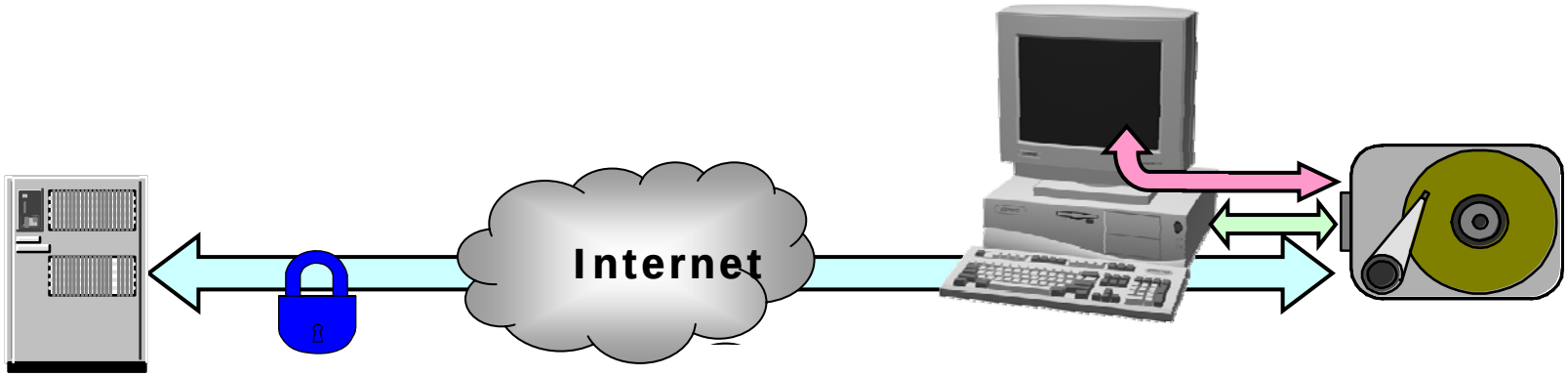
- Authentication – Who is allowed in
- User/method Table – what each authorized user is allowed to do
- Data Tables – some predefined, Application can create others



Root of Trust & Secure Communications

HDD security services can establish secure channel

- Can pass through untrusted BIOS, OS, app, WWW
- Can create session keys & secure sessions
- Can issue and respond to challenge/response sequences
- Supports PKI signing and verification
- Supports MAC & HMAC
- Has X.509 certificates for authentication



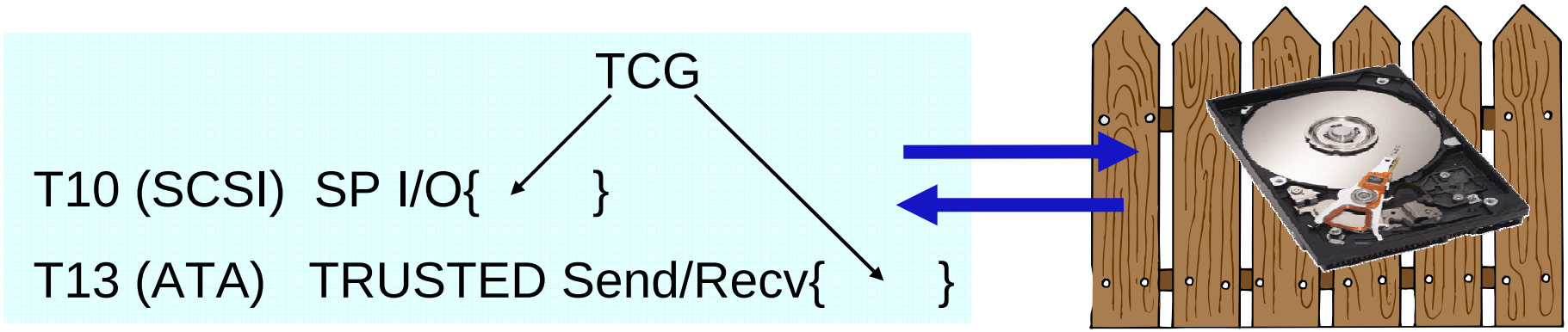
Standards Strategy

Security experts develop security access method (TCG)

Storage experts develop transportation (ATA & SCSI)

Get them to work together

Make usable by other security applications (Protocol ID: TCG, …)

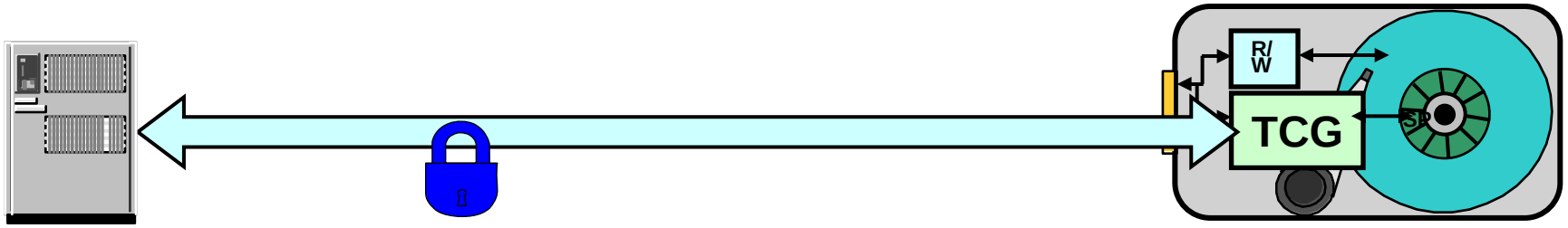


A New Model for Secure Storage

HDD = Root of Trust, encapsulated security server

TCG protocol = standard interface

- For secure messaging
- For invoking other security services
- Single set of methods for any security application
- For managing encryption function



Problem to be Solved: Unprotected Data

"We deeply regret this incident."
Kevin Kessinger, EVP CitiGroup


CitiFinancial Loses Data On 4 Million Customers

Protect Data: Loss of system should not mean data loss

- Laptop loss or theft
- Loss or theft of other equipment, like servers
- Asset re-purposing
- Secure disposal

Hard Drive-based Full Disc Encryption

Purposes

- Protect data from exposure due to equipment loss
- Enable instant, cryptographic erase of drive

Closed encrypting device

- Key can be generated in drive during manufacturing
- Key never leaves drive (except in an encrypted escrow)
- Encryption cannot be turned off
- Encrypted data not accessible
  - Security – protects against traffic analysis based attack
  - Business – no export restrictions
- Encryption bandwidth advantage when used in aggregated drives
- TCG protocol for encryption management, key management

Where is the Pain: In Servers, too

- 11/3/2004: Wells Fargo reported the theft of four servers from a company that prints loan statement leaves thousands of consumers who have taken out loans or obtained mortgages from Wells Fargo at risk from potential identity fraud, AP reports.

- Idaho Power said it hired Grant Korth of Nampa, Idaho, to recycle about 230 SCSI drives. Korth sold 84 of those drives to 12 parties, which have not been disclosed by the company, using the eBay Web site.

- Thieves who stole a number of laptops from VBi Triscan Systems also lifted hard disks from the fuel management firm's servers sometime between Tuesday, 27 March, and Saturday, 31 March

- Plus …

U.S. Federal and State Privacy Laws , plus…

There are 6 significant U.S. bills under consideration:

- **S 239 Notification of Risk to Personal Data Act of 2007**
- **HR 516 Federal Agency Data Privacy Protection Act**
- **HR 836 Cyber-Security Enhancement and Consumer Data Protection Act of 2007 (criminal law)**
- **HR 1685 Data Security Act of 2007‘**
- **S 495 Personal Data Privacy and Security Act of 2007**
- **S 1178 Identity Theft Prevention Act (Inouye)**

35 states have passed laws on data privacy w/ encryption safe harbors

Payment Card Industry Data Security Standard

GLB, HIPAA have data protection provisions

Personal Information Protection Law in Japan, of 2005

Presidential Order of June 26, 2006 (OMB)

U.S. Federal and State Privacy Laws Survey

Current bills:

S 239 Notification of Risk to Personal Data Act of 2007 (see S 495)

HR 516 Federal Agency Data Privacy Protection Act

SEC. 3. REQUIREMENT FOR USE OF ENCRYPTION FOR SENSITIVE DATA.

(a) Requirement for Encryption-

(1) IN GENERAL- All sensitive data maintained by the Federal Government, including such data maintained in Federal computer systems, shall be secured by the use of the most secure encryption standard recognized by the National Institute of Standards and Technology.

(2) UPDATING REQUIRED EVERY 6 MONTHS- Any sequence of characters (known as an encryption key) used to secure an encryption standard used on Federal computer systems shall be changed every 6 months, at a minimum, to provide additional security.

HR 836 Cyber-Security Enhancement and Consumer Data Protection Act of 2007 (criminal law)

(B) PRESUMPTION- If the data in electronic form containing a means of identification involved in a suspected breach has been encrypted, redacted, requires technology to use or access the data that is not commercially available, or has otherwise been rendered unusable, then there shall be a presumption that the breach has not caused a significant risk of identity theft. …

SEC. 8. PENALTIES FOR SECTION 1030 VIOLATIONS.

(c)(1) The punishment for an offense under subsection (a) or (b) is a fine under this title or imprisonment for not more than 30 years, or both.

U.S. Federal and State Privacy Laws Survey

HR 1685 Data Security Act of 2007

(3) BREACH OF DATA SECURITY-

(A) IN GENERAL- The term `breach of data security' means the unauthorized acquisition of sensitive account information or sensitive personal information.

(B) EXCEPTION FOR DATA THAT IS NOT IN USABLE FORM-

…

(ii) RULE OF CONSTRUCTION- For purposes of this subparagraph, information that is maintained or communicated in a manner that is not usable includes any information that is maintained or communicated in an encrypted, redacted, altered, edited, or coded form.

S 495 Personal Data Privacy and Security Act of 2007

b) Safe Harbor- An agency or business entity will be exempt from the notice requirements under section 311, if--

(1) a risk assessment concludes that--

(A) there is no significant risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach, with the encryption of such information establishing a presumption that no significant risk exists; or

S 1178 Identity Theft Prevention Act (no explicit encryption safe harbor)

(c) NOTIFICATION OF CONSUMERS-

(1) IN GENERAL- … In determining whether a reasonable risk of identity theft exists, a covered entity shall consider such factors as whether--

(A) data containing sensitive personal information is usable or could be made usable by an unauthorized third party; …

Existing Laws - GLB

Gramm-Leach-Bliley Act
15 USC, Subchapter I, Sec. 6801-6809

Sec. 6802. Obligations with respect to disclosures of personal information

a) Notice requirements

Except as otherwise provided in this subchapter, a financial institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless such financial institution provides or has provided to the consumer a notice that complies with section 6803 of this title.

HIPAA

Public Law 104-191

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

§ 164.312 Technical safeguards.

A covered entity must, in accordance with §164.306:

(a)(1) *Standard: Access control.* Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).

(2) *Implementation specifications:*

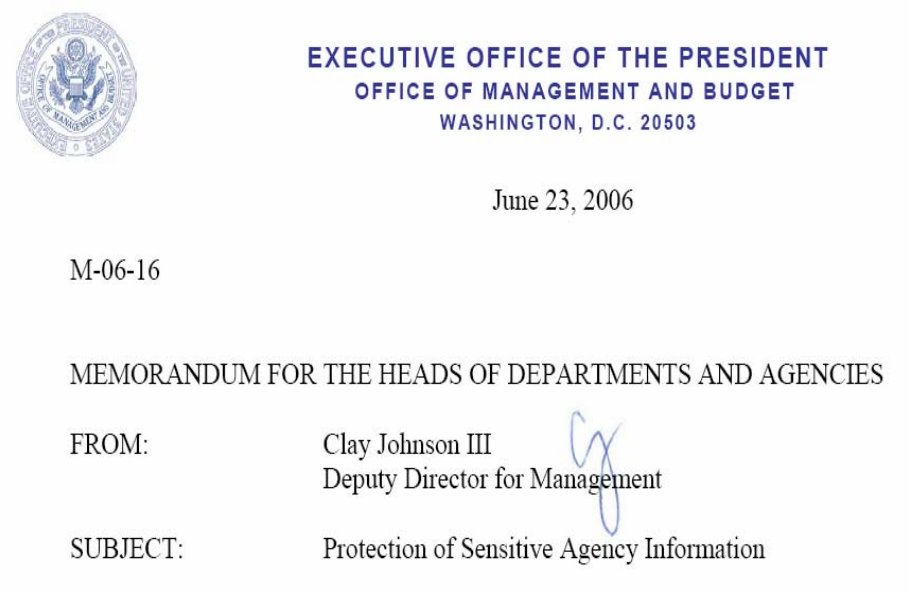
…

(iv) Encryption and decryption (Addressable).

Implement a mechanism to encrypt and decrypt electronic protected health information

…

And from the President:



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

June 23, 2006

M-06-16

MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

FROM: Clay Johnson III
Deputy Director for Management

SUBJECT: Protection of Sensitive Agency Information

…

In addition to using the NIST checklist, I am recommending all departments and agencies take the following actions:

1. Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing;

2. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access; …

Enacted State Data Protection Laws (as of 6/2007)

State *	Law	Effective
Arkansas	SB 1167	6/1/2005
California	SB 1386	7/1/2003
Connecticut	SB 650	1/1/2006
Delaware	HB 116	6/28/2005
Florida	HB 481	7/1/2005
Georgia	SB 230	5/5/2005
Idaho	SB 1374	07/01/06
Illinois	HB 1633	1/1/2006
Indiana	SB 503	7/1/2006
Louisiana	SB 205	1/1/2006
Maine	LD 1671	1/31/2006
Minnesota	HF 2121	1/1/2006
Montana	HB 732	3/1/2006
Nevada	SB 347	10/1/2005
New Jersey	A4001	1/1/2006
New York	AB 4254/ SB 5827	12/7/2005
North Carolina	SB 1048	2/17/2006
North Dakota	SB 2251	6/1/2005
Ohio	HB 104	2/17/2006
Pennsylvania	SB 712	7/1/2006

New State Laws	Law	Signed
Rhode Island	HB 6191	7/10/2005
Tennessee	HB 2220	7/1/2005
Wisconsin	SB 164	/31/2006
Utah	SB 69	1/1/2007
Washington	SSB 6043	7/23/2005
Arizona	SB 1338	4/26/2006
Colorado	HB 06-1119	4/26/2006
Hawaii	SB 2290	5/25/2006
Kansas	SB 196	4/19/2006
Nebraska	LB 876	4/10/2006
New Hampshire	HB 1660	6/22006
Michigan	SB 309	12/30/2006
Oklahoma	HB 2357	6/6/2006
Vermont	SB 284	5/18/2006
Texas	Bus. & Com. Code § 48.001	9/1/2005

Payment Card Industry

Protecting financial information is paramount. All major credit card issuers have agreed upon the new **Payment Card Industry (PCI) Data Security Standard** to protect cardholders' information and transactions.

The new standard defines new security requirements and best practices for credit card data that is processed, transmitted or stored via e-commerce, e-mail, POS, web sites, and customer databases.

Most merchants and service providers are required to comply with this standard by June 30, 2005 or face penalties, including fines and loss of the ability to accept credit cards. Failure to comply is a business risk not to be taken lightly. http://www.vigilantminds.com/sols_spci.php

FIVE LEADING PAYMENT BRANDS UNITE TO STRENGTHEN GLOBAL DATA SECURITY

WAKEFIELD, Mass. Sept. 7, 2006 - American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International today jointly announced the formation of an independent council designed to manage the ongoing evolution of the Payment Card Industry (PCI) Data Security Standard, which focuses on improving payment account security throughout the transaction process. https://www.pcisecuritystandards.org/

Will the PCI Security Standards Council enforce compliance?
No, the PCI Security Standards Council will not be replacing the individual brands' compliance programs. The individual participating payment brands will separately determine what entities must be compliant, including any brand-specific enforcement programs.
https://www.pcisecuritystandards.org/about/faqs.htm#q13

Payment Card Industry Data Security Standard

Note that these Payment Card Industry (PCI) Data Security Requirements apply to all Members, merchants, and service providers that store, process or transmit cardholder data. …. Applications include all purchased and custom applications, including internal and external (web) applications.

Requirement 3: Protect Stored Data

Encryption is the ultimate protection mechanism because even if someone breaks through all other protection mechanisms and gains access to encrypted data, they will not be able to read the data without further breaking the encryption. This is an illustration of the defense in depth principle.

…

3.4 Render sensitive cardholder data unreadable anywhere it is stored (including data on portable media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:

- One-way hashes (hashed indexes), such as SHA-1
- Truncation
- Index tokens and PADs, with the PADs being securely stored
- Strong cryptography, such as Triple-DES 128-bit or AES 256-bit with associated key management processes and procedures.

3.5 Protect encryption keys against both disclosure and misuse.

3.5.1 Restrict access to keys to the fewest number of custodians necessary

3.5.2 Store keys securely in the fewest possible locations and forms.

…

http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf#search=%22%20%22cisp_PCI_Data_Security_Standard.pdf%22%22

Personal Information Protection Law in Japan

Date of Enforcement: April 1, 2005

Background – The Japanese government has recognized the value of personal data and oblige private corporations and public organizations to protect it (for the benefit of all the parties involved).

Example of Incidents happened in the past 12 months

*** Jananet Takada**
Leaked 660K customer data and lost billions of yens because they had to stop TV sales.

*** Uji City Hall**
Leaked 190K resident data base and the court demeaned the city government pay $150 to each resident for compensation ($30M in total)

*** Lawson (Chain Convenience Store)**
Had to issue a $5 voucher to one million customers

* A series of same incidents happened NTT DoCoMo, Yohoo BB, Familiymart (Chain convenience store) and Tomato Bank

Summary of "Before" and "After" the Law Enforcement

	Before	After
Customer (Personal) Data	**Protected as "IP of corporations" or "Trade Secrets"**	**No longer treated as "IP of corporations"**
Disclosure of Personal Data	**Whatever the reason is, corporations are not legally obliged to disclose personal data**	**Obliged to disclose what personal data (of a person) corporations have when requested by such person**
Use of Personal Information	**Even when personal information is used for any purpose, no obligation to explain the reason to anybody**	**When personal information (of a person) is used, the purpose of such use is to be informed of the person before the information is used.**
Penalty for Information Leakage	**Compensation through civil lawsuit**	**Compensation through civil law suit and Administrative sanction**

Enterprise Computing FDE

Unlike Personal Computer or Notebook

- Aggregation
- Behind array controllers
- No internet access

3 key components

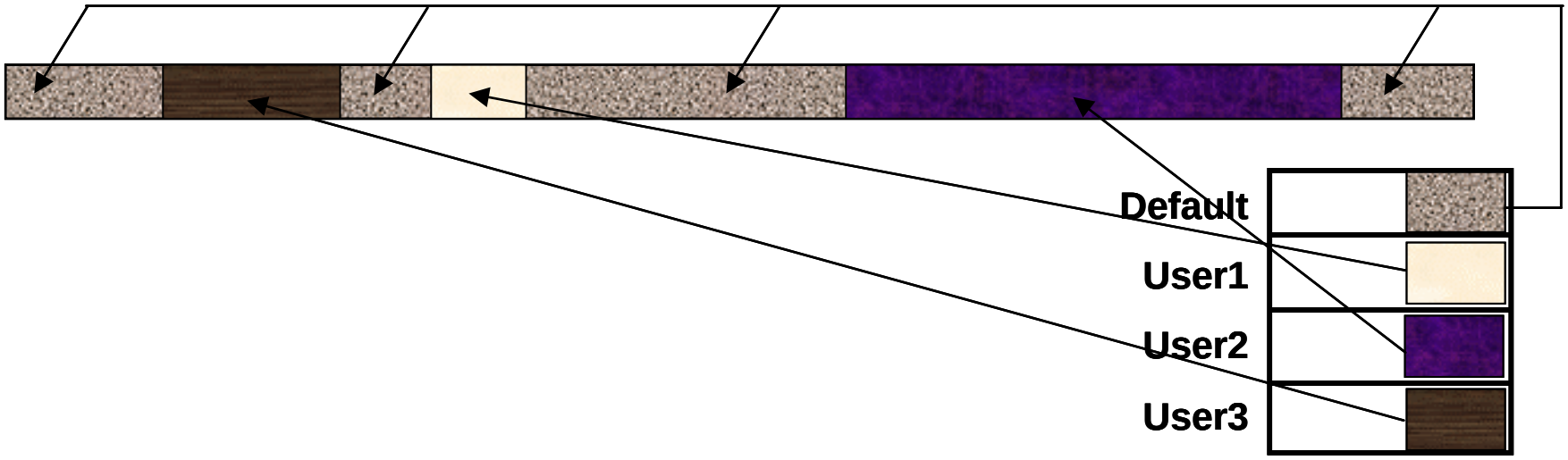
- FDE drives
- FDE support in array controllers
- Key management access
  - Independent of array controller
  - Need industry standard API

TCG Encryption Ranges

User can create non-overlapping bands. Owner of each range can allow 4 access conditions: no access (no key loaded), read only, write only and full access (read + write) allowed

Ranges cannot overlap and may be required to start on a particular LBA multiple (i.e. start and end sector must be divisible by 16)

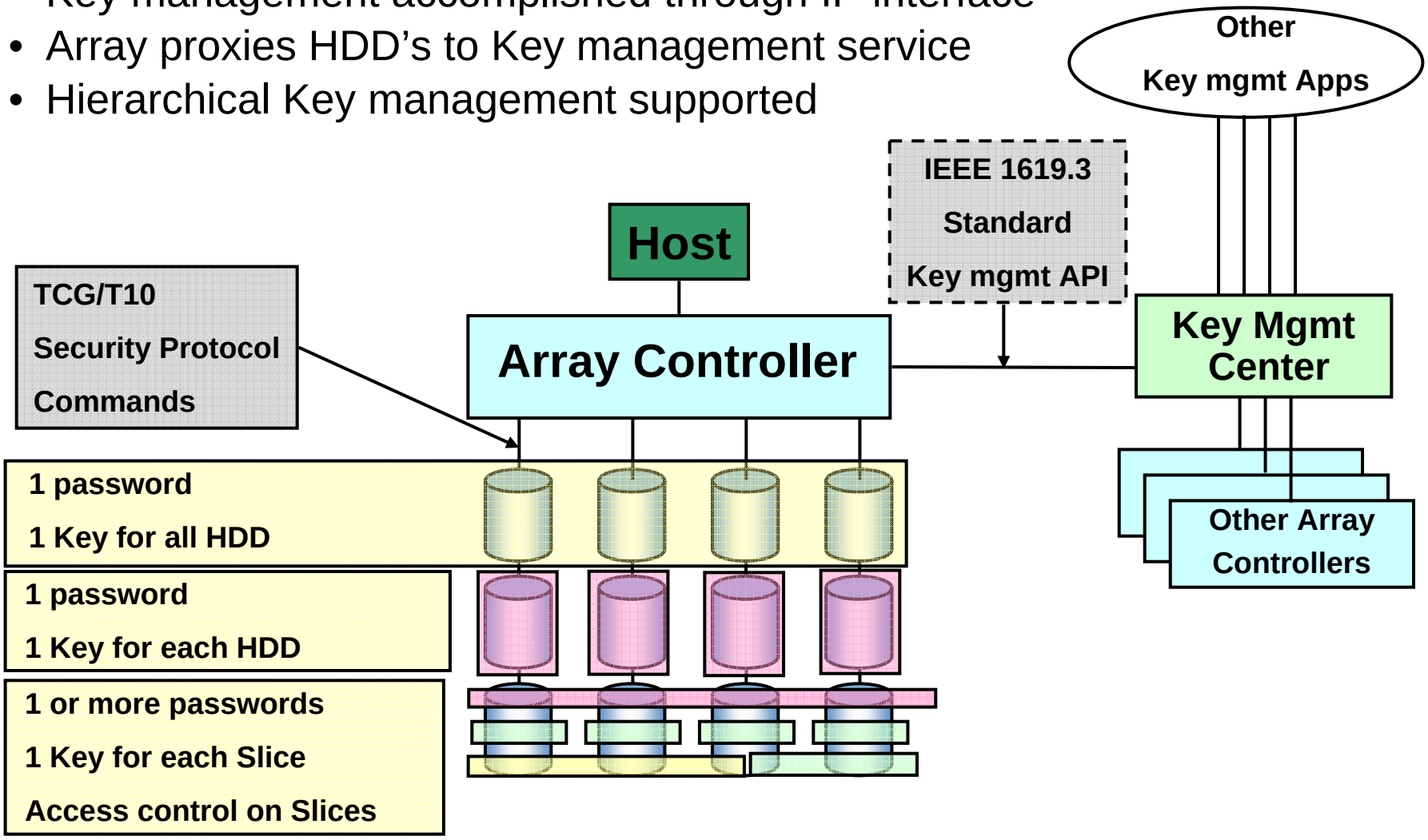
Default key applies to areas not covered by user bands



Key Management Possibilities

Key Management – via standard API

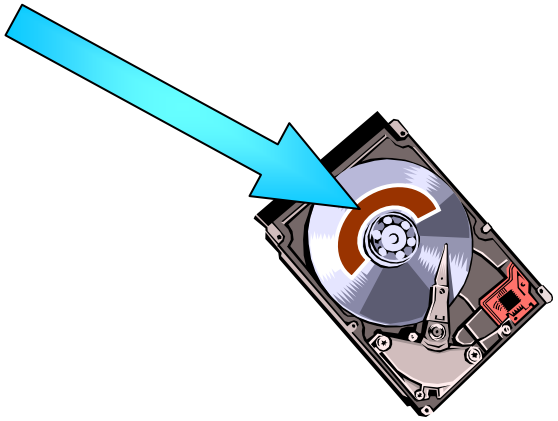
- Key management accomplished through IP interface
- Array proxies HDD's to Key management service
- Hierarchical Key management supported



TCG Use Cases

Enrollment and connection

Protected storage: impervious to unauthorized access



Locking and Encryption

Forensic Logging

Cryptographic Services, such as:

- Hashing: SHA-1, SHA-256
- Symmetric encryption/decryption: AES-128
- Public key encryption/decryption: RSA, ECC(?)
- Random number generation
- Secure messaging

Industry Supporting Activity

TCG Storage Working Group

- Developing standard for HDD-based security
  - Includes FDE, encryption bands, secure partition (SP), other features
  - Standard almost complete (expected public release in June)
  - Supporting transport commands in T13 and T10 are ratified

- Chartered a subcommittee to address EC Key management
  - Will develop use cases for IEEE
  - Walt Hubis of LSI is chair of KMSS

P1619.3 Key Management

- Matt Ball of Quantum is chair
- Umbrella key management standards group
- FDE key management will be a subset

TCG-Based HDD Security Benefits

Strongly resistant to network (malware) attacks

Specific advantages for encryption use case

- Recent headlines emphasize the need for data protection
- User cannot turn off FDE encryption
- Offers instant cryptographic erase

TCG standard interface enables software to integrate FDE with other security functions & provide key management

TCG protocol provides common methods for a wide range of security applications