Data & Report Security in VSE

Tony Thigpen

Thigpen Enterprises, Inc

Tony@VSE2PDF.com

- Regulatory
  - Sarbanes Oxley Act (SOX) – 2002
- Data Protection / Privacy Laws
  - Federal Laws
    - Gramm-Leach-Bliley Act – 1999
    - Health Insurance Portability and Accountability Act (HIPAA) – 1996
    - Fair Credit Reporting Act
    - And more
  - State Laws
    - California Online Privacy Protection Act (OPPA) – 2003
    - Restrictions on Social Security Numbers
  - Business Requirements
    - VISA-CISP, MasterCard, Discover, AMEX

We Must Protect

- Personally Identifiable Information (PII)
  - Name
  - SSN
  - Etc.
- Sensitive Data
  - Account Number
  - Credit Card Number
  - Etc.

VISA-CISP

“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.”

VISA-CISP

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)…

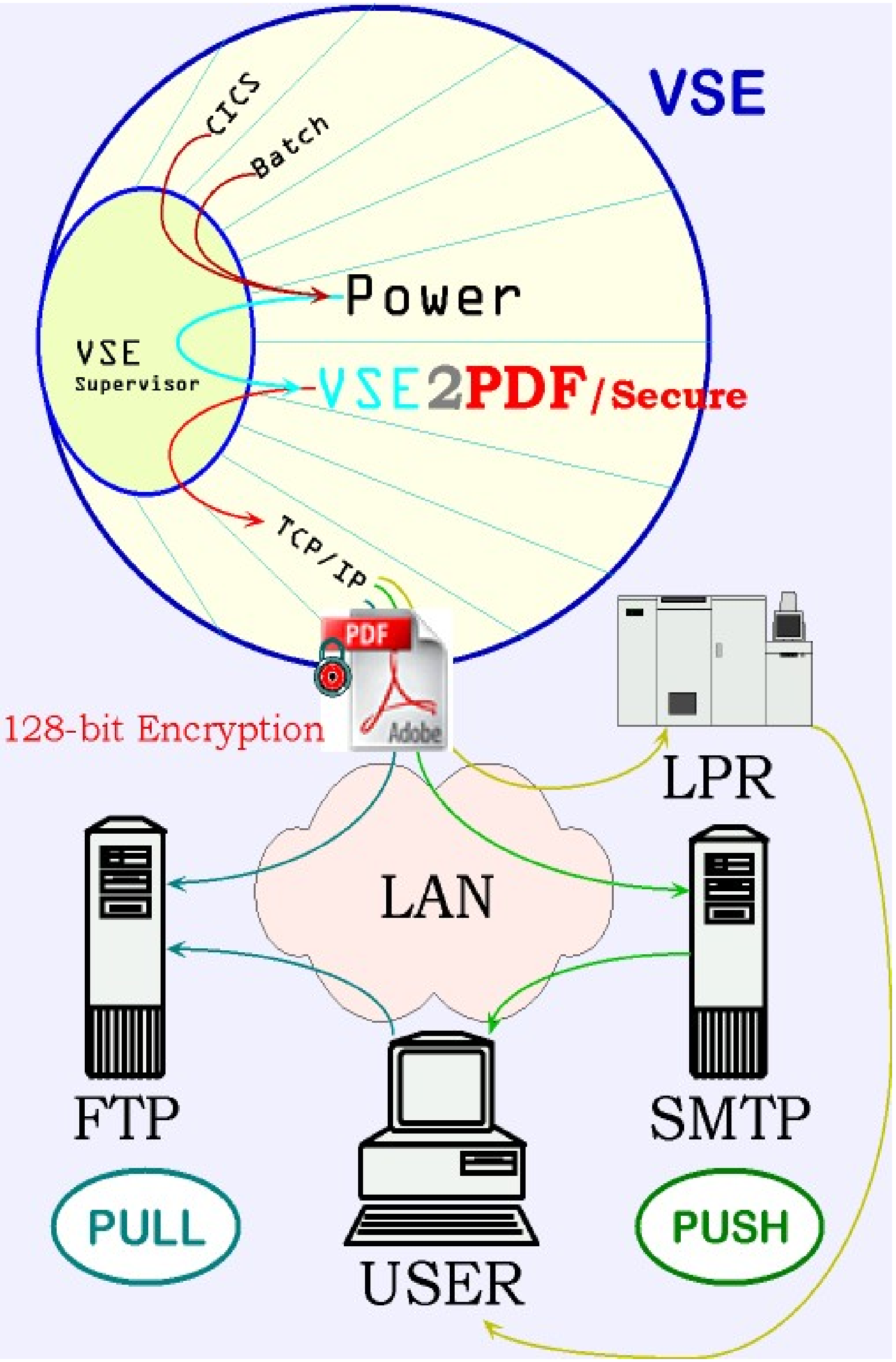
(Excerpts from "Payment Card Industry Data Security Standard")

TEI was the first in VSE with:

- 2Q 2004 – Report Encryption
  - VSE2PDF/Secure
- 2Q 2005 – HLL Data Encryption API
  - Dino-Protect
- 4Q 2005 – Tape Backup Encryption
  - Dino-Protect/IDCAMS
  - Dino-Protect/TC (Tape Copy)
- 2Q 2006 – File System Encryption (Disk & TAPE)
  - Dino-Protect/FS (File System)

VSE2PDF/Secure

2Q 2004


VSE
CICS
Batch
Power
VSE
Supervisor
VSE2PDF/Secure
TCP/IP
PDF
Adobe
128-bit Encryption
LPR
LAN
FTP
SMTP
USER
PULL
PUSH

VSE2PDF/Secure

- Internal PDF encryption using a 128 bit key
- HIPAA (Health Insurance Portability and Accountability Act)
- Protection from unauthorized update
- Non-exportable to some countries
- Requires the VSE2PDF base product

Dino-Protect

- The Dino-Protect product is a group of several utilities designed to help a shop satisfy audit requirements in the area of data encryption
- Although we have distinctive names for the different pieces, they are only sold as one product bundle

Dino-Protect/API

2Q 2005

Dino-Protect/API

- The original Dino-Protect product
- The base for the current Dino-Protect product line
- Does not require or use special CPU hardware or hardware features.

Dino-Protect/API

- Is a series of custom subroutines that can be called by any programming language or utility.
- Unique to each organization
- Three 128bit key seeds
  - Company level (known only to TEI)
  - Module level (known only to TEI)
  - Record level (known only to organization)

What are “key seeds”?

- A key seed is input to a routine that generates the real encryption key
- The “company seed” is processed by a sophisticated routine to “scramble” the seed
- The “module seed” is combined with the resulting scrambled seed which is then scrambled again.
- The “record seed” is combined with the resulting scrambled seed which is then scramble again.
- A final “scramble” creates the “real” encryption key.
- Nobody has access to the final encryption key. The original subroutine must be used to decrypt the data.

Dino-Protect/API

These custom modules are the property of the organization and can be used as needed in perpetuity. In other words, TEI will not hold any organization's data hostage. There is NO annual fee to use these modules.

Dino-Protect/API

A word on encryption methods.

- Anything less than 128bits is not secure.
- Symmetric vs. Asymmetric
  - Symmetric – one key
  - Asymmetric – two keys
- Stream Cipher vs. Block Cipher
  - We could not use the newest AES standard because it is a Block Cipher and requires the results to be stored in fields to have lengths that are multiples of 16 thus:
    - All record definitions would then require changes

Dino-Protect/API

- Dino-Protect uses a 128bit Symmetric Stream Cipher
- Auditors ask: Is this secure “enough”?
- The U.S. Department of Commerce still prohibits export of any 128bit symmetric cipher without a prior “determination of export eligibility” and/or individual export permission
- Dino-Protect allows for a different encryption key for each record to prevent “brute force” decryption

Dino-Protect/API

- Performance
  - Customer report that while a small increase in CPU usage results with the use of Dino-Protect, the increase were well within acceptable expectations, even on small CPU boxes
  - Yes, CPU will increase, but that is a function of encryption

Dino-Protect/IDCAMS

4Q 2005

Dino-Protect/IDCAMS

- Provides a new option to IDCAMS
  - “ENCRYPT” (“EN”)
  - “NOENCRYPT” (“NEN”)
- TEI provides a replacement “IDCAMS” phase that is to be placed in a special sublibrary. We also copy the original IDCAMS phase to a new name in that special library so we can call the IBM phase after we patch (“on the fly”) the new encryption function into the IBM phase.

Dino-Protect/IDCAMS

- Performance / CPU usage
  - A quick comparison of “total CPU” between creating encrypted and non-encrypted may lead to the INCORRECT conclusion that we are using a lot of CPU because you may see as much as a 400% increase of CPU. The fact is that IDCAMS was designed to use very little CPU so the non-encrypted CPU usage numbers create a very low divisor that skews the calculation.

Dino-Protect/IDCAMS

- Performance / Real “wall clock” time
  - Since tape backups spend a huge amount of time waiting on the tape device, the CPU cycles used to encrypt the tape do not appear to affect the total time used to create the backup UNLESS the CPU is already using all available cycles for other tasks.
  - Normally, backups are created during low-CPU usage times, so this may not be a factor at all.
  - Only real testing during the normal backup window will give an accurate indication of performance issues.

Dino-Protect/IDCAMS

- Performance / Tape Usage
  - Encrypted tapes do not compact AT ALL!
    - IDRC (hardware compaction) is ineffective on encrypted backups.
  - The data MUST be compacted prior to encryption or tape usage will double or even triple.

Dino-Protect/IDCAMS

- Performance / Tape Usage
  - Dino-Protect/IDCAMS performs software compaction prior to encryption using compaction routines built into VSE.
  - Only real world testing with your backup data can give an accurate indication of tape usage issues.

Dino-Protect/TC

4Q 2005

Dino-Protect/TC

- Provides a utility to copy unencrypted tapes to an encrypted “tape set”
- Provides a utility to copy an encrypted “tape set” to an unencrypted tape

Dino-Protect/FS

- VISA-CISP:
  - *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)…*
- Dino-Protect/API required program code changes for any program referencing encrypted fields.
- A centralized automatic encryption method was needed.

Dino-Protect/FS

- Dino-Protect/FS answers that requirement
  - Central management of encryption rules
  - Automatic encryption or decryption
  - Avoids encryption/decryption for special phases
    - FTP (VISA-CISP requirement)
    - IDCAMS
    - Other user specified phases
- Only sensitive fields need be encrypted

Dino-Protect/FS

- Intercepts all disk and tape LIOCS I-O calls
- Started at IPL
- Controlled by a single LIBR member
- Special step SETPARMs to override the normal action found in the control member
  - Special phase name overrides
  - Special file name overrides

Dino-Protect/FS

- Encryption/Decryption rules specify which fields to encrypt/decrypt on which records in which file
  - Dataset Selection
  - Record Selection
  - Field Selection

Dino-Protect/FS

- Dataset Selection
  - DSN=
  - DTF=
  - CATDSN=
  - CATDTF=
- Unspecified dataset selections are treated as “wildcards” and are ignored during file selection determination
    - DSN= is required

Dino-Protect/FS

- Record Selection
  - Record test field
    - POS=(pos,length)
    - OFF=(offset,length)
  - Condition
    - EQ
    - NE
  - Compare condition
    - TEXT=
    - HEX=
    - SPACE
    - NULL

Dino-Protect/FS

- Example record test rules
  - WHEN POS(1,2) EQ TEXT=AB
  - WHEN OFF(0,1) EQ HEX=FF
  - WHEN ALWAYS
- Rules are processed in order
- First true condition controls record encryption/decryption

Dino-Protect/FS

- Record encryption key information
  - KEY=(pos,length)
    - Specifies a record level key seed
  - HEXKEY=(32 hex characters)
    - Specifies a true RC4 encryption key
  - If no record level WHEN conditions, specifies the “encryption key” for all records in the file

Dino-Protect/FS

- Field Selection
  - FIELD=(pos,length)
  - OFF=(offset,length)

Dino-Protect/FS

```
CATALOG TEIDINO.CONTROL
DSN=MY.VSAM.FILE
DTF=MYDTF
CATDSN=MY.VSAM.CATALOG
CATDTF=MYCAT
KEY=(1,16)
WHEN POS=(2,2) EQUAL TEXT=ABCDEF
FIELD=(17,25)
FIELD=(50,50)
DSN=YOUR.VSAM.FILE
DTF=YOURDTF
CATDSN=YOUR.VSAM.CATALOG
CATDTF=YOURCAT
/+
```

We Protect You

We want to protect our customers. Most companies do not want anyone to know what encryption product they are running or how it works. To protect all our current and future customers, we will only discuss the sensitive details of the product with prospective customers under a non-disclosure agreement.