Voltage security

Encryption? Yeah, We Do That

Encryption facilities, challenges, and choices on System z

Session 13654

Agenda

- Tour System z encryption facilities
- Survey available IBM products
- Briefly discuss third-party technologies (not products)
- Examine criteria for making intelligent selections
  - ***Not*** judging/comparing products *per se!*

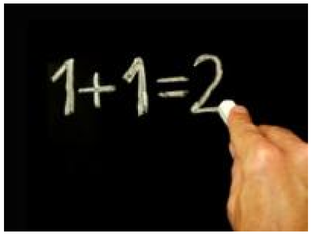
Some Fundamental Points about Encryption

- Encryption is not ***fun***

- Encryption does not make your job easier

- Encryption should not necessarily be noticeable

- Encryption is difficult and complex



So Why Would Anyone Want to Encrypt?

- Regulatory compliance
- Recovery from a breach
- General hygiene (breach prevention)
- ***Not*** encrypting may risk company's future

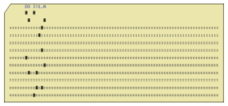
Do We Really Need to Care?

- **Mainframes are secure** – we all “know” this

- ***Not*** something you want to bet your job on!

So You Need To Encrypt Some Data…

- Where will the data live?
  - Network
  - DASD
  - Tape
  - Flash drives
  - DVDs
  - Punched cards
  - Smoke signals
- These are ***different***, require different solutions



Narrowing the Problem

- On mainframes, DASD and tape are the concerns
- DASD and tape are “data at rest”

Hardware vs. Software

- Encryption can be performed by hardware or software

- Crypto import/export controlled by many countries

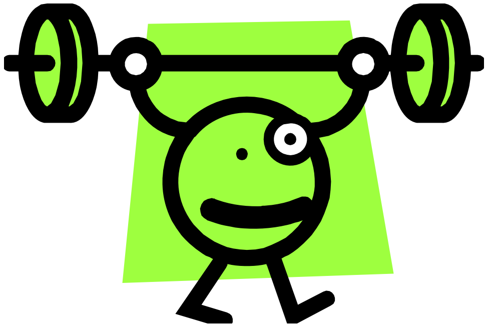
A Word about “Point” Solutions

- Many products include some form of encryption
- Not necessarily secure
- Such point solutions can proliferate

Encryption “Strength”

- Encryption **“strength”** refers to the likelihood that an attacker can “break” encrypted data
  - See “Understanding Cryptographic Key Strength” on **`youtube.com/user/VoltageOne`** for a good discussion/illustration

- The encryption community is collaborative



Proving Encryption Strength

- Cryptographers “cheat” in attacker’s favor when analyzing

- “Weaknesses” reported are often largely theoretical —only NSA could really exploit

More About Proving Encryption Strength

- This “cheating” ensures encryption strength is real*

- Makes it easy to spot the charlatans

*** Well, as real as the smartest minds in the business can make it!**

Voltage security

IBM System Facilities

System z and z/OS encryption capabilities

IBM Common Cryptographic Architecture

- Common Cryptographic Architecture CCA

> "…provides a comprehensive, integrated family of services that employs the major capabilities of the IBM coprocessors"

- Offers robust functionality across all IBM platforms

Integrated Cryptographic Services Facility

- z/OS Integrated Cryptographic Services Facility (ICSF)
- Active area for IBM development
- Powerful, albeit mostly just a toolkit

SSL on System z

- TLS (Transport Layer Security), aka SSL (Secure Sockets Layer), is transport-layer network traffic encryption

- TLS is standard technology, on all platforms nowadays

SSL on System z

- System SSL is IBM’s TLS on z/OS, IBM i, AIX
- Consistent across platforms, though not part of CCA
- Robust, well-documented API

IPSec on System z

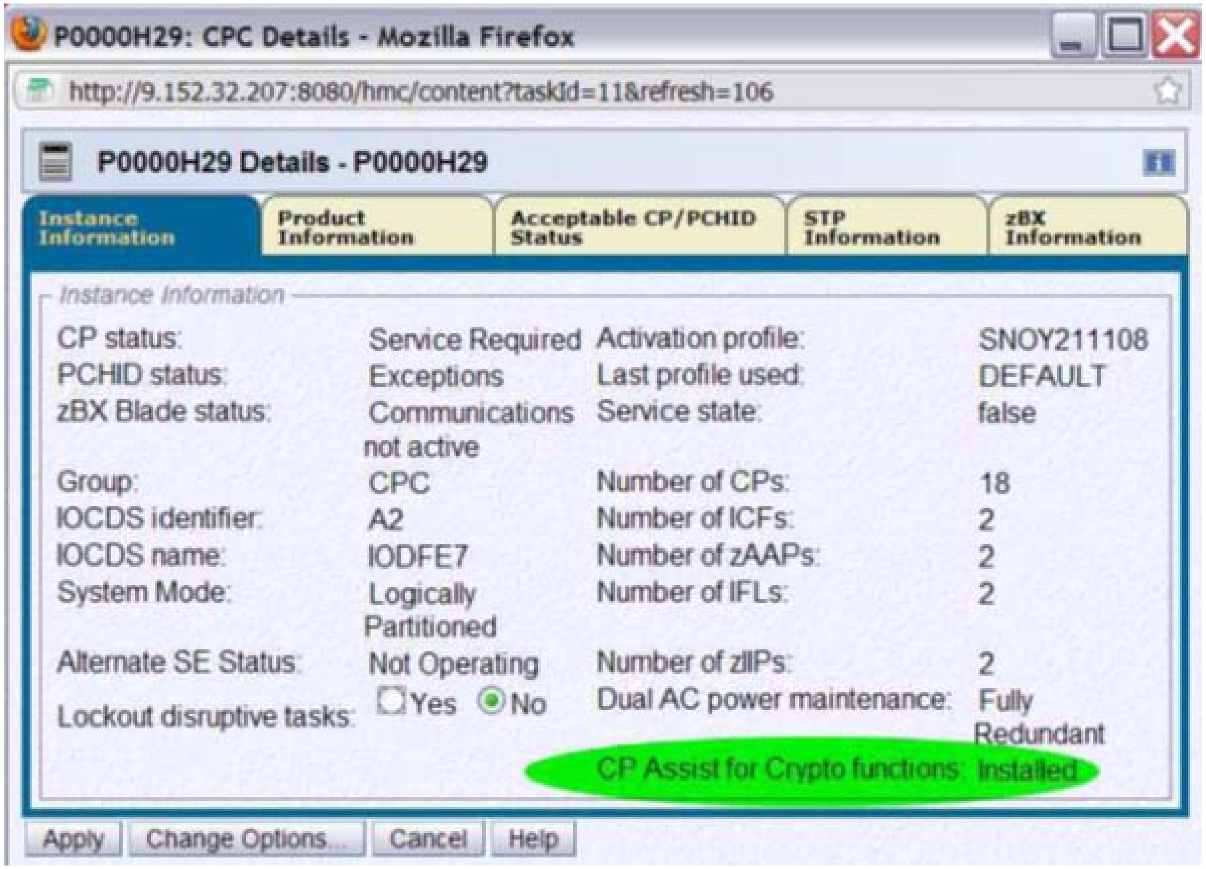
- IPSec is an IP-layer protocol for securing traffic
- Implemented in z/OS TCP/IP

CPACF

- Central Processor Assist for Cryptographic Functions
- Introduced with z9 in 2005
- CPACF reduces CPU usage ***quite*** significantly

CPACF Enablement

- CPACF is free but enabled via Feature Code 3863
- “How do I tell whether CPACF is enabled?”


P0000H29: CPC Details - Mozilla Firefox
http://9.152.32.207:8080/hmc/content?taskId=11&refresh=106
P0000H29 Details - P0000H29
Instance Information
Product Information
Acceptable CP/PCHID Status
STP Information
zBX Information
Instance Information
Apply
Change Options...
Cancel
Help

CP status:	Service Required	Activation profile:	SNOY211108
PCHID status:	Exceptions	Last profile used:	DEFAULT
zBX Blade status:	Communications not active	Service state:	false
Group:	CPC	Number of CPs:	18
IOCDS identifier:	A2	Number of ICFs:	2
IOCDS name:	IODFE7	Number of zAAPs:	2
System Mode:	Logically Partitioned	Number of IFLs:	2
Alternate SE Status:	Not Operating	Number of zIIPs:	2
Lockout disruptive tasks:	□ Yes ● No	Dual AC power maintenance:	Fully Redundant
		CP Assist for Crypto functions:	Installed

Crypto Express2 and Crypto Express3

- Crypto Express: IBM Cryptographic Security Module
- Crypto Express4S is current with zEC12/zBC12

CEX, CEX, and More CEX!

- A CEC can have up to sixteen crypto features installed
  - Eight two-engine cards or sixteen single-engine cards
  - Often limited by available slots

- Each interface can be configured two ways:
  1. As cryptographic coprocessor (CEX2C, CEX3C)
  2. As SSL accelerator, for RSA operations (CEX2A, CEX3A)

- CEX also support “User-Defined Extensions”

SSL Handshake Performance

- As a CEX2C/3C/CEX4SC, CEX still helps with SSL
  - IBM results using z196 Model 754 (4 full-speed engines)

Method	ETR	CPU%	Crypto%
Software	1204	100	n/a
8 CEX3C	14457	95.24	92.3
4 CEX3A	14429	99.72	80.7

  - With (plenty of) CEX, more than 10x improvement
  - CEX3A is about double CEX3C!
  - CPU utilization 100% without CEX, lower with

CKDS and PKDS

- ICSF can manage/use two special data sets
  - **CKDS**: Cryptographic Key Data Set
  - **PKDS**: Public Key Data Set

- Keys can be stored in CKDS/PKDS in encrypted form

ICSF Key Operation Modes

- **Clear** Key
- **Secure** Key
- **Protected** Key

CKDS, PKDS, and Secure Key Operation

- When an encrypted key from CKDS/PKDS is used:
  1. Application fetches key from *x*KDS
  2. Calls ICSF with data and encrypted key
  3. ICSF calls CEX
  4. CEX decrypts key with Master Key
  5. CEX performs operation on data
  6. Crypto result returned to ICSF, thence to application

- This is known as **Secure Key** operation

Protected Key Operations

- ICSF added **Protected Key** in 2009

- Stored keys in z/OS are still encrypted
  - CEX call decrypts key, re-encrypts with “wrapping key”
  - Copies wrapping key to protected HSA memory
  - Wrapped key returned and used on CPACF calls

Review: Key Operation Modes

- **Clear** Key
  - Fastest but least secure
- **Secure** Key
  - Slowest but most secure
- **Protected** Key
  - "Most of the performance with most of the security"

CPACF and Crypto Express Support

- System z operating systems support CPACF and CEX
  - z/OS ICSF uses CPACF or CEX as appropriate/available
  - z/VM guests can use CPACF, be given CEX access
  - z/VSE supports CPACF and CEX (no RSA Secure Key)
  - z/TPF supports CPACF, CEX as RSA/SSL accelerator
  - Linux for System z distros fully support both

ICSF and SAF (RACF, ACF2, Top Secret)

- SAF can control ICSF
  - CSFSERV resource class
  - If not activated, no controls over ICSF

- CKDS/PKDS are special to SAF (RACF, ACF2, TSS)
  - Each record (each key) is secured separately
  - Controlled by CSFKEYS resource class

Misconception: “CEX is Always Good”

- Easy assumption to make: “Using CEX is always faster”
  - Not true: CEX mainly for ***security*** not ***performance***
  - ***Certain*** operations (SSL/RSA) are faster
  - ***Most*** operations are slower: ICSF must do I/O to CEX

- For everyday cryptography (besides SSL handshakes):
  - Best **performance**: CPACF
  - Best **securi ty**: Crypto Express

- CEX ***might*** be cheaper CPU-wise with large data blocks

Approaches and Criteria

“They all claim they’ll solve all our problems!?!”

Hardware or Software?

- Hardware
- Software

Separation of Duties

- Separation of Duties (SoD) is important for real security
- Fully transparent solutions fail to provide SoD

Separation of Duties: The Reality

- Implementing true SoD requires application changes

“You can have peace. Or you can have freedom. Don't ever count on having both at once.”

— Robert A. Heinlein

Key Management

- Key management equally critical
  - What if you need data off a tape ten years from now?
  - Can you access keys in DR scenarios?

- Robust, flexible key management is a must
  - Key management involves three primary functions:
    1. Give encryption keys to applications that must protect data
    2. Give decryption keys to users/applications that correctly authenticate according to some policy
    3. Allow administrators to specify that policy: who can get what keys, and how they authenticate

Key Management

- Key servers generate keys for each new request

- What about distributing keys?

- Too many solutions focus on the encryption algorithm

Voltage security

IBM Encryption Products

System z and z/OS Hardware and Software from IBM

Encrypting Hardware

- IBM encrypting tape drives: TS1130, TS1140
  - Whole-tape encryption
  - Tivoli Key Lifecycle Manager (“TKLM”, aka IBM Secur Lifecycle Manager for z/OS) manages keys

- Encrypting disk array: DS8000
  - Whole-DASD encryption
- Performance impact of this encryption is minimal

InfoSphere Guardium Data Encryption

- Whole database encryption for DB2 and IMS databases
  - Formerly IBM Data Encryption for IMS and DB2 Databases
- Significant performance impact, so real SoD
- Limited value

Encryption Facility for z/OS

- File-level encryption; mainly targeted at backups
- Useful tool for specific purposes targeted
- Same product available for z/VSE

IBM® Sterling Connect:Direct®

- Automated, secure file transfer between systems
  - Formerly Sterling Commerce Connect: Direct
    - Formerly Sterling Network Data Mover
      - Formerly Systems Center NDM
  - Still commonly called “NDM”

- Mature, powerful product
  - Think “FTP or scp, only more programmable and secure”

Enterprise Key Management Foundation

- IBM Distributed Key Management System (DKMS) plus implementation services

- Longer-term, intended as IBM’s answer to All Things KM

ISV Encryption

Approaches and Options

Hardware or Software?

- Same criteria as with IBM products
- Separation of Duties is important
- Key management equally critical

Hardware Solutions

- Various hardware options

- Need to understand the problem being solved

Software Solutions

- z/OS encryption products fall into three categories
  1. Very narrow, “point” solutions (e.g., file encryption)
  2. SaaS/SOA/SOAP (web services) remote server-based
  3. Native (with or without hardware exploitation)

- Do you want to manage dozens of point solutions?
  – Also see *Enterprise Encryption 101* at www.share.org/Portals/0/Webcasts/2012%20Webcasts/Getting%20Started.wmv or http://bit.ly/wtMriL

Point (Narrow) Software Solutions

- Plenty of “encrypt a file” products available

- Many candidates

  - Rocket Software
  - CA Technologies
  - Code Magus
  - OpenTech
  - PKWARE
  - Innovation Data Processing

SOA (Web-based) Software Solutions

- Server (real or virtual) installed on your network

- Weaknesses:
  - Performance: SSL connections involve overhead, delay
  - System z folks often uncomfortable with operations “out there”
  - Effective as z/OS point solution, if performance acceptable

- Several candidates
  - Protegrity
  - Safenet
  - Liaison Techologies (formerly nuBridges)

Native Software Solutions

- APIs to add to existing applications

- Again, varied candidates :
  - **RSA** (EMC): C/C++ and Java APIs
  - **CFXWorks**, **Entrust**: Java-only APIs
  - **Redvers Consulting**: COBOL-only API
  - **Prime Factors, Advanced Software Products Group**: general-purpose APIs

Voltage security

Making Intelligent Choices

First Step: Understand the Problem

- “We need some encryption” isn’t sufficient
  - To protect what?
  - From whom?
  - What else will this of necessity affect?

- Requires executive sponsorship

- Expect a successful implementation to spread

Security-Related Questions

- Is algorithm strong, peer-reviewed?
- Does it support hardware assists?
- Is key management part of the solution?

Operational/Deployment Questions

- Is implementation cost reasonable?
- Is implementation under your control?
- Is it multi-platform?

Voltage SecureData

Voltage SecureData

- Voltage SecureData offers broad platform support:
  - z/OS, Windows, Linux, Solaris, AIX, HP Nonstop, Stratus VOS, HP/UX, Java/J2EE, .Net, TeraData, Hadoop, AWS, Azure…

- Implements several Voltage technologies
  - FPE (Format-Preserving Encryption)
  - SST (Secure Stateless Tokenization) ***Native on z/OS!***
  - SKM (Stateless Key Management)

- ***The simplest encryption API available anywhere***

Voltage SecureData for z/OS Benefits and Value

Benefit and Value	Details
Ease of use *Saves time and money*	Dead simple API—minimal learning curve Atomic calls simplify integration, error handling Callable from any z/OS environment Can be linked dynamically for easier upgrades
Native z/OS exploitation *Integrates with operations*	Operations performed on System z—no network latency Exploits hardware crypto (if available) Integrates with native security (RACF/ACF2/Top Secret) User exits allow further control
Centralized administration *Supports business goals*	Verify that applications are using the correct operations Granular control over whether users can protect/access Perform auditing, chargeback SMF data for performance analysis and capacity planning

Conclusion

Summary

- System z is a full player in the encryption world
- Many encryption approaches exist
- IBM, vendors offer varied products
- Voltage SecureData eases data protection effort!

Questions?

Phil Smith III

703.476.4511 (direct)
phil@voltage.com
www.voltage.com