





# Security Concepts: Linux for System z

## Vanguard Security Conference – June 2011

Jack Jones  
johnjone@us.ibm.com

© 2010 IBM Corporation



# Trademarks

The following are trademarks of the International Business Machines Corporation in the United States, other countries, or both.

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by © are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml):

\* AS/400®, e business(logo)®, DBE, ESCO, eServer, FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, S/30, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries. Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. UNIX is a registered trademark of The Open Group in the United States and other countries. LINUX is a registered trademark of Linus Torvalds in the United States, other countries, or both. ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

\* All other products may be trademarks or registered trademarks of their respective companies.

**Notes:**  
Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here. IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply. All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions. This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area. All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

2

© 2010 IBM Corporation

## Agenda

- Quick Security Level Set
- Key Security Technologies
  
- What does System z bring to Linux Security
  - ▶ Isolation and Certification
  - ▶ Cryptography
  - ▶ Integration
  
- Platform Synergy (z/OS, z/VM, & zLinux)
  - ▶ Network Security
  - ▶ Administration & Authentication
  - ▶ Configuration

3

© 2010 IBM Corporation

## Linux for System z is not ...

Linux® for System z is not z/OS®

Linux for System z is not RACF®  
z/OS Communication Server

Linux for System z is not ICSF  
System SSL

4

© 2010 IBM Corporation

## Linux is ...



Linux for System z has security-rich features.

Linux has a large active developer base enabling a thorough code review.

Linux for System z is open, no security through obscurity, anyone can see flaws and fix them.

IBM have provided about 7.6% of the changes to Linux since version 2.6.11 (Oracle 2.4%, HP 1.0% and Sun 0.5%)

Around 70% of the developers who contribute to Linux are employed to do so and getting paid for their work

Linux has a worldwide user base which allows testing on a wide range of hardware and diverse scenarios.



Linux benefits from almost immediate response to security advisories and rapid implementation of new technologies.

5

© 2010 IBM Corporation

## Distributions Embracing Security



- **Hardening**
- **Secure shell**
- **Enhanced Audit Capability**
- **Enhanced Authentication Options**
- **Virtual Private Network**
- **Enhanced Firewall Management**
- **Intrusion Detection Systems**
- **Cryptographic Libraries and Access to Hardware**
- **Host and Network Scanning Tools**
- **Certifications**

6

© 2010 IBM Corporation



Key Security Technologies

7

© 2010 IBM Corporation

### Linux on System z Security Building Blocks

|                            |   |
|----------------------------|---|
| Access Control (for Linux) | SELinux, AppArmor, sudo, IBM Tivoli® Access Manager, CA eTrust Access Control for Unix  |
| Access Control (for Web)   | IBM Tivoli® Access Manager, CA Siteminder   |
| Anti-Virus/Anti-Spam       | ClamAV, OpenAntiVirus, AmaViS, MIMEDefrag, TrendMicro's ServerProtect & ScanMail, Network Associates, Roaring Penguin's CanIt |
| Directory Services         | Open LDAP, NIS/NIS+, IBM Tivoli Directory Server, CA's eTrust Directory, PADL's XAD, Quest's VAS                              |
| Digital Certificates       | Freeware PKI, z/OS PKI Services   |
| Firewall                   | IPTables/NetFilter, ISS PSL for Linux on System z, webApp.Secure  |
| Intrusion Detection        | Snort, AIDE, Snare, PortSentry, TripWire, OSSEC, LIDS, IPLog, ISS PSL for Linux on System z, PredatorWatch, SafeZoneNet       |

Vendor Product  
Open Source Product

8

© 2010 IBM Corporation

# Linux on System z Security Building Blocks



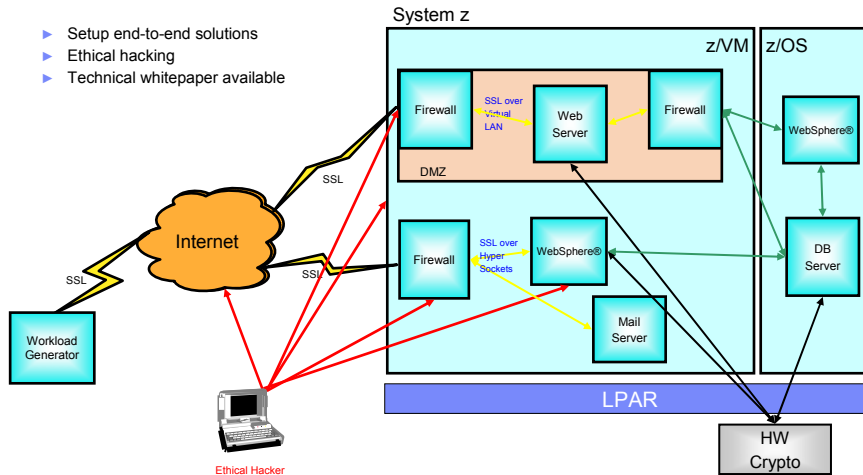
|                               |  |
|-------------------------------|--|
| Secure Network Communications | OpenSSH, GnuPG (OpenPGP compliant), USAGI IPv6, FreeS/WAN, CA's eTrust VPN, SecureAgent Software, PGP Command Line |
| Secure Socket Layer (SSL)     | OpenSSL, PKCS#11, GSKIT  |
| System Hardening              | Bastille, Tiger, RedHat, Novell  |
| Secure Data                   | dm-crypt, pppd, CFS, Network Associates' e-Business Server   |
| Identity Integration          | PAM, OpenLDAP, IBM Tivoli Directory Server for z/OS, IBM Tivoli Directory Integrator, CA's eTrust Directory        |
| Identity Management           | IBM Tivoli Identity Manager  |
| Proxy Server                  | Proxy Suite from SuSE, IBM Edge Server, IBM Tivoli Access Manager WebSEAL (secure proxy)                           |

Vendor Product  
Open Source Product

# Ethical Hacking



- ▶ Setup end-to-end solutions
- ▶ Ethical hacking
- ▶ Technical whitepaper available



For details see:  
 •Linux Security: Exploring Open Source Security for a Linux Server Environment (GM13-0636-00)  
 •zSeries Platform Test Report for z/OS and Linux Virtual Servers



# Isolation & Certification

11

© 2010 IBM Corporation



## System z Security Advantage Summary

- Image Isolation and Certification
  - LPAR
  - z/VM®
- Common Criteria Certification and z/VM System Integrity Statement
- Hardware Encryption
  - Asymmetric Cryptography provides SSL performance enhancements
  - Symmetric Instructions - DES, TDES, AES, and SHA
  - Secure key cryptography
- HiperSockets™ Provide Physical Security
- Qualities of Service – specialty engines (4.4 GHz... Quad Core Processor Up to 64 IFLs)

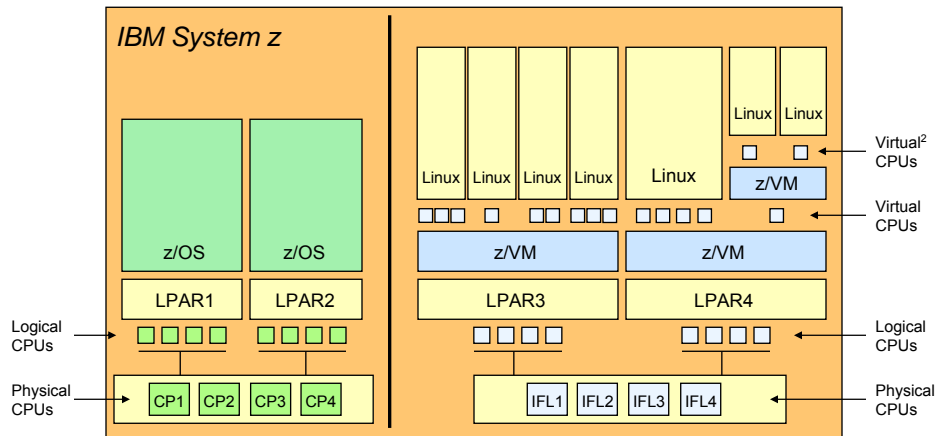


12

© 2010 IBM Corporation

## IBM System z Virtualization Leadership

### Extreme Levels of CPU Sharing



13

© 2010 IBM Corporation

## Logical Partition (LPAR) Certification

- IBM eServer zSeries 990 (z990)
  - ▶ 10/04 Common Criteria EAL4/EAL5
- IBM eServer zSeries 890 (z890)
  - ▶ 6/05 Common Criteria EAL4/EAL5
- IBM System z9 109
  - ▶ 3/06 Common Criteria EAL5
- IBM System z9 EC & BC
  - ▶ 8/06 Common Criteria EAL5
- IBM System z10 EC
  - ▶ 3/08 Common Criteria EAL5
- IBM System z10 BC
  - ▶ 10/08 Common Criteria EAL 5
- IBM System z196
  - ▶ In Certification Process – EAL 5

## z/VM Certification

- Statement of System Integrity
- Common Criteria
  - z/VM 5.1 certified 2Q 2005  
EAL 3+ for LSPP & CAPP
  - z/VM 5.3 certified 3Q 2008  
EAL 4+ for LSPP & CAPP
  - z/VM 6.x in certification  
EAL ? for OSPP

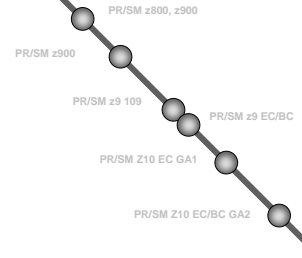
14

© 2010 IBM Corporation

## Logical Partition (LPAR) Certification



EAL5



- Access Control Devices and Systems(61)
- Boundary Protection Devices and Systems(97)
- Databases(43)
- ICs, Smart Cards and Smart Card related Devices and Systems(293)
- Network and Network related Devices and Systems (96)
- Other Devices and Systems(291)
- Biometric Systems and Devices(1)
- Data Protection(52)
- Detection Devices and Systems(26)
- Key Management Systems (28)
- Operating systems(93)
- Products for Digital Signatures (55)

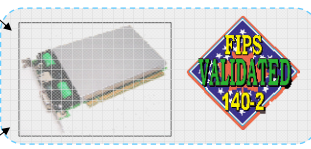
| EAL   | 1997 | 1998 | 1999 | 2000 | 2001 | 2002 | 2003  | 2004 | 2005 | 2006 | 2007  | 2008  | 2009  | Total  |
|-------|------|------|------|------|------|------|-------|------|------|------|-------|-------|-------|--------|
| EAL1  | 0    | 0    | 4    | 1    | 0    | 3    | 5     | 2    | 1    | 5    | 7     | 3     | 1     | 32     |
| EAL1+ | 0    | 0    | 4    | 3    | 9    | 2    | 0     | 0    | 0    | 0    | 1     | 1     | 2     | 22     |
| EAL2  | 0    | 1    | 1    | 1    | 2    | 7    | 7     | 17   | 46   | 39   | 31    | 31    | 3     | 186    |
| EAL2+ | 0    | 0    | 0    | 1    | 0    | 5    | 4     | 4    | 7    | 13   | 26    | 26    | 17    | 103    |
| EAL3  | 0    | 0    | 2    | 2    | 3    | 3    | 3     | 13   | 14   | 18   | 39    | 19    | 18    | 134    |
| EAL3+ | 1    | 0    | 0    | 0    | 1    | 0    | 2     | 17   | 13   | 24   | 16    | 17    | 14    | 105    |
| EAL4  | 0    | 1    | 1    | 5    | 4    | 12   | 14    | 8    | 10   | 13   | 16    | 9     | 3     | 96     |
| EAL4+ | 0    | 0    | 0    | 9    | 7    | 15   | 17    | 26   | 43   | 47   | 74    | 75    | 41    | 354    |
| EAL5  | 0    | 0    | 0    | 0    | 0    | 0    | 2 (2) | 2    | 1    | 0    | 4 (2) | 2 (1) | 1 (1) | 12 (6) |
| EAL5+ | 0    | 0    | 0    | 0    | 1    | 6    | 3     | 4    | 12   | 10   | 16    | 26    | 11    | 89     |
| EAL6+ | 0    | 0    | 0    | 0    | 0    | 0    | 0     | 0    | 0    | 0    | 0     | 1     | 0     | 1      |
| EAL7  | 0    | 0    | 0    | 0    | 0    | 0    | 0     | 0    | 1    | 0    | 0     | 0     | 0     | 1      |
| EAL7+ | 0    | 0    | 0    | 0    | 0    | 0    | 0     | 0    | 0    | 1    | 0     | 0     | 0     | 1      |
| Total | 1    | 2    | 12   | 22   | 27   | 53   | 57    | 93   | 148  | 170  | 230   | 210   | 111   | 1136   |

The use of a "+" sign to indicate augmentation is an informal shorthand used by product vendors.

## Linux for System z certifications by Distribution

| Version            | Certification Level | Status   |
|--------------------|---------------------|----------|
| <b>Novell SUSE</b> |                     |          |
| SLES 8             | CAPP – EAL 3 +      | Complete |
| SLES 9             | CAPP – EAL 4 +      | Complete |
| SLES 10            | CAPP – EAL 4 +      | Complete |

| Version       | Certification Level   | Status   |
|---------------|-----------------------|----------|
| <b>RedHat</b> |                       |          |
| RHEL 3        | CAPP – EAL 3 +        | Complete |
| RHEL 4        | CAPP – EAL 4 +        | Complete |
| RHEL 5        | CAPP / LSPP – EAL 4 + | Complete |



FIPS 140-2 Level 4



# Crypto

## z10 Hardware Cryptography Implementation

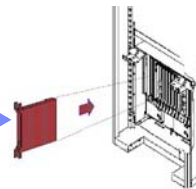
### CP Assist for Cryptographic Functions (CPACF)

- > A facility integrated in each PU
- > Standard orderable feature
- > Clear Key & Protected Key only
- > Symmetric, hash, ...



### Crypto Express 2/3 (CEX2C, CEX3C)

- > Priced feature
- > 0 to 8 features in a system
- > 2 secure **4764 coprocessors** per feature
- > Secure keys symmetric (DES, T-DES) and asymmetric (RSA)
- > PR/SM sharable
- > Manually configurable into an RSA accelerator (CEX2A, CEX3A)
- > **FIPS140-2 Certified** (As Coprocessor only)



**Accelerator**

FIPS140-2 = **NO**

**Coprocessor**

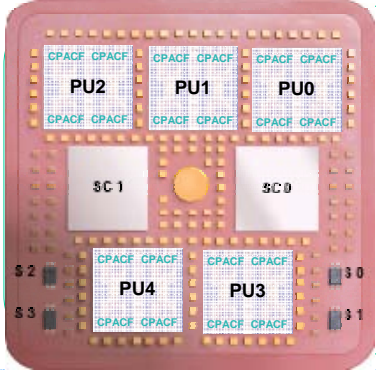
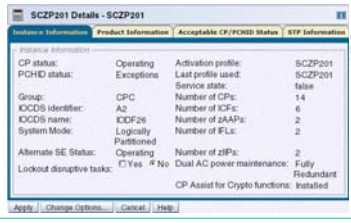
FIPS140-2 = **YES**

Details next slide

# The CP Assist For Cryptographic Functions (CPACF)

Available on:

- ✓ CP(GP)
- ✓ IFL
- ✓ zAAP
- ✓ zIIP

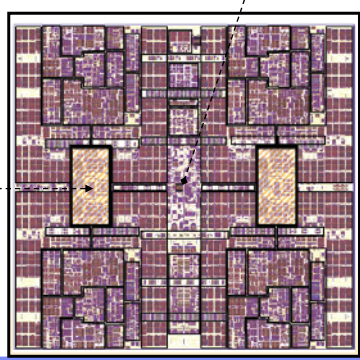
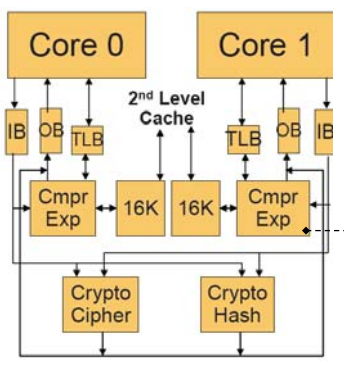


| Algorithms: | Clear Key |     | Protected Key |
|-------------|-----------|-----|---------------|
|             | z9        | z10 | z10           |
| DES, T-DES  | ✓         | ✓   | ✓             |
| AES128      | ✓         | ✓   | ✓             |
| AES192      | ✗         | ✓   | ✓             |
| AES256      | ✗         | ✓   | ✓             |
| SHA-1       | ✓         | ✓   | ✗             |
| SHA-256     | ✓         | ✓   | ✓             |
| SHA-384     | ✗         | ✓   | ✗             |
| SHA-512     | ✗         | ✓   | ✗             |
| PRNG        | ✓         | ✓   | ✗             |

Implementation of the IBM Message Security Architecture (MSA) Instructions (Refer to z/Architecture Principles Of Operation SA22-7832)      Enablement with FC 3863

# CPACF : Cryptography Accelerator

- Data compression engine
- Cryptography engine
- Accelerator unit shared by 2 cores



## The Cryptographic Express 2/3



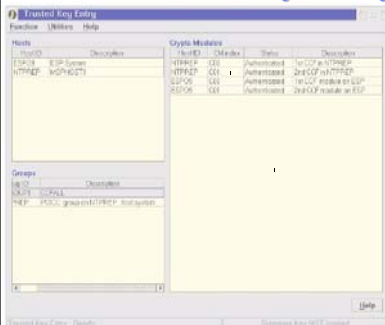
### Enablement with FC 3863

- **4764"** (PCIxCC) based technology
- Provides **secure key** functions (FIPS 140-2 Level 4 certified)
  - **Symmetric** DES, T-DES encryption/decryption
  - Message authentication, hashing
  - PIN processing
  - **RSA asymmetric** encryption/decryption and digital signature generation/verification
  - Key generation and management, random number generation
  - EMV support
  - 4753 support
  - **User Defined Extension (UDX)** – Built under contract by IBM or 3rd party approved vendor
- Provides clear key RSA functions for **SSL/TLS acceleration**

21

© 2010 IBM Corporation

## The Trusted Key Entry Workstation



- **Priced optional feature** - A highly secure alternative
- TSO/E for the management of secure coprocessors  
Master Keys and operational keys
- Encrypted and signed communications over TCP/IP
  - Listener in ICSF
  - End point is the coprocessor
- Increased security for
  - Access to secure cryptographic coprocessors
  - Authorities (security officers) identified by their password and digital signature
  - Option to require multiple signatures before performing a crypto function
  - smart card support
- Coprocessors can be administered as groups

Can be used on Linux with secure keys



22

TKE V5.2 for CEX2C in System z10.

TKE V6.0 for CEX3C in System z10. © 2010 IBM Corporation

## Clear Key / Secure Key / Protected Key

- **Clear Key** – key may be in the clear, at least briefly, somewhere in the environment



CPACF, CEX2A, CEX3A

- **Secure Key** – key value does not exist in the clear outside of the HSM (secure, tamper-resistant boundary of the card)



CEX2C, CEX3C

- **Protected Key** – key value does not exist outside of physical hardware, although the hardware may not be tamper-resistant



CEX3C (require CPACF)

23

© 2010 IBM Corporation

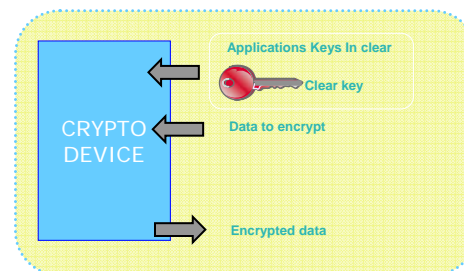
## Clear Key

CPACF, CEX2A, CEX3A



“Clear Key – key may be in the clear, at least briefly, somewhere in the environment”

- **Hardware Acceleration**
  - ▶ Asymmetric
    - Acceleration of RSA handshake
      - PCICC
      - PCICA
      - PCIXCC
      - Crypto Express2/3 Coprocessor and Accelerator (CEX2/3C & CEX2/3A)
  - ▶ Symmetric/HASH
    - DES, TDES, AES, SHA-1 and SHA-2
  - ▶ PRNG
- **Software Libraries for crypto access**
  - ▶ Kernel APIs
  - ▶ OpenSSL
  - ▶ PKCS#11
  - ▶ GSKit



24

© 2010 IBM Corporation

# Secure Coprocessor

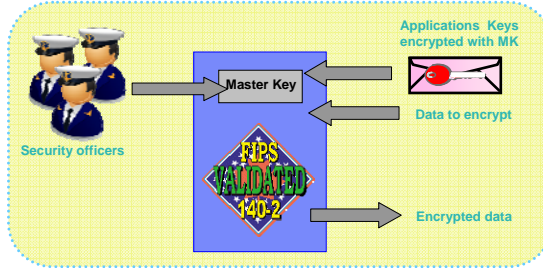
Secure Coprocessor (e.g. CEX2C, CEX3C)



“Secure Key – key value does not exist in the clear outside of the HSM (secure, tamper-resistant boundary of the card)”

- **Hardware Acceleration**
  - ▶ **Asymmetric, Symmetric and Financial**
    - CEX2C
- **Software Libraries for crypto access**
  - ▶ CCA – Common Cryptographic Architecture
  - ▶ PKCS#11 – Limited
    - key generation/encrypt/decrypt for TDES & RSA
  - ▶ Java/JCE – Limited as above
- **Card Management**
  - ▶ Trusted Key Entry (TKE)
  - ▶ Linux CCA Utility
  - ▶ Configure via z/OS then re-assign to Linux

<http://csrc.nist.gov/cryptval/140-1/1401val2006.htm>  
look for certificate #661



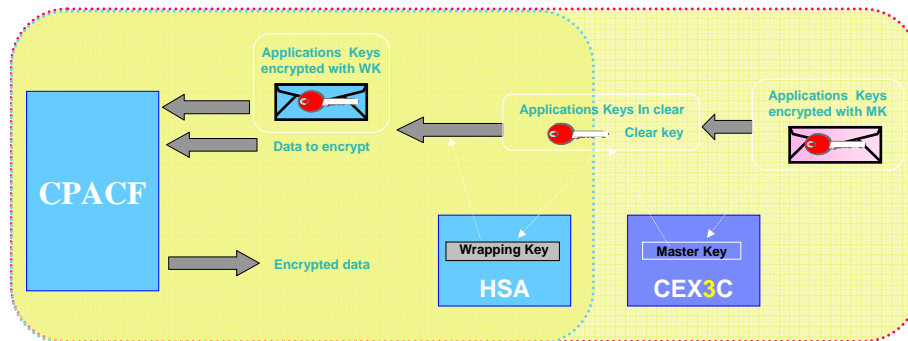
+ Master Key zeroization in case of tampering attempt

# Protected Key

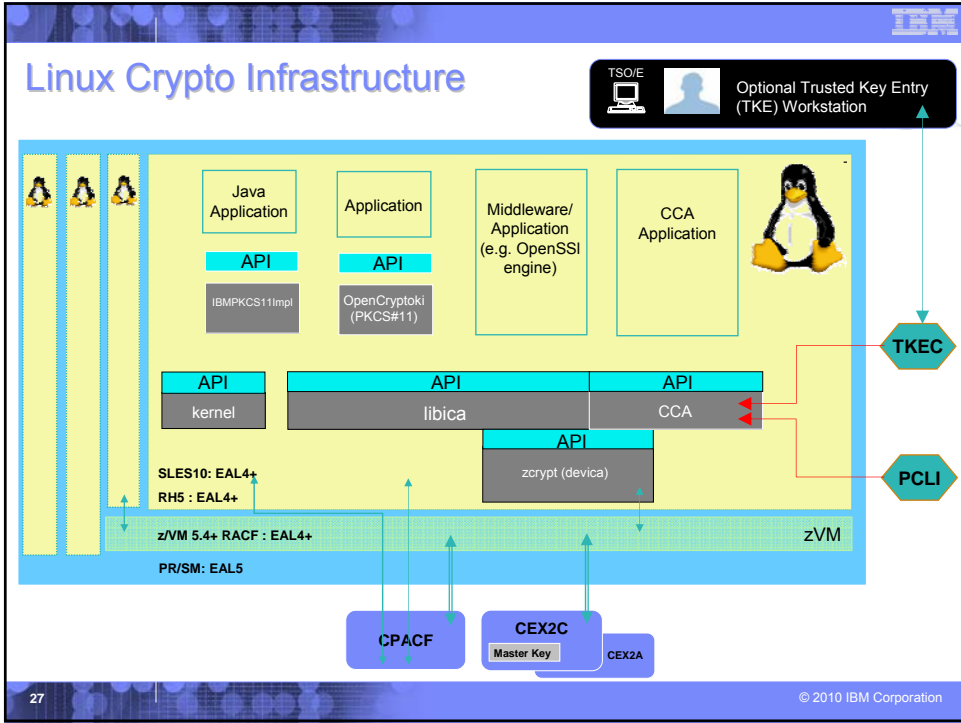


CPACF (CEX3C required)

“Protected Key – key value does not exist outside of physical hardware, although the hardware may not be tamper-resistant”



Coming soon for Linux on z



# Accelerated Linux kernel functions

The diagram shows a stack of layers: 'Linux' (yellow), 'zVMM' (green), and 'CPACF' (blue). A dashed circle highlights the 'Linux' layer.

The standard Linux kernel includes modules that exploit the CPACF capabilities of the System z hardware. Through the /proc file system, you can query the kernel about the cryptographic modules that are currently in use.

```
[root-]# modprobe aes_g
[root-]# modprobe aes_s390
[root-]# cat /proc/crypto
name      : cbc(aes)
driver    : cbc-aes-s390
module    : aes_s390
priority  : 400
refcnt    : 1
type      : blkcipher
blocksize : 16
min keysize : 16
max keysize : 16
ivsize    : 16
name      : ecb(aes)
driver    : ecb-aes-s390
module    : aes_s390
priority  : 400
refcnt    : 1
[...]
```

- Symmetric algorithms and hash functions CPACF currently includes:
  - SHA-1, DES and 3-DES with z990 / z890
  - SHA-256 and AES with 128 with z9
  - SHA-512 and AES with 192/256 bit keys with z10
- Algorithms exploiting CP assist functions can be used instead of generic software implementation
- AES fall-back support for unsupported key lengths on z9
- Priority based algorithm selection at runtime
- Pseudo random number generator
- Algorithm description at /proc/crypto

28 © 2010 IBM Corporation

## Accelerated Linux kernel functions (cont.)

**File System Encryption**

**eCryptfs** **Dm-crypt**

The additional cryptographic capabilities of System z can also be used to speed up the process of protecting your file system data using encryption.

**dm-crypt**  
One of the cryptography features of the Linux kernel is dm-crypt, which is a device mapper and a transparent disk encryption subsystem that allows you to encrypt whole block devices.

**eCryptfs**  
Native to the kernel, eCryptfs is a stacked cryptographic file system for Linux. A stacked file system is layered on top of an existing mounted file system, which is referred to as a lower file system. As the files are written to or read from the lower file system, eCryptfs encrypts and decrypts the files.

**Linux**  
zVM  
CPACF

**Random number generator**

**random** **urandom** **prandom**

An important aspect of cryptography is the availability of enough entropy to ensure secrecy because many cryptographic functions rely on randomly chosen values that are used, for example, to generate session keys or initialize the internal pseudorandom number generator (PRNG).

**Long Random numbers**

Long random numbers are also supported by System z. User-space applications can access large amounts of random data. The random data source is the built-in hardware random number generator on the CEX2/3C cards.

**IPSec**

**bulk**

IPSec has two major modes of operation:

- Tunnel mode
- Transport mode

29 © 2010 IBM Corporation

## Securing communication applications

**Network Security Services**

NSS comprises a set of libraries for cross platform development of security enabled client and server applications. NSS includes an open source implementation of: SSL v2 & v3, TLS, S/MIME, PKCS (#1, #3, #5, #7, #8, #9, #10, #12)

**SSL/TLS**

**bulk** **handshakes**

We can utilize hardware cryptographic devices to improve performance during SSL handshake

**Java** **PKCS#11**

The hardware cryptography extensions provided by both CPACF and the Crypto Express adapters are also available to you in the Java programming environment

Access to the hardware is mediated by the IBM Java PKCS#11 implementation (IBMPKCS11Imp) library that is, for example, provided with the IBM Java Runtime Environment (JRE).

**Linux**  
zVM  
CPACF CEX2/3C

**OpenSSL**

**libica** **zcrypt**

OpenSSL is most likely the most prominent open source cryptographic library

- The core library implements the basic cryptographic functions and provides various utility functions.
- The OpenSSL library has a plug-in mechanism that allows various engines to be used for cryptographic operations.
- One of these engines is the ibmca engine
- It uses CPACF and Crypto Express functionality if they are present in the system

**Key Management**

**NSS** **OpenSSL** **openCryptoki**

**IBM HTTP Server** **Apache httpd and mod\_ssl**

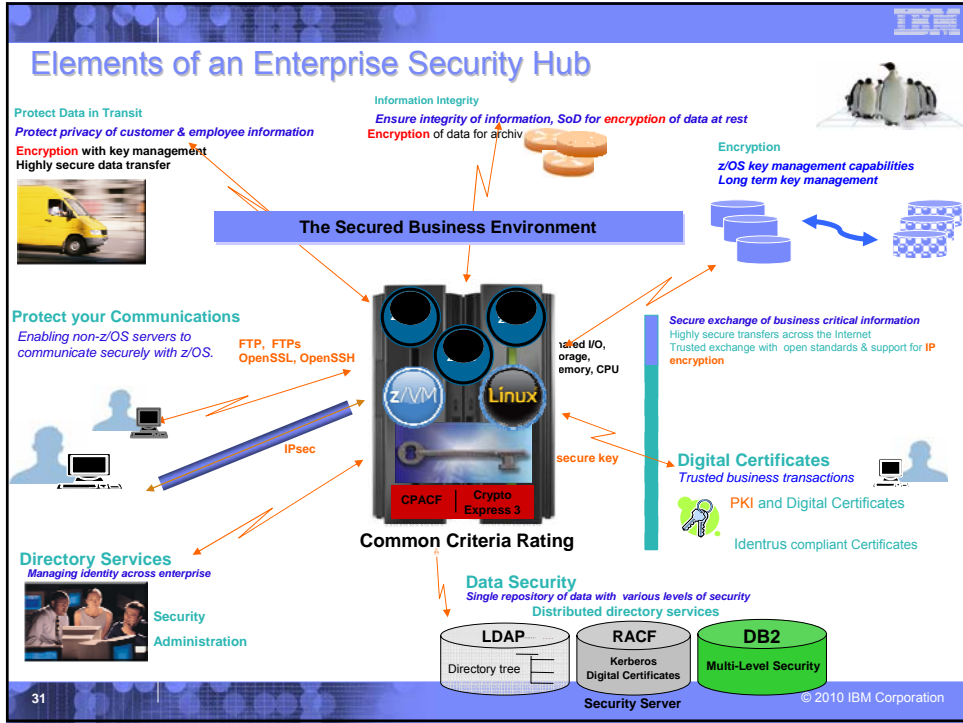
**IBM HTTP Server** **Apache**

**mod\_ibm\_ssl** **mod\_ssl** **mod\_nss**

**OpenCryptoki** **OpenSSL** **NSS**

**libica** **zcrypt**

30 © 2010 IBM Corporation





## Synergy Outlook



- Network Security
- Centralization with z/OS and z/VM
  - ▶ Authentication
  - ▶ Audit
- Other z/VM Highlights

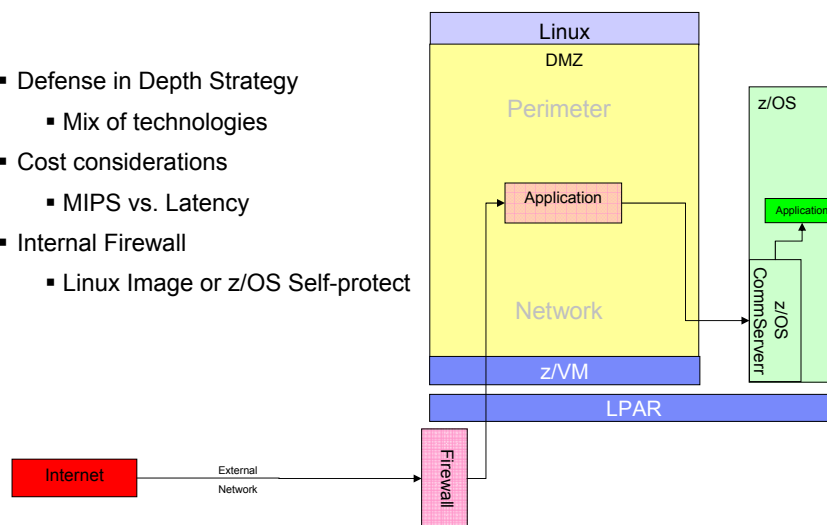
33

© 2010 IBM Corporation

## Mix of Firewalls



- Defense in Depth Strategy
  - Mix of technologies
- Cost considerations
  - MIPS vs. Latency
- Internal Firewall
  - Linux Image or z/OS Self-protect

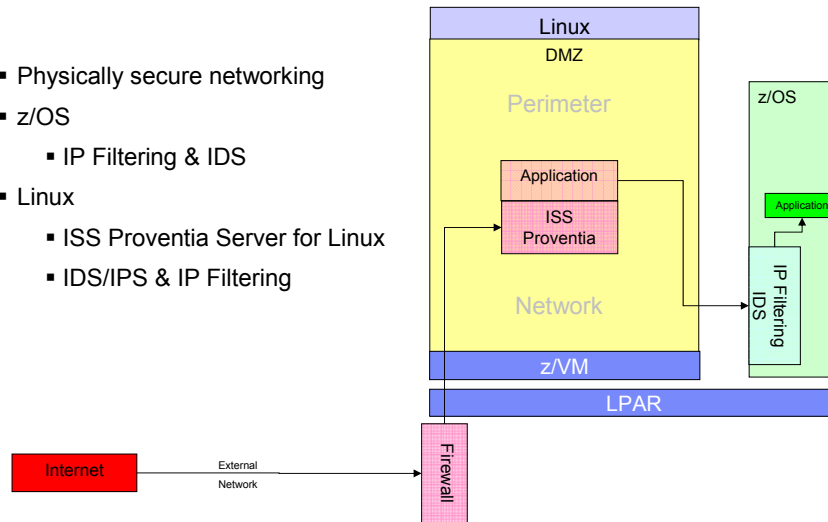


34

© 2010 IBM Corporation

## Host Firewalls

- Physically secure networking
- z/OS
  - IP Filtering & IDS
- Linux
  - ISS Proventia Server for Linux
  - IDS/IPS & IP Filtering



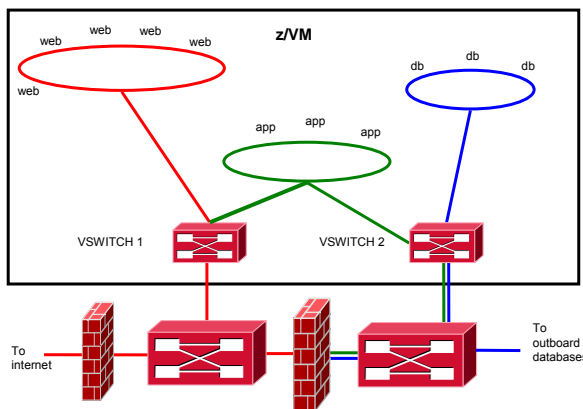
35

© 2010 IBM Corporation

## Virtual Network Management Multiple Security Zones

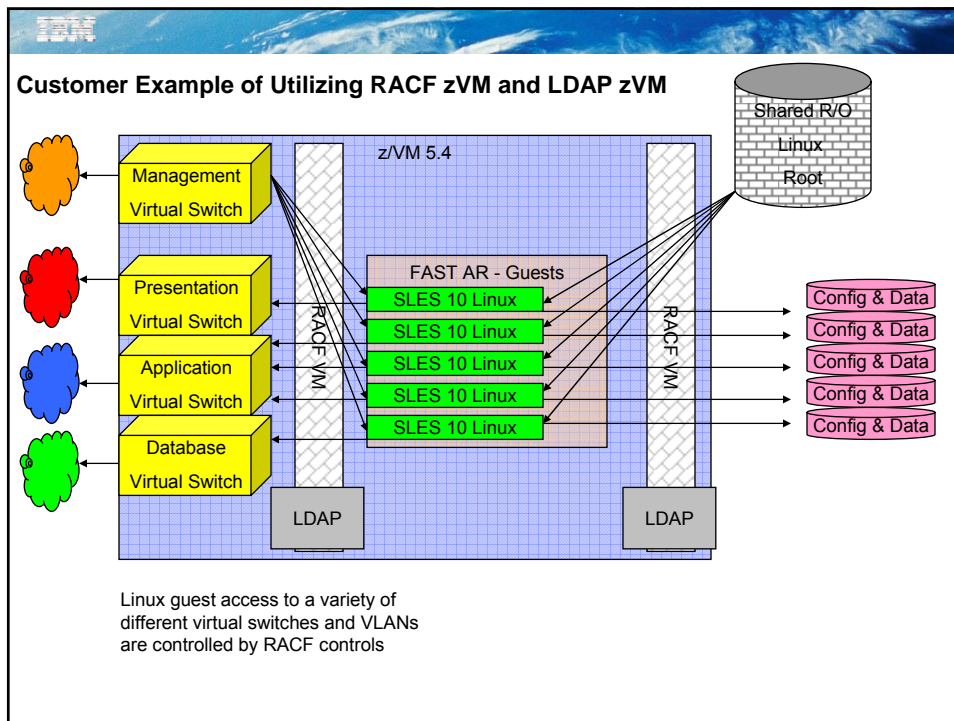
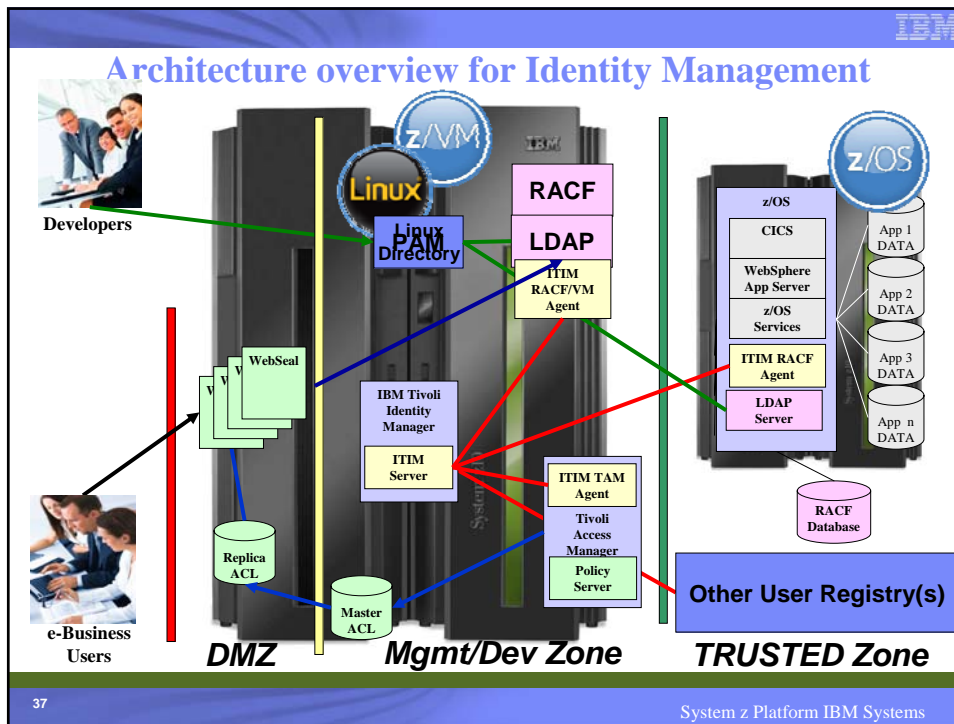
Use z/VM RACF Security Server to control and audit Linux and other virtual server access to networks.

- Control access to Virtual Switch (VSWITCH)
- Control access to specific VLANs on a VSWITCH
- Control and audit guest sniffing of virtual networks
- Better control of multi-tenant environments

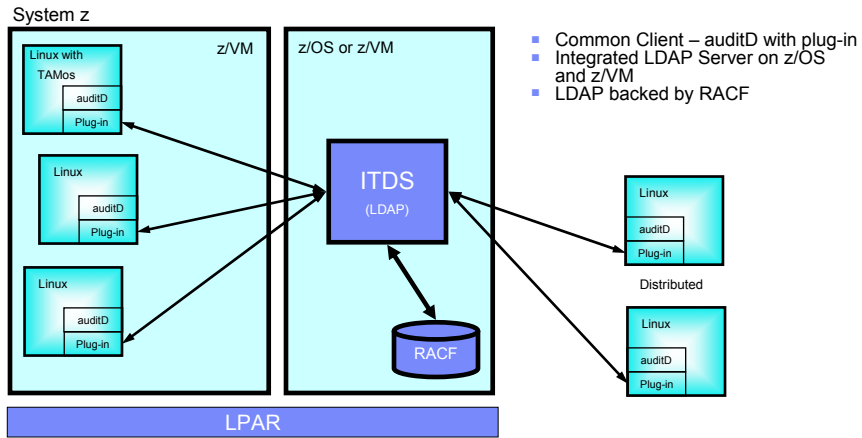


36

System z Platform IBM Systems



## Centralized Audit



RedBook: Enterprise Multiplatform Auditing (SG247472)

39

© 2010 IBM Corporation

## z(END)

- Questions?
- Comments!
- Suggestions?



40

© 2010 IBM Corporation