Linux on System z, z/OS, and You!

Vanguard 2007 – RTA1
Ben Rogers (bcrogers@us.ibm.com)
Systems and Technology Group Lab Services – System z Security

Trademarks

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

DB2*
DB2 Connect
DB2 Universal Database
e-business logo
GDPS*
Geographically Dispersed Parallel Sysplex
HyperSwap
IBM*
IBM eServer
IBM logo*
Parallel Sysplex*
System z
Tivoli*
VM/ESA*
WebSphere*
z/OS*
z/VM*
zSeries*
RACF*
Lotus*
Domino*
developerWorks*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Intel is a registered trademark of the Intel Corporation in the United States, other countries or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* 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.

Abstract

For many years the System z platform has provided the backbone of many IT shops, functioning as the secure, scalable, dependable data provider. In recent years, System z has expanded its mission to bring users the ability to integrate open standards and create N-Tier architectures 'in a box'.

This discussion will focus on how organizations can leverage the low Total Cost of Ownership of Linux on the System z platform coupled with the legendary capabilities of z/OS. Participants will learn about the strengths of each platform, z/OS and Linux on z, and learn about ways of tying them together to take advantage of common user repositories such as LDAP that accesses RACF, and technologies which eliminate problems such as network sniffing via the use of HiperSockets.

Building Blocks of a Secure N-Tiered Architecture “In a Box”

- Image Isolation
  - LPAR
  - z/VM®
- Hardware Cryptography
  - Asymmetric Algorithm (SSL) provides performance enhancements
    - PCICC, PCICA PCIXCC and CEX2 (CEX2C and CEX2A) cards
  - Symmetric Instructions - DES, TDES, AES-128,
  - Hashing functions – SHA-1, SHA-256, MDC-2, MDC-4
- HiperSockets™ Provide Physical Security
- Qualities of Service

Why Linux on System z:

Linux for System z has security-rich features.

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

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

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.

System z Security Components

Linux

- Firewall
- Proxy Server
- DMZ
- Intrusion Detection
- HiperSockets
- Hardware Cryptography

z/VM

- RACF
- ITDS (LDAP)
- Virtual LANs
- HiperSockets

z/OS

- RACF
- PKI Services
- ITDS (LDAP)
- Intrusion Detection
- IPSec
- HiperSockets
- Hardware Cryptography

System z Crypto Hardware Matrix

PCI Cards

Name	Supported HW	z/OS Support	Linux Support	Remarks
PCICC	G5, G6, z900, (not z800)	Secure key	Clear Key SSL only	1 processor/card
PCICA	z900 GA 2, z800, z990	Clear key SSL	Yes	5 processors/card
PCIXCC	z990 GA 2, z890	Secure key	Clear Key SSL only	1 card per adapter
CEX2C	z990 GA 4, System z9	Secure key Clear key SSL	Clear Key SSL only	2 cards per adapter (cards same as PCIXCC)
CEX2 (Coprocessor & Accelerator)	System z9 EC, System z9 BC	Secure key Clear key SSL	Clear key SSL + **secure key**	2 cards per book, each card can have a 2A or 2C personality

Instructions

Name	Supported HW	z/OS Support	Linux Support	Remarks
CCF	G5, G6, z900, z800	Yes	No	Replaced by CP Assist in z990
CP Assist Instructions	z990, z890	Yes	Yes	DES, TDES, SHA-1
CP Assist Instructions	System z9 EC/BC	Yes	Yes	AES-128, SHA- 256, PRNG

Clear Key Cryptography for System z

z/OS

- **Hardware Acceleration**
  - **Asymmetric**
    - RSA handshake
  - **Symmetric**
    - DES, TDES, AES
  - **PRNG**
  - **Hashing/Modification Detection**
    - SHA-1 and SHA-256
    - MDC-2, MDC-4
  - **Financial**
    - **CVV**
    - **PIN generate**
    - **MAC**
- **z/OS Software Libraries for crypto access**
  - GSKKYMAN
  - SystemSSL
  - Java JCE

Linux

- **Hardware Acceleration**
  - **Asymmetric**
    - RSA handshake
  - **Symmetric**
    - DES, TDES, AES
  - **PRNG**
  - **Hashing**
    - SHA-1 and SHA-256
- **Linux Software Libraries for crypto access**
  - Kernel APIs
  - OpenSSL
  - PKCS#11
  - GSKit

Secure Key Cryptography for System z

z/OS

- Hardware Acceleration
  - Asymmetric and Symmetric
    - CEX2C
- Software Libraries for crypto access
  - ICSF callable services
  - PKCS#11
    - New for z/OS V1R9
    - Full featured PKCS#11 support
  - Java – JCE
  - GSKKYMAN
- Card Management
  - ICSF
  - Trusted Key Entry (TKE)
  - Configure via the SE

Linux

- Hardware Acceleration
  - Asymmetric and Symmetric
    - 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

Demilitarized Zone (DMZ)

Definition:

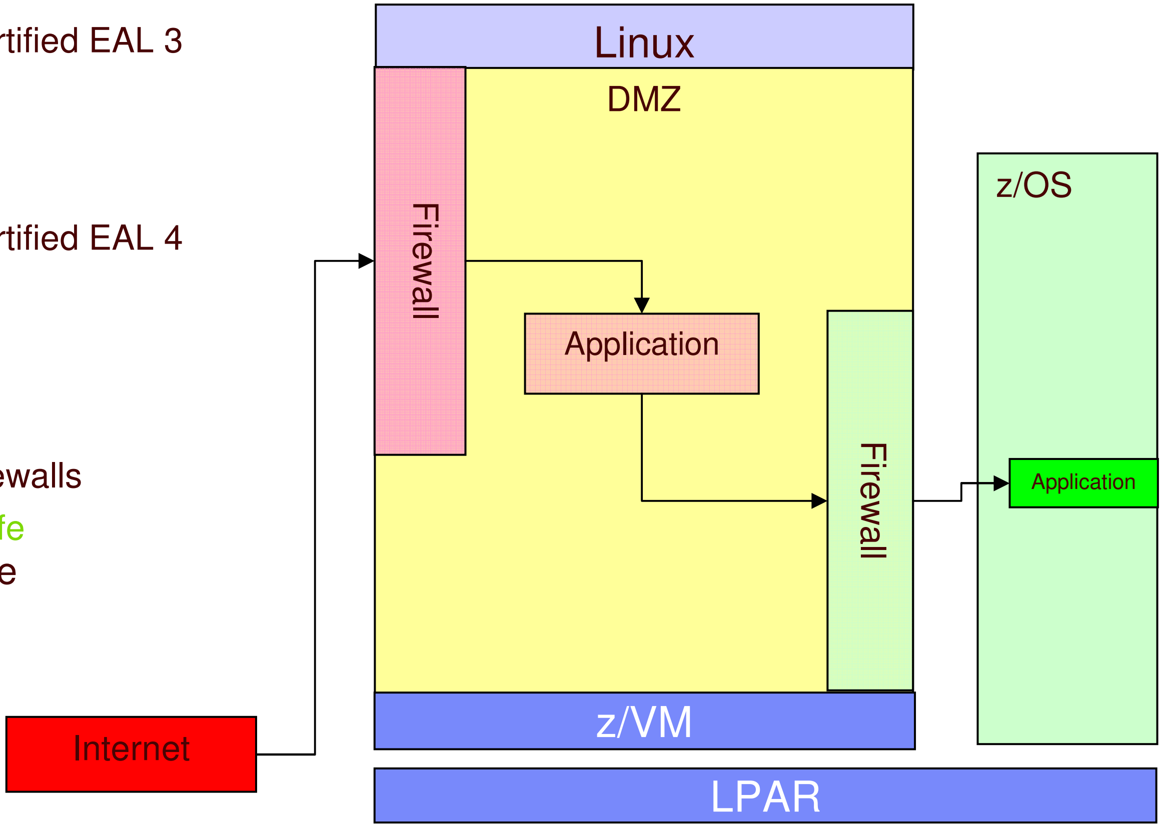
A DMZ is a perimeter network, between an external network and a private or protected network, that provides isolation for a publicly available service, with the ultimate goal of protecting the private network and private services in the enterprise. The DMZ is most often bounded by two firewalls.

Scenario:

A web server that is available to the Internet would need to be isolated, via DMZ, from the enterprise's internal network and/or transaction and data services.

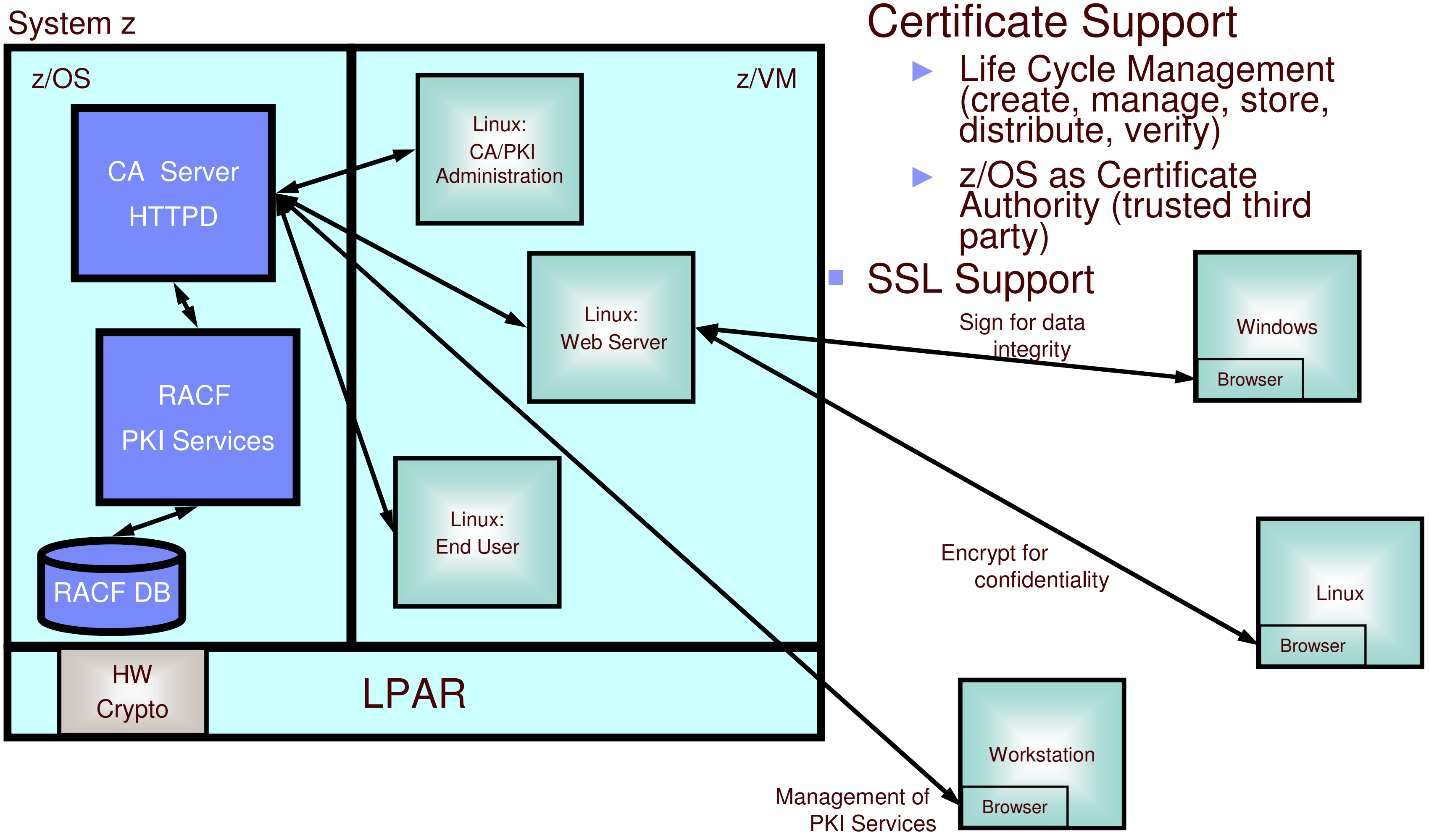
Anatomy of a DMZ on System z

- Isolation with LPAR
  - Common Criteria Certified EAL 4/5
- z/VM
  - Common Criteria Certified EAL 3
  - Integrity Statement
  - RACF
- Linux
  - Common Criteria Certified EAL 4
- Networking
  - HiperSockets
  - Virtual LANs
- Demilitarized Zone
  - Bastion & Choke Firewalls
  - Hot -> Caution -> Safe
- Application or public service
- Auditability



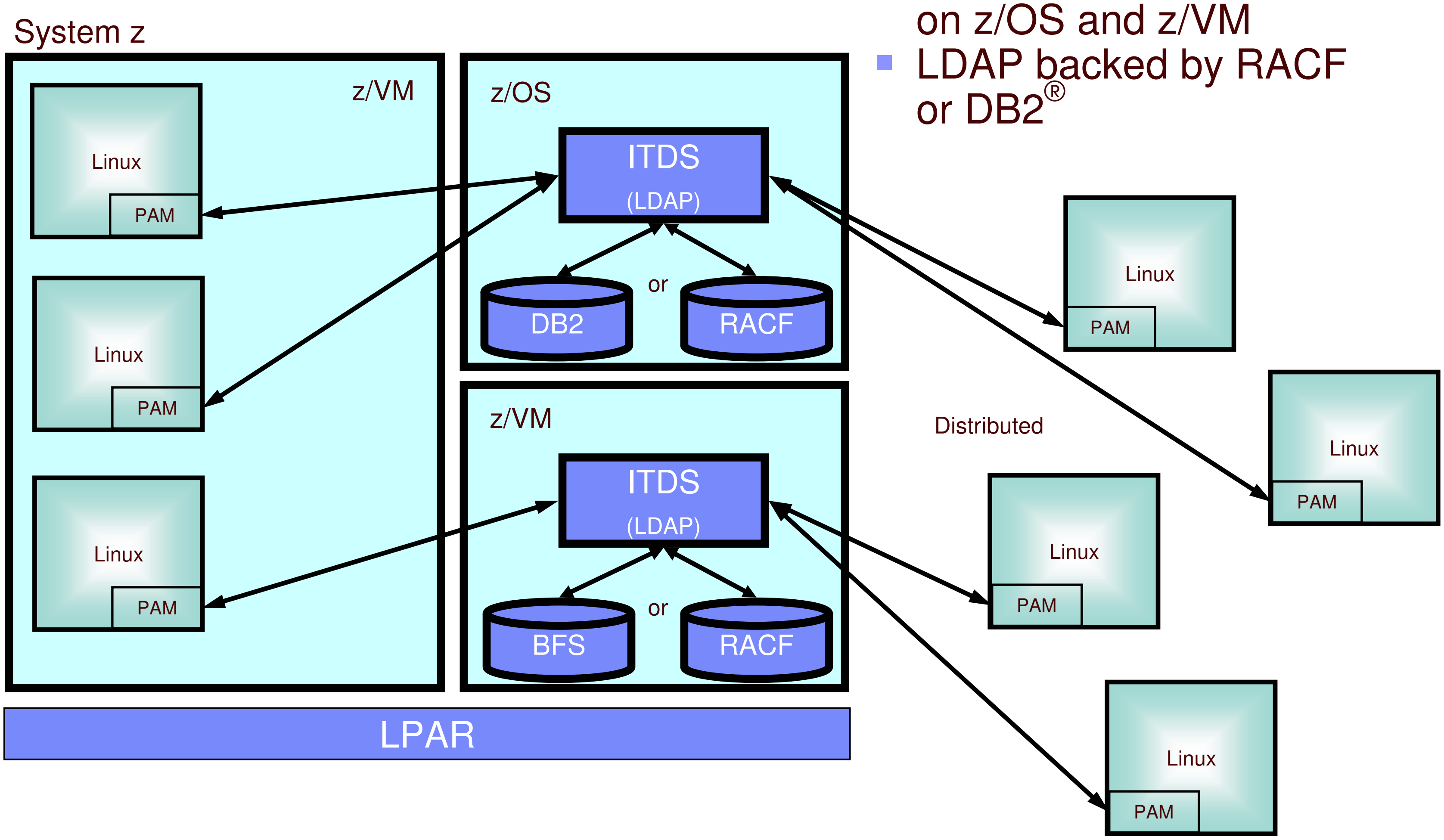
Public Key Infrastructure (PKI)

- Public/Private Key Pair
  - Confidentiality and Data Integrity
- RACF's Digital Certificate Support
  - Life Cycle Management (create, manage, store, distribute, verify)
  - z/OS as Certificate Authority (trusted third party)
- SSL Support



Centralized Authentication

- Common Client – PAM
- Integrated LDAP Server on z/OS and z/VM
- LDAP backed by RACF or DB2®



Questions?