IBM Systems Group

Linux
Sicherheit und Administration

GSE Dortmund, September 2004

Dr. Manfred Gnirss
IBM Deutschland Entwicklung GmbH
Technical Marketing Competence Center Boeblingen, Germany
gnirss@de.ibm.com

© 2004 IBM Corporation

Trademarks

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

AIX*	ESCON*	Multiprise*	S/390 Parallel Enterprise Server	VisualAge*
CICS*	FICON	Netfinity	SecureWay	WebSphere
DB2*	IBM*	OS/390*	System/390*	z/OS
DB2Connect	IBM logo*	PR/SM	VM/ESA*	zSeries
DB2 Universal Database	IMS/ESA	RS/6000*	VSE?ESA	z/VM
e-business logo	MQSeries*	S/390*	Virtual Image Facility	

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Lotus, Notes, and Domino are trademarks or registered trademarks of Lotus Development Corporation
LINUX is a registered trademark of Linus Torvalds
Penguin (Tux) complements of Larry Ewing
Tivoli is a trademark of Tivoli Systems Inc.
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.

IBM considers a product "Year 2000 ready" if the product, when used in accordance with its associated documentation, is capable of correctly processing, providing and/or receiving date data within and between the 20th and 21st centuries, provided that all products (for example, hardware, software and firmware) used with the product properly exchange accurate date data with it. Any statements concerning the Year 2000 readiness of any IBM products contained in this presentation are Year 2000 Readiness Disclosures, subject to the Year 2000 Information and Readiness Disclosure Act of 1998.

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.

© 2004 IBM Corporation

Credits

My very best thanks belong to:

Jack Hoarau
Karl-Erik Stenfors
Jean-Marie Le Rolle
Gerard Laumay
Laurent Dupin
Sylvain Carta
Jean-Yves Girard
Jacques Mazoyer - all from PSSC, Montpellier
Greg Geiselhart, ITSO Poughkeepsie

These people have contributed strongly to this presentation.

Agenda

- ➡ **Security Introduction**
- ➡ **zSeries Hardware**
  - **The zArchitecture integrity**
    - **LPAR**
    - **Crypto solutions**
- ➡ **zSeries Virtualizationsoftware**
  - **z/VM - summary**
- ➡ **Linux security**
  - **Is Linux really secure**
  - **General Linux security**
  - **Linux for zSeries security products**
- ➡ **Certification (Common Criteria)**
- ➡ **Examples**

Some elements to consider

Integrity

- Can the computing environment reliably protect data?

Confidentiality

- Is sensitive data involved?

Risk

- What is the potential cost of unauthorized access?

Threat

- Who is most likely to gain unauthorized access?
  - historically the majority of security incidents originate from within the organization

Vulnerability

- Where is an attack likely to succeed?

© 2004 IBM Corporation

Know your security objectives

What constitutes a 'secure' installation?

- Answer often depends on who is asked
- The most secure machine is:
  - Locked in separate room of bombproof bunker
  - Disconnected from any network
  - Powered off

Some level of paranoia is required

- Choose the correct level of security based on business objectives
- But, DO NOT take security for granted!

Choose the correct security level for your system

© 2004 IBM Corporation

Some vulnerabilities and attacks

Physical compromise / Social engineering

- Stealing, damaging, or manipulating systems
- Shoulder surfing / password guessing

Executable weaknesses

- Trojan horse
- Back door
- SUID executables
- Buffer overflows

Network attacks

- Denial of Service (DoS) attacks
- Scanning
- IP address spoofing
- Session hijacking

© 2004 IBM Corporation

Security Policy

For risk analysis, identify:

- Vulnerabilities
  - Where are the weak points?
- Threats
  - Where are the bad guys most like to attack?

Adopt a general policy

- That which is not expressly permitted is forbidden
- That which is not expressly forbidden is permitted

© 2004 IBM Corporation

Security Policy

One general accepted approach to create a security policy [Fites 1989] includes

the following steps:

1. Identify what you are trying to protect

2. Determine what you are trying to protect it from.

3. Determine how likely the threats are.

4. Implement measures which will protect your assets in a cost-effective manner.

5. *Review the process continuously and make improvements each time a weakness is found.*

Creating a security policy

Security policy:

- States operating procedures for secure computing environment
- Should be in writing!
- Includes guidelines for System administrators and users

For reference, see RFC2196: *Site Security Handbook*

http://www.ietf.org/rfc/rfc2196.txt?number=219

http://www.sans.org/resources/policies/

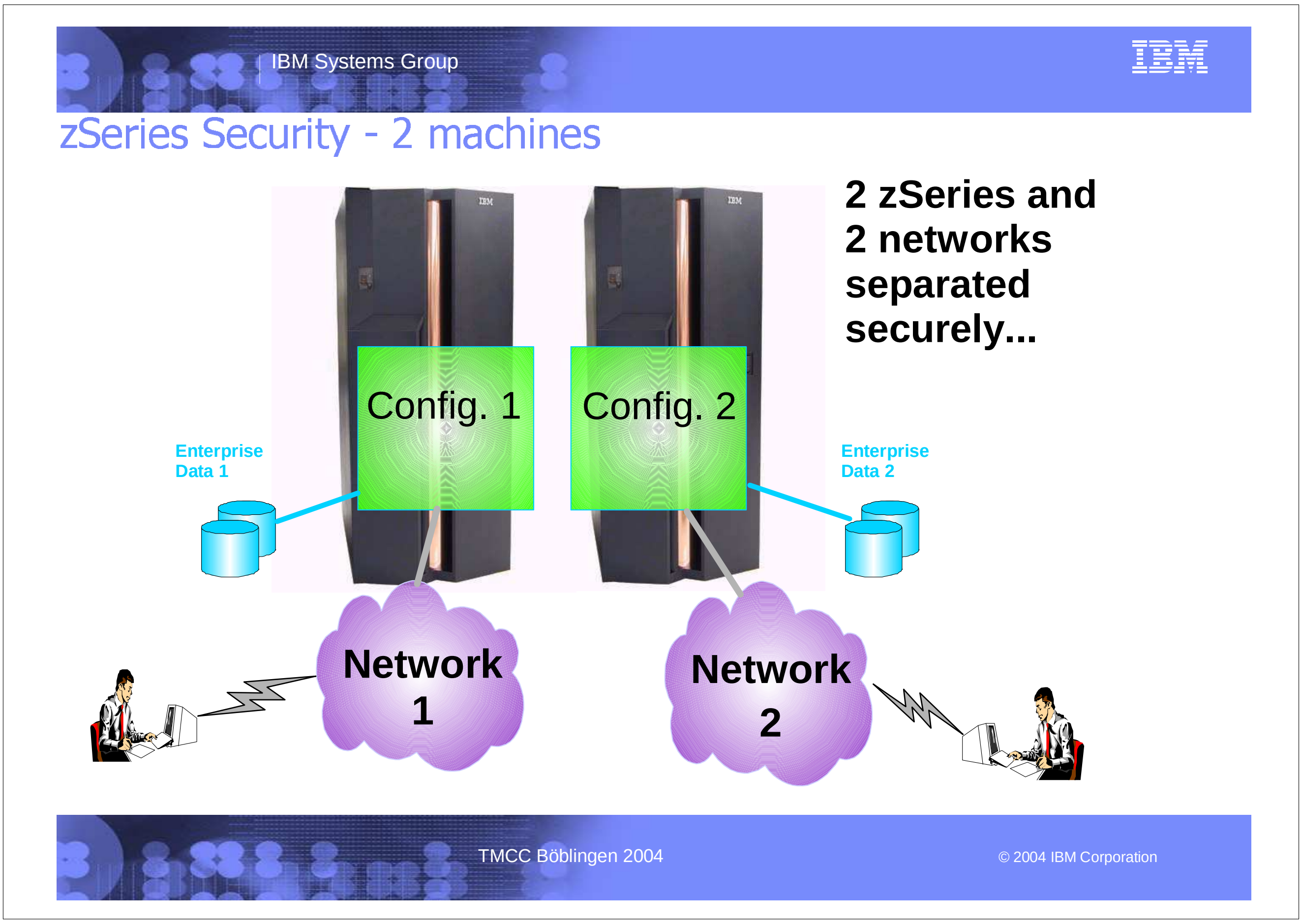
Mandatory.........!

Avoid the 'Alice in Wonderland syndrome':

Create a security policy
so you know what to measure against

The Most Secure Platform for Linux

- S/390 and zSeries
  - Logical Partitioning (LPAR)
    - Provides separation of operating environments
    - G5 and G6: ITSEC E4
    - zSeries: Common Criteria EAL4 and EAL5
  - Cryptographic hardware
    - Integrated Symmetric and Public Key Support
    - Currently FIPS 140-1 Level 4
    - Plans for Common Criteria EAL6
    - Linux drivers for SSL accelerator are available
  - Hipersockets
    - Increased physical security vs. channels
  - Physical security of IT environment



zSeries Security - 2 machines

2 zSeries and 2 networks separated securely...

Config. 1

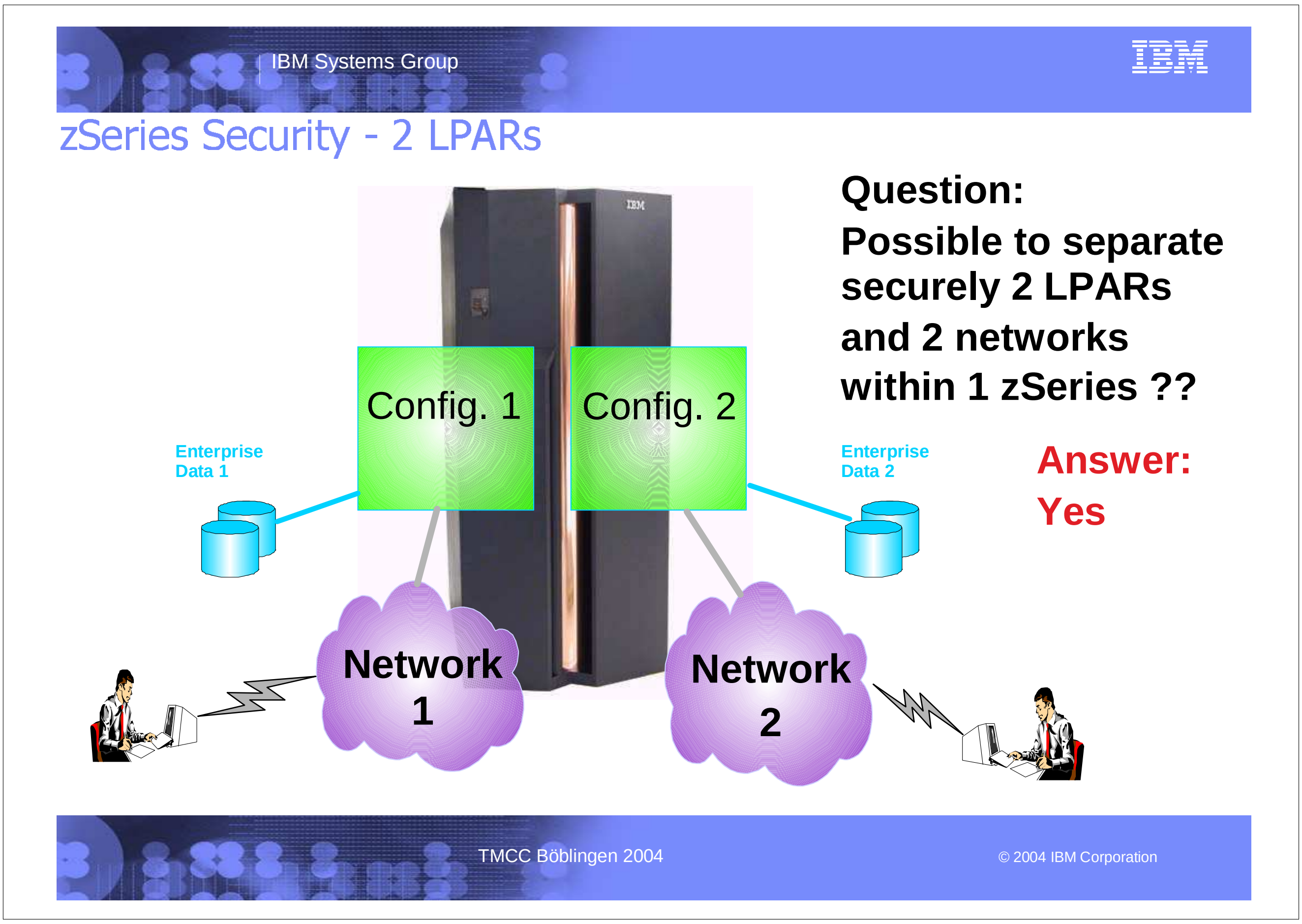
Config. 2

Enterprise Data 1

Enterprise Data 2

Network 1

Network 2



zSeries Security - 2 LPARs

Question: Possible to separate securely 2 LPARs and 2 networks within 1 zSeries ??

Config. 1

Config. 2

Enterprise Data 1

Enterprise Data 2

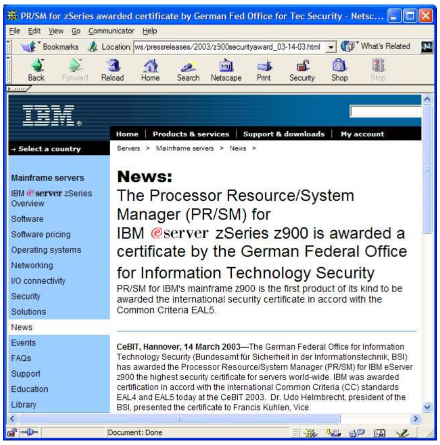
Answer: Yes

Network 1

Network 2

The Most Secure Platform for Linux . . .

- IBM eServer zSeries is the first server received the Common Criteria EAL4 and EAL5 certification level.


PR/SM for zSeries awarded certificate by German Fed Office for Tec Security - Netsc...
File Edit View Go Communicator Help
Bookmarks
Location: ws/pressreleases/2003/z900securityaward_03-14-03.html
What's Related
Back
Forward
Reload
Home
Search
Netscape
Print
Security
Shop
Stop
IBM
Home | Products & services | Support & downloads | My account
→ Select a country
Servers > Mainframe servers > News >
Mainframe servers
IBM eserver zSeries Overview
Software
Software pricing
Operating systems
Networking
I/O connectivity
Security
Solutions
News
Events
FAQs
Support
Education
Library
Document: Done

News:
The Processor Resource/System Manager (PR/SM) for IBM eserver zSeries z900 is awarded a certificate by the German Federal Office for Information Technology Security

PR/SM for IBM's mainframe z900 is the first product of its kind to be awarded the international security certificate in accord with the Common Criteria EAL5.

CeBIT, Hannover, 14 March 2003—The German Federal Office for Information Technology Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) has awarded the Processor Resource/System Manager (PR/SM) for IBM eServer z900 the highest security certificate for servers world-wide. IBM was awarded certification in accord with the international Common Criteria (CC) standards EAL4 and EAL5 today at the CeBIT 2003. Dr. Udo Helmbrecht, president of the BSI, presented the certificate to Francis Kuhlen, Vice

Def. of Evaluation Assurance Levels: see http://commoncriteria.org/docs/EALs.html

General information on zSeries LPAR definition

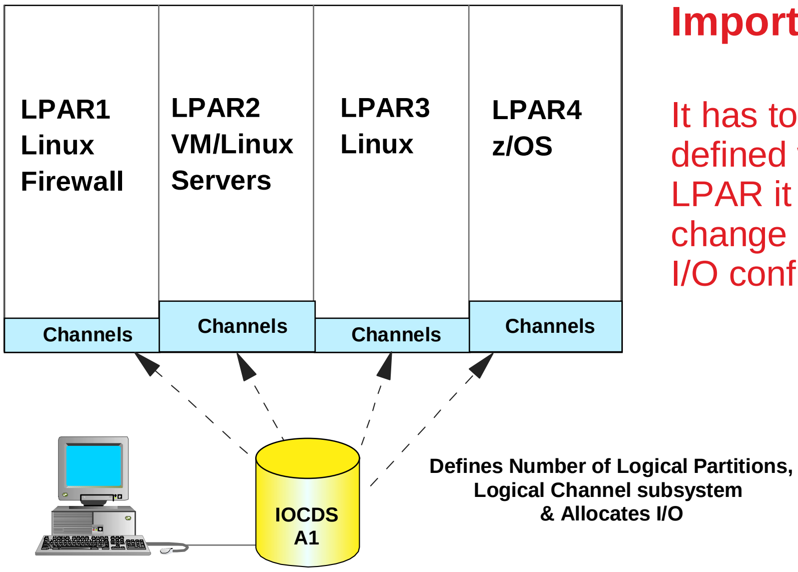
LPAR processors
- **General purpose CPs**
- **IFL (Integrated Facility for Linux): Exclusively for Linux workloads on zSeries. Lower price than for standard engine**

Logical partitioning security
- **Logical partitions built-in isolation**
  - **EAL4 anf EAL5 certification for zSeries PR/SM hardware and microcode**
- **LPARs resources definition and controls**
  - **IOCDS**
  - **Image profiles with LPAR security controls, logical cryptos, load parms, ...**
  - **HMC/SE controlled access**

Logical partition mode
- **Linux only: Can use general purpose CPs or IFL - Does not support other operating system than Linux or z/VM**

LPAR security controls
- **Logical Partition Isolation: Reserve reconfigurable unshared channel paths for the exclusive use of the partition**
- **I/O Configuration Control Authority: Ability of the LPAR to read/write IOCDS and dynamically change I/O configuration**
- **Global Performance Data Control Authority: Ability of the LPAR to view CP activity of other LPARs**
- **Cross Partition Authority: Ability to system reset, deactivate or reconfigure other LPARs**

I/O Definition & Partition Assignment



LPAR1 Linux Firewall

LPAR2 VM/Linux Servers

LPAR3 Linux

LPAR4 z/OS

Channels

Channels

Channels

Channels

IOCDS A1

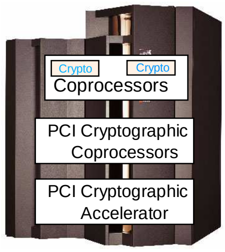
Defines Number of Logical Partitions,
Logical Channel subsystem
& Allocates I/O

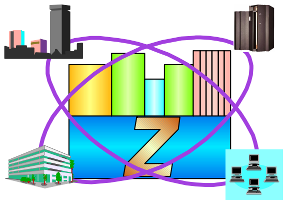
Important:

It has to be clearly defined who / in which LPAR it is allowed to change dynamically the I/O configuration!

zSeries Hardware Security Features

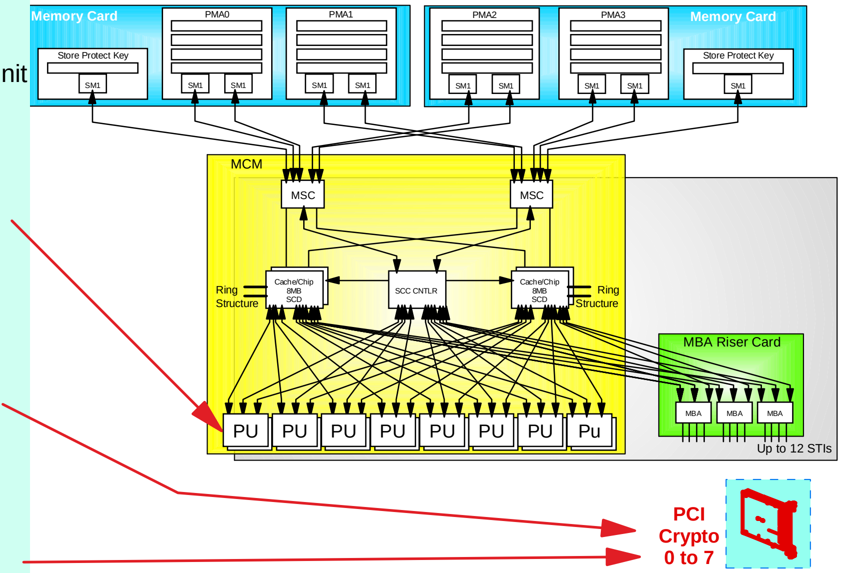
- **Cryptographic Hardware (zSeries)**
  - Cryptographic Coprocessor(s) Facility (CCF) [z800, z900]
  - PCI Cryptographic Coprocessors (PCICC) [z800, z900]
  - PCI Cryptographic Accelerator (PCICA)
  - CP Assist for Cryptographic Functions (CPACF) [z990,z890]
  - PCIX Cryptographic Coprocessor (PCIXCC) [z990,z890]
- **Enables 'End-to-End Security'**
  - 'Tamper-proof' CCF and PCICC, (FIPS 140-1 Level 4), PCIXCC
  - Traditional TDES encryption/decryption
  - Digital Signature Function
  - Secure Sockets Layer (SSL)
  - User-Defined Extensions (PCICC, PCIXCC)
- **z/OS ICSF**
  - Controls and manages cryptographic Hardware
  - Manages crypto service requests (CCF, ...)
- **Performance**
  - Up to 19x faster than a software-Implementation of RSA Digital Signatures Generate
  - Up to 7000 SSL handshakes/sec on z900 model 216
  - Up to 13000 SSL handshakes/sec on z990 2094-316





z990, z890 Hardware Cryptographic Coprocessors

- **CP Assist for Cryptographic Functions (CPACF)**
  - One CPACF per processing unit
  - standard orderable feature
  - 5 new published crypto instructions or through ICSF
  - non-secure (clear keys only)
- **PCI Cryptographic Accelerator (PCICA)**
  - priced feature
  - High performance SSL assist
  - 0 to 6 features in a system
- **PCIX Cryptographic Coprocessor (PCIXCC)**
  - priced feature
  - hardware tamperproof
  - 0 to 4 features in a system



- CPACF and PCICA exploitable by Linux
- up to 8 features total (PCIXCC and PCICA mix)

The z990, z890 CPACF

Functions

- **Clear key DES and hashing**
  - **DES (Single, double, and triple)**
    - **Up to 2**64 byte message, interruptible execution**
    - **Requires FC #3863 to enable (Export control)**
  - **SHA - Defined in FIPS PUB 180-1 publication**
    - **Always enabled**
- **Optimized for low-latency SSL transactions**
- **5 new instructions**
  - **known as the Message Security Assist (MSA)**
  - **see z/Architecture Principles of Operation, SA22-7832-02.**

Technical

- **Can be accessed via problem state instructions.**
- **DES / TDES functions use clear keys only - keys not enciphered under a master key.**
- **New ICSF CCA-like services also provide access.**
  - **Limited key management support.**
    - **RSA PKCS 1.2 key distribution only (via CSNDPKE/ CSNDPKD).**
  - **No CKDS support, at least initially.**
- **CPU affinity problems do not exist with these instructions.**

- **CP Assist for Cryptographic Function (CPACF)**
  - standard feature, z/Series z990 + FC#3863
    - 6/2003 : Support for OS/390 2.10, z/OS 1.2/1.3/ as webdeliverable
    - 6/2003 : Support for z/OS1.4 as orderable feature
  - High performance crypto engine in every CP
  - No special physical security (e.g. secure scan chains, tamper-resistant packaging, etc.)
  - NOT FIPS 140-2 Level 4 secure

The z990, z890 PCI XCC

Functions

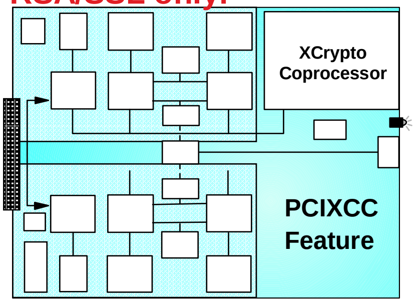
- New PCIX Cryptographic Coprocessor (PCIXCC)
  - Single Integrated xCrypto feature
    - Full CCF and PCICC functionality
  - Improved cost/performance over PCICC
  - Scalable (no CP affinity) - 0 to 4 Coprocessor features
  - Extensive RAS
  - Current applications will run without change
  - Hot pluggable, removal zeroization detection
  - Connection to STI interface; no external cables
  - Fully programmable, UDX support via a special contract with IBM
  - Instrumentation and measurement data provided

Technical

- PPC 405 processor.
- Hardware error checking.
- RSA / DES / TDES functions use both clear and master key enciphered keys
- Faster RSA / SHA / DES engines.
- More memory and flash.
- Embedded LINUX operating system.
- Hardware - assisted communications protocol.
- CCA performance at least 900 calls / second / card.

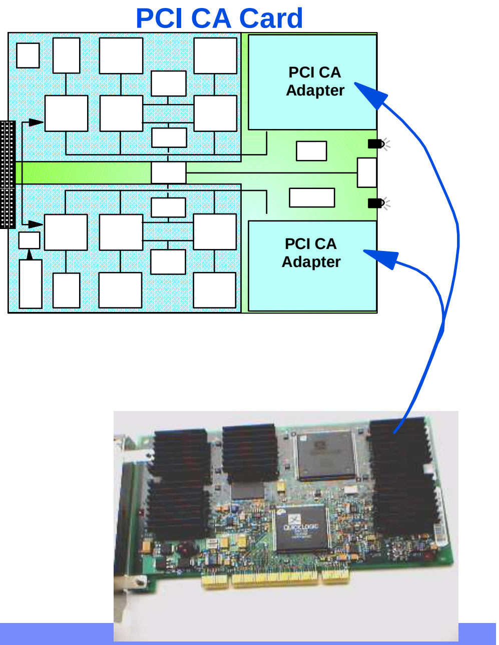
➡ Linux: RSA/SSL only!

- Peripheral Component Interconnect xCryptographic Card (PCI XCC)
  - Optional feature, z/Series z990 + FC#3863
    - 9/2003 : Support for z/OS 1.2/1.4
    - 17.10.2003 : Support for OS/390 2.10, 21.11.2003 z/OS 1.3
  - Maximum of 4 PCI XCC features
    - *PCI XCC - single-card book*
    - *requires a specific level of compatibility code*
    - *requires a configuration loaded CPACF as a corequiste device.*

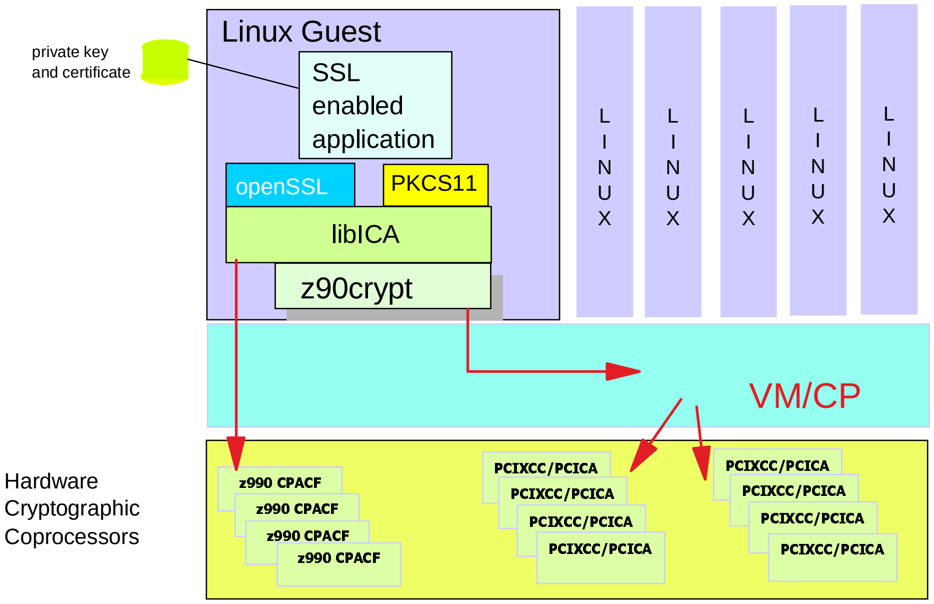


PCI Cryptographic Accelerator Card (FC0862) [z8x0, z9x0]

- Up to 6 features / 12 processors
- Total of PCICA and PCICC/PCIXCC features limited to 8
- Designed to provide increased SSL throughput and price performance (> 50%)
- High performance asymmetric encryption
- (Public Key) accelerator
- Up to 800 SSL handshakes/sec per z800
- Several thousands of SSL handshakes/sec per z900 or z990
- z/OS:
  - managed by ICSF (with CCF enabled)
  - access via PKCS #11 API
- Linux (CP or IFL):
  - access via PKCS #11 API or openSSL library



Linux Access to Crypto Hardware on z990, z890



private key and certificate

Linux Guest

SSL enabled application

openSSL

PKCS11

libICA

z90crypt

LINUX

LINUX

LINUX

LINUX

LINUX

VM/CP

Hardware Cryptographic Coprocessors

z990 CPACF

z990 CPACF

z990 CPACF

z990 CPACF

PCIXCC/PCICA

PCIXCC/PCICA

PCIXCC/PCICA

PCIXCC/PCICA

PCIXCC/PCICA

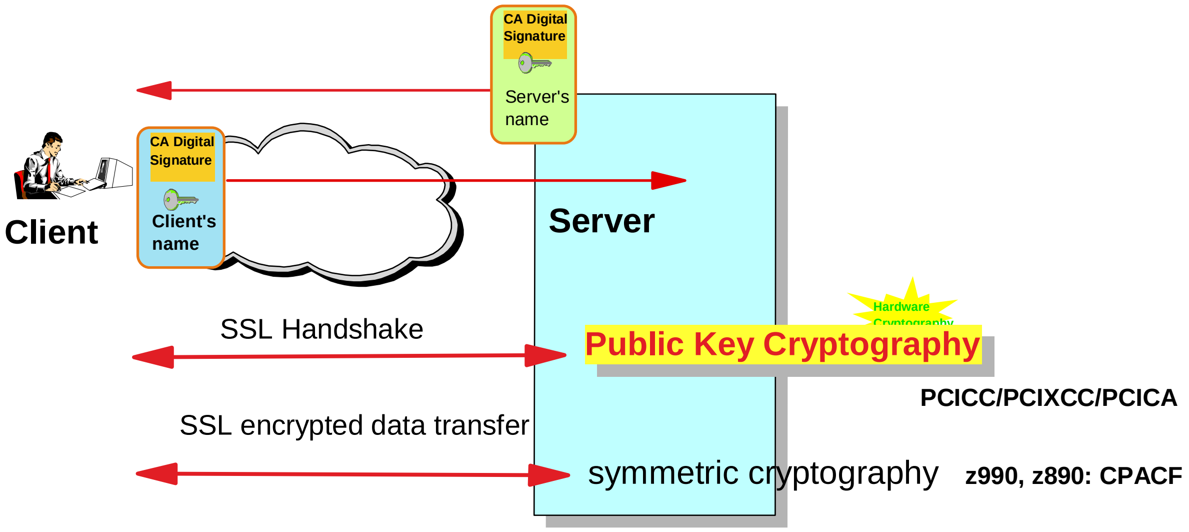
PCIXCC/PCICA

PCIXCC/PCICA

PCIXCC/PCICA

Hardware Supprot for Secure Socket Layer (SSL) Protocol

Secure Socket Layer is a communications protocol, developed by Netscape, for client/server secure socket communications



CA Digital Signature

Server's name

CA Digital Signature

Client's name

Client

Server

Hardware Cryptography

SSL Handshake

Public Key Cryptography

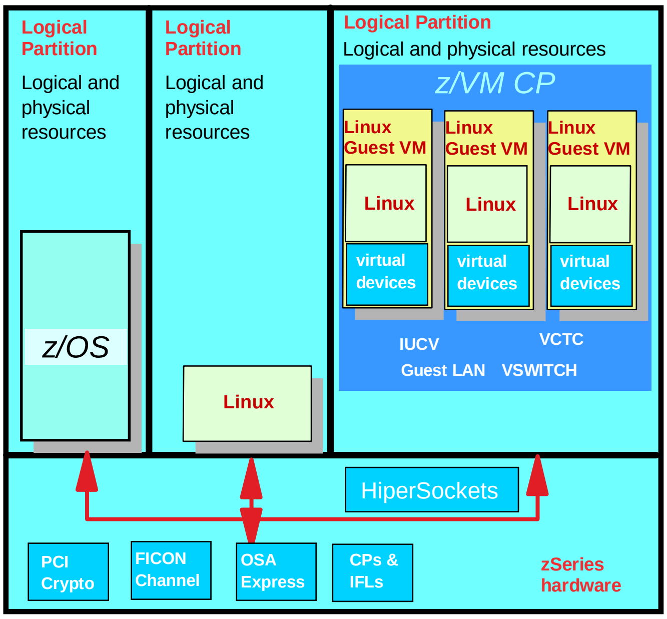
PCICC/PCIXCC/PCICA

SSL encrypted data transfer

symmetric cryptography

z990, z890: CPACF

zSeries Virtualization



Logical Partition
Logical and physical resources
z/OS

Logical Partition
Logical and physical resources
Linux

Logical Partition
Logical and physical resources
z/VM CP
Linux Guest VM
Linux
virtual devices
Linux Guest VM
Linux
virtual devices
Linux Guest VM
Linux
virtual devices
IUCV
VCTC
Guest LAN VSWITCH

HiperSockets
PCI Crypto
FICON Channel
OSA Express
CPs & IFLs
zSeries hardware

z/VM Control Program (CP) virtualization

- Virtual devices
- Virtual networks

LPAR Microcode virtualization

- Logical resources
- HiperSockets networks

VM Guest Isolation

Virtual guest machines isolation by z/VM Control Program (CP):

- Combination of software and hardware mechanisms (dynamic address translation, SIE guest storage extent limitation, Set Address Limit facility, disk extent limitation)
- IBM z/VM integrity statement (for details: see GIM)

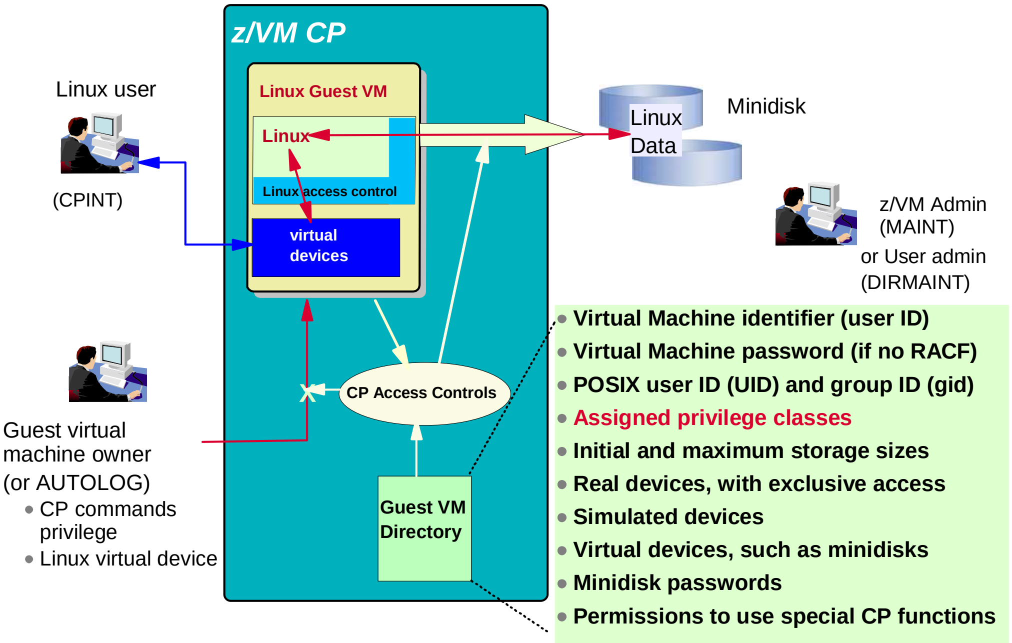
■ **Each Linux server image running under z/VM is entirely isolated from other server images**

- ► no access to storage
- ► shared data access and communications through physical pathways (virtual machine directory) or defined VM services (controlled via CP commands)

For Background Information see:
Alan Altmark, Cliff Laking, z/VM Security and Integrity. Technical Paper:
http://www.ibm.com/servers/eserver/zseries/library/techpapers/gm130145.html

Common Criteria Certification EAL 3+ is in progress ... (planned for 2004)

Virtual machine access control - VM Directory



- **Virtual Machine identifier (user ID)**
- **Virtual Machine password (if no RACF)**
- **POSIX user ID (UID) and group ID (gid)**
- **Assigned privilege classes**
- **Initial and maximum storage sizes**
- **Real devices, with exclusive access**
- **Simulated devices**
- **Virtual devices, such as minidisks**
- **Minidisk passwords**
- **Permissions to use special CP functions**

VM Directory Maintenance facility - DirMaint

Directory **Maint**enance facility
(safe, efficient, interactive maintenance of VM directory)

- Directory integrity and availability
- Directory changes through general users and system admin commands
- Enforcement of password change policy
- Minidisk allocation
  - automated allocation (gaps management and overlap control)
  - automated erasure
- Auditing of all transactions
- Automatic backup of directory
- Further Automation via exits

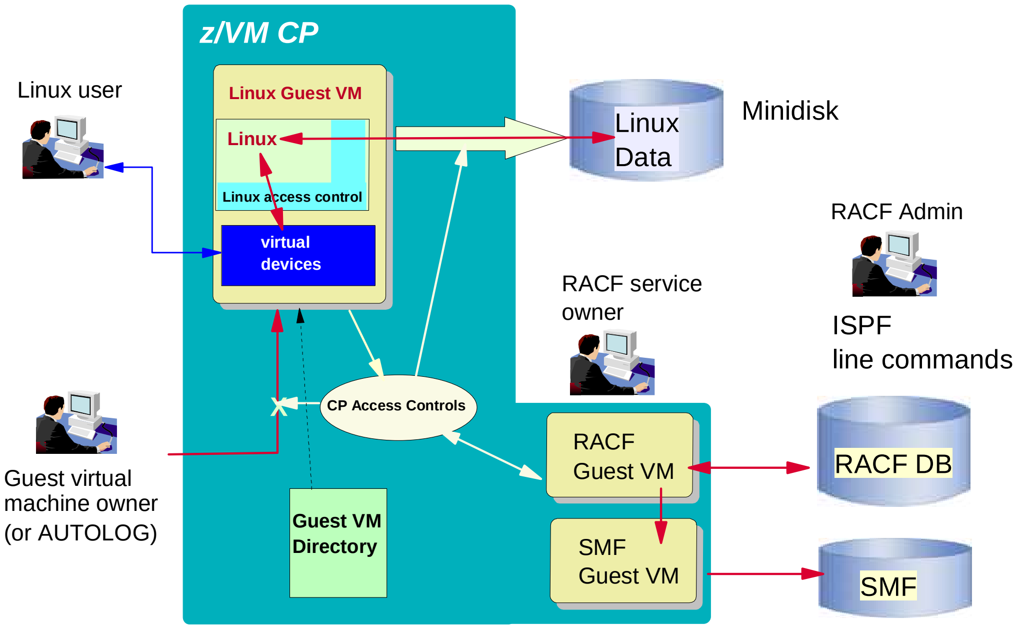
Feature for z/VM (priced)

External Security Manager feature - RACF

- Enhances auditing, authentication, logs, and access controls
  - reports
- Encrypt user passwords
- Use Access Control List for minidisks instead of minidisk password
- Well-defined programming interfaces
  - RACROUTE macro
  - CSL routines
- RACF/VM is a feature of z/VM 5.1 (priced)

Note: RACF databases not shared between z/VM and z/OS

Virtual machine access control - RACF



z/VM CP

Linux user

Linux Guest VM

Linux

Linux access control

virtual devices

Linux Data

Minidisk

RACF Admin

RACF service owner

ISPF line commands

CP Access Controls

X

RACF Guest VM

RACF DB

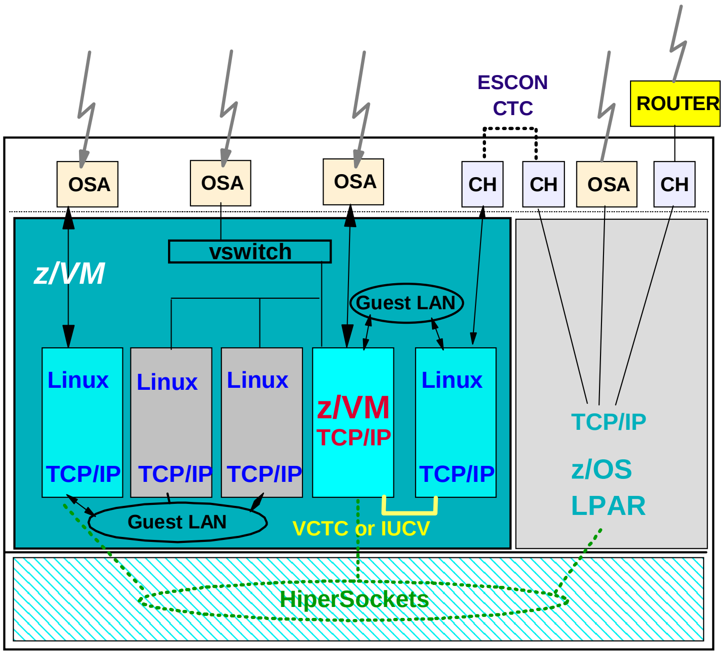
SMF Guest VM

SMF

Guest virtual machine owner (or AUTOLOG)

Guest VM Directory

Networking - connectivity of Linux guests



- ➤ESCON
- ➤OSA Card
- ➤ESCON CTC
- ➤Virtual CTC
- ➤IUCV
- ➤Guest LAN
- ➤Virtual Switch

Virtual Networks

- **IUCV** (point to point)
  - Access control by IUCV statement in directory
  - Be careful with IUCV ANY and IUCV ALL
- **Virtual CTC** (point to point)
  - DEFINE command or SPECIAL statement in directory can restrict partner to prevent unwanted connections
- **Guest LANs**
  - restricted or unrestricted
  - restricted LANs require specific authorization to connect
- **Virtual Switch (VLAN)**
  - Access list control (SET VSWITCH)
  - Restricted use
  - VLAN membership controls
- Enhanced authorization function using ESM for Guest LANs and VSWITH with z/VM 5.1

TCP/IP for z/VM

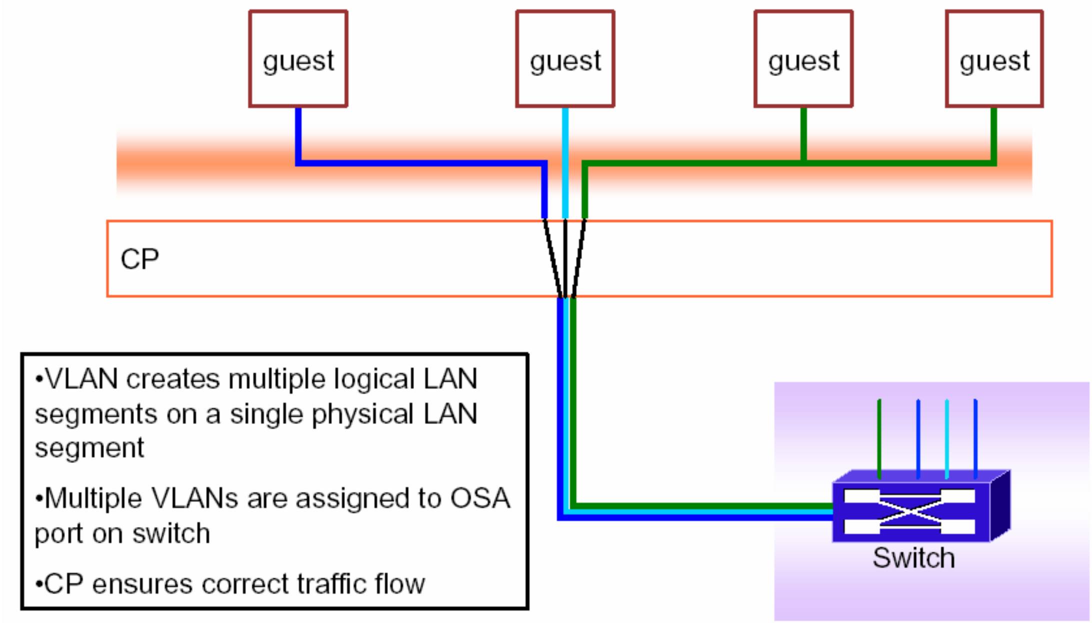
- TCP/IP for z/VM provides functions
  - Connectivity and Gateway, Server, Clients, Network status and management, Application and programming interfaces
- … and security facilities
  - Kerberos authentications service, SSL support, built-in protection against Denial Of Service attacks, exits to ESM.
- The z/VM TCP/IP stack runs in a dual-homed service machine
- The stack configuration is owned by TCPMAINT
- TCP/IP services via other virtual machines
  - FTP, DNS, ..., SSL server (with the SSLSERV Linux guest)

Connectivity with zSeries and z/VM

Other Security considerations

- In all cases guest systems must implement proper TCP/IP protection in their TCP/IP stack
- Configuration decision: who owns the physical interface to the physical network ?

z/VM advanced Networking -VLAN on Virtual Switch



- •VLAN creates multiple logical LAN segments on a single physical LAN segment
- •Multiple VLANs are assigned to OSA port on switch
- •CP ensures correct traffic flow

Linux for zSeries Security: kernel

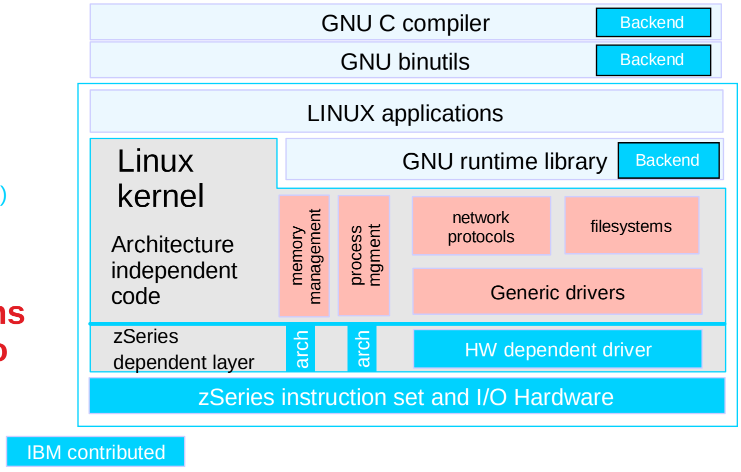
- Linux for zSeries is pure Linux
  - No kernel code changes for security on zSeries

Remember: Design guiderules

- Linux for zSeries remains Linux
  same structure, fully ASCII-based
- zSeries remains zSeries
  Linux object code uses S/390-zSeries instruction set.
  Specific drivers to exploit zSeries features (PCI cryptos, OSA-Express, FICON, ...)

Consequence:

- **All general Linux security methods, recommendations and guidlines apply also to Linux for zSeries !**



Is Linux secure..........?

- Linux for zSeries is as secure as Linux on all other platforms
- Linux for zSeries is open, no security through obscurity, anyone can see flaws and fix them
- Linux has a large active developer base ensuring a thorough code review
- Linux has a worldwide user base which ensures 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

Is Open Source Less Secure?

- Open Source: No 'security by obscurity'
  - Anyone can analyze the code for flaws and exploit them
  - Anyone can analyze the code for flaws and fix them
  - Peer review by an active developer base increases the likelihood of flaws being discovered and fixed
  - An active developer base usually means fixes appear quickly in response to CERT advisories
- Perhaps more importantly, how current is your software maintenance?

Linux OS Integrity

- Open Source vs. Vendor Source
  - Who issues the Vendor Integrity Statement?
  - Who's responsible for fixing code vulnerabilities?
  - Who's responsible for integration testing?
- Who Will Certify Linux Integrity?
  - Linus Torvald?
  - Distributors?
  - NSA?
  - Commercial Service Providers?
  - Independent Certification Orgs?
  - The customer?

➡ Service contract

Linux System logging

Linux logging is controlled by the syslog utility.

- syslogd daemon accepts incoming log messages form
  - Linux kernel
  - System devices (mail, cron, PAM, ...)
  - Application programs
- Configuration of syslogd: /etc/syslog.conf

Sample /etc/syslog.conf file

```
# /etc/syslog.conf - Configuration for syslogd
# entries are of the form: facility.level action
# Print most on /dev/console
kern.*;*.warn;news.emerg;mail.alert    /dev/console
# all mail messages in one file
mail.*                                -/var/log/mail
# Warnings in one file
*.=warn;*.=err                         /var/log/warn
# rest in one file
*.*;mail.none;news.none
/var/log/messages
# Log to a remote host
*.*                                    @192.168.10.1
```

- Using a Central log server
  - simplified log administration
  - Enhanced log file integrity

Data Encryption

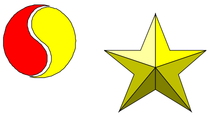
- Within the computer
  - ► encrypt files on disk or
  - ► entire data volumes
  - ► tools for encrypting Linux data
- Communications between systems
  - ► tools to encrypt email, data transfers
  - ► add cryptography to web servers
  - ► disable FTP and Telnet
    - – check your Linux distribution for secure versions
    - – warn users
    - – find other replacements
      - ● tcpd
      - ● use SCP instead of FTP

Linux user management - user types

ROOT user
id = 0 , gid =0

↓

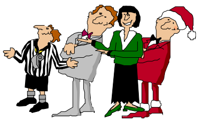
- ○ all privileges
- ○ no security control
- ○ can add user
- ○ can install sofware....



system users
system groups
0 < uid <= 499
0 < gid <= 499

↓

- ○ no password
- ○ cannot log into the system (open a shell)
- ○ Isolate application environment

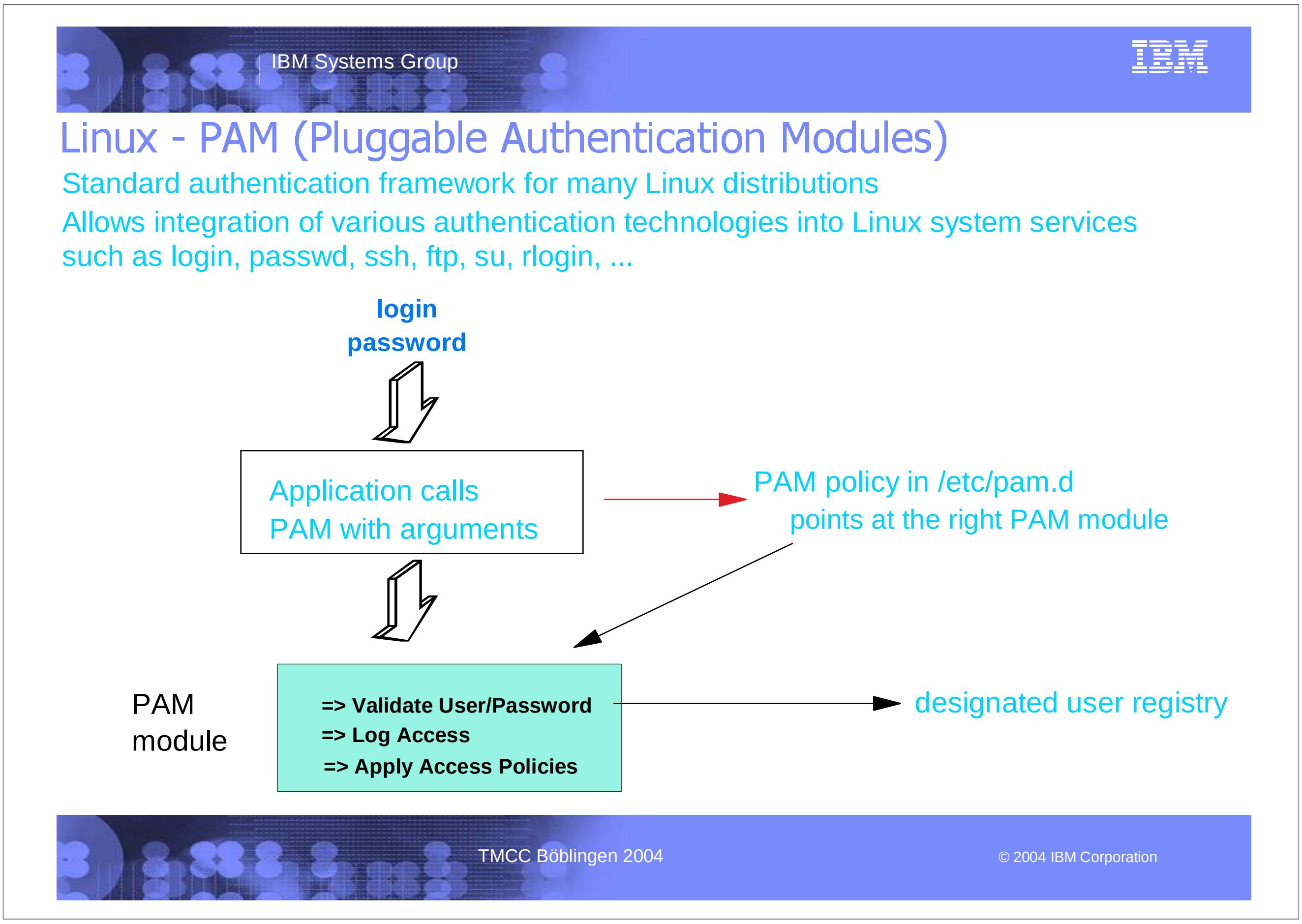


common users
common groups
uid >= 500
gid >= 500

↓

- ○ has a password
- ○ has an account
- ○ access controlled

Controlling permissions and privileges



Linux - PAM (Pluggable Authentication Modules)

Standard authentication framework for many Linux distributions

Allows integration of various authentication technologies into Linux system services such as login, passwd, ssh, ftp, su, rlogin, ...

login
password

Application calls
PAM with arguments

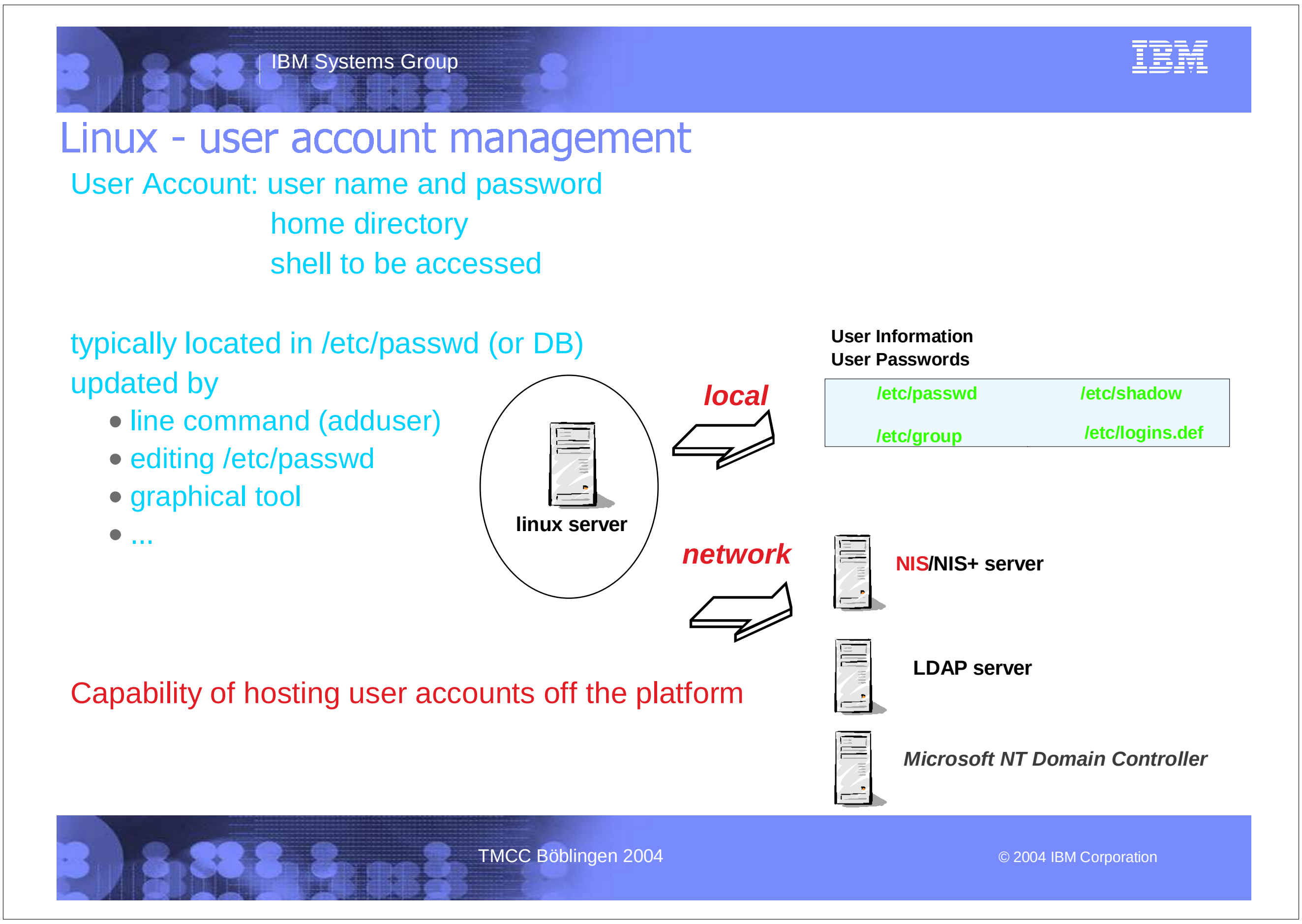
PAM policy in /etc/pam.d
points at the right PAM module

PAM
module

=> Validate User/Password
=> Log Access
=> Apply Access Policies

designated user registry

© 2004 IBM Corporation



Linux - user account management

User Account: user name and password
home directory
shell to be accessed

typically located in /etc/passwd (or DB)
updated by

- line command (adduser)
- editing /etc/passwd
- graphical tool
- ...

linux server

local

User Information
User Passwords

/etc/passwd	**/etc/shadow**
/etc/group	**/etc/logins.def**

network

NIS/NIS+ server

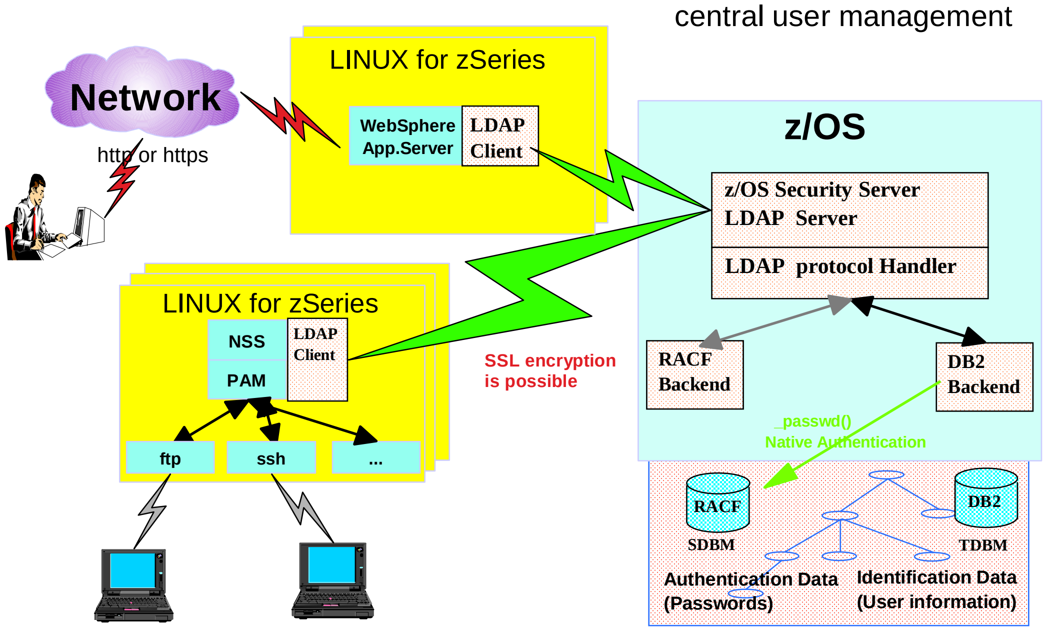
LDAP server

Microsoft NT Domain Controller

Capability of hosting user accounts off the platform

© 2004 IBM Corporation

Linux user authentication and identification: via LDAP (RACF)



central user management

Network

http or https

LINUX for zSeries

WebSphere App.Server

LDAP Client

z/OS

z/OS Security Server LDAP Server

LDAP protocol Handler

LINUX for zSeries

NSS

PAM

LDAP Client

ftp

ssh

...

SSL encryption is possible

RACF Backend

DB2 Backend

_passwd() Native Authentication

RACF

SDBM

DB2

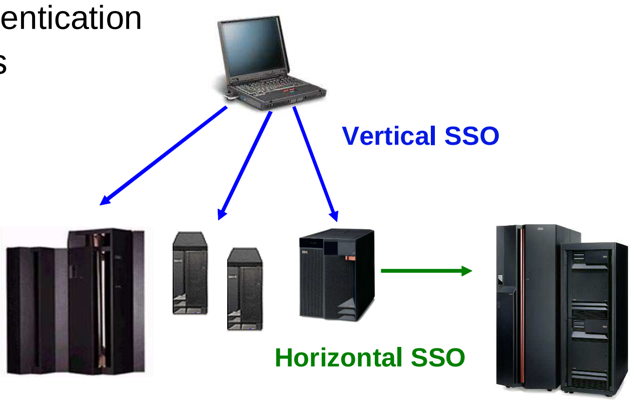
TDBM

Authentication Data (Passwords)

Identification Data (User information)

More complex: Single Sign-On (SSO)

- Sign-on once to the network using, for example user Id and password
- Subsequent connection requests to application services and resources are authenticated without prompting for user / pw
  - Network authentication protocols, such as Kerberos, are used to perform authentication
- Taking different identities for various applications for a single entity into consideration is desirable



Vertical SSO

Horizontal SSO

One Possiblity:
Using Kerberos in combination with Enterprise Identity Mapping (EIM)
- session for next GSE meeting ?

Hardening the platform

Basics

- Enterprise Linux implementations should have specific functions
  Keep in mind the services you need and don't need.
- Create hardened bases then clone them

More ...

- Daemons must have no shells
- Webserver – Careful use of ACLs minimize risk
- Use ssh (protocol 2) instead of telnet
- No mail (or only mail) on enterprise Linux servers
- X windows is basically insecure (go with SSH and X11 forwarding)
- Same with the file servers
- delete unused accounts
- use nobody for daemons
- physical console security

Hardening the platform . . .

And some tools ...

- Bastille to harden your Linux
- Check for vulnerabilities on your system
  e.g. NMAP for scanning
  FTPD
  NFS
  RSH (go with SSH)
  sendmail
  smb
  X serverE (go with SSH and X11 forwarding)

Linux - root (superuser) privileges

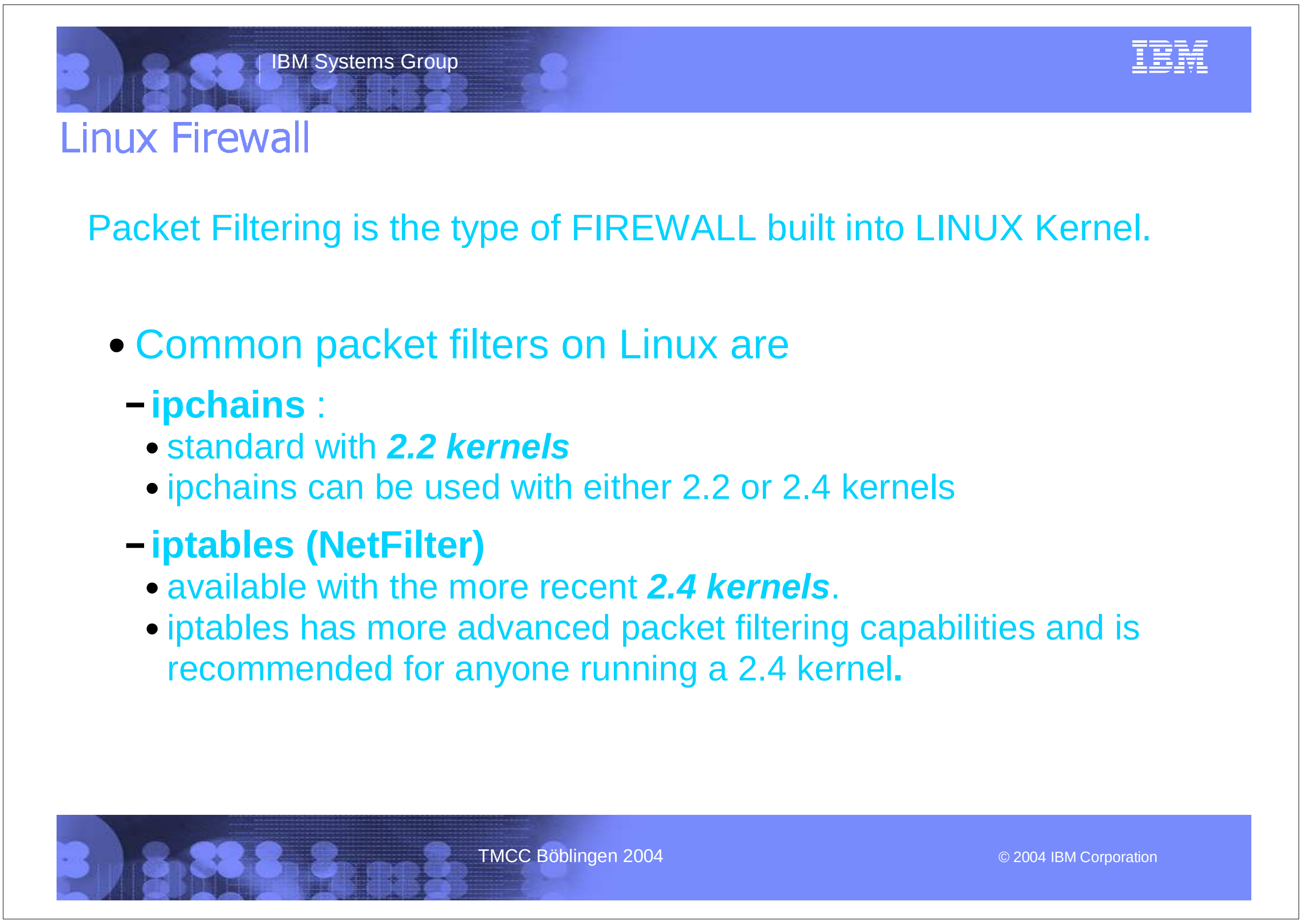
- Use of privileged account, root, to mission critical staff only
- Limit superuser login to secure terminal (using pam_securetty.so)
- Delegate superuser authority with 'sudo' utility.
  - Grant limited authorities to certain users or group of users
    - /etc/sudoers
    - commands that sudo users can run
    - host aliases
    - user aliases
    - user specifications (user list and run-as user (typically: root))
  - All sudo commands are logged to syslog
  - Example: Installation of a package: sudo rpm -Uvh package.rpm

© 2004 IBM Corporation

Firewalls/Communications

- Most Linux distributions have firewall support
- Commercial firewalls: Stonegate, zGuard
- LogCheck
  - automates log file checking, sniffs out problems
- SSH Secure Shell available for download: www.ssh.fi, www.openssh.org
  - implementation of SSL, not part of Linux
- Use firewalls outside and inside they system
- Virus (for Windows Systems) can be forwarded by email or files
  - check incoming email & downloaded files
- Trojan horses/worms
  - filter email
  - prevent Java/Javascript applets from running
  - RPM packages and signatures

© 2004 IBM Corporation

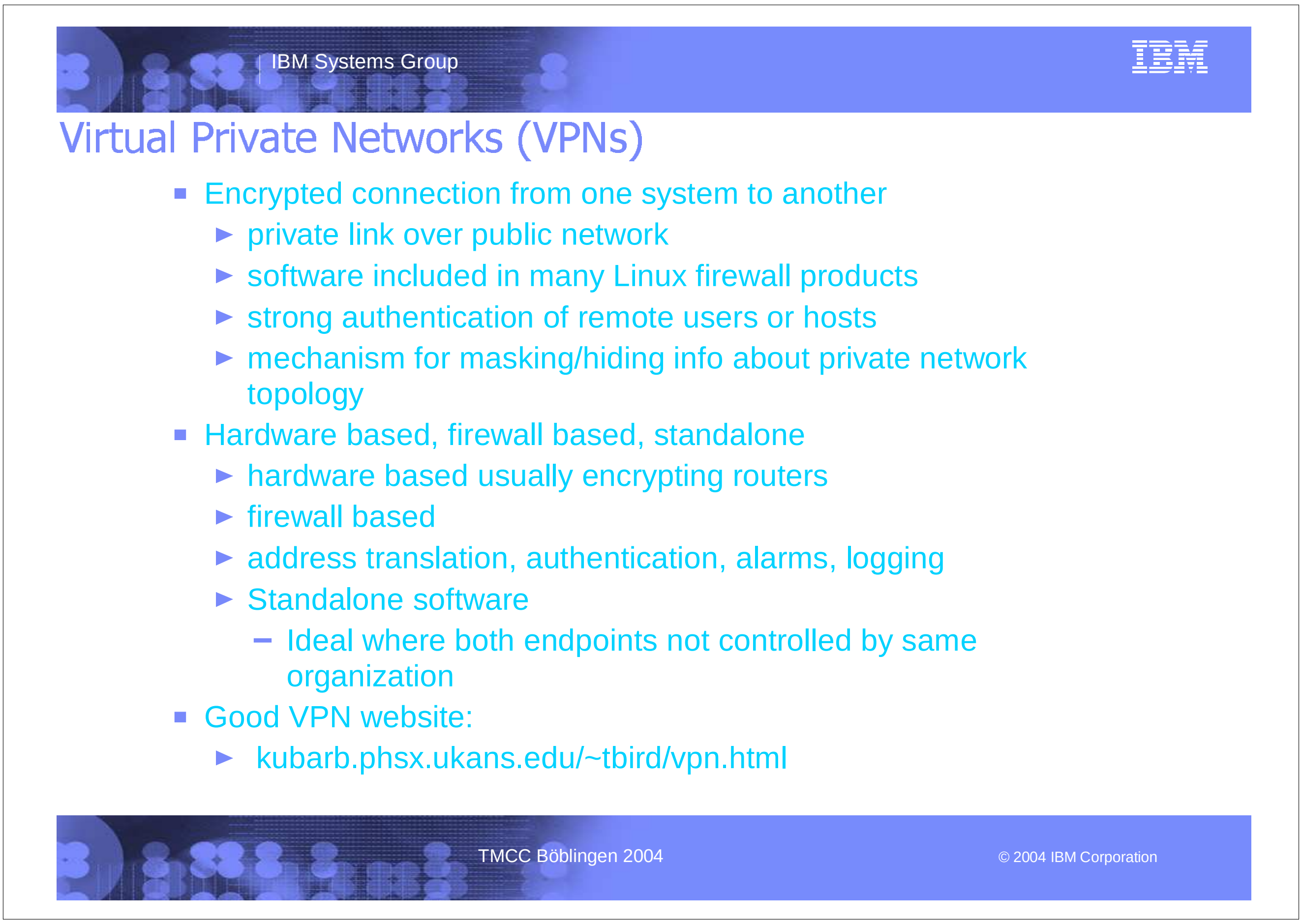


Linux Firewall

Packet Filtering is the type of FIREWALL built into LINUX Kernel.

- Common packet filters on Linux are
  - **ipchains** :
    - standard with ***2.2 kernels***
    - ipchains can be used with either 2.2 or 2.4 kernels
  - **iptables (NetFilter)**
    - available with the more recent ***2.4 kernels***.
    - iptables has more advanced packet filtering capabilities and is recommended for anyone running a 2.4 kernel.

© 2004 IBM Corporation



Virtual Private Networks (VPNs)

- Encrypted connection from one system to another
  - private link over public network
  - software included in many Linux firewall products
  - strong authentication of remote users or hosts
  - mechanism for masking/hiding info about private network topology
- Hardware based, firewall based, standalone
  - hardware based usually encrypting routers
  - firewall based
  - address translation, authentication, alarms, logging
  - Standalone software
    - Ideal where both endpoints not controlled by same organization
- Good VPN website:
  - kubarb.phsx.ukans.edu/~tbird/vpn.html

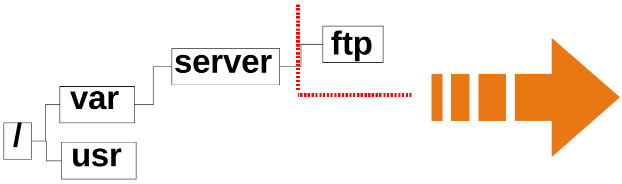
© 2004 IBM Corporation

Linux - Chroot Jail

Restrict filesystem scope of a process

The redefined root filesystem reference is passed in arguments

```
service ftp {
    socket-type     =   stream
    wait            =   no
    user            =    root
    server          =   /usr/sbin/in.ftpd
    server_args     =  -l /usr/sbin/chroot /var/servers/ftp
}
```



/

var

usr

server

ftp

ftpd server cannot not access /usr, /home only files located in /var/servers/ftp

Linux - Network Monitoring - IDS

- Running network security audit
  - Using Network Intrusion Detection Systems NIDS
  - Monitoring Log Files generated by network Services LFM
  - Verifying System Integrity SIV
- nessus
  - network security auditing tools
  - generate a security report
  - http://www.nessus.org
- snort
  - Intrusion Detection System
  - http://www.snort.org

Linux - TCP wrapper

- Program that intercepts requests before passing them onto the real deamon
- Can be used ensure that unauthorized users don't get to your services
  - /etc/ hosts. allow
  - /etc/ hosts. deny
- Also used to create logs to keep track of access attempts to services

- Example: hosts. deny and hosts. allow in /etc
  - /etc/hosts.allow

    ftpd: LOCAL,.company. com

    sshd: all
  - /etc/ hosts.deny

    ALL: ALL

Note:
- No protection against man-in-the-middle
- No protection against situations where network router is compromised
- All unencrypted network data is open for inspection
- TCP-wrapper only one part of a defense strategy.

Some security technologies for Linux

Access Control Lists	LoMac, Best Bits, IBM Tivoli Access Manager, CA's eTrust Access Control
Anti-Virus	AmaViS, MIMEDefrag, RAV AntiVirus, CA's eTrust AntiVirus
Hardware SSL Acceleration	PCICC/PCIXCC and PCICA , CPAF on z990 from IBM
Digital Certificates	Freeware PKI
Firewall	IPTables/NetFilter (IPChains), zGuard, StoneGate
Intrusion Detection	Snort, Snare, PortSentry, TripWire, LIDS, IPLog, IBM Tivoli Risk Manager, CA's eTrust, ISS RealSecure
Directory Services	OpenLDAP, IBM Directory, NIS/NIS+ (restrictions)

Vendor Product

Open Source Product

Some security technologies for Linux

Secure Network Communications	OpenSSH, PGP, GNU PGP, USAGI IPv6, FreeS/WAN, CA's eTrust VPN
Secure Socket Layer (SSL)	OpenSSL, GSKIT, PKCS#11
System Hardening	Bastille, Tiger, Distributions
Secure Data	CFS, TCFS, ppdd, McAfee's E-Business Server
Distributed Policy Management	IBM Tivoli Access Manager, CA's eTrust Directory
Proxy Server	Proxy Suite from SuSE, IBM Edge Server, SQUID

Security Patches

- Linux Loadable Security Module
  - Enhancements to Future Linux Kernel (2.6 now)
  - Interface to External Security Module
- NSA SE LINUX
  - NSA developed security patches
  - http://www.nsa.gov/selinux/
  - most of this in 2.6 now
- RSBAC
  - Patch providing Rule Set Based Access Control
  - ACLs, MAC, (but no audit)
  - http://www.rsbac.org/

Other Security Projects and Modules

- Auditing Project 'auditd'
  - Security Module for Improved Auditing
  - http://www.hert.org/projects/linux/auditd/
- Argus PitBull LX
  - Security Module Implementing Access Domains
  - http://www.argus-systems.com/product/
- Abacus Project
  - Improved Log Checking with Logcheck
  - http://www.psionic.com/abacus
- Bastille Project
  - Security Wizards for More Secure Linux Setup
  - http://www.bastille-linux.org/

© 2004 IBM Corporation

Secure Linux Distributions

- Astaro
  - well suited for appliances
- Gibralter
  - Debian version optimized as router/firewall
- EnGarde Linux
  - Secure Web hosting distribution
  - http://www.engardelinux.org/
- Immunix
  - package of tools to provide security bug tolerance
  - http://www.immunix.org/
- SmoothWall
  - based on VA Linux, turns PC into router/firewall
  - most suited for home/telecommuter
- Trinux
  - small, portable Linux distribution
- Trustix Secure Linux
  - hardened Linux distribution for servers
  - OpenSSL, OpenSSH, Apache with SSL, many others

➡ Service ?!

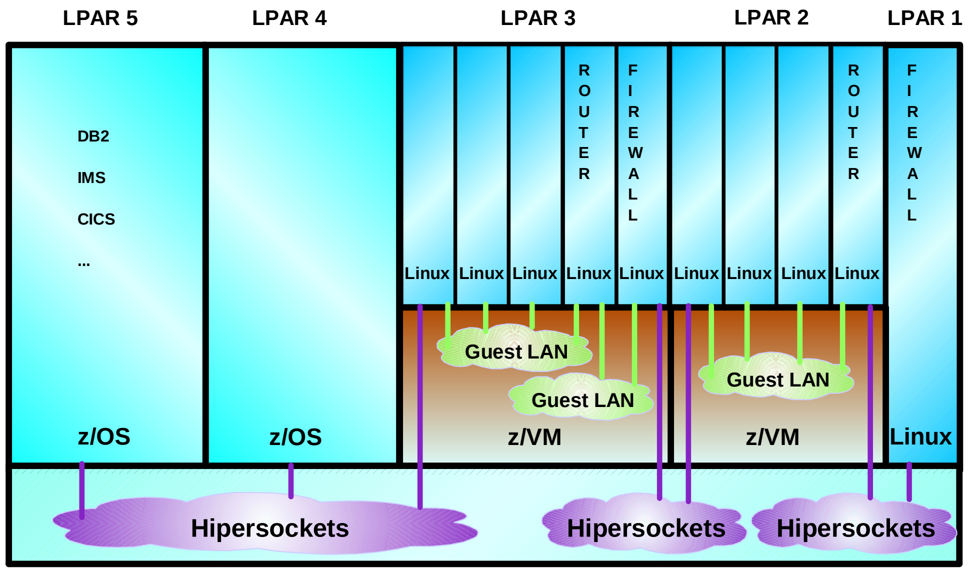
© 2004 IBM Corporation

Some IBM security products for Linux for zSeries

- Tivoli Acces Manager for operating systems
  - Provides base security infrastructure
- Tivoli WebSeal
  - Use as reverse proxy for access to back-end
- IBM Directory Server
  - LDAP server for Linux for zSeries

© 2004 IBM Corporation

Sample: Using a Combination of Hipersockets and Guest LANs for Internal Communication within a zSeries



LPAR 5
LPAR 4
LPAR 3
LPAR 2
LPAR 1

DB2
IMS
CICS
...
z/OS
z/OS

Linux Linux Linux Linux Linux Linux Linux Linux Linux
ROUTER
FIREWALL
ROUTER
FIREWALL
Guest LAN
Guest LAN
Guest LAN
z/VM
z/VM
Linux

Hipersockets
Hipersockets
Hipersockets

Internal Network:
Very hard to install
a Sniffer from outside

Note: External network connections are not included in this diagramm

© 2004 IBM Corporation

Security Certification Details (Summary)

For details see: http://www-1.ibm.com/servers/eserver/zseries/security/ccs_certification.html

Logical Partitioning Certification – IBM eServer™ zSeries® 900 (z900) and IBM eServer zSeries 800 (z800) are first to receive Common Criteria Certification at EAL5.
In the meantime also z990/z890 are also certified.

SUSE LINUX Certification – SUSE LINUX on zSeries SLES 8 has been certified at Controlled Access Protection Profile (CAPP) EAL3+.

Red Hat Enterprise Linux 3 achieved Controlled Access Protection Profile compliance under Common Criteria for Information Security Evaluation (CC), commonly referred to as CAPP/EAL3+.

z/OS® Certification – z/OS 1.6 with the RACF optional feature is in evaluation for Common Criteria certification at Controlled Access Protection Profile (CAPP) EAL3+ and Labeled Security Protection Profile (LSPP) EAL 3+ .

z/VM® Certification – IBM plans to obtain Common Criteria certification of z/VM, its premier virtualization technology, in 2004. It is anticipated that z/VM will be certified to conform to the requirements of the Labeled Security Protection Profile (LSPP) and the Controlled Access Protection Profile (CAPP), both at EAL3+. z/VM helps enable mainframe customers to run tens to hundreds of instances of the Linux operating system on a single zSeries server.

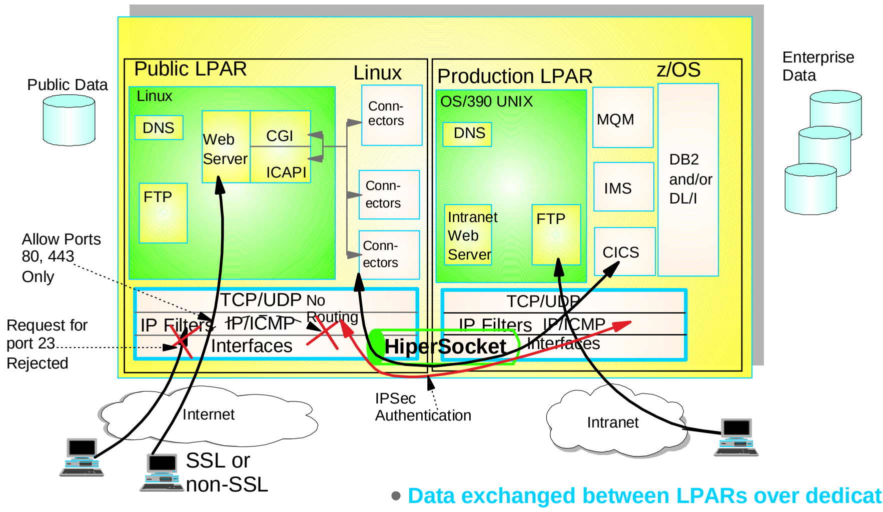
An Explanation of Evaluation Assurance Levels (EAL)

There are seven levels of evaluation designed to meet the variety of security levels required within government and commercial entities.

- EAL-1 examines the product and its documentation for conformity, establishing that the product does what its documentation claims.
- EAL-2 tests the structure of the product through an evaluation, which includes the product's design history and testing.
- EAL-3 evaluates a product in design stage, with independent verification of the developer's testing results, and evaluates the developer's checks for vulnerabilities, the development environmental controls, and the product's configuration management.
- EAL-4 is an even greater in-depth analysis of the development and implementation of the product and may require more significant security engineering costs.
- EALs 5-7 require even more formality in the design process and implementation, analysis of the product's ability to handle attacks and prevent covert channels, specifically for high-risk environments. In the United States, evaluation to EALs 5-7 must be done by the National Security Agency (NSA) for the U.S. Government.

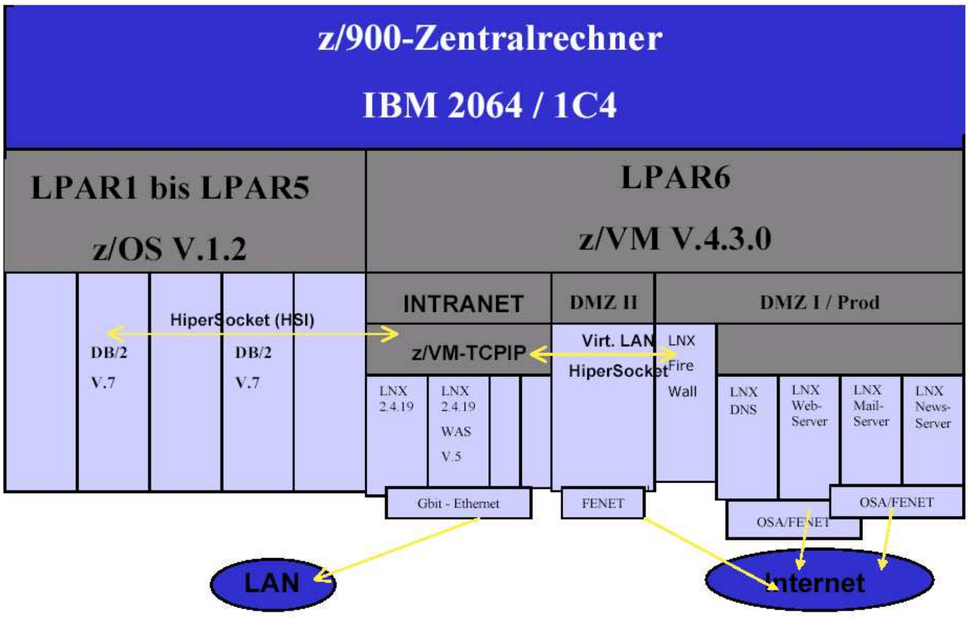
Public/Production Systems on a Single zSeries

HiperSockets used between LPARs for Inter-LPAR data traffic Linux - z/OS



- **Public System**
  - IP filters allow use of selected zSeries ports only
    - ex: Web (80, 443), Anon FTP
  - Routing Disabled
    - Connectors establish new connections to applications in Production LPAR
- **Data exchanged between LPARs over dedicated link**
  - HiperSocket
  - IPSec can optionally be used to authenticate traffic between systems
    - Prevents intranet host from spoofing connectors

A european Bank: DMZ and Production within one box



Customer's Responsibilities

- Define and deploy a security policy
- Examine audit trails periodically
- Apply recommended service
- Follow guidelines:
  - actions, applying restrictions, to complete system integrity.
- Data integrity must be managed by customer
  - e.g. No multi-write links by virtual servers unless running application that implements data integrity measures such as reserve/release

Summary:

Don't fear the pinguin

Thank You for listening.

Questions?

Section: Appendix

- Resources and Further Information

BACKGROUND LPAR Security ...

Common Criteria EAL 5 (semiformally designed and tested)

EAL5 permits a developer to gain maximum assurance from security engineering, based upon rigorous commercial development practices, supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialized techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require rigorous development approach without incurring unreasonable costs attributable to specialist security techniques.

An EAL5 evaluation provides an analysis that includes all of the implementation. Assurance is supplemented by a formal model and a semiformal presentation of the functional specification and high-level design, and a semiformal demonstration of correspondence. The search for vulnerabilities must ensure resistance to attackers with a moderate attach potential. Covert channel analysis and design are also required.

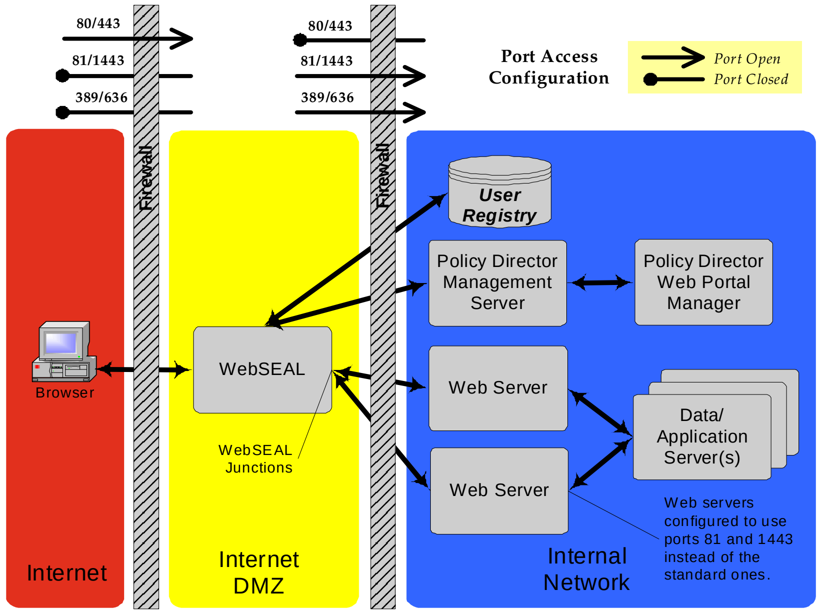
PR/SM certification ITSEC E4 - EAL4

Information Technology Security Evaluation Criteria, evaluation level E4 certifies that PR/SM can separate and isolate partitions as if they were running on physically separate systems. This includes topics such as the following:

- Identification and authentication
  - PR/SM will associate a unique identifier with each logical partition in the current configuration.
  - Each LPAR is uniquely identified, based on IOCDS definitions.
  - The identifier is used to mediate access control.
- Audit and accountability
  - All security relevant events are recorded in an audit log.
  - The audit log is protected from unauthorized deletions or modifications.
  - Applications in LPARs cannot read the audit log.
- Access control
  - LPAR security controls define a partition's access to IOCDSs, performance data, crypto, and reconfigurable channels.
  - Access to control units and devices on shared channels can be restricted.
  - Dedicated channels, storage, and CPs are never shared.
  - PR/SM will prevent the transfer of a message between a logical partition and any resource not explicitly allocated to it.
- Object reuse
  - Storage will be cleared prior to allocation or re-allocation.
  - All information in physical processors or coprocessors will be reset before dispatching the processor to a new logical partition. Non-shared channel paths and attached I/O devices will be reset prior to allocation to a LPAR

Example TAM WebSeal

An Example Policy Director WebSEAL Architecture


80/443
81/1443
389/636
80/443
81/1443
389/636
Port Access Configuration
Port Open
Port Closed
Firewall
Firewall
User Registry
Policy Director Management Server
Policy Director Web Portal Manager
Browser
WebSEAL
WebSEAL Junctions
Web Server
Web Server
Data/ Application Server(s)
Web servers configured to use ports 81 and 1443 instead of the standard ones.
Internet
Internet DMZ
Internal Network

Is Open Source Secure? . . .

- European Parliament considers Open Source encryption software over proprietary because "this is the only way of guaranteeing that no backdoors are built into programs". (German Rep. Gerhard Schmid)
- The German Military's website is Linux http://www.bundeswehr.de
- German embassies are connected to the government via VPN based on Linux systems.

Is Open Source Secure? . . .

- Open Source community continually looking for hacker holes
- Holes exposed before installed on your box
- No more "security through obscurity" base for proprietary systems
- Most security defects in Linux fixed within 48 hours

Where to Go For Linux for zSeries Info

- www-1.ibm.com/servers/eserver/zseries/os/linux
- www.linux.org/LDP/Is_quickref/QuickRefCard.pdf
- www.sse.ie/securitynews.html
- www.tripwire.org/poster/tripwire_exploit.pdf
- securityfocus.com/linux
- www.linuxsecurity.com/docs
- www.debian.org/security
- www.vm.ibm.com/linux
- linas.org/linux/i370.html
- oss.software.ibm.com/developerworks/opensource/linux390/index.html
- linuxvm.org
- ltc.linux.ibm.com
- linux.nl.ibm.com/ibmlinux/index.shtml
- www.securityfocus.com
- http://www.ibm.com/servers/eserver/zseries/library/techpapers/gm130145.html
- **http://www-124.ibm.com/developer/opensource/linux/papers/security/Linux-Security-IBM-White-Paper.pdf**
- http://www-1.ibm.com/linux/Securing_Linux_Servers_xSP_external.pdf

- see whitepapers for complete list ...

Where to Go For Linux for zSeries Info

- G5 and G6 ITSEC E4 document:
  http://www.bsi.de/zertifiz/zert/reporte/0142.pdf
  http://www.bsi.de/zertifiz/zert/reporte/0157.pdf
- zSeries z900 and z990 EAL4 and EAL5 documents:
  http://www.bsi.bund.de/zertifiz/zert/reporte/0178a.pdf
  http://www.bsi.bund.de/zertifiz/zert/reporte/0179a.pdf
  http://www.bsi.bund.de/zertifiz/zert/reporte/0239a.pdf
- latest PR/SM info:
  http://www-3.ibm.com/security/standards/st_evaluations.shtml

- Alan Altmark, Cliff Laking, z/VM Security and Integrity. Technical Paper:
  http://www.ibm.com/servers/eserver/zseries/library/techpapers/gm130145.html

- **Linux on IBM zSeries and S/390: Securing Linux for zSeries with a Central z/OS LDAP Server (RACF) Published: June, 21, 2002**
  More details are available at:
  http://www.redbooks.ibm.com/redpapers/abstracts/redp0221.html
- **Advanced LDAP User Authentication: Limiting Access to Linux Systems Using the Host Attribute.**
  http://publib-b.boulder.ibm.com/Redbooks.nsf/RedpaperAbstracts/redp3863.html?Open
- **ITSO Redbooks: zSeries Crypto Guide Update, SG24-6870**
- **ITSO Redbooks: Linux on IBM eServer zSeries and S/390: Best Security Practices, SG24-7023**