IBM System z –
Security Hub for the Enterprise

April, 2008

Mary E. Moore
STG – Enterprise Systems
Security Offerings Manager

IBM Systems

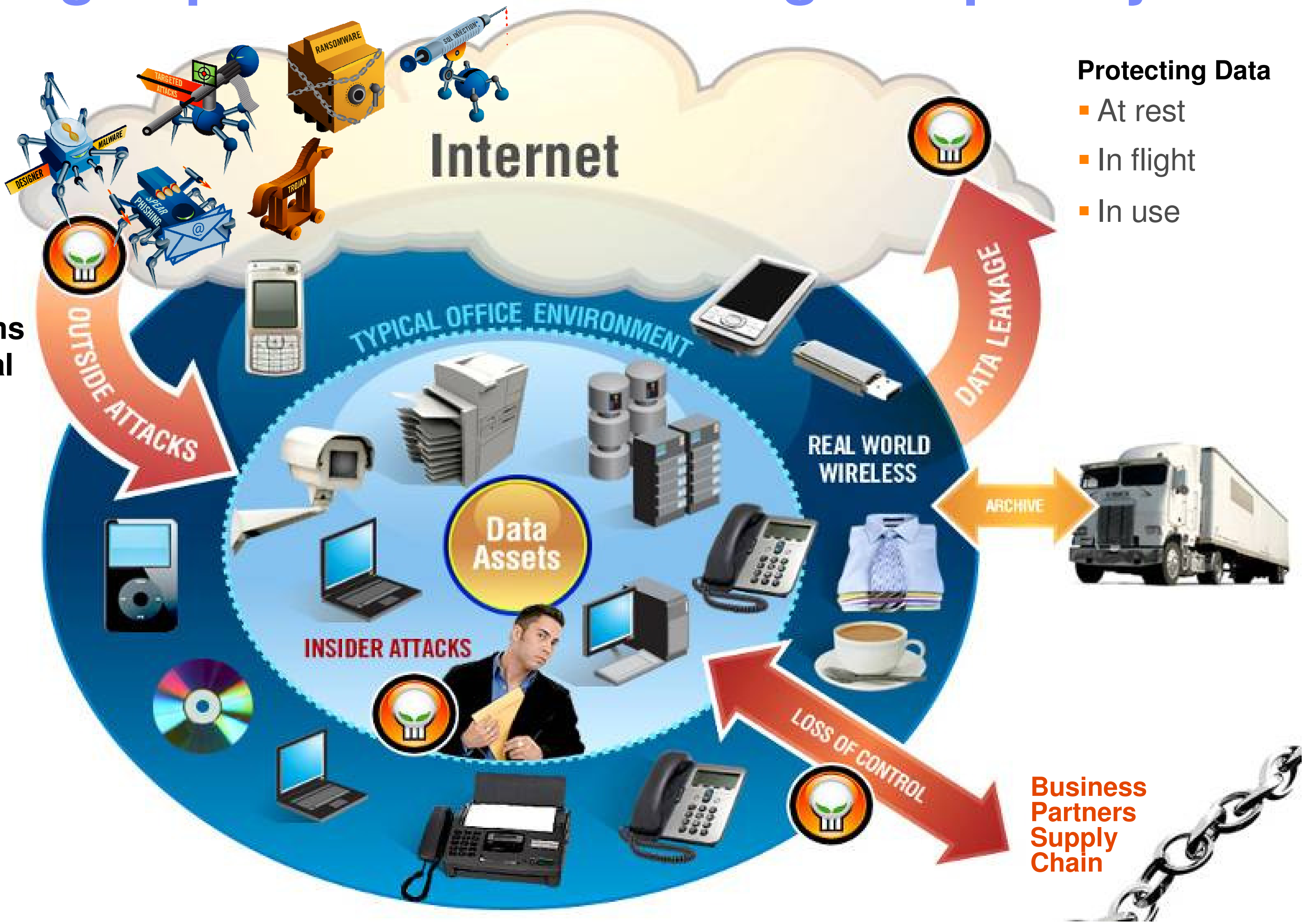
AGENDA

- Enterprise Security Requirements
- System z - Security by Design
- Encryption Solutions

Information security –
Increasing importance – Increasing complexity

Protecting Systems Against Intentional Attacks

- Viruses
- Malware
- Intrusions

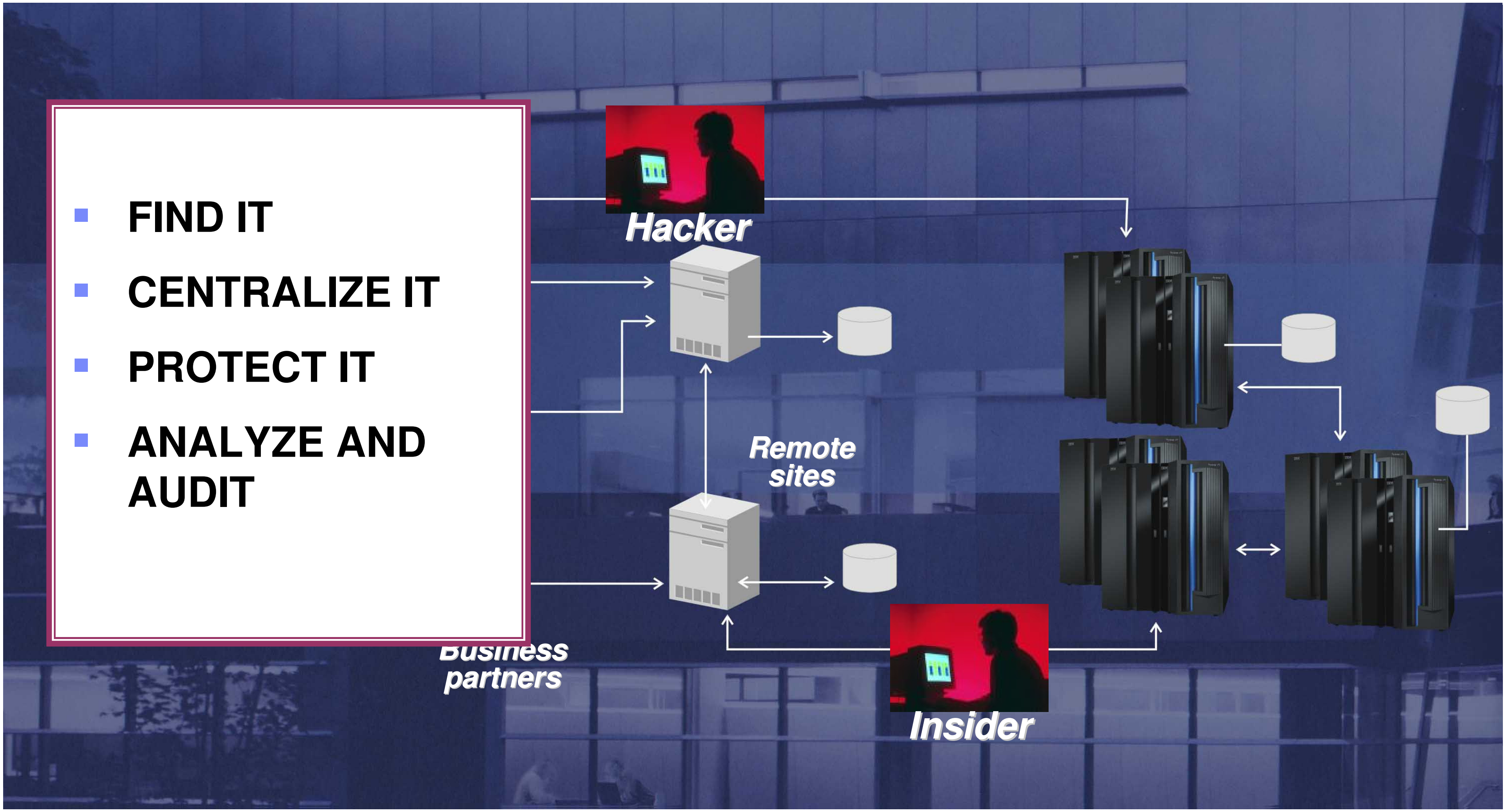


Business Partners Supply Chain

Protecting Data

- At rest
- In flight
- In use

Protecting Sensitive Data



- FIND IT
- CENTRALIZE IT
- PROTECT IT
- ANALYZE AND AUDIT

Forrester Survey – *“Please rank which operating system category you feel is inherently more secure?”*

April 10, 2007
Operating System Vendors: Do More To Help Users
With Server Security
by Jennifer Albornoz Mulligan

	Rank	
More secure	1	Mainframe
	2	Unix
	3	Macintosh
	4	Linux
Less secure	5	Windows

Figure 3 - Security Decision-Makers’ Opinions On OSes’ Security

Analyst Bob Djurdjevic, President of Annex Research.

“If IBM has a shortcoming, it’s that it hasn’t bragged enough about its security capabilities.

Their home turf is the mainframe. That’s the Fort Knox of IT today, as it has been the last several decades. That’s the most secure environment you will ever find.”

System z as the security hub for the enterprise

Leverage the mainframe security policies and processes that have been developed over many years in your enterprise

- Security-rich holistic design to help protect system from malware, viruses, and insider threats
- Granular access controls integrated across the platform
- Network security features to help address outside threats
- Encryption solutions to help secure data from theft or compromise
- Tivoli tools allowing you to address compliance needs with more confidence

The industry’s most securable platform!

And a few more reasons!

- High availability
- Disaster recovery
- Scale / Performance
- Consolidation / Virtualization
- Systems management tools
- Robust middleware
- ....

System z Architecture:
Security Built In By Design

Security is only meaningful in the presence of system integrity

- Integrity prevents bypass of security controls
- Audit trail confirms conformance

- Integrity through Hardware and Software integration
  - Storage protect keys
  - Virtual storage management
  - User isolation

Allows customers to confidently place critical workloads on single z/OS image

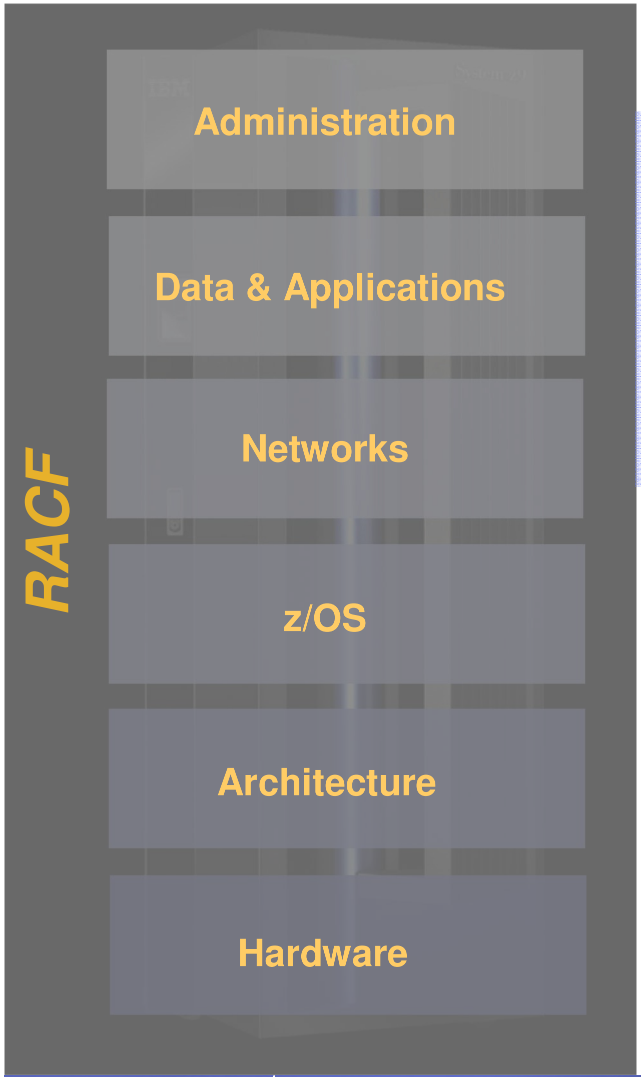
and hundreds of Linux images in a virtual partition

Can help prevent intrusion from malware, viruses and worms

Proven over 40 years of secured operations!

The backbone of mainframe security
Resource Access Control Facility (RACF)

Authentication
Authorization
Administration
Auditing



RACF

Administration

Data & Applications

Networks

z/OS

Architecture

Hardware

Enables application and database security without modifying applications

Can reduce security complexity and expense:

- Central security process that is easy to apply to new workloads or as user base increases
- Tracks activity to address audit and compliance requirements

- Integration with distributed system security domain
- Checking for “Best Practices” with z/OS HealthChecker
- Serving mainframe enterprises for over 30 years

z/OS System Integrity Statement

Designed to help protect your system, data, transactions, and applications from accidental or malicious modification

- **System integrity is the inability to bypass the lock on system resources**
- IBM will always take action to resolve if a case is found where the above can be circumvented

z/OS integrity statement and the Common Criteria certifications can be helpful proof points in addressing compliance requirements.

ibm.com/servers/eserver/zseries/zos/racf/zos_integrity_statement.html

Network security –
z/OS Intrusion Detection Services

Detects events such as:

- Scans Attacks Flooding

Provides Defenses on z/OS

- Packet discard
- Limited # connections

Reports:

- Logging - Console
- Packet trace
- Notifications

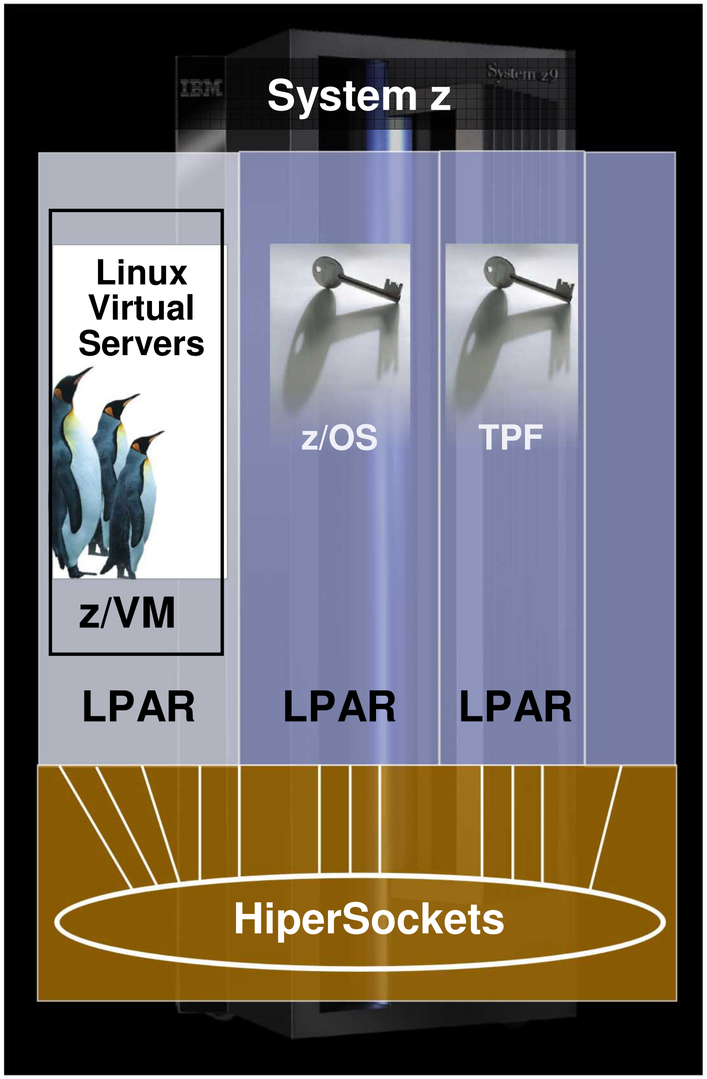
A component of z/OS
Integrated in the IP stack

- Compliments network based IDS
- Enables further detection of attacks and application of defensive mechanisms
- Can be extended with Netview IDS

- Evaluates many known attacks
- Can evaluate unknown attacks
- Detects problems in real-time
- Policy based
- With z/OS 1.8, no longer requires LDAP

Helps protect against network attacks
Can evaluate IPsec inbound data after decryption

Security through virtualization



- **Virtual servers on a single mainframe:**
- **Logical Partitions (LPAR)**
  - Uses hardware isolation architecture to enforce LPAR isolation
  - Only server with EAL5 Common Criteria certification
- **z/VM**
  - Using the same hardware isolation instruction
  - The inability of a guest to circumvent system security features and access controls
  - IBM Integrity Statement for z/VM

- **Virtual network in the server: HiperSockets**
  - Provides an integrated TCP/IP network through system memory
  - Highly secure connection – no external network exposed

The Pluses of the Mainframe for PCI Compliance
An auditor's view

- The mainframe using any of the three standard security tools is viewed by the PCI Co and the Card Companies as **inherently more secure than mid tier devices**
- It is very difficult to take data off the mainframe without an SMF record being cut to **allow for full identification of the incident**
- Mainframes have been accepted by VISA and the Acquirer Banks **allowing the application and the data base to be in the same physical device**
- Mainframes can have all the PCI data isolated to a single LPAR without violating the requirements
- Encryption tools are available for the Mainframe

Howard Glavin,
PCI Auditor
IBM Internet Security Systems

Mainframe Differentiation
The view of an “ethical hacker”

Ray Evans MBCS CITP CISSP

z/OS: Designed for Reliability and Security

- Buffer Overflow - not a real problem on z/OS
  - Address spaces and storage keys prevent applications from storing into someone else's storage
- RACF protects the complete system
  - All access to the system requires authentication with RACF
  - Auditing to SMF, not log files
- Daemons are protected against modification and misuse
  - Security critical programs must run in a controlled environment
- TCP/IP stacks, ports and network addresses can be RACF protected
  - Can prevent rogue programs from taking over ports
  - Protects system and network from insider attacks, modification and misuse

Payment Card Industry Compliance– How System z can help

Build & Maintain a Secure Network

System z integrity features

z/OS Network Policy Agent

z/OS Intrusion Detection Services

HiperSockets

Linux on z as a DMZ

Protect Cardholder Data

Encryption Infrastructure

Database Encryption Tools

Network encryption:

SSL/TLS, IPSec, OpenSSH

Tape encryption

Maintain Vulnerability Mgmt Program

z/OS Network Policy Agent

z/OS Intrusion Detection Services

Tivoli Compliance Insight Manager

IBM Internet Security Solutions

Implement Strong Control Measures

System z integrity features

RACF

Certificate Authority

Tivoli zSecure

Tivoli Identity Manager

Monitor & Test Networks

z/OS Healthchecker

Tivoli zSecure

Tivoli NetView

IBM Services:
Penetration Testing

Maintain Information Security Policy

z/OS Network Policy Agent

EAL & FIPS Certifications

IBM Services:
Internet Security Solutions
Security & Privacy Consulting

*It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.

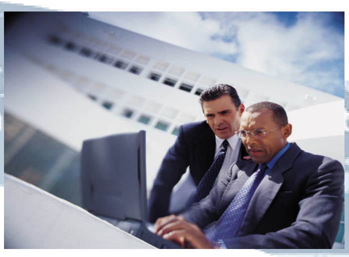
The Power of Mainframe Encryption

Helping to reduce risk

Privacy over the **Internet** to customers and partners

Highly secure transmissions to

- **printers**
- **ATMs**
- **POS**
- **network devices**

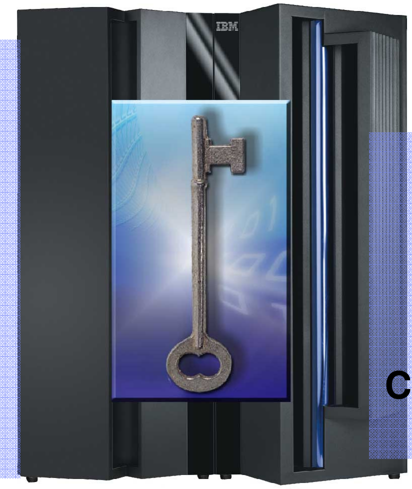


Data in DB2 for z/OS

Data transferred on **tape**

Customer objectives:

- **Only intended party is allowed to decrypt**
- **Availability of the keys and decryption services when you need them**



Encryption acceleration

Secure-key processing

Centralized key storage

Archived data

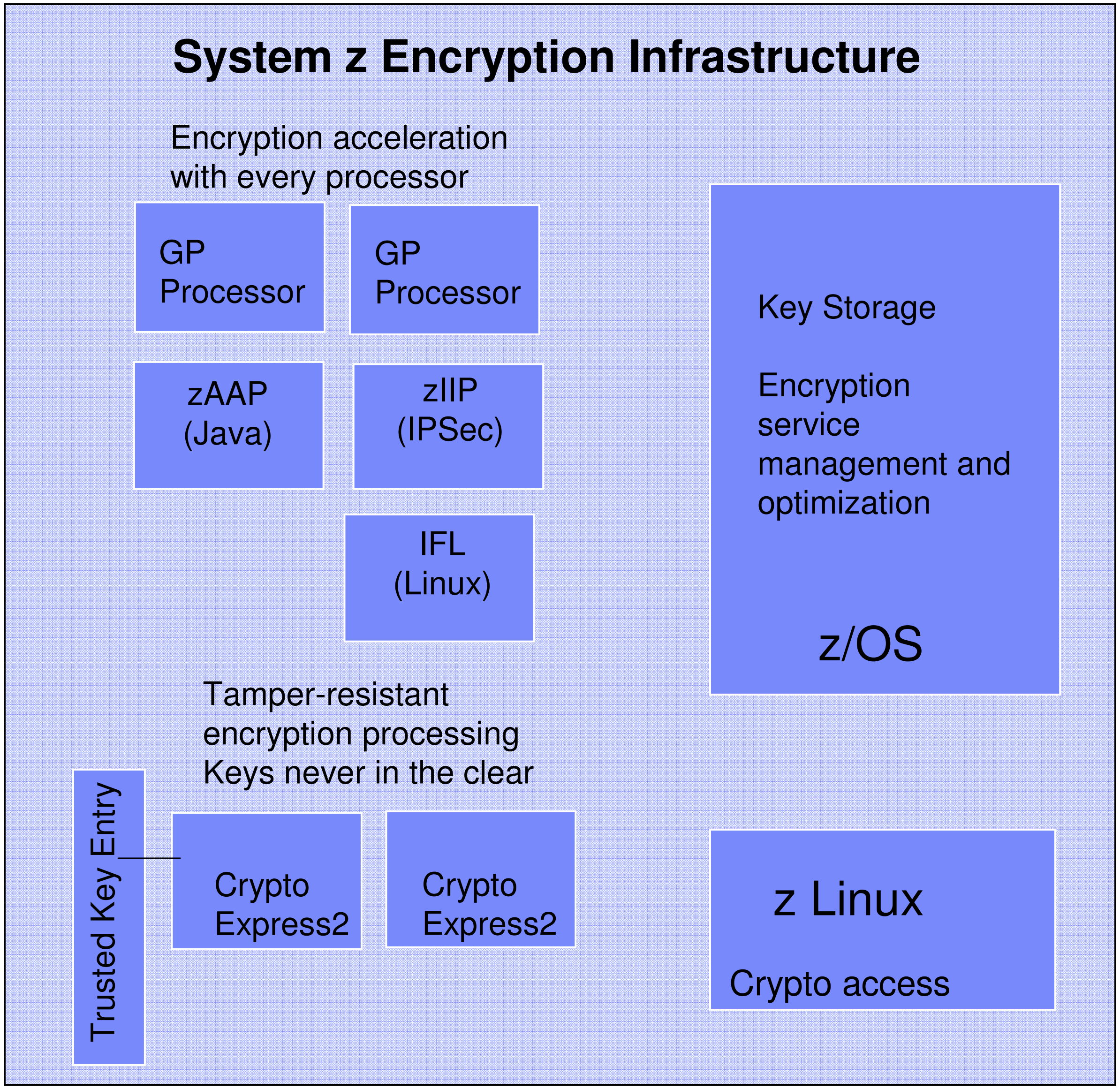
IBM PRESS RELEASE Nov. 1, 2007
IBM Acts to Transform Risk Management for Businesses

“Whether your security initiative is part of compliance adherence or business continuity, one important step is to ensure that data integrity mechanisms are in place,"

said *Debbie Wheeler, Chief Information Security Office at Fifth Third Bank*.

"We're proud to leverage IBM's 30 years of mainframe encryption technology to drive stronger customer confidence. Fifth Third Bank has formed an <u>internal team focused on proper and effective use of cryptographic controls</u>. That team is working closely with IBM to ensure that our emerging needs are understood, as well as developing strategic partnerships between IBM and other vendors to maximize the value of our existing and future investments."

Encryption Solutions



System z Encryption Infrastructure

Encryption acceleration with every processor

GP Processor

GP Processor

zAAP (Java)

zIIP (IPSec)

IFL (Linux)

Key Storage

Encryption service management and optimization

z/OS

Tamper-resistant encryption processing Keys never in the clear

Trusted Key Entry

Crypto Express2

Crypto Express2

z Linux

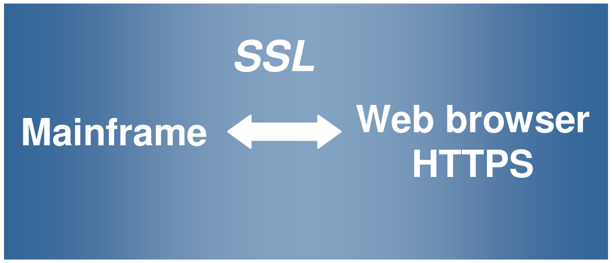
Crypto access

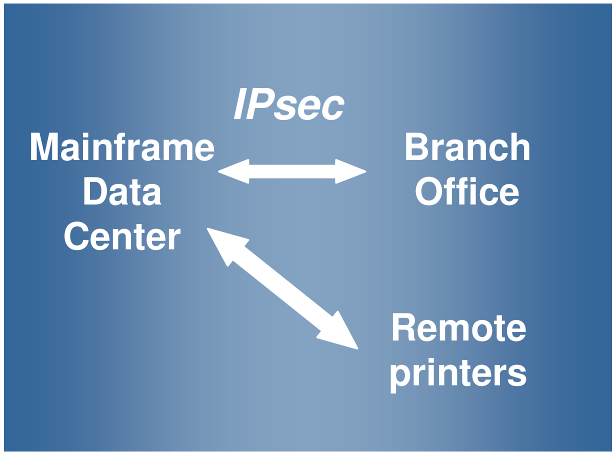
Encryption Solutions

- Internet Access
- Tape
- Future Disk Encryption*
- Database
- Web applications
- Java Applications
- POS/ATM
- Digital Certificate Hosting

* IBM statement of direction

Network security – encryption over the Internet





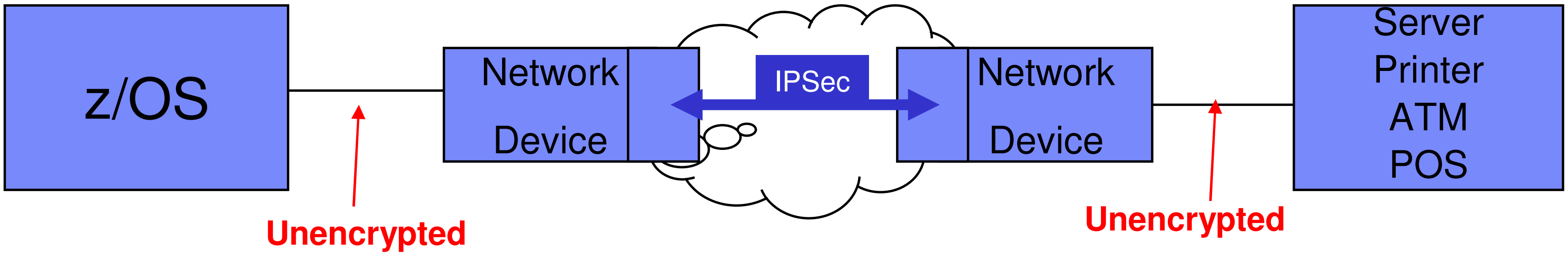
- **File transmission encryption**
  - Multiple options including FTP, OpenSSH, SSL
  - Encryption Facility for z/OS
- **Application-based encryption (with SSL and TLS)**
  - Encryption acceleration in the System z server
- **End-to-end network encryption (with IPsec)**
  - Allows secure tunnel (Virtual Private Network)
  - **More compelling on System z with support for zIIP specialty processor**

Simpler and consistent configuration with
z/OS Network Security Configuration Assistant

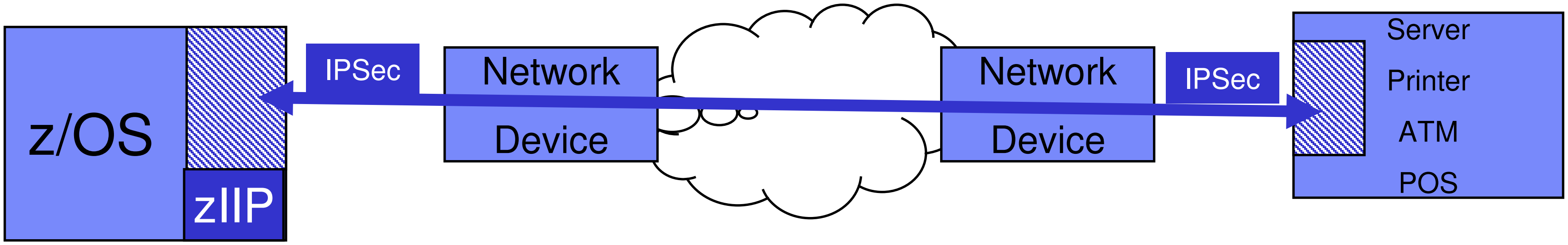
End-to-end network encryption

Growing requirement for companies that outsource some part of their network

zIIP specialty engine support helps reduce the cost of adding IPSec protection



Encryption in network devices

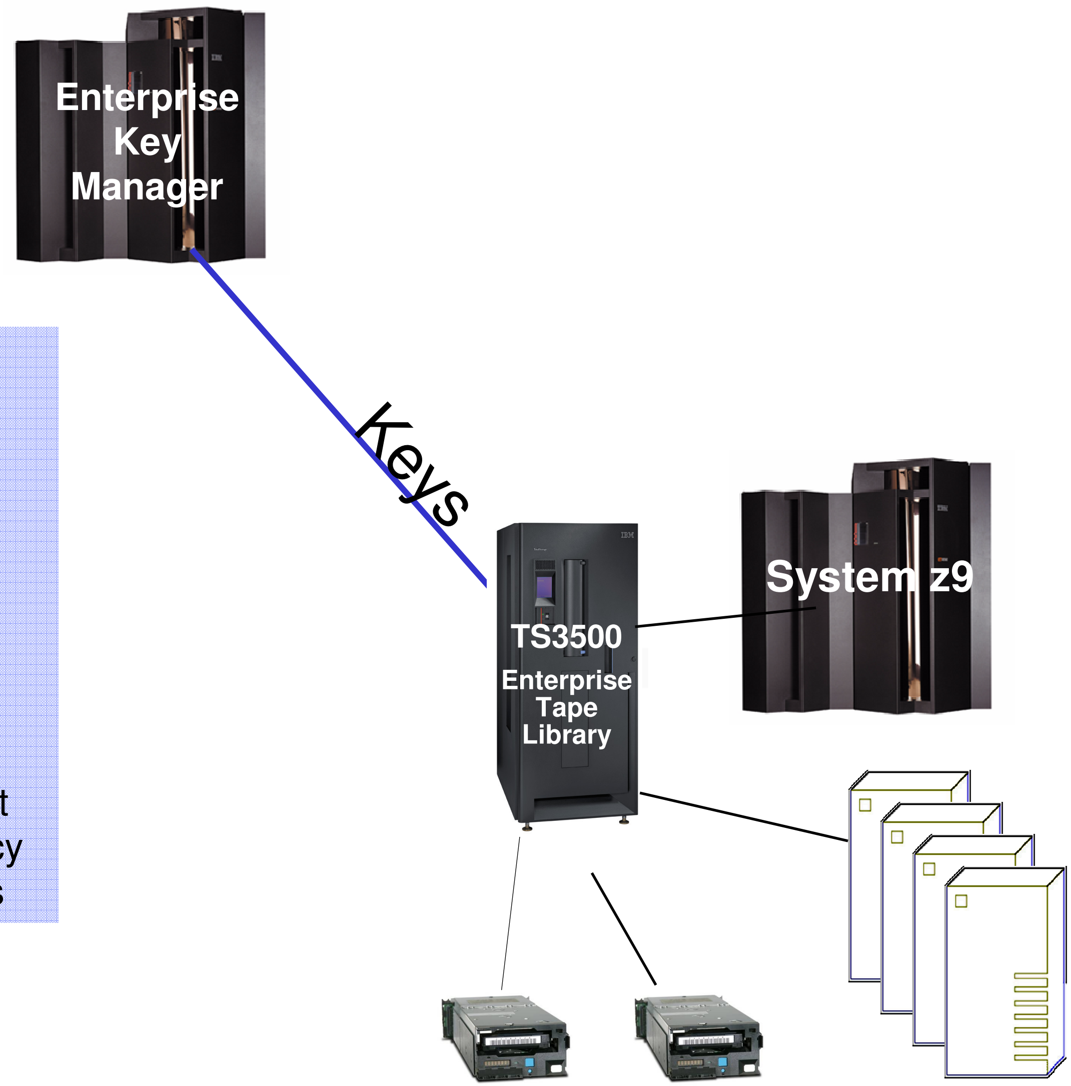


End-to-end encryption

Tape encryption and enterprise key management

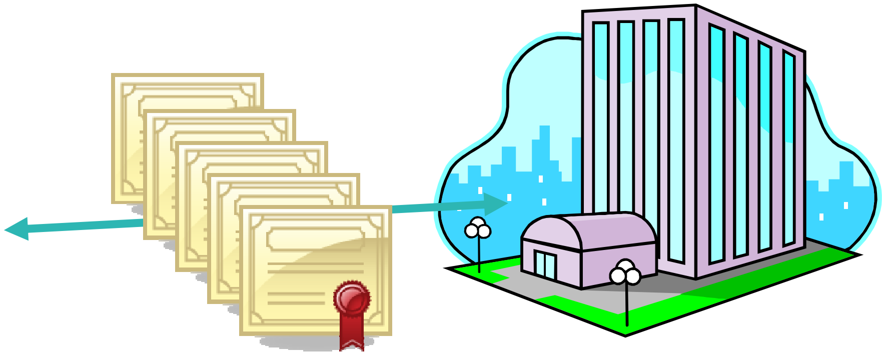
Encryption Key Manager using System z features:

- Protect private keys
  - Secure-key processing with CrytpoExpress2
- Manage key stores with mainframe qualities of service
  - ICSF key store management
  - Parallel sysplex for resiliency
  - Disaster recovery processes



Securing IT traffic with encryption
Establishing trusted connections with Digital Certificates

Digital Certificates
- •Authenticates a user, device, server or application
- •Provides a secure exchange of "public" encryption keys

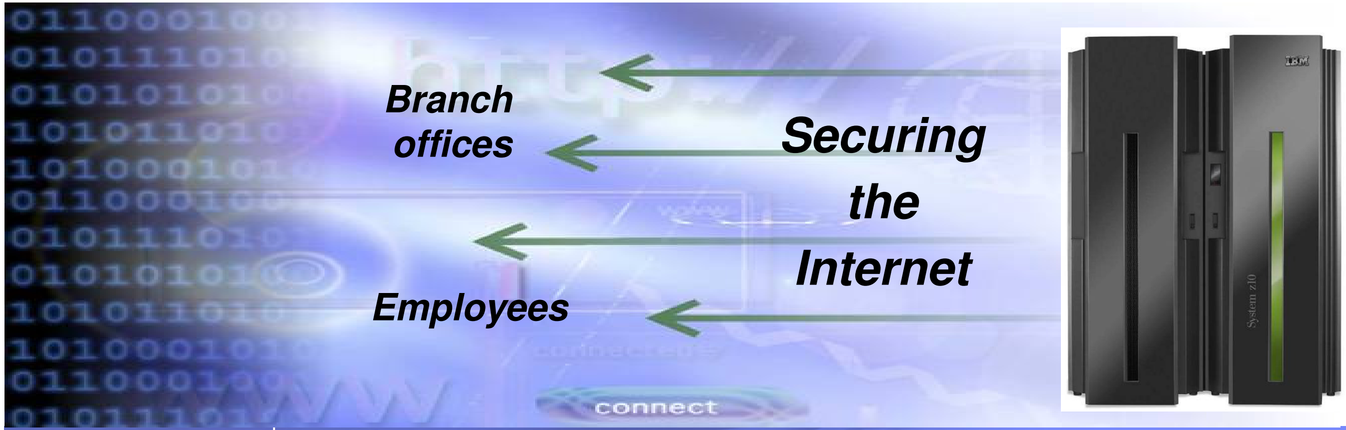


- Online shopping (exchange credit card data)
- Smart cards (Digital Certificate hosted on card)
  - Drivers licenses, passports, employee identification,
- Secure VPNs (virtual private networks) using SSL or IPSec standards
- Digital document signing (non-repudiation)
- Program signing (non-repudiation)
- Tape encryption and future disk encryption (enterprise encryption key management)

Banco do Brasil saves over $16 M a year!
System z as a Certificate Authority

Establishes a more secure enterprise network

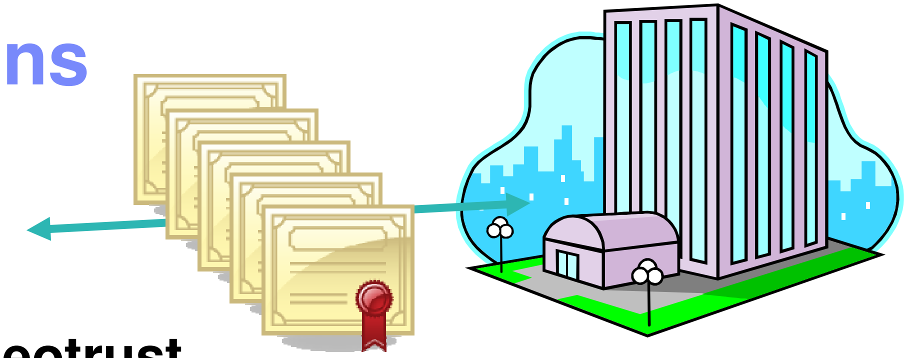
- Outsourced network management
- Created a VPN (Virtual Private Network) between each device in the network
- Using z/OS PKI Services to host digital certificates



BANCO DO BRASIL

- **30 million accounts**
- **4,000 locations**
- **20 million transactions per day**
- **Hosting certificates for all network devices at branch offices**

Certificate Authority Options



- **Third parties – Verisign, Entrust, Geotrust ...**
  - **Annual cost of certificates**
    - **$5 - $995 per certificate**

System z differentiation:
Save $10Ks - $M's
No per-issue certificate cost
Relatively low mips to drive millions of certificates

- **In-house hosting products**
  - Microsoft
    - ***Microsoft PKI for Windows Server***
  - System z - z/OS *PKI Services*
    - No charge feature of z/OS

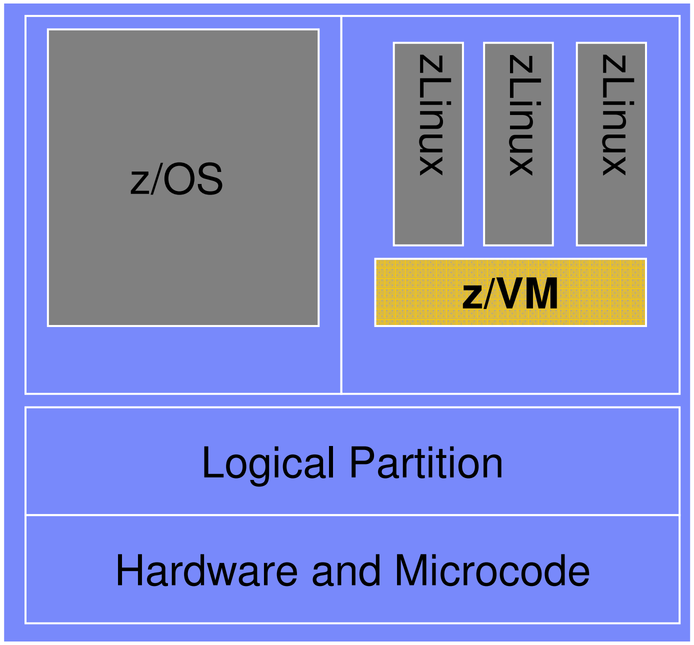
System z differentiation:
Availability and resiliency
Scale
Security and auditing
Crypto Express2 to secure private keys

Certifications on System z

z/OS

- **Common Criteria EAL4+**
  - with CAPP and LSPP
  - z/OS 1.7 + RACF
  - z/OS 1.8 + RACF

- **IdenTrust™ certification** for z/OS as a Digital Certificate Authority (PKI Services)



z/VM

- **Common Criteria** EAL3+
  - with CAPP and LSPP
  - **z/VM 5.1 + RACF**
  - **Under evaluation for EAL4+**

Linux on System z

- **Common Criteria**
  - **SUSE LES9 certified at EAL3+ with CAPP**
  - **Red Hat EL4 EAL4+ with CAPP and LSPP**

Virtualization

- Common Criteria EAL5 for Logical partitions

Cryptography

- **FIPS 140-2 level 4** for Crypto Express 2

System z as the security hub for the enterprise

Leverage the mainframe security policies and processes that have been developed over many years in your enterprise

- Security-rich holistic design to help protect system from malware, viruses, and insider threats
- Granular access controls integrated across the platform
- Network security features to help address outside threats
- Encryption solutions to help secure data from theft or compromise
- Tivoli tools allowing you to address compliance needs with more confidence

The industry's most securable platform!