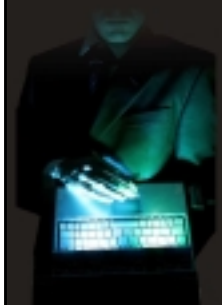


A Fresh Look at the Mainframe

The New Face of Mainframe Security

The spread of security threats affects everyone



"The average loss to the financial industry is approximately \$17,000 per compromised identity. An identity thief can net \$17,000 per victim.. By comparison, the average bank robbery nets \$3,500..."
www.idtheftcenter.org

MasterCard says 40 million files are put at risk.
New York Times, May 18, 2005

At least 130 reported breaches have exposed more than 55 million Americans to potential ID theft this year.

An adviser for the Treasury Department's Office of Technical Assistance estimates cyber crime proceeds in 2004 were \$105 billion, greater than those of illegal drug sales.

Government agencies and companies in the U.K. are under attack by a concerted series of Trojan horses out to steal information.
TechWebNews, June 16, 2005

At least a million machines are under the control of hackers worldwide.
ZDNET March 16, 2005

The number of bank accounts accessed illegally by a New Jersey cybercrime ring has grown to 676,000, according to police investigators.
ComputerWorld, May 20, 2005

ODI's Security Perspective

We need stronger security to protect our online business applications...



**On Demand Insurance
CEO**

IBM mainframes offer the best security.



IBM

- Regulatory compliance issues raise security visibility; executives are personally accountable
- New online business solutions will require a security environment that actively protects against intrusions
- We need additional protection capabilities for confidential data which will be shared with business partners

08 - The New Face of Mainframe Security v3.9.ppt

3

System z Hardware and Architecture: Powerful Security Built In By Design

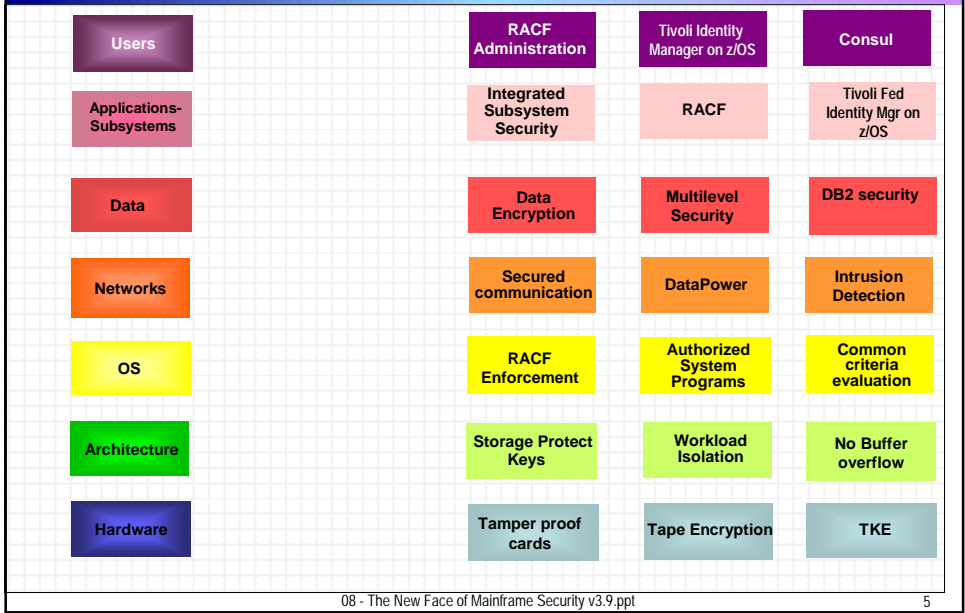
- Enforced Isolation
 - ▶ Each user has its own unique address space
 - ▶ LPAR separation ensures integrity
 - ▶ Supervisor state or system programs protected
- Authorized program facility (APF)
 - ▶ Executables are only accessible to authorized users
- Storage Protection Keys
 - ▶ Controls access to protected storage
 - ▶ Cross memory services prevent unauthorized access to other users' data
- Access Control Environment Element
 - ▶ z/OS security control block is protected by z/OS
- The US Government Common Criteria program certifies IBM software at the highest levels
 - ▶ z/OS and RACF at a high level of certification (EAL4+)

**Proven secure by 40
years of secured
operations!**

08 - The New Face of Mainframe Security v3.9.ppt

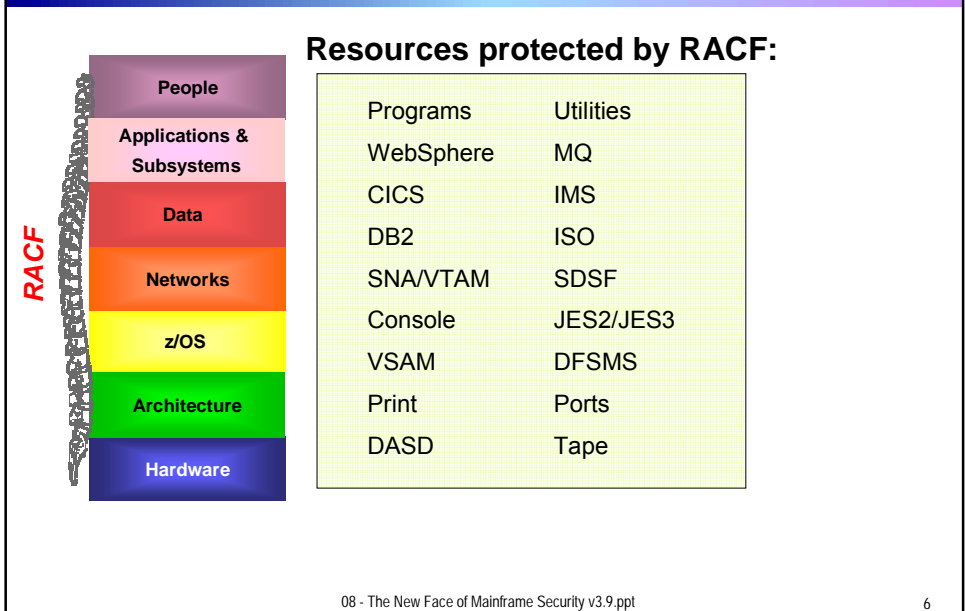
4

Integrated Security Throughout the Stack Leverages System z



The Backbone of System z Security: RACF

Integrated Security Throughout the Stack



RACF Provides Comprehensive Security for System z and the Extended Enterprise

- Resource Access Control Facility (RACF) part of the Security Server for z/OS

- RACF controls access to System z resources

- What does RACF do?

- ▶ Identifies and authenticates users
- ▶ Matches security classification of users and resources to authorize access
- ▶ Identifies users optionally via digital certificates
- ▶ Logs and reports access attempts
- ▶ With remote sharing, allows administrators to manage several systems centrally



- It is impossible to bypass RACF because SAF interface is enforced by z/OS
 - ▶ System Authorization Facility

08 - The New Face of Mainframe Security v3.9.ppt

7

Network Security

Security features of System z Communications Server in z/OS

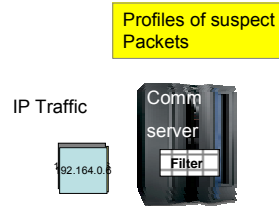
- Intrusion Detection Services
 - ▶ Detects, records, and defends against scans, stack attacks, flooding
- Protect system integrity
 - ▶ Protects against Denial of Service attacks
 - ▶ IP packet filtering eliminates malicious traffic
 - ▶ Intruders cannot access system log
- Protect Network resources
 - ▶ Protect users from sending to certain TCP/IP addresses, ports, FTP, network commands, socket options
- Protects network data
 - ▶ Encryption with Triple DES
 - ▶ Uses crypto hardware assist
- Transparent Application Security
 - ▶ Enable stronger network security without changing application code (AT-TLS features)
- Network security protocols supported
 - ▶ Secure Sockets Layer SSL
 - ▶ Kerberos support
 - ▶ Secure Domain Name Server (DNS)
 - ▶ SNMPv3

08 - The New Face of Mainframe Security v3.9.ppt

8

System z Communications Server Provides Intrusion Defense

- Defines profiles of suspected IP traffic
- Monitors incoming packets
- Provides a built in alternative to firewalls
- Can evaluate encrypted data *after* decryption
- Defends against malicious attacks real time:
 - ▶ Scans, Attacks, Flooding
- Filters inbound and outbound packets according to rules:
 - ▶ Packet information, IP address, port, protocol, time
- Proactive– active defense against intrusions
 - ▶ Packet discard, Limits number of connections, Logs errors
- Reporting:
 - ▶ Logs to NetView for a single source of network information



08 - The New Face of Mainframe Security v3.9.ppt

9

Mainframe Hardware Accelerates Encryption

Cryptography for System z

- CP Assist for Cryptographic Functions (CPACF)
 - One CPACF chip per processor, scales out
 - Supports DES/TDES and SHA-256
 - Provides AES support in hardware
- Crypto Express2 (CEX2)
 - Tamper evident packaging
 - Configurable either as a Coprocessor or Accelerator
 - Very fast SSL processing
 - Available with System z9 EC, z990 and z890
- TKE Workstation
 - Highly secure remote key entry
 - Runs on embedded operating system
 - Smart Card reader

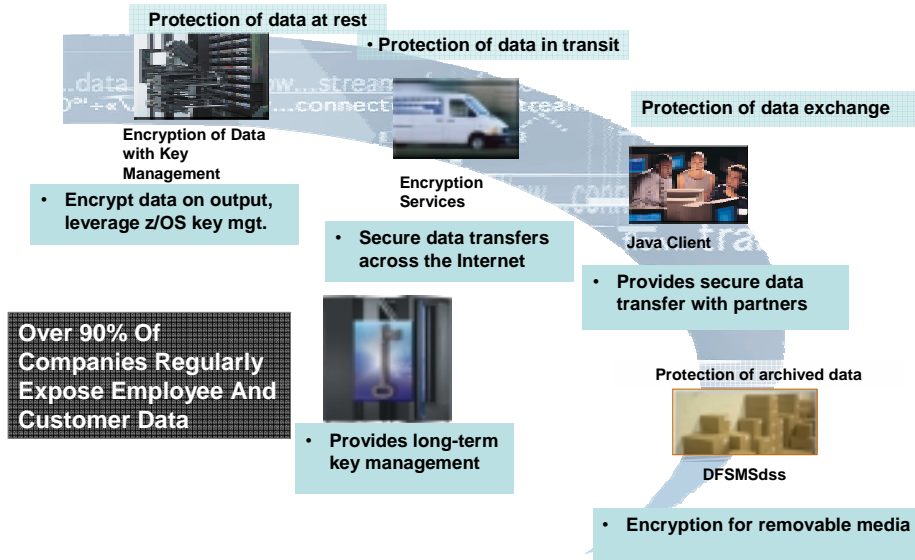
08 - The New Face of Mainframe Security v3.9.ppt

10

Secure "Smart Card" Solution Fights Fraud and Reduces Costs

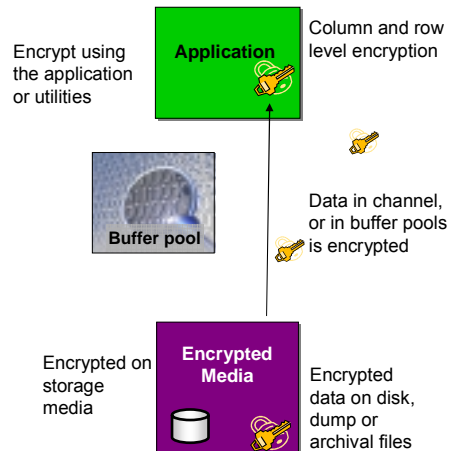
- One of the largest banks in Latin America
 - ▶ Approximately 3,000 branches, 20,400 automated teller machines and 42,200 employees
 - ▶ 15M checking accounts, 9M savings accounts, 6M credit cards
- **Situation:**
 - ▶ To meet efficiency objectives and ensure the security of its 12 million issued debit cards, the Bank replaced its regular cards with security chip-enabled smart cards.
 - ▶ Need improved security to fight fraud
- **Problem:**
 - ▶ Performance bottleneck with Thales e-Transactions security servers (which process "smart cards")
- **Solution:**
 - ▶ Leverage superior mainframe security, eliminate separate security server and migrate smart card solution to the mainframe
 - ▶ All core business systems run on mainframes
 - ▶ System z reliability and technical support also key factors in this decision
 - ▶ Better price performance
 - ▶ Install mainframe PCI Cryptographic Coprocessor cards (PCICC)
 - ▶ Encryption keys are generated and stored on PCICC cards and used for smart card authentication, blocking and password change
 - ▶ Use IBM z/OS V1.6 security APIs
- **Result:** **Reduced fraud from stronger smart card security, reduced costs, PLUS increased stability, efficiency, and faster processing**

Data Protection Throughout the Life Cycle



Additional Information Protection for DB2

- IT shops must conform with privacy regulations.
- Resources and skills are scarce. Security solutions must be efficient and easy to implement.
- DB2 v8 + also offers encryption options:
 - ▶ Column level encryption
 - Enabled by the application
 - ▶ Row level encryption
 - IBM Encryption Tool for DB2
- Encrypt DB2 System Resources helps prevent unauthorized access and use
 - ▶ Table and Index encryption
 - ▶ Image copies encrypted
 - ▶ Logs/archives encrypted
- Exploit System z Crypto Express2 hardware

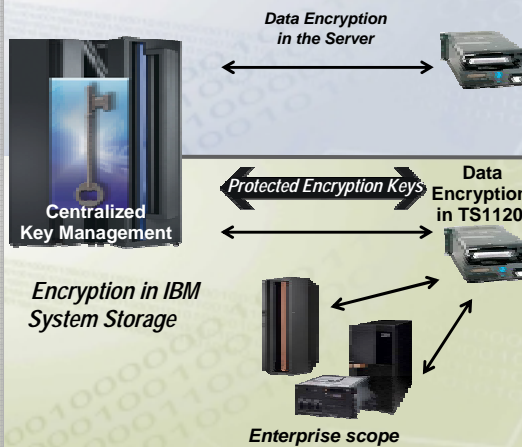


New Tape Solution Offloads Encryption

z/OS centralized key management

- Solution to protect and manage keys
 - Highly secure and available key data store
 - Long term key management
 - Key recovery
 - Single point of control
 - Does not require host MIPS
 - Tivoli Storage Manager support of encryption keys

Encryption Facility for z/OS, V1.1



- Flexible options for business partner exchange
- Partners can encrypt and decrypt using no-charge JAVA client
- Supports public key or password based exchange

- Highly secure tape library
- High performance archive encryption
- Transparent to existing applications
- Can help with audit compliance

System z Encryption

- Security of keys
 - ▶ Provide a *single* vendor solution.
 - ▶ IBM provides a solution for long-term key management
 - ▶ RACF provides *access control* for keys (not available on other platforms).
- Availability
 - ▶ System z availability maximizes *uptime* of key managers
 - ▶ Disaster recovery for back-up and recovery of key information.
- Auditing
 - ▶ RACF auditing to meet regulatory requirements
 - ▶ Tape solution offloads host-based encryption of data

Compliance is Enabled by Solid Security

ODI must comply with regulations.
We also need to enforce policy and protect against inadvertent mistakes.



On Demand Insurance
CEO

RACF and Consul provide many capabilities around auditing and reporting to help you comply with Sarbanes-Oxley, Basel II, privacy and other regulations.



IBM

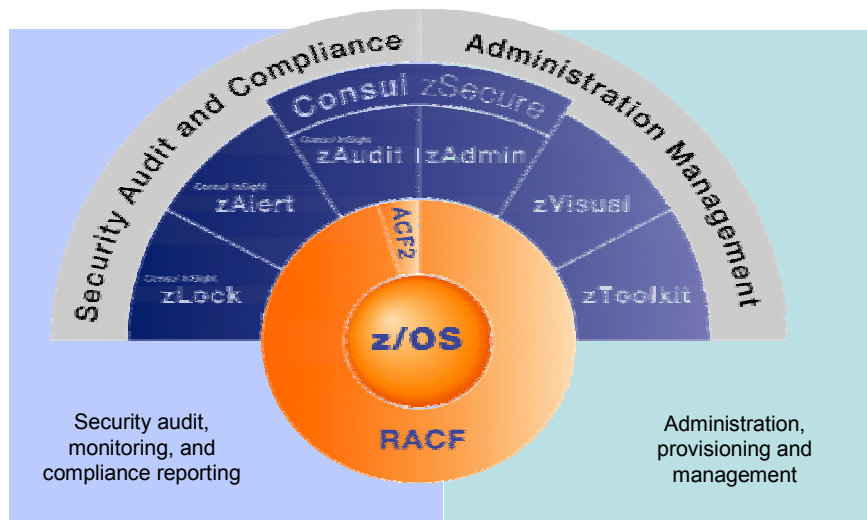
Common Logging via RACF Enables Consistent Auditing

- All subsystems log RACF records system events from multiple subsystems
- Reports access to protected resources, security violations, unauthorized actions
- Monitors user activities:
 - ▶ Issues SMF records
 - ▶ Provides a Report Writer and XML reporting interfaces
- RACF SMF Data Unload Utility creates file from relevant SMF data.
- Used with Consul to help organizations prevent unauthorized commands from being executed and provide audit reports.

"On a typical day, the security team logs 38,000 attempts – by unauthorized individuals or automated probes – to access the state's networks.
That's about one every 2.3 seconds."

Defending Data: a Never-Ending Vigil-Dan Lohrman, CSO, State of Michigan Baseline, 2004

The Consul Suite and RACF for Administration and Compliance



zAdmin for Powerful RACF Administration

Enables more efficient and effective mainframe administration using significantly less resources than would be necessary using native RACF.

- Cut mainframe administration costs in half
- Increase quality of mainframe security

Z Toolkit also allows simple mainframe administrative tasks to be conveniently run from a CICS environment.

Consul/zSecure RACF USER overview 1 s elapsed, 0.4 s CPU
All users with name ROB 18 Jan 2002 14:25

User	Complex	Name	DfltGrp	Owner	RIRP	SOA	gC	LCX	Grp
CRMAROB	CRM4	VAN HOBOKEN, ROB	CRMA	CRMA	S	A	g	L	12
CRMAR02	CRM4	VAN HOBOKEN, ROB	CRMA	CRMA	A				10
RCOPROB	CRM4	ROB VAN HOBOKEN	CRMA	CRMA	R	L		X	5
RCOPROX	CRM4	DATASETS ROB	CRMA	RCOPROB	I			X	1
RCOPRO2	CRM4	ROB VAN HOBOKEN	CRMA	CRMA	R	A		X	3

***** BOTTOM OF DATA *****

Logon attributes:
R - Revoked
I - Inactive
R - Restricted
P - Protected

Authorities:
S - Special
O - Operations
A - Auditor

Add. Auth:
g - group SOA
C - Class auth

Special userid:
L - RACLINK
C - Certificates
X - Expired password

Command ==>>> Scroll==>>> CSR

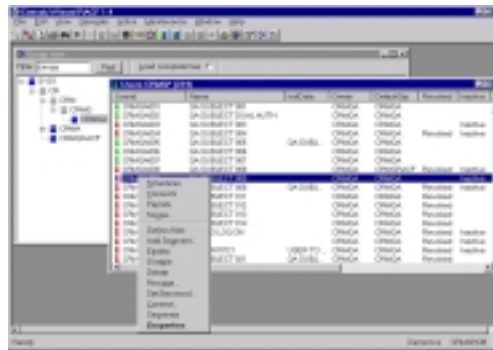
08 - The New Face of Mainframe Security v3.9.ppt

19

zVisual – for Windows Based Administration in a Decentralized Environment

Limit the need for RACF expertise through the use of a Windows-based tool. Ideal for decentralizing RACF admin.

Provides a Windows based GUI for RACF administration. zVisual establishes a secure connection directly with RACF to enable decentralized administration from a Windows environment.



08 - The New Face of Mainframe Security v3.9.ppt

20

z/OS Status Audit- Security Event Audit and Monitoring

```

Trusted userids (0)
Pri Complex T
10 DINO
Pri Reasons Use
10 356 CR
Pri Cnt Audit concern
== 10 1 Can use Trojan attacks via the .profile of trusted user OMVS
== 10 1 Can use Trojan attacks via the .profile of trusted user CRMAROB
== 10 1 Can use Trojan attacks via the homedirectory of trusted user CRMAROB
== 10 4 Can submit jobs for trusted user
== 9 1 Can make HFS file APF-authorized, APF program can bypass security
== 9 1 User privileges and rules may be changed directly on disk
== 9 3 Security-relevant parameters may be changed
== 9 11 JCL that runs with high authority may be changed
== 9 72 May change APF program that can bypass security
== 8 1 Can alter the RMM control data set, thus gaining access to any tape
== 8 1 Can change userid with set(re)uid or spawn
== 8 1 Can change APF program and hence bypass security
== 8 1 Superuser authority, can do anything in USS
== 7 4 May mark jobs as propagated from any user
== 6 1 Can dump all data sets, gaining access
== 6 1 Can dump and delete all data sets, gaining access
Command ===>

```

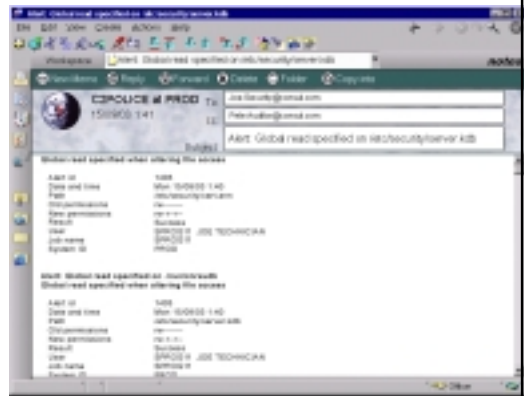
zAudit looks across mainframe systems, measuring and auditing status and events. It provides standard or customized reports, and alerts on policy exceptions or violations which helps identify security breaches.

zAlert for Real Time Threat Monitoring

zAlert goes beyond conventional intrusion detection solutions to encompass intrusion prevention, as it can take instant action to stop an attack.

- Send WTO to trigger Automated Operations
- Issue commands autonomously

- Monitor sensitive data
- Fix configuration mistakes early
- Detect and stop security breaches
- Lower cost associated with Incident Response



zLock Intervenes to Locks Out Non-compliant RACF Commands from Executing

...Against the creation of default passwords

```

CDB431E Use of default value for DFLTGRP not allowed, command terminated
RCDRY
CDB431E dflt(cadm)
CDB431E Password must be different from DFLTGRP, command terminated
RCDRY
CDB431E dflt(cadm) pass(mgwd)
RCDRY
    
```

Ensures mainframe compliance to company policy and procedures by preventing erroneous commands, thereby increasing control and decreasing the security risk and clean-up cost.

```

ECHKR001 CDB431E LAST ACCESS BY 18.08.18 ON MONDAY, FEBRUARY 25, 2003
ECHKR001 CDB431E LOGIN IN PROGRESS AT 18.09.25 ON FEBRUARY 25, 2003
ECHKR001 NO SIGNIFICANT REVISIONS
RCDRY
CDB431E USERID(CADM) 3 GROUP(CADM) 3 WWWID(CM) BOMBE 01 3
CDB431E USER ID TESTUSER EL1046 3
ECHKR001 CDB431E ACCESS AUTHORITY
FROM RCDRY USER ID * * *
ACCESS INTENT(SUPRSE) 1 ACCESS ALLOWED(SMME) 3
CDB431E User id TESTUSER not allowed in naming conventions, command terminated
RCDRY
    
```

...Against the creation of wrong usernames

Consul and RACF Helps Companies Comply with Regulations and Policy

Pass audits, improve security	Prepare reports that auditors and regulators require. Reduce costly security breaches through more secure mainframe administration.
Reduce costs	zAudit reduces hours needed to audit, report and clean-up administrative databases.
Increase operational effectiveness	zAudit shows JCL, parameters or load modules that were changed, thus reducing downtime of applications caused by improper modifications.
Improve speed of incident reaction	Because e-mail alerts contain the relevant details, administrators can quickly diagnose and remediate failures.
Eliminate in-house software efforts	Reduces or eliminates need for internal applications and fixes to enforce compliance.

DEMO: Consul's Insight Suite Helps Address Regulatory Challenges

Offers modules to help accelerate clients' policy, and regulatory compliance initiatives.

Supports RACF records and other input sources.



08 - The New Face of Mainframe Security v3.9.ppt

25

Tivoli Security Leverages System z Security

- Tivoli security products extend System z security
 - ▶ Enable System z customers to participate in a secured end to end security solution
 - Provide a standards based approach to security
 - Provide seamless provisioning across platforms
 - Authenticate users with more precision
 - ▶ Provide audit and compliance to:
 - Report on security events
 - ▶ Provide a seamless approach to leveraging System z security capabilities outbound from the host
 - Leverage System z authentication and resource authorization
 - ▶ Develop secured SOA applications
 - Authenticate more seamlessly across a federated environment

08 - The New Face of Mainframe Security v3.9.ppt

26

Tivoli Federated Identity Manager

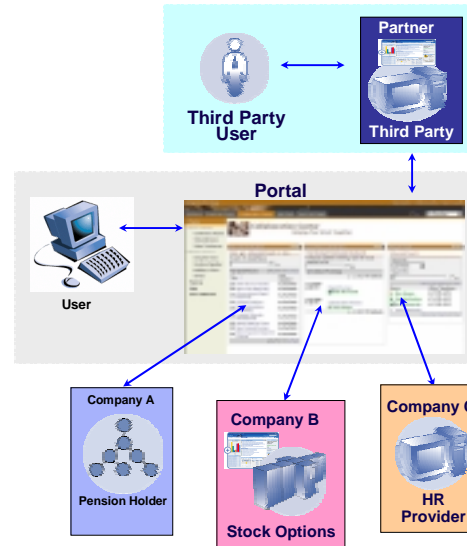
Cross-Domain Security for Web Services and Credential Transformation

Typical Scenarios

- Used for multiple enterprises or multiple businesses in an enterprise
- Share user information among trusted partners in a transaction

Value Proposition

- Lowers identity management and help-desk costs
- Improves user experience
 - ▶ Streamlined registration
 - ▶ Federated SSO
- Enables secure, trusted business exchanges



08 - The New Face of Mainframe Security v3.9.ppt

27

Tivoli Directory Integrator Enables Consistent Identity Management

Maintain data consistency across multiple identity repositories to synchronize user information quickly and efficiently

- Most customers have multiple directory structures in place – no single version of the truth
- Cost-effective synchronization of identity data sources
- Links data residing across IBM and non-IBM directories, databases, password stores, and applications.
 - ▶ Uses multidirectional data flows called Assembly Lines to coordinate changes
 - ▶ Provides clients access through LDAP, HTTP, JMS, Web services and Java API.
- Automatically detects directory changes and pushes modifications out
 - ▶ Triggers: e-mails, database/ directory updates, SOAP messages
- Uses a browser based administrative interface

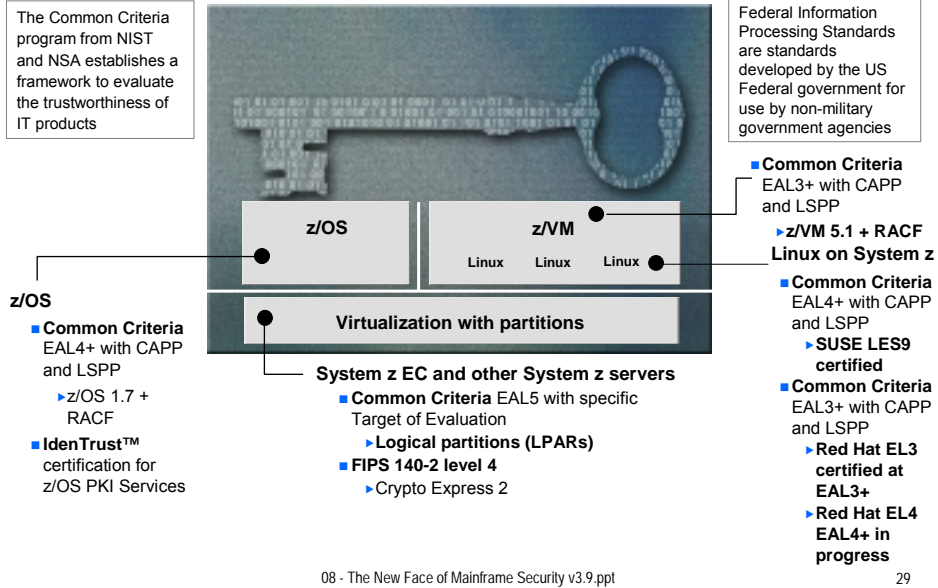
08 - The New Face of Mainframe Security v3.9.ppt

28

Certifications on System z

The Common Criteria program from NIST and NSA establishes a framework to evaluate the trustworthiness of IT products

Federal Information Processing Standards are standards developed by the US Federal government for use by non-military government agencies



Summary: System z Provides Comprehensive Security Capabilities

- Integrated throughout the stack
- Network security
- Compliance and audit support
- Data lifecycle protection
- Excellent cryptography
- Meets stringent standards

Rock Solid Security



