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

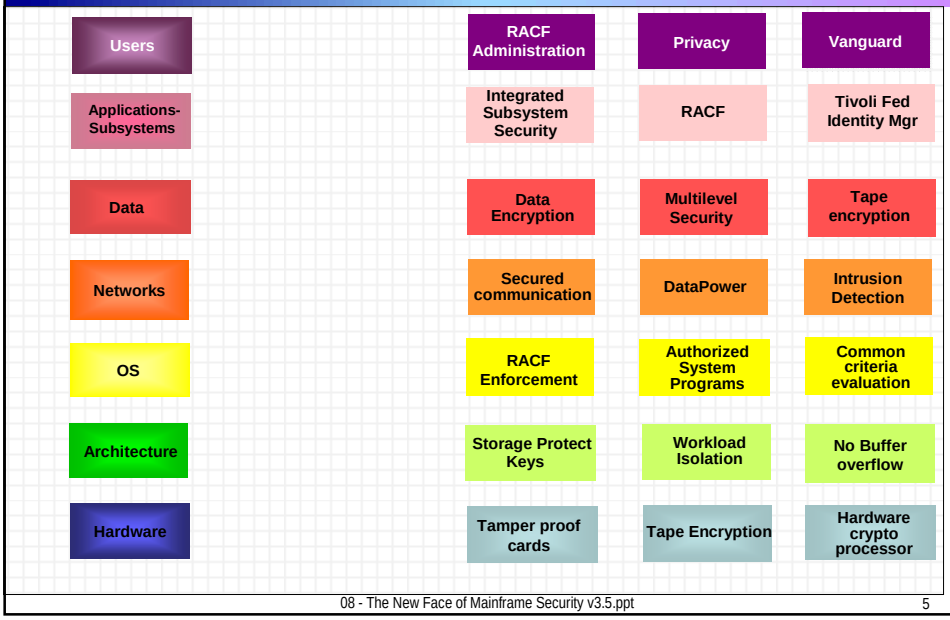
- Regulatory compliance issues raise security visibility; executives are personally accountable
- New online business solutions will require a security environment that actively protects against intrusions
- We need additional protection capabilities for confidential data which will be shared with business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

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+)

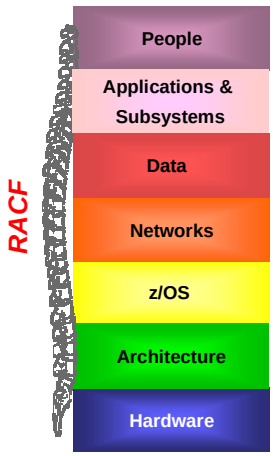
Proven secure by 40 years of secured operations!

Integrated Security Throughout the Stack Leverages System z



The Backbone of System z Security: RACF

Integrated Security Throughout the Stack



Resources protected by RACF:

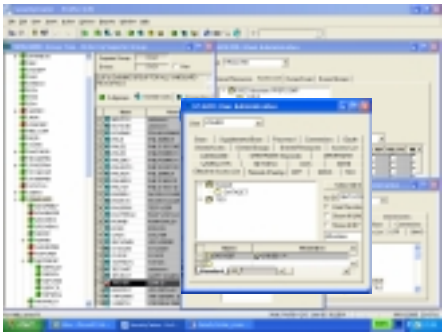
Programs	Utilities
WebSphere	MQ
CICS	IMS
DB2	ISO
SNA/VTAM	SDSF
Console	JES2/JES3
VSAM	DFSMS
Print	Ports
DASD	Tape

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

Simplifying z/OS Administration and Audit Vanguard Security Solutions

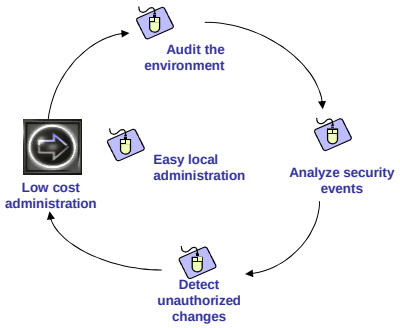


- IBM & Vanguard Security Solutions
  - Vanguard Security Center offers ease-to-use graphical user interface for RACF and DB2 security administration on z/OS
  - Vanguard Administrator provides advanced security server management and analysis with automation and power utilities
  - Vanguard Analyzer assists with security system snapshots or full-scale System z9 security audits
  - Vanguard Enforcer manages and enforces security policy in z/OS and RACF
  - Vanguard Advisor provides event detection, analysis and reporting capabilities for the z/OS and RACF

Vanguard Improves Productivity

Vanguard Administrator

- Administration productivity
- Reduces errors
- Eliminates tedious, repetitive tasks
- Designed for security administration
- Addresses skills shortage



Vanguard Administrator lets me implement broad security changes without errors.

ODI Security Administration

Vanguard Administrator
Provides automated administration, data mining, reporting and analysis tool enhances IBM's RACF to become a policy and role-based user provisioning tool.

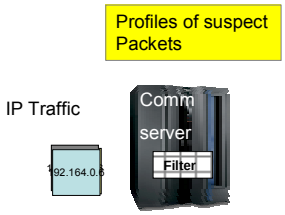
Network Security

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

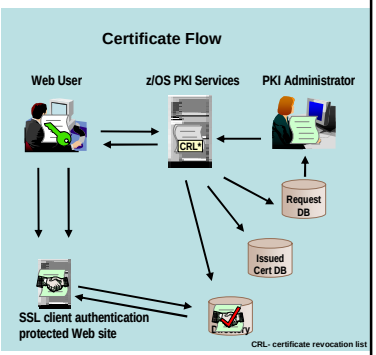
System z Communications Server Provides Intrusion *Defense*

- 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



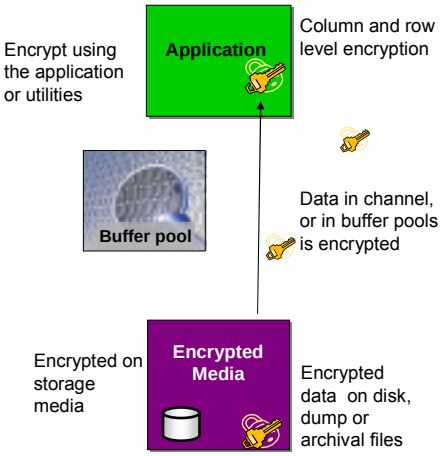
Digital Certificates for Secured Network Transactions

- A PKI infrastructure is the standard for public-key cryptographic security that ensures the security of digital certificates.
- PKI Services is part of RACF
  - Customers can issue their own certificates
  - No need for extra infrastructure
  - No need to pay third party costs
- IdenTrust™ compliant certification
  - IdenTrust is a standard used by over 60 banks
- Leverages System z capabilities:
  - Secures private keys with System z cryptography
  - Provides digital certificate life cycle management
  - Administer certificates via RACF
  - Dynamically checks for expired certificates
  - Support smart cards



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



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

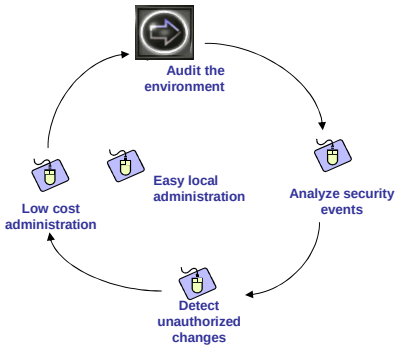
RACF and Vanguard provide many capabilities around auditing and reporting to help you comply with Sarbanes-Oxley, Basel II, privacy and other regulations.

IBM

Detect Security Events Using Vanguard Advisor

Vanguard Advisor

- ODI wants an intuitive reporting tool
- Complete detailed reporting offers an intuitive interface
- Reports can be set-up and configured for email delivery
- Reduce learning curve for new administrators



I need to automatically receive detailed information on *any* suspect activity.

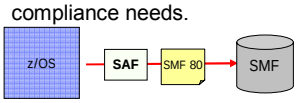
ODI Security Administration

Vanguard Advisor: Event detection, analysis, real-time alerts, reporting and electronic report distribution.

Common Logging via RACF Enables Consistent Auditing to Address Regulations

- 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.

RACF enables consistent and consolidated auditing to address compliance needs.



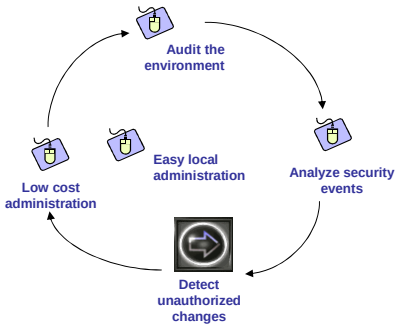
"On a typical day, the security team logs 38,000 attempts – by unauthorized individuals or automated probes – to access the state's networks.
That's about one every 2.3 seconds."

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

Detect Unauthorized Changes with Vanguard Enforcer

Vanguard Enforcer

- Protects critical data and resources
- Ensures policies and rules are in force
- Provides continuous monitoring
  - Periodically scans z/OS and RACF comparing against baselines
- Logs discrepancies, takes corrective action



We need our security rules enforced for us automatically, and continuously.

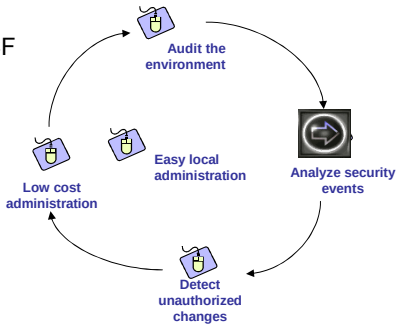
ODI Security Administration

A proven intrusion detection and management solution for protecting critical data, user groups and assets.

Easy Auditing of z/OS Environment with Vanguard Analyzer

Vanguard Analyzer

- Easy auditing of z/OS environment & RACF
- Provides best practices and expert advice
- Reduces errors
- Helps with preparing for external audits
- Enables less experienced people to check changes to the environment

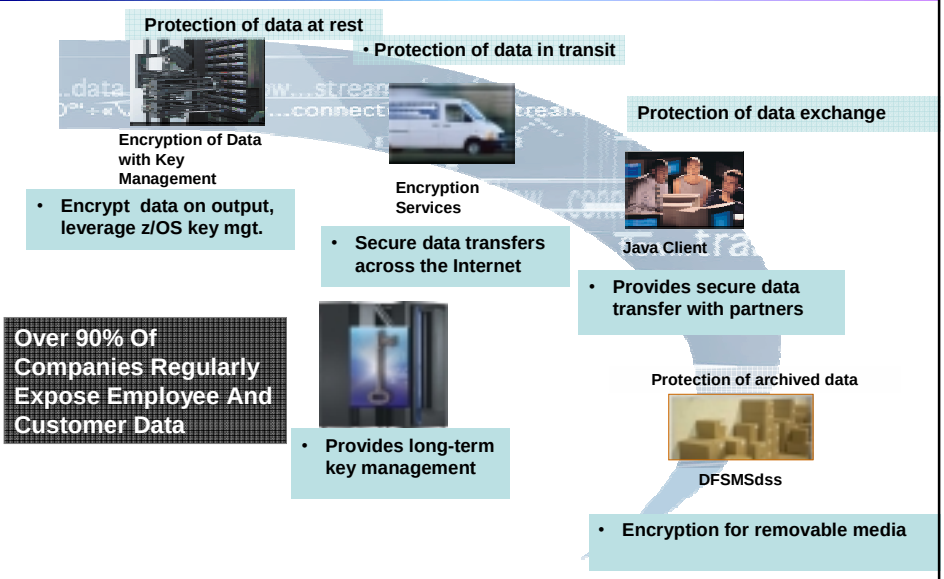


If unauthorized changes are made I need to know as soon as possible, before exposures occur!

ODI Security Administration

A system integrity, assessment, risk identification, threat analysis and problem rectification solution.

Data Protection Throughout the Life Cycle

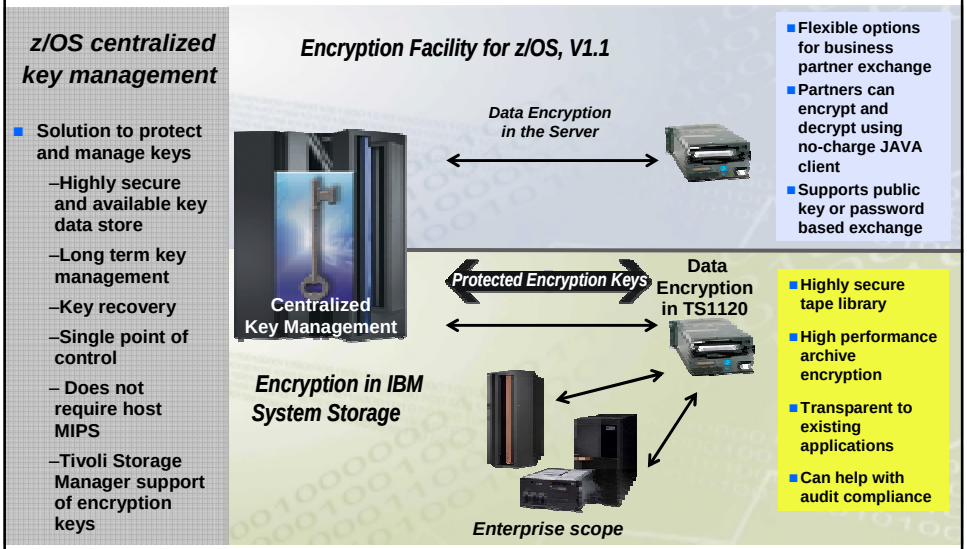


Mainframe Hardware Accelerates Encryption

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

New Tape Solution Offloads Encryption



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 strategy
    - Provide a standards based approach to security
    - Provide seamless provisioning across platforms
    - Authenticate users with more precision
  - Provide audit and compliance to:
    - Report on System z 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

Tivoli Federated Identity Manager

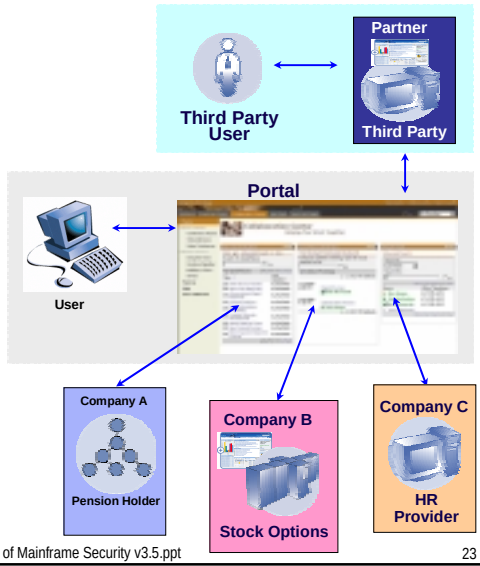
Cross- Domain Security for Web Services and Credential Transformation

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



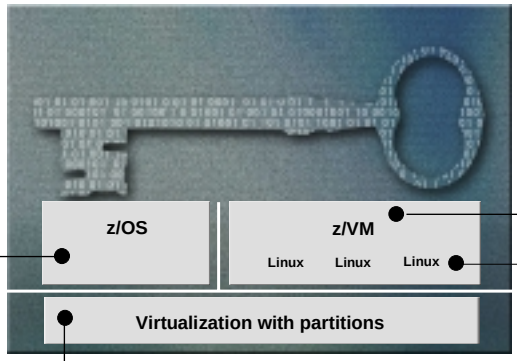
Tivoli Directory Integrator Enables Consistent Identity Management

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

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

z/OS

- **Common Criteria** EAL4+ with CAPP and LSPP
  - z/OS 1.7 + RACF
- **IdenTrust™** certification for z/OS PKI Services

System z EC and other System z servers

- **Common Criteria** EAL5 with specific Target of Evaluation
  - **Logical partitions (LPARs)**
- **FIPS 140-2 level 4**
  - Crypto Express 2

- **Common Criteria** EAL3+ with CAPP and LSPP
  - **z/VM 5.1 + RACF**

Linux on System z

- **Common Criteria** EAL4+ with CAPP and LSPP
  - **SUSE LES9 certified**
- **Common Criteria** EAL3+ with CAPP and LSPP
  - **Red Hat EL3 certified at EAL3+**
  - **Red Hat EL4 EAL4+ in progress**

Summary: System z Provides ODI with Comprehensive Security Capabilities

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

Rock Solid Security