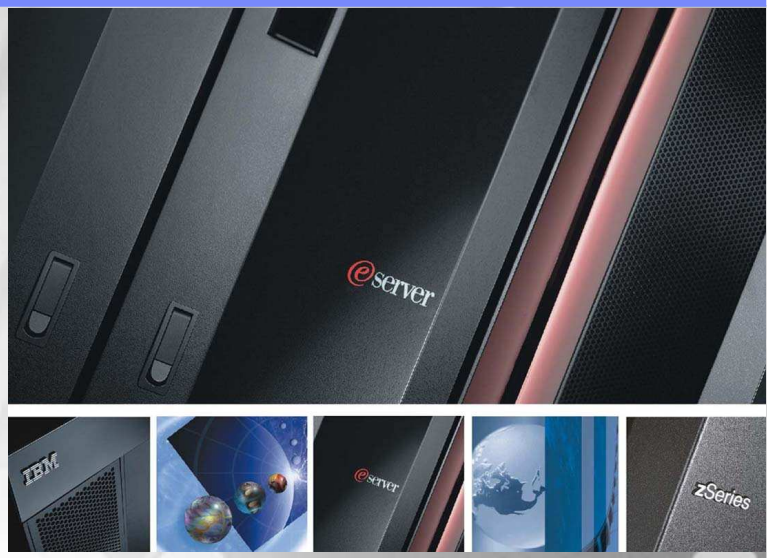
IBM Software Group

IBM zSeries

RACF User Group
Security Built in



Barbara Sannerud
Software Group, Competitive Project Office
sannerud@us.ibm.com

April 2006

ON DEMAND BUSINESS™

Trademarks

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

IBM*
IBM eServer*
IBM logo*
CICS*
DB2*
Domino*
FICON*
GDPS*
Geographically Dispersed Parallel Sysplex
HiperSockets
HyperSwap
IMS
MQSeries*
Parallel Sysplex*
RACF*
Rational*
Redbooks
Resource Link
System z9
Tivoli*
Virtualization Engine
WebSphere*
z/OS*
z/VM*
zSeries*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States, other countries or both.
Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries
Linux is a trademark of Linus Torvalds in the United States and other countries..
UNIX is a registered trademark of The Open Group in the United States and other countries.
Microsoft is a registered trademark of Microsoft Corporation in the United States and other countries.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

- Drivers for security
- Market validation
- A framework to describe security value
- zSeries security capabilities and value
- Calls to action

"The pessimist sees difficulty in every opportunity. The optimist sees the opportunity in every difficulty."

Winston Churchill

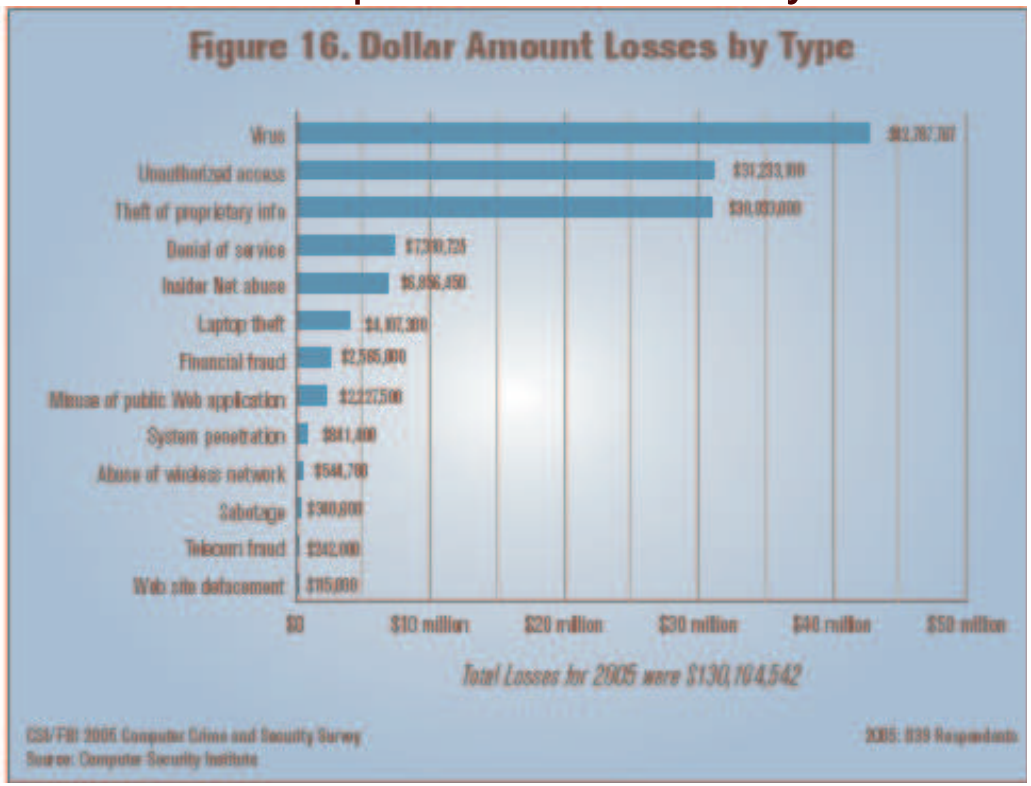
A Security Perspective

- Organizations are seeking more comprehensive security approaches. Niche solutions don't cut it.
- Organizations do not find themselves more secure after buying additional security tools
- Every new technology generation unveils new vulnerabilities.
- Attackers revise their tactics. They are getting smarter.
- The global workforce introduces additional risks; processing hubs must be especially resilient.
- Regulatory compliance requirements raise security visibility to the executive suite.
- Skills are hard to find. Security needs to be baked in.

Cost of Security Incidents

- Computer Crime Survey indicates virus attacks still continue as the source of the greatest financial losses.
- Unauthorized access, and theft of proprietary information show a dramatic cost increase year to year.
- **Loss from unauthorized access to information**:
  - $51,545 in 2004 ->$303,234 in 2005
- **Loss from theft of proprietary information**
  - $168,529 in 2004 -> $355,552 in 2005.
- The percentage of organizations ***reporting*** computer intrusions to law enforcement has continued a multi-year decline.
- Major reason for non reporting is concern over reputation damage.

CSI/FBI Computer Crime Survey 2005

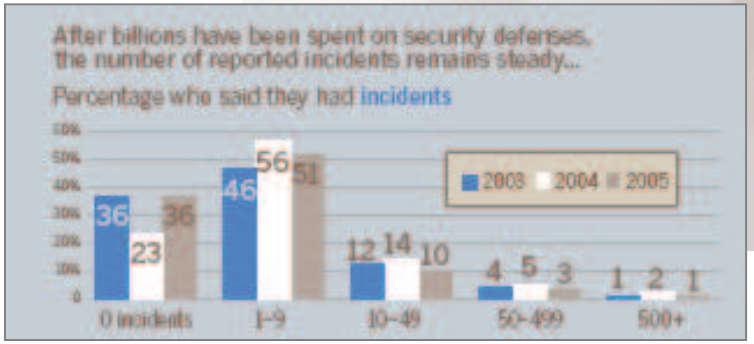


The Security Landscape – Investments Today

- Companies continue to spend on security and security remains a top priority for 2006.
- Inadvertent mistakes and error remain weak links.
- Compliance remains top of mind, driving investments in security.
- Gartner - According to a 2005 survey, 27% of IT security spending is justified as risk and cost avoidance.
- Point security solution investments help fight off skirmishes, but after sinking money into security defenses, security incidents have not changed.

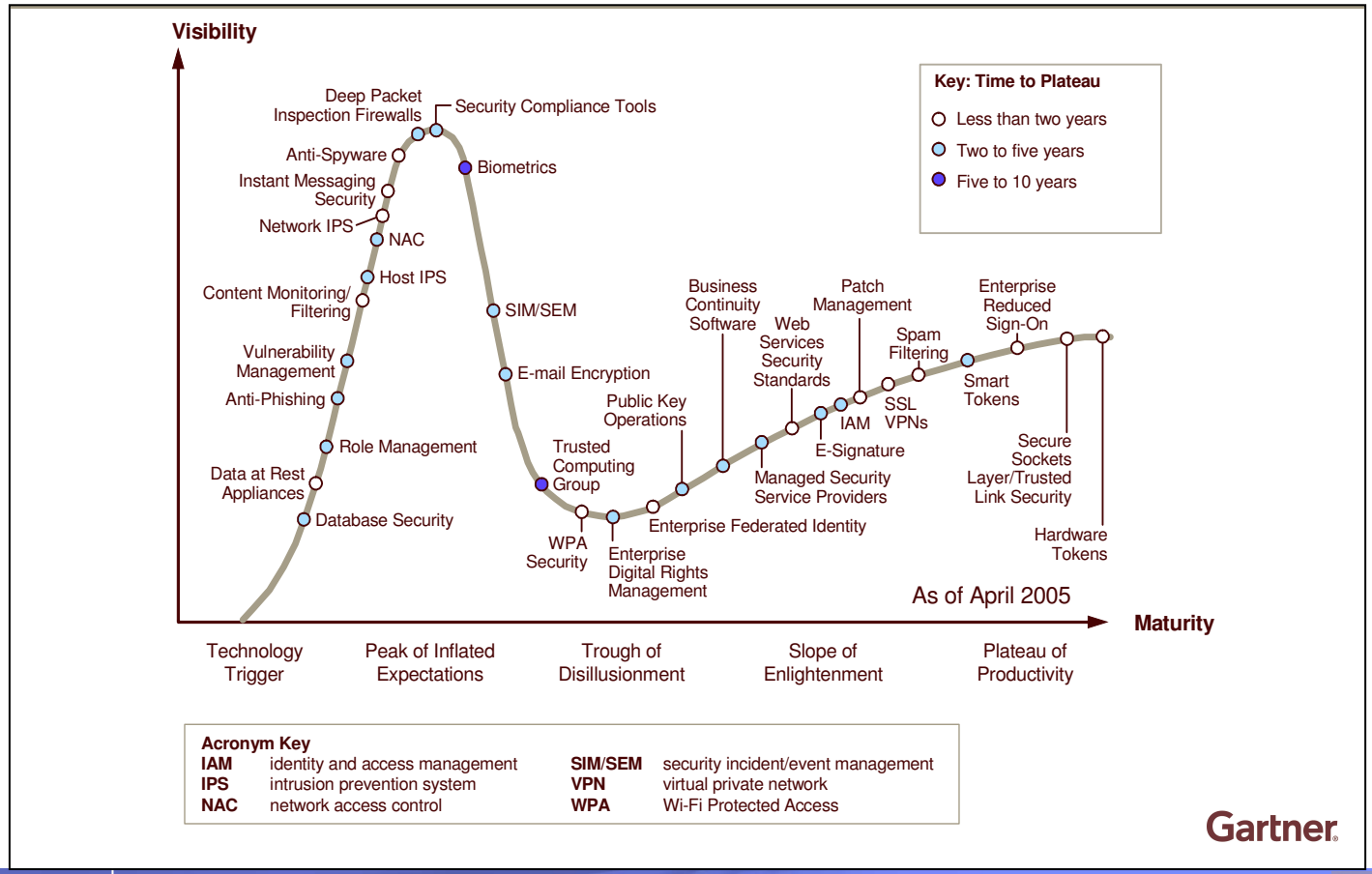
Worldwide, IDC estimates that security spending will be **$38 billion** in 2005 up from $32 B in 2004

The Global State of Information Security 2005
Study CIO Magazine/PwC September 15, 2005



We can address both current and emerging security needs. IBM offers a full suite of capabilities to defend against disruptions, improve processing integrity and provide security assurance.

Gartner's Hype Cycle for Security Technology



Gartner June 2005

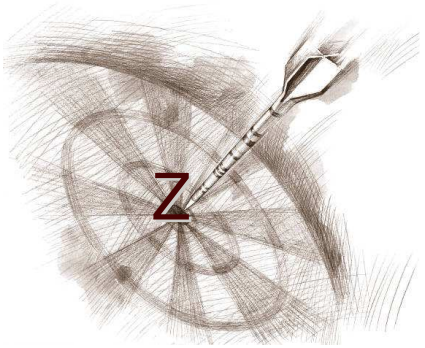
Vic Wheatman

Point Security Approaches Often Miss the Mark

zSeries offers a fortified infrastructure based on several pillars:

I. Infrastructure security – a trusted computing environment

- The infrastructure foundation needs to be impervious to service attacks, denial of service, viruses or worms.
- A hardened security solution provides assurance against malicious attacks as well as inadvertent errors
- Even if malware were introduced it would have no impact..



II. Data and business process integrity

- prevents loss or corruption of data and preserves the integrity of processing
- Prevent viruses and malware
- Integrity also includes integrity of applications during failover

III. Regulatory compliance and risk mitigation

- checklist based audit approaches rarely address security gaps.
- Address multiple evolving regulations; preserve privacy and operational resiliency

What We Read About Other Solutions…

Information Week Jan 25 2006
"Just five days after Oracle released a critical security update that patched 82 vulnerabilities, a Gartner researcher said in an online advisory that "Oracle can no longer be considered a bastion of security."
…. "The database products alone include 37 vulnerabilities, many rated as easily exploitable and some potentially allowing remote database access. Oracle has not yet experienced a mass security exploit, but this does not mean that one will never occur."

17 Nov 2005 | SearchSecurity.com

"Microsoft is aware of public reports of proof-of-concept code that seeks to exploit a possible vulnerability in Microsoft Windows 2000 Service Pack 4 (SP4) and in Microsoft Windows XP Service Pack 1 (SP1)," the company said. "This vulnerability could allow an attacker to levy a denial-of-service attack of limited duration."

Information Week Nov 7 2005

Cisco issued a security advisory for a serious IOS "heap-overflow" vulnerability that could let hackers get control of routers and switches running certain versions of the software. .. "In the event of successful remote code execution device integrity will have been completely compromised."

IDG News Service, 10/19/05

Oracle released a bundle of critical security patches for its software on Tuesday, fixing 88 vulnerabilities in products including its database and application servers and in some PeopleSoft and JD Edwards applications. …

Security - Empowered by zSeries

- Built in security to address the full spectrum of security requirements
- Policy based security management
- Addresses security functional domains
- Designed to meet evolving applications needs
- Addresses multiple resource types- applications, data, networks
- Positions zSeries as a “secured vault”
- Proven heritage and experience base
- Common criteria certified
- Simplifies security infrastructure
- Most importantly ---**IT WORKS!**

“Whilst the performance and resilience characteristics are formidable, it is the security features that are likely to attract most attention”
Tony Lock – Chief Analyst, Bloor Research 2005

Proven secure by 40 years of operation!

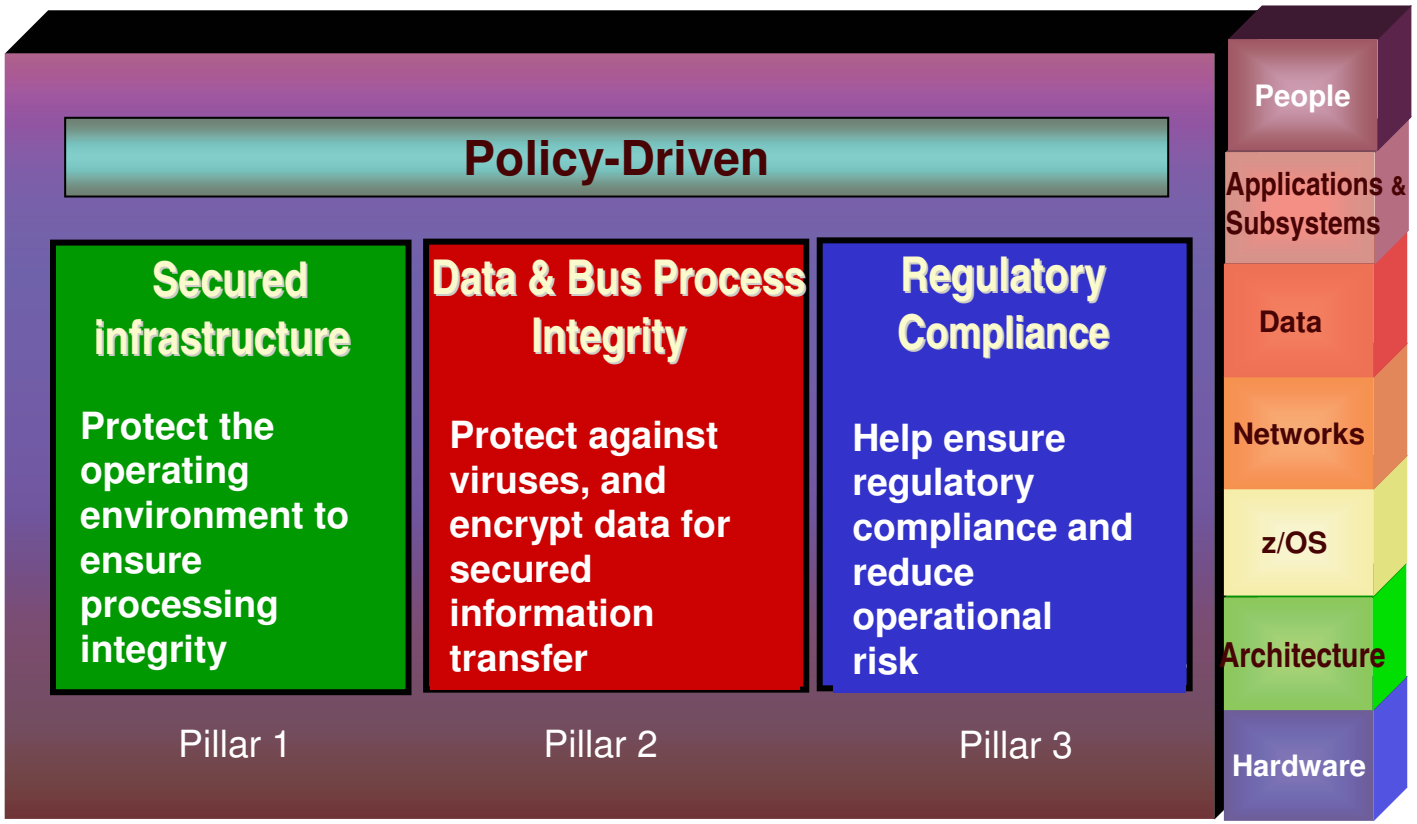
Requirements for a World Class Security Solution …

- The infrastructure foundation needs to be impervious to service attacks, denial of service, viruses or worms.
  - A hardened security solution provides assurance against malicious attacks and inadvertent errors
  - Introduction of malware should not disable system.
- Data and business process integrity prevents loss or corruption of data regardless of location, and preserves the integrity of processing and protection of information
  - Application integrity around OLTP sustains information integrity.
  - Includes integrity of applications during failover
- A secured solution enables regulatory compliance and risk mitigation.
  - Address multiple evolving regulations; preserve privacy and protect operational resiliency
- Security cannot be a veneer on an exposed environments. With integrated security better end-to-end security be achieved.

In 2005 more than 50M Americans had personal information compromised, many from highly-publicized losses of unencrypted tape

Security upgrades remain a top priority listed only second after regulatory compliance efforts.
Forrester-The State Of Security In SMBs And Enterprises. 9-05

zSeries Security fulfills these Requirements



- ✓Secured infrastructure provides a hardened foundation
- ✓Information integrity for integrity of business applications
- ✓Enables compliance reducing operational risk
- ✓Policy driven

Security upgrades remain a top priority listed only second after regulatory compliance efforts.
Forrester-The State Of Security In SMBs And Enterprises. 9-05

Security Integrated Throughout the Stack

Includes identity management and sustaining the privacy of individuals

Applications, OLTP and other subsystems must maintain processing integrity

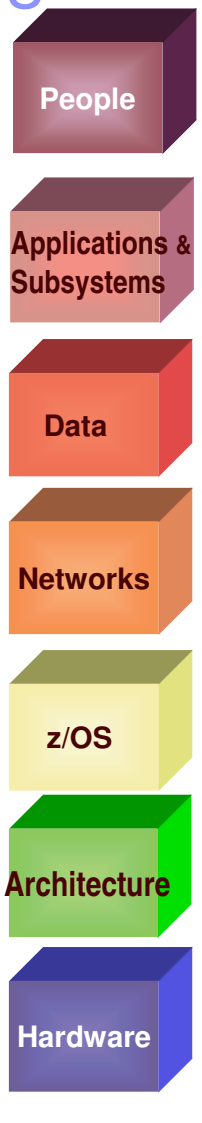
Information must be protected against unauthorized access regardless of location

Internetworked eCommerce environments require integrated security

RACF built into z architecture, helps ensure integrity and operational resiliency

Security must be hard wired into operating system to prevent malware and viruses

Communications and firmware must enable encryption, provide availability and process integrity



RACF Vanguard	Privacy SPARCLE	Authentication, Identity Mgt/EIM
CICS	IMS	Websphere
RACF- Access, Audit	MLS	Encryption
Authentication	SSL, AT-TLS	IDS, IPSEC, VPN
IDS, PKI	RACF, LDAP, IDS	Common Criteria
Storage Protect Key Encryption	Secured virtualization	LPAR Isolation
Cryptography	GDPS	Physical security

zSeries Security End to End Resource Coverage

Platforms

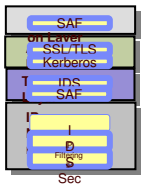
IBM zSeries
Common Criteria
Hardware Resiliency
Hipersockets

Storage protect key
Workload Isolation
Workload mgt.
Partitioning
Error recovery

Encryption
Acceleration &
Compression
Hardware enabled

PCICC

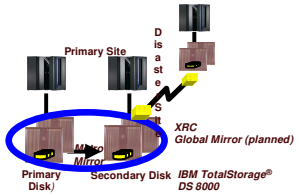
Networks



Secured communications
Intrusion Detection

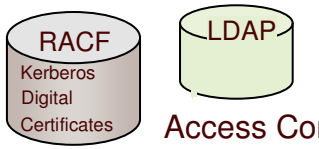
Secure Sockets Layer (SSL)
Communications Server

GDPS for failover , integrity



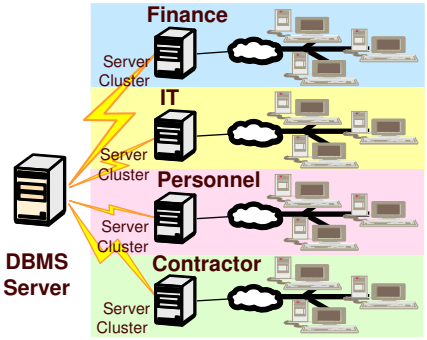
Data

Policy based management
Protection for databases, TP,
DB2, CICS, WAS, IMS



Access Control
Administration
Auditing
Authentication

Multilevel Security



zSeries Security End to End Functional Coverage

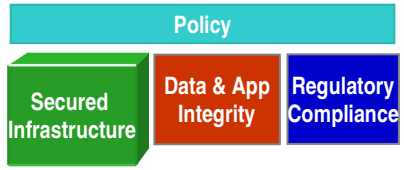
- **Integrity**
  - Prevent Trojan horses, worms & viruses
  - Logical Partitioning and workload isolation
  - Virtual LANs limit potential network intrusion
  - Workload resource management
- **Authentication**
  - RACF and LDAP
- **Data Confidentiality**
  - Secured storage and transport of data
  - Encryption for data at rest and in transit
- **Intrusion Detection**
  - Prevent malicious attacks
  - Network security
- **Privacy**
  - MLS
  - SPARCLE
- **Access**
  - Controlled access to files, programs, interfaces
  - Pass tickets
- **PKI and Certificate Authority**
  - Identify users, issue certificates
- **Integrity of Operations**
  - Maintain continuous processing
  - Manage updates to systems with integrity
- **Auditing and compliance**
  - Track and log security activity
  - Enforce security policy
- **Identity Mgt/Directory**
  - RACF/LDAP
  - EIM for SSO

Pillar I. Unmatched Secured Infrastructure
Ensures System Integrity

Security by design

- Isolation
  - z/OS provides each user with a unique address space
  - Private areas in user address spaces isolated from one another
  - In-memory data can be shared between processes in both Unix and z/OS
  - In z/OS, a user can access another user's address spaces with special authorization for *cross-memory services*
  - An address space includes both system code and data, as well as user code and data managed automatically by z/OS
  - Dynamic address translation (DAT) is used to translate a virtual address during a storage reference into a physical location in real storage
  - Because of workload isolation, storage protect keys, user buffer overflows do not crash systems software code

Security is preserved through a combination of software and microcode-preventing malware, viruses and worms



Unmatched Secured Infrastructure

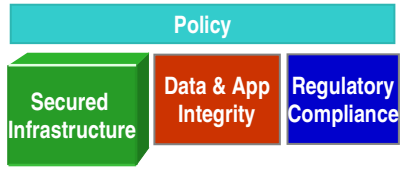
System protection, built in

Security by design (continued)

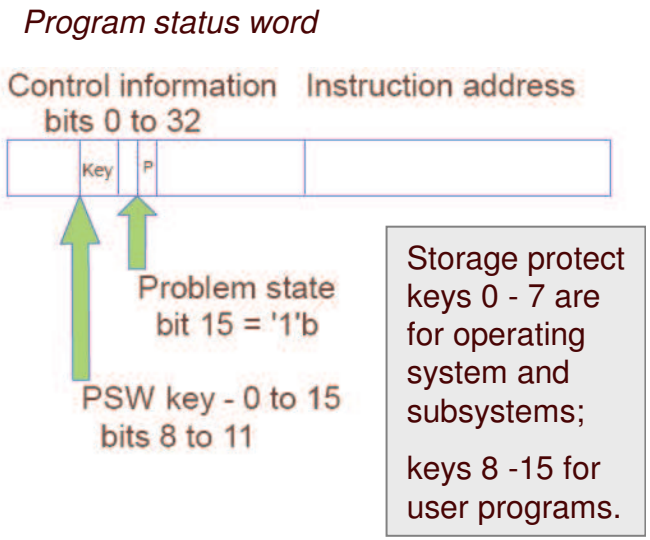
- z/OS cross-memory services require programs to have special granted authority, authorized program facility (APF), to securely access data owned by others
- All authorized programs are store-protected
  - Programs in supervisor state or system programs can't be modified by non system state programs
  - Register save areas and work areas store protected
- APF Authorized programs
  - APF-authorized programs reside in authorized libraries.
  - Authorized programs pass control to unauthorized programs **only** by disabling authorization
- Control blocks for system resources reside in system key designated areas
- Controls blocks and tables used for serialization reside in protected storage

You can't clobber system code

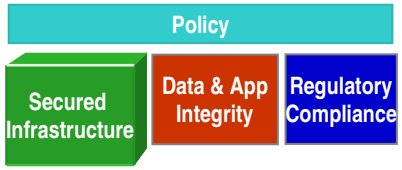
Storage Protection Built in



- Storage protect keys provide additional integrity, **built into the hardware.** (A key is associated with each 4K frame of real storage)
- Checks built into software to validate processing
- Storage & fetch protection bits are not accessible by user programs
- Information in real storage is protected from unauthorized use
- If a request is made to **read** or **modify** real storage, the key of the requestor is compared to the key in storage
- User programs are store-protected and data is fetch-protected from other jobs
- Invalid requests result in a program exception interrupt

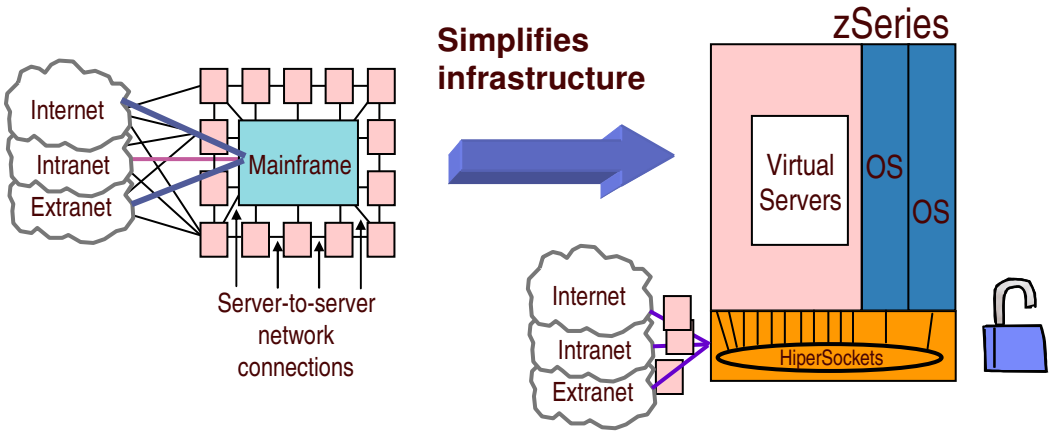


IBM storage protection maintains processing integrity



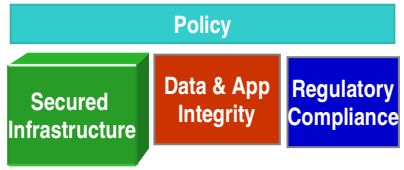
Hipersockets: Secured LAN in a Box

- Data networked via Hipersockets never need travel outside the box!
- Very secure connection – no need for extra encryption
- Communication is through system memory - the virtual servers connected form a “virtual LAN”
- Enables a “Data Center” in a box with a mixture of z/OS and Linux images
- HiperSockets provides an integrated TCP/IP network for consolidation of complex workloads into a single system image
- HiperSockets works transparently to applications
- Virtual network has the benefits of a network without the extra infrastructure



Data in the box travels securely to reduce risk, encryption and network costs.

Common Criteria –Trusted Computing Base



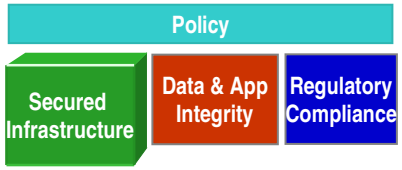
- zSeries is the only server platform that has earned Common Criteria EAL5 certification for logical partitions
  - PR/SM LPAR for zSeries 890 and 990, evaluated at Common Criteria EAL 5 and EAL 4
- z/OS 1.7 and RACF at EAL 4
- z/OS 1.6 and RACF IBM EAL3+ certification
- z/VM V5.1 in evaluation for EAL3
- DB2 UDB also under evaluation at EAL3
- Many IBM products have been evaluated or are in process

Common Criteria program developed by NIST and NSA establishes an organizational and technical framework to evaluate trustworthiness of IT Products & protection profiles

For updates see www.CCEVS.com site

EAL	Requirements
1	Examines if product functions as per documented.
2	Tests the product structure; evaluation includes product design history & testing
3	Evaluates product design by verifying test results.
4	In-depth analysis of product development & implementation – at potentially high costs.
5-7	Requires even more formality in the design process and implementation, analysis of the product's ability to handle attacks & prevent covert channels, for high-risk environments. *Ratings at this level are country specific*
+	Means maintenance is included

Our multiple certified products provide evidence of a deep commitment to security

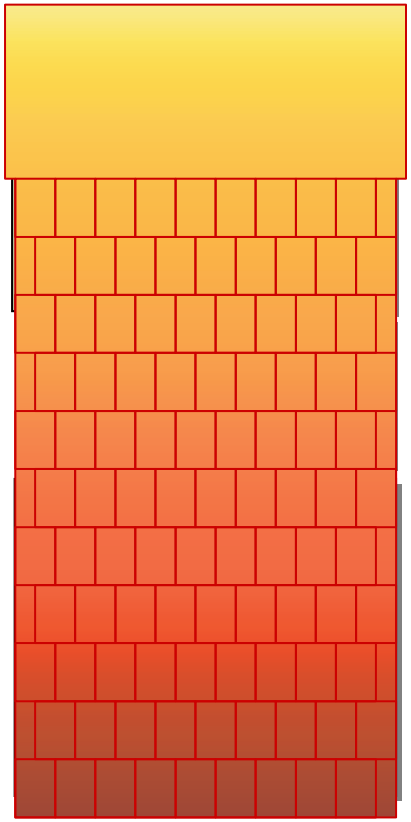


Security Services for the Network Stack

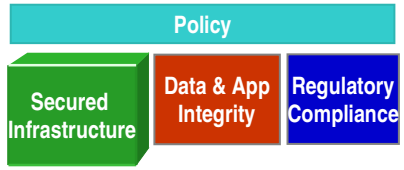
Resource Protection extends to Networks!

Communications Server protects data and other resources on the system

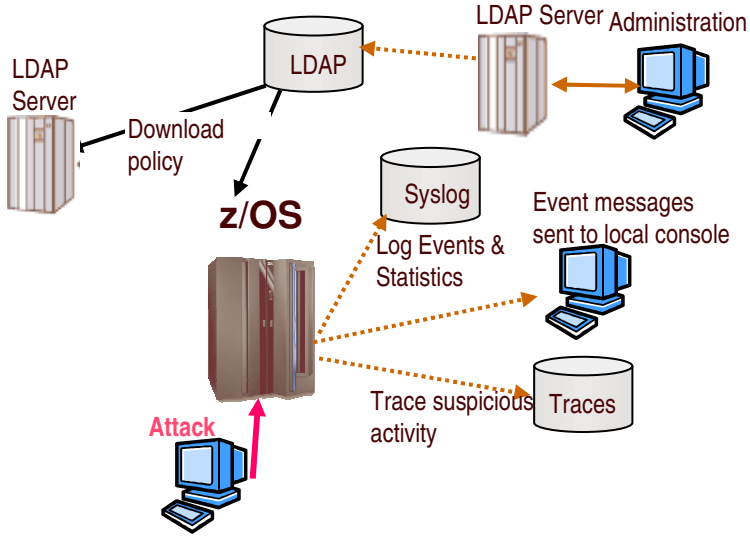
- **Many firewall capabilities automatically provided!**
  - part of integrated z/OS 1.7 IP stack
- Supports cryptographic- based network security protocols
  - IPSec, SSL, SNA sessions
- Support for Kerberos
- Prevent unauthorized user access to TCP/IP resources (i.e. ports, networks)
- IP Packet filtering
- Regulates number of TCP connection requests
- Intrusion detection services
  - provided at both the IP and transport layers



Integrated Intrusion Detection



- **Integrated into z/OS Communications Server**
- Intrusion Detection Services (IDS) are really Intrusion Defensive services
- Enables detection of attacks and application of defensive mechanisms on z/OS server



Detects events:

- Scans Attacks Flooding

Provides Defenses on z/OS

- Packet discard
- Limited # connections

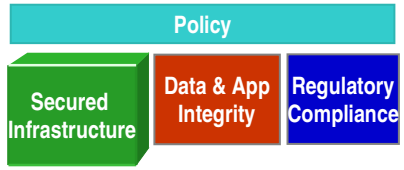
Reports:

- Logging -Console
- Packet trace
- Notifications

Intrusion detection

- Evaluates inbound encrypted data after decryption on target
- Evaluates many known attacks
- Less overhead
- Detects problems in real-time
- Policy based

Protects against network attacks even for encrypted data

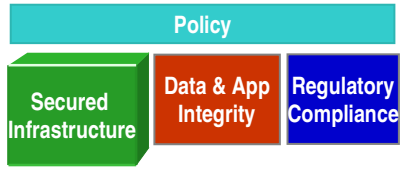


Application Transparent-Transport Layer Security Simplifies Use

- Connection level protocol for TCP/IP applications- Provides Transport Layer Security for applications without requiring application modification.
- Shields complexity of security coding from applications
- Delivered automatically as part of Communications Server
- AT-TLS provides integrity and secured communications managed at the application level
- Transparent to applications - Previously, applications needing secured data connections had to be heavily modified
- Support for C/C++, COBOL, CICS sockets and other languages
- AT-TLS offers policy-based configuration that reduces administrative costs for configuration and offering a consistent policy-based solution
- Also support for SNA session encryption, SSL, IPSec, Kerberos

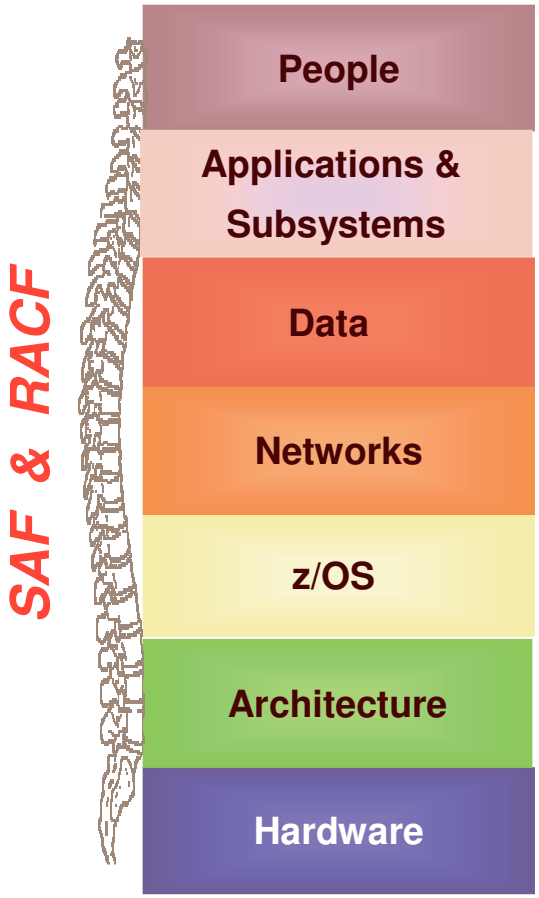
**Transport Layer Security is the evolution of Secure Socket Layer (SSL) technology.*

Secured SSL communications without additional application maintenance.



The Backbone of Security: RACF

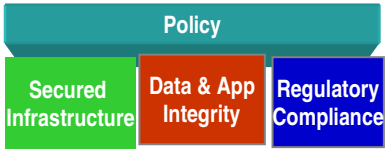
RACF and z/OS SAF provide security throughout the stack



- Offers **administrative** tools, reporting, auditing
- Provides remote **administration**
- Works with LDAP to **authenticate** users
- **Access** control to all classes of resources for applications and middleware
- Provides **auditing** without modifying applications
- Integrates into the **operating system**
- Provides Enterprise Identity Management
- Supports **cryptographic** services
- Supports digital certificates

Proven security, integrated throughout the stack.

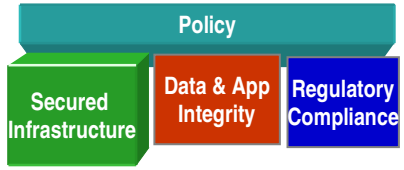
RACF - Consistent Security Policy



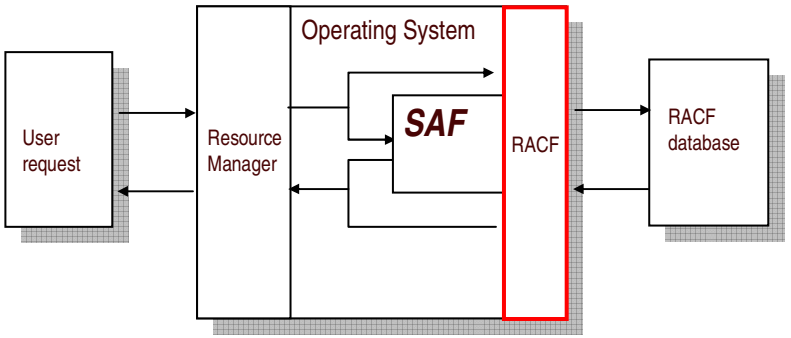
- A single security solution to control access to z/OS Security Server and other system resources
- RACF protects resource access, authorizes users, and logs unauthorized access
- RACF gives you the ability to identify and authenticate users
- Provides flexible access - centralized or decentralized profile controls
- Supports these functions (user identification, access control, and auditing) without modifying applications
- Helps enforce *segregation of duties* by allowing the administrator to change access rules but not change auditing controls
- Reliable, consistent security addressing required security needs

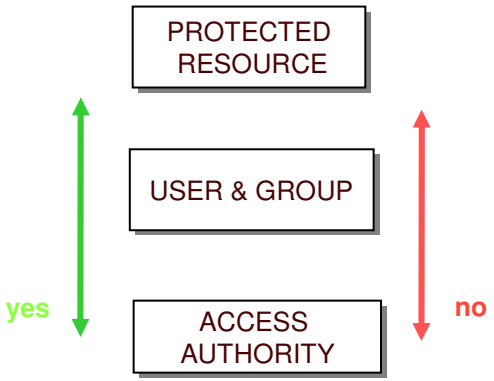
RACF and z/OS provide consistent security for multiple resources, end to end throughout their lifecycle.

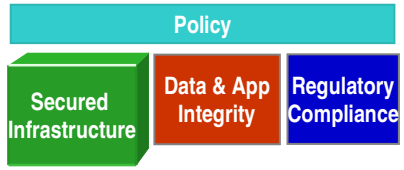
A Proven Approach to Protecting Resources



- RACF acts as a layer in the operating system that verifies user identities and grants requests to resources
- RACF can protect a multitude of network and application resources
- RACF can authorize when a user can access resources
- RACF provides global access checking. Customers can establish system-wide authorization levels
- RRSF allows a security administrator to manage remote RACF databases such as in the case of a disaster recovery center
- RACF allows for Pass Tickets, one-time non-reusable passwords alternatives for applications that span platforms



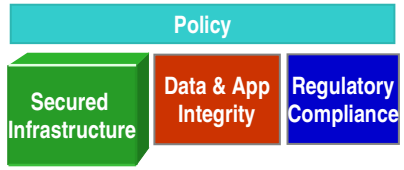




SAF- A Common Base for Resource Control

- SAF (system authorization facility) is a part of z/OS that directs control to RACF when receiving requests from a resource manager
- Resource managing components invoke SAF for access control or authorization checking
- The SAF router is a system service- *part* of the operating system
- SAF provides consolidation and co-location for multiple security services
- SAF simplifies security and removes the overhead of security for multiple systems software products
- It enables the use of common controls across products and systems
- The SAF router, the main element of SAF, can also work with 3rd party security tools

SAF interface is extensible, simplifies security and is part of operating system.



Public Key Infrastructure

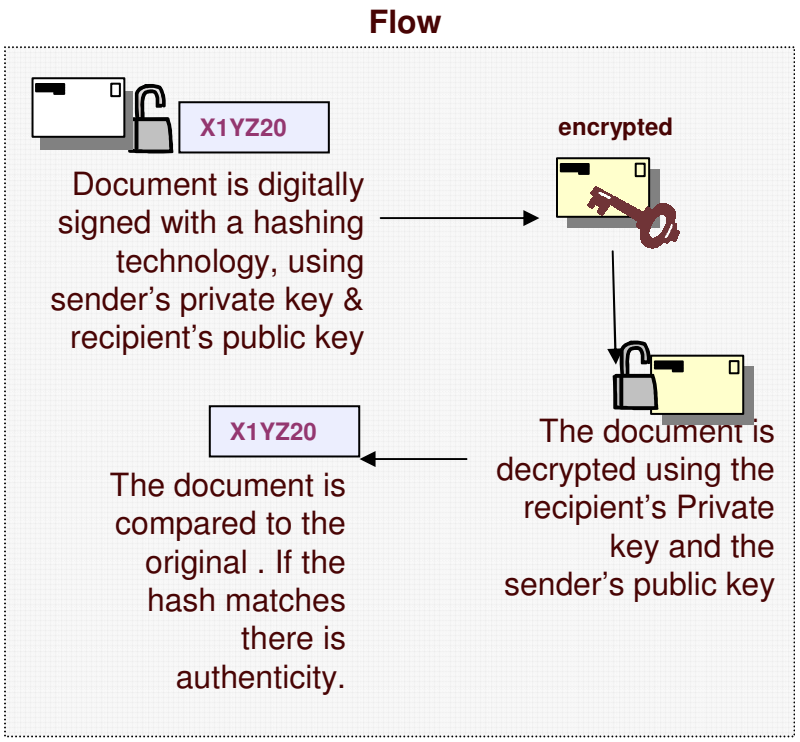
A PKI (public key infrastructure) enables users of a public network (Internet) to securely and privately exchange data through the use of a public and a private cryptographic key pair obtained and shared through a trusted authority.

A public key infrastructure provides applications with a framework for functions including:

- Authenticating parties in transactions
- Authorizing access to systems
- Verifying the author of messages through digital signatures
- Encrypting the content of communications

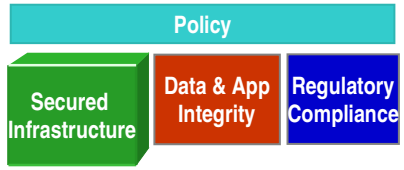
PKI and z/OS

- PKI Services is part of z/OS Security Server
- Interfaces with SAF and RACF
- Used to authenticate users
- Digitally signs electronic documents
- Authentication / authorization of Web users



PKI Services is a critical component needed for secured eCommerce and other applications

PKI Services part of z/OS security server



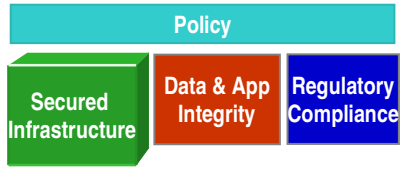
- PKI services included in z/OS security server –no additional cost
- Combines PKI technology with the z/OS qualities of availability & scalability
- Serve as a certificate authority for users, issue and administer digital certificates and provides certificate *life cycle management*
- Leverage RACF for administering system and resource access
- Run in separate z/OS partitions independently of other workloads
- Scalable to drive thousands of certificates
- Secured with zSeries cryptography
- Online Certificate Status Protocol (OCSP) for dynamic checking of certificate status (revocation)
- Use Cryptographic Coprocessor for private keys
- z/OS customers can serve as their own *Certificate Authority (CA)* issuing and administering digital certificates
- Eliminate cost of digital certificates from other sources

PKI Services for z/OS has been certified Identrus compliant at the Identrus 3.1 specification level.

It typically takes a year or more plus a $5 M to $10 M up-front investment for a financial institution to build its own digital CA infrastructure.- Identrus

PKI Services is automatically provided with z/OS Security Server. Full life cycle certificate mgt. z/OS customers automatically get a Certificate Authority with z.

Vanguard Extends the Power of RACF



Security administrators on different platforms can administer RACF on zSeries with an intuitive user interface.

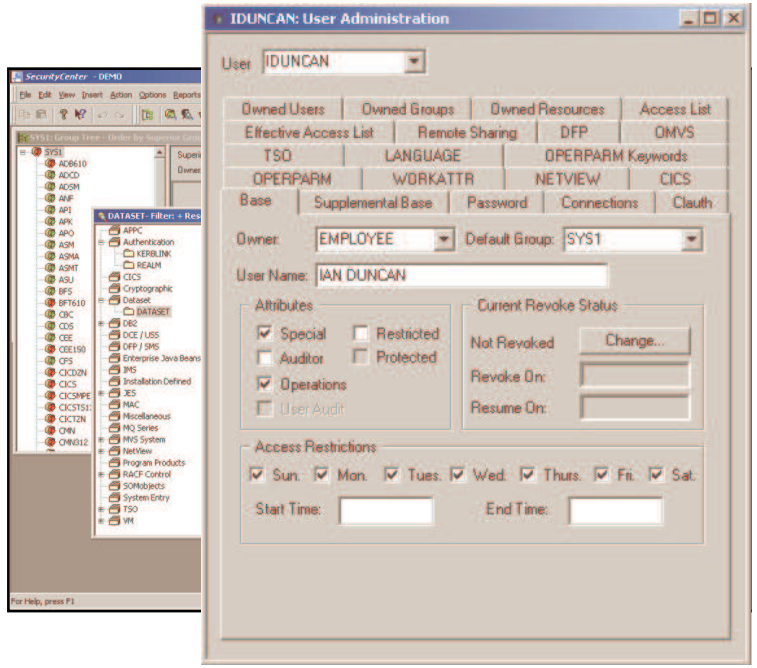
Security Center — A windows interface to IBM's zSeries Security Server. It allows administrators administer RACF using a Windows user interface

Administrator — Automated administration, reporting & analysis tool enhances IBM's RACF as a policy & role-based user-provisioning tool.

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

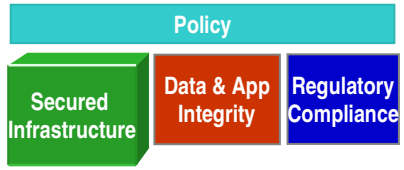
Analyzer — A system integrity, assessment, risk identification, threat analysis and problem rectification solution.

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



Leverage the benefits of RACF using a Windows-based user interface

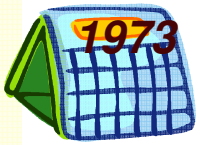
IBM's Unique Integrity Statement



Integrity Statement and Security Statements

- IBM will **accept all APARs* that describe exposures to the System Integrity of MVS** or that describe problems where the installation of the indicated release of any of the programs listed below **introduces an exposure** to MVS System Integrity, as defined below
- A lapse to integrity would allow unauthorized users to circumvent protection mechanisms
- In z/OS unauthorized problem programs cannot
  - circumvent or disable store or fetch protection
  - access an OS password-protected or RACF-protected resource
  - obtain control in an authorized state supervisor state (protect key <8) or Authorized Program Facility (APF) authorized

Since…



***authorized program analysis report (APAR).** A request for correction of a problem caused by a defect in a current program release.

IBM commits to providing system integrity-can other vendors claim the same?

Pillar 2: Protecting Data Integrity

Protect privacy of customer & employee data in transit

Protect Data in Transit

Encryption with key management

Highly secure data transfer

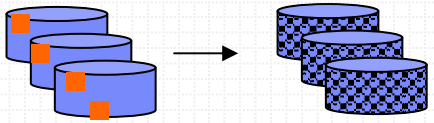
Ensure integrity of data encryption of data at rest

Protect Data at Rest

High volume encryption of data for archival

Preserve confidentiality of information across the enterprise

Protect Data in the Enterprise



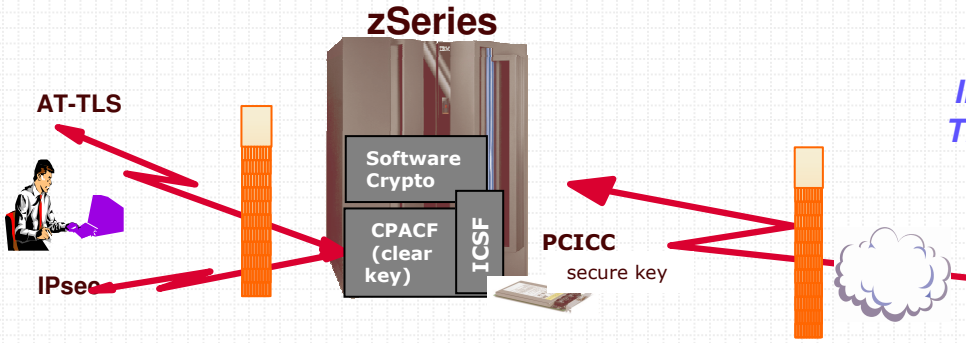
Secured CICS, IMS, WAS data encryption support

Trusted data exchange

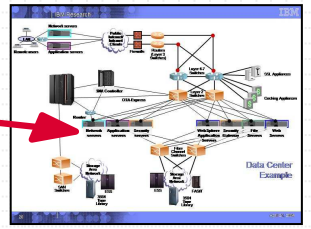
PKI and Digital Certificates

Key Management

PKI/ trusted data exchange with Identrus standards support

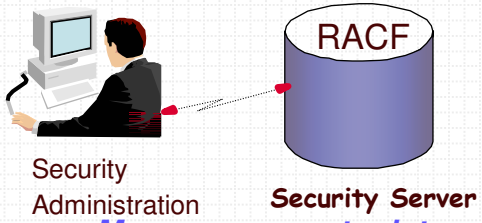


Intrusion prevention, i.e. Trojan horses



Communications Server

Protect Data by Policy

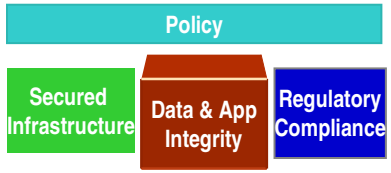


Manage access to data

Data integrity preserved throughout its life cycle

Data Integrity Begins with Encryption

Accelerates encryption and provide secure key services



- New cryptography features offer built in performance and encryption-Fast and Secure
  - CP assist for Cryptographic function (CPACF) built into every CP and IFL
  - Support for DES & 3DES encryption.
  - AES-128 and SHA-256 for z9-109
  - Pseudo Random Number Generator
  - Crypto Express 2 feature on z9-109
  - PCI-X adaptors configurable as coprocessors and/or as accelerators
  - High performance SSL handshakes
  - TKE Smart Card Reader –logically secure channel for master key
  - Tamper resistant
- Cryptographic Coprocessor Security Module FIPS 140-2 level 4 certified

On 16 December 2005, ABN AMRO Mortgage Group acknowledged that a computer tape containing data on approximately 2 million customers — including social security numbers — had disappeared in transit.

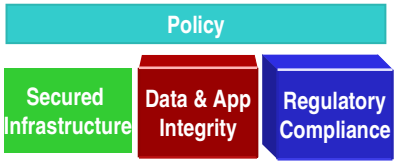
Gartner December 12th 2005

IBM Encryption Facility for z/OS, V1.1
Summary:

- Supports encrypting /decrypting of data at rest
- Can use Public/Private keys or passwords
- Can use hardware compression if transmitting to z/OS system with Encryption Facility
- Allows encryption and compression of dump data sets created by DFSMSdss

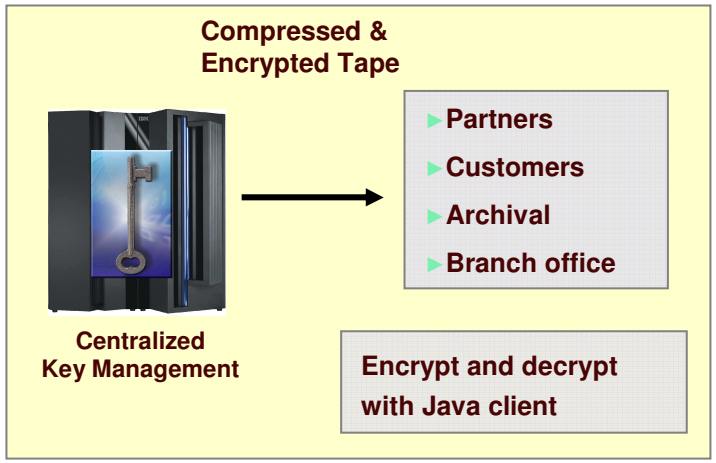
Encryption solutions for data in transit and at rest. Provides privacy, security and reduces risk

Data Integrity- Leading Edge Cryptography



Hardware based encryption for acceleration and secure key services

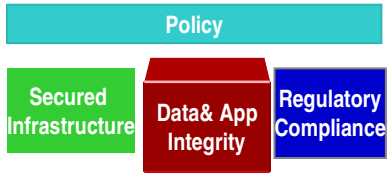
- **z/OS based centralized key management**
  - ICSF helps to protect and manage encryption keys, generates keys, managing keys based on customer policies, and recover keys; single point of management.
  - Other solutions offer encryption only
  - Enables long-term key management for archived data, remote sites, sharing data externally
  - Creates trusted exchange with other systems with support for standards based encryption
- **Integrated z/OS security features**
  - RACF for authorization and authentication
  - Provides transparency from application into cryptographic functions
  - Cryptographic features are virtualized
- **Enables third-party programming**
  - User defined extensions callable from applications
- **Extensible**
  - Java client allows partners/customers to decrypt & encrypt tapes for exchange with z/OS systems



Over 90% Of Companies Regularly Expose Employee And Customer Data

Built in encryption, compression with key management

Multi Level Security Access (MLS)

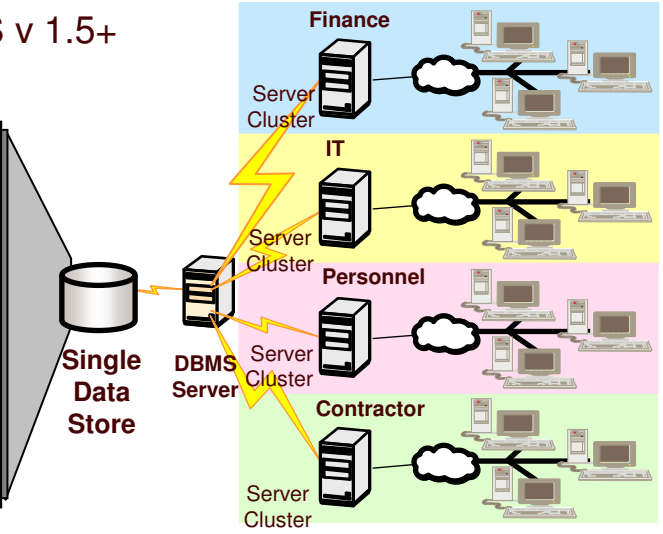


Definition: The concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization

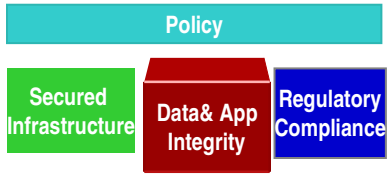
- MLS represents a mechanism to classify data based on both hierarchical security levels combined with a non-hierarchical security categories
- A single secured repository features different sensitivity attributes accessible by users with varying clearance levels
- Eliminates need for duplicate IT infrastructures, silos, redundant software
- Implemented through RACF with DB2 UDB for z/OS v8 and z/OS v 1.5+
- DB2 also supports row level encryption

Single image of data is sharable by multiple enterprise departments with different levels of "need to know"

SECURITY LABEL	Col 1	Col 2	Col 3
Personnel	234	USA	50%
Finance	198	France	23%
Personnel	2	UK	9%
Finance	234	USA	11%
IT	87	USA	14%
Contractor	23	UK	20%
IT	223	USA	10%
Contractor	45	Canada	29%



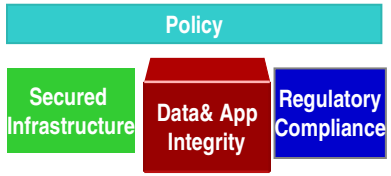
MLS Leverages z/OS to Simplify Security



- MLS is integrated with z/OS leveraging the value of virtualization
- Eliminates need for redundant, isolated infrastructures to achieve security
- No more difficult to maintain custom SQL views
- One consolidated DB2 database with security provided by DB2 leveraging RACF security -share resources with mixed security levels in one image
- MLS provides additional functions as well:
  - The system does reuse a storage object until purged.
  - The system labels hardcopy with security information.
  - The system creates audit records around security events
  - Can mask names of data sets, files and directories from users without proper access
  - Prohibits user declassification (Write-Down) of data except with explicit authorization to do so

MLS reduces risk and helps with compliance

DB2 UDB for z/OS v8+ Security



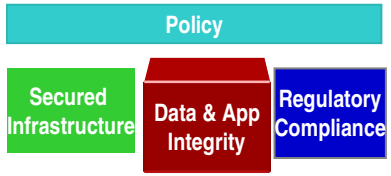
Improved security

- Quality of end to end security
  - Row level security
  - Leverages RACF and zSeries security
- Common Criteria in process
- Improved auditing
- Encryption
- Rolling maintenance & upgrades
- Trusted Database roles vNext
- Trusted context vNext

- Gartner published an advisory on its Web site just days after Oracle's latest quarterly patch cycle, which included a total of 103 fixes with 37 flaws in Oracle database products.
- "the range and seriousness of the vulnerabilities patched in this update cause us great concern..."

  Date: 23 January 2006

DB2 UDB value is one of availability and integrated security, not one featuring rapid repair and a commodity server approach



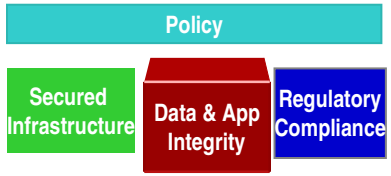
Security: CICS

- CICS security managed by security profiles defined in RACF
- CICS users authenticated by RACF
- Users can be authenticated by userid and passwords or through SSL certificates
- CICS also provides transaction security
- Transactional integrity
- Resource security applies to CICS resources used by a CICS transaction
- System programming commands protected
- Thread-safe mode:
  - Isolates user transaction storage from other user-key transactions
- Violations logged to SMF

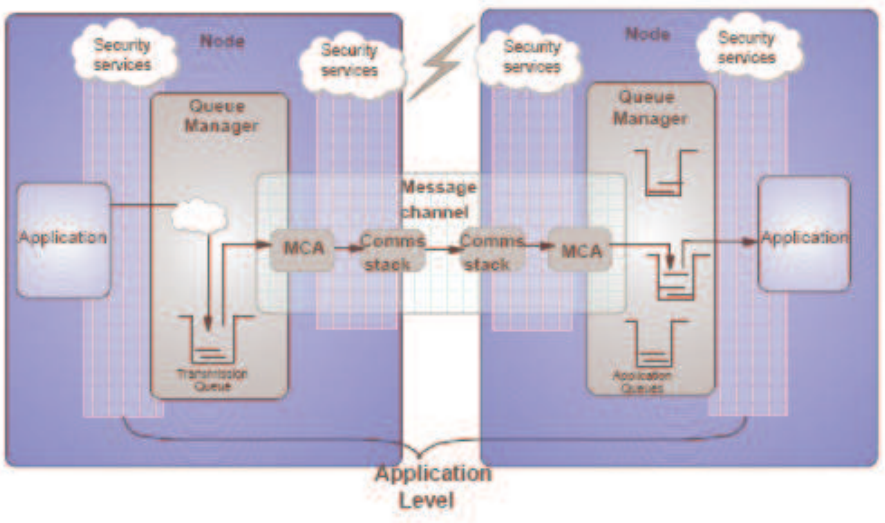
CICS handles over 30 billion transactions/day!

Middleware uses RACF to protect transactions and other defined resources

Security: Websphere MQ

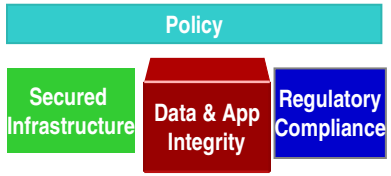


- MQ also exploits the SAF exit of RACF and macros
- Queues, commands, MQ resources & other objects protected
- Support for Secure Socket Layer (SSL)
- Channels for messaging between queues secured; data Integrity over the network is provided using SSL
- Standard auditing
- Application level security provided between the application and queue manager such as queue level encryption.
- Access control facilities control which users may access Queue Manager, even though they may access application libraries.



MQ Security based on standard z constructs provides value to MQ both in Messaging and also as an ESB technology.

Integrated IMS Security



- IMS transactions and resources also protected by RACF
- Data is protected at the row level for DB2 and the segment level for IMS.
- IBM Data Encryption for IMS and DB2 Databases
- IMS Transaction authorization works with RACF:
  - IMS post version 1.9 will use RACF instead of the Security Maintenance utility (SMU)
  - At *control region* initialization, RACF builds profiles for transactions to be checked against user's privilege
  - At *transaction authorization time,* RACF compare transaction profiles in storage against the user access privilege to return authorized or unauthorized indication
  - IMS offers a protected view of data through the combined Program Specification Block (PSB) and Program Control Block (PCB)

RACF provides:

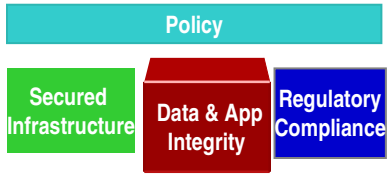
. IMS user verification
. IMS trans. authorization
. Authorization to IMS control region resources

Over 50B transactions per day run through IIMS

IMS customers have run over 3000 days without an outage

IMS benefits from transaction security through RACF

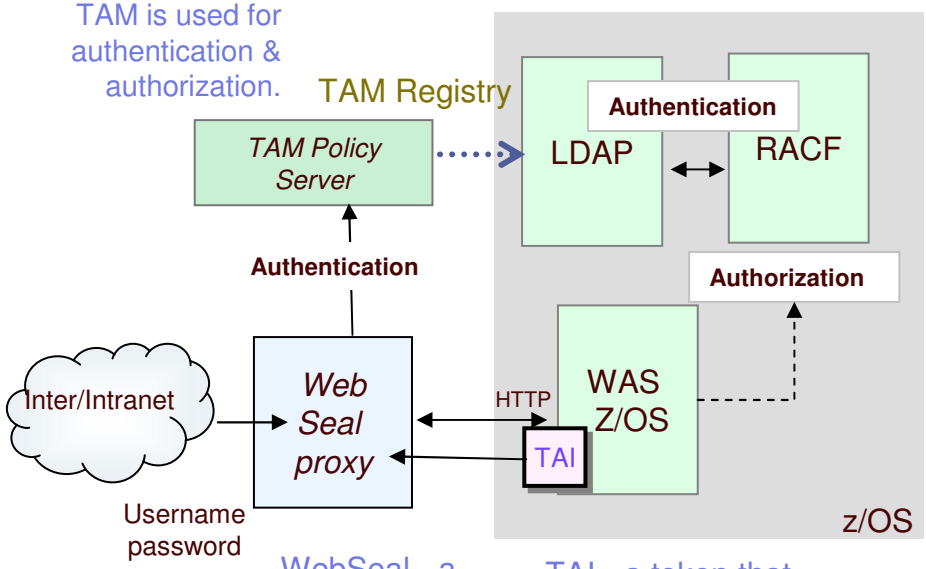
WAS Security on z/OS



- Websphere security can use a combination of RACF based security along with J2EE security
- Websphere integrates with RACF via the WebSEAL proxy server providing a policy based model for security of EJB and web resources
- Authentication is done against z/OS LDAP, which checks passwords against RACF
- Websphere for z/OS uses RACF for authorization
- RACF provides consistent policy
- RACF protects files, configuration data and TCP/IP resources
- Proof of concept for SOA based security

WebSphere uses LDAP and RACF for Authentication

TAM is used for authentication & authorization.

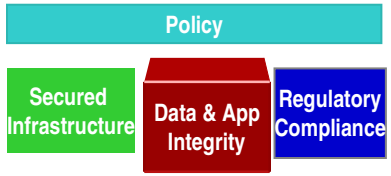


WebSeal - a SSO solution for WAS for z/OS and interfaces with TAM.

TAI - a token that integrates 3rd party security server with WAS and establishes trust to WebSeal

WAS benefits from RACF and z-based security & LDAP authentication

zSeries Advantage for Linux



What does Linux provide?

- Linux security is not the same as z/OS
- Linux on its own does not offer granular resource access or auditing
- With an open source heritage – many third party point products exist to address gaps
- **BUT …**Linux for zSeries can take advantage of zSeries additional security capabilities built into the architecture…..

What does zSeries provide?

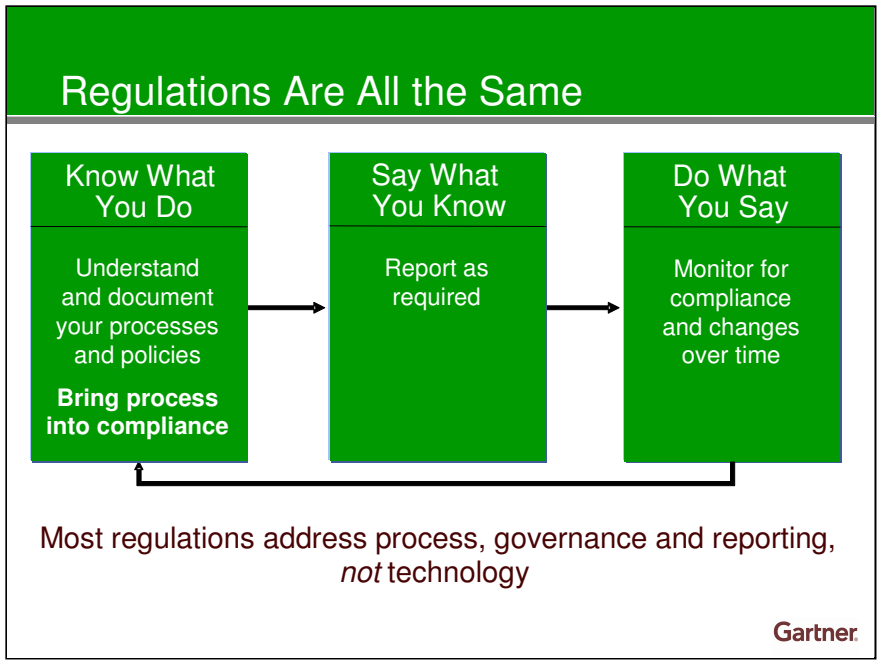
- Image Isolation
  - LPAR
  - Linux under z/VM
- Encryption of data with and accelerated performance
- Common Criteria rating on z
- SSL-secured network communications
- Centralized Authentication
- Public Key Infrastructure (PKI)
- Secured communications/hipersockets

- SUSE Enterprise Server 9 achieved EAL4+
- Red Hat Enterprise Linux 3, Update 2, at EAL3

Leverage the benefits of open source with the resiliency of the z architecture

Pillar 3: Addressing Regulatory Compliance

Regulatory Compliance



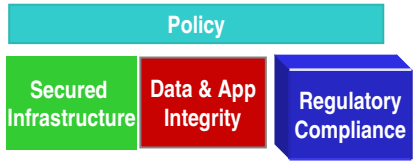
- "IT Security is like **spinach** — A nutrient necessary for well-being, but which few enjoy. However, the advent of **compliance** offers a rare opportunity for businesses to improve both **security** and the benefits derived from it.
- IBM in general, and the **System z9 in particular,** deserve credit for delivering superior security over the long term and for adapting to **business compliance** with new **security solutions that continue to stand out from the competition.**"

Infrastructure Associates 15 November 2005 "IBM Mainframe Encryption: Upgrading the Gold Standard for Security." Wayne Kernochan

"Sixty-one percent of companies will increase spending on security technologies to support compliance with SOX"

Forrester, " IT Execs Wake Up To Sarbanes-Oxley Compliance", 05/23/04

Reducing Operational Risk



- Basel II is a wake up call for banks and financial institutions to improve information security and risk mgt.
- Protection of privacy and confidentiality very important to multiple industries
- Manage security and integrity of financial data for financial reporting
- Maintain operational resiliency
- Maximize availability
- Improve security controls in applications and IT
- Reduce people, process and technology risk

REGULATIONS

• Basel II -proposes methods for banks to calculate capital provisions needed against credit, commercial, & operational risk- the risk of loss resulting from inadequate or failed internal processes, people or systems, or from external events.

• Sarbanes-Oxley - Strengthen financial reporting, internal controls **(security),** transparency

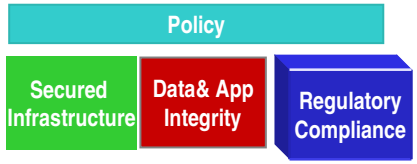
• HIPAA - **Secure** medical records & usage

• Patriot Act - Prevent **fraudulent** use of the financial system to support illegal activities

• Gramm-Leach-Bliley Act - Protection of personally identifiable financial information **(confidentiality)**

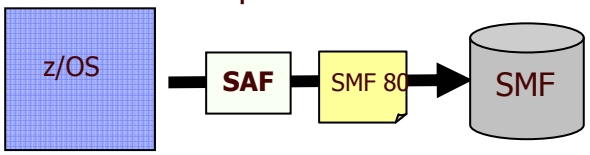
• SB 1386 mandates the disclosure of **security breaches** where private information of has been compromised

Auditing Needs



- RACF records system events, enabling monitoring of users and their activities; reports on attempts to perform unauthorized actions
- RACF cuts SMF records for post processing and provides a Report Writer, XML interfaces for reporting
- The report describes attempts to access RACF-protected resources by user ID, of successful access, or security violations
- Common approach avoids auditing integration and compliance challenges posed by inconsistent distributed systems logging
- IBM has built auditing capabilities into all its subsystems which cut records which can be used for audit purposes

RACF enables consistent auditing - critical for compliance needs.

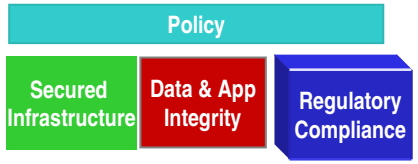


On a typical day, the security team logs 38,000 attempts – by unauthorized individuals or automated probes – to access the state's networks. **That's about one every 2.3 seconds.**

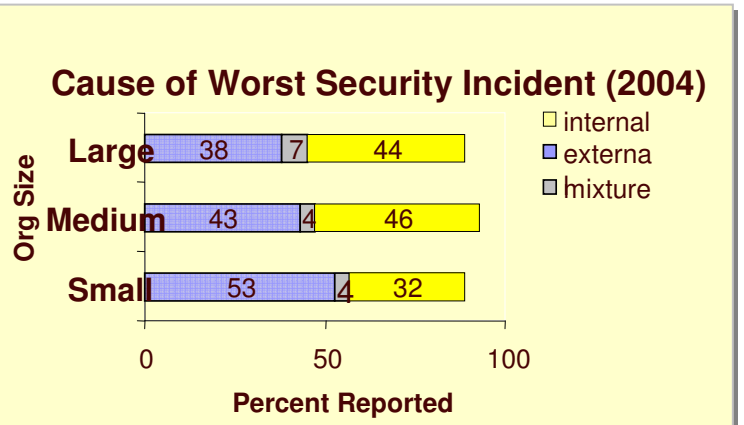
"Defending Data: a Never-Ending Vigil"
Todd Spangler quoting Dan Lohrman, Chief Security Officer for the State of Michigan Baseline, 2004

Provide improved consistent auditing and reporting critical for today's compliance needs

Integrated Health Checker - For Integrity



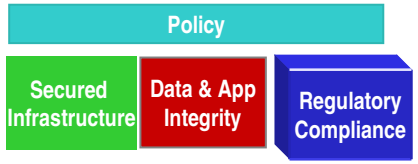
- Identifies potential configuration problems over an IPL
- Health checker consists of:
  - A framework to manage scheduling, processing, reporting of health checks
  - Checking mechanism that evaluates software settings
  - Extensible solution - authored by IBM, ISVs, or users.
- RACF supplies checks for use by the IBM Health Checker for z/OS
  - Checks that RACF is protecting z/OS **providing additional protection**!
  - Checks APF libraries & RACF data sets
- Interim checking between releases
- Integrated into z/OS 1.7



2004 PwC ISBS UK based study

The percent incidents due to internal causes accounted for a significant percentage of all security breaches.

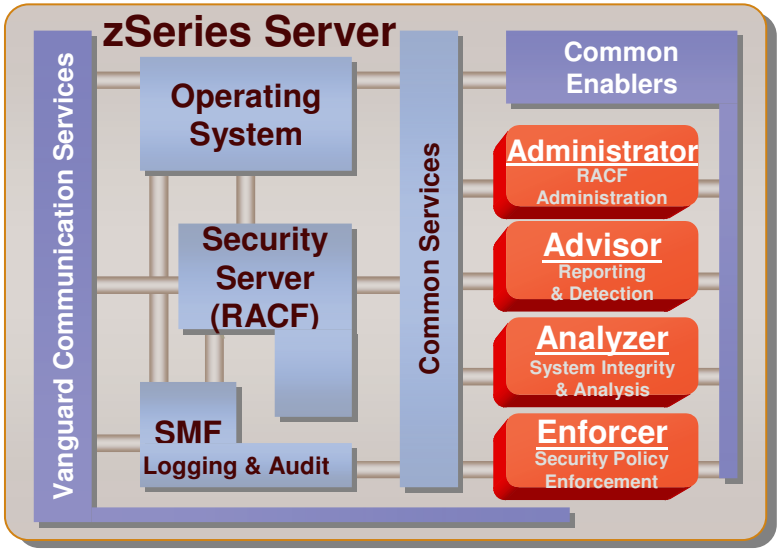
Helps avoid potential security problems resulting from introduction of invalid systems software



Vanguard Enforcer

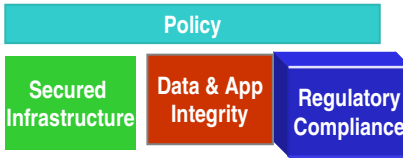
Enforcer is an intrusion detection and management solution for the mainframe

- Enforcer protects critical data and resources by ensuring that standards, policies, rules and settings are in force
- Helps document existence of controls for regulations
- The baselines contain security policies and rules for the system being monitored
- Enforcer scans the operating system and RACF database at intervals comparing this against baselines
- If discrepancies are found, Enforcer logs the discrepancy for further analysis, notifies individuals and takes corrective action



"I do not believe I would have been able to survive the SOX audit without the Vanguard Analyzer."

Gary Godek
Information Security Administrator
Eaton Corporation



Protecting Operational Integrity

SMP/E - an integral tool for systems software integrity

- Helps ensure that the right software is actually installed
- Provides value from an audit and integrity perspective
- Difficult to introduce corrupted code into the system
- Reduces likelihood of inadvertent errors
- Rigorous process for introducing updates, fixes
- Proven procedures
- Secured communications
- Integration with RACF

IDM Net Australia, Sept 20 2005.

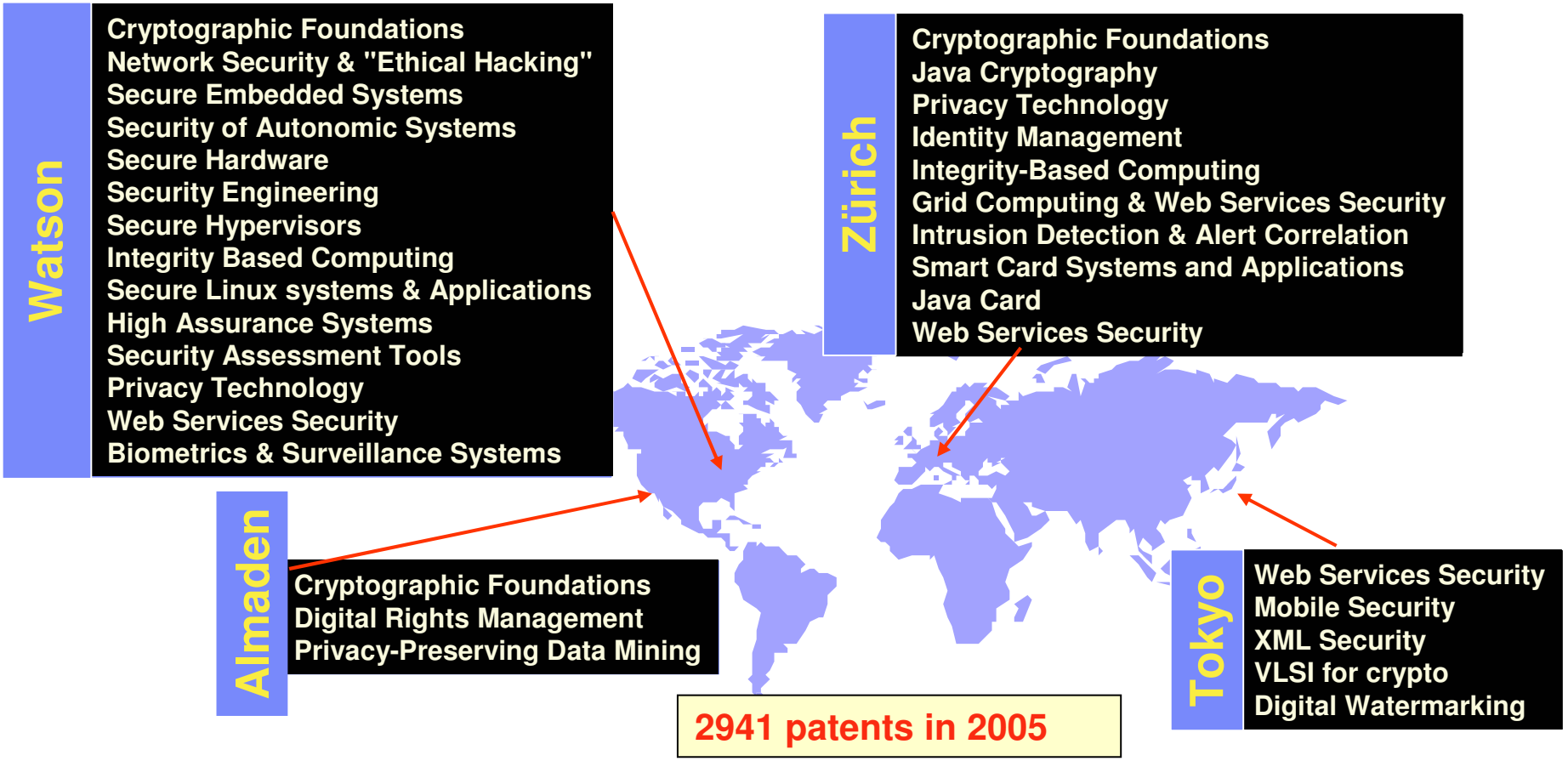
[A] recent case involved a prison officer who upon applying to see his police file received **1,000 files on other people who shared his surname**, which also included the names and addresses of victims and alleged offenders.

While the breach was due to **human error and was not malicious,** the **damage it caused was far reaching**, with major **legal ramifications.**

SMP/E maintains all the co-requisite and prerequisite information about IBM products and services.

Reduce the risk of systems software maintenance introduced corruptions

Continued Innovation In Security



On November 15th, 2005, the White House named IBM a winner of the U.S. National Medal of Technology- - the highest honor awarded by the President of the United States for technology innovation

Continuing the evolution of security

Creating a "Secure Vault" for Heterogeneous Environments

- Today, up to 99.999% availability* across zSeries resources to avoid both planned and unplanned outages
- Minimizes interruption through management of system resources based on business priorities
- Enables End-to-end integrity of zSeries data
- Can secure at a granular user level

Initial Focus*

- Enable asset and resource associations to be mapped by business function.
- Extend GDPS to heterogeneous environments and single site environments.
- Extend zSeries ability to provide seamless integration of Security through utilization of open technologies.

Extension of on demand value*

- Provide capability to monitor business functions and identify appropriate recovery actions.
- Extend zSeries resiliency into heterogeneous environments through utilization of common interfaces.
- Position zSeries to lead in managing heterogeneous assets and resources.

Future Vision*

Become the *"secure vault"* across the enterprise.

- Become the "world's most resilient enterprise" through zSeries autonomic management based on business policy support for heterogeneous assets and resources.
- Become the ***enterprise trust authority*** through integration of zSeries Security leadership with the ODOE.

Note : Based on Parallel Sysplex implementation

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The Security Value of zSeries is Unmatched

- ✓ **Resiliency**
- ✓ **Security built in**
- ✓ **Never hacked**
- ✓ **Policy based**
- ✓ **Advanced Cryptography**
- ✓ **Common Criteria**
- ✓ **World-class Services**
- ✓ **Integrity Statement**
- ✓ **Continued research**
- ✓ **Throughout the stack**

And customers agree…

"Mainframes are a special breed of computer,..They're more scalable, have high integrity and don't make mistakes, which is something other servers don't have. They're very secure, and they come from what is now a 40 to 50-year heritage."
IBM Offers Mainframe Makeover TechNewsWorld. 7-27-05

"The overriding issues are often found at the operating system-level itself," … "You have so many break-ins on the NT boxes, and companies don't have time to patch or are even unaware of the vulnerabilities. …."
Moving Cobol to the Web safely proves challenging
IT World Canada September 28 2005

For …

The Most Secured Infrastructure

Unmatched Data and Application Integrity

Business Compliance and Risk Management

Useful Sites

- **www.ibm.com/servers/eserver/zseries**
- **www.ibm.com/servers/eserver/zseries/zos**
- **www.ibm.com/servers/eserver/zseries/zos/racf**
- **www.ibm.com/servers/eserver/zseries/zos/security**

zSeries SWG Competitive Project Office
https://w3-03.ibm.com/sales/competition/compdlib.nsf/pages/swgcpo