IBM eServer™

IBM zSeries and z/OS Security Facilities
- or -
Mainframes: Are They Secure?

Mark Nelson, CISSP
z/OS Security Server (RACF) Design and Development
IBM Poughkeepsie

Trademarks

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

IBM*
IBM logo*
IBM ^
DB2*
e-business logo*
Enterprise Storage Server
ESCON*
FlashCopy
HiperSockets
Multiprise*
OS/390*
Performance Toolkit for VM
Resource Link
S/390*
Tivoli*
Tivoli Storage Manager
VM/ESA*
VSE/ESA
xSeries*
z/OS*
z/VM*
zSeries*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries
UNIX is a registered trademark of The Open Group in the United States and other countries.
Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.
SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

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

Notes:

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

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

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

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

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.

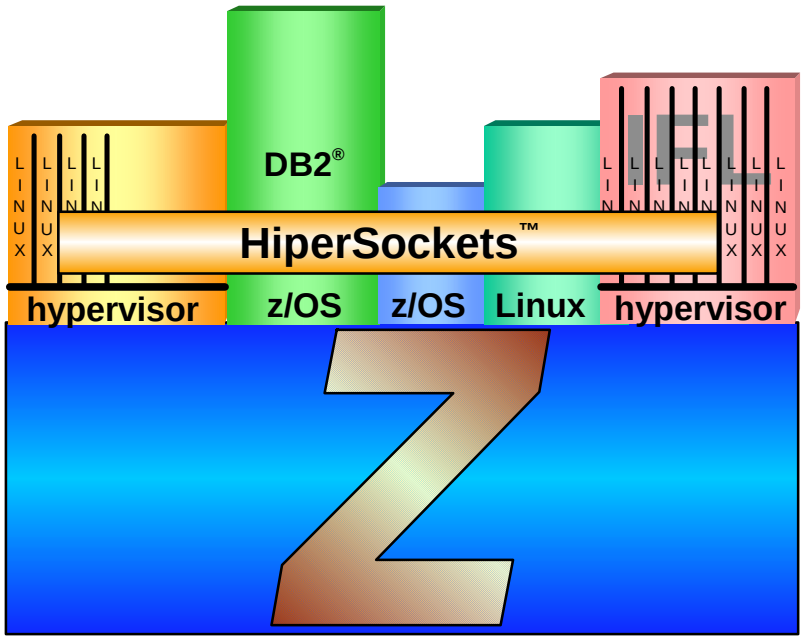
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

- zSeries Hardware
  - Virtualization: Partitions and HiperSockets
  - Cryptographic facilities
- z/OS
  - z/OS Security Server
    - RACF
    - PKI Services
    - LDAP
    - Distributed Computing Environment (DCE)
    - Open Cryptographic Enhanced Plug-ins (OCEP)
    - Network Authentication Services (Kerberos)
  - Communications Server
    - IP Filtering
    - Controlling Access to TCP/IP Resources Using RACF
    - Intrusion Detection Services

zSeries servers - Logical Partitioning

Deploy a wide variety of applications easily in secure, isolated partitions

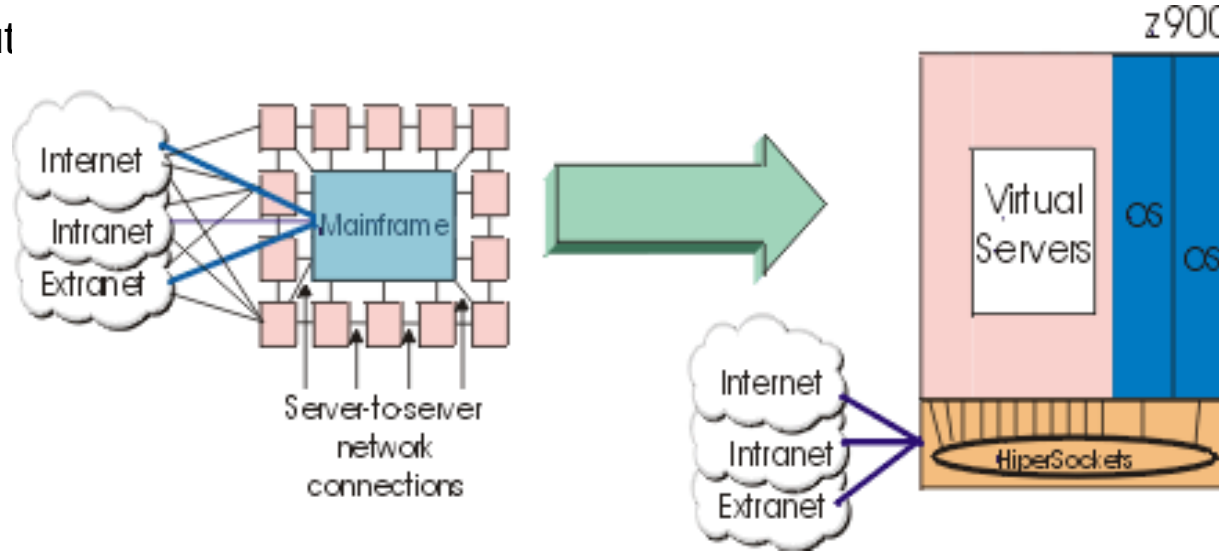


- Up to 30 logical partitions in a single zSeries server
- Processor independent
- Each partition completely isolated
  - EAL4 security rating for zSeries
- Allocate memory / communication resource among partitions
- Run z/OS®, Linux, z/VM®, VSE/ESA™, TPF in any combination

zSeries servers - HiperSockets - Inter-partition communications

Simple, secure, efficient cost effective access to data and applications

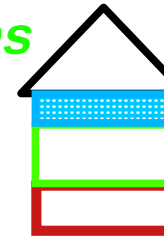
- In memory inter-partition communication network
- Simple yet cost effective
  - Helps to reduce/eliminate complex and costly external network
- Secure
  - Inter-server communication within zSeries server
- Efficient
  - Up to 13 times more throughput than Gigabit Ethernet between database and application servers with HiperSockets

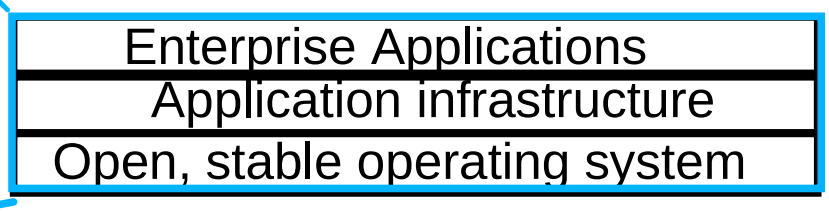


Linux for zSeries

A stable, open operating system environment for enterprise applications

- Fast operating system offering:
  - Stability
  - Security
  - Economical
  - Evolves rapidly
- Wide range of infrastructure tools / enablers from ISV's and Open Source
  - System management solutions
  - Infrastructure and middleware solutions
  - Enterprise Applications





The most sophisticated and complete suite of hypervisor function available

IBM ^ zSeries 990 (z990) provides a greater degree of balanced resource to the hypervisor for use by Linux and other OS's

Linux is designed to be hardware independent, ***but*** when running Linux for zSeries, it can retain the advantages of the openness of Linux, while leveraging the flexibility and manageability of the sophisticated hypervisor function, while inheriting the strength, robustness, and security of modern mainframes

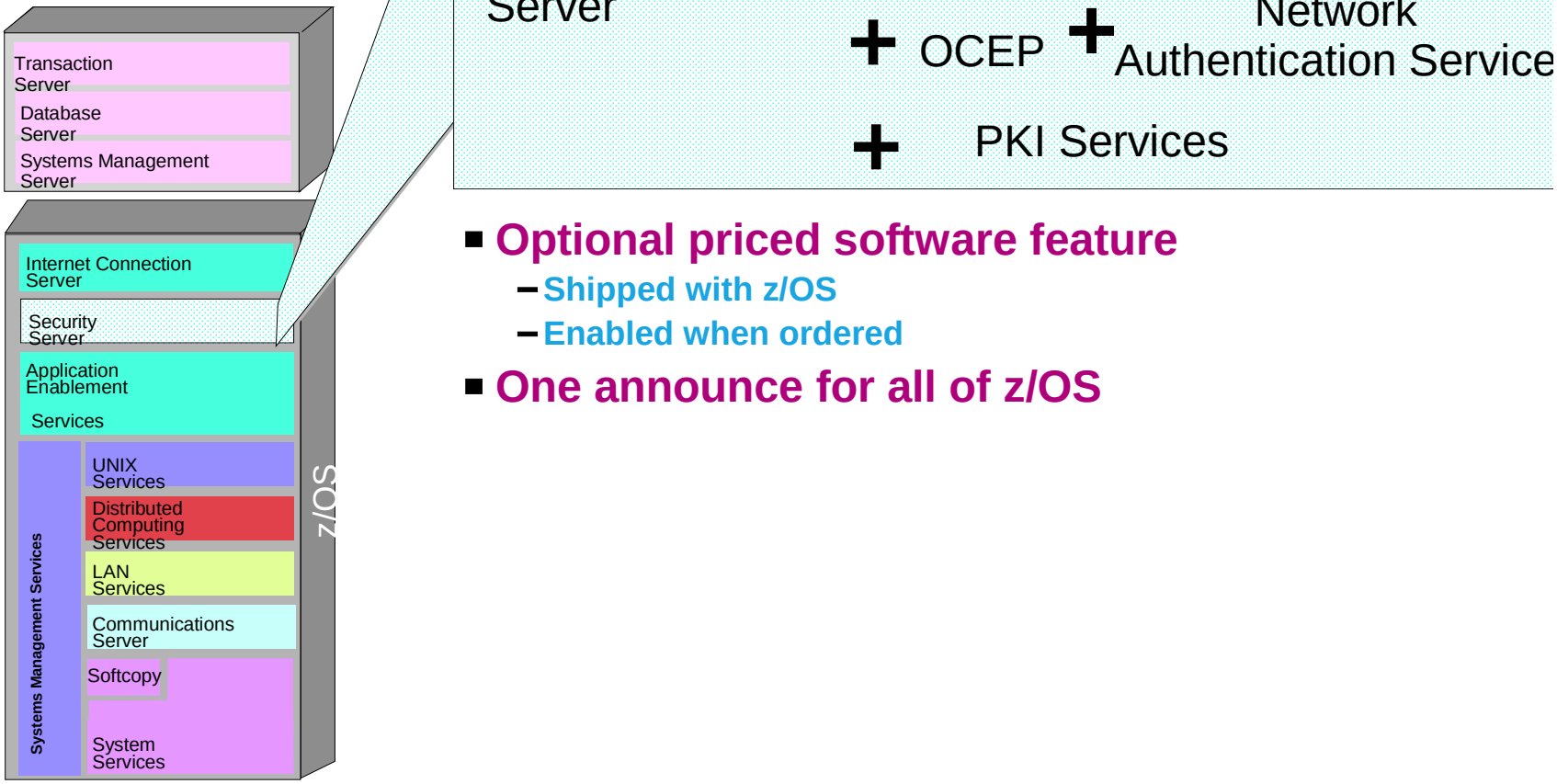
Cryptographic Facilities on zSeries

- Cryptographic Coprocessor Facility (CCF)
  - Available on CMOS and zSeries processors
  - Limited to two per CPU
  - Tamper resistant, tamper evident
  - Can support T-DES, DES, CDMF, RSA, and DSS
- Peripheral Component Interconnect (PCI) Cryptographic Coprocessor ("PCICC")
  - Assists the CCF
  - Tamper resistant, tamper evident
  - May have up to eight per CPU
  - Programmable
- PCI Cryptographic Accelerator ("PCICA")
  - zSeries only
  - Requires z/OS R2 or later
  - Two engines per card, up to six cards per CPU
- New crypto instructions in zSeries (z990) architecture

Cryptographic Facilities on zSeries...

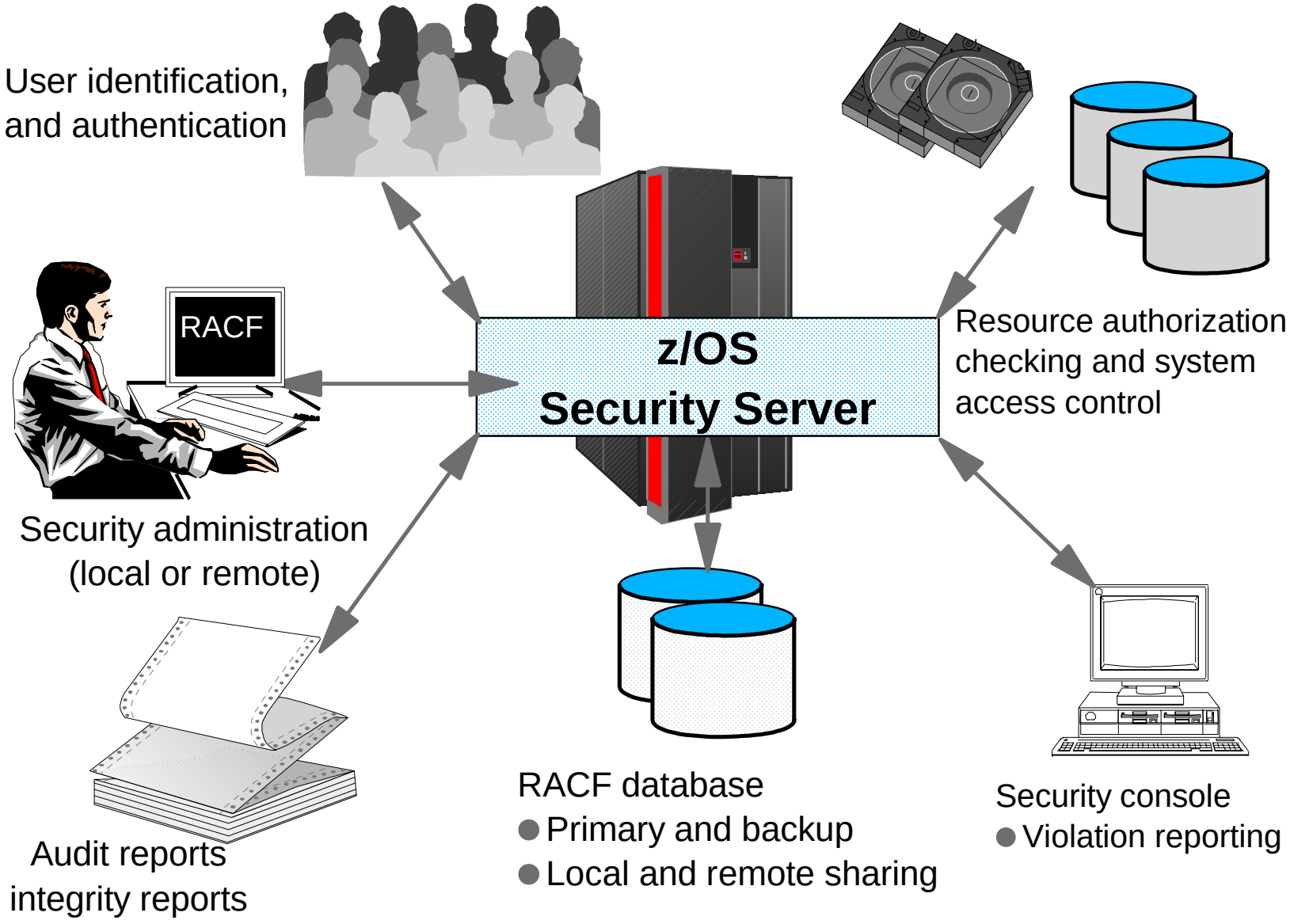
- CCF, PCICC, and PCICA may be shared across LPARs
- Managed through the Integrated Cryptographic Service Facility (ICSF) of z/OS
  - Controls the loading of system master keys
  - Provides APIs for application use

z/OS Security Server

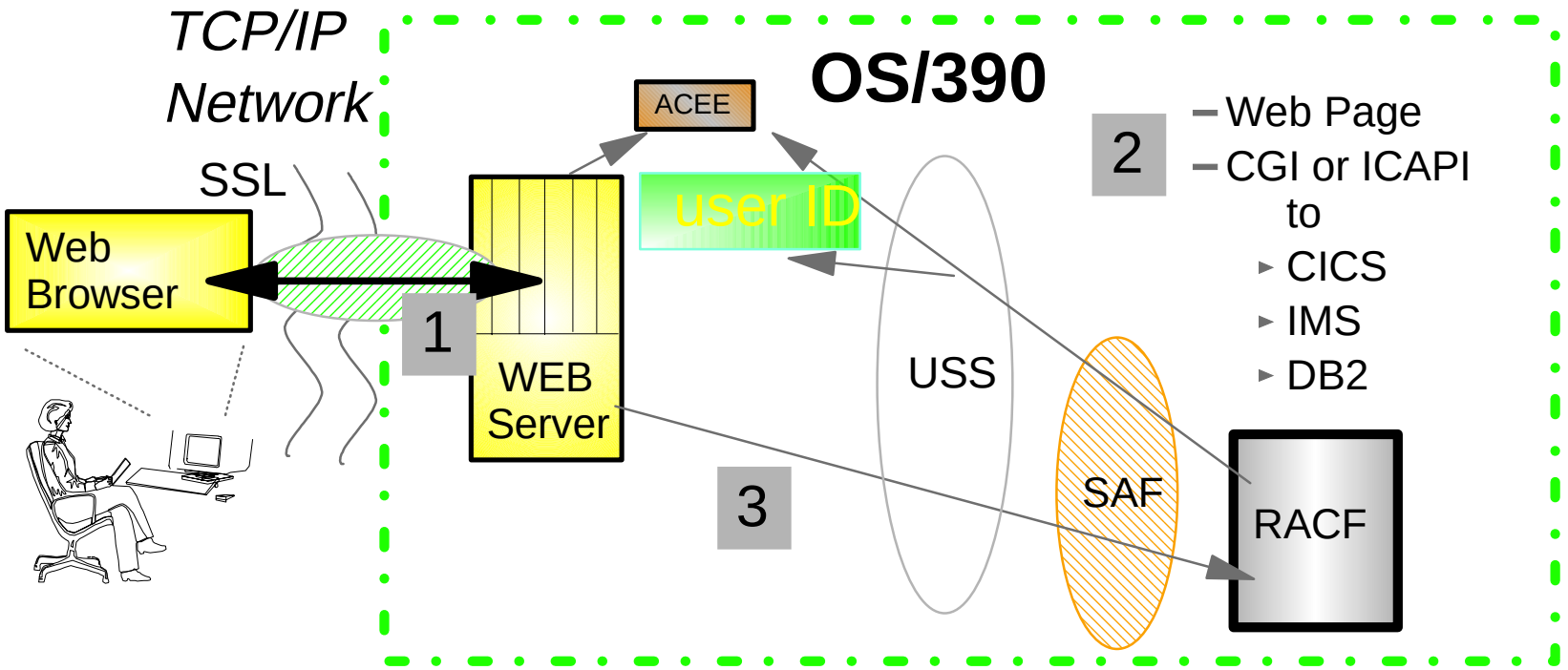


- **Optional priced software feature**
  - **Shipped with z/OS**
  - **Enabled when ordered**
- **One announce for all of z/OS**

RACF



Digital Certificate Support in RACF



1- User authenticates to Secured Sockets Layer (SSL)

2- User requests OS/390 secured resource via browser

3- Web Server invokes RACF via USS to build local security context (ACEE),

passing SSL validated certificate instead of prompting for user ID & password

PKI Services

- Component of the z/OS Security Server
  - Always enabled but closely tied to RACF
- Complete Certificate Authority (CA) package
  - Full certificate life cycle management
    - User request driven via customizable web pages
      - Browser or server certificates
    - Automatic or administrator approval process
      - Administered using same web interface
    - End user / administrator revocation process
- Manual - "z/OS Security Server PKI Services Guide and Reference"

z/OS PKI Services Architecture

- HTTP Server
  - Provides browser/CGI interface for end-users and administrators
    - Web page logic defined in certificate templates file
    - CGIs - Read template file, control flow
      - Optional customer provided exit - pkiexit
      - Invoke z/OS PKI Services through SAF interface R_PKIServ
- R_PKIServ - SAF callable service backed by RACF (or other)
  - End-user functions - Request, retrieve, verify, revoke, or renew a certificate
  - Administrator functions - Query, approve, modify, or reject certificate requests, query and revoke issued certificates
  - Interface to call PKI Services
  - SMF auditing
- PKI Services Daemon
  - Services threads for incoming requests
  - Background threads for certificate/certificate revocation list (CRL) issuance
  - VSAM DBs for requests (ObjectStore) and issued certificate list (ICL)

LDAP

- Lightweight Directory Access Protocol
  - De-facto standard (TCP/IP-based) for directory management
  - General purpose directory server for z/OS
  - LDAP V3 Protocol support
  - Utilizes DB2 as the backend store
  - Allows the use of RACF for user, group, and connection information

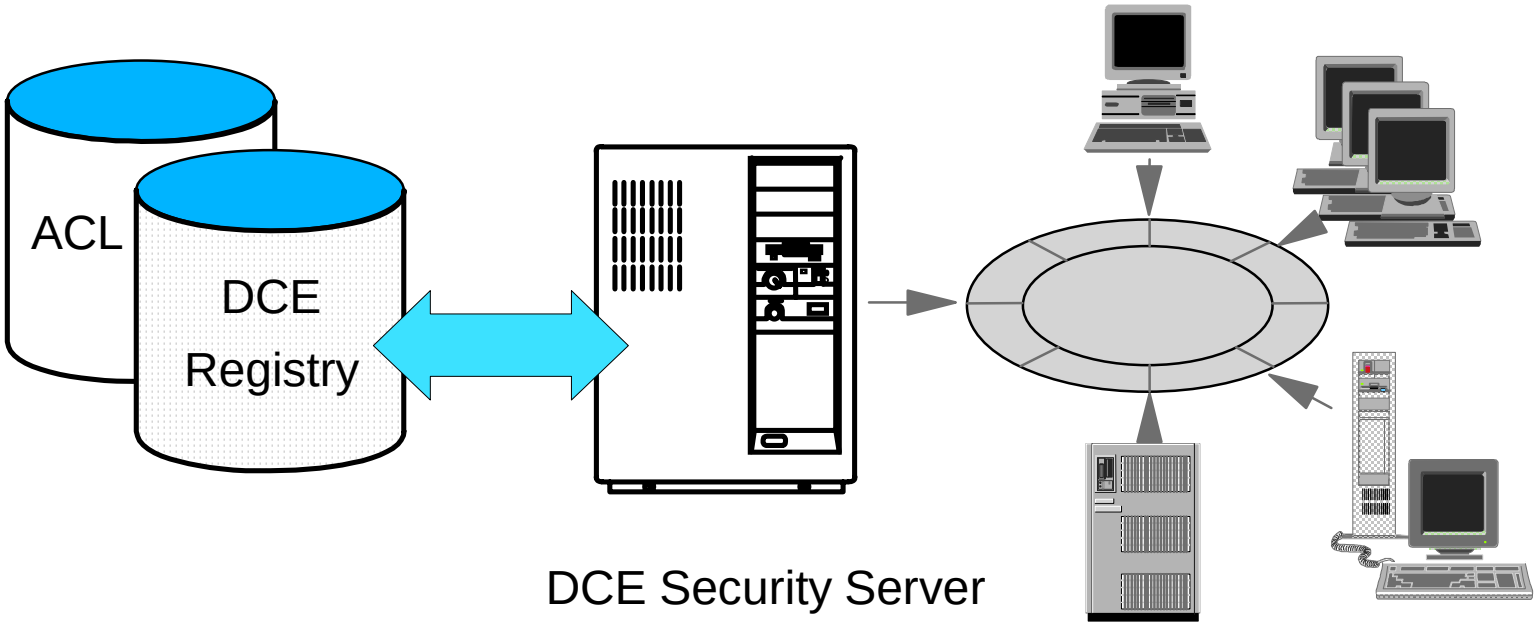
Distributed Computing Environment

authenticated RPC

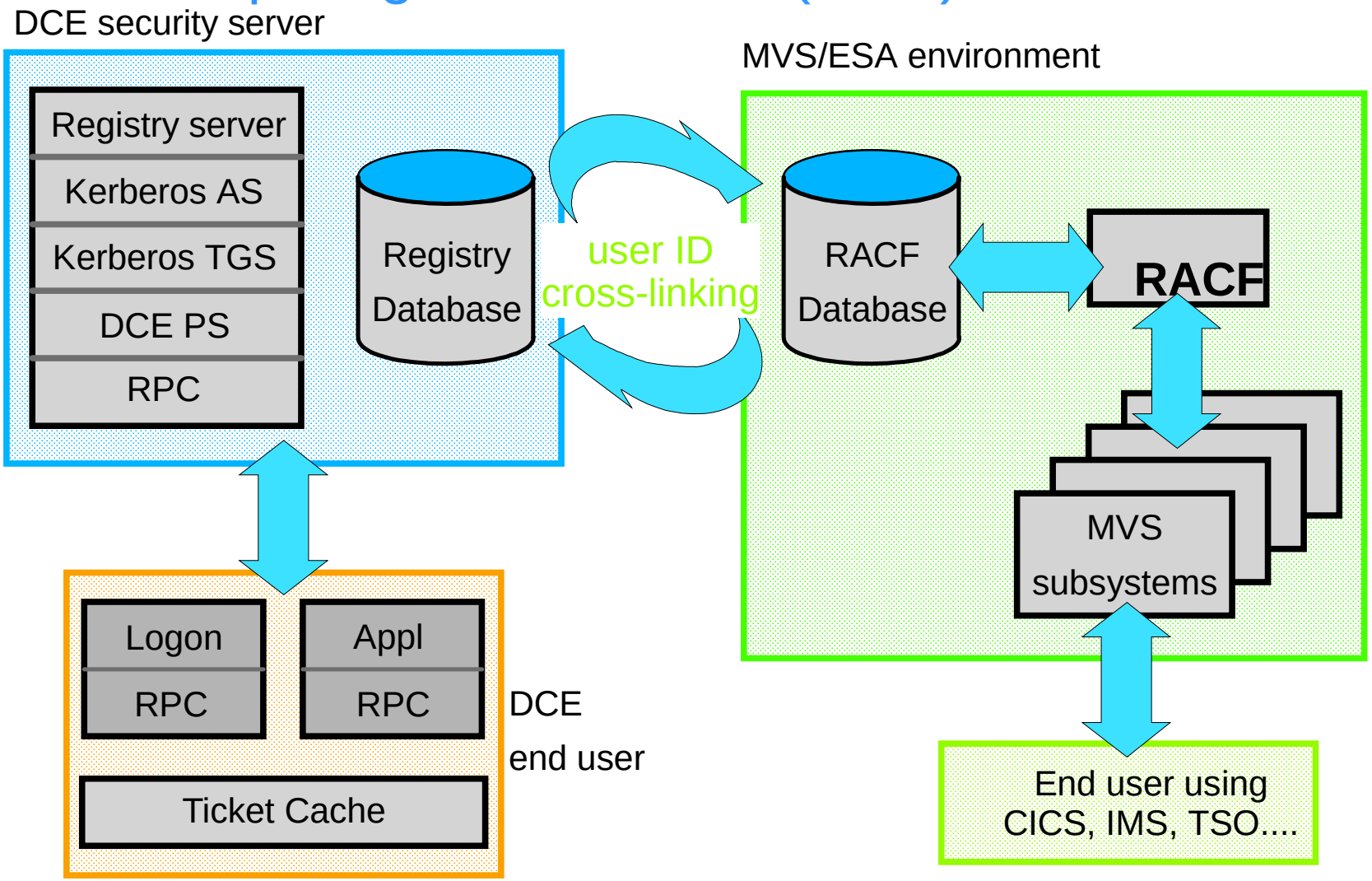
- Authentication of principals
- Verification of data integrity
- Provision for data privacy

} via Security Server

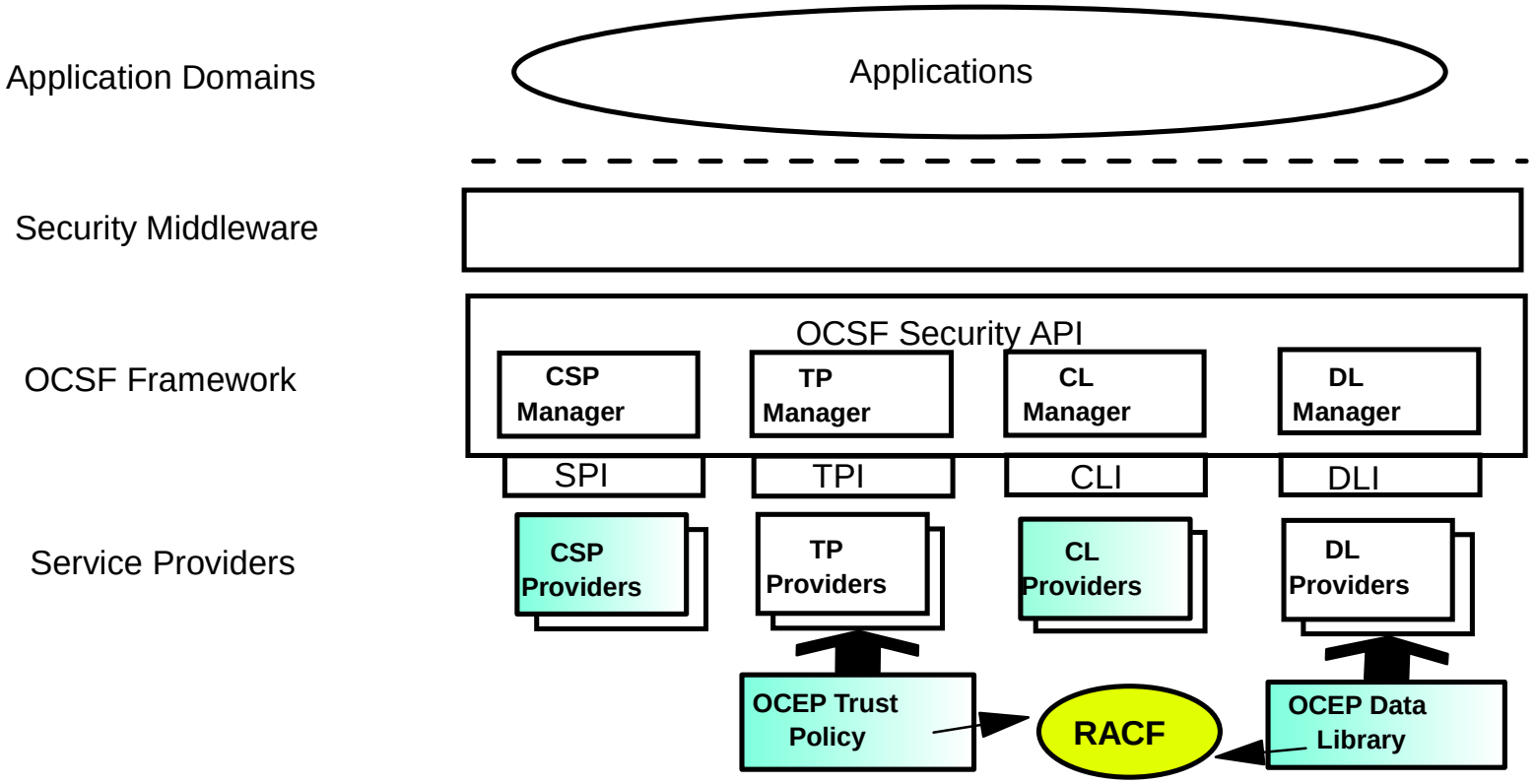
- Authorization of principals for use of resources → Up to applicatio



Distributed Computing Environment (DCE) and RACF



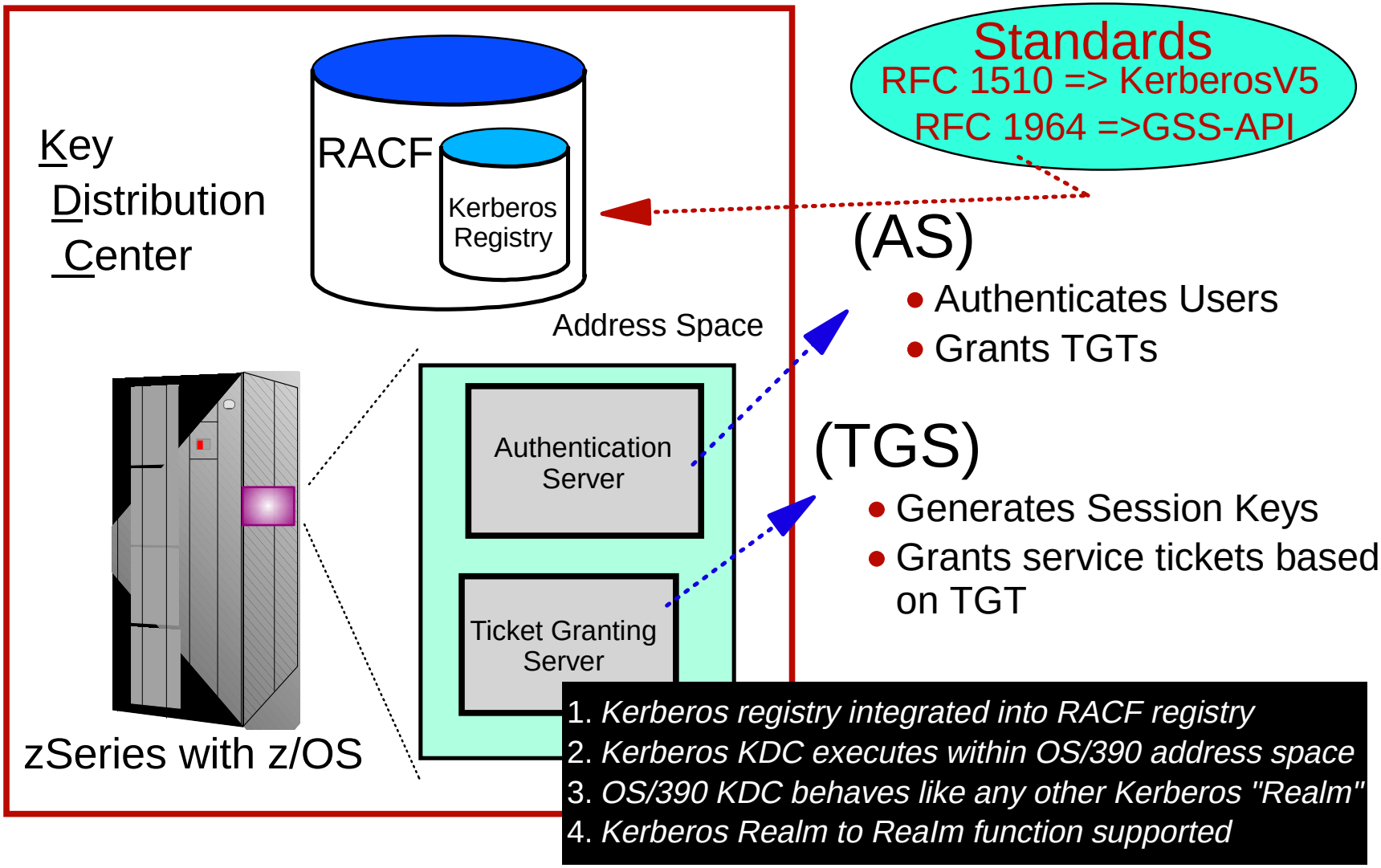
Open Cryptographic Support Facility (OCSF) and Open Cryptographic Enhanced Plugin (OCEP)



OCSF part of z/OS Cryptographic Services (base element)

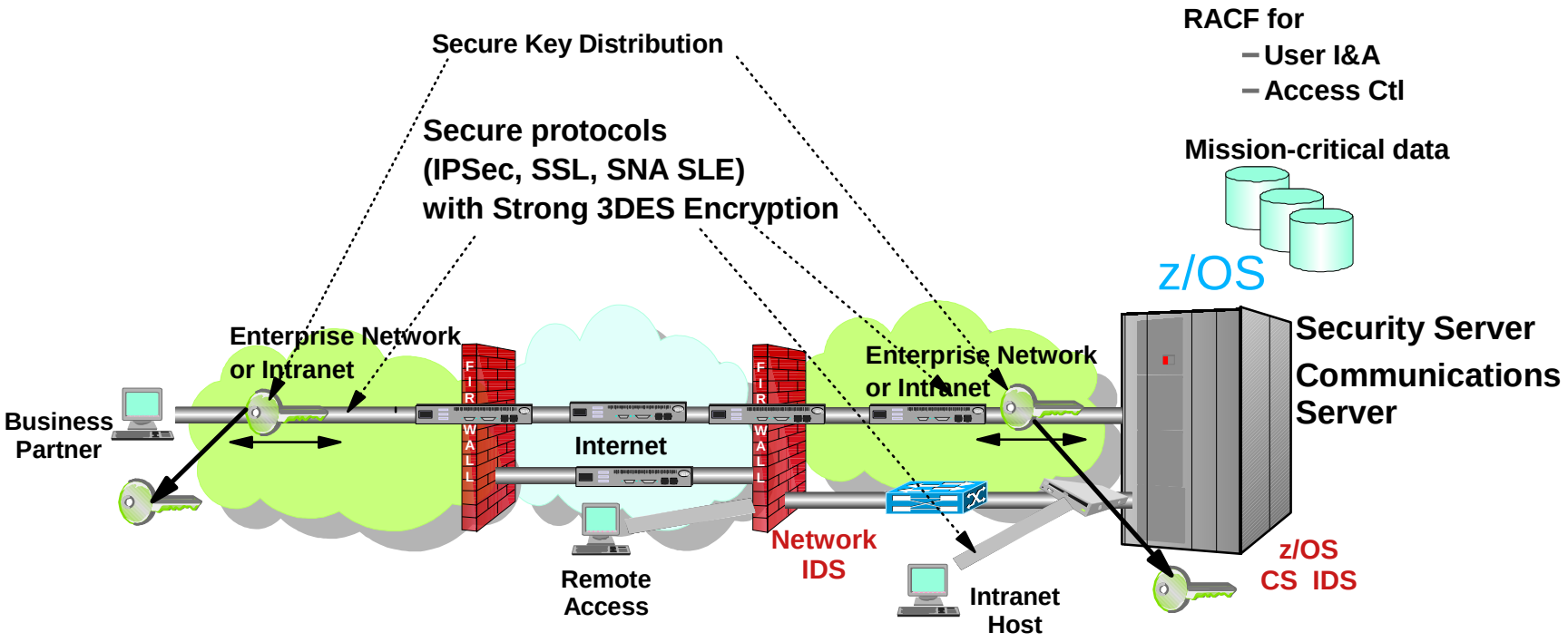
OCEP part of z/OS Security Server

Network Authentication Services



z/OS Communication Server Enables e-business on z/900

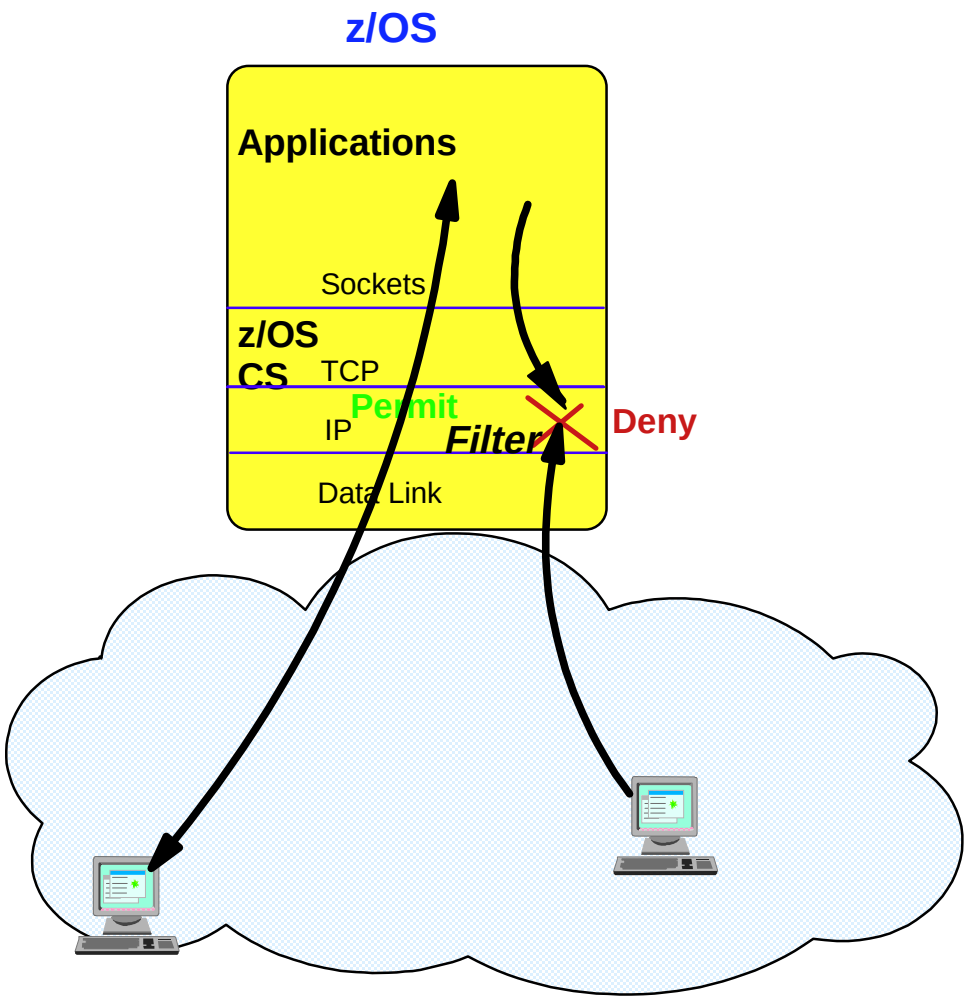
- ✓ Secure access to both TCP/IP and SNA applications
- ✓ Focus on end-to-end security and self-protection
- ✓ Exploits strengths of S/390 and z900 hardware and software



z/OS Communications Server Secures Mission-Critical Data

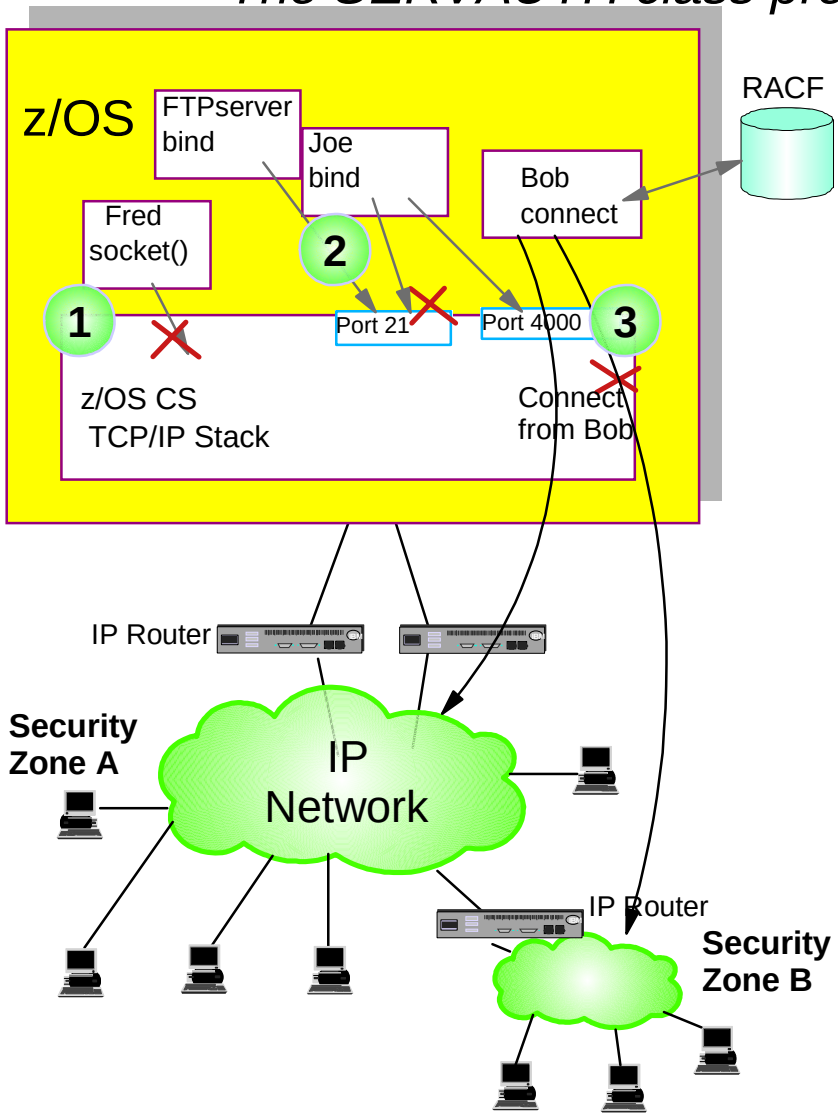
IP Packet Filtering

- **Packet filtering at IP Layer**
  - Filter rules defined to discard or permit packets based on:
    - IP source/dest address
    - IP protocol
    - Source/dest Port
    - Direction of flow
    - Time
  - Used to control
    - traffic being routed
    - access at destination host
- **Packaging (Firewall Technologies)**
  - Security Server
    - Configuration thru z/OS UNIX command line interface or Configuration GUI
  - Communications Server
    - Runtime IP packet filtering



User Access Control to TCP/IP Resources Using RACF

The SERVAUTH class protects TCP/IP Resources



1. *Stack Access Control*

- **Controls user ability to open socket**
  - CS OS/390 TCP/IP stack is considered a resource
- **Access to stack via TCP or UDP socket allowed if user permitted to new SAF resource (SERVAUTH class)**
  - ✓ EZB.STACKACCESS.sysname.tcpname

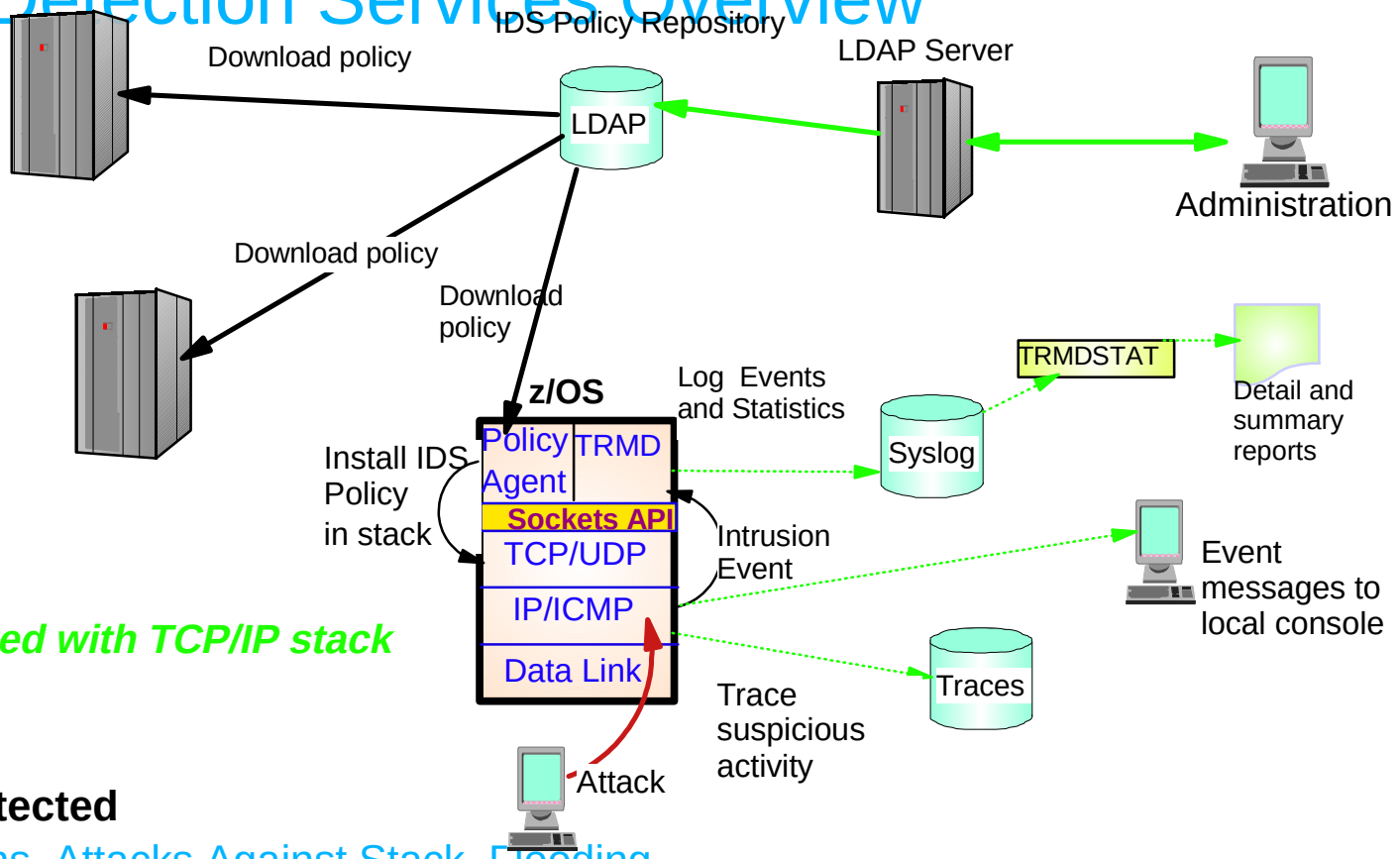
2. *Local Port Access Control*

- **Controls user access to a local TCP or UDP port**
  - Port is considered a resource
- **Function enabled**
  - Via new SAF Keyword on PORT or PORTRANGE
- **Access to port allowed if user permitted to new SAF resource (SERVAUTH class)**
  - ✓ EZB.PORTACCESS.sysname.tcpname.SAFkeyword
- **Access to port not permitted for any user**
  - Via New RESERVED Keyword On PORT Or PORTRANGE

3. *Network Access Control*

- **Controls local user access to network resources**
  - Network considered a resource
    - ✓ Network/Subnet/Specific host
- **Allows Management Of Security Zones**
  - Via new NETACCESS statement In TCP/IP Profile
    - ✓ NETACCESS statement allows grouping of network resources
- **Access to security zone allowed if user permitted to new SAF resource (SERVAUTH class)**
  - ✓ EZB.NETACCESS.sysname.tcpname.zonename

z/OS Intrusion Detection Services Overview



Events detected

- Scans, Attacks Against Stack, Flooding

Defensive methods

- Packet discard, limit connections

IDS Recording

- Event and statistics logging, event messages to local console, IDS packet trace

IDS Reporting

- trmdstat program for IDS reports

zSeries Security Summary

Integrated H/W Crypto

- DES, TDES, RSA and more
- FIPS 140-1 Level 4 certified

www.ibm.com/servers/eserver/zseries/zos/security/cryptography.html

Kerberos

www.ibm.com/servers/eserver/zseries/zos/commserver/kerberos.html

Enterprise Identity Mapping

www.ibm.com/servers/eserver/security/eim/

WEB Security

- SSL
- Digital Certificates

www.ibm.com/servers/eserver/zseries/zos/pki/

Virtual Private Network and IKE support

www.ibm.com/software/network/

Logical Partitions

www.ibm.com/servers/eserver/zseries/zos/security/hwareislation.html

www.ibm.com/servers/eserver/zseries/security/certification.html

Access Controls

www.ibm.com/servers/eserver/zseries/zos/security/securityserver.html

Server Intrusion Detection

- TCP/IP (z)
- Signed O/S (p, i)

Directory - LDAP

www.ibm.com/software/network/directory/

eServer Security Wizard

www.ibm.com/servers/security/planner

Agenda

- zSeries Hardware
  - Virtualization: Partitions and HiperSockets
  - Cryptographic facilities
- z/OS
  - z/OS Security Server
    - RACF
    - PKI Services
    - LDAP
    - Distributed Computing Environment (DCE)
    - Open Cryptographic Enhanced Plug-ins (OCEP)
    - Network Authentication Services (Kerberos)
  - Communications Server
    - IP Filtering
    - Controlling Access to TCP/IP Resources Using RACF
    - Intrusion Detection Services

IBM zSeries and z/OS Security Facilities
- or -
Mainframes: Are They Secure?

Mark Nelson, CISSP
z/OS Security Server (RACF) Design and Development
IBM Poughkeepsie