2009 System z Expo

October 5 – 9, 2009 – Orlando, FL

z/VSE Security Concepts and News

zES01

Ingo Franzki, IBM

Authorized IBM Training

Trademarks

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

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

*, AS/400®, e business(logo)®, DBE, ESCO, eServer, FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, S/30, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* 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.

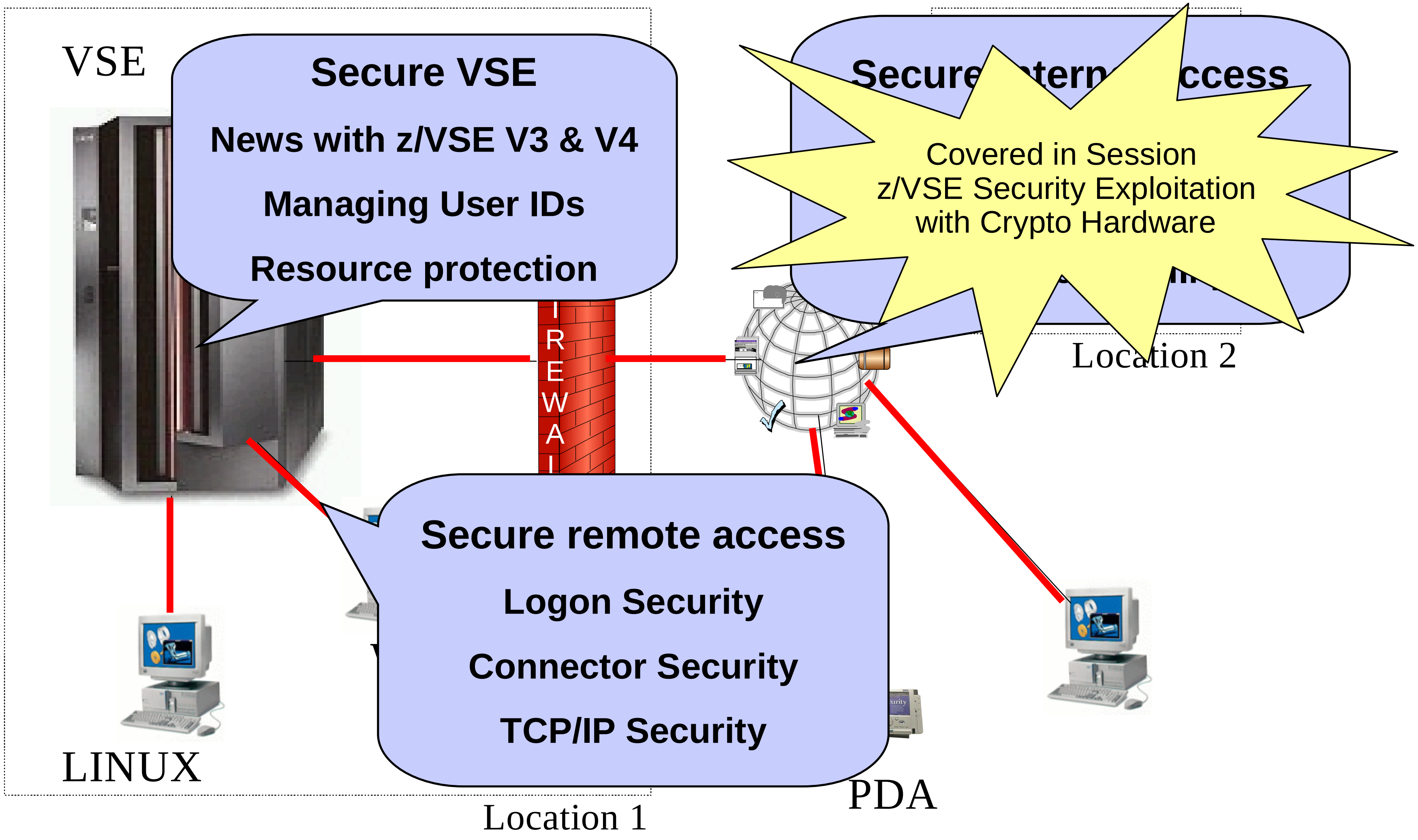
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products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

Security requirements

- Security requirements are increasing in today's world
  - Data security
  - Data integrity
  - Keep long-term data audit-save
- The number of attacks increase daily
  - Industrial spying
  - Security exploits, Denial-of-Service attacks
  - Spam, Phishing, …
- Not paying attention to security requirements can be very expensive
  - Your data is the heart of your company
  - Loosing your customer data is a disaster
  - You can loose customers
- IT Security gets more and more important
  - You need to consider the whole IT Environment not only single systems

Security in a heterogeneous environment



Secure VSE

News with z/VSE V3 & V4

Managing User IDs

Resource protection

Secure tern ccess

Covered in Session
z/VSE Security Exploitation
with Crypto Hardware

Secure remote access

Logon Security

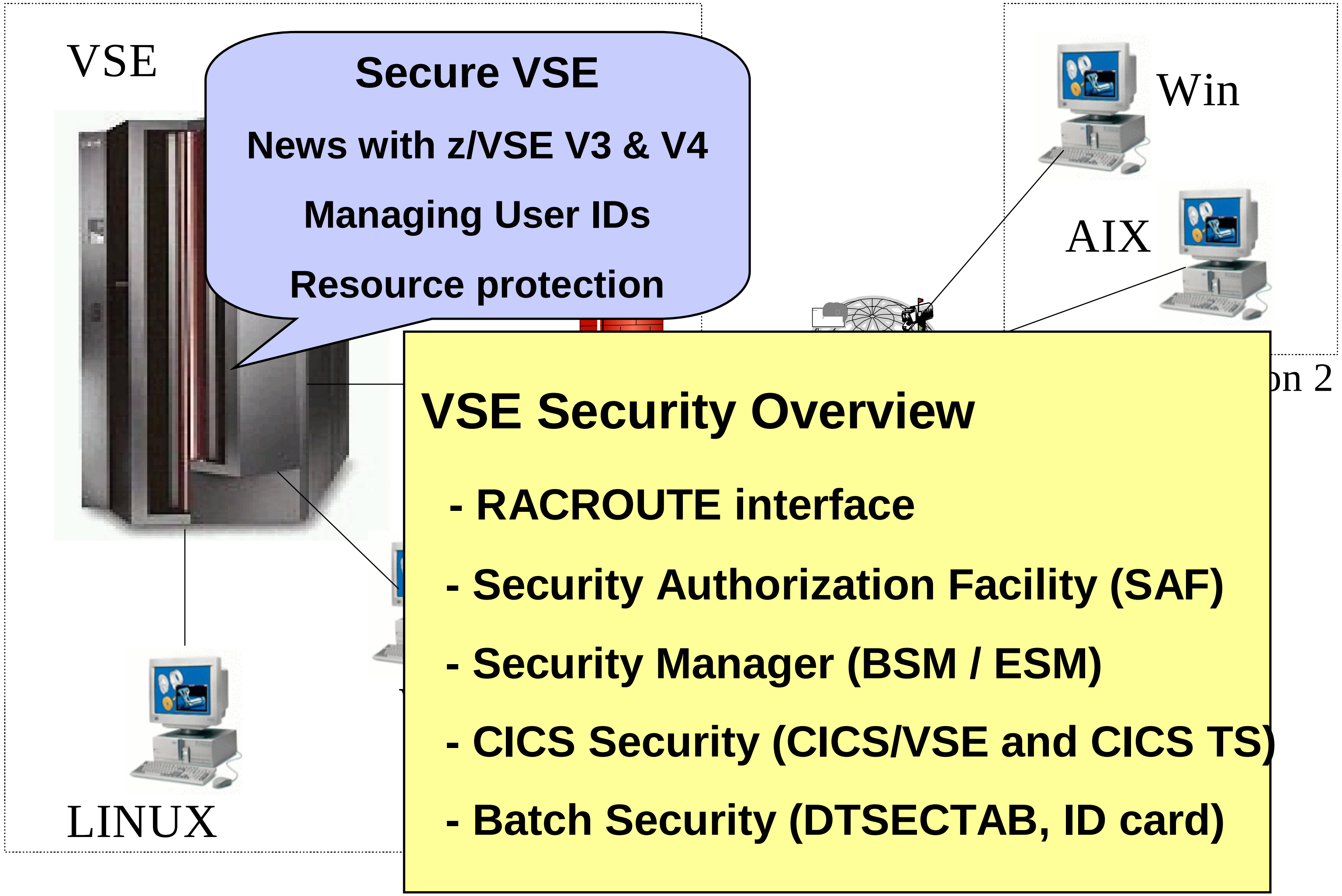
Connector Security

TCP/IP Security

Security in a heterogeneous environment

- Security is very important
  - Restrict access to systems
  - Keep secrets
  - Prove identity of users
  - Prevent data modification
- Security can be very complex
  - In an heterogeneous environment
  - A lot of different servers and technologies
- You must know what you are doing !
  - Incomplete security setup can be more dangerous than NO security

Security in a heterogeneous environment



Secure VSE

News with z/VSE V3 & V4

Managing User IDs

Resource protection

VSE Security Overview

- **- RACROUTE interface**
- **- Security Authorization Facility (SAF)**
- **- Security Manager (BSM / ESM)**
- **- CICS Security (CICS/VSE and CICS TS)**
- **- Batch Security (DTSECTAB, ID card)**

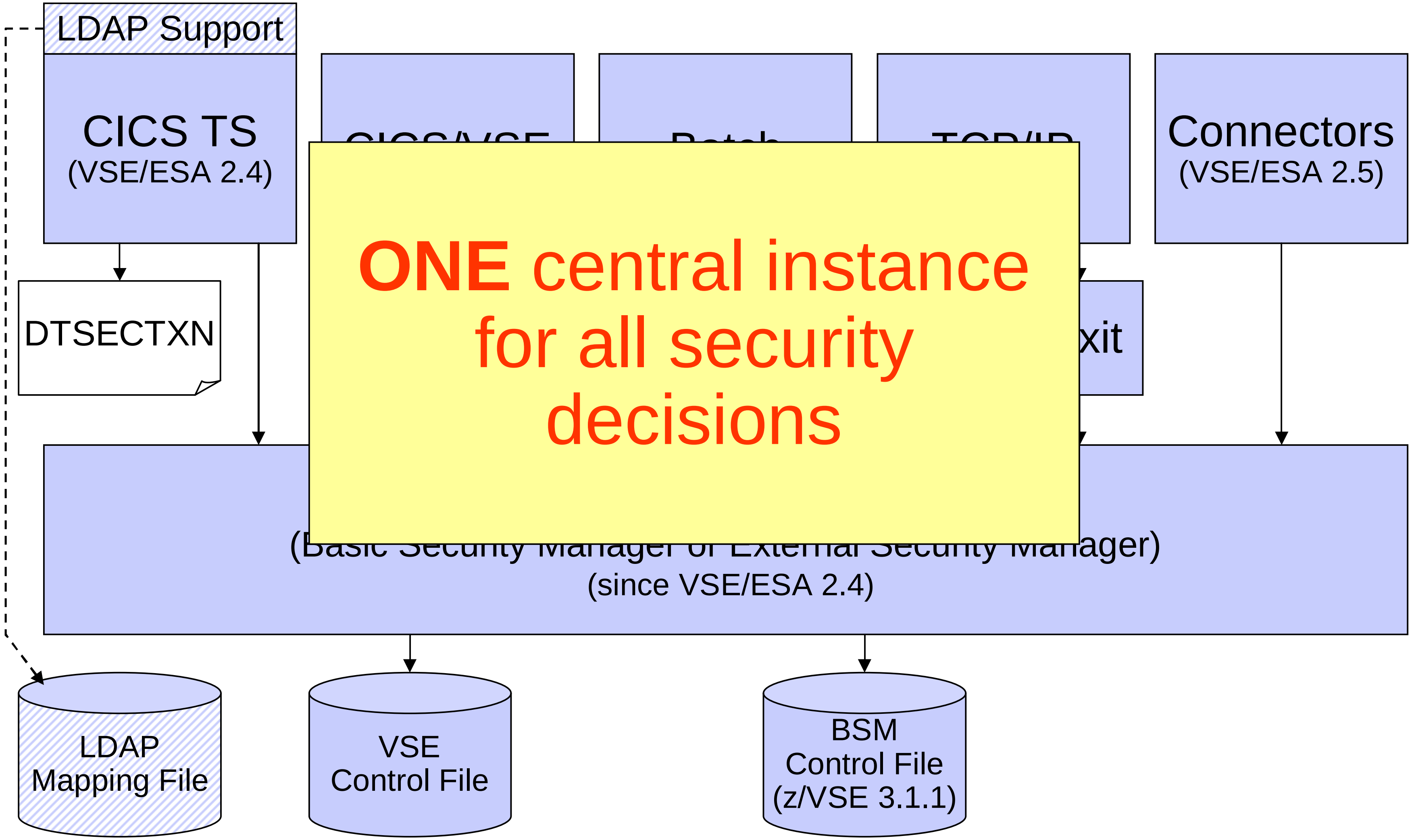
Why secure VSE ?

- Prevent unauthorized access to VSE and data
  - Keep secret data secret
  - Data modification by unauthorized users
- Prevent users from damaging the VSE system (maybe by accident)
  - Deletion of members or entries
  - Submission of jobs

VSE Security Overview

- VSE/ESA 2.3 (or below)
  - SECHECK macro (DTSECTAB)
  - CICS/VSE internal security
- VSE/ESA 2.4-2.7, z/VSE 3.1
  - Security Server (BSM/ESM)
  - Security decisions delegated to Security Manager
  - Architecture defined interface (RACROUTE)
- New with z/VSE 3.1.1: BSM enhancements
  - User Groups
  - Description field for all profiles
  - BSM Resource Profiles
  - New resource classes
- New with z/VSE 4.1: Audit-logging and reporting
- New with z/VSE 4.2: LDAP Signon support

VSE Security Components

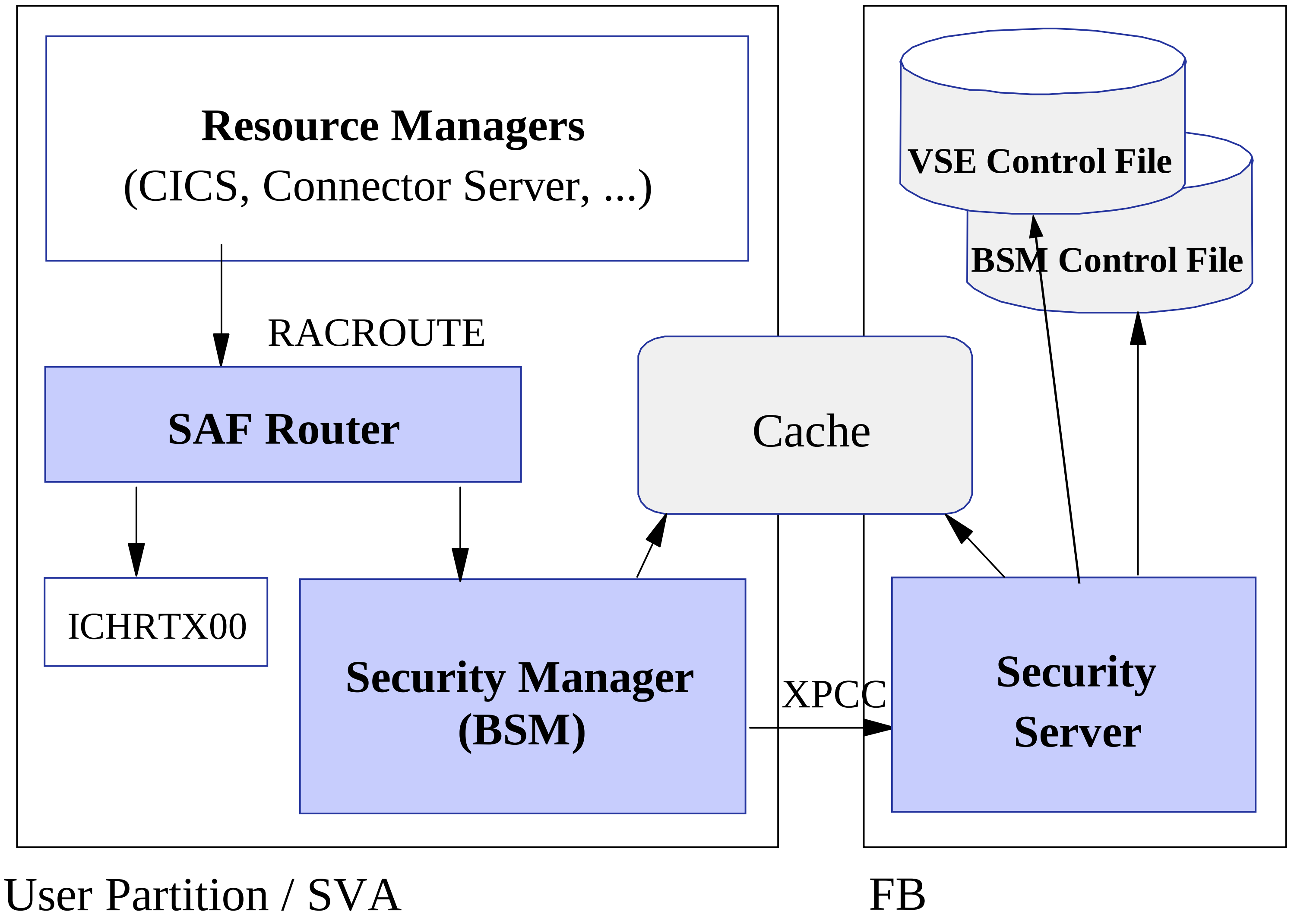


ONE central instance for all security decisions

Security Managers

- Basic Security Manager (BSM)
  - Part of VSE Central Functions
  - Sign on Security
  - Transaction Security
  - Resource Security
- External Security Manager (ESM)
  - CA-Top Secret
  - BIM Alert
  - Vendor

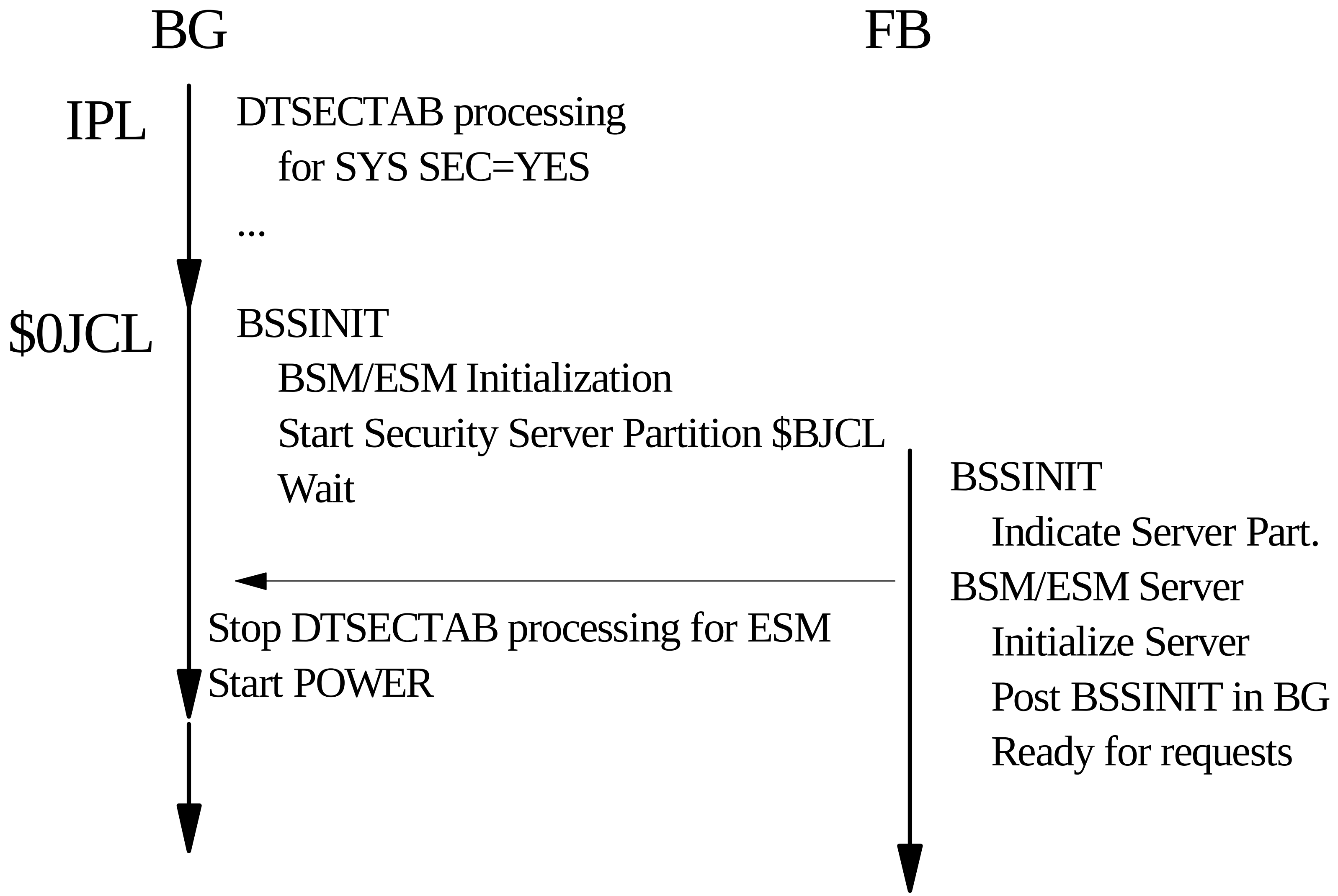
Security Authorization Facility (SAF) and Basic Security Manager



RACROUTE interface

- Architecture defined interface
- External interface to the Security Authorization Facility (SAF)
- To be used by Resource Managers and Subsystems
  - CICS TS
  - VSE Connector Server
  - DITTO/ESA for VSE
  - TCP/IP Security Exit
  - Interactive Interface Sign on

Common Security Startup



BG

FB

IPL

DTSECTAB processing
for SYS SEC=YES
…

$0JCL

BSSINIT
BSM/ESM Initialization
Start Security Server Partition $BJCL
Wait

BSSINIT
Indicate Server Part.
BSM/ESM Server
Initialize Server
Post BSSINIT in BG
Ready for requests

Stop DTSECTAB processing for ESM
Start POWER

Common Security Startup (continued)

- Security manager (BSSINIT) has to initialize before other partition or POWER are active
- BSSINIT will fail, if there are other partition active
- Static partition required for Security Server
- SYS ESM=phasename in IPL proc to start ESM
- If no ESM is started, BSM is activated
- For SYS SEC=YES with ESM a DTSECTAB protection is active until ESM is initialized

Basic Security Manager - Recovery

- If an active Security Manager does not allow to recover from a problem
  - IPL cuu LOADPARM ..P
  - STOP=DPD
  - 0 SYS SEC=RECOVER
  - BSSINIT will not start a Security Manager
  - Re-IPL required to start Security Manager again

Basic Security Manager

- Provides RACROUTE support for
  - Sign on (CICS and VSE Connector Server)
  - Batch sign on (ID statement)
  - Transaction security
- Supports also the SVC-based security calls
  - SECHECK
- Resource classes
  - USER
  - DATASET
  - VSELIB, VSESLIB, VSEMEM
  - TCICSTRN
  - New with z/VSE 3.1.1: MCICSPPT, FCICSFCT, JCICSJCT, SCICSTST, DCICISDCT, ACICSPCT, APPL, FACILITY

Basic Security Manager - New with z/VSE 3.1.1

- New BSM repository
  - BSM Control File (VSAM file)
  - Maintains a copy in data space for performance reasons
  - Replaces DTSECTXN
- New resource classes (see next foil)
- Description field for all profiles (20 characters)
- User Groups
  - Replaces the security classes concept for CICS
- Password rules can be changed by command
- New admin functions
  - BSTADMIN (console or batch)
  - Interactive Interface Dialogs

Basic Security Manager - New with z/VSE 3.1.1

- New resource classes
  - TCICSTRN - Transactions (as on VSE/ESA 2.7)
  - MCICSPPT - Application programs
  - FCICSFCT - Files
  - JCICSJCT - Journals
  - SCICSTST - Temporary storage queues
  - DCICISDCT - Transient data queues
  - ACICSPCT - Transactions (CICS START)
  - APPL - Applications
  - FACILITY - Miscellaneous resources

Basic Security Manager - New with z/VSE 4.1

- Audit-Logging and Reporting
  - All access attempts to protected resources can be logged
    - Allowed access as well as disallowed access
  - Possible attacks can be detected
    - E.g. multiple logon attempts with invalid password
  - You can comprehend who did when access which resource
  - Analysis can be done using a reporting tool
    - Summary report
    - Detailed report of all access attempts
  - Uses the CICS DMF Tool
    - Creates SMF records containing logging information
  - New with z/VSE 4.2:
    - Logging of important BSTADMIN commands

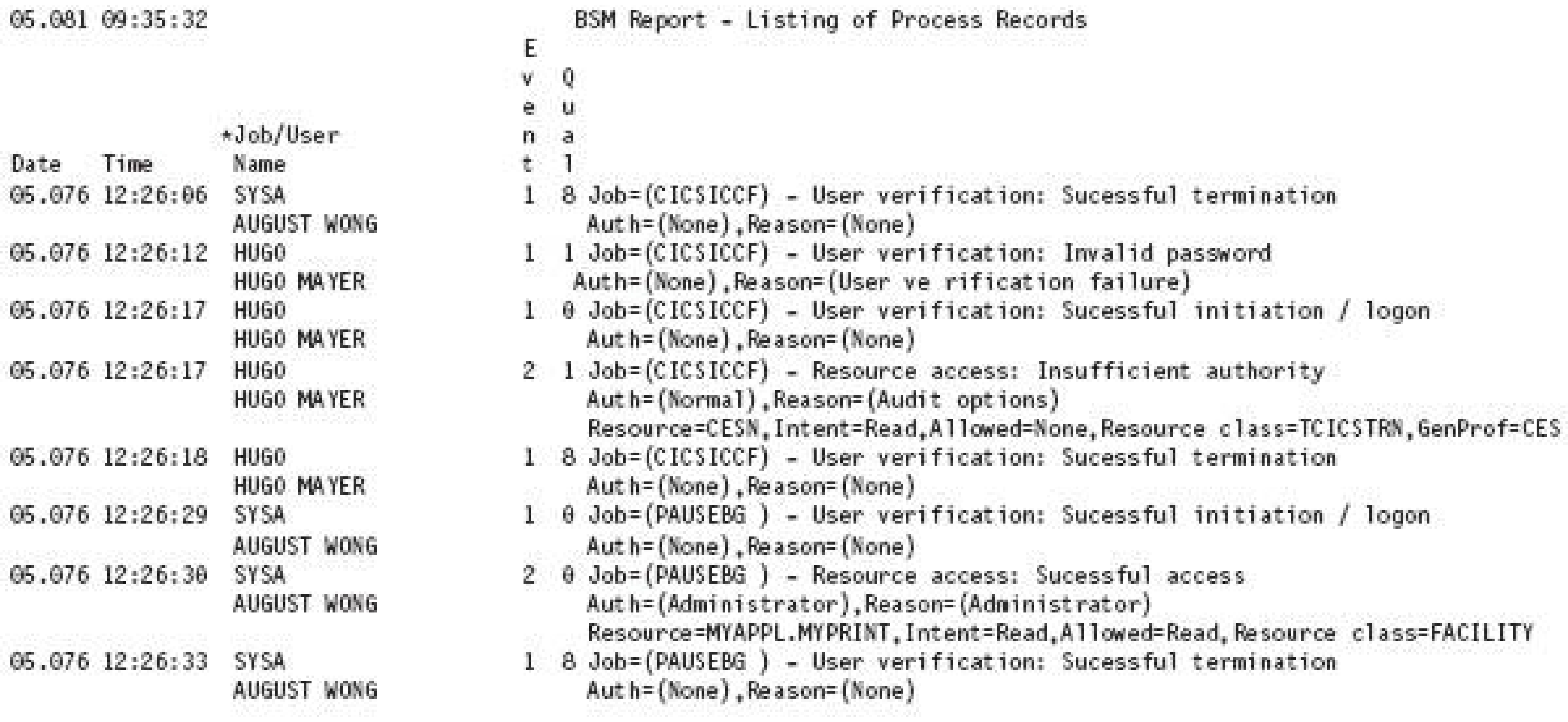
Audit-Logging and Reporting

- To activate logging for a specific resource, you need to specify the AUDIT option (BSTADMIN) on the resource profile
  - AUDIT(***audit-level, access-level***) ß New with z/VSE 4.2
    - **audit-level:**
      - **ALL:** Specifies that all authorized accesses and detected unauthorized access attempts should be logged.
      - **FAILURES:** Specifies that all detected unauthorized access attempts should be logged (the Default).
      - **SUCCESS:** Specifies that all access attempts that were authorized should be logged.
      - **NONE:** Specifies that no logging should be done.
    - **access-level:**
      - **ALTER:** Logs ALTER access-level attempts only.
      - **READ:** Logs access attempts at any level. READ is the default value if the access-level is omitted.
      - **UPDATE:** Logs access attempts at the UPDATE and ALTER level.
- **Note: You should use the auditing function with care. It will increase the BSM and DMF processing and might negatively affect the performance of your z/VSE system!**

Audit-Logging and Reporting

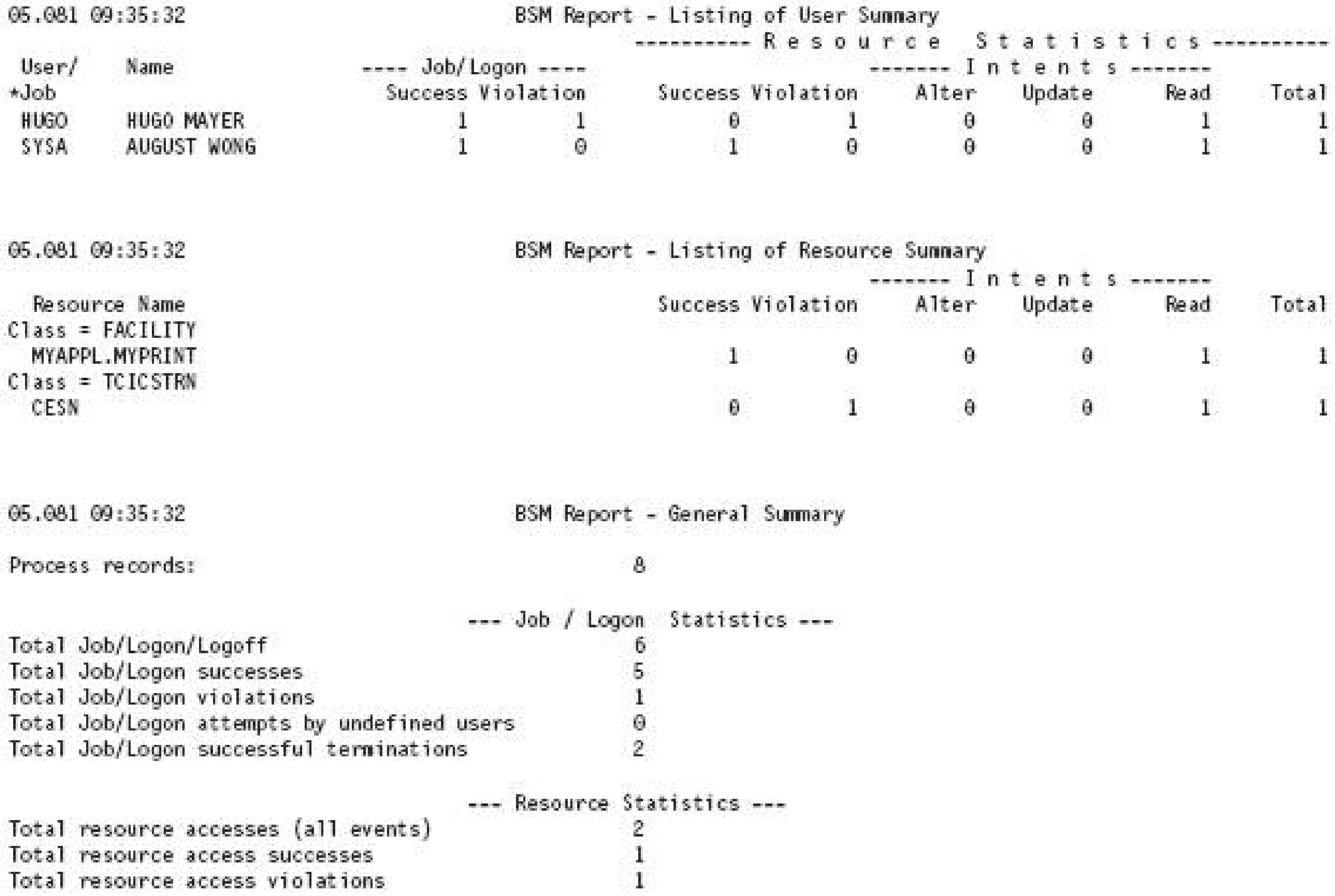
- **Audit-Logging uses the CICS DMF facility to store the recorded SMF records**
- **Use the DMF dump utility DFHDFOU to dump the audit records (type 80) to a intermediate file**
- **Use the BSM Report Writer to create a readable report from the audit records**
- **The report contains**
  - A detailed listing of the processed records
  - A summary of the user entries
  - A summary of the resource entries
  - A general summary

Audit-Logging and Reporting



```
05.081 09:35:32                            BSM Report - Listing of Process Records
                                       E
                                       v  Q
                                       e  u
                *Job/User              n  a
Date   Time      Name                  t  l
05.076 12:26:06  SYSA                  1  8 Job=(CICSICCF) - User verification: Sucessful termination
                 AUGUST WONG                Auth=(None),Reason=(None)
05.076 12:26:12  HUGO                  1  1 Job=(CICSICCF) - User verification: Invalid password
                 HUGO MAYER                Auth=(None),Reason=(User ve rification failure)
05.076 12:26:17  HUGO                  1  0 Job=(CICSICCF) - User verification: Sucessful initiation / logon
                 HUGO MAYER                 Auth=(None),Reason=(None)
05.076 12:26:17  HUGO                  2  1 Job=(CICSICCF) - Resource access: Insufficient authority
                 HUGO MAYER                 Auth=(Normal),Reason=(Audit options)
                                            Resource=CESN,Intent=Read,Allowed=None,Resource class=TCICSTRN,GenProf=CES
05.076 12:26:18  HUGO                  1  8 Job=(CICSICCF) - User verification: Sucessful termination
                 HUGO MAYER                 Auth=(None),Reason=(None)
05.076 12:26:29  SYSA                  1  0 Job=(PAUSEBG ) - User verification: Sucessful initiation / logon
                 AUGUST WONG                Auth=(None),Reason=(None)
05.076 12:26:30  SYSA                  2  0 Job=(PAUSEBG ) - Resource access: Sucessful access
                 AUGUST WONG                Auth=(Administrator),Reason=(Administrator)
                                            Resource=MYAPPL.MYPRINT,Intent=Read,Allowed=Read,Resource class=FACILITY
05.076 12:26:33  SYSA                  1  8 Job=(PAUSEBG ) - User verification: Sucessful termination
                 AUGUST WONG                Auth=(None),Reason=(None)
```

Audit-Logging and Reporting



```
05.081 09:35:32                            BSM Report - Listing of User Summary
                                                     ----------- R e s o u r c e   S t a t i s t i c s ----------
 User/    Name                ---- Job/Logon ----                        ------- I n t e n t s -------
*Job                            Success Violation      Success Violation    Alter    Update      Read     Total
 HUGO     HUGO MAYER                   1         1            0         1         0         0         1         1
 SYSA     AUGUST WONG                  1         0            1         0         0         0         1         1


05.081 09:35:32                            BSM Report - Listing of Resource Summary
                                                                         ------- I n t e n t s -------
  Resource Name                                        Success Violation    Alter    Update      Read     Total
Class = FACILITY
  MYAPPL.MYPRINT                                              1         0         0         0         1         1
Class = TCICSTRN
  CESN                                                        0         1         0         0         1         1


05.081 09:35:32                            BSM Report - General Summary

Process records:                                     8

                                       --- Job / Logon  Statistics ---
Total Job/Logon/Logoff                               6
Total Job/Logon successes                            5
Total Job/Logon violations                           1
Total Job/Logon attempts by undefined users          0
Total Job/Logon successful terminations              2

                                       --- Resource Statistics ---
Total resource accesses (all events)                 2
Total resource access successes                      1
Total resource access violations                     1
```

Basic Security Manager – Repositories

- VSE Control File (IESCNTL)
  - VSAM KSDS file
  - Contains all user profiles
- DTSECTAB
  - Contains resources like files, libraries, sub libraries and members
  - Only 2 user ids are still needed in DTSECTAB
    - (FORSEC, DUMMY)
- DTSECTXN (replaced by BSM Control File)
  - Transaction security profiles
  - Dialog (28) to define the profiles
- BSM Control File
  - Resource Profiles
  - Password rules
  - User groups

Basic Security Manager – User Profiles

- VSE Control File (IESCNTL)
  - All Users must be defined here (SNT no longer supported by CICS TS)
  - VSE/ESA 2.4 (or above) Control File records are NOT compatible with previous releases
  - New: description field
  - Definition
    - User Maintenance Dialog (211)
    - Batch utility IESUPDCF
- DTSECTAB
  - Contains 2 user ids for ASI procedure
  - No CICS TS user settings

Basic Security Manager – User Groups

- User Groups are stored in BSM Control File
- User IDs can be added (connected) into a group
- Replaces the security classes for CICS resources
- Definition
  - Security Maintenance Dialogs (282)
  - Batch utility BSTADMIN

Migrating to the new BSM Resource Profiles

- DTSECTXN no longer used
  - Use the new BSM Control File to protect CICS resources
- Migration steps:
  - Create group profiles from existing User-IDs
    - User Maintenance Dialog 211 – press PF6
    - Creates a group for each security class (GROUP01-GROUP64)
  - Migrate DTSECTXN definitions
    - Use Migrate Security Entries Dialog 285
- Detailed description:
  - See Administration Guide

Administrating new BSM resources

- BSTADMIN provides command to administrate the new BSM profiles
  - From the console in a PAUSE job
  - In a batch job

- Commands
  - ADD, CHANGE, DELETE
  - ADDGROUP, CHNGROUP, DELGROUP
  - CONNECT, REMOVE
  - LIST, LISTG, LISTU
  - PERFORM
  - STATUS

- Security Maintenance Dialogs – 28x

Password rules

- Password rules can be changed
  - Use BSTADMIN

```
PERFORM PASSWORD HISTORY|NOHISTORY
                 LENGTH(5)
                 REVOKE(4)
                 WARNING(3)
```

  - **HISTORY**: a password history is maintained
  - **LENGTH**: minimum password length of password
  - **WARNING**: number of days a warning is displayed before password is expired
  - **REVOKE**: number of unsuccessful sign-on attempts before user id is revoked

- Do not use IESIRCVT anymore !
  - Remove it from USERBG.PROC

LDAP Signon Support - New with z/VSE 4.2

- The LDAP sign-on support enables users to sign on to z/VSE using long, “company-wide” (corporate) user-IDs and passwords
  - The userid and password are authenticated using an LDAP server that is reachable via the TCP/IP network

- This use of “company-wide” user-IDs connects z/VSE with the centralized management of user-IDs
  - LDAP authorization is designed to integrate z/VSE into “Identity Management Systems”, such as IBM Tivoli products
- Covered in more details in separate session (Monday 8:00)

CICS Security

- CICS/VSE uses SNT for user verification
  - Duplicate user definitions
  - SNT users can not change password

- CICS TS uses RACROUTE calls for
  - Sign on
  - Resource Security
  - Transaction Security

CICS TS Sign on

- Native CICS TS sign on (CESN)
- VSE/Interactive Interface sign on (IEGM)
- Private sign on programs based on CICS SIGNON

- Sign on characteristics
  - Inherit user identification and password verification by Security Manager
  - CICS TS and Interactive Interface extracts subsystem specific user settings
    - CICS: Operator ID, Operator classes, ...
    - II: User type, Initial panel, access flags, ...
  - No user definitions to subsystems necessary

CICS TS Resource Security

- Most CICS TS resources can be protected now
  - Protection via Resource Classes and Resource Profiles, held in VSE.BSTCNTL.FILE
  - Transactions – as in previous releases
  - Programs, Files, Journals, Temporary storage, Transient data, Start Transactions, VTAM Applications, miscellaneous resources
- This is similar to Resource Level Checking under CICS/VSE
  - RSLC=YES defined within a transaction
  - RSLKEY defined for
    - Users being allowed to access protected resources
    - Resources for being allowed to be accessed

CICS TS Resource Security

- Resource security definitions under CICS TS
  - DFHSIT

SEC=YES	Enables security
XTRAN=YES	Resource Class TCICSTRN
XDCT=YES	Resource Class DCICSDCT
XFCT=YES	Resource Class FCICSFCT
XJCT=YES	Resource Class JCICSJCT
XPCT=YES	Resource Class ACICSPCT
XPPT=YES	Resource Class MCICSPPT
XTST=YES	Resource Class SCICSTST

CICS TS Resource Security

- Resource security definitions under CICS TS
  - Definition within single resource definition (e.g. file FILEA and FILEB)
    - Within DEFINE FILE: RESSEC(YES)
    - With BSTADMIN Resource Profiles for Resource Class FCICSFCT:
      - ADD FCICSFCT FILEA UACC(NONE) (resource = FILEA)
      - ADD FCICSFCT FILEB UACC(NONE) (resource = FILEB)
      - PERMIT FCICSFCT FILEA(GROUP1) ACCESS(UPDATE)
      - PERMIT FCICSFCT FILEB(GROUP1) ACCESS(READ)

CICS TS Resource Security

- **Enhancement for Report Controller Facility (RCF) to browse reports**
  - **Access protection under CICS/VSE 2.3**
    - RSLKEY for program DFHPSBRS – just 1 level of protection for all repots
    - All users with that RSLKEY can access all reports
  - **Access protection under CICS TS 1.1.1 (requires APAR PK11491)**
    - RSL concept retained for compatibility reasons
      - RSL keyword within SPOOLOPEN REPORT unchanged
    - For browsing purposes profile names
      - DFHRCF.BRSL01 – DFHRCF.BRSL24
    - There are 24 levels for browse protection now –
      - user must be authorized on access list of these related profiles DFHRCF.BRSLxx (RSLxx within SPOOLOPEN)
    - Protection based on report, not on browse program
  - **Definition for RCF protection**
    - ADD FACILITY DFHRCF.RSLnn UACC(NONE)
    - PERMIT FACILITY DFHRCF.RSLnn ID(usergroup1) ACCESS(READ)

CICS Security - Prefixing

- CICS Prefixing can be used to differentiate between two or more CICS TS running on the same VSE system
- CICS Prefix is identical with the user id of the CICS startup job
  - SECPRFX=YES in SIT
  - SYS SEC=YES: user id in * $$ JOB or ID statement is used
  - SYS SEC=NO: user id in ID statement is used
  - When no user id is given: FORSEC is used

CICS Security - DTSECTXN Macro

- Macro to support CICS transaction profiles
  - Replaced by new BSM Control File
    - Can still be used for compatibility
  - CICS-region = user id in CICS startup job
  - transid = up to 4 characters
  - class = 1-64
  - 1 = public transactions
  - 64 = interactive interface transactions

```
DTSECTXN NAME={CICS-region.}transid,
         TRANSEC=(class)
         [,SUBTYPE={INITIAL | FINAL}]
         [,TYPE=GENERIC]
```

CICS Security - Coexistence

- Exit program for CICS/VSE to do user verification against BSM user profiles
- DFHXSE and DFHXSSCO in PRD1.BASE
  - Requires RACROUTE macro from GENLIB
- Requires default user entry in SNT
- Activate ESM in CICS/VSE
  - EXTSEC=YES in SIT

CICS Security – Migration from CICS/VSE

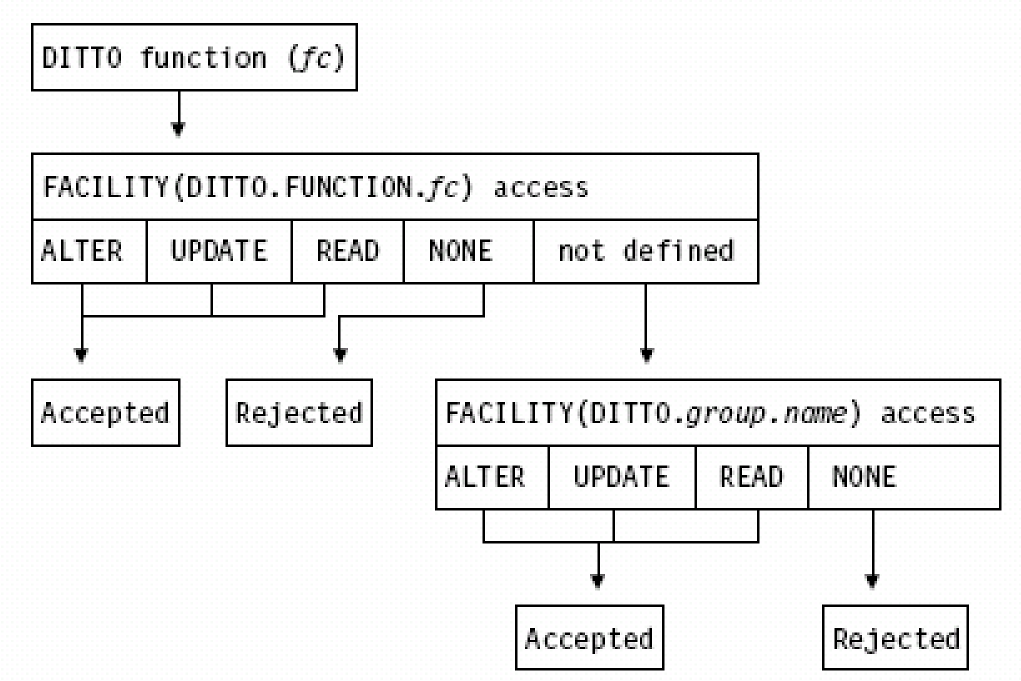
- Security related resource to be migrated
  - Interactive Interface user profiles from an old VSE control file
  - ICCF user records in DTSFILE
  - CICS user profiles from a CICS/VSE sign on table (SNT)
  - Transaction definitions from CICS/VSE PCT
  - For Batch security users: DTSECTAB
  - VSE migration utility IESBLDUP
  - migrate user profiles
- see VSE System Utilities manual

Batch Security

- ID statement or * $$ JOB specifies user id and password for a job
- User id and password are verified against
  - DTSECTAB
  - Security Manager (RACROUTE)
- Subsystems (LIBR, VSAM, ...) uses this user id to verify access rights against DTSECTAB

DITTO Security

- DITTO uses the FACILITY profiles to protect access to data

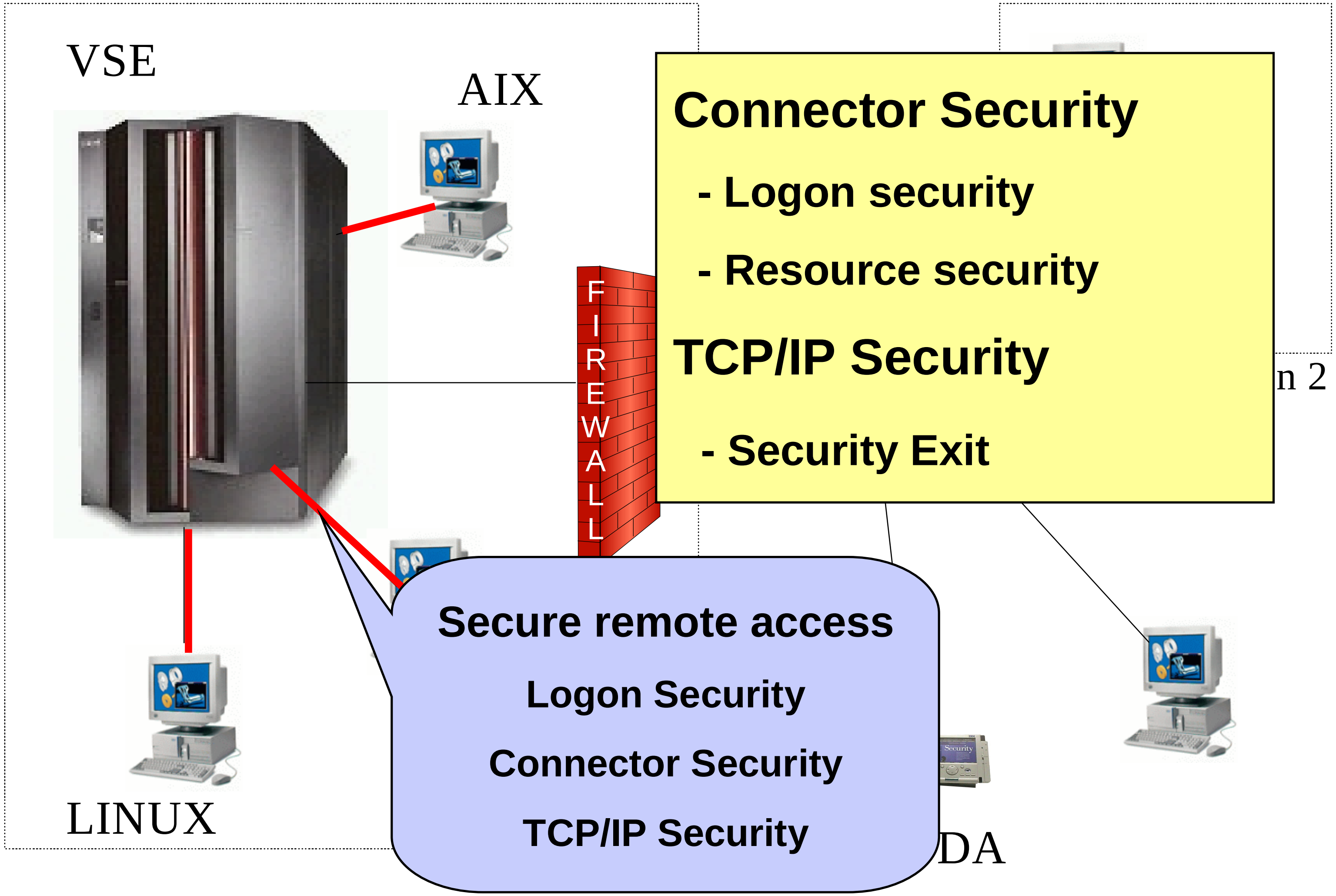


- Make sure batch security is active
  - IPL SEC=YES
- Make sure you define the FACILITY profiles
- ALTER, UPDATE and READ means accepted, NONE means rejected

Security Checklist for VSE

- SYS SEC=YES/NO
  - YES if batch security is required
- CICS SIT SEC=YES (!)
  - If NO, all users can logon without a password
- Change passwords for predefined users
  - POST, PROG, OPER, SYSA, ...

Security in a heterogeneous environment



Connector Security

- **Logon security**
- **Resource security**

TCP/IP Security

- **Security Exit**

Secure remote access

Logon Security

Connector Security

TCP/IP Security

Why secure remote access ?

- Today most computers are part of a network
  - Can connect to your VSE system
- Prevent unauthorized access to VSE and data
  - Requires to authenticate the user (logon)
- FTP allows to access production data
  - VSAM
  - POWER entries (listings)

Connector Security

- VSE Connector Server acts as a Resource Manager
  - Issues RACROUTE calls for
    - User id and password verification
    - Resource security
- Connector user ids are the same as for CICS TS and Batch
- No additional user profile setup required

- But:
  - Additional access restriction by user id and/or IP address possible

Connector Security - Logon

- VSE Connector Server requires a client to logon with valid user id and password
- User id and password is checked via RACROUTE calls
- Additional information is extracted from ACEE and IUI or AF segment
  - User type, access flags, ...
- The user's ACEE is kept during the whole session
- Used to do resource access checking
- Multiple logon attempts with same userid is possible

Connector Security – Resource Security

- When a client issues a resource access request
  - The server does RACROUTE calls to check if the user is allowed to access the resource
  - Access is done only if user is allowed to access the resource
- VSE Connector Server runs under a special userid (VCSRV)
  - specified in ID statement in startup job
  - should be allowed to access all resources

Connector Security - User types

- Type 1 (Administrator)
  - read and write access for all resources
- Type 2 (Programmer)
  - read only access for all resources
  - allowed to submit jobs
- Type 3 (Application User)
  - read only access for selected resources

Connector Security – Resource classes

- The following Resource class are used
  - VSELIB, VSESLIB, VSEMEM (LIBR)
  - DATASET (VSAM)
- Resource not protected by Security Manager
  - POWER queue entries
    - protected by user type and access flag
  - Console
    - protected by user type and access flag
    - If user is allowed to access the console, he can issue all console commands, even REIPL NOPROMPT (!)
  - ICCF Libraries and Members
  - VSAM Record Mappings

Connector Security – Additional Security

- Configuration member allows to restrict logon (connect) by
  - User id
  - IP address
- See skeleton SKVCSUSR in ICCF library 59

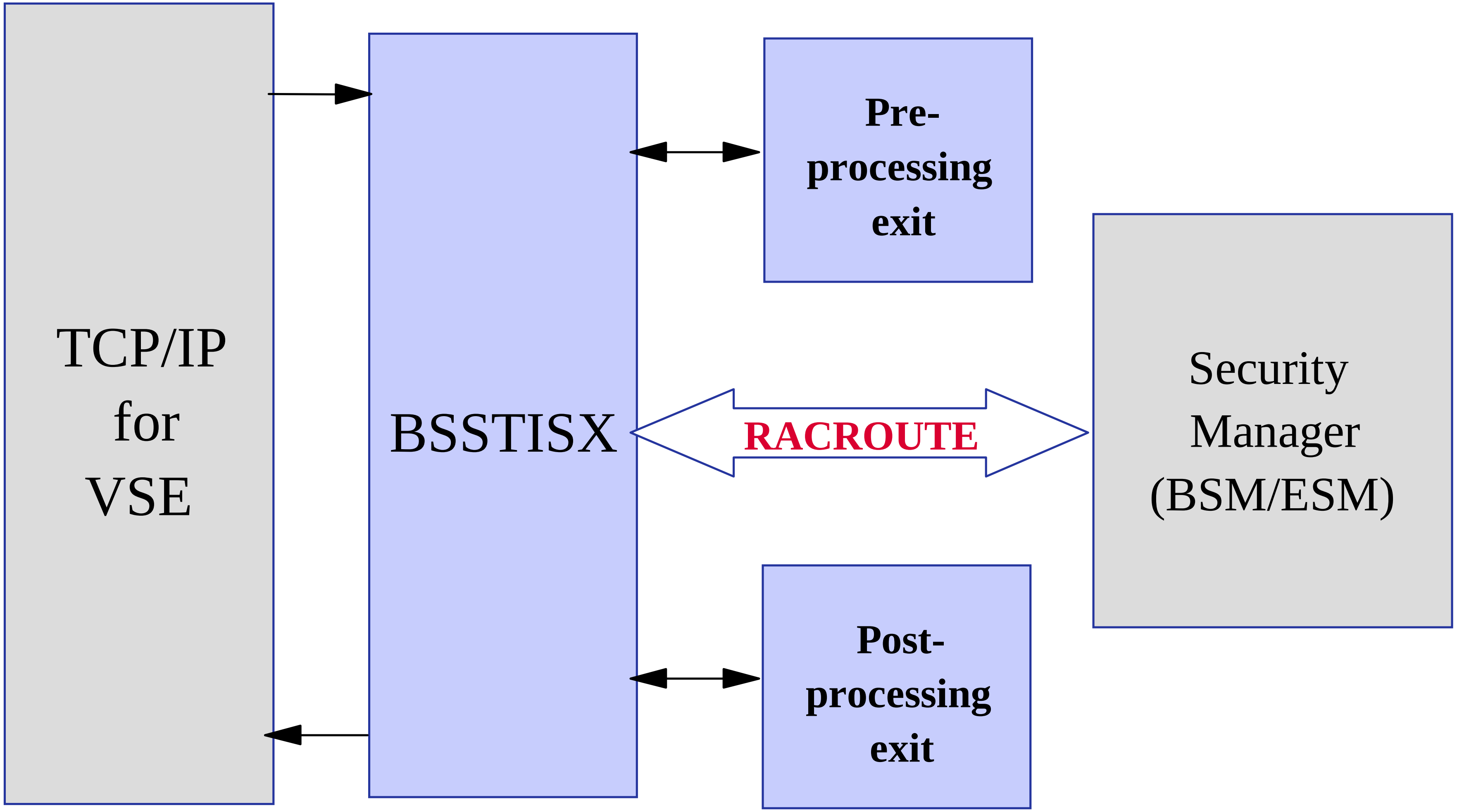
```
* ******************************************************************
* USERS FROM THIS IP'S ARE ALLOWED TO LOGON
* ******************************************************************
IP   = *,             LOGON = ALLOWED
* IP = 9.164.123.456, LOGON = DENIED
* IP = 9.165.*      , LOGON = DENIED
* IP = 10.0.0.*     , LOGON = ALLOWED
* ******************************************************************
* THIS USERS ARE ALLOWED TO LOGON
* ******************************************************************
USER = *,             LOGON = ALLOWED
* USER = BOBY,        LOGON = ALLOWED
* USER = SYS*,        LOGON = DENIED
```

TCP/IP Security

- In general TCP/IP uses its own user id definitions
  - DEFINE USER,ID=user,PASSWORD=pwd
  - Readable in initialization member (IPINITxx.L)
  - Duplicate user definitions

- Security Exit available from IBM to check the user ids and resource access via Security Manager

TCP/IP Security Exit



TCP/IP Security Exit

- Issues RACROUTE calls for
  - User identification and verification
  - Resource access control
    - VSE files, libraries, members
    - POWER entries
    - SITE commands
- Provides a pre- and post-processing exit interface
  - Activation
    - DEFINE SECURITY,DRIVER=BSSTISX[,DATA=data]
      - DATA=‘anonym_uid,anonym_pwd,preproc,postproc’
  - SET SECURITY=ON
- Also see new “RACROUTE encapsulation services”
  - Available on z/VSE Homepage for download

TCP/IP Security - HTTPHACK.L

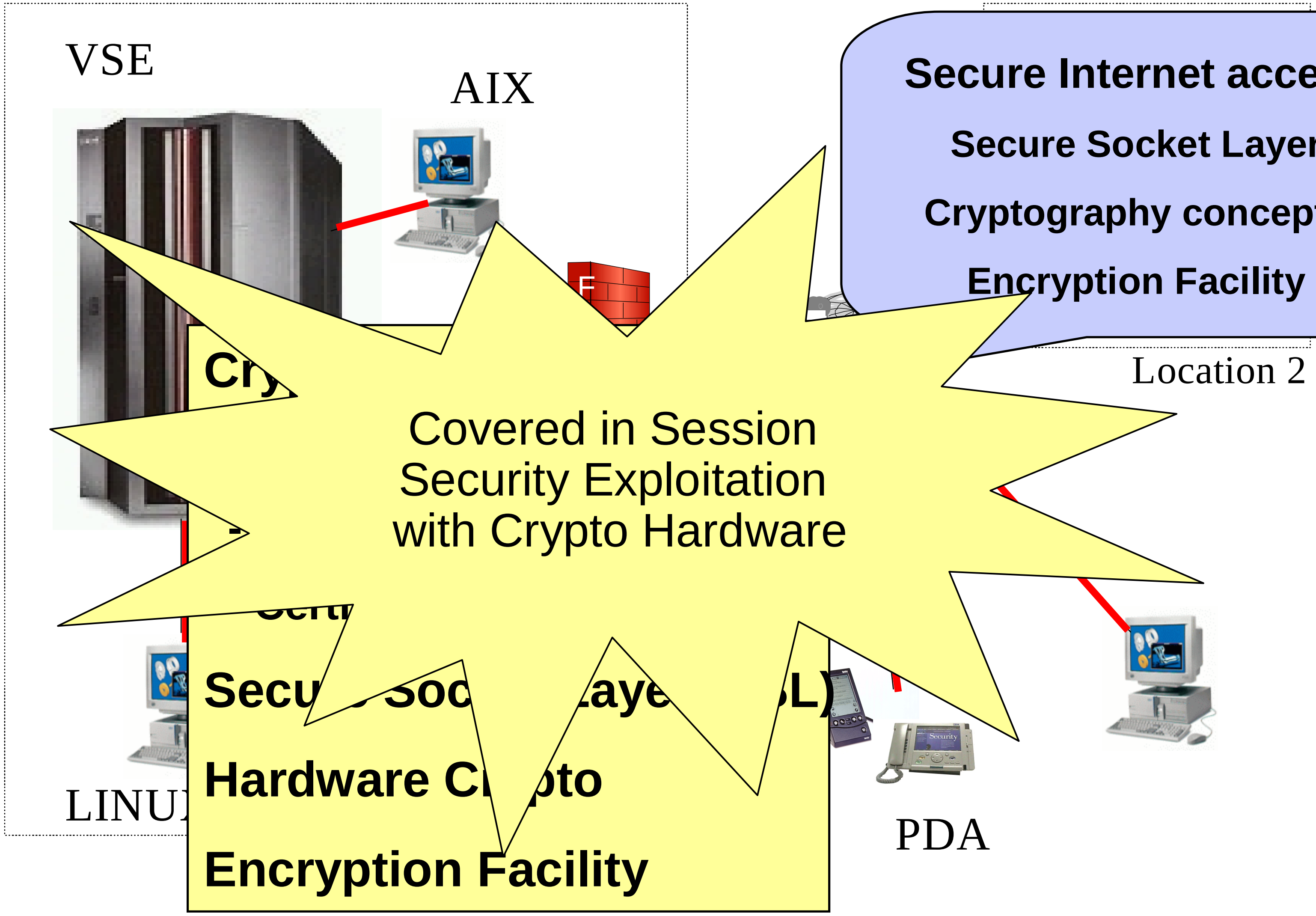
- Typical hacker attacks are normally no problem for VSE, only for Windows
- Rejects hacker attacks
  - by filtering known URL prefixes
- HTTPHACK.L:

```
* Example:
*
* "SCRIPTS/" will cover...
*       GET /SCRIPTS/ROOT.EXE?C+D
*       GET /SCRIPTS/ROOT.EXE?CAT+PASSWD
*       etc...
* =======================================================
SCRIPTS/
MSADC/
_VTI_BIN/
_MEM_BIN/
C/WINNT/SYSTEM32/CMD.EXE
D/WINNT/SYSTEM32/CMD.EXE
CGI-BIN/
```

Security Checklist for TCP/IP

- Connector Security
  - Set SECURITY=FULL (SKVCSCFG)
  - Define resource access rights (BSM/ESM)
  - Restrict remote access to specific users and IPs (SKVCSUSR)
- TCP/IP Security
  - SET SECURITY=ON in IPINIT member
  - Use Security Exit
  - Do not define users in IPINIT member

Security in a heterogeneous environment



Secure Internet access

Secure Socket Layer

Cryptography concepts

Encryption Facility

Covered in Session
Security Exploitation
with Crypto Hardware

Cry

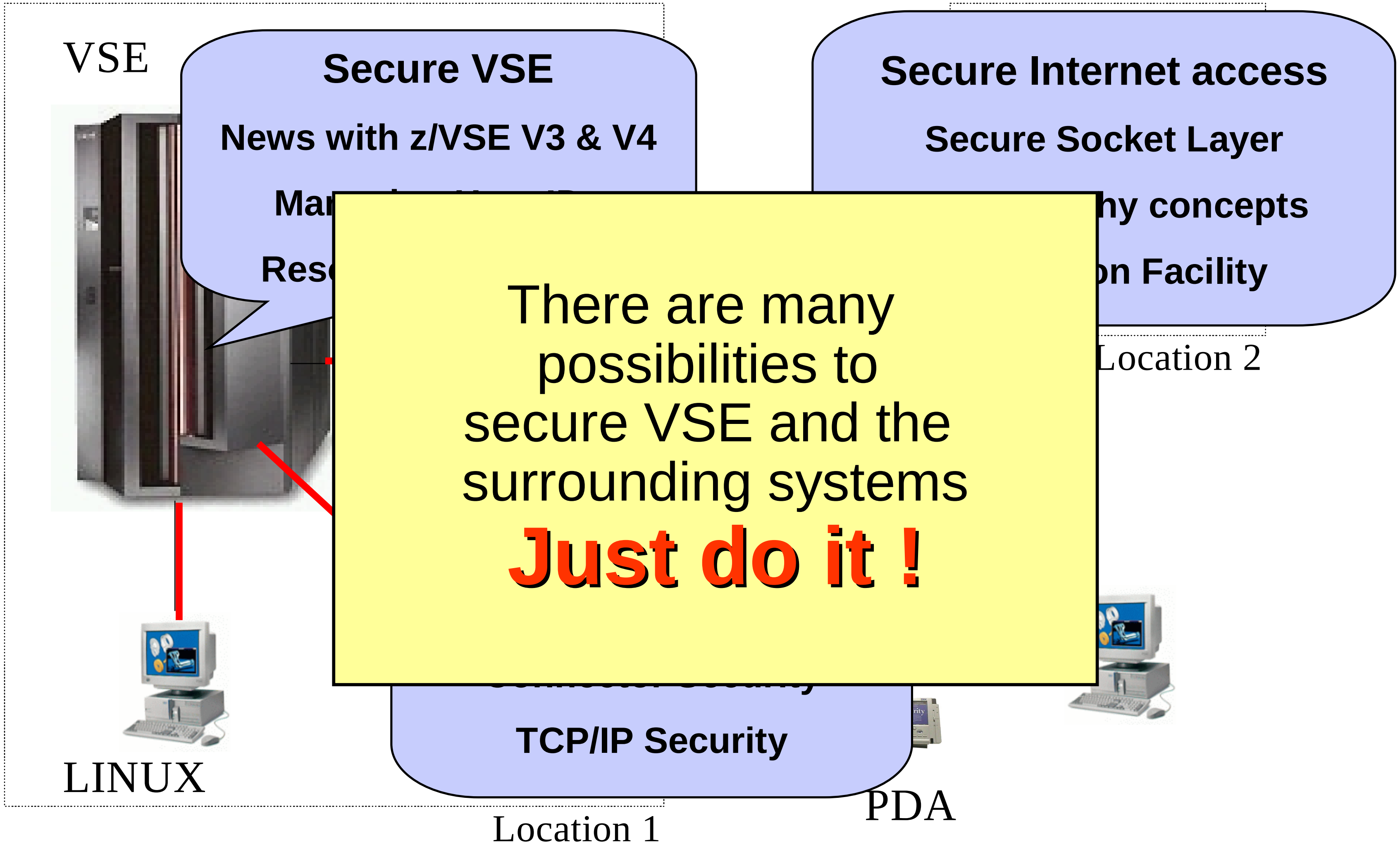
Certi

Secu Soc Laye SL)

Hardware Cr pto

Encryption Facility

Security in a heterogeneous environment



VSE

Secure VSE

News with z/VSE V3 & V4

Mar

Res

Secure Internet access

Secure Socket Layer

hy concepts

on Facility

Location 2

There are many possibilities to secure VSE and the surrounding systems

Just do it !

TCP/IP Security

LINUX

PDA

Location 1

Related Documentation

- New RedBook: Security on IBM z/VSE - SG24-7691
  - http://www.redbooks.ibm.com/redpieces/abstracts/sg247691.html
- IBM System z cryptography for highly secure transactions
  - http://www.ibm.com/systems/z/security/cryptography.html
- VSE Security Homepage
  - http://www.ibm.com/servers/eserver/zseries/zvse/documentation/security.html
- z/VSE Planning
- z/VSE Administration
- OS/390 Security Server External Security Interface (RACROUTE) Macro Reference (GC28-1922)
- OS/390 Security Server (RACF) Data Areas (SY27-2640)
- z/VSE V4R2.0 e-business Connectors, User's Guide
- CICS Enhancements Guide, GC34-5763

Questions ?

?