IBM System z Technical University

October 4–8, 2010 — Boston, MA

z/VSE Security – Best Practices

zDS01

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.

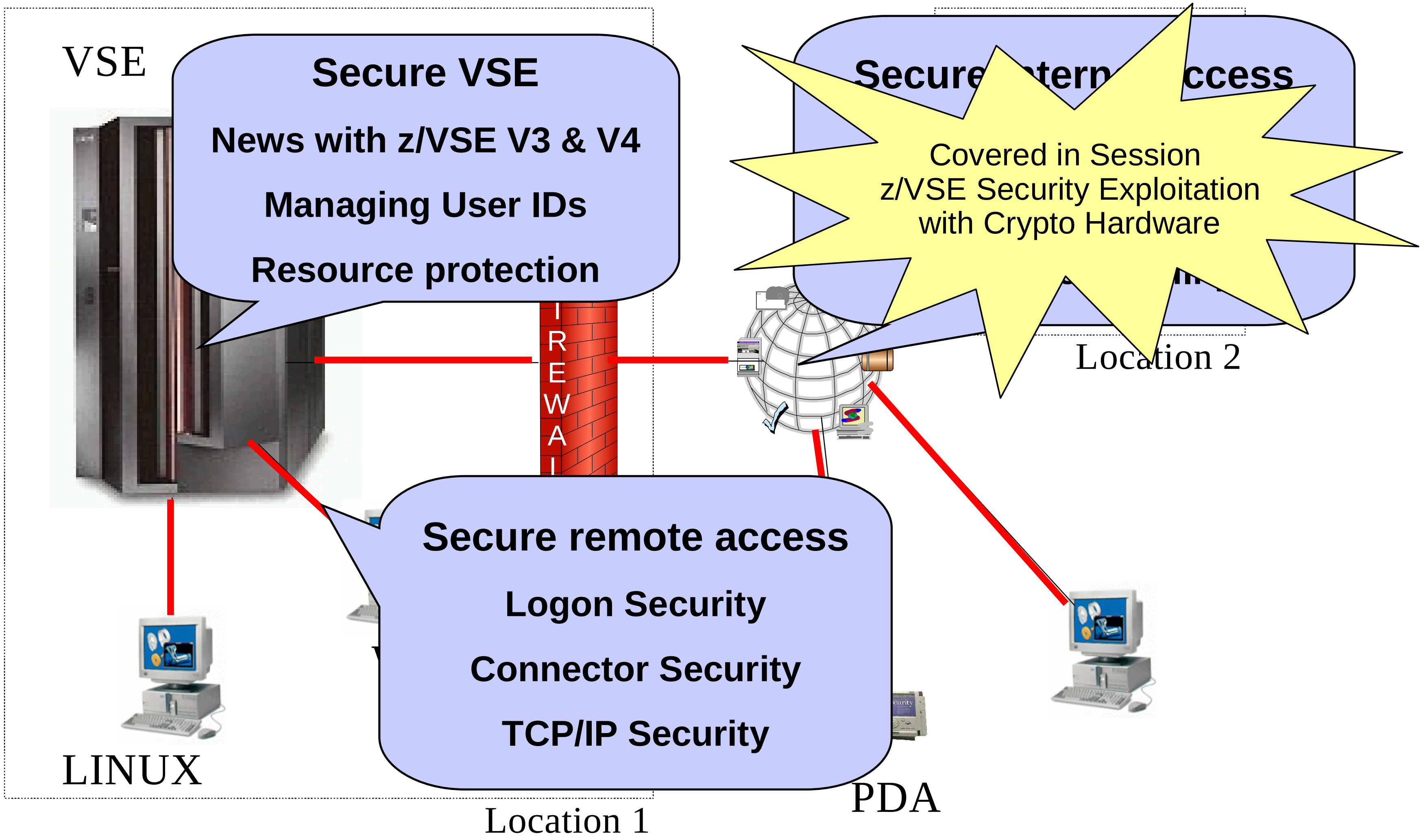
* All other products may be trademarks or registered trademarks of their respective companies.

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.

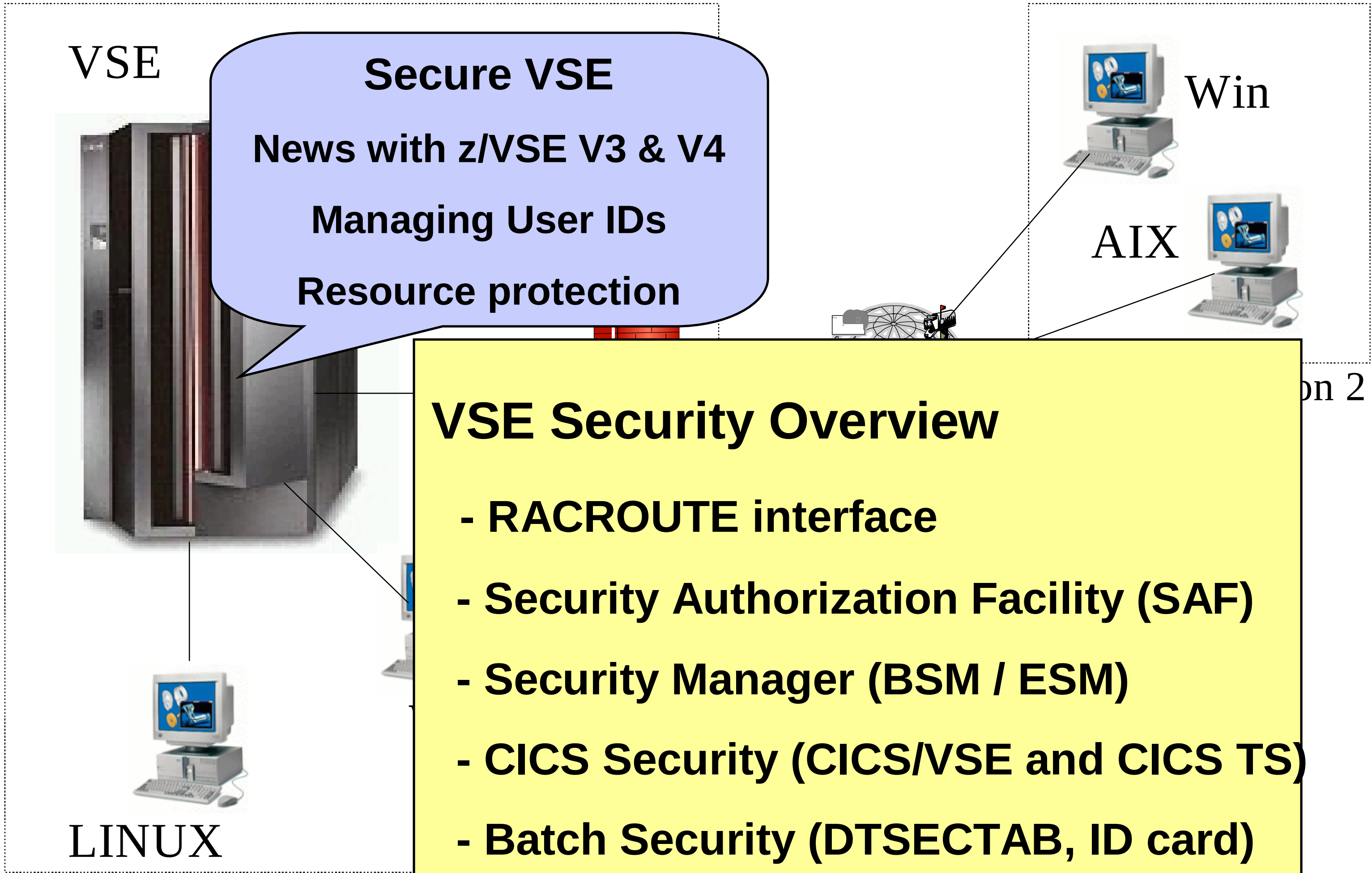
Security requirements

- **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



Security in a heterogeneous environment



Secure VSE

News with z/VSE V3 & V4

Managing User IDs

Resource protection

VSE Security Overview

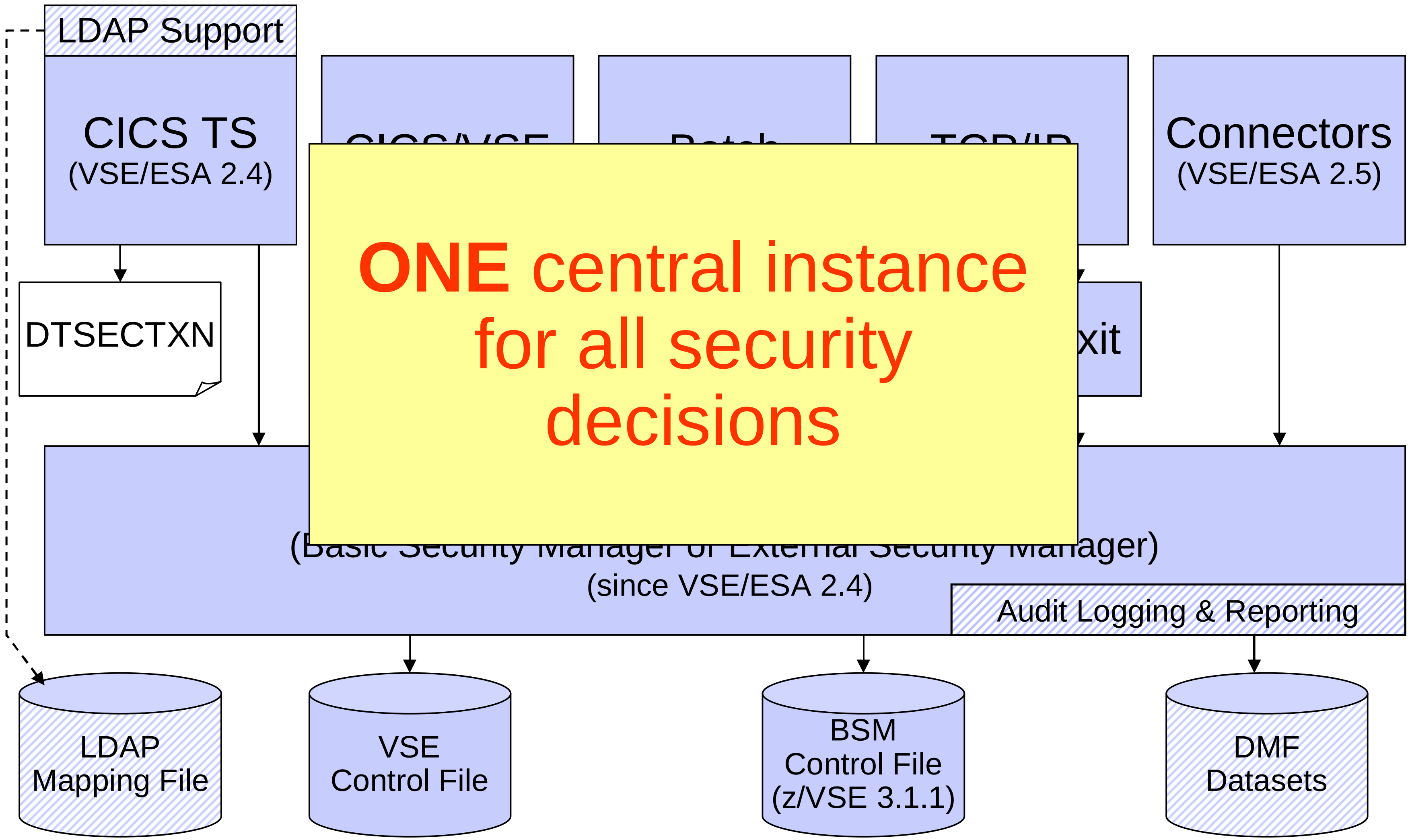
- RACROUTE interface
- Security Authorization Facility (SAF)
- Security Manager (BSM / ESM)
- CICS Security (CICS/VSE and CICS TS)
- Batch Security (DTSECTAB, ID card)

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 Components



Security Managers – BSM & ESM

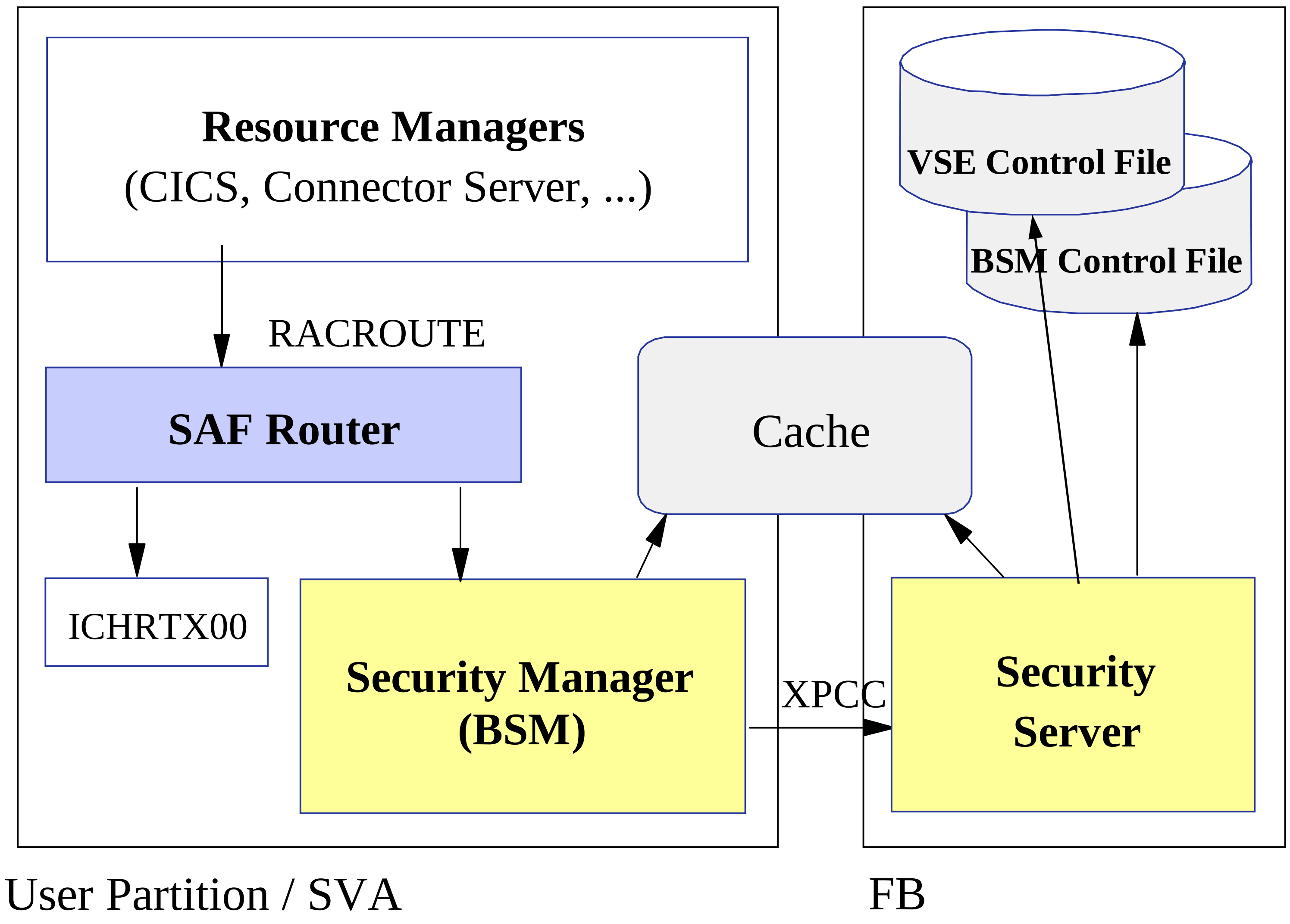
Basic Security Manager (BSM)

- 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



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**
  - User IDs can be added (connected) into a group
  - Permission can be granted based on groups or individual users
  - Replaces the security classes concept for CICS

- **Password rules can be changed by command**

- **New admin functions**
  - BSTADMIN (console or batch)
  - Interactive Interface Dialogs (28x)

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

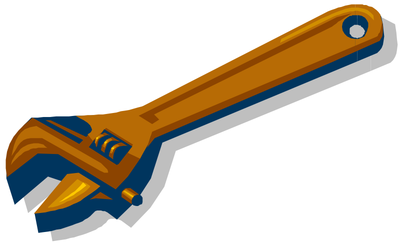
```
05.081 09:35:32                                BSM Report - Listing of Process Records
                                           E
                                           v  Q
                                           e  u
                          *Job/User        n  a
Date    Time               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 verification 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=R
05.076 12:26:18  HUGO                      1  8 Job=(CICSICCF) - User
                 HUGO MAYER                       Auth=(None),Reason=(No
05.076 12:26:29  SYSA                      1  0 Job=(PAUSEBG ) - User
                 AUGUST WONG                      Auth=(None),Reason=(No
05.076 12:26:30  SYSA                      2  0 Job=(PAUSEBG ) - Resou
                 AUGUST WONG                      Auth=(Administrator),R
                                                  Resource=MYAPPL.MYPRIN
05.076 12:26:33  SYSA                      1  8 Job=(PAUSEBG ) - User
                 AUGUST WONG                      Auth=(None),Reason=(No
```

```
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
```

Auditors can use reporting tools to generate

- Summary reports
- Detailed reports of all access attempts

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

- Enables users to sign on z/VSE using a single, comprehensive, corporate-wide ‘Identity Management’ systems (i.e. IBM Tivoli Identity Manager, e…)
- LDAP user-IDs and passwords can be up to 64 characters.
- Helps overcome VSE int… limits:
  - 4 character VSE/ICCF
  - 4 and 8 c…
  - up to 8 chara…
- LDAP sign… …BSM, ESM, etc.)
- z/VSE LDAP client…
  - IBM Tivoli Di…
  - z/VM LDAP server (w… …F repo…tory)
  - Microsoft Active Direc… OpenLDAP, Apache Directory server, Novell eDirectory, and many others.

Covered in more details in session zES03 - Integrating z/VSE into an Identity Management System

- Potential benefits include improved protection, consistent access rules, ease of use for end-users

Defining a new user-ID

- **Define a new user-ID**
  - Interactive Interface dialog **Maintain User Profiles** (211)
- **Connect the new user-ID to groups**
  - Interactive Interface dialog **Maintain Security Profiles** (282)
  - Show **User List** (option 6) and add the user-ID to the group
  - Add the user-ID or groups to the access list of the desired resource profiles, if needed
  - You can also use BSTADMIN to do this in batch.
- **Perform a BSM Security Rebuild to activate the changes**
- **If you are using LDAP Authentication, you also need to add the user-ID to the LDAP mapping file via IESLDUMA**

Maintaining user-IDs

If you make changes to a user-ID, don‘t forget to update the groups and resources as well:

- **When deleting a user-ID**
  - Remove it from the groups it is belonging to
  - Remove it from the access lists of any resource profiles
- **When updating a user-ID**
  - Adapt the groups it is belonging to, if required
  - Adapt the access lists of all resource profiles, if required

- Use the BSM Cross Reference Tool to find out where the user-ID is referenced (see separate foil)
- Perform a BSM Security Rebuild to activate the changes
- If you are using LDAP Authentication, you also need to update the user-ID in the LDAP mapping file via IESLDUMA

Group maintanance

- Per default there are GROUP01 to GROUP64
  - coresponding to the 64 CICS transaction security keys
- Define a new group
  - Interactive Interface dialog **Maintain Security Profiles** (282)
  - Use option 1 (Add) to add a new group
- Add user-IDs to the newly created group
  - Show **User List** (option 6) and add the User-ID to the group
- Do NOT create groups that are named the same as user-IDs
- You can also use BSTADMIN to do this in batch.
- Perform a BSM Security Rebuild to activate the changes

Resource profiles

- There are 2 repositories for resource profiles:
  - **DTSECTAB:** It contains the entries for z/VSE files, libraries, sublibraries, and members
  - **BSM Control File:** It keeps the profiles for all the new resource classes supported by BSM
- Access List specifies who (base on user-ID or group) has access (Read, Update, Alter) to the resource
- If the access list contains both, a user-ID and a group that contains the user-ID
  - then the access rights specified with the User-ID is effective

Migrating from older BSM versions

- Since z/VSE 3.1.1, BSM uses the BSM Control File instead of DTSECTXN
  - You may need to migrate transaction security definitions from DTSECTXN to BSM Control file

- The steps you can follow partly depends on:
  - The VSE system level from which you installed z/VSE
  - Whether you performed an FSU (Fast Service Upgrade) or an initial installation.
  - Whether you wish to retain the use of your previous security definitions.

- Please see Administration Manual Chapter 22 (page 325) for details
  - See the table that describes the steps you need to perform before and after migration of VSE

CICS Security

CICS/VSE 2.3:

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

CICS TS 1.1:

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

CICS TS Sign on

- **CICS signon is performed using**
  - 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 (BSM or ESM)
  - 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

- **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

- **Grant access to a ressource**
  - Per individual user
  - Per group

- **Resource security definitions under CICS TS**
  - Definition within single resource definition (e.g. file FILEA and FILEB)
    - Within `CEDA 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)
```

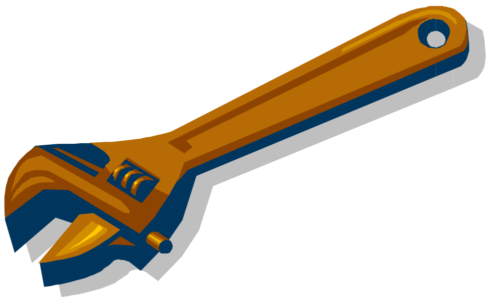
CICSUSER considerations & critical transactions

- **Every transaction runs under the context of a user-id**
  - If no user is signed on, it runs under the default user
    - DFHSIT: DFLTUSER=CICSUSER
- **CICSUSER is predefined after base install:**
  - Type 3 (ICCF is not allowed)
  - Is in GROUP01, GROUP60-GROUP64
    - GROUP01 and GROUP60 is required by Interactive Interface
- **Actions to perform after installation**
  - Do not allow this user to use critical transactions
  - Adjust groups this user is belonging to
- **You need to protect critical transactions to prevent system damage by users**

Transaction	Description
USER	Display Activity Dialog, send Message to all users
CEMT	Master terminal
CEDA	Resource definition online
CEDB	Like CEDA, but no INSTALL possible
CEDC	Like CEDA, but read only
CECI	Command level interpreter
CEDF/CEDX	Execution diagnoistic facility
CETR	Trace control
CESN/CESF	Sign on/sign off
DITT	Online Ditto
others ?	

CICS Security – Coexistence of CICS/VSE and CICS TS

- If you run both, CICS/VSE and CICS TS in parallel
  - You want to use the user profiles
- 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



Batch Security

- **ID statement or * $$ JOB specifies user id and password for a job**

```
* $$ JOB JNM=MYJOB,...,SEC=(user,password)
```

or

```
// ID USER=user,PWD=password
```

- **User id and password are verified against**
  - DTSECTAB
  - Security Manager (RACROUTE)

- **Subsystems (LIBR, VSAM, ...) uses this user id to verify access rights against DTSECTAB**

- **When you have batch security active (SYS SEC=YES), all your jobs need to specify a user-ID and password**
  - Either using the // ID statement within the job
  - or in the * $$ JOB card

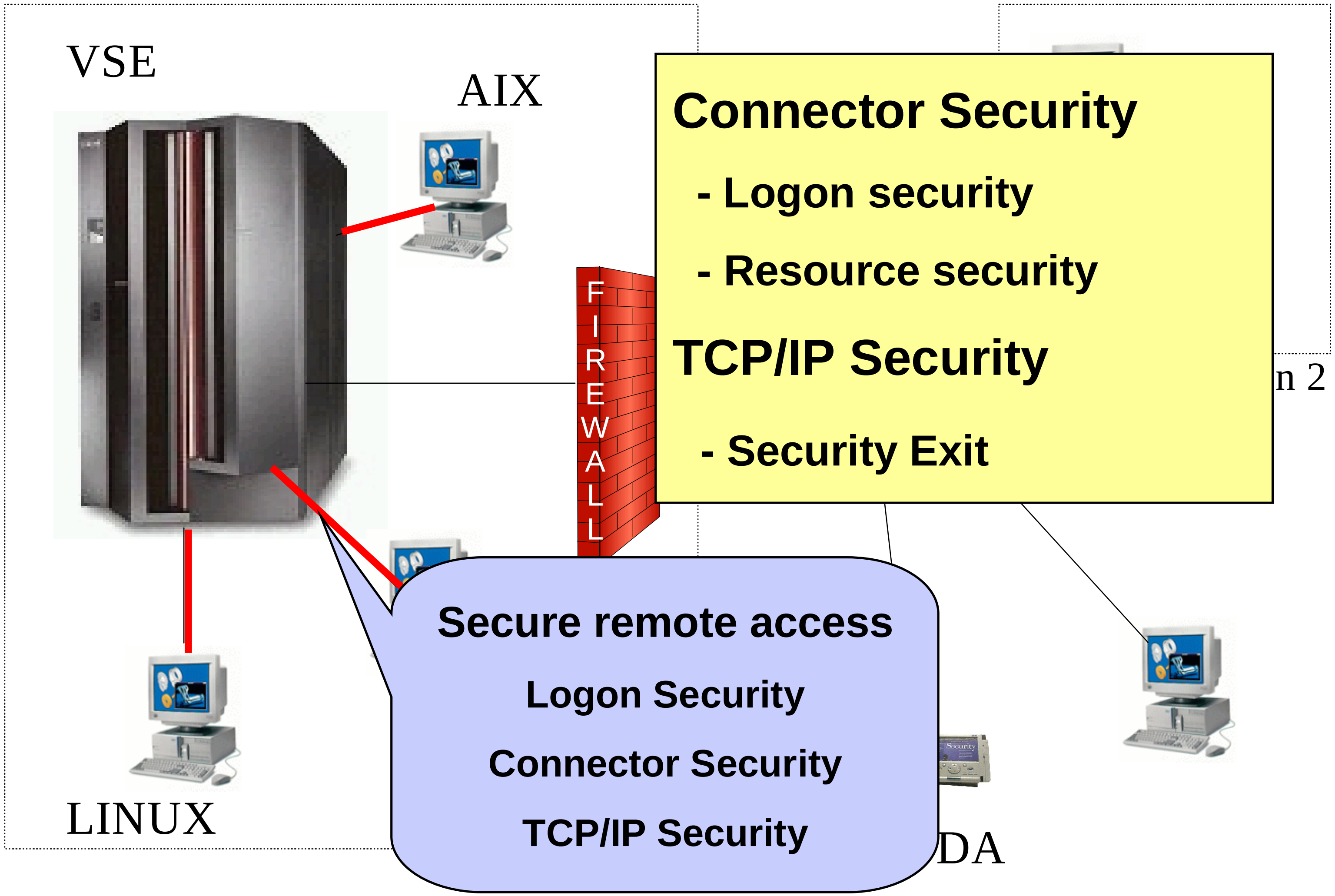
- **When you submit jobs from the ICCF library**
  - The submitted job automatically inherits the user-ID and password from the submitting user
  - No need to specify a // ID statement or user-ID in the * $$ JOB card

- **Inheritance only works if batch security is active at the time you do the submit**
  - Jobs that have been submitted prior to activating batch security do not have any inherited security information, you may have to re-submit those jobs

Security Checklist for VSE

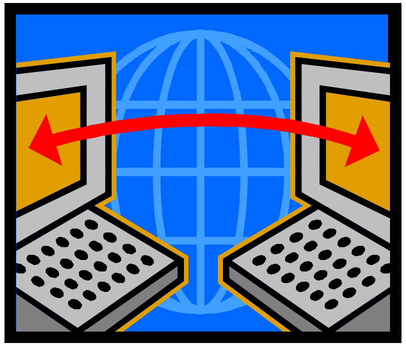
- **SYS SEC=YES/NO**
  - YES if batch security is required
  - Setup appropriate permissions for your resources
- **CICS SIT SEC=YES (!)**
  - If NO, all users can logon without a password
  - Protect the critical CICS transactions
- **Change passwords for predefined users**
  - POST, PROG, OPER, SYSA, ...

Security in a heterogeneous environment

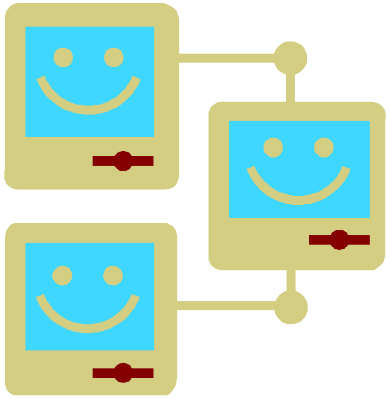


Why secure remote access ?

- **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)

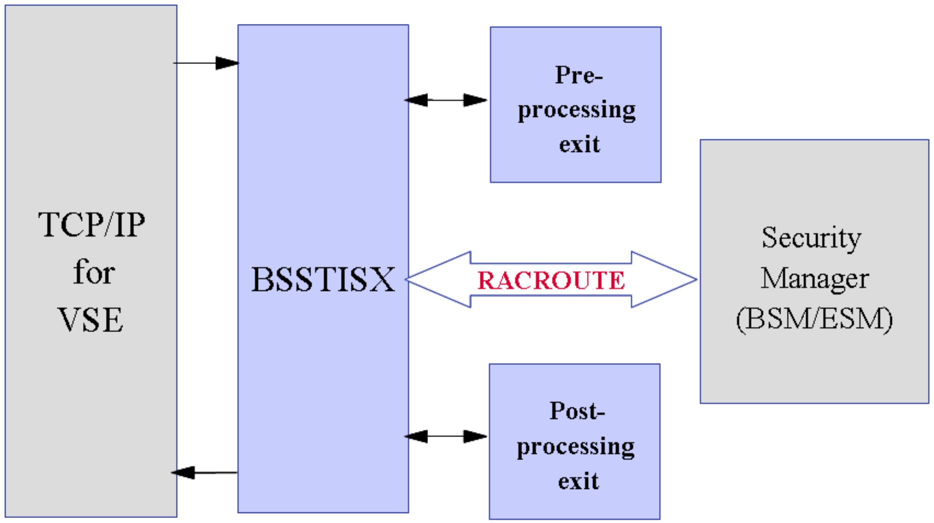


TCP/IP Security



- **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**
  - –Issues RACROUTE calls for
    - User identification and verification
    - Resource access control
    - VSE files, libraries, members
    - POWER entries
    - SITE commands



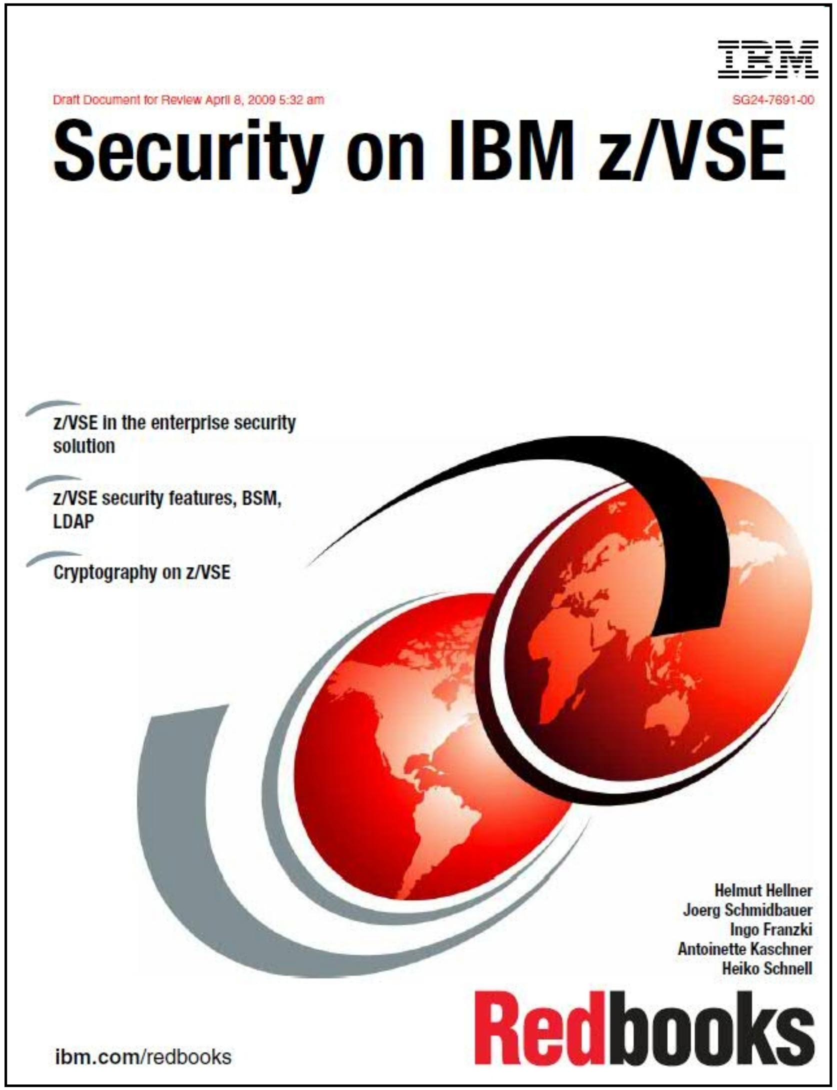
New Redbook: Security on IBM z/VSE - SG24-7691

Available since October 20, 2009
http://www.redbooks.ibm.com/redpieces/abstracts/sg247691.html

Explains security concepts as well as step by step setup

It covers:

- Basic Security Manager
- LDAP Authentication
- Cryptography & SSL
- TCP/IP Security
- SecureFTP & Secure telnet
- CICS Web Support Security
- Connector Security
- Security APIs



BSM Cross Reference Tool

- The z/VSE BSM Cross Reference Tool is intended to help administrators control the profile definitions in the BSM control file.
- Example:
  - When you delete a user-ID, you can use it to ensure that you have removed the user-ID from all access lists and groups.
- The following functions are provided:
  - List all groups and resource profiles which contain a specified user-ID.
  - List all resource profiles where a specified group is on the access list.
  - List all user-IDs found in the BSM control file but is not defined in the VSE control file.
  - List all resource profiles that allow any user-ID to access a resource (UACC not NONE).

```
// EXEC BSTXREF,PARM='GROUP=*'
1S54I  PHASE BSTXREF  IS TO BE FETCHED FROM IJSYSRS.SYSLIB

                                                 BSM Cross Reference
   Report
                                                       of All Groups


 Occurrences of group GROUP01

 Group description TRANSEC CLASS MIGRAT
 Connect group for user $SRV
 Connect group for user CICSUSER
 Connect group for user OPER
 Connect group for user PROG
 Update authority in access list of profile FACILITY DFHRCF.BRSLPU
 Update authority in access list of profile FACILITY DFHRCF.BRSL01
```

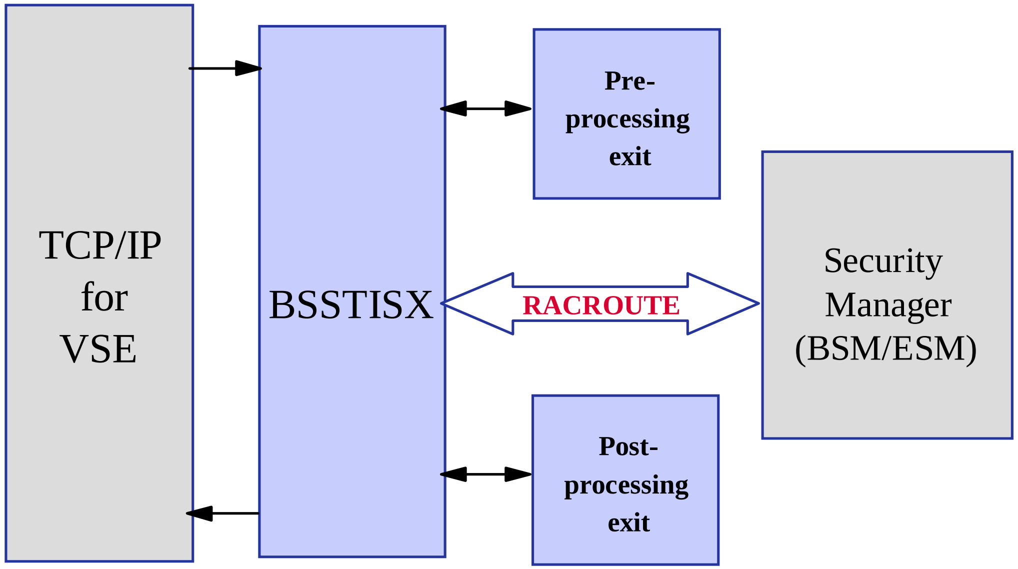
http://www.ibm.com/systems/z/os/zvse/downloads/tools.html#bsmxref

RACROUTE encapsulation services for TCP/IP

- The IBM-provided TCP/IP security exit BSSTISX supports a pre- and post-processing interface
  - These interfaces are solely intended to be used by customers to add self-written security checks

- In particular when it is used to exploit the security definitions of the security manager, e.g. special profiles of the resource class FACILITY, normally one has to use the RACROUTE macro interface
  - However, coding of RACROUTE requests can be very complex

- Therefore these services were provided with BSSTXRRS to encapsulate the three basic RACROUTE requests:
  - sign on
  - sign off
  - authorization checking for resource access.



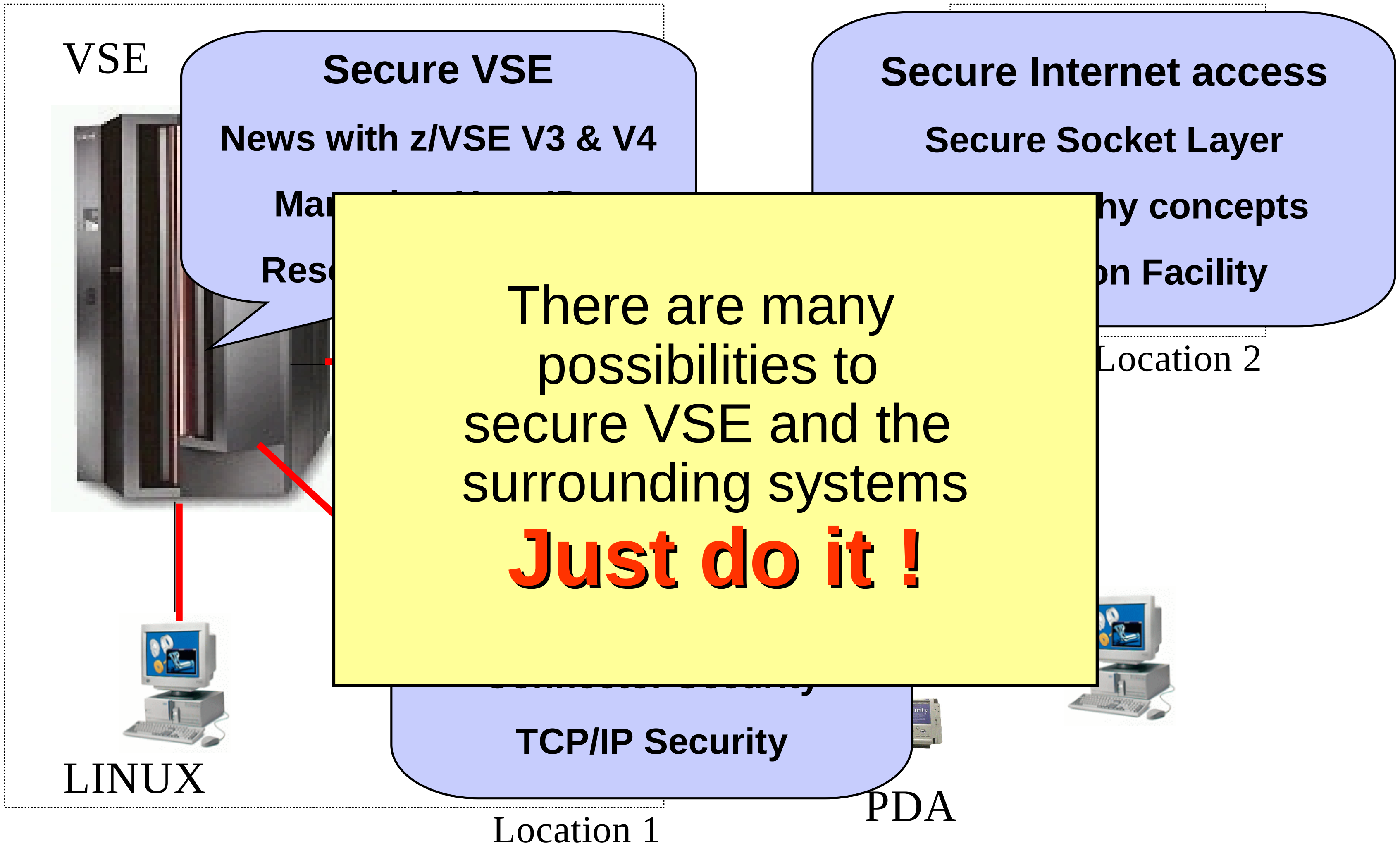
http://www.ibm.com/systems/z/os/zvse/downloads/tools.html#racroute

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
- **z/VSE Security Homepage**
  - http://www.ibm.com/systems/z/os/zvse/documentation/security.html
- **IBM Manuals**
  - 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 e-business Connectors, User's Guide
  - CICS Enhancements Guide, GC34-5763

IBM

Security in a heterogeneous environment



Questions ?

?