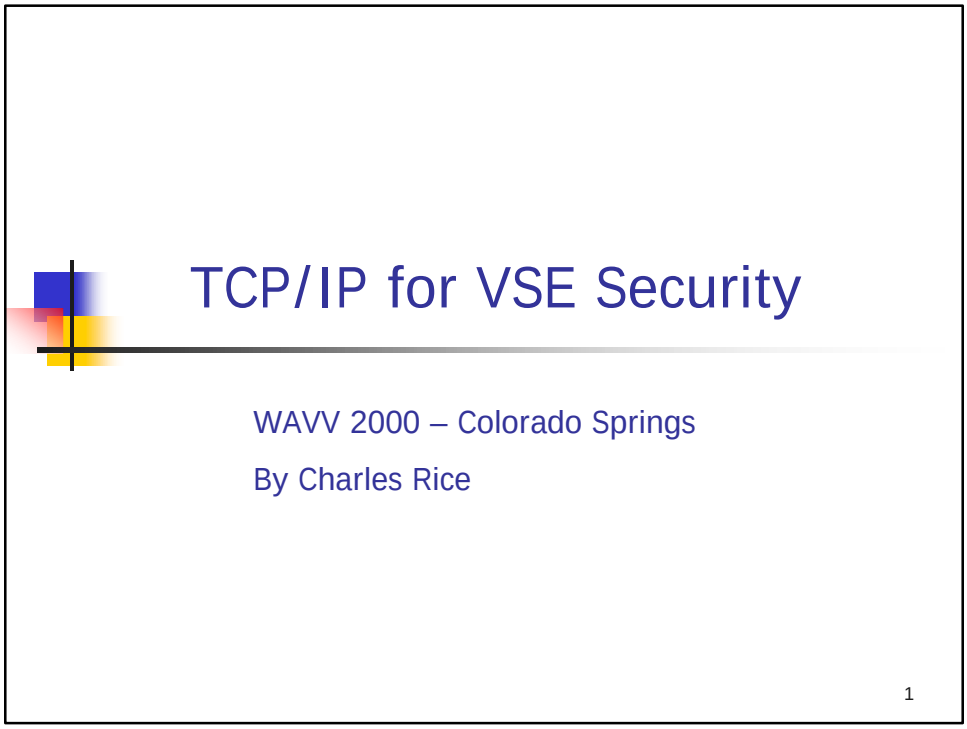
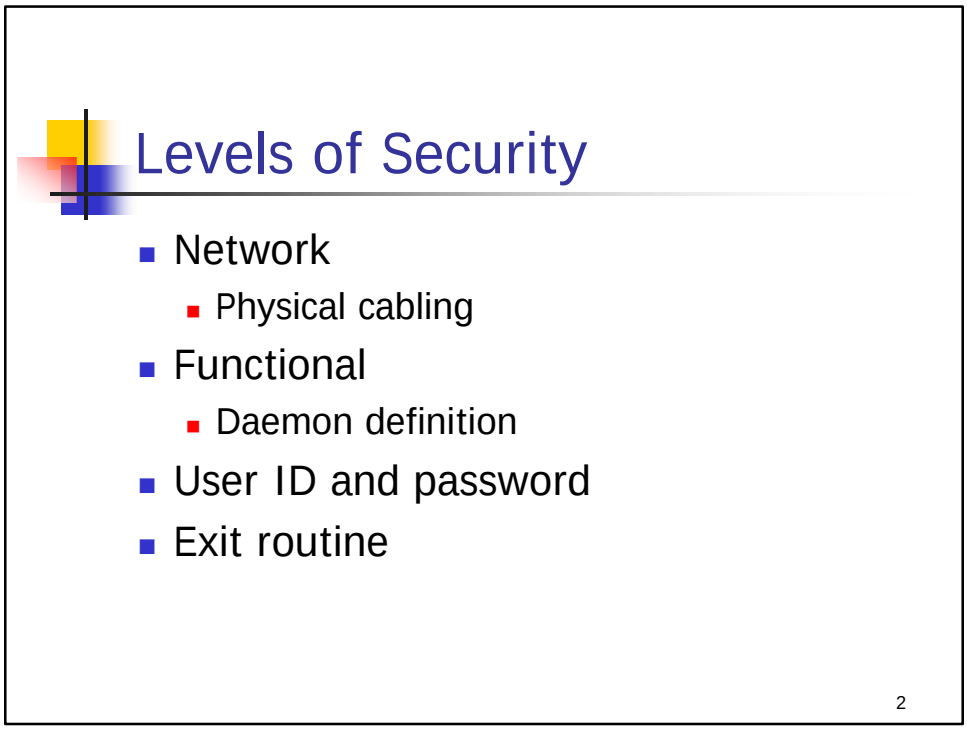

TCP/IP for VSE Security
WAVV 2000 – Colorado Springs
By Charles Rice
1


Levels of Security
Network
Physical cabling
Functional
Daemon definition
User ID and password
Exit routine
2

Data Set Security

- Do not define files unless you need access to that file via FTP or NFS
- Use “DEFINE FILE” statement for each file to be made available
- Use the “READ-ONLY” option
- Do not use “DEFINE FILESYS”
- Understand implications of using “DEFINE VSAMCAT”

3

User ID and Password

- Defined with a “DEFINE USER” command
- Part of the initialization deck
- Anyone who can issue VSE operator commands can define User Ids
- SET PASSWORD command
  - Requires a password be entered to msg the TCP/IP partition
  - Password will appear on SYSLOG

4

SET CONSOLE_PORT

- Use of this command prevents TCP/IP commands from being entered on the operator console
- TCP/IP commands can only be entered via TELNET to the specified port number

5

SET ISOLATION

- Default is OFF
- When set to ON
  - Remote users cannot initiate connections
  - FTP is not functional in either direction
  - LPR and Telnet are functional
  - Only sockets specifying ACTIVE are accepted

6

SET SECURITY

- When ON
  - Remote user is prompted for User ID and Password
  - Passed to security exit for validation if present
  - If no security exit, user table is searched
- When OFF
  - Remote user is prompted for User ID and Password
  - No validation takes place

7

TN3270 Security

- Use the “IPADDR” option on the “DEFINE TELNETD” command
- Use a port number other than the default
- Use on “MENU” option with User-ID and Password will require validation at Logon
- Use the “TARGET” option to restrict access to a particular VTAM application

8

FTP Security

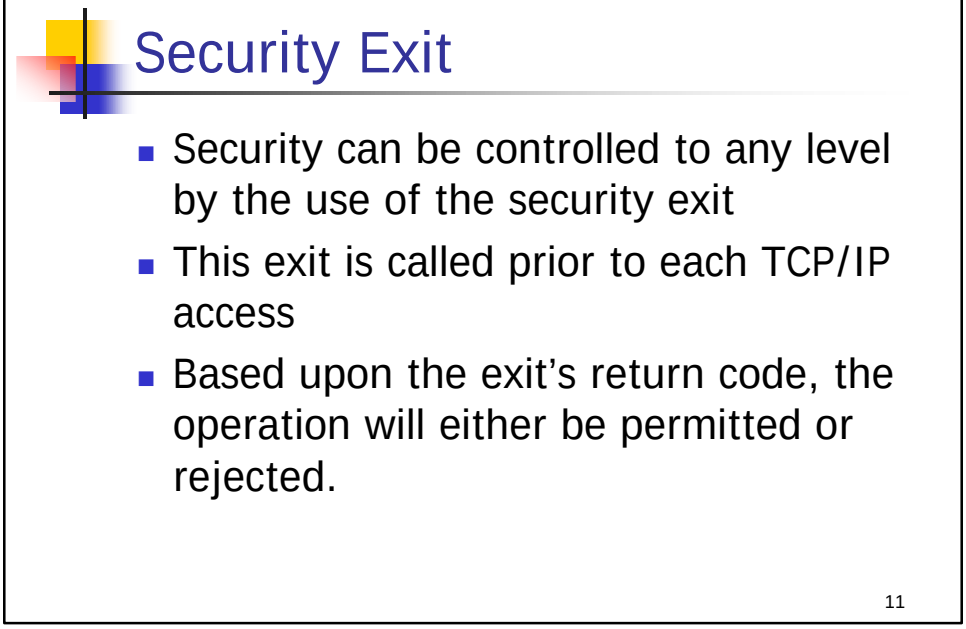
- Do not define any FTP deamons
- Use the “IPADDR” option on the “DEFINE FTPD” command
- Use a port number other than the default

9

HTTP Security

- Confine access to one sub-library
  - Use Root and Confine parameters on Define HTTPD
- SECURE=YES parameter on Define HTTPD
  - PASSWORD.HTML
  - VIOLATED.HTML
  - BLANKING.HTML

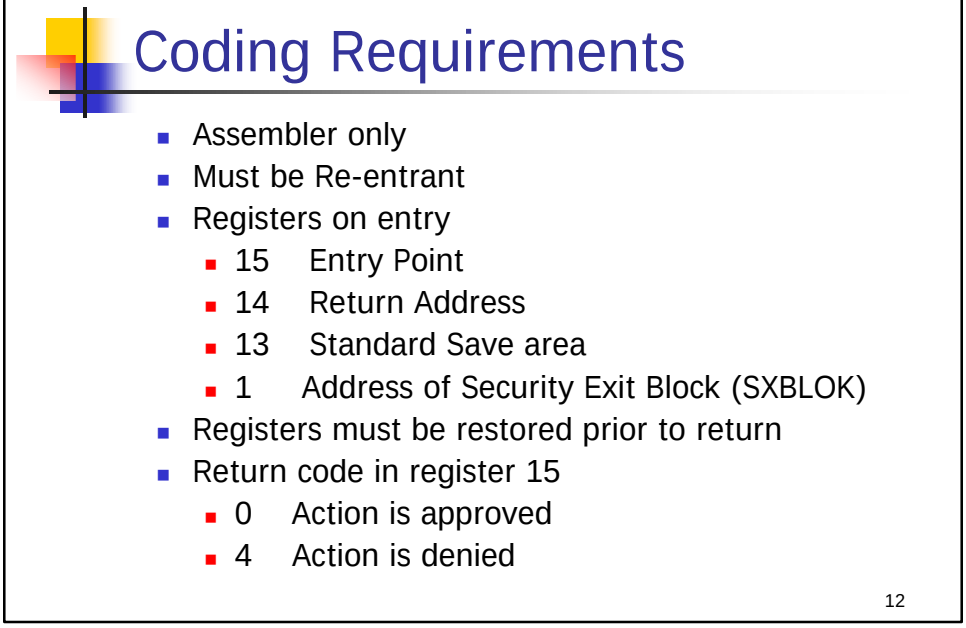
10



Security Exit

- Security can be controlled to any level by the use of the security exit
- This exit is called prior to each TCP/IP access
- Based upon the exit's return code, the operation will either be permitted or rejected.

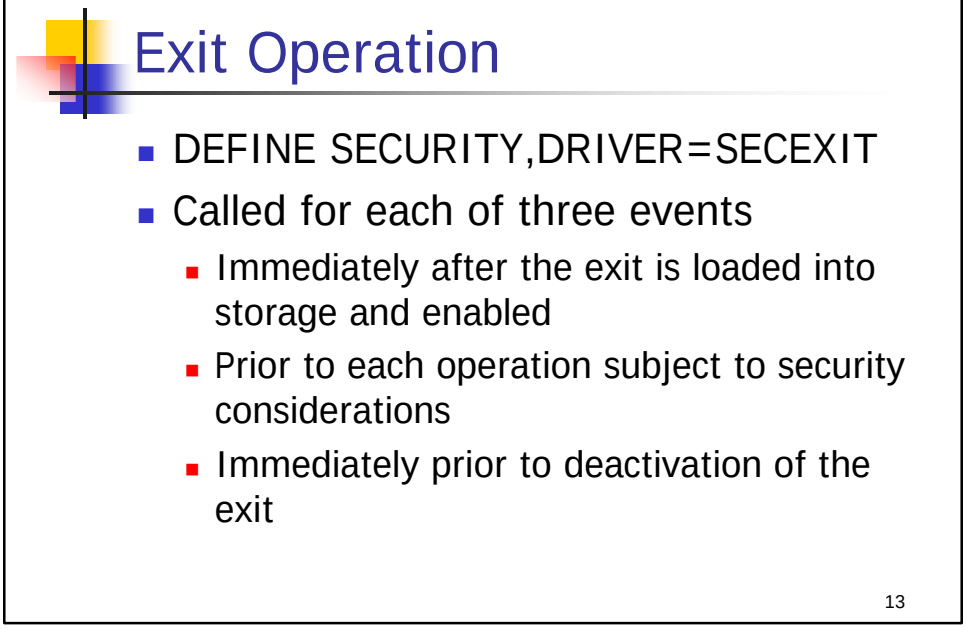
11



Coding Requirements

- Assembler only
- Must be Re-entrant
- Registers on entry
  - 15 Entry Point
  - 14 Return Address
  - 13 Standard Save area
  - 1 Address of Security Exit Block (SXBLOK)
- Registers must be restored prior to return
- Return code in register 15
  - 0 Action is approved
  - 4 Action is denied

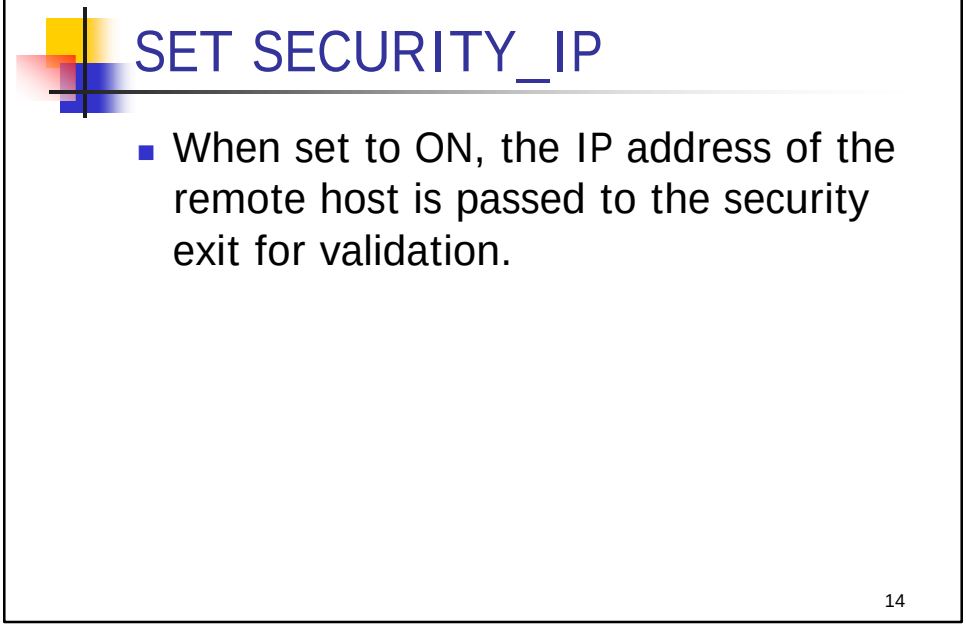
12



Exit Operation

- DEFINE SECURITY,DRIVER=SECEXIT
- Called for each of three events
  - Immediately after the exit is loaded into storage and enabled
  - Prior to each operation subject to security considerations
  - Immediately prior to deactivation of the exit

13



SET SECURITY_IP

- When set to ON, the IP address of the remote host is passed to the security exit for validation.

14

SET SECURITY_ARP

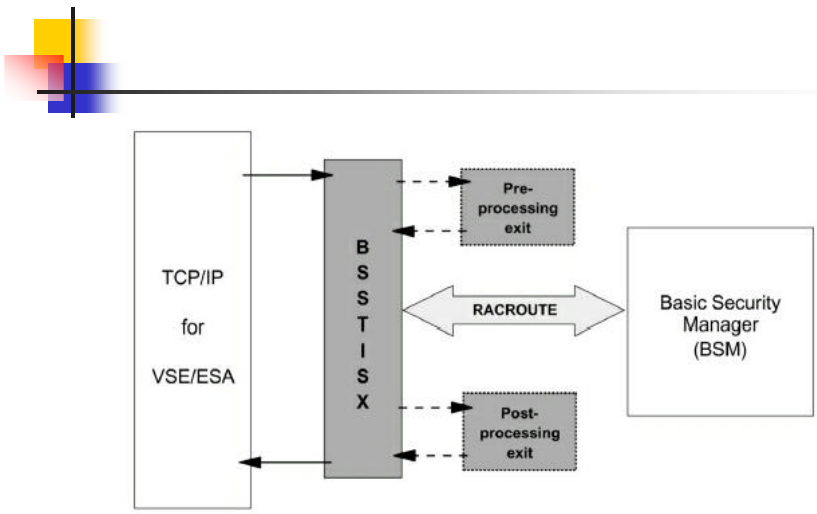
- When set to ON, each ARP request will be passed to the security exit for validation.

15

Using Basic Security Manager

- TCP/IP security exit provided with interface to BSM
- Available on VSE/ESA 2.4 with APAR DY45309
- Shipped with VSE/ESA 2.5
- Documented in SC33-6601-03 – TCP/IP for VSE/ESA – IBM Program Setup and Supplementary Information

16

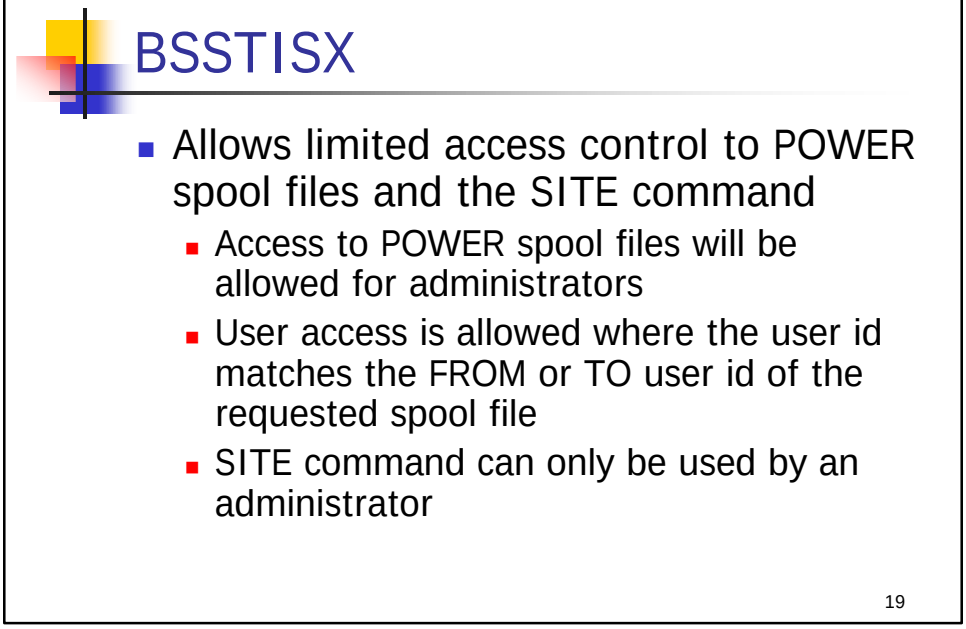


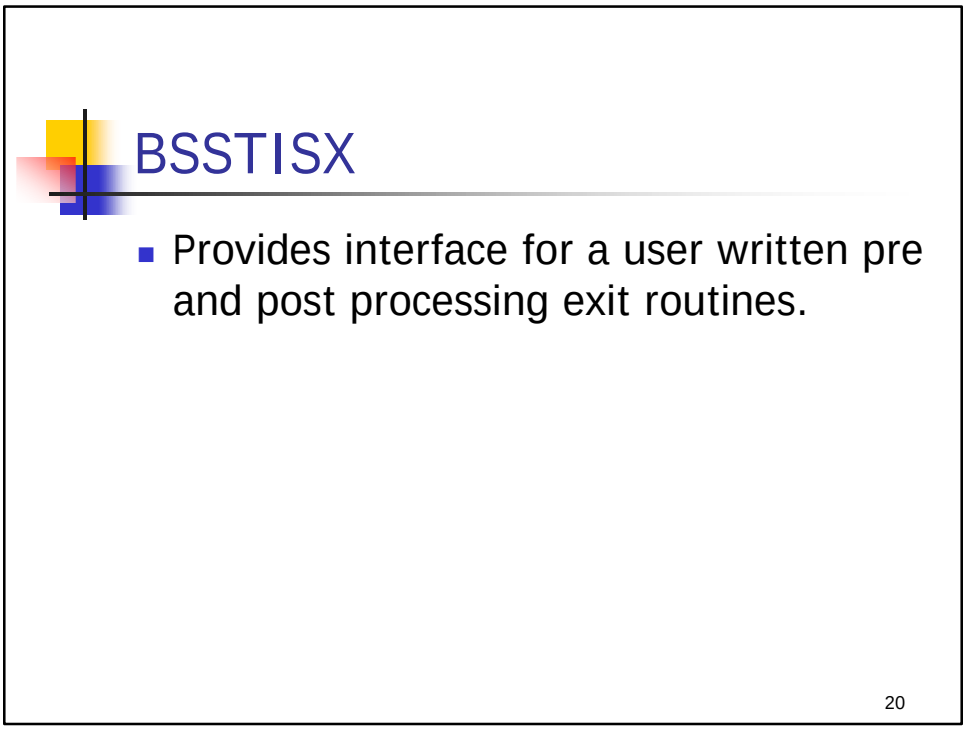
17

BSSTISX

- Issues RACROUTE requests to process user id and password
- Issues RACROUTE requests to process resource access control for VSE files, libraries, and members.
- Works with Top Secret also

18


BSSTISX
Allows limited access control to POWER spool files and the SITE command
Access to POWER spool files will be allowed for administrators
User access is allowed where the user id matches the FROM or TO user id of the requested spool file
SITE command can only be used by an administrator
19

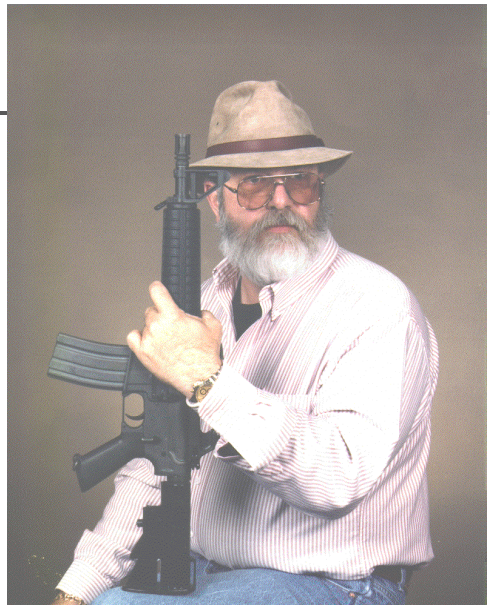

BSSTISX
Provides interface for a user written pre and post processing exit routines.
20

TCP/IP for VSE Security

If all this fails ...

21

THE LAST RESORT



22