E79 -CA-Top Secret

2000 VSE/ESA Technical Conference

Orlando, FL

RETURN TO INDEX

Agenda

- CA-Top Secret Overview
  - – VSE/ESA 2.4 What is new ?
  - – The CA Solution !
  - – Fundamentals
  - – Implementation
  - – Customization
  - – VSE/ESA to OS/390 migration path

VSE/ESA 2.4 What is new ?

- New CICS/TS 1.1 with External Security
- New RACROUTE security router support
- Limited OS/390 macro call support
- Next release will offer CICS/TS 1.3 Web based access
- New RACROUTE based DITTO/ESA
- BSM and DTSECTAB instead of RACF
- CA-Top-Secret marketed by IBM as ESM product

The CA Solution !

- CA-Top Secret for VSE/ESA 3.0 !
- A Complete RACROUTE based security solution for VSE/ESA 1.4 and above !
- Based upon CA-Top Secret for OS/390 5.1
- Runs on ANY IBM supported VSE/ESA release.
- Sold and marketed by IBM as the preferred security solution (ESM) for VSE/ESA 2.4 !!

The CA Solution ! (cont.)

- Supports CICS/2.3 and CICS/TS 1.1
- Not just signon and transactions, ANY CICS resource is protected.
- Full support for VSE Library, Sub-Library, VSAM and native Datasets.
- Shares Security Database with CA-Top Secret for OS/390 5.1 and CA-Top Secret for VM 1.4

The CA Solution ! (cont.)

- Prevents accidental deletion of protected datasets
- Provides for audit tracking and reporting of security events
- Allows for various password protection and algorithms
- Provides APF like protection scheme on VSE/ESA 2.4 systems
- Provides API calls to Vendor and user applications, including many Computer Associates products

The CA Solution ! (cont.)

- Provides OS/390 JES2 like VERIFYX processing for NODES protection of jobs.
- Allows for Automatic Userid inheritance of jobs submitted from CMS or CICS
- Uses CA-CIS ENF (CA-90s) ENF services to add Record and screen level security to CICS.
- Interfaces with IBM Ditto utility via RACROUTE calls.
- Allows network propagation of Security via CPF
- Interfaces to Unicenter/TNG security

CA-Top Secret Overview

- CA-Top Secret Fundamentals
- CA-Top Secret Implementation
- CA-Top Secret Customization

CA-Top Secret VSE Fundamentals

- System Entry Validation
- Resource Protection
- Distributed Security
- Information Repositories
- Logging And Audit Capabilities
- CA-CIS Architecture

System Entry Validation

- Accessor ID (ACID) And Password
- Password Protection Controls
- Facility Access Restriction
- Terminal (Port) Or CPU Access
- Day Of Week / Calendar Access
- Time Of Day Access

Password Protection Controls

- Definition And Change Criteria
- Expiration Interval, First Use Expiration
- Password History
- Password Violation Threshold

Definition And Change Criteria

- Minimum Length
- Reject “Close Variant” Of ACID Or Name
- Limit Repeating Characters
- Force Structured Passwords Via Masks
- Restricted Password List
- Random Passwords

What Is A Facility ?

- A Way Of Grouping Control Options Within A Subsystem That Users Sign On To
- Facilities Matrix Table
- Batch, CICSPROD, CICSTEST
- Restrict Access By Facility Name

Resource Protection

- Resource Definition Table (RDT)
- Resource Must Be Owned By An ACID
- Access Permitted To Other ACIDs
- Ownership Implies Full Access
- Security Validation Algorithm

Resource Definition Table

- Unique Resource Class
- DSNAME, VSELIB, OTRAN, FCT
- Access Levels And Attributes
- Default Protection
- Pre-defined At Install Time, Can Be Modified

Distributed Security

- Shared Security File - VSE, MVS, VM
- Command Propagation Facility (CPF)
- CA-Unicenter TNG - Workstation Administration
- Goal Is Single-Point Administration

Information Repositories

- Security File - Encrypted Security Records
- Parameter File - Control Options, Facility Matrix
- Backup File - Automatic Or By Request
- Recovery File - Record Administrative Changes
- CPF Files - Recovery And Journal
- Audit/Tracking File(s) - Violation, Access, Audit

Logging And Audit Capabilities

- Audit / Tracking File(s)
- Violation And Access Recording
- All Changes To Security File
- Selective Auditing Of Users And/Or Resources
- CICS Data Management Facility
  - SMF compatible records

Logging And Audit Utilities

- TSSTRACK - Online Realtime Monitor
- TSSUTIL - Report Audit/Tracking File Events
- TSSAUDIT - Report Recovery File Events
- TSSCHART - Security File Block Charts
- TSSCFILE - Flat File From TSS LIST Output

CA-CIS Architecture

- CAIENF - Event Notification Facility
- CAISSF - Standard Security Facility
- CAICCI - Common Communications Interface
- CAIESI - External Security Interface
- CA-EARL - Ad-hoc Report Generation Language

CA-Top Secret Implementation

- Security Modes
- Defining ACIDs
- Defining Administrators
- Resource Security Validation
- Displaying Information
- CICS Specific Security

Security Modes

- Dormant - Validation Not Active
  - Administrators go through normal logon processing
  - User ACID logons do not display messages
- Warn - Log Violations But Allow Access
- Implement - Fail Only Defined Users/Resources
- Fail - Full Access Control

Security Mode Levels

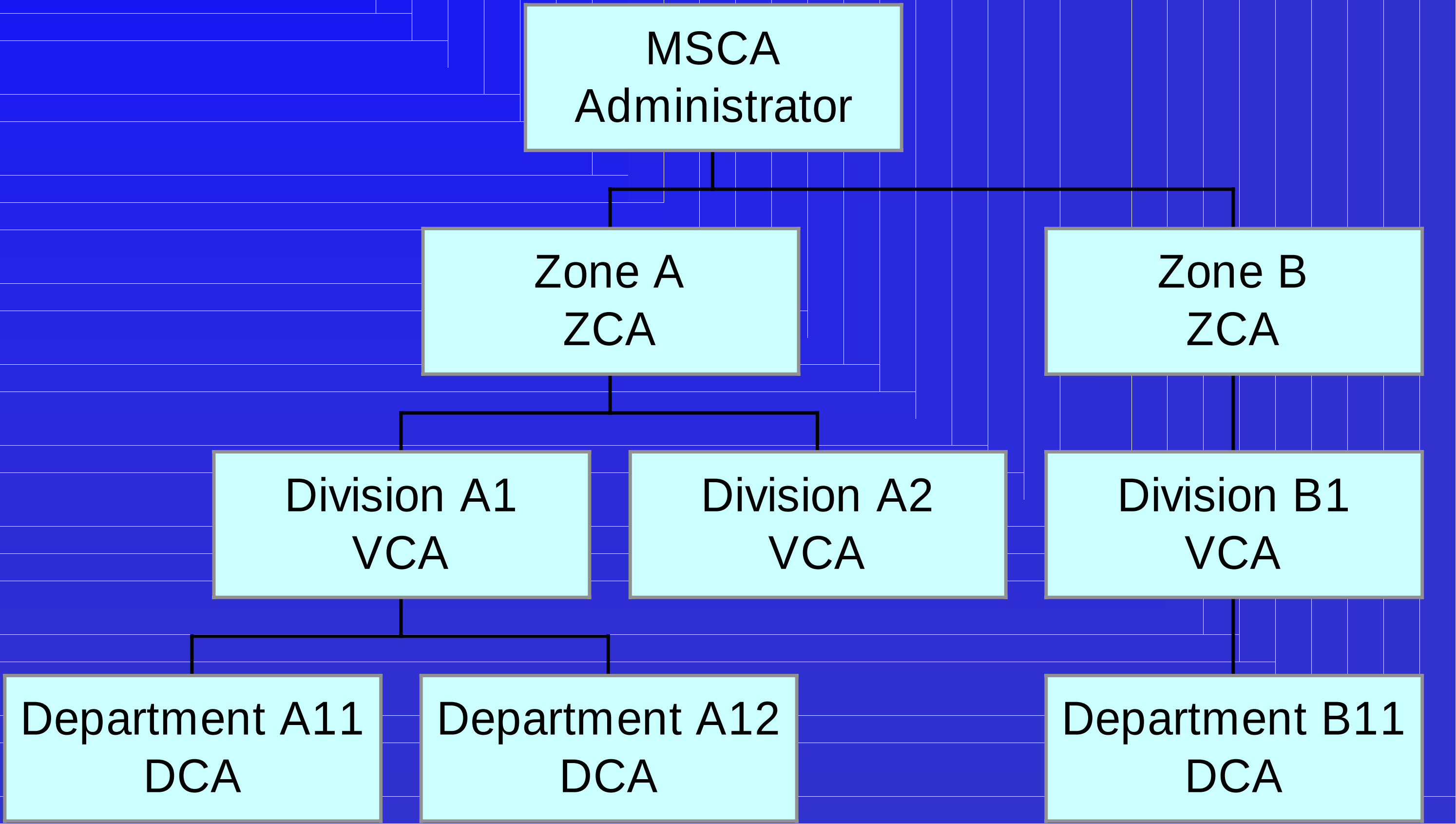
- Global - Control Option
- Facility - Facility Matrix
- Profile - Permit Mode
- User - Permit Mode
- Resource - Permit ACTION(FAIL)

Defining ACIDs

- Functional ACIDs
  - User, Profile, Control
- Organizational ACIDs
  - Department, Division, Zone
- Structured Hierarchy

Organizational Chart

Organizational Hierarchy



MSCA
Administrator

Zone A
ZCA

Zone B
ZCA

Division A1
VCA

Division A2
VCA

Division B1
VCA

Department A11
DCA

Department A12
DCA

Department B11
DCA

Defining ACIDs

- TSS CREATE(USER01) NAME(‘USER01’) TYPE(USER) PASSWORD(USER01,30,EXP) DEPT(DEPT01) FAC(BATCH,CICSPROD)
- Every User And Profile Acid Must Be Associated With A Single Department ACID

Special ACIDs

- ALL Record
  - – Identifies resources globally accessible to all signed on users
- AUDIT Record
  - – Stores resource names to be audited
- APPCLU Record
  - – Stores names and security requirements of logical units (Lus) involved in APPC conversations

Special ACIDs

- Resource Descriptor Table Record
  - – Contains pre-defined resource classes and their attributes
- Field Descriptor Table Record
  - – Defines fields that can be attached to ACIDs, such as OPIDENT
- Static Definition Table Record
  - – Stores static data for authorization purposes, such as CALENDAR, TIMEREC, MASKREC, SELECT

Defining Administrators

- MSCA - Master Security Control Acid
- SCA - Central Control Acid
- LSCA - Limited Central Control Acid
- ZCA - Zone Control Acid
- VCA - Division Control Acid
- DCA - Department Control Acid

Assigning Administrative Authority

- ACID - Create, Maintain, Audit
- Data - Password, CICS, Admin
- Resource - Own, XAUTH, Info
- Facility - Grant Authorization
- Scope - LSCA Only

Assigning Administrative Authority

- MISC1 - LTIME, Suspend, RDT
- MISC2 - SMS, TSO, PC
- MISC3 - Static Definition Table (SDT)
- MISC8 - List RDT, SDT, FDT
- MISC9 - Bypass, Generic

Resource Security Validation

- Define Resources - RDT
- Assign Resource Ownership
  - Department, Division, or Zone ACID
- Permit Resource Access
  - User or Profile ACID

Assigning Resource Ownership

- TSS ADD(DEPT01) DSN(PAYROLL.FILE.001)
- Generic Prefixing
  - DSN(PAYROLL)
- Dataset Name Masking
  - floating pattern, variable character substitution
  - index substitution, fixed position substitution
  - ACID substitution

Permit Resource Access

- TSS PERMIT(PROF01) DSN(PAYROLL) ACCESS(READ)
- TSS ADD(USER01) PROFILE(PROF01)
- Permit Access To Profiles
- Add Profile To User (Maximum 254)

Restricting Resource Access

- Facility
- Source - Terminal Or CPU
- Time / Date
- Program Path
- Access Level - READ, UPDATE, CREATE,…
- RLP And SLP In CICS

Security Validation Algorithm

- Search User, Profile, And “ALL” ACIDs
- Search For “Best Fit” Permit
  - TSS PER(PROF01) OTRAN(CE)
  - TSS PER(PROF01) OTRAN(CECI)
- OVERRIDE|MERGE , ALLOVER|ALLMERGE
- Control Option Or RDT Attribute

Displaying Information

- TSS LIST - Any ACID And RDT,SDT,FDT
- TSS WHOHAS - Resource Permissions
- TSS WHOOWNS - Resource Ownership
- TSS WHOAMI - Current User
- TSS MODIFY - Control Options / Facility Matrix

TSS WHOOWNS

– Examples:

```
TSS WHOOWNS DSN(ABCXYZ.PROD)
KENN  OWNS DATASET ABCXYZ.
TSS3001       WHOOWNS FUNCTION SUCCESSFUL


TSS WHOOWNS DSN(ABC)
TCSLFMD       OWNS DATASET     ABC.JCL.CNTL
STRTE01       OWNS DATASET     ABCD.
KENN  OWNS DATASET     ABCXYX.
SPDEPT        OWNS DATASET     ABC1.
SPDEPT        OWNS DATASET     ABC2
TSS300I       WHOOWNS FUNCTION SUCCESSFUL


TSS WHOOWNS DSN(XYZ)
QASDEP2       OWNS DATASET     XYZ.
KENN  OWNS DATASET     XYZ99.TEST.LOAD
TSS300I       WHOOWNS FUNCTION SUCCESSFUL
```

TSS WHOHAS

```
 TSS WHOHAS   FCT(DFH)
    RESOURCE = DFH                   OWNER(CICSDEPT)
       XAUTH = DFHCSD                 ACID(TLC532  )
      ACCESS = ALL
       XAUTH = DFHCSD                 ACID(TLC569  )
      ACCESS = READ
       XAUTH = DFHCSD                 ACID(SPPGRP1 )
      ACCESS = READ
      ACTION = FAIL,DENY
       XAUTH = DFHKHI                 ACID(TLC569  )
      ACCESS = ALL
       XAUTH = DFHKHI                 ACID(SPPGRP1 )
      ACCESS = ALL

TSS300I WHOHAS FUNCTION SUCCESSFUL
```

VSE/ESA to OS/390 Conversions

- Same Security Databases used
- Almost Identical Resource names
- CICS considerations identical
- But, consider implications for APF
- Maybe minor User callable services changes
- RACROUTE calls are identical

Closing

- Questions ???