SHARE
Technology · Connections · Results

CA Top Secret and CA ACF2 101

Reg Harbeck
CA

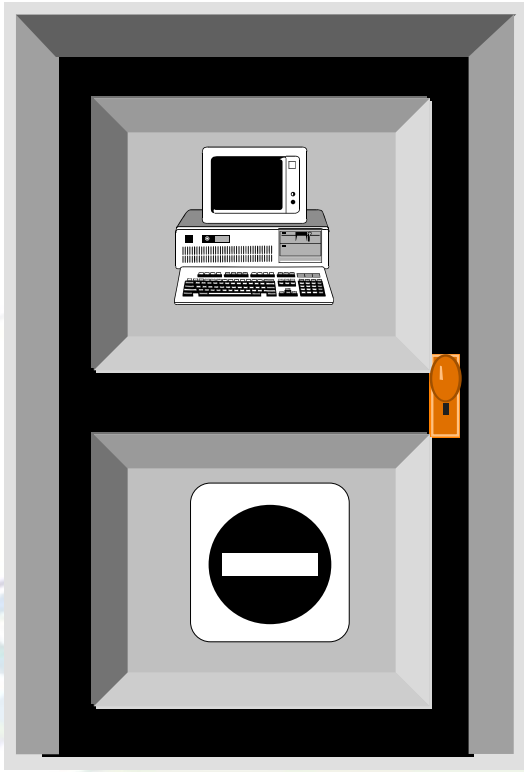
Wednesday, August 15, 2007
Session 1784

Agenda

- External Security
- CA Top Secret (TSS)
- CA ACF2 (ACF2)
- How to learn more
- Q & A

Data Security

- Protection of resources and data on a computer system from unauthorized
  - Destruction
  - Disclosure
  - Modification
- Protect by
  - System Entry Validation
  - Control Access
  - Audit Events



Native Security

- PASSWORD data set
- Security bits
- SYS1.UADS for TSO
  - Account Authority
  - Operator Authority
- DFHSNT for CICS
- Internal Application Security Tables
- etc. etc. etc.

Advantages of External Security

- One ID (LID, ACID) and Password
- Password rules
  - Expiry
  - Metrics
- Administration
- Granularity
- Based on Policy, not technical limitations

Data and Resource Controls

- Who can use what assets and how
- Assets include but are not limited to:
  - Files
  - Commands
  - Administrative functions
  - Facilities

Data and Resource Controls

- Controls include
  - Access level
  - Time, date, shift, source
  - Temporary access
  - Suspension on excessive access violations

Audit Concerns

- Individual accountability
- Separation of duties
- Violation logging
- Access logging
- Audit trail for sensitive data and resources
- Administrator accountability
- Regulatory Compliance
- “Capricious Malice” avoidance

Multilevel Security (MLS)

- Primary Goals:
  - Prevent unauthorized users from accessing data at a higher classification than their authorization
  - Prevent users from declassifying data
- MLS is an optional layer of security and works in conjunction with Discretionary Access control
- MLS can be controlled / limited to a set of resources and users
- MLS is controlled through the setting of security labels, security levels, and optional categories

Security Directories

- Security products store ID and access information in directories
- Often proprietary format
- Enterprise security directories may be designed using X.500 and/or LDAP
- Mainframe external security directories are accessible from X.500 using LDAP

Enterprise Identity Mapping (EIM)

- Single Enterprise-Wide identity for a user or resource
- Relates it to all its other representations within the organization
- Simple solution for managing multiple user registries, platforms and directories

CA Top Secret

Top Secret Security (TSS) Structure

- ACIDs (ACcessor ID's)
  - Any "node" in the hierarchical tree - Control ACIDs, Zones, Divisions, Departments, and users
- Users
  - Anything that can logon, whether front-line user, started task or Control ACID
  - Access to resources by ownership or permission

TSS Structure

- MSCA
  - “Master Security Control ACID”
  - Owns Everything (“Root”)
  - For Installation, Maintenance
  - Encryption Key
  - Console messages issued for logons and failed logons
  - Never use it unless you have to

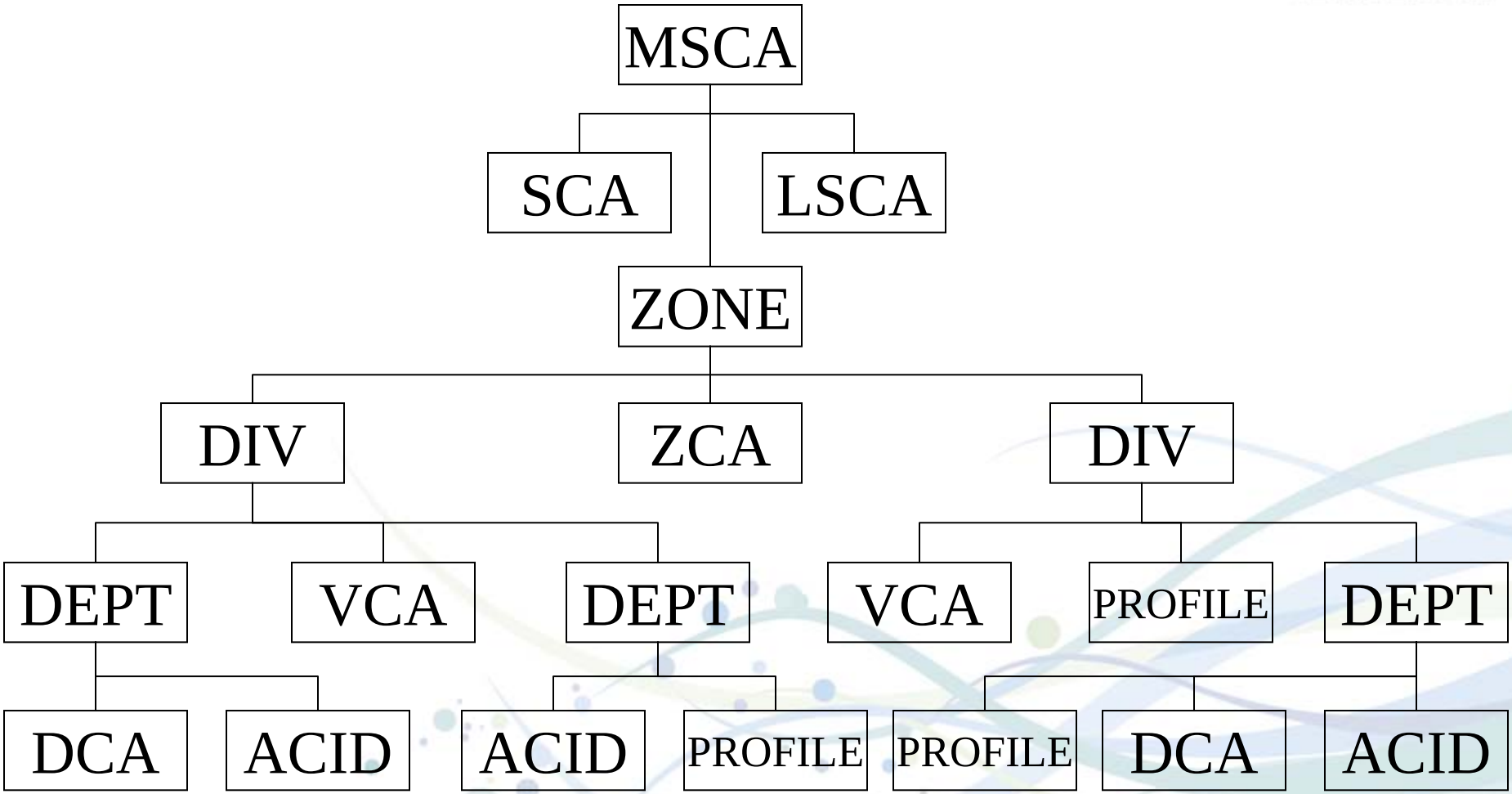
TSS Structure

- SCA's, LSCA's, ZCA's, VCA's, DCA's
  - SCA — Central Security Control ACID
  - LSCA — Limited Central Security Control ACID
  - ZCA — Zone Control ACID
  - VCA — Divisional Control ACID
  - DCA — Departmental Control ACID

TSS Structure

- Zones, Divisions, Departments
  - Hierarchy
  - Users can only belong to Departments (except for Control ACIDs)
  - Departments can only belong to Divisions or the MSCA
  - Divisions can only belong to Zones or the MSCA
  - Zones only belong to the MSCA

TSS Structure



TSS Structure

- PROFILEs
  - Have access to resources and facilities, just like users
  - A user can have many PROFILEs
  - Many users can have the same PROFILE
  - An excellent way to give many users the same access, with the same changes
  - Can be temporarily added
- GROUPs
  - Like profiles, but especially for use with UNIX System Services

TSS Structure - Permissions

- Resources
  - Datasets
  - Programs
  - Transactions
  - Other (see FDT, RDT)
  - Owned
  - Permitted to users, PROFILEs and GROUPs
  - May be temporarily permitted
  - Permission may be conditional on date, time, source, facility, SYSID and program path

TSS Structure - Permissions

- Data Set Access Levels
  - ALL
    - Data set can be accessed in any way.
  - UPDATE
    - Data set can be updated; READ and WRITE access is implied.
  - READ
    - Data sets can be read (opened for input); the default. READ implies FETCH.

TSS Structure - Permissions

- Data Set Access Levels (continued)
  - WRITE
    - Data can only be written into the data set (opened for output).
  - CREATE
    - Data set can be created.
  - FETCH
    - Programs from the data set (library) can only be executed, not read.

TSS Structure - Permissions

- Data Set Access Levels (continued)
  - SCRATCH
    - Data set can be scratched.
  - CONTROL
    - VSAM data set can be used for control interval update processing (for example, for an IDCAMS VERIFY function).
  - NONE
    - Data set can't be used in any way.

TSS Structure - Masks

- For “generic” permissions to Data Sets and RDT entries with “MASK” attribute
- “-” = “Floating Pattern” -- any number of any characters
- “*” = 0 to 8 of any characters (** = 0 to 16, *** = 0 to 24) except second
- “*.” = index masking
- “+” = fixed position substitution
- “%s#%” = partial ACID
- Mix and match any but “-”

TSS Structure - Attributes

- Facilities
  - Attributes, not resources
  - Not owned
  - May be added to ACIDs and PROFILEs
  - Examples include: CICSPROD, CICSTEST, TSO, BATCH, STC

TSS Structure

- Started Task ACIDS
  - STC Table
  - Master Facility
  - Mode
  - Resource access
  - Example: CICSPROD

TSS Structure - Other Records

- RDT (Resource Descriptor Table)
  - Stores both predefined and user-defined resources
- FDT (Field Descriptor Table)
  - Stores both predefined and user-defined fields.
- SDT (Static Data Table)
  - Stores internal, non-volatile data used to protect records, fields, screens, calendars, and other resources.

TSS Structure - Other Records

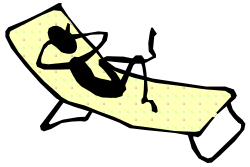
- NDT (Node Descriptor Table)
  - Contains data for assigning Pass Tickets and Session Keys to applications. It also contains VAX-related data.
- ALL Record
  - Identifies resources that are globally accessible to all users.
- STC (Started Task Command)
  - Defines a started task command to CA Top Secret.

TSS Configuration - Data Sets

- Security Database (encrypted)
- Audit/Tracking file
- Recovery File
- CPF Recovery File
- Backup Database

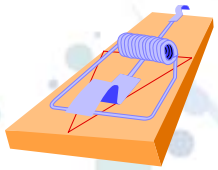
TSS Security Modes

- Dormant Mode
  - *Make sure the product is functional*



- Warn Mode
  - *Look for violations, patterns*
- Implement Mode
  - *Only what's explicitly secured*

- Fail Mode
  - *Mousetrap security*



CA ACF2

CA ACF2 Control Database

- Three VSAM key-sequenced data sets
  - Logonid
  - Access rules
  - Infostorage
- Shared-DASD support
- All changes and violations journaled to SMF
- Automatic daily backup
- Recovery utility provided

Logonid Database

- One record per logonid
- Central source for most user data*
- LOGONIDs known as “LIDs”

*Other user data on Infostorage Profile records

About the UID

- Allows for grouping of users
- Constructed of Logonid record fields, such as department, location, and job function
- Often contains user-defined fields
- Format is defined in the ACFFDR-@UID macro
- Maximum 24 characters in length
- Allows grouping in access rules
- Multi-valued Logonid fields-allows multiple views of a single UID.

Design Considerations
How do we share resources?

- Organizational structures
- Naming conventions
- Access controls
- Policies to be enforced
- Administration of users
- Use all of the above considerations in designing and implementing the UID string

@UID Macro Example

For True Lock:

@UID LOC,DIV,DEPT,JOBF,LID

LOC	=	1st and 2nd characters in string
DIV	=	3rd character
DEPT	=	4th and 5th characters
JOBF	=	6th through 8th characters
LID	=	9th through 16th characters

@UID Macro Example

@UID LOC,DIV,DEPT,JOBF,LID

CH	F	OP	SCH	TLC492
LOC		=		Chicago
DIV		=		Finance & Data Processing
DEPT		=		Operations
JOBF		=		Scheduler
LID		=		TLC492

How are UID Strings Used?

- Define groups of users to CA ACF2
- To validate access to data and resources
  - DATASET1 UID(CHFOPSCHTLC492) READ(A)
  - DATASET2 UID(CHFOPSCH) READ(A)
  - DATASET3 UID(CHFOP) READ(A)
  - DATASET4 UID(CH) READ(A)

How are UID Strings

- As a key component in rule writing
- Determine data and resource sharing conditions
- Can be masked in rule writing
  - DATASET5 UID(***OP) READ(A)

What Are Access Rules?

- Sets of rules allowing for controlled sharing of data set resources

Why Are Access Rules Needed?

- By default, CA ACF2 does not allow access to data unless rules authorize it
- As a reference for auditors to see who has access to what and under what conditions

Access Rule Sets

- One rule set exists for each DSN high-level index
- Rule sets can exist for entire volumes of data in DASD or tape
- Key (up to 8 characters) to record on database is DSN high-level index for data set rule sets
- Rule sets are compiled and stored much like programs

Access Rule Types

- READ
- WRITE
- ALLOCATE
  - DELETE
  - CREATE
  - RENAME
- EXECUTE
- READ implies EXECUTE
- EXECUTE can be given without READ

Access Permissions

- Allow - No audit
- Log - Allow with auditing
- Prevent - Prevent with audit

Sample Rule Set

```
$KEY(SYS1)
BRODCAST    UID(CHFSPSYS) R(A) W(A) A(L) E(A)
BRODCAST    UID(*) R(A) W(A)
PARMLIB     UID(CHFSPSYS) R(A) W(A) A(L) E(A)
PARMLIB     UID(*)
PROCLIB     UID(CHFSPSYS) R(A) W(A) A(L) E(A)
```

Sample Data Set Masks

$KEY(PAYROLL)

DSN Mask	Matches	Does not Match
TEST.DATA	PAYROLL.TEST.DATA	Anything else
ABC*.LOAD	PAYROLL.ABCC.LOAD	PAYROLL.ABC.LOAD
	PAYROLL.ABC1.LOAD	PAYROLL.AB.LOAD
	PAYROLL.ABC2.LOAD	PAYROLL.ABCDE.LOAD
*BC.LOAD	PAYROLL.ABC.LOAD	PAYROLL.AB.LOAD
	PAYROLL.XBC.LOAD	PAYROLL.AABC.LOAD

Sample Data Set Masks

$KEY(PAYROLL)

DSN Mask	Matches	Does not Match
ABC-.LOAD	PAYROLL.ABC.LOAD	PAYROLL.AB.LOAD
	PAYROLL.ABC1.LOAD	PAYROLL.AB.DEF.LOAD
	PAYROLL.ABC123.LOAD	
	PAYROLL.ABCDE.LOAD	
-.LOAD	PAYROLL.LOAD	PAYROLL.LOAD.DATA
	PAYROLL.ABC.LOAD	
	PAYROLL.ABC123.LOAD	
	PAYROLL.A.B.C.LOAD	

Infostorage Database

- Multiple record types available
- Dynamic update facility
- Security administrator maintains

Infostorage Database

Infostorage Record Classes

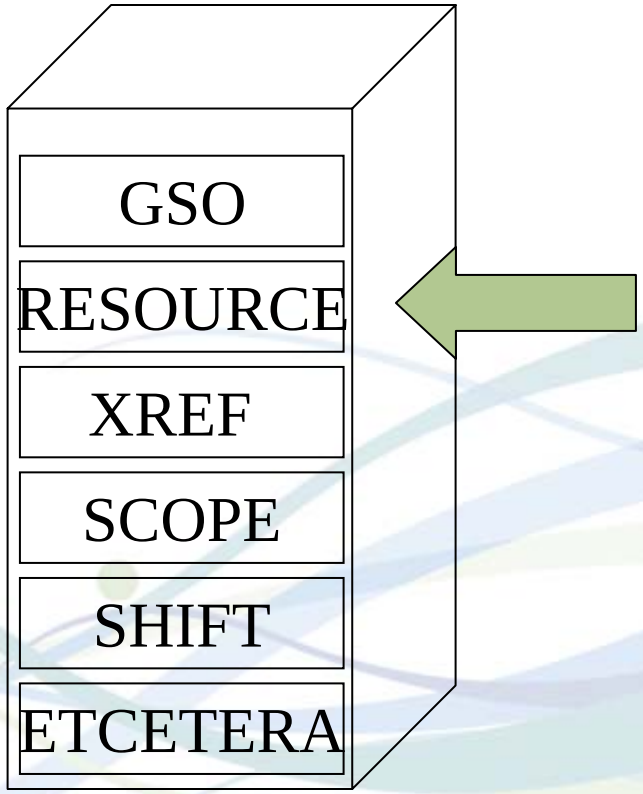
- GSO
  - Global options used to initialize CA ACF2
- Resource Rulesets
  - Control the use of logical system resources
- XREF
  - Allows for grouping of sources or resource rules
  - Treats groups as single entities

Infostorage Record Classes

- Scope
  - Limit authority of privileged users to particular CA ACF2 records
- Shift
  - Identify particular periods of time and dates

Resource Records

- TSO account numbers
- TSO logon procedures
- CICS resources
- IMS resources
- CA IDMS resources
- Other defined resources



Resource Rule

- Resource Validation Process
  - User identification
  - Resource check
  - Similar to data set rule

Resource Access

- Access permissions
  - Allow
  - Log
  - Prevent
- Service levels
  - Execute
  - Read
  - Update
  - Delete
  - Add

CA ACF2 Security Modes

- QUIET
  - System entry validation
- LOG
  - System entry validation
  - Access rule validation and logging
  - Access to data NOT prevented
- WARN
  - Same as LOG mode
  - Warn message issued to user

CA ACF2 Security Modes

- ABORT
  - Unauthorized access prevented
  - Violation message issued
- RULE
  - System entry validation
  - Access rule validation
  - Selectable mode for each rule set

Want to Know More?

- http://support.ca.com/
- http://www.ca.com/education/

Course Number	Title
AC200	CA CA ACF2® Security: Basic Administration
AC210	CA ACF2® Security: Intermediate Administration
AC220	CA ACF2® Security: Advanced Administration
AC230	CA ACF2® Security: Advanced Technical
AC240	CA ACF2® Security: for CICS Interface
AC250	CA ACF2® Security Option for DB2: Administration

Course Number	Title
TS001	CA Top Secret Security: Basics
TS002	CA Top Secret Security: Intermediate Administration
TS003	CA Top Secret Security: Advanced Administration
TS010	CA Top Secret Security: Advanced Technical
TS025	CA Top Secret Security: Advanced Technical
TS120	CA Top Secret Security Option for DB2: Administration

Q & A