Surveillance of Privileged Users

Finn T Christensen
Cryptographic Competence Centre Coper
IBM Denmark
ccftc@dk.ibm.com

A Banking Security Principle

Banks do not accept that a single employee can commit fraud against the bank.

Banks accept that a conspiracy among employees do enable them to commit fraud.

This is a well proven concept, which is much older than computers.

Privileged Users

But some computer administration users do typically have the ability to commit fraud as individuals.

Salary administration inventing artificial employees, and even paying income tax for these, is a famous example.

Security administration have the ability to allow themselves to update databases.

Storage administrators are also effectively able to update any dataset.

DB2 SYSADM or SYSCTRL users have similar privileges in DB2.

Privileged users at Danske Bank

- Users with system SPECIAL somewhere
- Users with SYSADM, SYSCTRL or SYSOPR in DB2
- Users that are members of specific group
- Users with UID(0) in OMVS
- (OPERATIONS users already handled)

"Division of responsibility" means that no human have several of the attributes above (emergency userids may have both SPECIAL and OPERATIONS).

RACF Database and SMF Unload output loaded to DB2 5 nights a week.

Daily Actions

For every threat, one or more exception QMF reports are run daily. Exceptions are sent by email (Lotus Notes) to internal auditors and head of security administration).

Standard users violating rules (e.g. too high UACC on some personal datasets) are sent email with information on company standards and helpdesk access information. QMF report is attached as a file.

All QMF reports can optionally run with any date/time or SMF-id or userid selection/exception criteria and these extra filters then get printed in page headings.

Perceived RACF Threats

- SPECIAL permits own user/group directly
- SPECIAL permits own user/group via FROM
- SPECIAL connects own user to new group
- SPECIAL creates new profile, and does not remove own userid (and ADDCREATOR enabled)
- SPECIAL creates shortlived userid, and permits it
- SPECIAL misuse an emergency userid (e.g. via SURROGAT or password reset)
- SPECIAL creates another SPECIAL user
- SPECIAL make somebody UID(0) or permits to FACILITY BPX.SUPERUSER

Perceived RACF Threats *(continued)*

- SPECIAL connects with GROUP OPERATIONS
- SPECIAL alters UACC(NONE) or sets WARNING on resource profile
- SPECIAL permits ID(*) with access above NONE
- SPECIAL modifies GLOBAL class member lists and thus effectively permits also own user
- SETROPTS modifications (e.g. set class to NOCLASSACT) - checked daily and at IPL - incl. CDT changes
- RVARY used to activate/inactivate RACF
- SPECIAL sets pswd for other userid, and misuses it
- Loss or suppression of SMF data

Perceived RACF Threats *(continued)*

- User has over frequent use of PASSWORD cmd to change own password (circumventing SETROPTS PW(HISTORY(..)))
- CONNECTs to group defining additional privileged users
- Modifications to sensitive access lists or groups
- z/OS changes in general (changes in local classes of CDT, SETROPTS changes, checksums for security related exits logged daily and at IPL)
- Non privileged user sets high UACC, ID(*) access or WARNING

Perceived RACF Threats *(continued)*

- RACF command summaries for users connected to specific group
- Changes to "locked" profiles (mail detailing changes sent to "lock owner" who must be member of specific group)
- RACLINK used to cause password changes for SPECIAL users (RACLINK, ADDUSER, ALTUSER)
- Mixing SPECIALs and UID(0) or BPX.SUPERUSER
- User has over-frequent password changes (daily, weekly or monthly threshold passed) - check required by law

Sample SPECIAL Permit report

```
               PERMIT TO USER/GROUP ENCOMPASSING SPECIAL USERS
                       1998-03-01 < DATE <= 1999-01-15


-----------------------------------------------------------------------
DATE:1999-01-06         TIME:11.49.13         SYSTEM:MVSG
ADMINISTRATOR:CCFBK     RESULT:SUCCESS
COMMAND:PERMIT AD                                                    +
           CLASS(IBMOPC) ID(CCFBK) ACCESS(READ)
```

Sample SMF Suppression Report

```
                   INAPPROPRIATE SUPPRESSION OF SMF RECORDS
                       2000-01-01 < DATE <= 2002-02-25
 MINIMUM MASK FOR SMF RECORD TYPES 000:127 : FFFF1FFFFFFFFFFE83FFFFFFEFFFFFFF
 MINIMUM MASK FOR SMF RECORD TYPES 128:255 : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
            AREA=SYS IS DEFAULT WHEN NO SPECIFIC SUBSYSTEM RECORD
          SUBTYPE INDEX: 005=SET 009=IPL 013=SETSMF 015=SMF RESTART


                    SYS-
                    TEM  SUB       SMF TYPE 000:127
DATE       TIME      ID  TYPE AREA SMF TYPE 128:255
-----------------------------------------------------------------------
2002-02-05 22.45.36 ACPU 009  STC  F3FFF7FF CF7FFFFE E3FFFFF7 EFFFFFFF
                                   FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
2002-02-05 22.45.36 ACPU 009  JES2 F3FFF7FF CF7FFFFE E3FFFFF7 EFFFFFFF
                                   FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
2002-02-05 22.45.36 ACPU 009  HSC  00000000 00000000 00000000 00000000
                                   00000000 00000000 00000000 00000001
2002-02-05 22.45.36 ACPU 009  SYS  F3FFF7FF CF7FFFFE E3FFFFF7 EFFFFFFF
                                   FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF

                     LAST PAGE OF REPORT : TRU16B
```

Sample CDT report header

```
                    CLASSES WITH MULTIPLE POSIT NUMBERS
                      2001-12-09 < DATE <= 2001-12-10

                    -----------------------------------


         SMF   NEW     NEW               OLD     OLD
CLASS    ID   POSIT TIMESTAMP           POSIT TIMESTAMP
-------- ---- ----- ------------------- ----- -------------------
```

Sample Exit Modification Report

```
                       EXIT MODULES WITH CHANGED MDC
                       2001-12-09 < DATE <= 2001-12-10

            "OTHER" MEANS LATEST OCCURRENCE OUTSIDE AUDIT INTERVAL
            ======================================================


-------------------------------------------------------------------
SYSTEM: MVSF    AUDIT ICHDEX01 E66D01710D4545C4  2001-12-10-11.53.41
EXIT: ICHDEX01  OTHER ICHDEX01 7EB958268706530F  2001-12-09-17.56.24
-------------------------------------------------------------------
SYSTEM: MVSF    AUDIT ICHPWX01 B11021F64929424A  2001-12-10-11.53.41
EXIT: ICHPWX01  OTHER ICHPWX01 C99B38E59BDAF04D  2001-12-09-17.56.24
-------------------------------------------------------------------
SYSTEM: MVSF    AUDIT ICHRCX02 7D836FC8233951D5  2001-12-10-11.53.41
EXIT: ICHRCX02  OTHER ICHRCX02 B64A8AE4189921DB  2001-12-09-17.56.24
-------------------------------------------------------------------
SYSTEM: MVSF    AUDIT ICHRDX02 91710520024F307E  2001-12-10-11.53.41
EXIT: ICHRDX02  OTHER ICHRDX02 6EB361E4ECF4C369  2001-12-09-17.56.24
-------------------------------------------------------------------
SYSTEM: MVSF    AUDIT ICHRFX02 7519588529D1D6A1  2001-12-10-11.53.41
EXIT: ICHRFX02  OTHER ICHRFX02 EC7C7F3D7A97552A  2001-12-09-17.56.24
-------------------------------------------------------------------
SYSTEM: MVSF    AUDIT ICHRFX04 33D2A57E2B21D9B5  2001-12-10-11.53.41
EXIT: ICHRFX04  OTHER ICHRFX04 457B7612B2FFBA50  2001-12-09-17.56.24
-------------------------------------------------------------------
```

DB2 threats

For every DB2 threat (list not shown here) similar reports are run.

DB2 Performance Monitor enables us to load all GRANT and REVOKE statements into a DB2 table. This is included as basis for the DB2 threats.

Future

Real time control have been investigated - and rejecte

As no of LPARs checked grows, tolerance of late SMF records from individual systems must be added.

The exit checksum generation process should suppor z/OS Dynamic Exits facility.