IBM Software Group

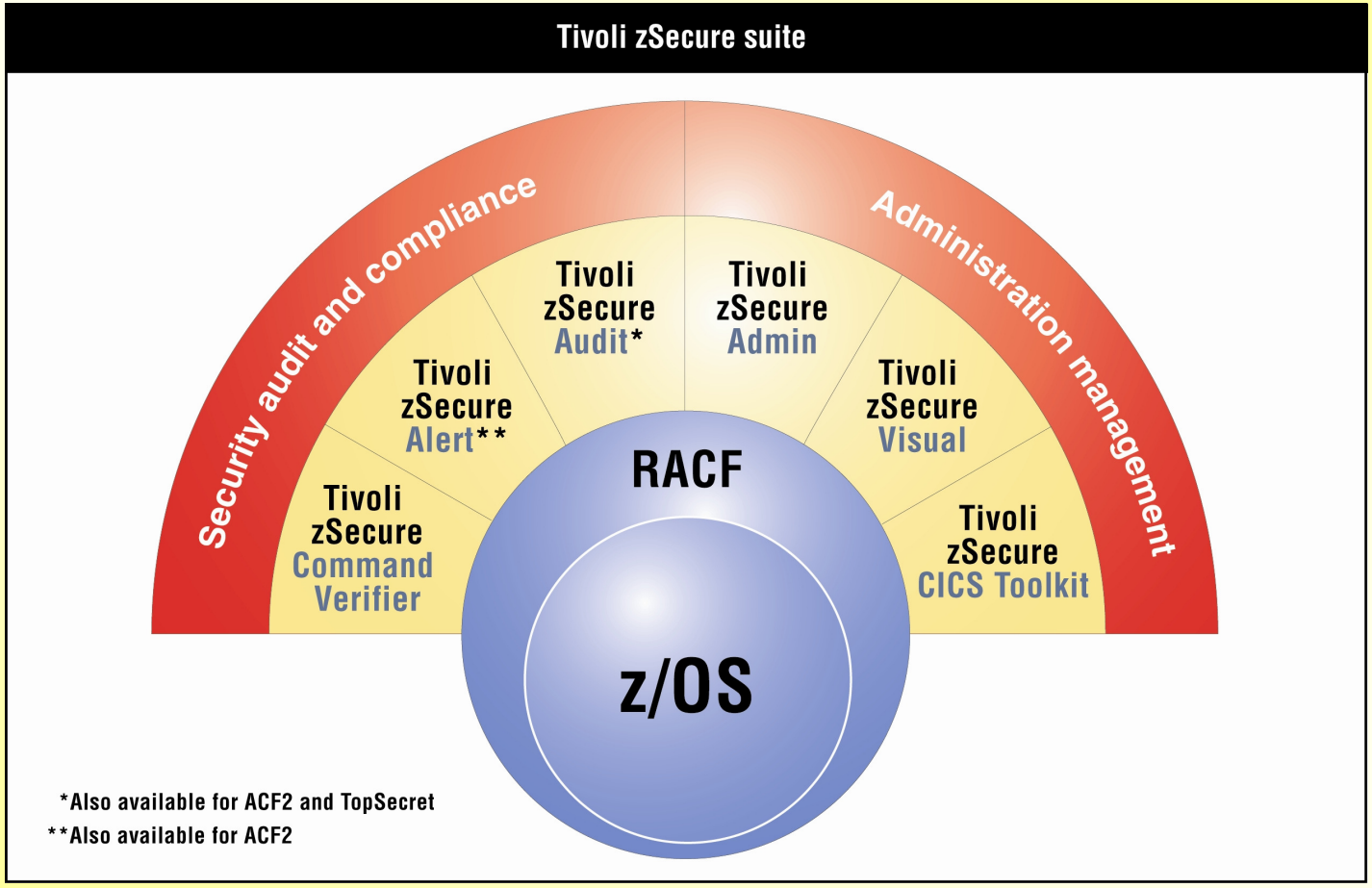
The System z security hub: RACF administration

Rob van Hoboken
zSecure Architect
Rob.vanHoboken@nl.ibm.com

@business on demand.

Introducing the IBM Tivoli zSecure Suite

Making z/OS security management more effective



Security administration is not easy

- Situation:
  - Technical users perform administration
  - User administration by non-technical users
  - Technical aspects of security by technical teams
- Best Solution Available?:
  - Use RACF commands via ISPF
    - Output is not easy to interpret
  - Use unloaded RACF database in DB2
    - Information not up to date

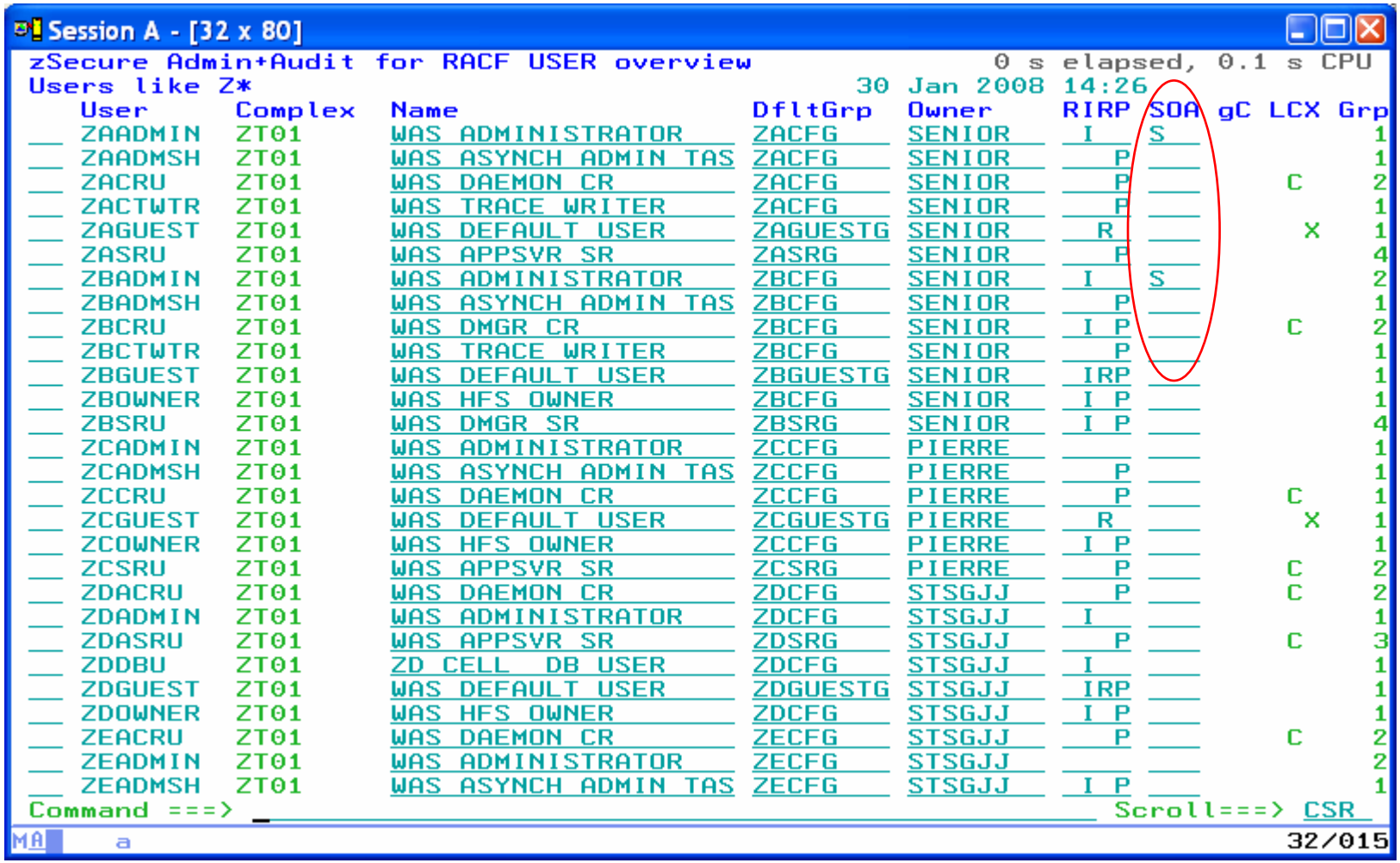
zSecure Solution

- Easy RACF administration – zSecure Admin
  - Overview of profiles, show context of security
  - Overtype fields to make corrections
  - Reports showing differences and effective security
- Actual information from active RACF database

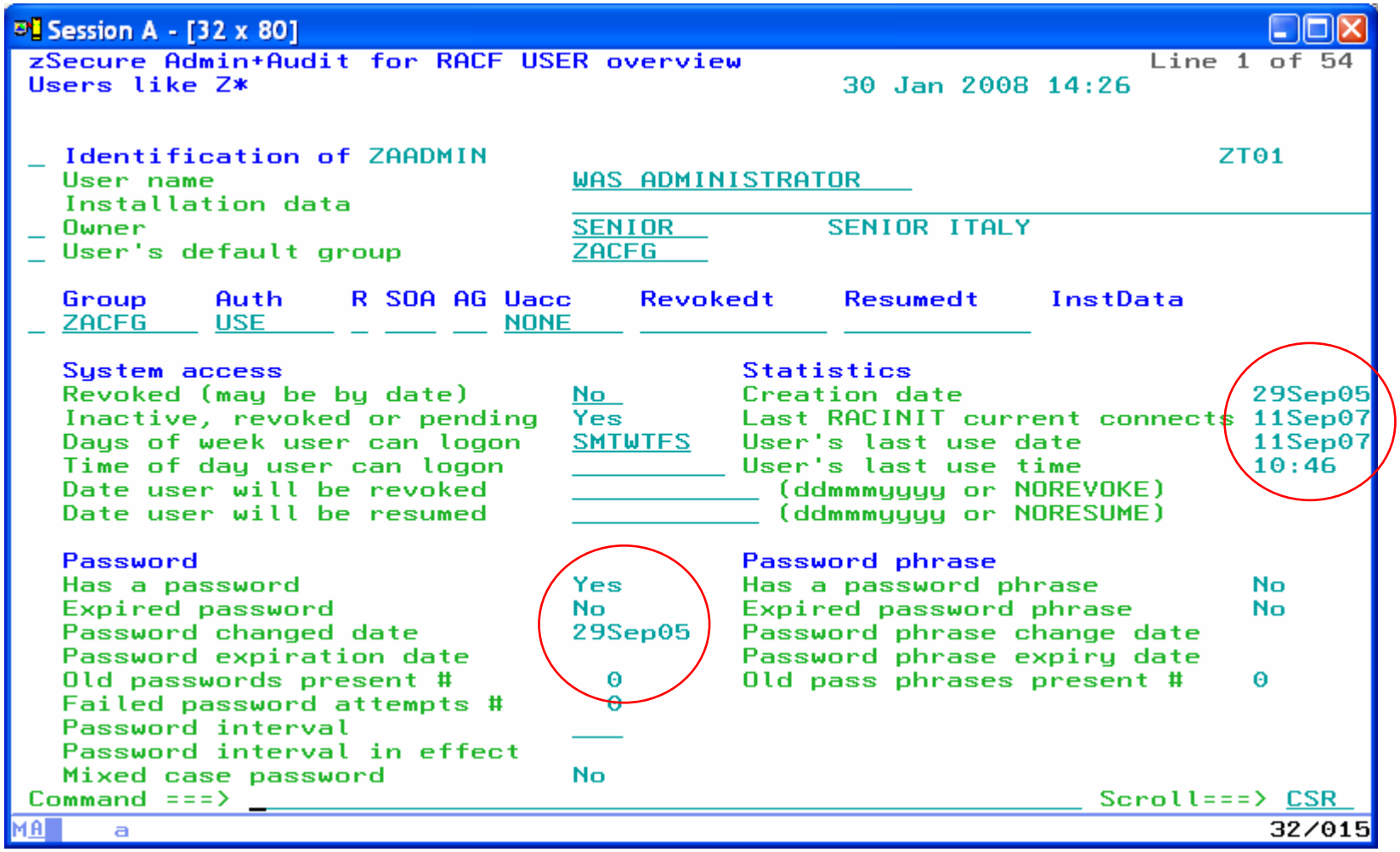
RACF LISTUSER (LU) command output

```
 COMMAND OUTPUT BROWSE ------------------------------------------------------
 COMMAND ===> _
********************************************************** Top of Data *****
listuser ZPU001
USER=ZPU001  NAME=BANKING USER 1         OWNER=ZPDEPT31  CREATED=07.095
 DEFAULT-GROUP=ZPDEPT31 PASSDATE=00.000 PASS-INTERVAL=120 PHRASEDATE=N/A
 ATTRIBUTES=NONE
 REVOKE DATE=NONE   RESUME DATE=NONE
 LAST-ACCESS=UNKNOWN
 CLASS AUTHORIZATIONS=NONE
 NO-INSTALLATION-DATA
 NO-MODEL-NAME
 LOGON ALLOWED   (DAYS)          (TIME)
 ----------------------------------------
 ANYDAY                          ANYTIME
  GROUP=ZPDEPT31   AUTH=USE      CONNECT-OWNER=ZPDEPT31  CONNECT-DATE=07.095
    CONNECTS=    00  UACC=NONE     LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=NONE
    REVOKE DATE=NONE   RESUME DATE=NONE
  GROUP=ZPACC02    AUTH=USE      CONNECT-OWNER=SYS1      CONNECT-DATE=07.095
    CONNECTS=    00  UACC=NONE     LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=NONE
    REVOKE DATE=NONE   RESUME DATE=NONE
SECURITY-LEVEL=NONE SPECIFIED
CATEGORY-AUTHORIZATION
 NONE SPECIFIED
SECURITY-LABEL=NONE SPECIFIED
******************************************************* Bottom of Data ***
```

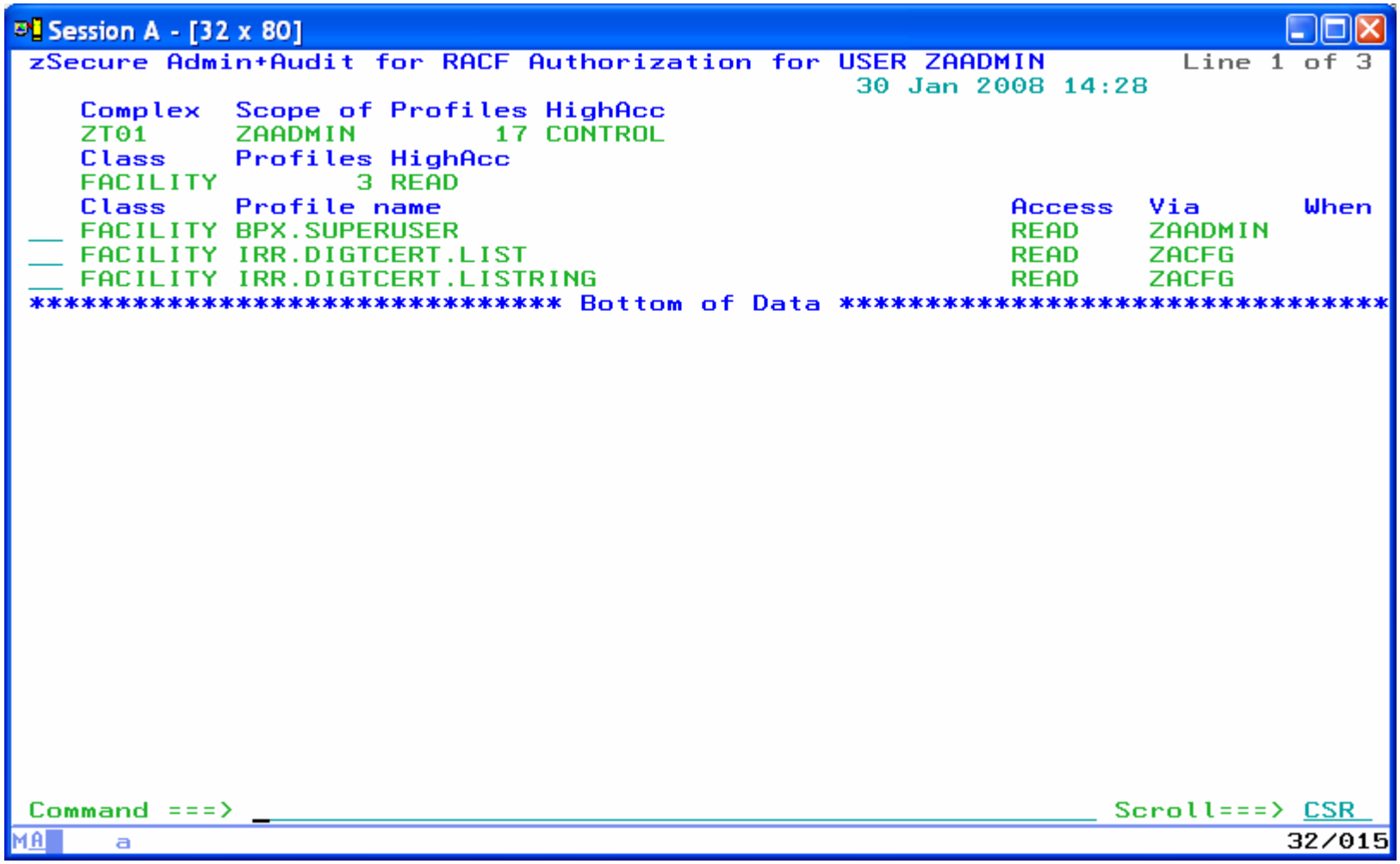
zSecure Admin: Overview of user profiles



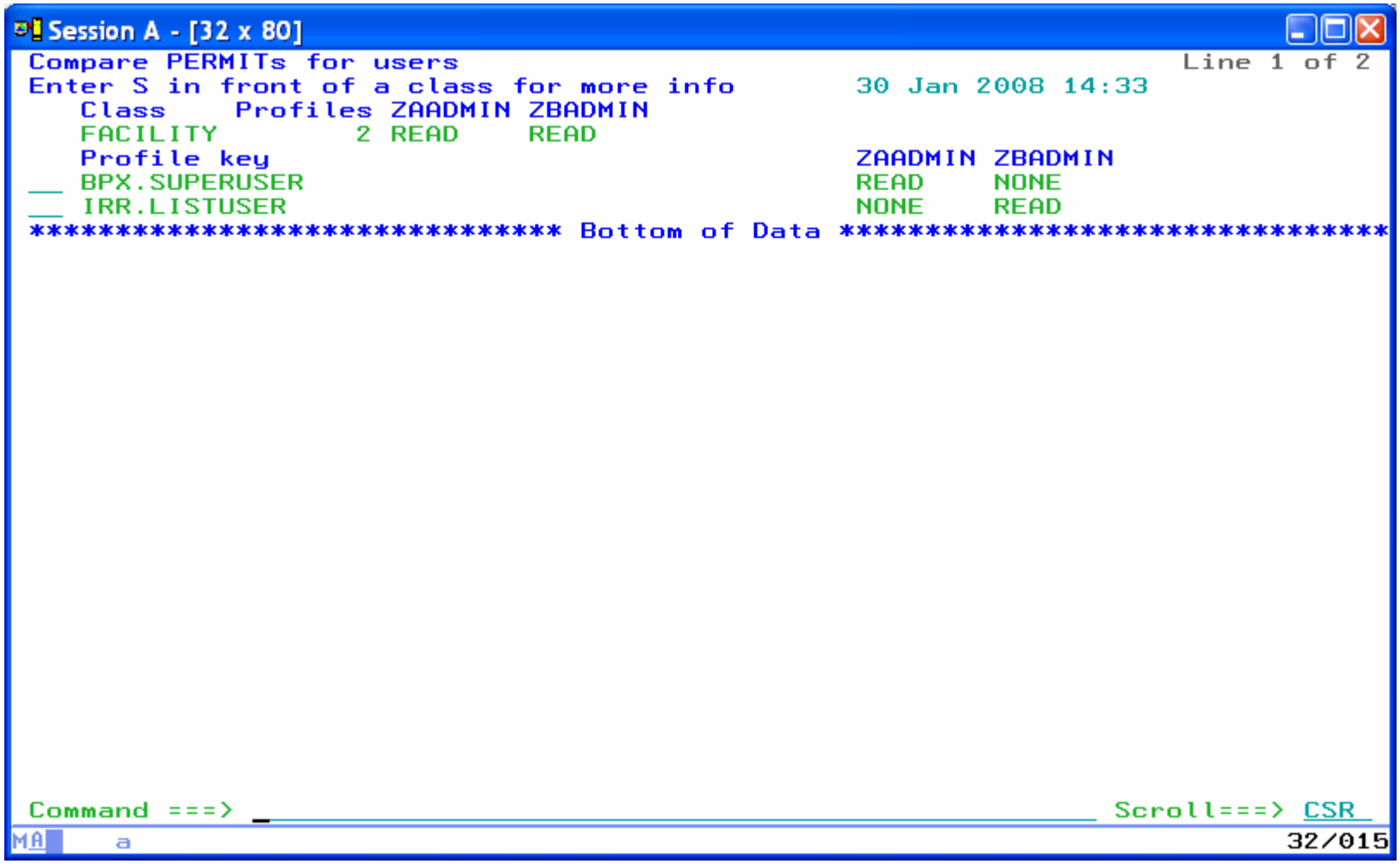
Details of a user profile



Access granted to the user via Permit and Connect



Compare access between users



Make changes by typing over the data

Session A - [32 x 80]

```
zSecure Admin+Audit for RACF USER overview                      Line 1 of 44
Users like Z*                                  30 Jan 2008 14:35
   User      Complex  Name                     DfltGrp   Owner     RIRP SOA gC LCX Grp
__ ZAADMIN   ZT01     WAS ADMINISTRATOR        ZACFG     SENIOR    rI   S              1
__ ZAADMSH   ZT01     WAS ASYNCH ADMIN TAS     ZACFG     SENIOR     P                 1
__ ZACRU     ZT01     WAS DAEMON CR            ZACFG     SENIOR     P          C      2
__ ZACTWTR   ZT01     WAS TRACE WRITER         ZACFG     SENIOR     P                 1
__ ZAGUEST   ZT01     WAS DEFAULT USER         ZAGUESTG  SENIOR      R            X    1
__ ZASRU     ZT01     WAS APPSVR SR            ZASRG     SENIOR     P                 4
__ ZBADMIN   ZT01     WAS ADMINISTRATOR        ZBCFG     SENIOR    rI   S              2
__ ZBADMSH   ZT01     WAS ASYNCH ADMIN TAS     ZBCFG     SENIOR     P                 1
__ ZBCRU     ZT01     WAS DMGR CR              ZBCFG     SENIOR     I P        C      2
__ ZBCTWTR   ZT01     WAS TRACE WRITER         ZBCFG     SENIOR     P                 1
__ ZBGUEST   ZT01     WAS DEFAULT USER         ZBGUESTG  SENIOR     IRP               1
__ ZBOWNER   ZT01     WAS HFS OWNER            ZBCFG     SENIOR     I P               1
__ ZBSRU     ZT01     WAS DMGR SR              ZBSRG     SENIOR     I P               4
__ ZCADMIN   ZT01     WAS ADMINISTRATOR        ZCCFG     PIERRE                       1
__ ZCADMSH   ZT01     WAS ASYNCH ADMIN TAS     ZCCFG     PIERRE     P                 1
__ ZCCRU     ZT01     WAS DAEMON CR            ZCCFG     PIERRE     P          C      1
__ ZCGUEST   ZT01     WAS DEFAULT USER         ZCGUESTG  PIERRE      R            X    1
__ ZCOWNER   ZT01     WAS HFS OWNER            ZCCFG     PIERRE     I P               1
__ ZCSRU     ZT01     WAS APPSVR SR            ZCSRG     PIERRE     P          C      2
__ ZDACRU    ZT01     WAS DAEMON CR            ZDCFG     STSGJJ     P          C      2
__ ZDADMIN   ZT01     WAS ADMINISTRATOR        ZDCFG     STSGJJ     I                 1
__ ZDASRU    ZT01     WAS APPSVR SR            ZDSRG     STSGJJ     P          C      3
__ ZDDBU     ZT01     ZD CELL  DB USER         ZDCFG     STSGJJ     I                 1
__ ZDGUEST   ZT01     WAS DEFAULT USER         ZDGUESTG  STSGJJ     IRP               1
__ ZDOWNER   ZT01     WAS HFS OWNER            ZDCFG     STSGJJ     I P               1
__ ZEACRU    ZT01     WAS DAEMON CR            ZECFG     STSGJJ     P          C      2
__ ZEADMIN   ZT01     WAS ADMINISTRATOR        ZECFG     STSGJJ                       2
__ ZEADMSH   ZT01     WAS ASYNCH ADMIN TAS     ZECFG     STSGJJ     I P               1
Command ===>                                                  Scroll===> CSR
MA    a                                                                  10/063
```

Security administrators make mistakes

- Situation:
  - Security management outsourced
  - User administration delegated to non-technical users
  - Departments with their own applications, responsibility and security administrators
- Best Solution Available?:
  - Solution (?): implement GROUP SPECIAL, GROUP AUDITOR
    - Impractical when profile ownership is not clearly specified in RACF

zSecure Solution

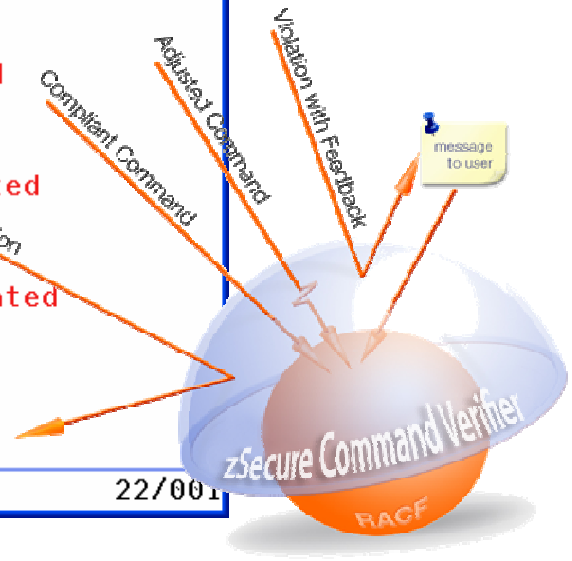
- RACF command screening – zSecure Command Verifier
  - Each security change verified against granular policy
    - Using masks for classes and profiles
  - Inappropriate commands prevented
  - Missing or incorrect parameters can be fixed
  - Even controls command by system special users

zSecure Command Verifier

Prevent commands that would cripple your security

```
Session A - [24 x 80]
setr password(nohistory)
 C4R751E SETROPTS PASSWORD.HISTORY not allowed, command terminated
 READY
setr password(interval(180))
 C4R751E SETROPTS PASSWORD.INTERVAL not allowed, command terminated
 READY
permit irr.password.reset class(facility) id(ibmuser) access(update)
 C4R607E ACL setting for self to UPDATE not allowed, command terminated
 READY
ralter facility irr.password.reset uacc(update)
 C4R600E UACC UPDATE setting not allowed, command terminated
 READY
setropts noclassact(facility)
 C4R754E CLASSACT not allowed for class FACILITY, command terminated
 READY
permit 'sys1.parmlib' gen id(ibmuser) access(update)
 C4R646E Management of locked profiles not allowed, command terminated
 READY
connect ibmuser group(sys1)
 C4R548E You may not connect yourself to group SYS1, command terminated
 READY

MA    a                                                    22/001
```



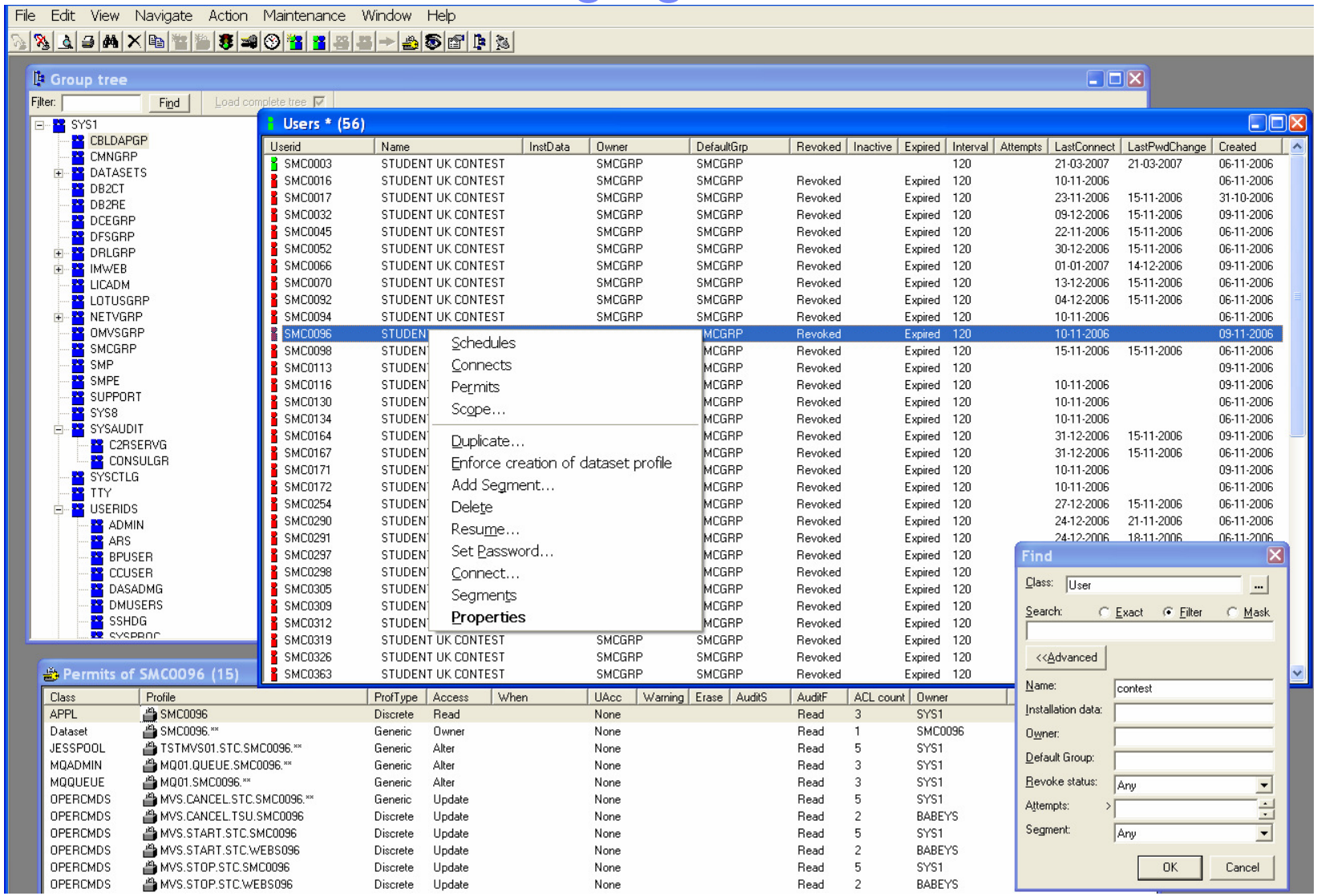
Decentralized security administration

- Situation:
  - Password administration by helpdesk
  - User administration delegated to non-technical users
  - Departments with their own applications, responsibility and security administrators
- Best Solution Available?:
  - Write ISPF/Rexx front-end
  - Front-end using unloaded RACF info on Windows/Unix
  - Implement identity management solution

zSecure Solution

- Graphical user interface: zSecure Visual
  - Windows GUI for RACF management
  - Work with active RACF information
  - Supports scoping for decentralized administration

zSecure Visual – leveraging a GUI for RACF



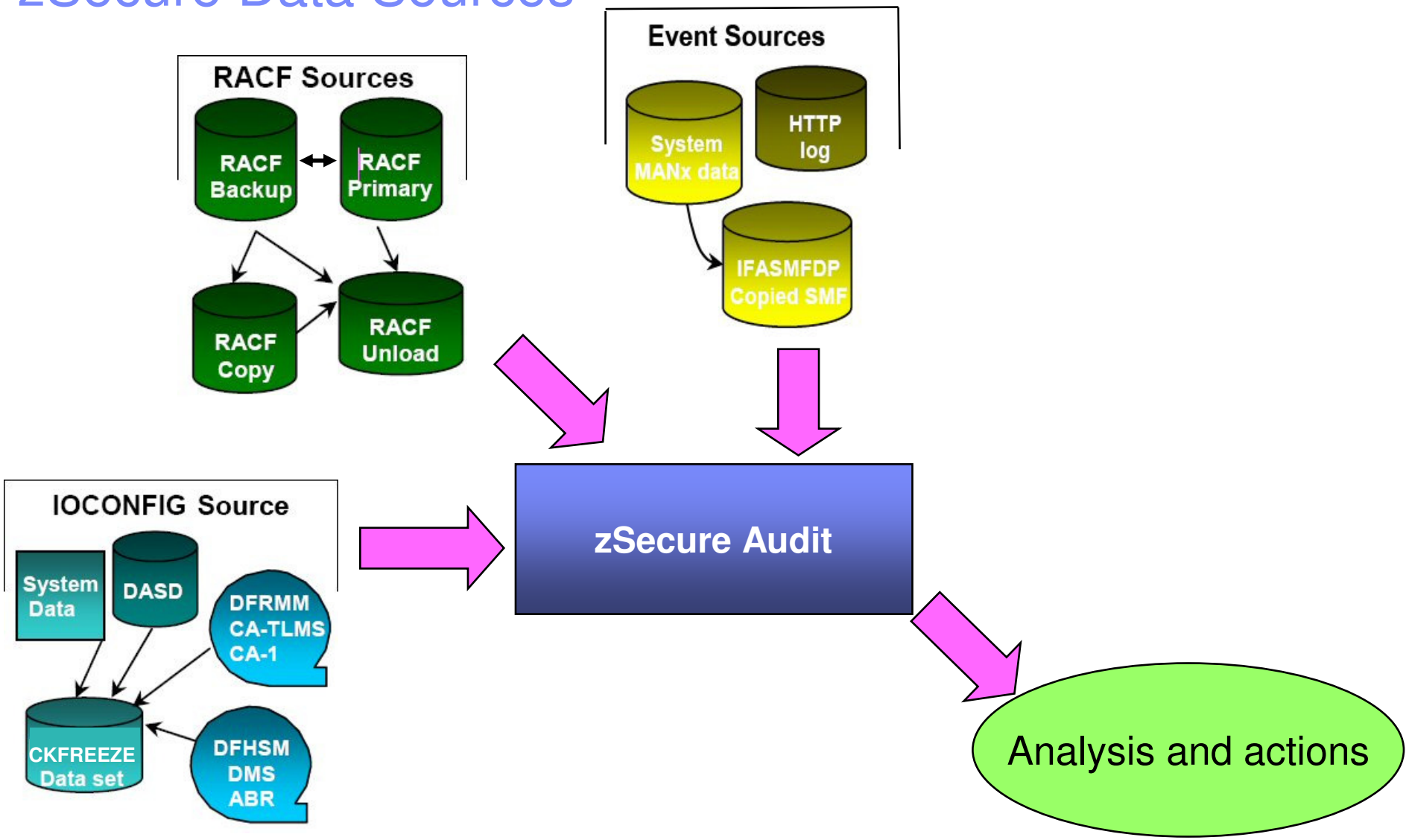
Find mis-configuration and vulnerabilities

- Situation:
  - z/OS and RACF protect each other
    - System datasets must be protected…
  - Verifying the protection is time consuming
- Best Solution Available?:
  - Individual reports for RACF, PARMLIB, UNIX....
    - Manual correlation and verification?
  - Annual external audit

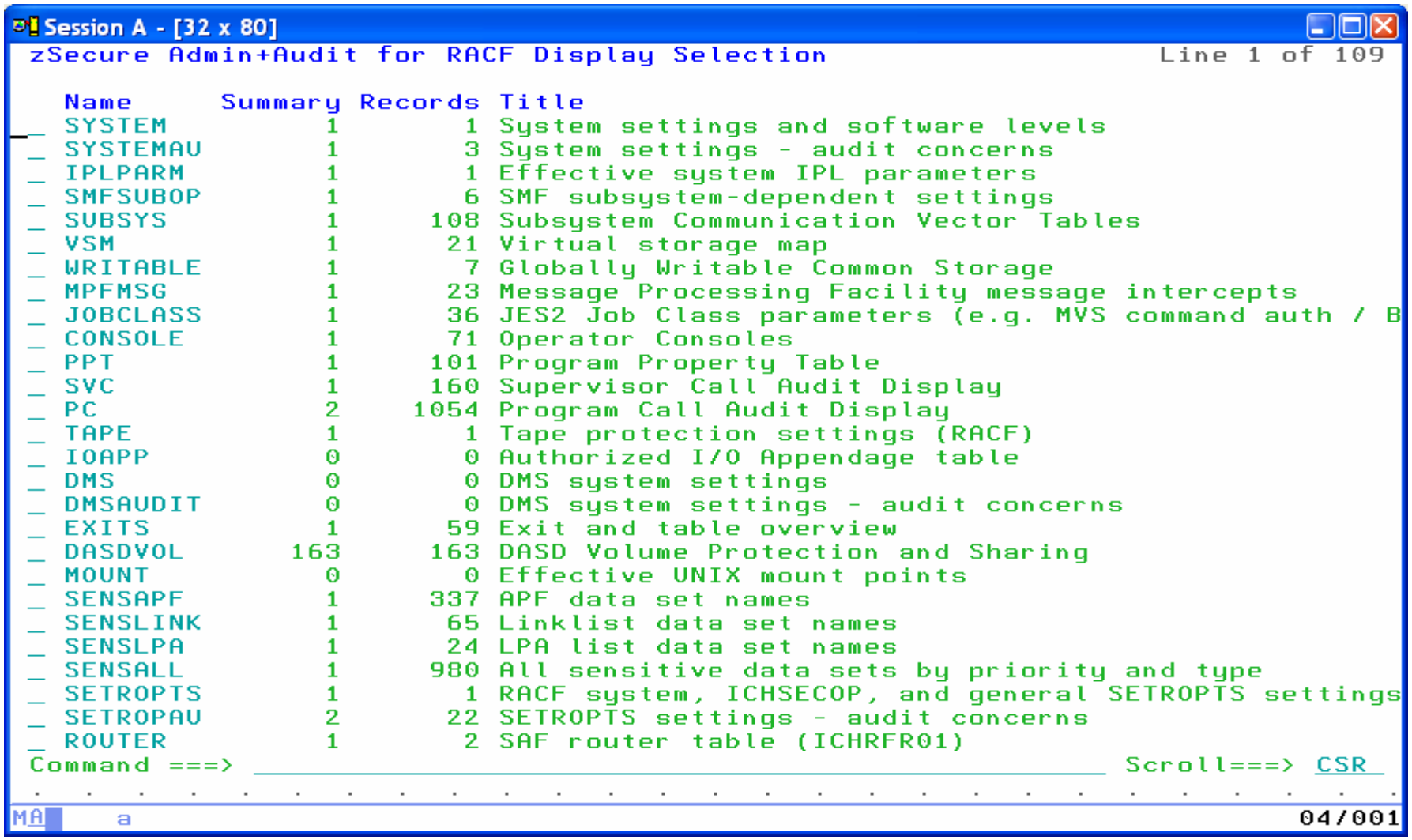
zSecure Solution

- zSecure Audit takes information from RACF, z/OS, UNIX
  - Identifies inconsistencies and vulnerabilities
  - Shows the privileged users that can chance z/OS, RACF
    - Or bypass security
  - Adhoc reports via ISPF
  - Automatic reporting and monitoring in batch jobs

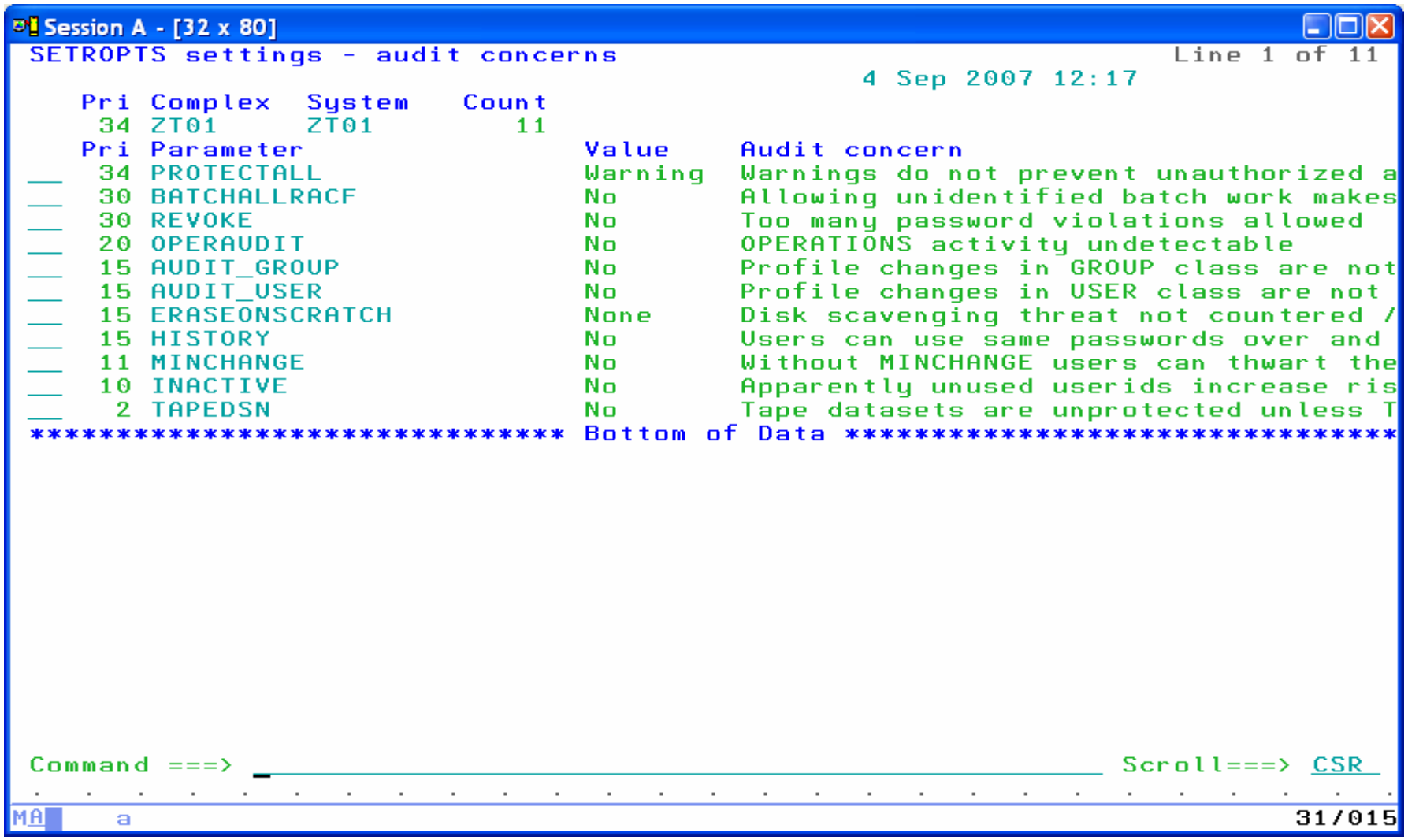
zSecure Data Sources



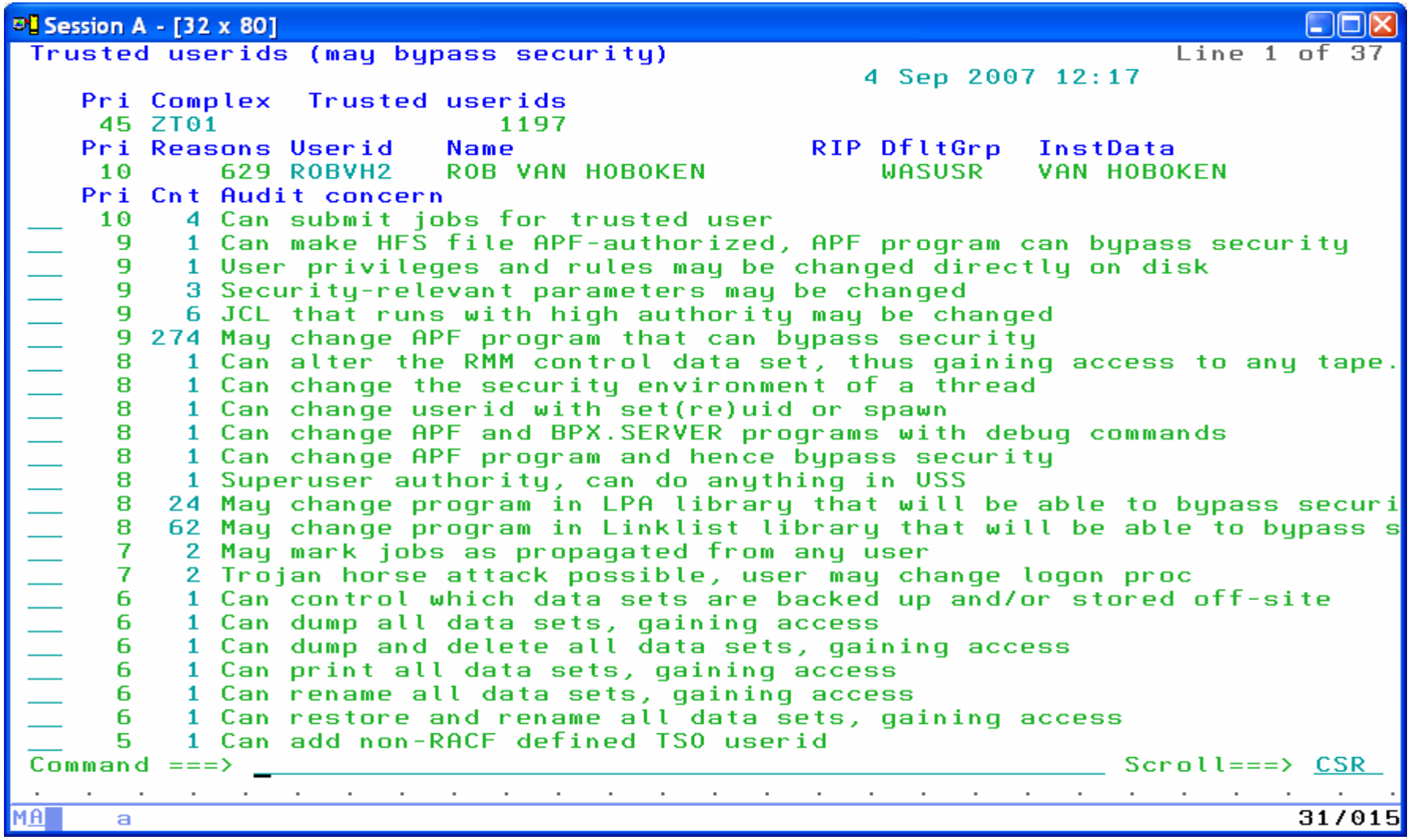
z/OS Status Audit – detailed reports



Automated vulnerability assessment



Trusted Userid Report



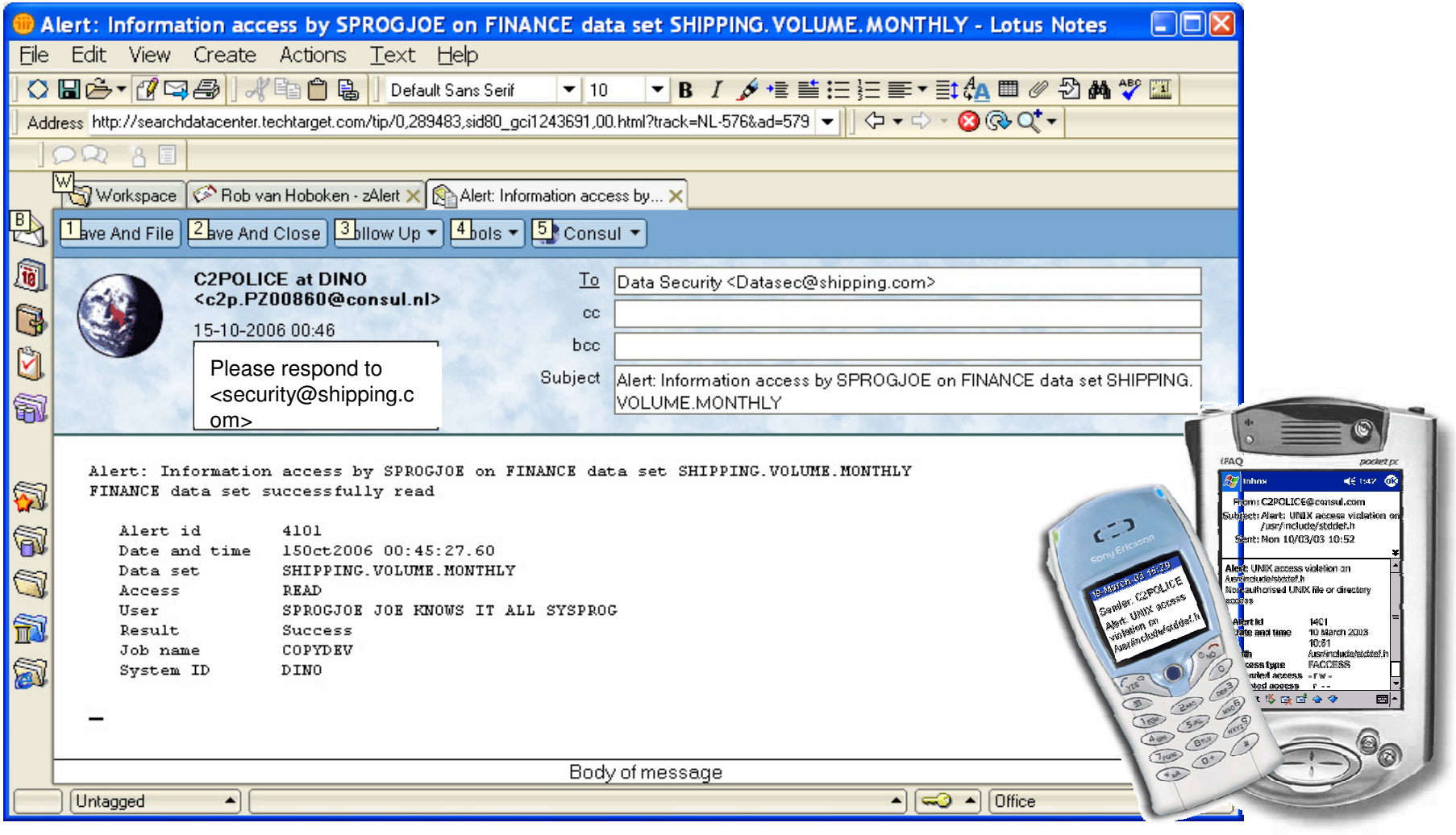
If access controls are not strong enough

- Situation:
  - Too many technicians with access to business databases
  - Must keep financial data confidential to prevent insider trading
  - Allow technicians to do their work
- Best Solution Available?:
  - Need to restrict access to financial data
    - Storage admin and sysprogs reading business datasets
    - Security admins granting themselves authority
    - Data security administrators granting improper access
  - Access reduction for privileged users
    - Impractical due to technical limitations
    - If you remove my ability to …. I cannot commit to ….

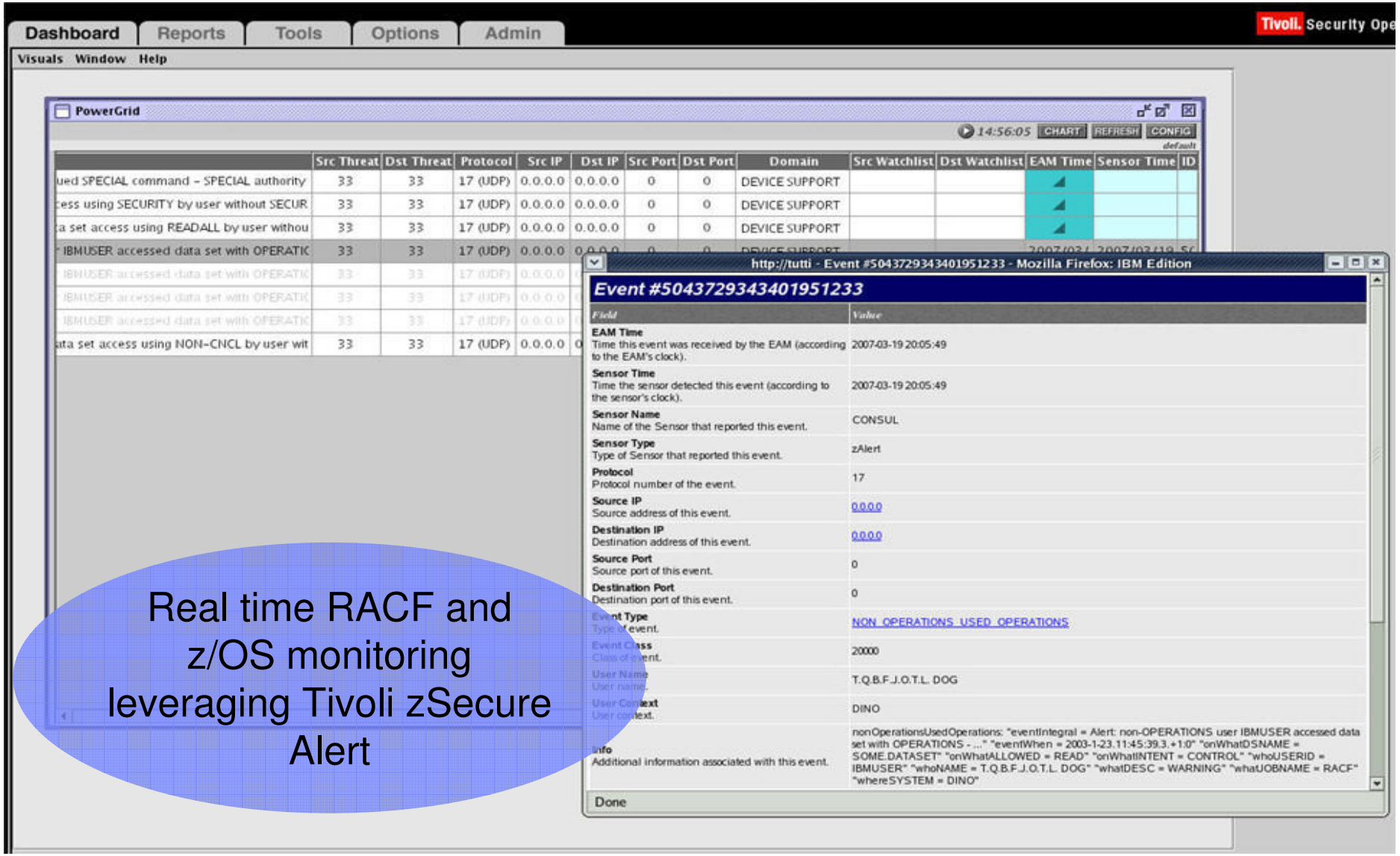
zSecure Solution

- Real-time alert as mitigating control – zSecure Alert
  - Reduce need to implement separation of access
  - sysprogs keep their “must be able to read/change anything” status
  - No need for political battle or costly re-orgs
  - Quick install, instant visibility

zSecure Alert issues alert for dangerous access



Integration with Tivoli Security Operations Manager



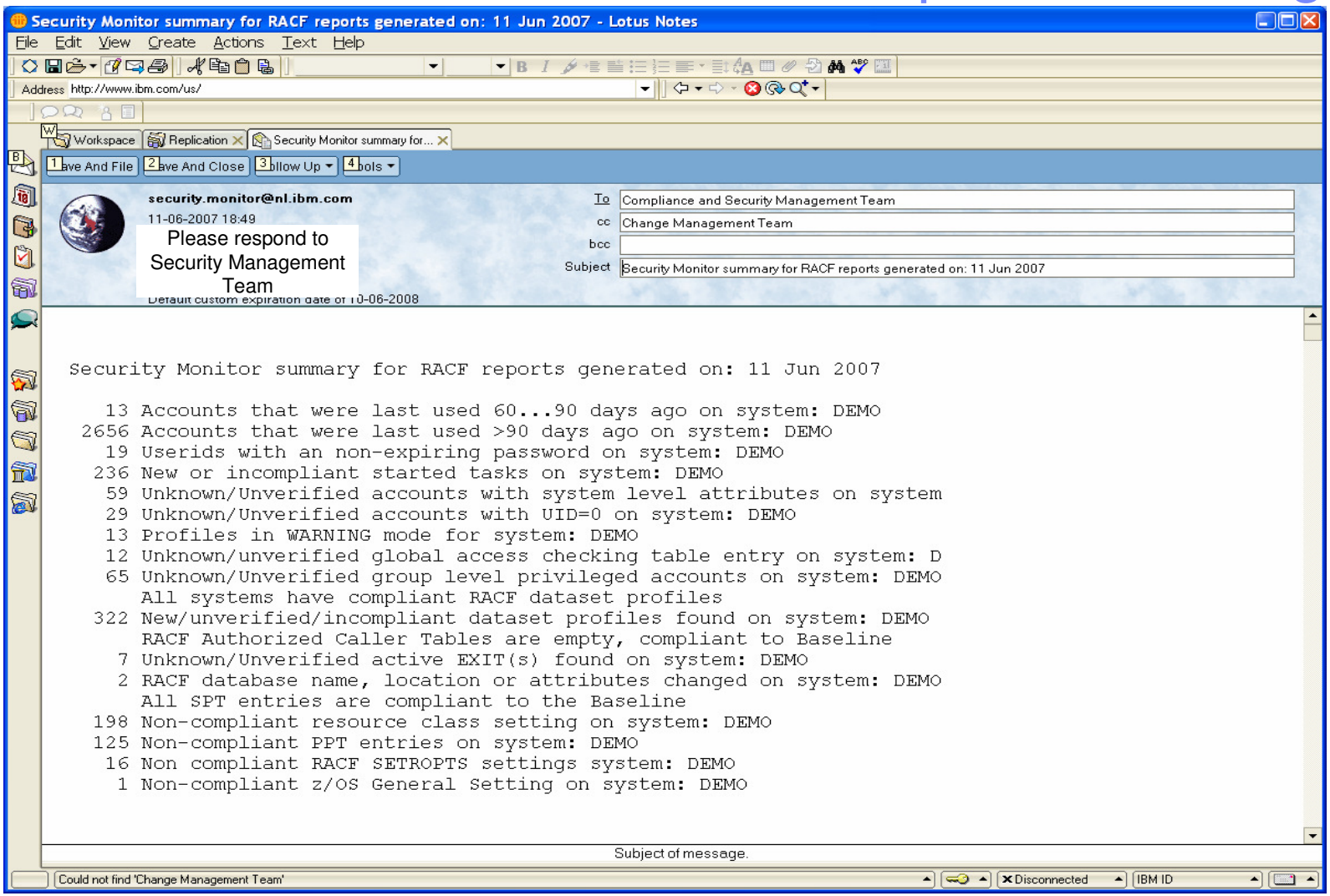
Case study: SOX reports

- Sarbanes Oxley requirements
  - Monitor changes to operating system and security (RACF and ACF2)
  - Monitor activities of privileged users
  - Monitor irregular logons
  - Verify operating system parameters against baselines
  - Verify users with specific (high) application authority
- Best Solution Available?:
  - Costly daily verification
  - Manual creation of queries and reports
  - Difficulty in baselining versus current state

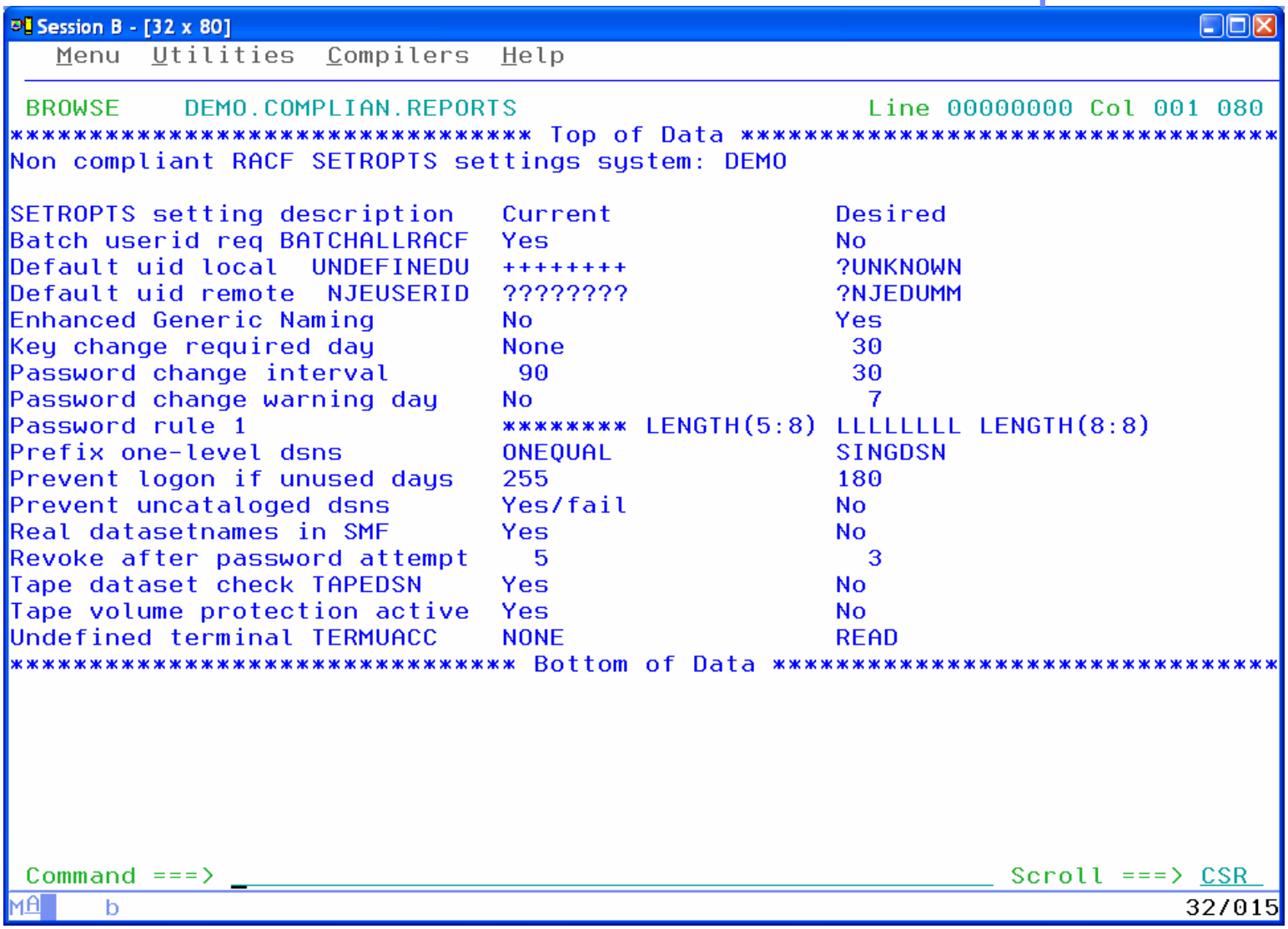
zSecure Solution

- zSecure Audit customized reporting
  - Baselines document the security implementation standards
    - Show parameters that are in conflict
    - Approved changes must be reflected in the baseline
    - Inappropriate changes will show up until they have been addressed

zSecure Audit: Statistics for the Compliance Manager



zSecure Audit: Details for the Technical Specialist

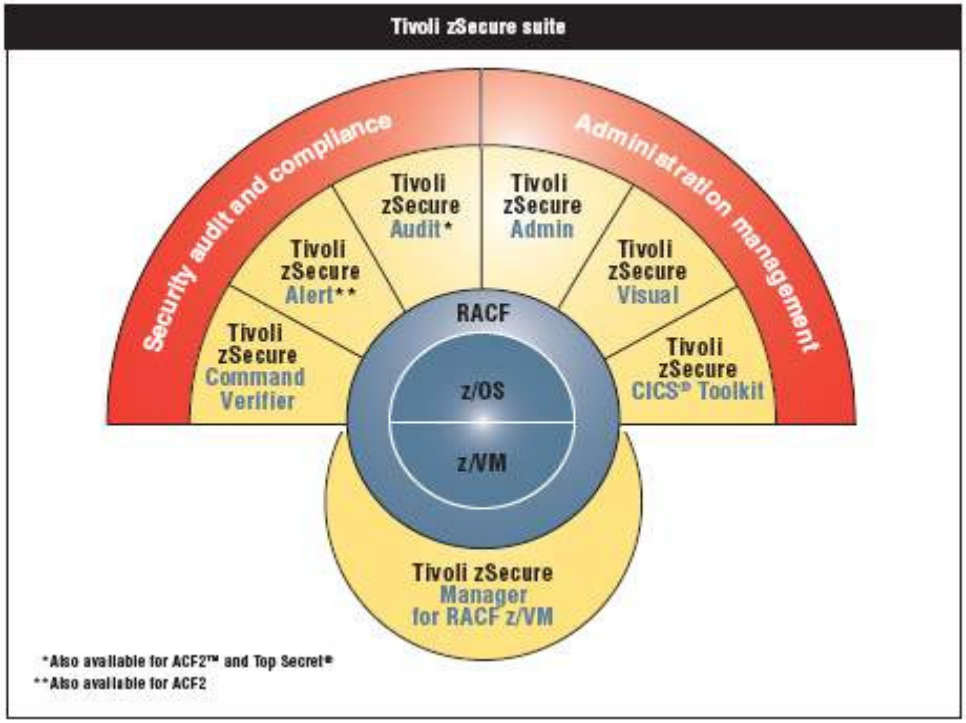


SOX report automation

- Solution: automated reporting for >25 LPARs
  - Exceptions summarized in an email
  - Detail reports available for review and archiving
  - Daily verification and maintenance < 0.5 FTE

Summary and Final Thoughts

- IBM Tivoli zSecure Suite – The Next Generation of RACF Security
- Regulation Challenges and Reality
  - The ever present auditor and privileged users
- The Tivoli zSecure Suite – Providing Futuristic RACF Security Today
  - Administration management
  - Security audit and compliance
  - Real-time alert
- Also for RACF on z/VM,
  CA ACF2 and CA Top Secret



Thank You for Joining Us today!

Go to **www.ibm.com/software/systemz** to:

- Replay this teleconference
- Replay previously broadcast teleconferences
- Register for upcoming events