IBM

Aloha from

TIVOLI NATION

Mainframe Security War Stories From The Trenches:

AKA - how to avoid a security disaster

Warning: Contains Technical Material – Parental Guidance recommended

Mike Cairns
IBM Tivoli zSecure Technical Specialist

AGENDA

- PART ONE – the headlines
- PART TWO – the real world issues
- PART THREE – a message from our sponsors
- PART FOUR – Q&A

PART ONE – the headlines

- Why you came today
- Sensationalism – ‘hackers’ at work!
  - Does happen – potentially high profile – headline grabbing
  - But not very often, and often kept as quiet as possible
- It’s the ‘smaller’ ones that happen day to day are the real concerns

What's it all about?

- SPECIAL, SPECIAL, SPECIAL…

RACF Release Timeline

September, 1976, Version 1 Release 1

- User identification/verification
- Data set authorization checking
- Journaling
- UT100, UT200, BLKUPD

July, 1977 Version 1 Release 2

- TAPE and DASD Volume protection
- Dynamic control of RACF options (SETROPTS)
- In-storage index blocks

July, 1978 Version 1 Release 3

- General resources
- In-storage profiles
- Report Writer (9/80)

November, 1981 Version 1 Release 4

- Password processing support
- List-of-groups
- RACF data manager interface (ICHEINTY)

- Q: Privilege Escalation – how do they do it?
  - A: the standard methods – just like any other system…

Standard Methods:

- From outside:
  - Enumeration
  - Fingerprinting
  - Vulnerability scanning
  - Pen-test
  - Trojan
- From inside:
  - Accident
  - Malicious
  - Privileged users/administrators

Standard Responses:

- From outside:
  - But it's a mainframe – no way: Enumeration
  - So what – how does this help them?: Fingerprinting
  - But this is only relevant for users: Vulnerability scanning
  - I trust all my users: Pen-test
  - How exactly?: Trojan
- From inside:
  - We all know this happens: Accident
  - We don't like to think this happens: Malicious
  - We really hope this never happens (to us): Privileged users/administrators

How about an example?

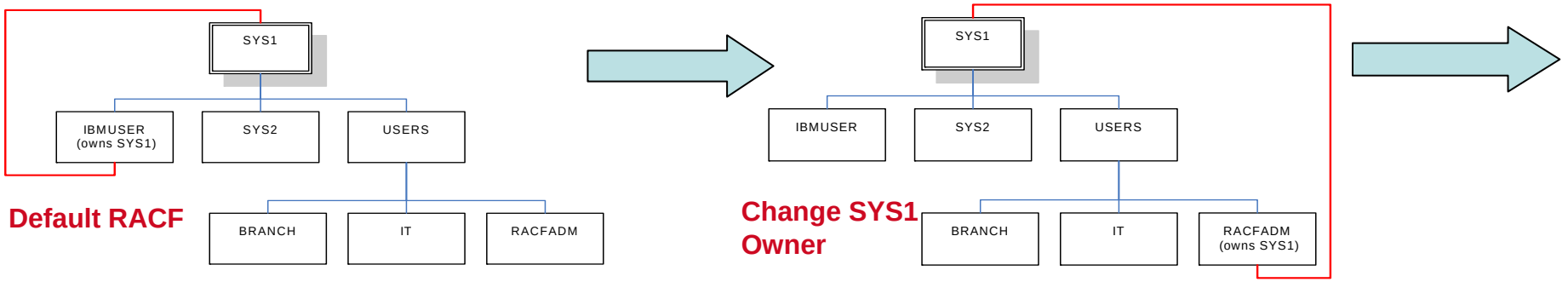
- Simplest method – Trojan Horse technique:
  - Attack Vectors include:
    - Cataloged Procedure datasets
    - Logon CLISTs and REXX execs
    - Any scripts regularly run by privileged users
- Mitigation:
  - Know the datasets vulnerable to this technique
  - Audit these at the necessary access level
  - Most important – least often performed: Review these Audit Reports!
  - Monitor in real-time

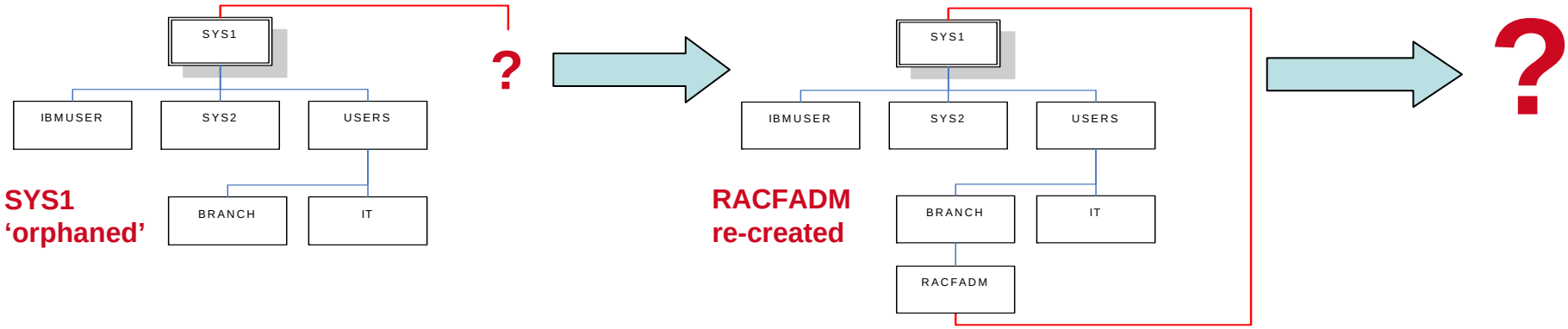
More technical examples

- The SVC that didn't play nicely:
  - Doesn't validate either its caller, and/or and target data area properly
    - Can be called by anyone with BAS skills – even 'script kiddies' could get relevant code in theory
    - Used by professional z/OS Pen-testers
    - Almost always a method to get SPECIAL this way
- The 'magic SVC' installed for 'maintenance/emergency' use
  - There really is no justification for these nowadays
  - If you really must – then make sure it's internally protected
  - And audit/report on this protection as a priority

But it doesn't have to be that technical

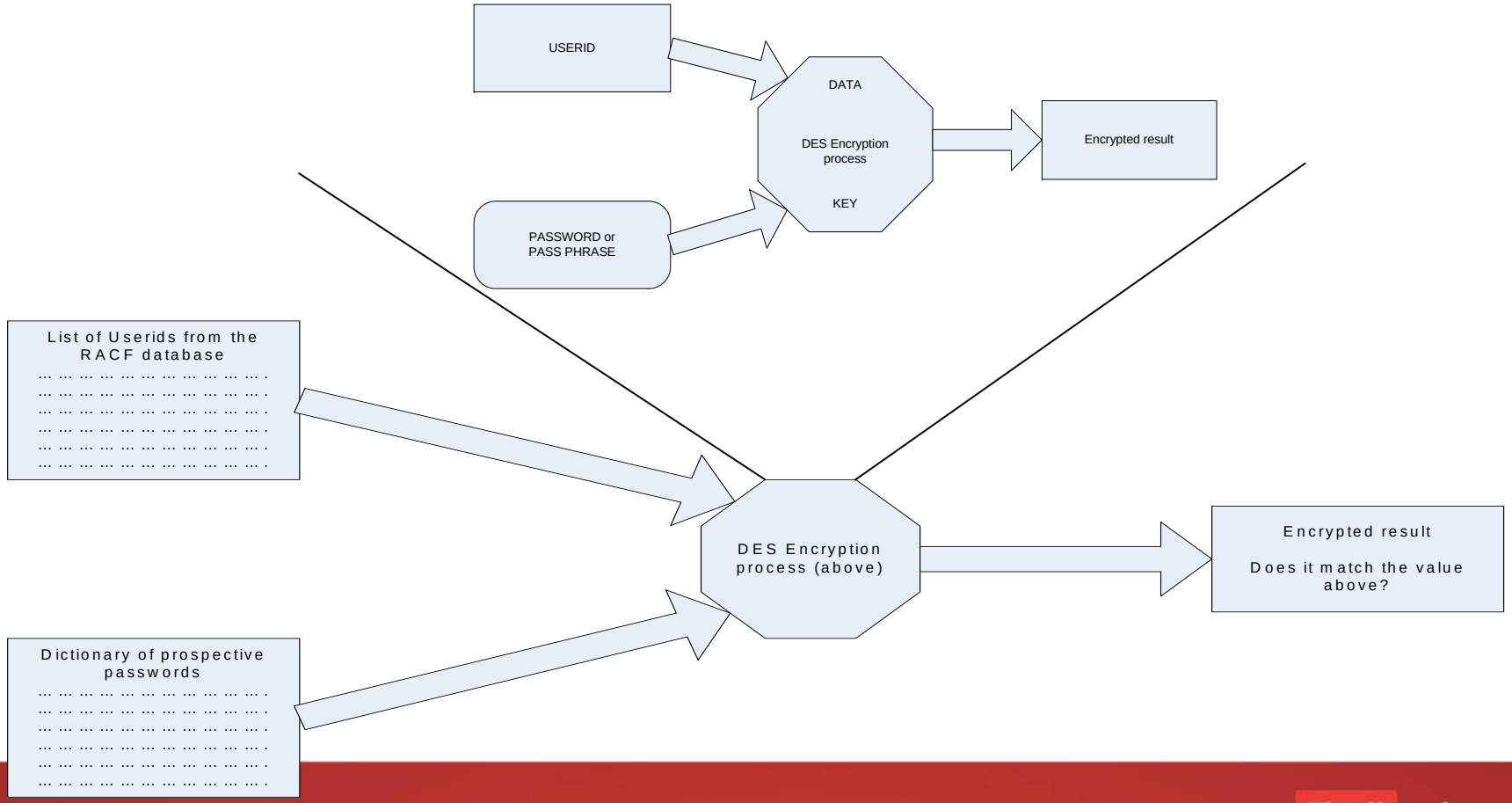
- Seemingly minor administrative actions may cumulatively introduce a serious exposure – Group Special example





The simplest mistake

- READ access to RACF or an exact database copy:
  - Offline brute force attack



Three avenues for total control of z/OS

- SPECIAL
  - Gimme SPECIAL – Gimme your system… :->
- APF authorisation
  - Update to AFP plus BAS skills is enough – but now you can also download programs that extract passwords from RACF
- Copy of RACF database
  - Brute force offline – opens up both above attacks

What to do next?

- Our ‘hacker’:
  - Trojan – wait until I have SPECIAL; he, he, he…
  - SVC attack – get SPECIAL temporarily, grant permanently
  - Group Scope issues – reset a SPECIAL users password
  - Sensitive data in general – discover passwords and config
- Our z/OS security and sysprogs:
  - Trojan – separate logon procs etc for SPECIALs etc
  - SVC attacks – technical z/OS audit and reporting
  - Group Scope issues – control RACF commands
  - Sensitive data in general – data and user classification…

PART TWO – the real world issues

- Data exposures
- Accidental damage/system errors
- Administrator mistakes
- Security ‘not important’ – must deliver application service no matter what the cost…

Data scrubbing and job routing example

- Data from production used in test and development jobs
- User able to specify the output class for jobs
- Test system configured to route work to prod if specified

- User submitted test job, routed to prod system, specifying auto-mailer output class.

- Job printed real customer names/addresses, false statement balances, and was automatically sent to Australia Post

- IT executives spend evening in Aussie Post mail sorting room emptying sacks of mail – you don't want that…

Accidental damage example

- System SPECIAL and AUDITOR activates full SMF auditing for all access
  - System immediately fills SMF datasets
  - Then buffers,
  - Then halts.

- The privileged user again
  - Did they really need that privilege at the time?

More Accidental damage

- System OPERATIONS
  - Should be entirely unnecessary in modern systems
  - If you must retain it – audit it and control the access with RACF
  - Never on personal userids
  - Move towards STGADMIN RACF control
- Falls into the ‘too much access’ bucket
- IT Sec 101: ‘need to know’
- Segregation of authorities is vital…

Administrator error damage example

- System Admin deleted all FTP related userids – oops
- Major international bank – all FTP with mainframe down
- Real problem:
  - Easy to recreate the userids and access
  - Hard to restore the passwords to hard coded values
- Lucky in this case – had software that would fix this
  - Zero outage – corrected before problem was noticed

Delivery over security example

- Batch userids with security administration rights
- Combined with RACF SURROGAT access to these userids by all support staff
- Overall – over 400 staff with the ability to readily ‘hack’
- Large Aussie finance company
- Support staff respond: “We need this access”…
  - Security admin: “All of it?! Full security admin rights as well! For everyone?”

More Delivery over security

- Major system replacement developed in isolated lpar
- Shortly before production implementation
  - RACF differences discovered
- 3 month, high risk/profile project to rectify
  - hundreds of thousands of RACF commands issued
- Really a project management and IT governance issue

What to do next?

- Data exposures
  - Use real/near-time auditing and monitoring to improve security implementation
- Accidental damage/system errors
  - Segregate the ‘killer’ access/privileges
- Administrator mistakes
  - See above + automated controls
- Security ‘not important’ – must deliver application service – no matter what the cost…
  - Business and App Dev governance

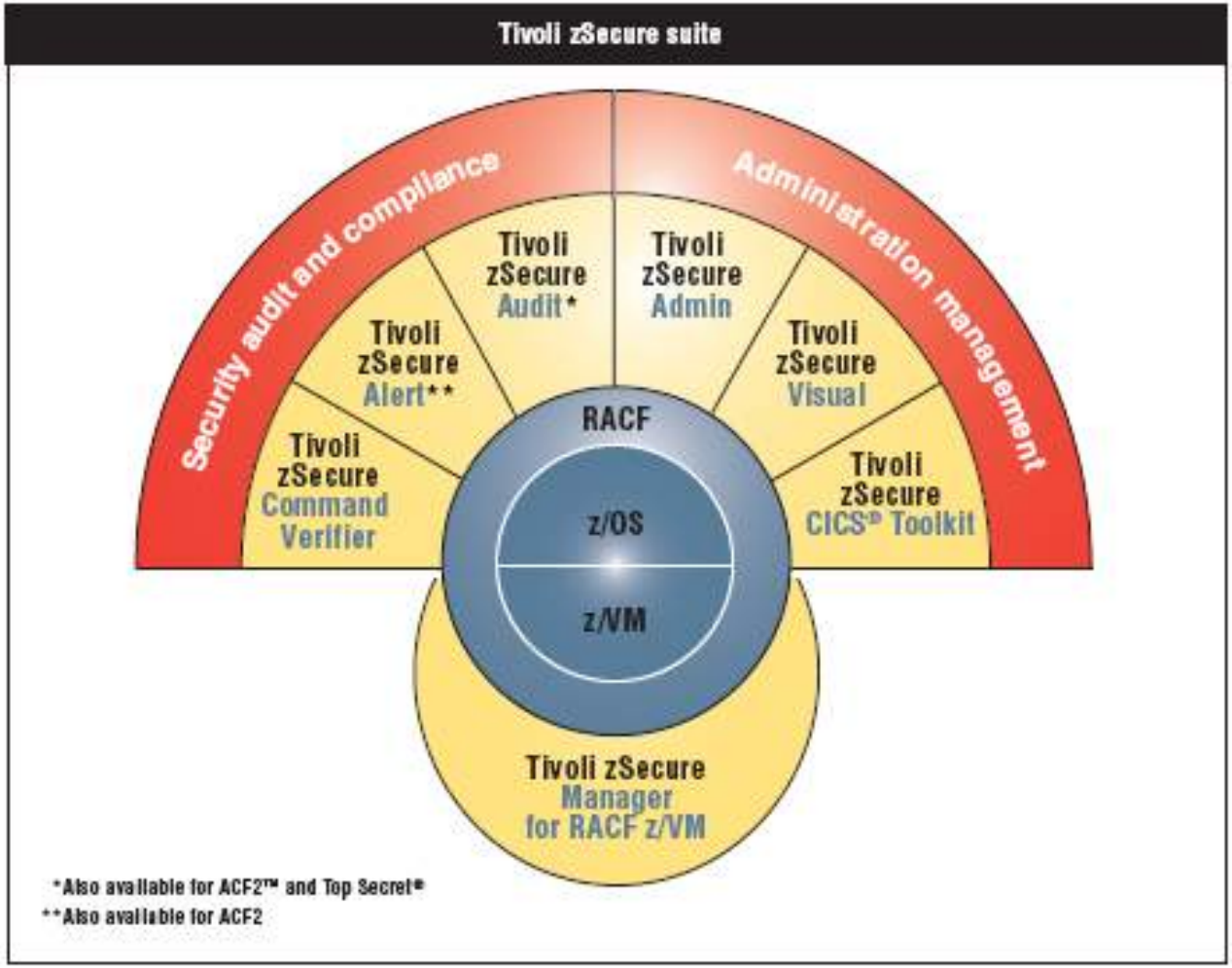
Privacy and confidentiality

- Data classification
  - Classify your data – somehow!
- Role based user access systems
  - Classify your users – provisioning

- Then you can have an ‘access matrix’ – users vs data

- On which you can now implement – Auditing and Monitoring
  - Auditing – once every few months
  - Monitoring – real time

PART THREE – a word from our sponsors



Introduction - A bit of Consul history

- 1987 Collect program IOCONFIG version 1 (now zSecure Collect)
  - Collects system snapshot in IOCONFIG file (now CKFREEZE)
- 1989 Consul enters security market with Consul/RACF (now Admin)
  - CARLa command language (somewhat like SAS)
- 1993 Consul/RACF 1.3.0, introduction of Consul/Audit
  - Fully integrated with Consul/RACF from the start
- 1994 Consul/RACF 1.4.0, introduction of CNGRACF component (now CKGRACF)
- 1996 Consul/Command Verification Option for RACF (now Command Verifier)
- 1998 Consul/RACF+Audit 2.3.0, introduction of Consul/Audit for ACF2
- 1998 Consul/RACF Administrator for Windows 1.1 (now Visual)
  - Windows front-end to Consul/RACF
  - Client/server communication shared with Consul/Enterprise (now TCIM)
- 1999 Consul acquires Palace Guard Software, CICS/RACF Toolkit 3.10
- 1999 Consul/Enterprise Audit 2.1 ships OS/390 event source (now TCIM Enabler for z/OS)

Introduction – Consul zSecure Suite

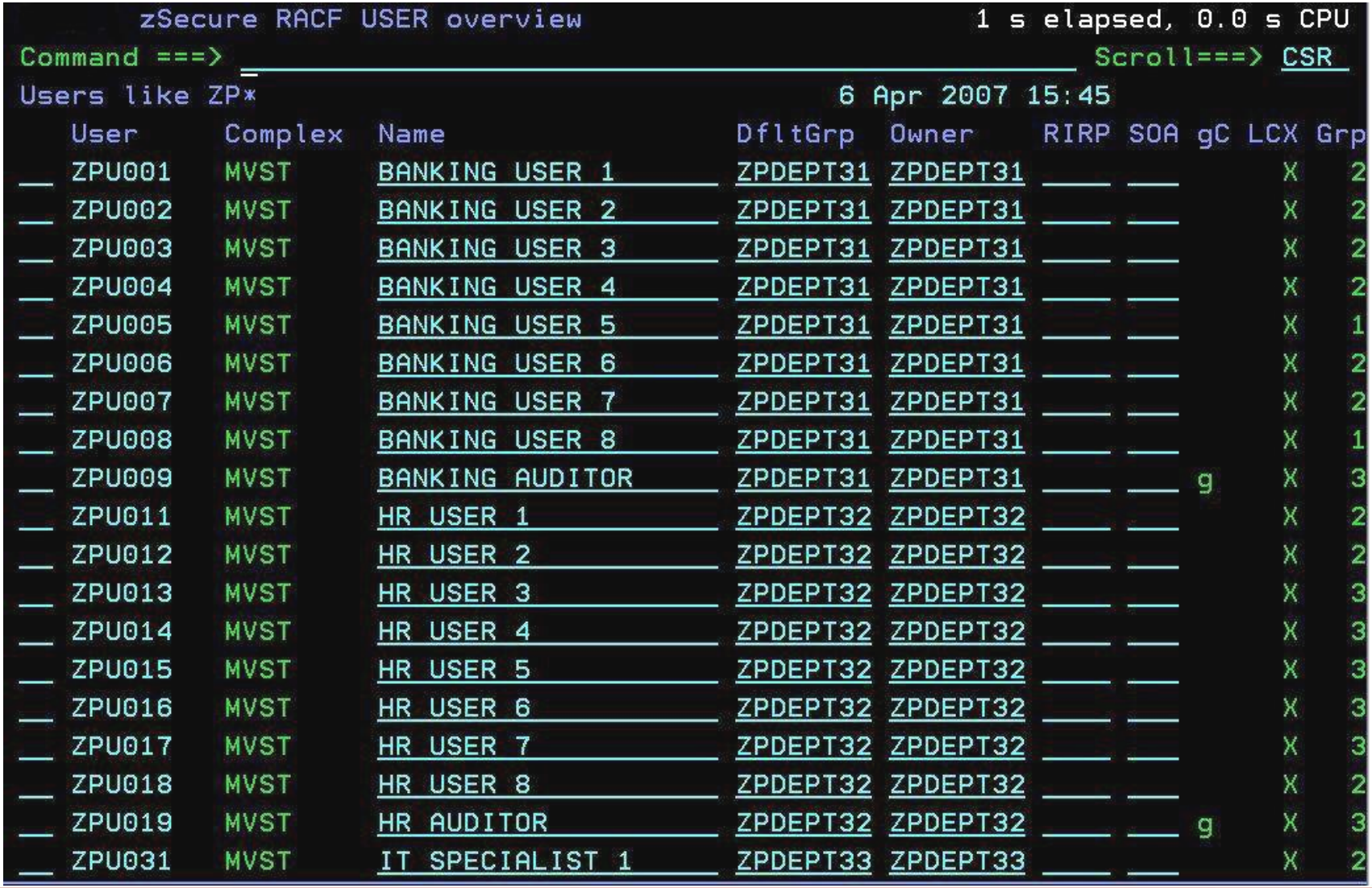
- 2001 The z/OS era: zSecure name introduced for existing products
  - Version numbers follow z/OS (as Collect had already done for OS/390 for some time)
  - 2001 Consul/zAdmin+zAudit 1.1.0, together called Consul/zSecure
  - 2001 Consul/zVisual 1.1.0
  - 2002 Consul/zLock 1.1.0 (née Command Verification Option)
  - 2002 Consul/zToolkit 1.2.0
- 2003 Version 1.4.5, introduction of Consul/zAlert
  - Alert Address Space does the real-time monitoring
  - Invokes CARLa engine to format and send alerts
- 2005 Version 1.6.0, introduction of Consul zAudit TSS
  - Top Secret support mostly consists of SMF and Audit Tracking File support
  - Product names now without “/”, and “InSight” inserted before zAudit, zAlert, zLock
- 2007 Version 1.8.0, introduction of Consul zAlert ACF2

Since IBM

- 2007 The Tivoli era: IBM ramps up development and integration
  - Compare Users/Groups function
  - RACF offline
  - CICS SMF type 110 support
  - More z/OS IP Comms Server support
  - DB2 Trace support
  - Tivoli suite integration

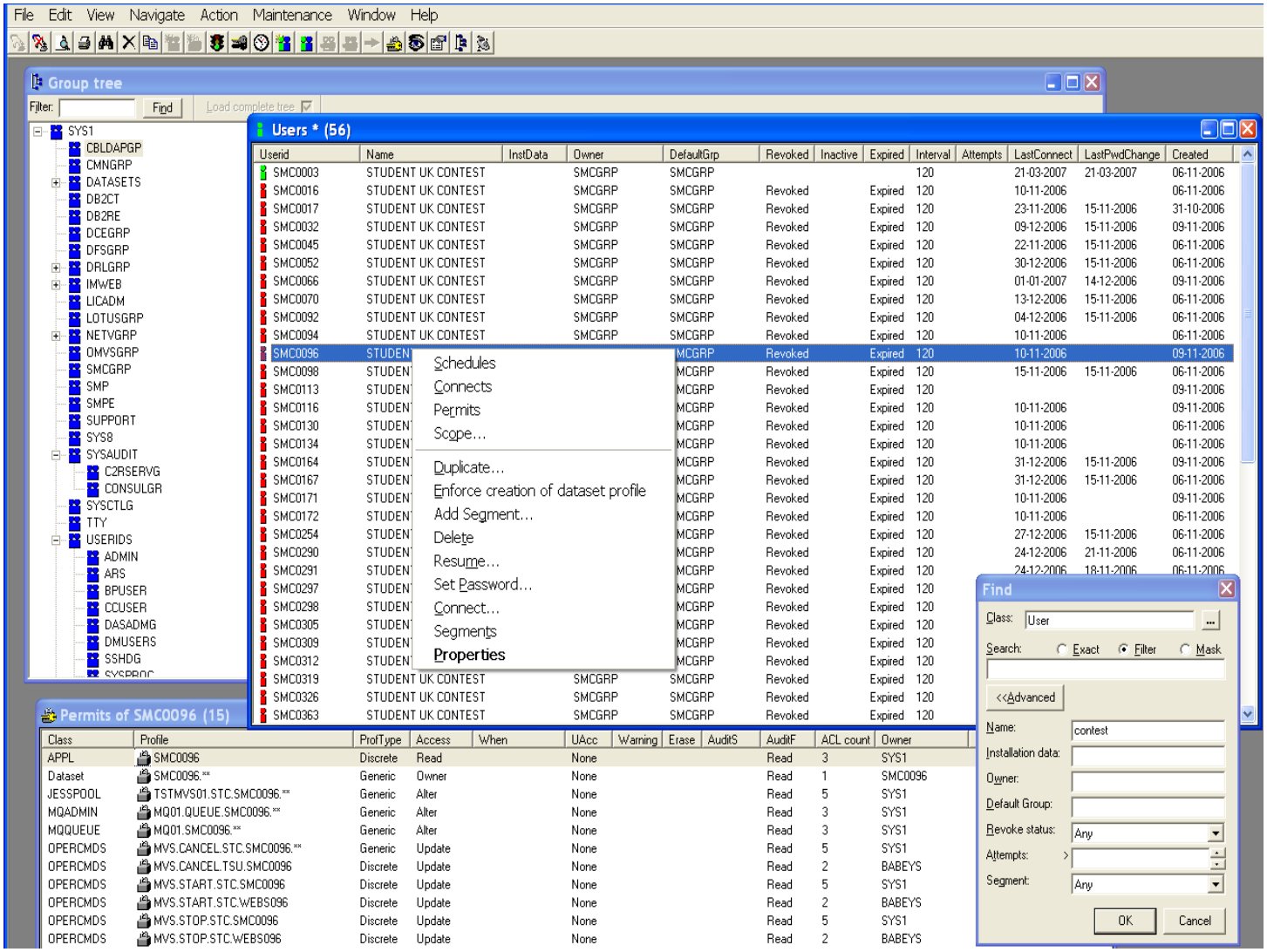
- Demonstrates tighter integration into z/OS development

zSecure Admin

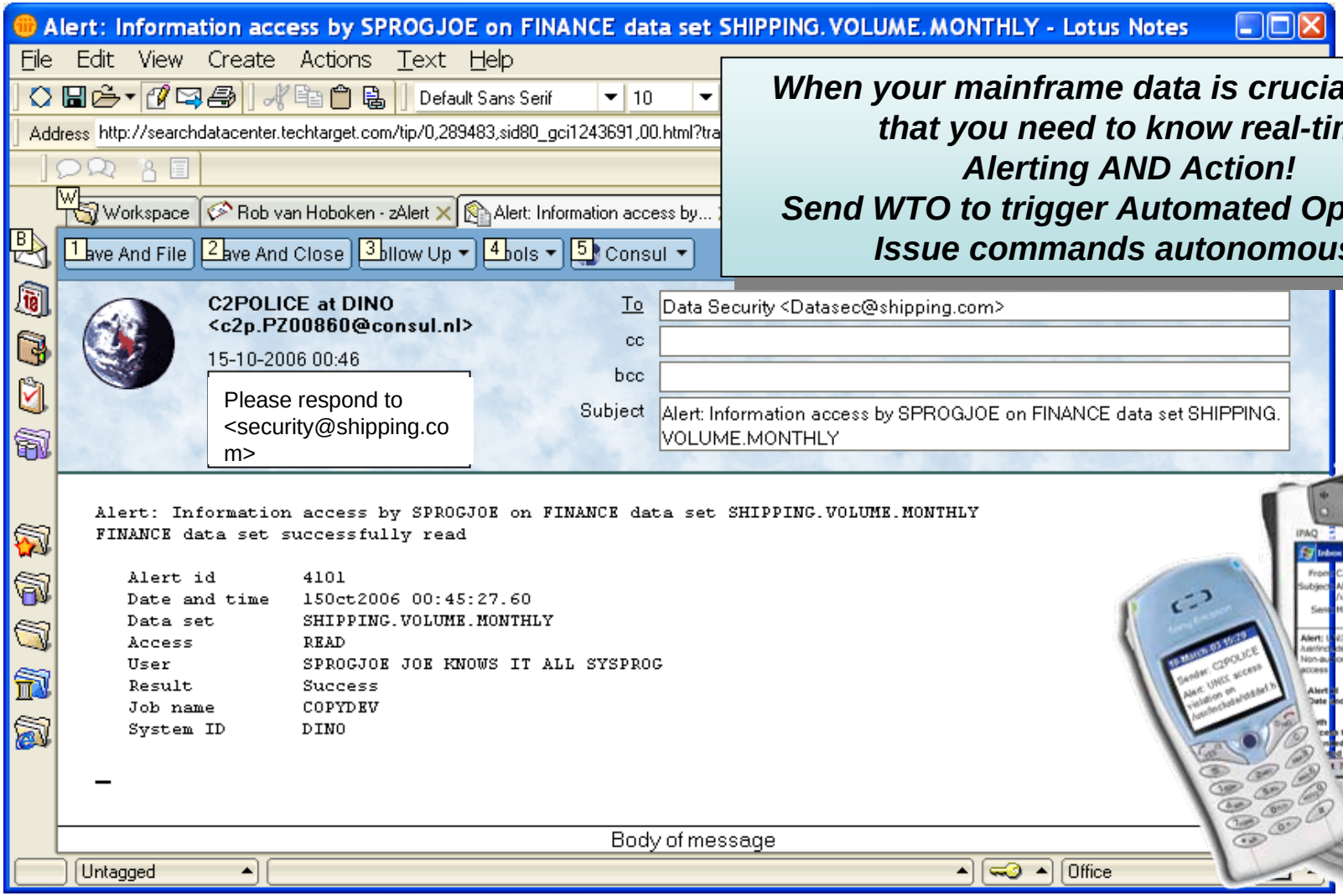


```
      zSecure RACF USER overview                          1 s elapsed, 0.0 s CPU
Command ===> _                                                Scroll===> CSR
Users like ZP*                                    6 Apr 2007 15:45
   User     Complex  Name                 DfltGrp   Owner    RIRP SOA gC LCX Grp
__ ZPU001   MVST     BANKING USER 1       ZPDEPT31  ZPDEPT31                X   2
__ ZPU002   MVST     BANKING USER 2       ZPDEPT31  ZPDEPT31                X   2
__ ZPU003   MVST     BANKING USER 3       ZPDEPT31  ZPDEPT31                X   2
__ ZPU004   MVST     BANKING USER 4       ZPDEPT31  ZPDEPT31                X   2
__ ZPU005   MVST     BANKING USER 5       ZPDEPT31  ZPDEPT31                X   1
__ ZPU006   MVST     BANKING USER 6       ZPDEPT31  ZPDEPT31                X   2
__ ZPU007   MVST     BANKING USER 7       ZPDEPT31  ZPDEPT31                X   2
__ ZPU008   MVST     BANKING USER 8       ZPDEPT31  ZPDEPT31                X   1
__ ZPU009   MVST     BANKING AUDITOR      ZPDEPT31  ZPDEPT31          g     X   3
__ ZPU011   MVST     HR USER 1            ZPDEPT32  ZPDEPT32                X   2
__ ZPU012   MVST     HR USER 2            ZPDEPT32  ZPDEPT32                X   2
__ ZPU013   MVST     HR USER 3            ZPDEPT32  ZPDEPT32                X   3
__ ZPU014   MVST     HR USER 4            ZPDEPT32  ZPDEPT32                X   3
__ ZPU015   MVST     HR USER 5            ZPDEPT32  ZPDEPT32                X   3
__ ZPU016   MVST     HR USER 6            ZPDEPT32  ZPDEPT32                X   3
__ ZPU017   MVST     HR USER 7            ZPDEPT32  ZPDEPT32                X   3
__ ZPU018   MVST     HR USER 8            ZPDEPT32  ZPDEPT32                X   2
__ ZPU019   MVST     HR AUDITOR           ZPDEPT32  ZPDEPT32          g     X   3
__ ZPU031   MVST     IT SPECIALIST 1      ZPDEPT33  ZPDEPT33                X   2
```

zSecure Visual

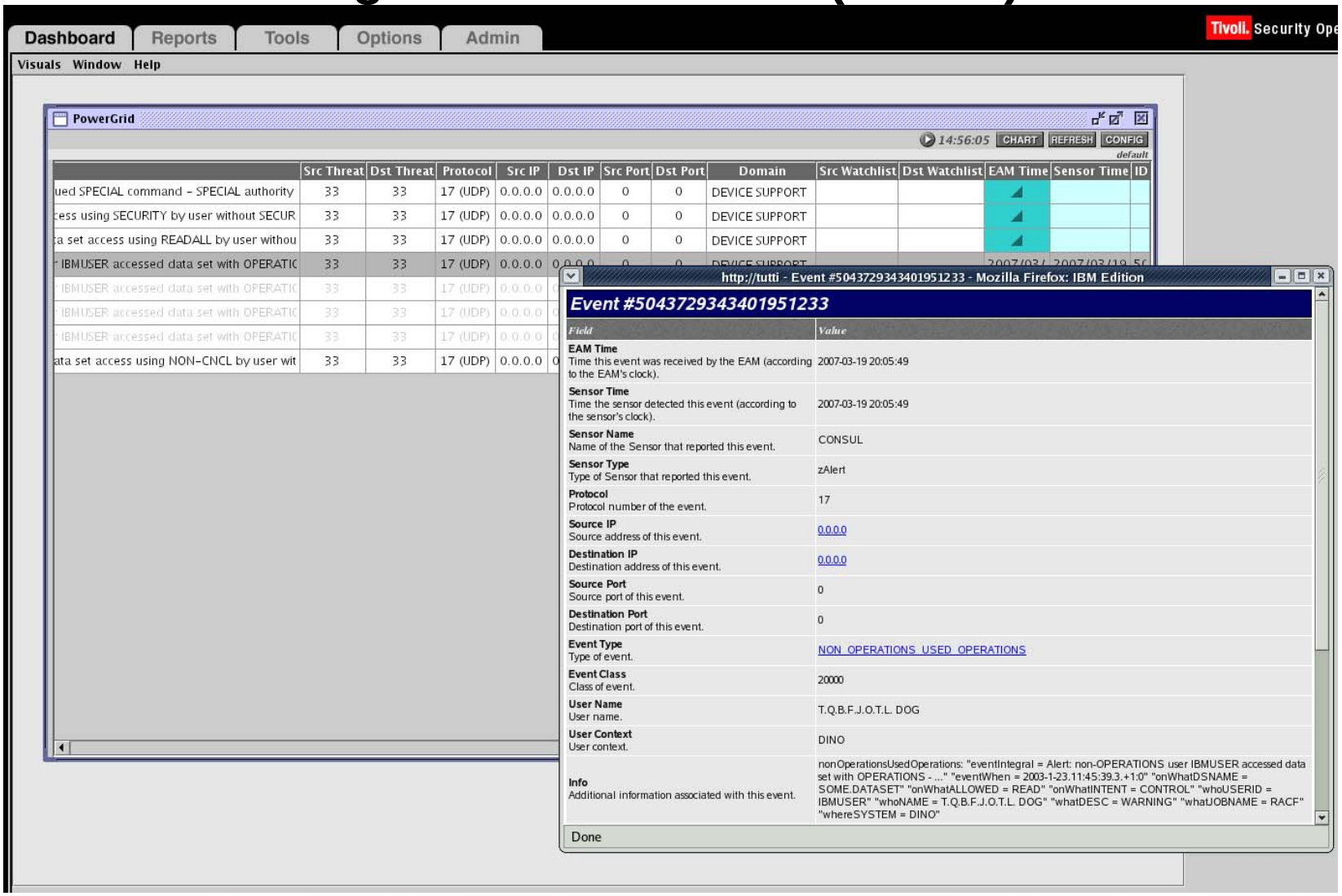


zSecure Alert

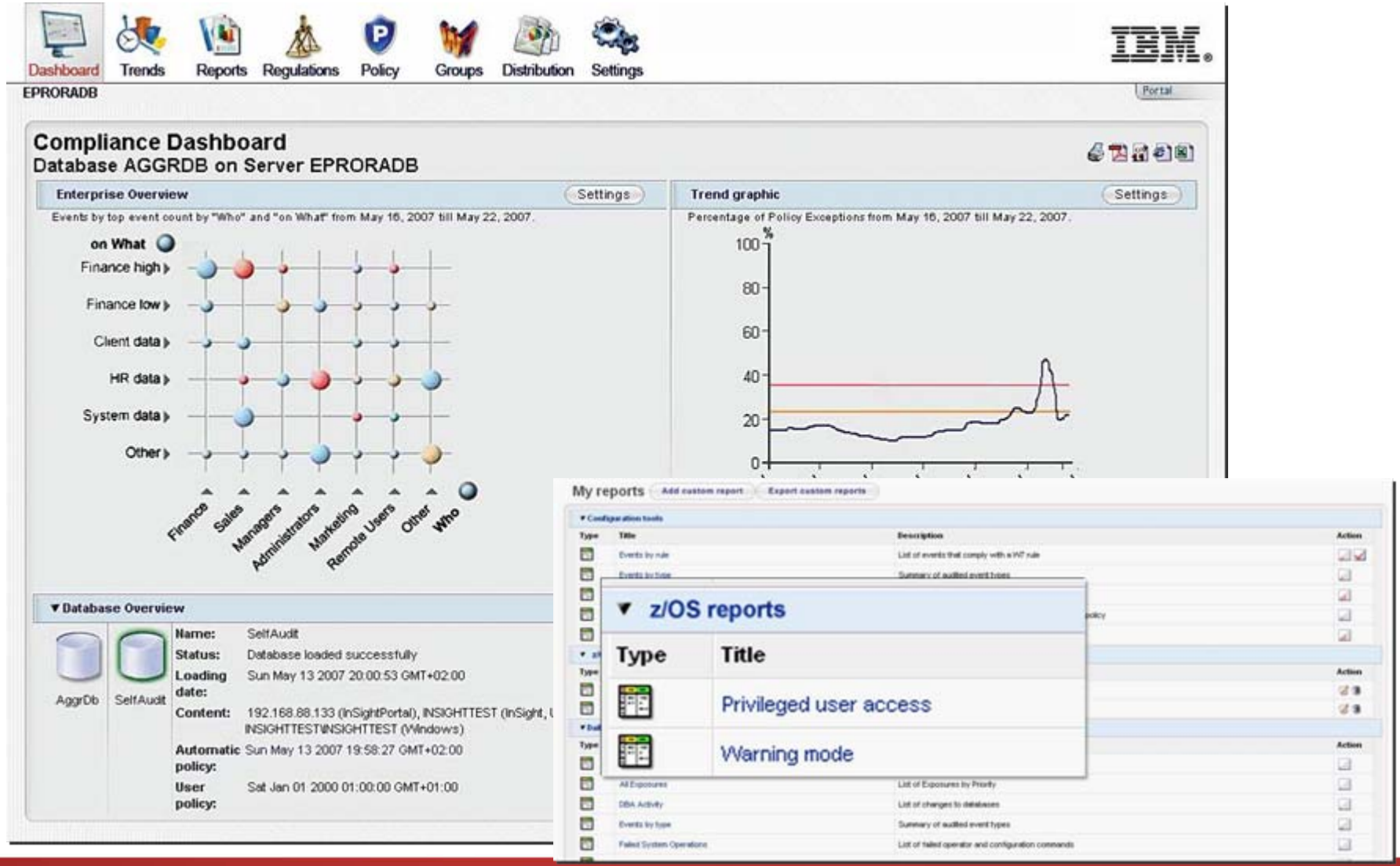


When your mainframe data is crucial enough that you need to know real-time
Alerting AND Action!
Send WTO to trigger Automated Operations
Issue commands autonomously

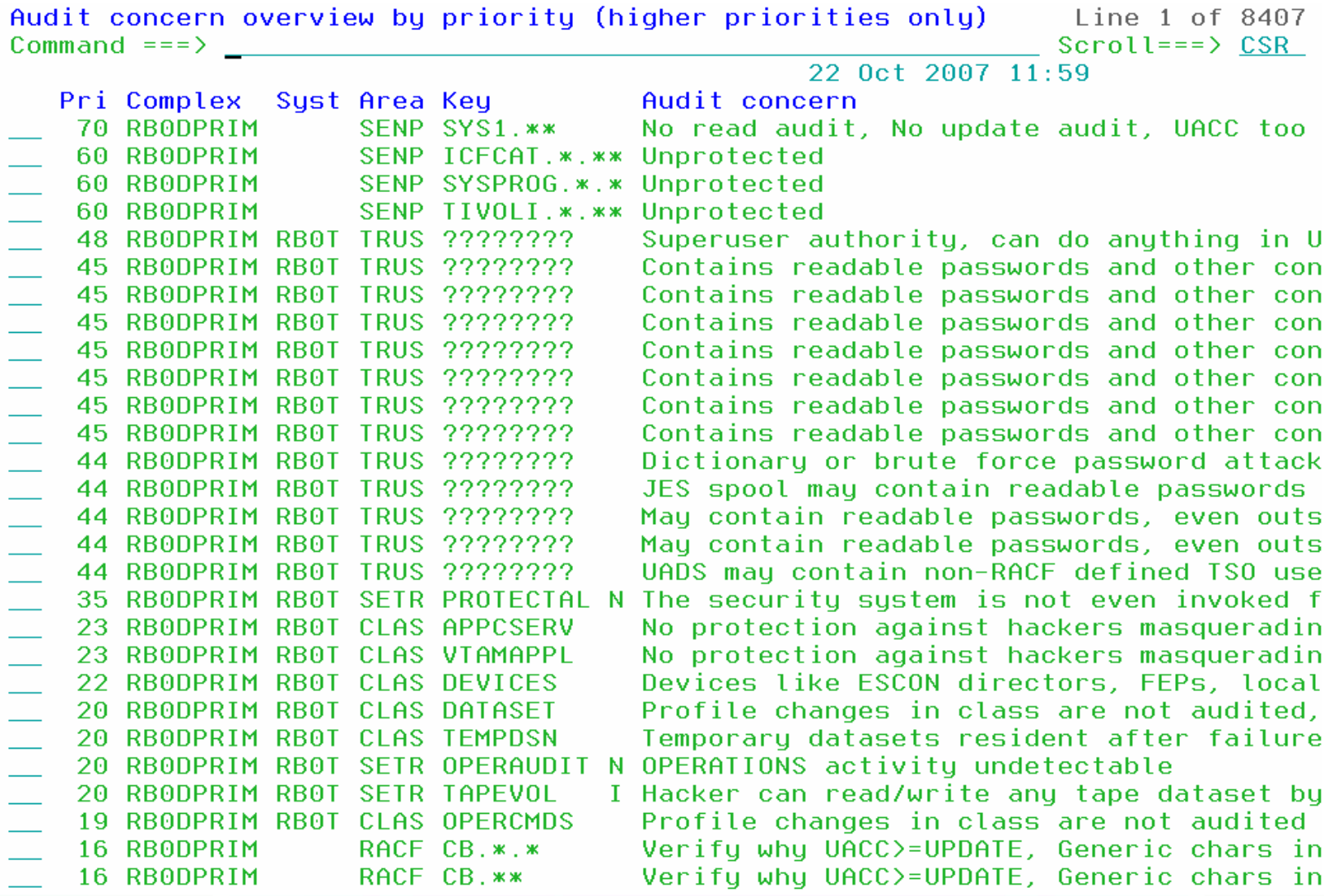
zSecure Alert integration with TSOM (TSIEM)



zSecure integration with TCIM

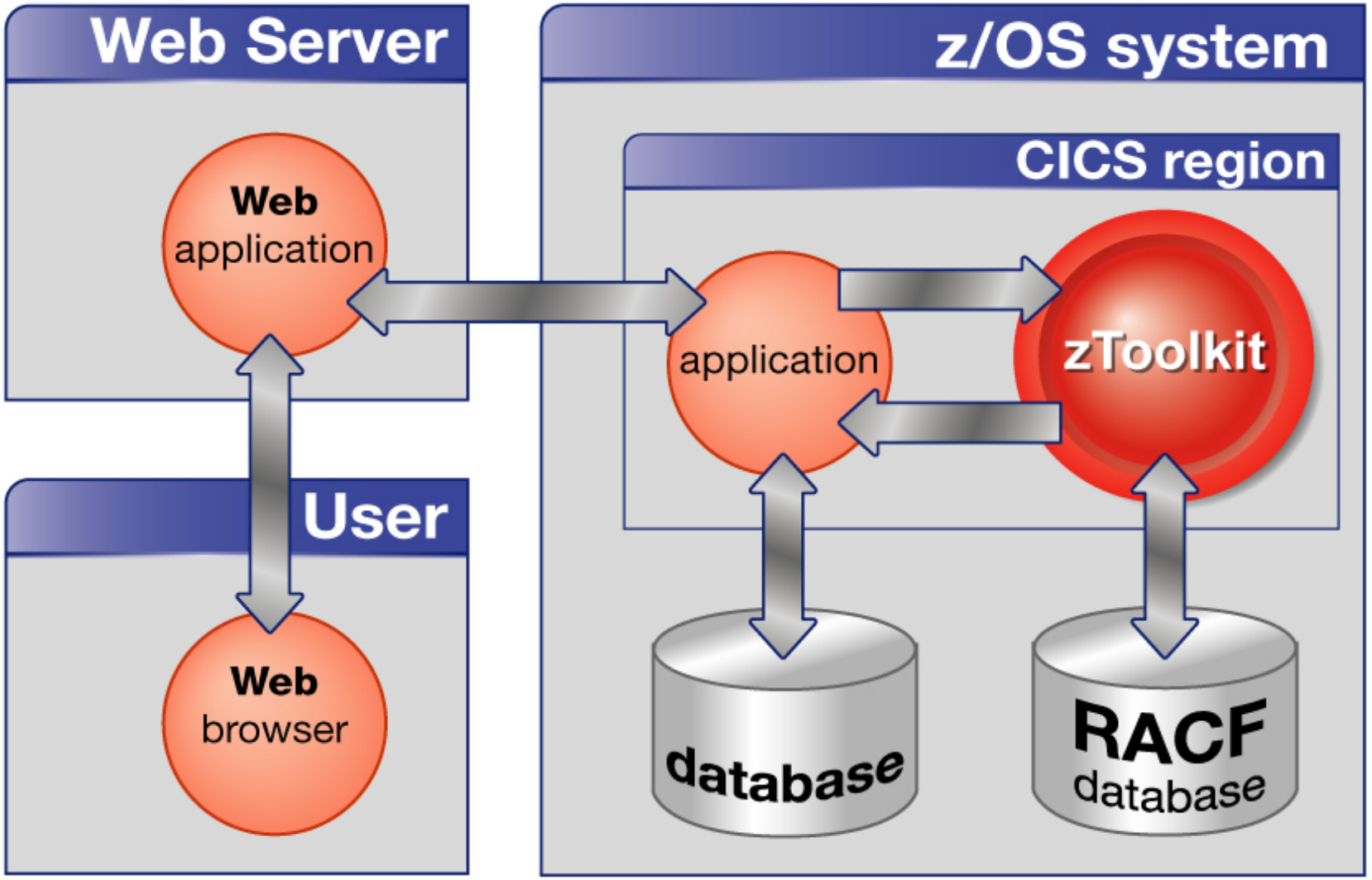


zSecure Audit



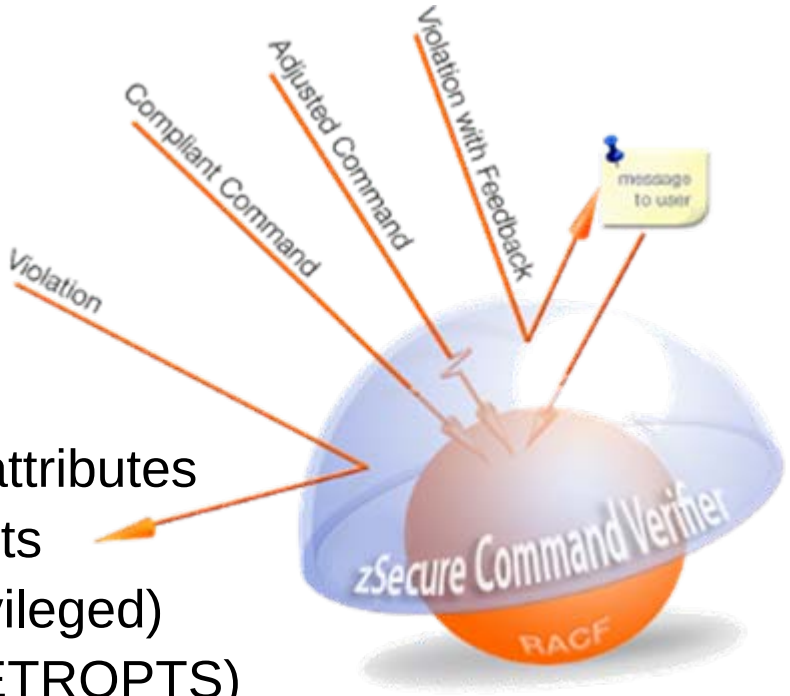
```
Audit concern overview by priority (higher priorities only)      Line 1 of 8407
Command ===> _                                                  Scroll===> CSR
                                                          22 Oct 2007 11:59
   Pri Complex  Syst Area Key          Audit concern
__  70 RB0DPRIM      SENP SYS1.**      No read audit, No update audit, UACC too
__  60 RB0DPRIM      SENP ICFCAT.*.**  Unprotected
__  60 RB0DPRIM      SENP SYSPROG.*.*  Unprotected
__  60 RB0DPRIM      SENP TIVOLI.*.**  Unprotected
__  48 RB0DPRIM RB0T TRUS ????????    Superuser authority, can do anything in U
__  45 RB0DPRIM RB0T TRUS ????????    Contains readable passwords and other con
__  45 RB0DPRIM RB0T TRUS ????????    Contains readable passwords and other con
__  45 RB0DPRIM RB0T TRUS ????????    Contains readable passwords and other con
__  45 RB0DPRIM RB0T TRUS ????????    Contains readable passwords and other con
__  45 RB0DPRIM RB0T TRUS ????????    Contains readable passwords and other con
__  45 RB0DPRIM RB0T TRUS ????????    Contains readable passwords and other con
__  45 RB0DPRIM RB0T TRUS ????????    Contains readable passwords and other con
__  44 RB0DPRIM RB0T TRUS ????????    Dictionary or brute force password attack
__  44 RB0DPRIM RB0T TRUS ????????    JES spool may contain readable passwords
__  44 RB0DPRIM RB0T TRUS ????????    May contain readable passwords, even outs
__  44 RB0DPRIM RB0T TRUS ????????    May contain readable passwords, even outs
__  44 RB0DPRIM RB0T TRUS ????????    UADS may contain non-RACF defined TSO use
__  35 RB0DPRIM RB0T SETR PROTECTAL N The security system is not even invoked f
__  23 RB0DPRIM RB0T CLAS APPCSERV    No protection against hackers masqueradin
__  23 RB0DPRIM RB0T CLAS VTAMAPPL    No protection against hackers masqueradin
__  22 RB0DPRIM RB0T CLAS DEVICES     Devices like ESCON directors, FEPs, local
__  20 RB0DPRIM RB0T CLAS DATASET     Profile changes in class are not audited,
__  20 RB0DPRIM RB0T CLAS TEMPDSN     Temporary datasets resident after failure
__  20 RB0DPRIM RB0T SETR OPERAUDIT N OPERATIONS activity undetectable
__  20 RB0DPRIM RB0T SETR TAPEVOL   I Hacker can read/write any tape dataset by
__  19 RB0DPRIM RB0T CLAS OPERCMDS    Profile changes in class are not audited
__  16 RB0DPRIM      RACF CB.*.*      Verify why UACC>=UPDATE, Generic chars in
__  16 RB0DPRIM      RACF CB.**       Verify why UACC>=UPDATE, Generic chars in
```

zSecure CICS Toolkit



zSecure Command Verifier

- Complete control over all RACF commands (similar to TAMOS)
- Control over command execution
- Enforces installation standards
  - Naming Conventions
  - Defaults for missing values
  - Mandatory values
  - Access Level Standards
  - Elevation of Authority not allowed
    - group special may not pass along attributes
  - Prevent changes to Access Control Lists
  - Prevent use of keywords (Trusted, Privileged)
  - Prevent changes to RACF settings (SETROPTS)
- Optional logging to SMF
- Optional audit trail in RACF profiles



PART FOUR – Q&A

- Some resources for further information
  - www.ibmsystemsmag.com
    - http://www.ibmsystemsmag.com/mainframe/julyaugust05/tipstechniques/9785p1.aspx?ht=
    - http://www.ibmsystemsmag.com/mainframe/marchapril07/tipstechniques/12532p1.aspx?ht=
  - Tivoli zSecure software, education and support
    - http://www-306.ibm.com/software/tivoli/sw-atoz/indexZ.html
    - http://www-306.ibm.com/software/tivoli/education/edu_prd.html#Z
    - http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivolizSecureSuite.html
  - RACF User Group online – RACF-L
    - http://listserv.uga.edu/archives/racf-l.html

Disclaimers and Trademarks

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements (e.g. IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided.

IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.

The following terms are trademarks or registered trademarks of the IBM Corporation in either the United States, other countries or both: DB2, e-business logo, eServer, IBM, IBM eServer, IBM logo, Lotus, Tivoli, WebSphere, Rational, z/OS, zSeries, System z.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

ITIL® is a Registered Trade Mark, and a Registered Community Trade Mark of the Office of Government Commerce, and is Registered in the U.S. Patent and Trademark Office.

COBIT® is a registered trademark of the Information Systems Audit and Control Association and the IT Governance Institute.

ISACA® is a Registered Trade mark of The Information Systems Audit and Control Association

IT Infrastructure Library® is a Registered Trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

IBM, the IBM logo, Candle, CICS, CT, CT/DS, CUA, DB2, eServer, ETE, RACF, IMS ,iSeries, MVS, NetView, OMEGAMON, OMEGAMON II, OMEGAVIEW, AIX, Rational, Redbooks, S/390, Tivoli, Tivoli Enterprise, Tivoli Enterprise Console, VTAM, Lotus, WebSphere, z/OS, and zSeries are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and Windows NT® are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries. Other company, product, and service names may be trademarks or service marks of others.