

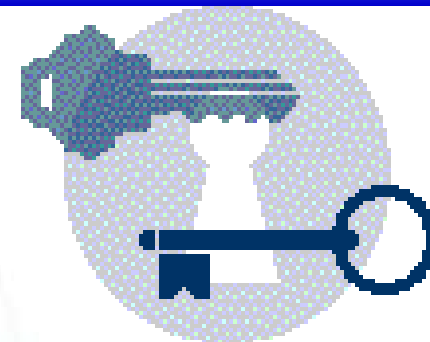


IBM Systems and Technology Group

Common Criteria Testing in a Common Security Environment The RACF Story

Diana Robinson
2455 South Road
Poughkeepsie NY, 12603
dianar@us.ibm.com
(845) 435-4865

Presented by: William Penny, IBM



9ICCC

Common Criteria Testing in a Common Security Environment, The RACF Story
September 23 – 25 2008, Jeju, Korea

© 2008 IBM Corporation

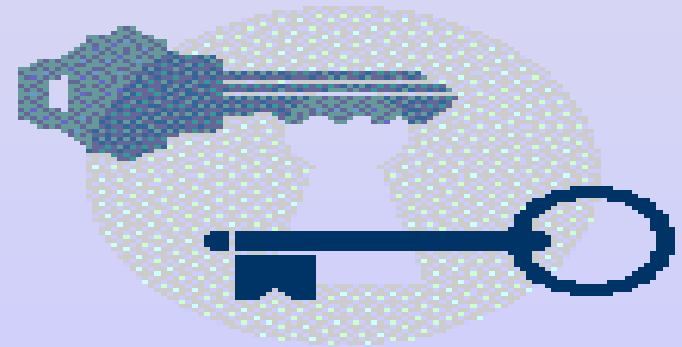
Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

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

Agenda

- ✓ Problem Statement
- ✓ What is RACF
- ✓ How does RACF work
- ✓ What is COMSEC
- ✓ How do RACF and COMSEC Relate
- ✓ Challenges Porting Testcases to COMSEC
- ✓ Why test in a common security environment
- ✓ Meeting the Challenge
- ✓ Proactive Approach to the Future
- ✓ Summary



Problem Statement

Testcases that previously executed successfully in the RACF function test (FCT) environment, failed when executed in a COMSEC environment.

WHAT IS RACF?

RACF (***Resource Access Control Facility***) is a security management product which gives authorized users access to use requested resources on a computer system (such as a file, a printer queue, space to run a program, and so forth).

How does RACF work?

RACF identifies and authenticates a user, determines the resources to which the user is authorized, and logs and reports attempts to get access to protected resources (by authorized or unauthorized users).

What is COMSEC

COMSEC (Common Security Environment)

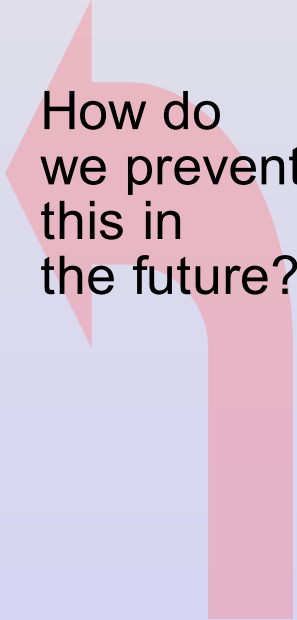
Is a system setup with the evaluated configuration, and is explicitly used for Common Criteria testing.

How do COMSEC and RACF relate?

Function test teams (including RACF) provide automated tests which are placed into COMSEC's test bucket for execution and regression.

Challenges porting testcases to COMSEC

Failing testcases were isolated		
Testcases were debugged		
What types of problems were uncovered?	Where were they injected?	Can the problems be fixed?
Is there a pattern?		



How do we prevent this in the future?

Challenges porting testcases to COMSEC

RACF TEST SYSTEM

Vanilla
System/

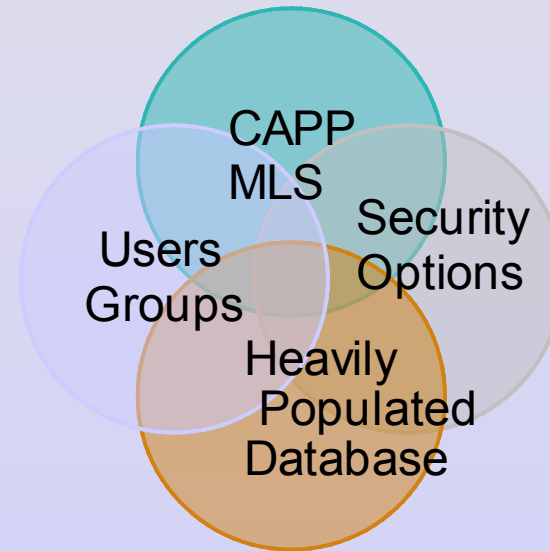
No Predefined
Resources

VS

COMSEC TEST SYSTEM

Evaluated Configuration

Profiles



Multiple users

System resources

- Pre-populated with 1000's of users, groups, profiles,
- system options, security options

Challenges porting testcases to COMSEC

- ✓ Identical userid, group and profile names
- ✓ Unable to access or allocate datasets
- ✓ Testcases modify common critical userid, IBMUSER (superuser)
- ✓ Default group inconsistencies (different on both systems)
- ✓ Testcase results assumed a common default group
- ✓ Evaluated configuration required additional protections
- ✓ Testcases that previously ran “successfully” now wSystem options and security options

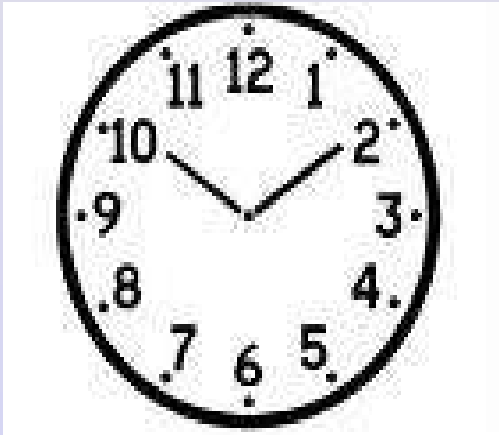
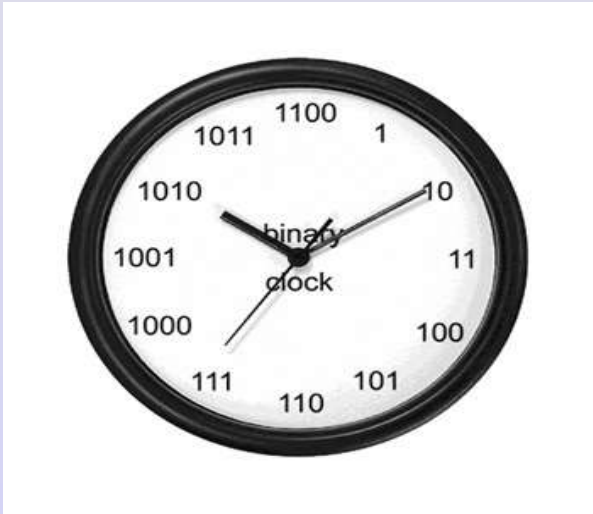
Why test in a common security environment?

What are
the benefits
of testing on a
Common System?



Why test in a common security environment?

Saves time



Why test in a common security environment?

Saves Money



Why test in a common security environment?

SIMPLY PUT.....

It's Cost-Effective!

What's the solution?

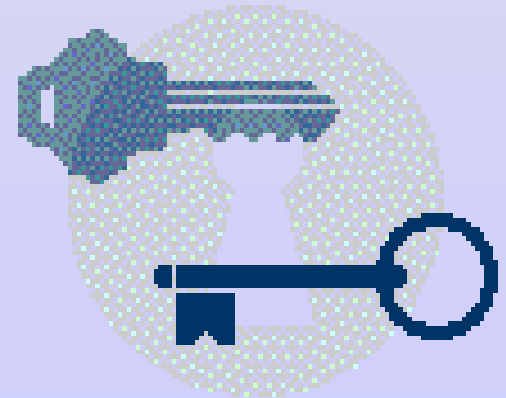
- ✓ Pre-test on RACF system with the evaluated configuration
- ✓ RACF protect all datasets
- ✓ Provide product specific prefixes for resource names
- ✓ Create a SUPER USER (other than IBMUSER) that is system independent
- ✓ Create common default groups - educate testers and provide examples on how to create default groups.

Pro-active approach to the future

- ✓ Once a week, during status meetings, one “Common Criteria/COMSEC testcase hint” was highlighted, which addressed the porting problems to educate testers.
- ✓ Provided education to the general test population at a zSeries Test Community general meeting.

Summary

- ✓ Perform a test dry run, executing testcases with the evaluated configuration turned on in function test to avoid unexpected testcase results in COMSEC
- ✓ RACF protect datasets
- ✓ Create unique resource naming conventions
- ✓ Create a super user that can be modified
- ✓ Create a unique default group



END OF DOCUMENT