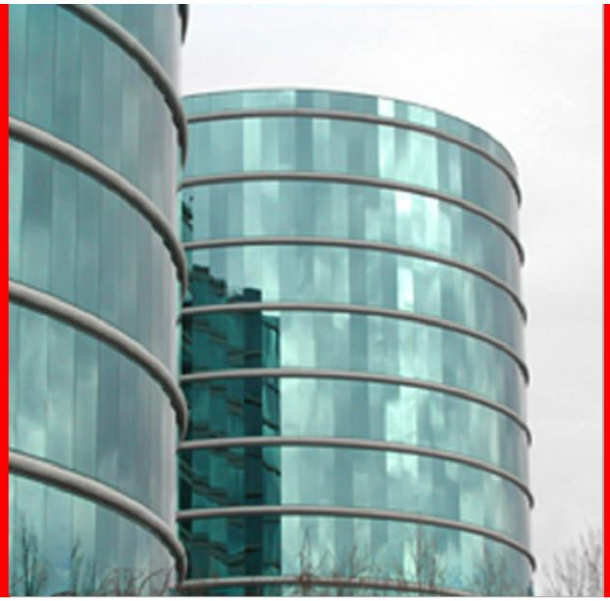

ORACLE®

CCRA - fragmentation or cohesion?

Shaun Lee
Security Evaluations Manager,
Global Product Security

Petra Manché,
Principal Evaluations Analyst,
Global Product Security

Agenda

- **Introduction and Background**
- The Issues
- Conclusions

CCRA - Component parts

- Primary
  - Arrangement on the Recognition of Common Criteria in the Field of Information Technology Security
- Supporting
  - Multiple or commercial CBs MC policy procedure
  - Time criteria to change from CCP to CAP MC policy
  - Voluntary Periodic Assessment
  - Conducting Shadow Certification

Growth of The Arrangement

- Then (Arrangement Dated May 2000)
  - 12 Participants
  - 6 Compliant CBs
- Now (http://www.commoncriteriaportal.org)
  - 24 Participants
  - 12 Compliant CBs

The Arrangement – Preamble

- The purpose contains four objectives shared by the participants, objective c being:

  "to eliminate the burden of duplicating evaluations of IT products and protection profiles"

- Has this been achieved?
- Is it maintainable?

Agenda

- Introduction and Background
- **The Issues**
- Conclusions

CCRA is CC's "Ace"

- For a vendor who wishes to perform an independent eval, why is CC attractive? Because…
- Evaluate once, recognised everywhere
  - Saves repeating work
    - Saves time and money
      - More cost effective
- Makes the decision to do an evaluation at all more worthwhile

Perceived Issues

- Increasing member numbers.
- The EAL4 limit
- Article 3 Exceptions / additional requirements
- Impact of evaluations for non-CCRA members

Bigger is Better?

- Membership has doubled – issuing and accepting
- Original membership of like minded participants, now an increasing geographical, ideological and political spread
- Newer members may have requirements that are not satisfied by current CCRA
- Further new members could increase the (perceived) differences?

The EAL4 limit

- Provides a simple go/no-go criterion for recognition but:
  - Why can't EAL5 automatically imply CCRA acceptance at EAL4?
  - Is this simplistic view still appropriate?
- The current implementation of EALs has itself been questioned in conference:
  - Rooted in TCSEC and ITSEC principles and time to move on
  - The selection of components needs to be looked at again - e.g. less design trace, more VA and test
    - Additional things could be done by vendors now, but wouldn't have recognition

Article 3 / Additional Requirements

- National Security Exemption
  - A reasonable concept, but the range of systems or products should not be unnecessarily large.
- National Requirements
  - Participants who expect greater detail for their purposes than Certification Reports currently provide
- Agency Requirements
  - Specific government agencies having preference for ‘local’ evaluations either by inference or by specifying requirements over the CCRA recognition limit

Evaluations for non-CCRA members

- Still some significant non-members
- If vendors have to support other evaluation schemes for significant customers/nations, re-use benefit provided by CC can be diluted.
  - limited resources split between schemes but doing similar work. Thus, CCRA countries do ultimately lose out through missed opportunity
  - In extreme, could be performing 3 evaluations for acceptance in 3 or 4 countries, so less cost effective.
- Vendors can apply some pressure through industry associations and govt. affairs/lobbying, but:
  - CC has to be able to sell itself as better than indigenous schemes
  - Politics plays a large part
  - Consider diplomacy to invite in significant non-members?

Agenda

- Introduction and Background
- The Issues
- **Conclusions**

The Verdict

- Eliminating the burden of duplicating evaluations has, to a large degree, been achieved
- Some signs of fragmentation because of diversity of membership, though generally contained for now
- The basics of CCRA have remained unchanged through 3 versions of the CC. V4 is good time to compromise on differences so CCRA members are again united. Invite other countries to participate, don't await applications passively
- Because **CCRA is what makes the scheme worthwhile for vendors**

For More Information

Oracle Security Evaluations:

http://www.oracle.com/technology/deploy/security/seceval/

General Oracle Security information:

http://www.oracle.com/technology/security

http://www.oracle.com/solutions/security


Q&A


ORACLE IS THE INFORMATION COMPANY