EAL1: Resuscitate or Euthanize

The low assurance problem

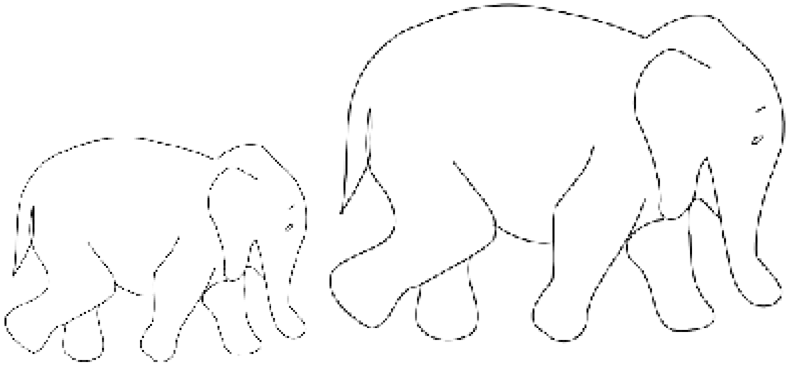
Julian Straw

9ICCC, Jeju, Korea

24 September 2009

Outline

- Background to EAL1
- The low assurance problem
- Options for change



Background to EAL1

- A new idea in CC
  - TCSEC C1 ↔ ITSEC E1 ↔ CC EAL2
    ↓
    CC EAL1
- Entry level assurance
- Boost number of certifications
- Minimum set of useful evaluation work
- Could be done without vendor assistance
- Certification for the mass market
- Extend reach of evaluation schemes to new territory

Evaluations since Jan 2007

Level	Number	%
EAL1	11	4
EAL2	75	26
EAL3	64	22
EAL4	113	38
EAL5	10	10
EAL6	0	0
EAL7	0	0

- EAL1 a very small proportion of evaluations
- No significant change since CC3.1

Source: www.commoncriteriaportal.org

What went wrong?

- High overhead of evaluation (especially in CCv2)
  - ST requirements in CCv2 were same for all EALs
  - Designed “downwards”
  - Scheme entry procedures
  - ISO17025 and CEM overheads
- Low demand from consumers
  - Alternative testing approaches available at this level
  - Can be done internally by consumers
  - Little evidence of government mandates
- Unpopular with labs
  - High cost of CC sales means labs prefer higher assurance with more margin

What went wrong?

- Stigma of entry level assurance
  - Entry levels have always been unpopular
  - Is EAL1 there simply to boost EAL2?
- Bad press
  - Little promotion to industry and non-classified arena

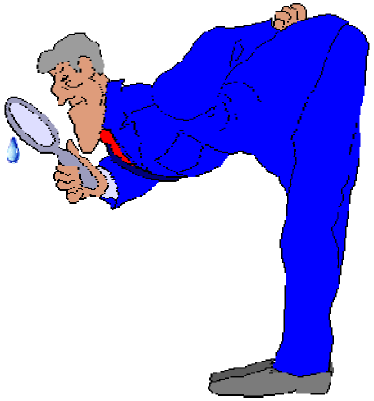
Does EAL1 have value?

- Clear presentation of security functions
- Functional testing
- Resistance to known vulnerabilities
- Quality of guidance
- Internationally recognised

Problem is recognised

- Schemes have seen low take-up
- Problems:
  - Security Target
  - Vulnerability assessment
  - Scheme overheads
  - Duration
  - Price
  - Perception
- Action taken in CCv3.1

EAL1 Activities (CC3.1)



Security Target (ST-lite)

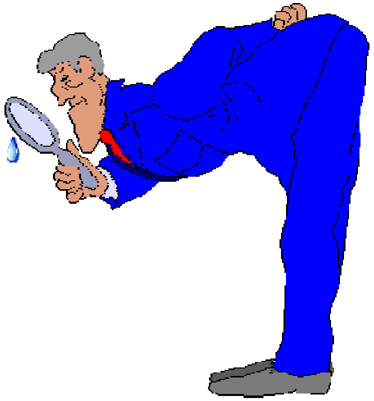
- ASE_INT.1 ST introduction
- ASE_CCL.1 Conformance claims
- ASE_OBJ.1 Security objectives for the operational environment
- ASE_REQ.1 Stated security requirements
- ASE_ECD.1 Extended components definition
- ASE_TSS.1 TOE summary specification

~~Security problem definition~~

~~Rationales~~

~~Objectives for the TOE~~

EAL1 Activities (CC3.1)



Guidance documents

- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures

Development

- ADV_FSP.1 Basic functional specification

Life-cycle support

- ALC_CMC.1 Labelling of the TOE
- ALC_CMS.1 TOE CM coverage

Tests

- ATE_IND.1 Independent testing – conformance

Vulnerability assessment

- ADV_VAN.1 Vulnerability survey

Problems remain

- ST issue resolved
- Vulnerability search introduced

…..but

- No evidence of increase in demand
- Scheme overhead
- Duration/Price
- Perception

What are the options for CCv4?

- Do nothing
  - No evidence of harm
  - Makes EAL2 look better
- Remove entirely
  - EALs are just examples
  - Leave components?
  - Numbering change would cause confusion
- Change EAL1 content
  - Add requirements to raise value
  - Reduce requirements to lower price
- Reposition in market

ST modification

- Action already taken in CCv3.1 (ST- lite)
  - No security problem definition
  - No security objectives for the TOE
  - No objectives rationale
  - No requirements rationale
- Removes a great deal of work
- Not clear whether this is well understood by the market
- Possible further changes
  - Little scope for further reduction of effort
  - Optional use of CC Part2?
    - SFRs not well understood & may improve ST perception
    - But need for clear testable claims

Other possible economies

- CC - Remove functional specification
  - Testing derived from TSS and guidance
- CEM/Scheme - Remove ETR
  - Reduces evaluator effort
  - Reduces scheme overhead
  - Perhaps replace with testing report
  - Lab produces certification report
  - Scheme certifies on the basis of lab ’s quality system & audits
- Target – max 20 days of evaluator effort

Possible additions

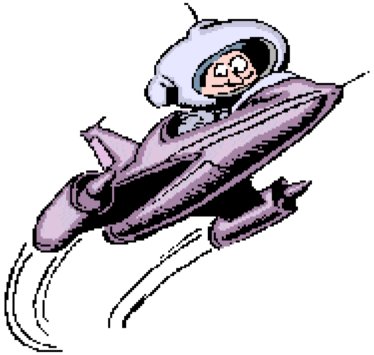
- Architectural summary (mod. ADV_ARC.1)
- Review of developer testing (ATE_FUN.1, ATE_COV.1)
- Independent vulnerability analysis (mod. AVA_VAN.2)
- Advocate flaw remediation (ALC_FLR.1)

- All possible now without CC changes!
- No evidence of demand
  - perhaps because lack of awareness
  - Perhaps concept of augmentation too complex

CC use in service certification

- CC currently has little to offer for service certification
- Covers development, delivery and flaw remediation processes
- Consider where IT products are being used to provide a service
  - E.g. a service to clear and recycle PCs
  - Antivirus outsourcing service
- Components could be provided to cover
  - Searching for weaknesses in operational procedures
  - Checking conformance to operational procedures
  - Reviewing performance of the service with clients
- More than just compliance checking
- Low assurance appropriate where other non-IT factors are important
- Extending CC utility to other areas

Relaunch



- Little evidence that CCv3.1 changes have had any effect
- Some scheme organisations have already gone their own way with new low assurance programmes (E.g. UK CCTM Scheme)
- Need to examine these schemes and draw on ideas
- Modified EAL1 could be relaunched as an economical minimum standard for security products
- Need to target new markets, away from government classified forum
- May require support from different organisations in government (e.g. industry ministries)
- “Results that are valued by end customers”
- “The standard that customers trust” - Samsung
- Security products are now for everyone, and therefore everyone needs the CC

Summary

- Low demand for EAL1 by consumers
- Therefore little used by vendors
- Perception of poor cost/benefit
- No real impact from CC3.1 changes
- May have done enough in CCv3.1 - but too late?
- International recognition gives and advantage over other schemes
- Need for further changes and re-education/relaunch
- Should anyone buy a security product without it?

Thank you

Questions?

EAL1?