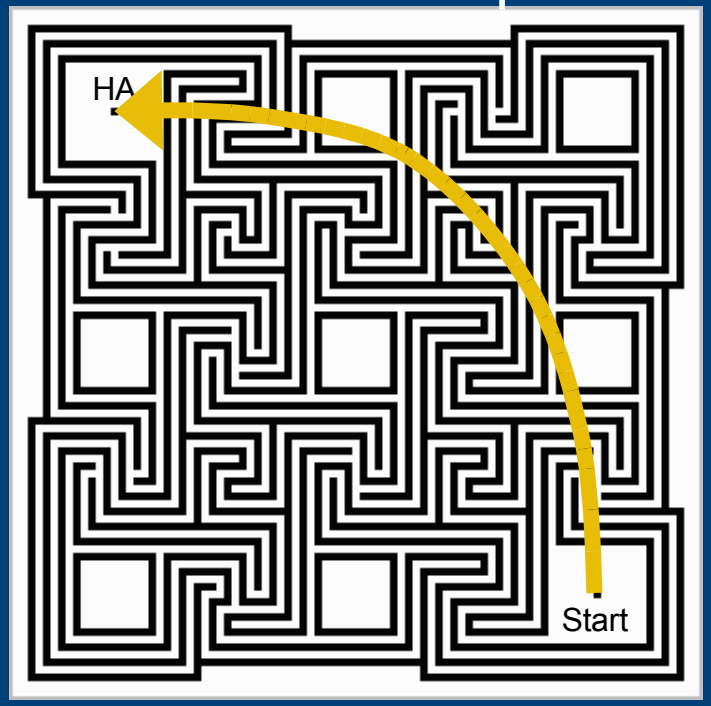
High-Assurance Development and Evaluation: Rethinking the Common Criteria and EAL 7

Presentation to the
2008 International Common Criteria Conference

Rance DeLong and John Rushby
SRI International, Menlo Park CA USA

Is there a better way to high assurance?

Standards-based process



Common Criteria Have Been Successful

- Uniform application - common language, common evaluation criteria, and *Common Evaluation Methodology*
- Established evaluation infrastructure - national schemes and CCTLs (Common Criteria Testing Laboratories)
- International acceptance - the Mutual Recognition Agreement
- Many evaluated products

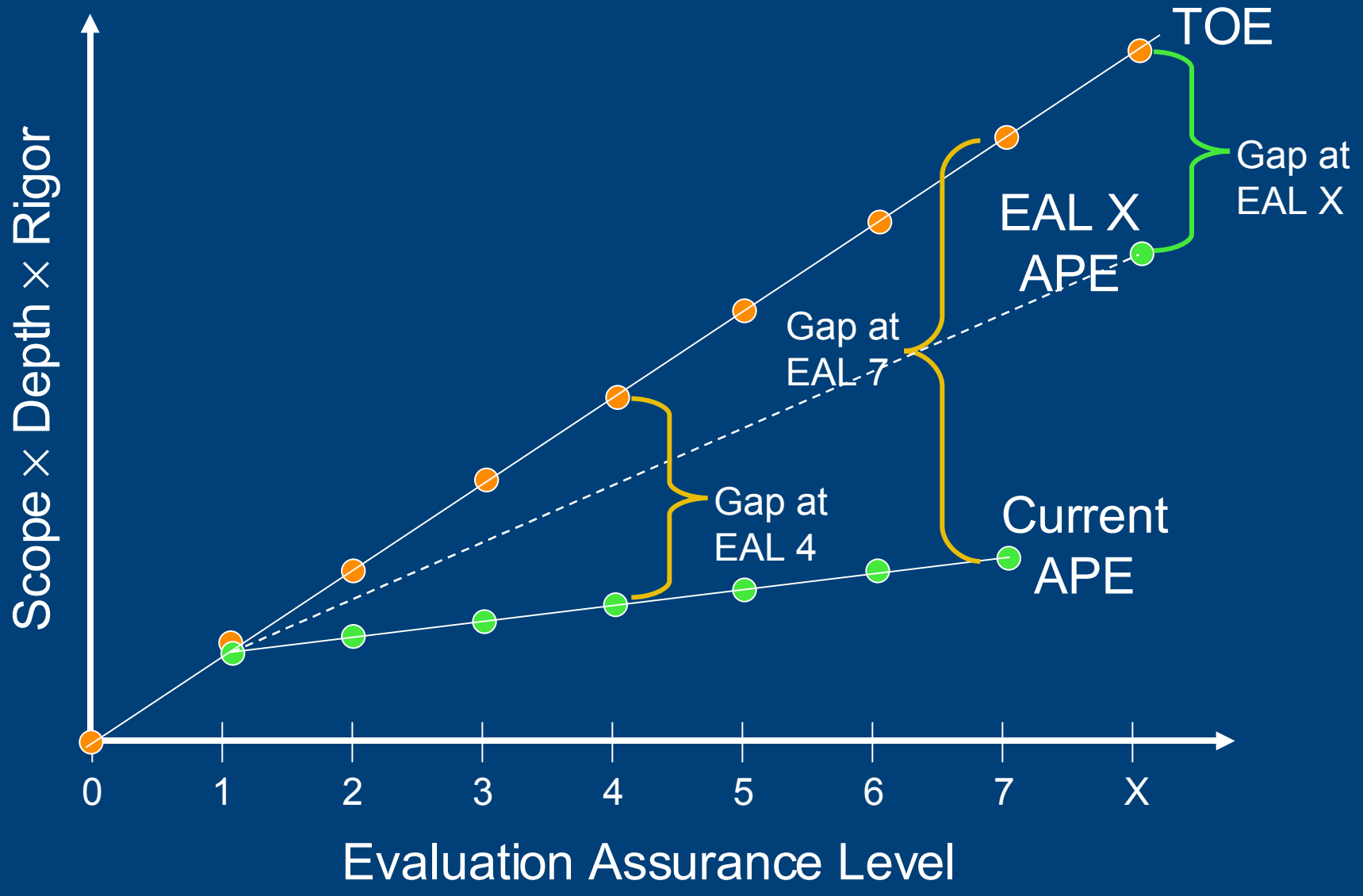
…And Less Than Successful

- Few evaluations above EAL 4
- Very few at EAL 6 or EAL 7
- National systems departing from CC
  - US High Assurance Separation Kernel Protection Profile does not correspond to any EAL
- Some question the whole approach
- Citing excessive cost
- And uncertain benefit

Our Diagnoses

- CC has not kept pace with technology
  - Some automated fully formal analyses have become cheaper than semi-formal
  - Need more flexible choices of scope, depth, rigor
- CC has not kept pace with system development practices
  - Need to support component-based system assembly and evaluation
  - And product evolution, product families
- Rapid increase in scope, depth, rigor for TOE at higher EALs, but not for PP, creates an "abstraction gap" that is expensive to bridge

The “Abstraction Gap” between PP and TOE



Flexible Choices of Scope, Depth, Rigor

- We need a rational way to choose and justify specific choices of scope, depth, rigor
- And the methods and tools to achieve these
- There's not much evidence to support some of the choices
  - e.g., little evidence that formal specification adds much assurance unless supported by formal analysis—but that's a different level
- Need to revisit the basic framework for assurance and evaluation

A Critique of Current Certification Regimes

- Usually standards based - achieve certification by faithfully following standard and generating required evidence
- Processes, evidence are prescribed
- The reason that certain evidence or processes are required may not be evident
  - e.g., Safety Integrity Levels (SIL) - for higher levels, "do more work"
  - Even "the CC philosophy asserts that greater assurance results from the application of greater evaluation effort … the increasing effort is based on … scope …, depth …, and rigor."
- Difficult to innovate to find new and better ways to do things, since the rationale may not be exposed
- Lags modern business practices and commercial realities

Goal-Based Assurance Cases

- All assurance is founded on
  - Stated goals or claims (e.g., about security, safety) that the system is to achieve
  - Evidence about the system and its development
  - An argument, based on the evidence, that the goals are satisified
- In standards-based assurance, like CC, the required evidence is specified, but the goals and argument are generally implicit
  - Hence, hard to choose alternative evidence
- Goal-based assurance cases require explicit goals, evidence, argument
  - More responsibility, more flexibility

A (new) CC-Based High-Assurance Evaluation and Validation Process

- Not prescriptive, only suggestive
- Establish the assurance goals and objectives to be met
- Require applicant to develop and present an explicit assurance case
- Incorporate quantitative techniques and tools to combine evidence and calculate assurance achieved
- Fully support incremental evaluation, compositional evaluation, and other real-world considerations
- For high EALs, formalized protection profiles that:
  - provide formal specification that explicitly represents the bound and free aspects of the TOE description
  - provide an abstract formal policy model to be refined by the developer
  - provide a top-level reference assurance case to be extended by the ST and presented in complete form for final evaluation
  - use parameterization (polymorphism) for product families, EALs
  - are available in “machinable” form for extension to STs and beyond

Impacts on the CC Itself

- Should support explicit assurance case in conjunction with security environment and objectives
- Should comprehensively address component-based design and evaluation
- Should accommodate product families, product evolution, and other business considerations
- CC “meta-process” should become more rigorous at higher assurance levels (reduce PP to TOE gap)
- CC should be a “machinable” artifact to facilitate the use of tools and lessen the need for transcription

Proposed CC Enhancements

- We propose specific enhancements to the CC for high assurance levels
- For the purpose of this presentation we will call the new level incorporating the enhancements EAL X.
- Goals are to achieve the ends desscribed with minimal changes
  - Make explicit the assurance case linking the claims and the evidence to be developed
  - Accommodate component-based systems and product familes and enhancements
  - Close the gap between a PP and a TOE at EAL X
    - By increasing the formality required in the PP

EAL X - Assurance Case

- Assurance Class - AAC - Assurance Case (AC) (patterned after ACM)
  - AAC_AUT - Automated Assurance Case
    - AAC_AUT.1 Partial AC Automation
      - Employ an automated means to support the development, maintenance and presentation of the assurance case, e.g., an assurance case editor (syntactic)
    - AAC_AUT.2 Complete AC Automation
      - **Employ an automated and quantitative method of calculating the assurance afforded each claim, and the root claim, by the combined legs of the assurance case (analytic)**
  - AAC_CAP - Assurance Case Capabilities
    - AAC_CAP.1 informal
    - AAC_CAP.2 formally syntactic - logical connectives
    - AAC_CAP.3 formally analytic - quantitative Bayesian analysis
  - AAC_SCP - Scope of Assurance Case
    - AAC_SCP.1 product
    - AAC_SCP.2 techniques and tools

EAL X - Composition

Assurance Class - ACO - Composition (extends CC 3.1 ACO)

- Support an explicit assurance case
- Support a more flexible composition model

ACO_COR - Composition Rationale

ACO_COR.1 Composition rationale (current)

ACO_COR.1.1D Developer shall provide composition rationale for base component.

ACO_COR.1.1C The composition rationale shall demonstrate that a level of assurance at least as high as that of the dependent component has been obtained for the support functionality of the base component …

ACO_COR.2 Composition rationale (new proposed)

ACO_COR.2.1D Developer shall provide an assurance case-based composition rationale for the composite.

ACO_COR.2.1C The composition rationale shall demonstrate that the level of assurance obtained for the components yields the threshold level of assurance required of the composite.

EAL X - Protection Profile

Assurance Class - APE - Protection Profile evaluation

- Permits single PP to encompass a range of functionality and multiple EALs without breaking the PP evaluation methodology
- Builds more formality into PPs at highest EALs

APE_PPP - Polymorphic (parametric) Protection Profile (new family)

APE_PPP.1 Sub-profiles

APE_PPP.2 Product Configurations

APE_PPP.3 Hierarchical Configurations (Product Families) - hierarchical functional sets and EALs

APE_PFO - Protection Profile Formalization

APE_PFO.1 Formalized abstract security policy model

APE_PFO.2 Formalized abstract model of the TOE

Conclusions

- We suggest that for the CC to better accommodate high assurance it should incorporate explicit assurance cases and enhance the rigor of the CC process itself at higher EALs
- Business and technical concerns motivate compositional evaluation, support for product familes and evolution

Thanks to Carolyn Boettcher of Raytheon and Wilmar Sifre of AFRL

and to sponsorship from USAF Cryptomod and AFRL