

## **Common Criteria V4.0, Basic/Entry Level Assurance, and the Role of Tools in Software Assurance**

Audrey Dale Director US CCEVS

David Martin (CESG UK) CCDB Chair

## Get Ready for a High Speed Tour!



Three subjects in only 30 minutes

- Major changes underway in Common Criteria
- Basic Assurance schemes (e.g. UK's CCTM)
- Assurance through the use of tools



Improving Assurance

# Towards Common Criteria Version 4.0

*Increasing the relevance and  
effectiveness of Common Criteria*



## Please Note



- This talk covers work that is only just underway
- Some of the development work may not lead to the benefits that we expect or may prove impractical to implement
- The work that you will hear about here is very much a 'work in progress'.
- We are briefing early because we want to encourage dialogue and input

# Improving Assurance

## Note Also

- This is aimed at general software products - particularly the larger, complex products
- Smartcards and similar devices continue to be handled well by existing CC (with the JIWG, JHAS, ISCI support)
- U.S. Lost Laptop Protection Profile (PP) being developed using existing CC

## CC V 4.0 Background

- In 2005 the UK and US recognized problems with CC and began research on potential fixes & trialed them on MS Virtual Server
- CC Development Board has been listening to and interacting with users and vendors
- CCDB has also been considering general assurance developments such as increased availability of software tools

# Lessons Learned From Trial

- Highly skilled “subject matter experts” essential
- Can use “real” development artifacts
- Examining vendor’s development and update process can support extension of certification validity
- The process provided better information for the creation of more meaningful reports
- Must develop evaluator support tools

## What Does Industry Want?

- An assurance process that gives them credit for all of their assurance efforts
- An efficient process (both fast and cost effective)
- A process that helps them further improve
- Results that are valued by end customers
- Results that are widely applicable
- Results that are widely recognized



## What Do Users Want?

- *”Confidence that an IT product will operate as intended, throughout its reasonably anticipated life cycle, even in the presence of adversarial activity”*
- Meaningful outputs from evaluations for system accreditors and integrators
- Evaluations that allow for qualitative product comparisons
- Evaluations of real products as they are delivered and used in the marketplace



# CC V 4.0 Working Groups

At the CCDB meeting in April 08 five working groups were created:

- Evidence Based Approach
- Evaluator Skills and Interaction
- Predictive Assurance
- Meaningful Reports
- Tools

# Progress of Working Groups

- Met in London June 08
- Whole day discussion per workgroup
- All agreed that these were difficult problems!
- Brainstormed each issue and identified work items
- Produced outline plans for progressing each task

## Evidence Based Approach

- Led by the US and Sweden
- Considering how to provide a parallel paradigm that acknowledges and provides credit for alternative techniques and methods to provide assurance
- Any documentation produced during the development process may be considered
- Increased evaluator and developer interaction
- Will take into account the vendor's use of tools



# Predictive Assurance

- Led by Germany
- Analysis of the vendor's product development process
- Together with a greater understanding of the product's roadmap (e.g. key future changes),
- Will consider vendor's flaw remediation process
- Longer validity for the certification report.

# Improving Assurance

## Meaningful Reports

- Led by Canada
- Making reports (and other evaluation information) more meaningful
- Providing the end users with the information that they need to make assurance decisions
- Help with overall system security architecture
- Effective use of product security mechanisms
- Residual risks, and strengths/weaknesses of the product and development process



# Evaluator Skills and Interaction

- Led by the UK and US
- Underpins the other work items
- Considering how to provide increased commonality in evaluator
  - Training,
  - Assessment, and
  - Interaction (within and between schemes)

## Tools

- Led by UK and Spain
- Original aim - to define tools that will support all of the working methods described in the other work areas.
- Redirected to define workflows (allowing development of tools) AND
- To encourage use of tools by vendors.

# Improving Assurance General CC V 4.0 Development Process

- To minimize resource loading on schemes as much as possible, much of work will be pursued electronically
- Wikis used during the start up meetings & will be used for further development
- Similar approach likely for external interaction
- Each workgroup will set up appropriate timing and collaboration methods





# Improving Assurance Example

The screenshot shows a web browser window with the address bar displaying <http://www.commoncriteriaportal.org/twiki/bin/view/Main/WebHome>. The browser's history and bookmarks bars are visible. The main content area of the browser shows a Twiki page with the following structure:

- Main** (breadcrumb)
- Log In or Register** (link)
- Main Web** (header)
  - Create New Topic
  - Index
  - Search
  - Changes
  - Notifications
  - Statistics
  - Preferences
- Twiki Tip of the Day**
  - Raw Text link**: At the bottom of the page next to Edit and Attach, there is a Raw Text link that allows one to ... [Read on](#)
- Webs**
  - Main
  - Sandbox
  - Twiki
- Twiki > Main Web > WebHome** (15 Sep 2008, DavidMartin) [Edit/Attach](#)
- ## Welcome to the CCV4 Working Group Wiki
- This is a site that will facilitate discussions for each of the 5 working groups. To register go to the registration link below. To use the working group pages go to:-

  - [EvidenceBased](#)
  - [SkillsandInteraction](#)
  - [PredictiveAssurance](#)
  - [DetailedReports](#)
  - [ToolSupport](#)
- The original calling notice is at [CallingNotice](#), a background summary of aims is at [AimsSummary](#) and a brief information note for the CCPortal is at [StatusNote](#)
- ### Development site for public Wiki
- Each of the working groups intends to engage with industry (vendors and labs etc.) at the appropriate time. The pages below are intended to provide a location where the working groups can agree on the initial content of these. The lead nations should transfer across the elements that they consider appropriate.

  - [EvidenceBasedPublic](#)
  - [SkillsandInteractionPublic](#)
  - [PredictiveAssurancePublic](#)
  - [DetailedReportsPublic](#)
  - [ToolSupportPublic?](#)
- The first day's brainstorming identified a need to add more detail to the status note to explain why we are doing the work and how the items fit together to suitably improve assurance. The updated note is provided here - [http://www.commoncriteriaportal.org/twiki/pub/Main/WebHome/CC\\_Changes\\_Overview\\_v1.0.pdf](http://www.commoncriteriaportal.org/twiki/pub/Main/WebHome/CC_Changes_Overview_v1.0.pdf)
- ### Main Web Utilities

At the bottom of the browser window, a status bar shows the following information: UK: Mon 15:37, US Pacific: Mon 07:37, GMT/UTC: Mon 14:37, Korea, South: Mon 23:37, Washington, DC: Mon 10:37, <http://www.commoncriteriaportal.org/twiki/bin/view/Main/PredictiveAssurance>



## Eventual Aim

Once the development work is complete and the improvements have been adopted by a suitable combination of agreement between schemes and changes to the criteria/CEM etc., then evaluations will have the following characteristics:

# Improving Assurance

## Eventual Aim

- Evaluations will be performed by the optimum combination of subject matter experts and assurance experts.
- Readily accessible body of knowledge ('case law') will exist to draw upon.
- Supporting interactions with other evaluators both nationally and internationally (with suitable protection for developer's IP)
- Common assessment levels for evaluator skills.

# Improving Assurance

## Eventual Aim

- Evaluators will examine evidence produced as a normal part of the development of a product
- Examine the development process including the use of tools.
- Clear focus on the flaw remediation process and the strategic future product development plans
- Supporting the provision of 'predictive assurance'

# Improving Assurance

## Eventual Aim

- Certificates used for international mutual recognition, BUT -
  - The most important outputs from the evaluation process will be in the form of detailed reports aimed at a range of audiences:- e.g. system accreditors/risk owners, system developers, system users, subsequent evaluation teams, etc.
- Reports will use language and concepts best suited to each of their needs.



# Improving Assurance

## Brief Question Break



# Low Assurance Scheme (UK)

- “CESG Claims Tested Mark” (CCTM) Scheme
- Operated by CESG
- Addresses Security Products & Services
- Provided at reasonable evaluation cost
- Evaluation performed by appointed Test Laboratories (ISO 17025 accredited)
- Checks conformity to “Security Target” claims
- Checks ease of use, public vulnerabilities
- Results in award of CCT Mark Certificate

# CESG Claims Tested Mark

- Strong take up from vendors
- 36 products assessed (including services)
- 7 Test Laboratories
- UK only in scope
- Use encouraged (with FIPS) at lower impact levels

# CESG Claims Tested Mark

- Inputs: IA Claims Document (ICD) & user guidance
- ICD specifies security claims & test approach
- Test Lab performs basic checks on ICD
- Test Lab (generic or specialist) evaluates security claims
- Based on light methodology (CEM test philosophy)
- Test Lab uses any existing CC/ITSEC processes
- Testing/reporting limited to about 20 days maximum
- Results detailed in Test Report (TR)
- CESG Decision Authority validates ICD & TR
- UKAS audits evaluator skills & competencies
- CESG publishes ICD & Test Report Summary
- CESG approves Marketing Statement

## Low Assurance Scheme (FR)

- “First Level Security Certification” Scheme
- Operated by DCSSI
- Addresses Security Products
- Offers certification of open source software
- Provided at reasonable evaluation cost
- Evaluation performed by Licensed Eval Facilities (not ISO 17025 accredited)
- Checks product conformity to Security Target
- Checks product efficiency/effectiveness

# First Level Security Certification

- Inputs: Security Target & user guidance
- Evaluates I&A, access controls, A-V, etc
- Based on light criteria and methodology
- Uses existing CC/ITSEC processes selectively
- Based on fixed schedule and workload
- Results detailed in ETR
- DCSSI validates Security Target & ETR
- DCSSI audits evaluator skills & competencies
- DCSSI publishes ST & sec recommendations

## Who else has seen this need?

- Germany – an accelerated EAL 1 like process
- Australia – considering similar requirements
- Korea (one of the newest schemes) – has developed a higher speed assessment outside of CC
- Other schemes are likely to follow

# Low Assurance CC Certificates

- 847 EAL1-EAL7 CCRA certificates (20/08/08)
- Few EAL1 certificates
  - 30 at EAL1 and 19 at EAL1 augmented
- Many more EAL2 certificates
  - 158 at EAL2 and 63 at EAL2 augmented
- But EAL3 less popular
  - 101 at EAL3 and 74 at EAL3 augmented

# EAL1/EAL2 Evaluation Issues

- Costly compared to industry specific assurance schemes
- Preparation & evaluation can be time consuming
- Security Target (ST) is significant extra document
  - SFRs are not well understood by developer or customers
  - Requires CC experts/consultants to produce
- CCRA documents are large part of overall costs/time
  - ST, ETR & Certification Report
- Emphasis on documentation rather than product security testing
- Bottom line – too costly & slow; not enough value for money

## Another CC V 4.0 Workgroup

- New Workgroup created to study the needs of basic/entry level assurance
- Considering a more 'directed testing' based approach
- Also to take account of vendor tool usage
- Will interact with the other 'Version 4' workgroups
- Would result in Mutual Recognition – very important for vendors



## CCRA Wide PPs

- CCDB considers PP compliance to be increasingly important
- Producing a register of technology areas requiring PPs
- PP authors will then take into account community requirements
- Feasibility of PP supporting evaluation methodology elements to be considered



# Improving Assurance

## Brief Question Break



# Role of Development Tools

- Evaluation schemes are still seeing simple coding errors (unsafe library calls, buffer/variable overflow, etc.)
- Variety of tools available to developers (see NIST lists, OWASP, etc)
- Tools vary in efficacy (see comparisons such as NIST SAMATE, SCANSTUD, etc) – BUT better to have them than not!

## Not Just Analysis Tools

- Build tools/OS/HW can provide:
  - Address Space Randomisation (although limited use in 32 bit architectures)
  - Data Execution Prevention
  - Stack/Heap canary protections

## Role of Development Tools

- CCDB keen to encourage usage
- Already have a proposal from Spain for incorporation into CC
- Version 4 Tools workgroup taking this further
- Would like to see tools (together with the necessary supporting process elements) used in all levels
- Will ensure that these are taken into account during evaluation



# Improving Assurance

## Questions

