

# *Has the Common Criteria Delivered?*

*Anthony Apted/  
James Arnold*

**26 September 2007**

- Back to Basics – Why Evaluate?
- Evaluation Scheme Goals
  - US Scheme Evolution – a Case Study
  - A Sample of other Schemes
- Evaluation Criteria Goals
  - Historical Perspective and Previous Approaches
  - Common Criteria and Mutual Recognition
- CC Metrics
  - Does achievement equate to success?
- New Approaches
- Conclusions and Recommendations

# Why Evaluate?

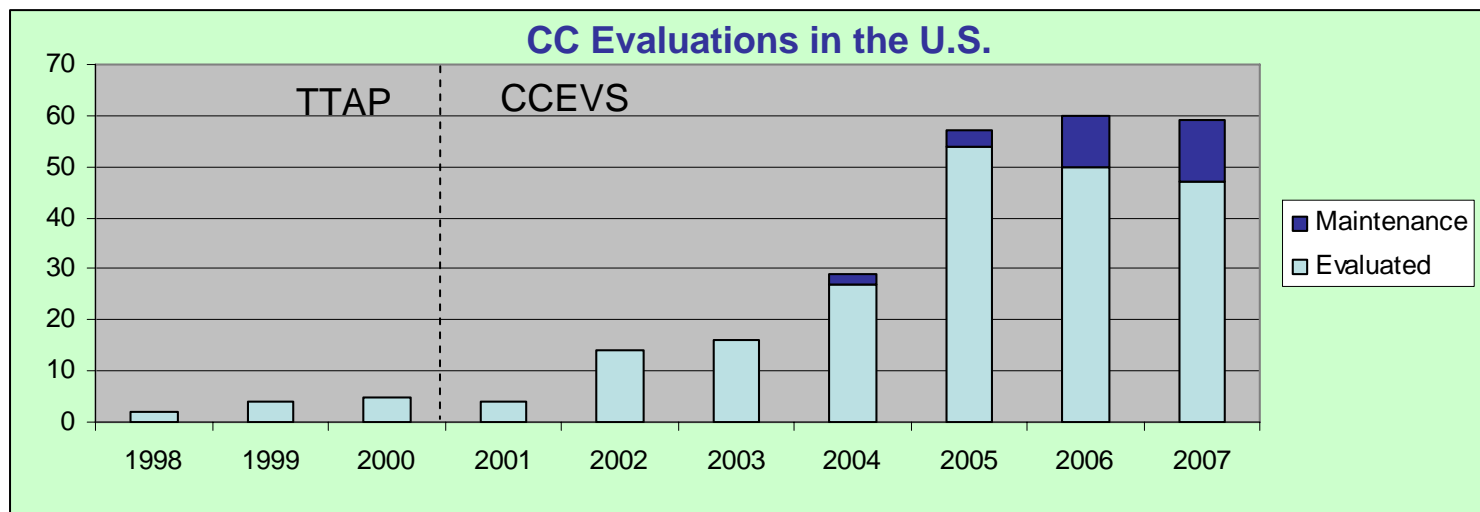
- Establish appropriate level of assurance (“trust”) in COTS products
  - The product provides claimed/required capabilities (security functionality)
  - The product is not vulnerable to attack (relative to level of assurance)
  
- Why Commercial Evaluation?
  - Governments unable to adequately resource evaluation capability

- Trusted Product Evaluation Program (TPEP, 1983-1998)
  - Established to perform evaluations against Trusted Computer System Evaluation Criteria (TCSEC, aka “Orange Book”)
  - Operated by NSA, using government resources
  - Over 100 products evaluated
  - TCSEC, TNI, TDI
    - Operating systems
    - Network components
    - Database systems
    - Subsystems

- Trusted Technology Assessment Program (TTAP, 1997-2000)
  - First foray into commercial evaluation process
  - 14 products evaluated
  - TCSEC, CC, TDI
    - Firewalls
    - Database systems
    - Operating system
    - Hardware switch

- Common Criteria Evaluation & Validation Scheme (CCEVS, 2001- )
  - Objectives
    - To meet the needs of government and industry for cost-effective evaluation of IT products
    - To encourage the formation of commercial security testing laboratories and the development of a private sector security testing industry
    - To ensure that security evaluations of IT products are performed to consistent standards
    - To improve the availability of evaluated IT products.

- CCEVS (2001-current)
  - CC & numerous validated protection profiles
    - 212 products currently evaluated in CCEVS with 29 maintenance updates and 10 retired/archived evaluations
    - 43 PPs currently validated and 8 retired/archived PPs
    - 118 products *in evaluation*



- UK IT Security Evaluation and Certification Scheme
  - Established 1989
  - Objectives:
    - Evaluate and certify trustworthiness of security features in IT products and systems
    - Provide framework for international mutual recognition of such certificates
  - Commercial evaluation scheme since inception
  - ITSEC, CC
  - Over 100 products evaluated

- Australasian Information Security Evaluation Program (AISEP)
  - Established 1994
  - Objectives:
    - Ensure the ready availability of a comprehensive list of independently assured IT products that meets the needs of Australian and New Zealand government agencies in securing their official resources
  - Commercial evaluation scheme
  - ITSEC, CC

- TCSEC
  - provide users with a yardstick with which to assess the degree of trust that can be placed in computer systems for the secure processing of classified or other sensitive information
  - provide guidance to manufacturers as to what to build into their new, widely-available trusted commercial products in order to satisfy trust requirements for sensitive applications
  - provide a basis for specifying security requirements in acquisition specifications.
- ITSEC (Harmonised criteria of France, Germany, Netherlands, UK)
- Canadian Criteria
- Federal Criteria

- CC Objectives
  - Permit comparability between results of evaluations
  - Establish a level of confidence that the product meets the claimed requirements
  - Provide a useful guide for development, evaluation and/or procurement
  - Address confidentiality, integrity, and availability
- As presented in Part 1 of the CCv2.1 and CCv2.3 the overall objectives remain essentially unchanged.

*Ref: CCv2.X Part 1 Scope, CCv3.1 Part 1 Introduction*

- Common Criteria Recognition Arrangement
  - Objectives
    - to ensure that evaluations of Information Technology (IT) products and protection profiles are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and profiles;
    - to improve the availability of evaluated, security-enhanced IT products and protection profiles;
    - to eliminate the burden of duplicating evaluations of IT products and protection profiles;
    - to continuously improve the efficiency and cost-effectiveness of the evaluation and certification/validation process for IT products and protection profiles.

## Common Criteria Recognition Arrangement Participants

### ▪ Certificate *Authorizing* Members

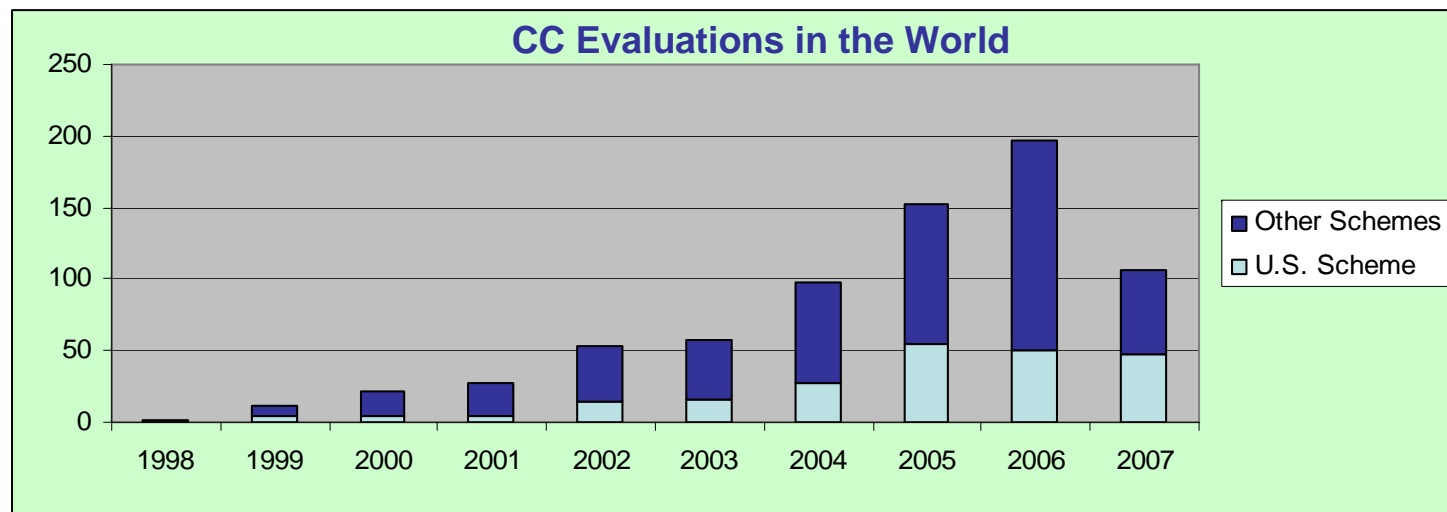
- Australia and New Zealand
- Canada
- France
- Germany
- Japan
- Republic of Korea
- Netherlands
- Norway
- Spain
- United Kingdom
- United States

### ▪ Certificate *Consuming* Members

- Austria
- Czech Republic
- Denmark
- Finland
- Greece
- Hungary
- India
- Israel
- Italy
- Sweden
- Turkey

- Primary objective of evaluation schemes essentially the same
  - Ensure availability of evaluated IT products
- National schemes may have specific national objectives
  - Support national government agencies
  - Support national industry
- How well does the CC meet these objectives?
  - Availability of evaluated IT products increased by Mutual Recognition between schemes
  - CC and CEM support consistent and comparable evaluations

- Raw numbers indicate CC is a success
  - Increasing numbers of evaluated products and PPs
  - Growth in number of CCRA participants
  - Growth in numbers of EAL4 evaluations
  - Evaluations outstripping validation resources in some schemes



- However, usual complaints are still made:
  - Evaluations take too long
  - Evaluations cost too much
  - Evaluation results are not meaningful because evaluated configuration is unrealistic
- Are these CC issues or scheme issues?
  - Do all CC assurance requirements deliver value?
  - Do scheme requirements impose unnecessary overhead?
  - Have product developers and consumers been properly educated?

- Appears to have “missed the boat”
- No significant changes to Part 2 (so previous problems remain)
- Part 3 changes have not improved value of many requirements

- Apparently “in the works”
- “Issues for CC v4.0” is being presented at 8<sup>th</sup> ICCC

- Common Assurance Assessment (CAA)
  - CC Issues
    - By many measures, CC is a big success, but...
      - Product consumers and vendors see significant issues
    - Product consumers want more relevant results
      - Not seen as predicting real-world assurance in operation
      - Difficult specialist vocabulary
    - Doesn't reflect current commercial development practice
      - Focus on design-level issues and waterfall development model
      - Focus on security features, not assurance technology
      - Tied to static product definition
  - Goals
    - Assess assurance in operation  
“Confidence that an IT product will operate as intended, throughout its reasonably anticipated life cycle, even in the presence of adversarial activity”
    - Provide meaningful assurance information to certifiers, accreditors, ISSEs, and system architects/designers
    - Evaluate real products as they are delivered and used in the marketplace
    - Evaluate in a predictable and cost-effective manner
    - Enable qualitative product assurance comparisons
    - Provide a framework equivalent to current Common Criteria activities

## Conclusions and Recommendations

- The CC and CEM are tools to assist evaluation schemes achieve their objectives
- If those objectives are not being adequately met, is it because:
  - The objectives are not clearly defined and articulated?
  - The tools are not being used correctly?
  - The tools are not the correct tools to use?

## Contact



Anthony Apted

SAIC Accredited Testing & Evaluation Labs  
Senior Evaluator

[Anthony.J.Apted@saic.com](mailto:Anthony.J.Apted@saic.com)

James Arnold

SAIC Accredited Testing & Evaluation Labs  
AVP/Technical Director

[James.L.Arnold.Jr@saic.com](mailto:James.L.Arnold.Jr@saic.com)

<http://www.saic.com/infosec/cctl.html>