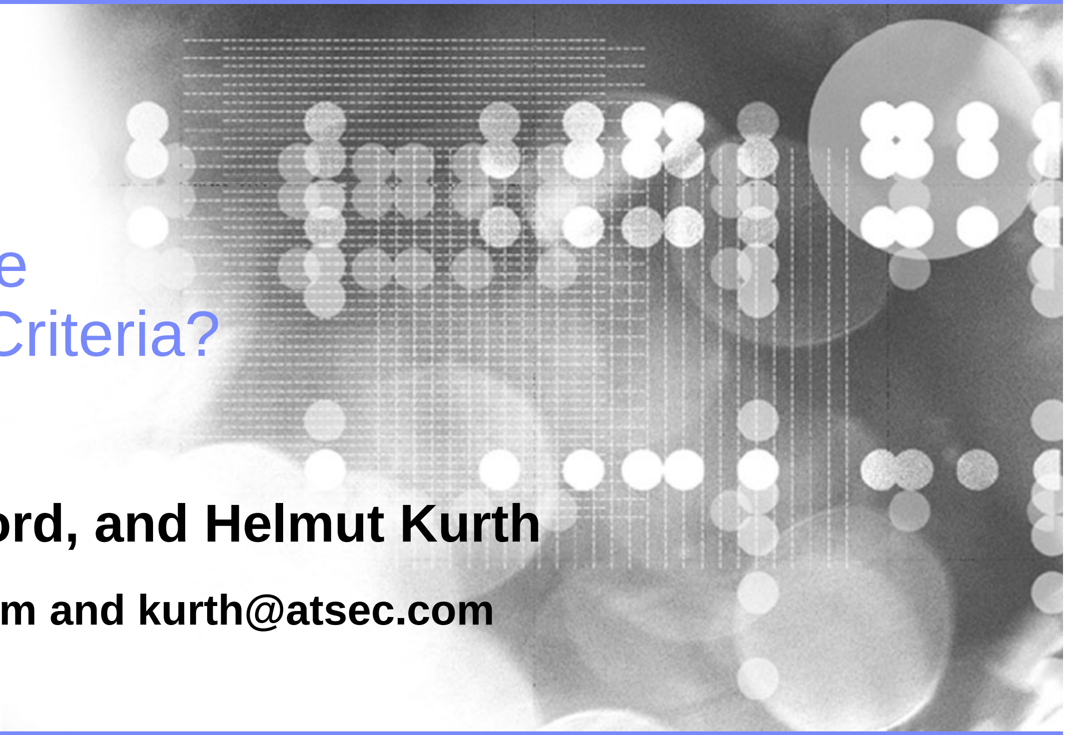
Thomas J. Watson Research Center



Sed Quis Custodiet Ipsos Custodes (Who Watches the Watchers) of the Common Criteria?

Paul A. Karger, David Safford, and Helmut Kurth

(karger | safford)@watson.ibm.com and kurth@atsec.com

10 December 2009

Disclaimer

- **Talk describes incidents related to CC evaluations**
  - No names of actual products, evaluation agencies shown
  - Products from multiple companies
  - Evaluations by multiple evaluators
  - Certificates in multiple countries

Outline

- **Why do we do security evaluations?**
- **History of Security Evaluation Criteria**
- **Evaluation Process**
- **Problem areas**
  - Composite Evaluation Problems
  - Failures of the Evaluation Process
- **Recommendations**
- **Conclusions – Major Need for Reform**

Why do we do Security Evaluations

- **Objective means of comparing the quality of security offered by different products**
- **Independent third party evaluations to ensure technical accuracy**
- **Range of levels to encourage manufacturers to compete on the basis of security and to gradually improve their products**
- **This paper strongly supports independent third party security evaluation**
- **Purpose is to show how the Common Criteria needs some improvement to meet these goals**

History of Security Evaluation Criteria

Nibaldi proposal	1979
TCSEC V1	1983
TCSEC V2	1985
Germany, UK, and France	1989
ITSEC (EU criteria)	1991
Japan, US Federal Criteria, and Russia	1992
Canada	1993
Common Criteria V1.0	1996
Common Criteria V2.0	1998
Common Criteria ISO Version	1999
Common Criteria V3.0R2	2005
Common Criteria V3.1R3	2009

Evaluation Process under Common Criteria

- **Sponsor of evaluation selects a commercial evaluation lab**
- **Evaluation lab goes over product documentation and implementation**
- **Issues evaluation report**
- **Certifying body is supposed to validate/confirm that**
  - the evaluation has been conducted in accordance with the provisions in effect
  - the conclusions are consistent with the evidence presented
  - the conclusions are documented in the evaluation report
  - and then issues a certificate

Problem Areas

Composite Evaluation Problems

- **Composite evaluation is process for evaluating an upper level product that runs on a lower-level evaluated product without having to re-do the lower level evaluation**
  - –operating system on evaluated CPU
  - –trusted database on evaluated operating system
- **Problem Areas**
  - –Mismatched Security Assumptions
  - –Missing Lower Level Evaluations
  - –Insufficient Information in “Lite” Evaluation Reports

Mismatched Security Assumptions

- **Upper level product assumes features not present in the lower level product**
- **Smart card example**
  - Many smart card chips evaluated with assumption that all software is loaded before the card is issued (now being fixed with new protection profile)
  - JavaCard software evaluated with feature that allows download of software after card has been issued
  - Certifying bodies missed that the intended use cases were not addressed by the evaluation, rendering the evaluation meaningless.
  - Only one evaluated JavaCard product properly points out the hardware assumption and warns that downloading software will invalidate the CC certificate

Missing Lower Level Evaluations

- **Many product evaluations assume that lower level products that perform critical security functions have been evaluated, but they haven’t been**
- **Many examples of products written in Java assume that the JVM provides critical security functions**
- **No full JVM has ever been Common Criteria evaluated**
  - Java Card JVMs have been evaluated, but they are much smaller and simpler
- **Implication: One needs to re-examine the assumptions being made by Java based products about the evaluations of the JVMs upon which they depend**

Insufficient Information in “Lite” Evaluation Reports

- **Lower level evaluation reports are censored and not made available to higher level developers or evaluators**
- **Can lead to many serious security problems**
  - Documented in: **Karger, P.A. and H. Kurth. *Increased Information Flow Needs for High-Assurance Composite Evaluations*. in** Second IEEE International Information Assurance Workshop**. 8-9 April 2004, p. 129-140.**
- **Common Criteria V3.0 begins to address this problem with new composite evaluation approach**
- **European Certifying Bodies have rejected V3.0 approach and assert with NO technical support that censored reports are sufficient, despite ample published evidence to the contrary**

Failures of the Evaluation Process

- **Evaluator Does Insufficient Vulnerability Analysis**
- **Evaluator evaluates own work**
- **Evaluator waives basic Common Criteria Requirements**
- **Certifier Overrides Evaluator Results without Explanation**

Evaluator Does Insufficient Vulnerability Analysis

- **In one composite evaluation, the lower-level product evaluator missed a very serious and quite obvious vulnerability**
- **Vulnerability was concealed by the lack of details in the "Lite" evaluation report**
- **After the certificate had been issued, the serious vulnerability was discovered in the lower-level product**
- **Only then did it come to light that the evaluator's vulnerability analysis had been very incomplete – the class of vulnerability was well known in text books.**

Evaluator Evaluates own Work

- **Evaluation labs often assist the product developer in writing the Security Target, as that document essentially lays out the security strategy for the evaluation**
- **However, some evaluation labs have been writing other documents for the product developers, then putting the product developers' names on the documents, and then evaluating the quality of their own development documents**
- **This violates the assumption that the evaluator is an independent third party**
- **Proper approach is if the product developer needs help on other critical security documents, they should hire contractors that are NOT affiliated with the evaluation lab.**

Evaluator waives basic Common Criteria Requirements

- **Product developer identified serious problem in configuration control and verified that it had caused mysterious system crashes**
- **Developer disclosed the problem to the evaluator to ask advice on how to resolve the problem without disrupting the evaluation schedule**
- **Evaluator said to simply ignore the problem, despite the fact that it violated Common Criteria requirements and that it was causing real software problems**
- **Fortunately, developer chose to fix the problems, and ignored the evaluator’s bad advice!**

Certifier Overrides Evaluator Results without Explanation

- **In one instance, a certifying body overruled the EAL recommendation in an evaluator's report**
- **Usually, the certifier and evaluator would resolve this prior to publication of any results**
  - **But not in this case**
- **Lack of a public document explaining the disagreement is unfair to the developer as well as consumers of the products and competitors of the developer**

Recommendations

- **"Who watches the watchers?"**
  - –How do we prevent/detect these evaluation failures?
- **Biggest Recommendation: Open Up the Evaluation Reports**
  - –Scientific method requires repeatability of experimental results – not possible with closed evaluation reports
  - –Open evaluation reports helped improve Linux
  - –Published evaluation reports on Windows have some of the best Windows internals documentation, even though closed-source
  - –Care must be taken if there are unresolved security vulnerabilities
- **Make explicit rules about who can write documents**
- **Strengthen oversight of evaluations and certifications**

Conclusions

- **Reform of the Common Criteria Process is Needed**
- **Current requirements CAN and DO produce good evaluations with real value to customers**
  - Dropping requirements (as some have proposed) is NOT the solution
- **Real danger of the Common Criteria becoming an Imperial Fashion Statement**
  - Anderson, H.C., *Keiserens nye Klæder*, in *Eventyr, fortalte for Børn. Tredie Hefte*. 1837, C.A. Reitzel Publishers: Copenhagen, Denmark. p. 107-111.

Imperial Fashion Statement

Pedersen, V., *Keiserens nye Klæder*, in *Gesammelte Märchen. Mit 112 Illustrationen nach Originalzeichnungen von V. Pedersen. Im Holz geschnitten von Ed. Kretzschmar.* 1849, Carl B. Lorck: Leipzig, Saxony.

Possible Discussion Topics

- **What is the difference between openness and reproducible results?**
- **How can we better make reports open, even when the product is closed-source?**
- **Orange Book reports tended to be much more open than Common Criteria reports. Why?**