Addressing consumer needs to increase the demand for Common Criteria-evaluated products

7th ICCC 2006, Lanzarote/Spain

David Ochel
atsec information security

Objectives

- Analyze some persistent problems with the CC cited by consumers.
- Realize that these problems can be addressed by embracing common risk management methodologies.
- Enhance consumer awareness by updating/creating appropriate guidance.

Agenda

- What are the consumer's needs?
- How does the CC help the consumer?
- How does it not help?
- Common obstacles…
- …and how (and why) these obstacles can be addressed by non-CC means.
- Proposed actions

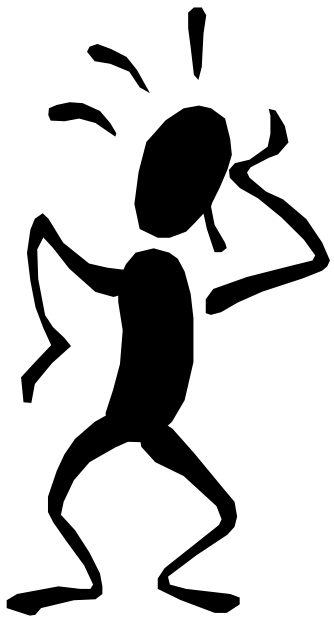
What are the consumer's needs?

- Protect assets!
- How? Manage risks:
  - Estimate asset value
  - Identify threats
  - Assess risks
  - Implement countermeasures
  - Qualify countermeasures
  - Re-assess
  - …
- CC-evaluated products offer countermeasures (i.e., security functionality) for sale

How does the CC help?

- Provides assurance into security functionality of commercial off-the-shelf (COTS) products
  - minimizes risk of vulnerabilities, malfunctions, bypassability,
  - provides trust into quality of commercially obtained countermeasures
  - by independent review of architecture, code, development environment, …

How does the CC **not** help?



- Does not take the consumer's individual context into account.
  - security problem definition and TOE boundaries are static, i.e., inflexible
  - not used for system certification

Consumer obstacle: No patch management allowed

- Applying (security) patches to TOE invalidates evaluated configuration.
  - Assurance maintenance approaches so far have widely failed:
    - No detailed CCRA agreement
    - Lack of Scheme guidance
    - Lack of vendor persistence
  - Flaw remediation doesn't help here.

Consumer obstacle: Cannot use non-evaluated functions

- Evaluated configurations prohibit use of non-evaluated functionality or interfaces.
  - e.g., device drivers, SUID programs, plugins for replacing TSFs, …

The doctrine

- "If you violate the evaluated configuration, the certificate is not valid anymore!" (…which must be avoided)

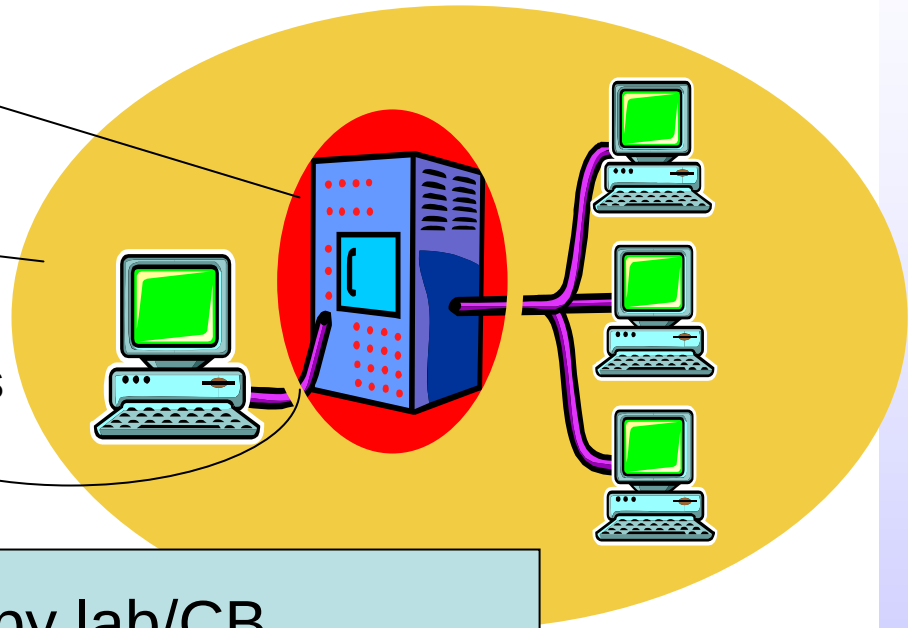
- But a CC certificate is not a certificate of insurance!
  - The certificate itself has little value.
  - The analysis performed to achieve certification has value!

It’s all about risk management!

Scope of lab CC analysis

Consumer’s Information Security Management domain

Assessment of boundaries and integration is consumer’s responsibility!



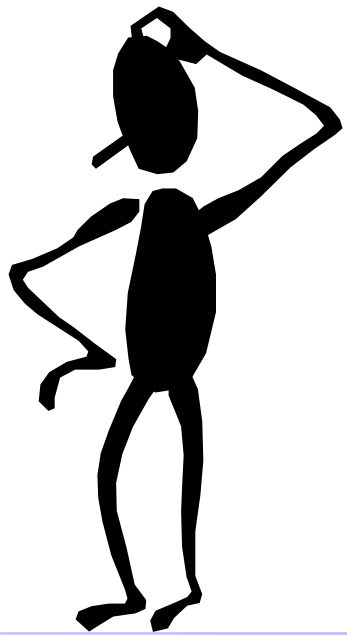
Analysis performed by lab/CB

\+ Gap/integration analysis performed by consumer

= Input for consumer’s risk management

What to do?

- De-mystify the use of evaluated products in non-evaluated configurations!
  - Explain the limitations of the CC to consumers.
  - Enable consumers to deal with the limitations by providing reassurance and guidance.
  - Define clear boundaries of evaluated products that allow consumers to begin their analysis where the CC-provided analysis ends.



Example 1

- Evaluated configurations are restricted to a specific patch level. Why?
  - There is no way for the lab to ensure (and for the CB to certify) that code that has been updated does not introduce malfunctions/vulnerabilities into the evaluated functions.
- Does that mean I cannot apply a security patch?
  - Assess the risk:
    - Likelihood that the vulnerability addressed by the patch will be exploited in your environment … and the potential damage to your assets that would result.
    - Likelihood that the evaluated security functionality will be compromised by the patch … and the potential damage to your assets that would result.
- Answer: It depends!

Example 2

- The evaluated configuration of my operating system does not allow the installation of a device driver for my storage device. Why?
  - Privileged code might compromise the evaluated security functionality. Evaluation cannot realistically include all third party device drivers on the market.
- Does that mean I cannot install the device driver?
  - Assess the risk:
    - Likelihood that device driver contains malfunctions/vulnerabilities or undermines the evaluated TSF.
    - Potential damage to your assets vs. benefit of using the specific storage device.
- Answer: It depends!

Example 3

- The evaluated configuration excludes certain product (security) functionality. Why?
  - Several possible reasons: Might have been excluded to reduce evaluation effort. Might contain a vulnerability/architectural flaw.
- Does that mean I must not use this option?
  - Assess the risk:
    - Likelihood that the non-evaluated code contains potential, unknown security flaws.
    - Likelihood that the code was excluded because it contains a bug known to the developer or contributes to an insecure product configuration.
    - Potential damage to assets vs. benefit of using the functionality.
- Answer: It depends!
  - It would really help the consumer to know the developer's motivation for excluding the functionality!

The CC's intention (David's interpretation ;-)

- The evaluated configuration is not carved in stone, but merely represents the configuration in which the product was evaluated.
  - Evaluations perform independent analysis that a consumer cannot practically perform, focusing on typical configurations.
    - The consumer typically has neither access to necessary information (design, code) of COTS products, nor necessary security expertise and/or manpower.
  - Consumer can use results of CC analysis as input for consumer's existing (hopefully!) ISMS.
    - The consumer needs to know that deviations from the evaluated configuration are OK and expected. The consumer should understand the evaluation results, and then perform additional analysis based on the proposed use of the product in his own environment, including analyzing associated risks. If those risks are acceptable, the consumer can use the product with confidence.

Conclusion

- Policy should **not** be:
  - Use certified products in their evaluated configurations to assemble infrastructure.
- Policy should be:
  - Use certified products to gain assurance into commercially provided security functionality; manage risk of product integration into proprietary infrastructure.

But can we do that? We need to acknowledge that…

- The value of product certification is relative, not absolute!
  - "Commercial EALs" usually assume non-malicious developer.
  - 80% of functionality evaluated is better than 0% and still provides for an assessment of the product's development life-cycle.
- Certification cannot replace risk management:
  - Risk involved with employing a specific product's security functions is reduced, not eliminated.
  - Organizational assumptions made during an evaluation are relative. Besides technical aspects, an organization's "people factor" needs to be taken into account: Product certification cannot counter social engineering, misuse of privileges, etc.
  - Certification should be one input among many to the consumer's overall risk mitigation.

What's next?

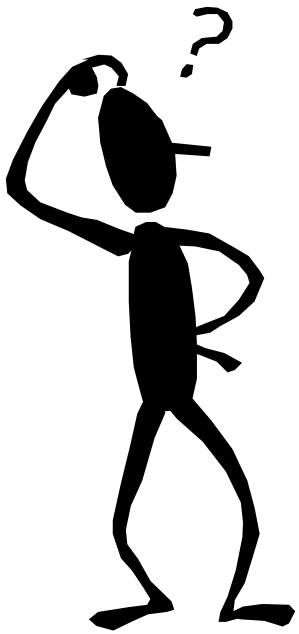
- If the CC community endorses the presented views:
  - CC User Guide (October 1999, commoncriteriaportal.org) could be updated to address the perceived obstacles.
  - A separate guide on integrating certified products could be offered to consumers.
  - CC evaluation as a valuable tool for consumers' information security management could be promoted.
  - Developers could be advised to provide more integration guidance (cf. composite evaluation schemes).

Other consumer-cited issues…

…that we are not addressing today:

- price and timeliness of evaluations
- adequacy of the CC assurance requirements
- lack of vendor/consumer communication about desired product functionality
- …

Questions?



david@atsec.com