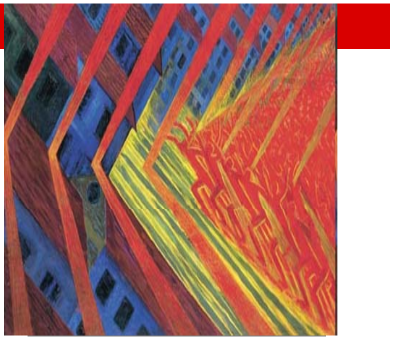
the information security provider

Security Evaluations: Who Watches the Watchers?

Helmut Kurth, atsec information security corp.

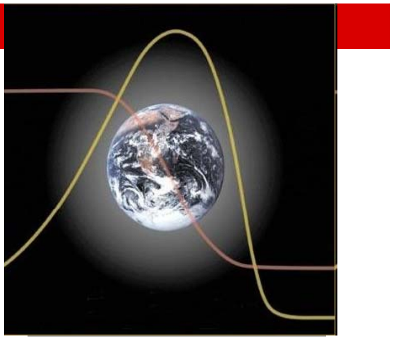
atsec Evaluation Background

- **CC Evaluation Labs accredited in three countries**
  - US, Germany, Sweden
- **Mainly high-profile Evaluations**
  - z/OS, z/VM, DB2 (for z), Oracle Database, Linux (Red Hat, Novell SUSE and Oracle), Microsoft Hyper-V, ….
  - More than 70 successful evaluations
- **Some employees with more than 20 years of evaluation experience**
- **Attempted to improve the criteria**
  - With some limited success



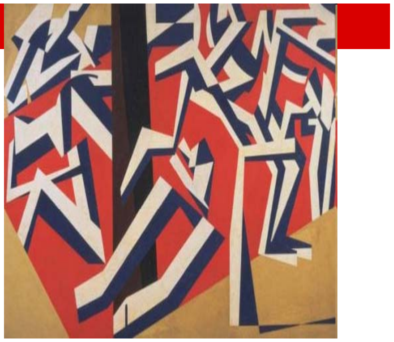
Experience with Products

- **Very different**
- **Sometimes we find good security design and only small problems**
  - Still we find security problems in most evaluations
- **Sometimes we find major design problems**
  - Fixing those usually takes time and slows down the evaluation significantly
- **Quite often we find documentation problems**
  - Inconsistencies and wrong advice that may lead to security problems in operation
- **Very often we find other problems**
  - Functions with unnecessary privileges
  - Unnecessary large attack surface, overly complex
  - Non-security related problems



Experience with Vendors

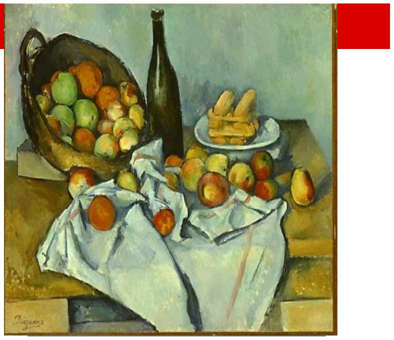
- **Very different**
- **Some just want "the stamp" – as cheap as possible**
  - Those usually have the worst products!
- **Some want to perform a serious evaluation, but don't want the lab to have a "too close" look**
  - Fear loss of IP
  - Fear disruption of their development people
- **Some take it serious**
  - Provide more documentation than required by the CC
  - Are open for discussions (even on vulnerabilities)
  - Are willing to change product and processes to improve security
  - Integrate evaluation into their development lifecycle



Experience with Processes

- **Usually an area for significant improvement**
  - No strict control of attack surface additions/changes (common to all vendors)
  - No enforcement of least privilege for software components (common to all vendors)
  - No security impact analysis on design changes (many vendors)
  - No security reviews during implementation (many vendors)
  - No security focused testing (still some vendors)

- **Suggestions for process improvements are a common result of our evaluations**



Experience with Certifiers

- **Differences within the schemes are larger than differences between schemes**
  - Depends on the person and their expertise
  - Sometimes certifiers want to influence the product
    - Which is **very dangerous**
- **The more technical experience they have, the better for the evaluation**
  - Although some focus just on those aspects they know
- **Certifiers believe they get knowledge also of security problems fixed during the evaluation**
  - The vendors would kill us if we would tell the certifiers (or anyone else)!
  - Certifiers only see the end product, not the initial one

Experience with the CC

- **CC was developed by government people**
  - With no or limited development experience
  - With no or limited evaluation experience
- **The result is as expected**
  - CC/CEM V2.3 was not good, CC V3.1 is even worse
  - CC and CEM often focus on the wrong aspects
  - You have to know the intention to perform a useful evaluation (and sometimes “re-interpret” the CC/CEM)
- **Too much focused on documentation**
  - Not stating what those documentation should be used for
  - Some labs just check that the documentation exists and don’t use it further in the evaluation process

Summary

- **CC/CEM need major modifications to be more useful**
  - Vendor and lab input need to be taken into account
- **Vendors need to take security more serious**
  - Not just wanting a “security stamp” even for bad products
  - More willingness to co-operate with evaluators
- **Schemes need to accept that evaluations have some level of subjectivity**
  - If they are totally objective, they are useless
- **Evaluators need to understand the product in detail and prove this to the certifiers**
  - This should be the basis for a discussion of security between vendor, evaluator and certifier