Seminar Term Paper

Formal Methods for Fun and Profit

Summer Semester 2005

Theme: Certification of Hardware and Software

Supervisor: Jr. Prof. Beckert
Presented by: Kiptoo A. Kiprop
Registration number: 201210795
University of Koblenz
Institute of Computer Science

- **Security Issues**
- **Certification**
- **CC**
  - ✓ **PP**
  - ✓ **ST**
  - ✓ EALs
- **Product Certification**
  - Examples
  - Formal methods application
- **Conclusion**

Certification of Hardware and Software

- Security Issues
- Certification
  - Common Criteria
    - Protection Profiles
    - Security Target
    - Evaluation Assurance Levels (EALs)
- Product certification
  - Examples
    - Linux Server v.8, JVCM
  - Application of formal methods
    - B-Method
- Conclusion

Certification of Hardware and Software

- **Security Issues**
- **Certification**
- **CC**
  - ✓ **PP**
  - ✓ **ST**
  - ✓ EALs
- **Product Certification**
  - Examples
  - Formal methods application
- **Conclusion**

- Security Issues
  - Avoid financial loses
  - Preserve health and life
- Where security is needed
  - high risk systems – banking systems, military, ..
  - complex and expensive tools – rockets, ..
  - everywhere ..
- Provision and control of security in ICT
  - producers, developers?
  - Government e.g. through BSI
  - EU level

Certification of Hardware and Software

- **Security Issues**
- **Certification**
- **CC**
  - ✓ **PP**
  - ✓ **ST**
  - ✓ EALs
- **Product Certification**
  - Examples
  - Formal methods application
- **Conclusion**

- Certification
  - Act of conferring legality, formal warrant
  - Some requirements must be fulfilled first
- Certification problems
  - Extend of validity, e.g. over borders
  - Requirements may be too lenient
  - Time limits for validity
- Certification advantages
  - Some quality of security
  - Standardization
  - Source of income

Certification of Hardware and Software

- **Security Issues**
- **Certification**
- **CC**
  - ✓ **PP**
  - ✓ **ST**
  - ✓ EALs
- **Product Certification**
  - Examples
  - Formal methods application
- **Conclusion**

- Department of Data Security – Schleswig Holstein
  - an example of a functioning certifying body.
  - issued by the State of Schleswig-Holstein (independent).
  - product not compulsory.
  - issue seal of approval.

VOM DATENSCHUTZ
EMPFOHLEN*

  - Approval of ICT products as well as data processing methods.
  - go after citizen complaints about products.
  - citizen assistance.

Certification of Hardware and Software

- **Security Issues**
- **Certification**
- **CC**
  - ✓ **PP**
  - ✓ **ST**
  - ✓ EALs
- **Product Certification**
  - Examples
  - Formal methods application
- **Conclusion**

- Common Criteria
  - To develop standard collection of necessary requirements.
  - A short history of national standards
    - From Trusted Computer Systems evaluation criteria TCSec – USA (“Orange Book”) to CC v.3.0.
  - Flexible enough for newer standards
  - Requirements under unique categories:
    - **Functional requirements** – define the desired security behaviour in classes (e.g. Audit, Privacy), families and components.
    - **Security assurance requirements** – countercheck to determine if security measures are effective and correctly implemented, e.g. Development

- **Security Issues**
- **Certification**
- **CC**
  - ✓ **PP**
  - ✓ **ST**
  - ✓ EALs
- **Product Certification**
  - Examples
  - Formal methods application
- **Conclusion**

Certification of Hardware and Software

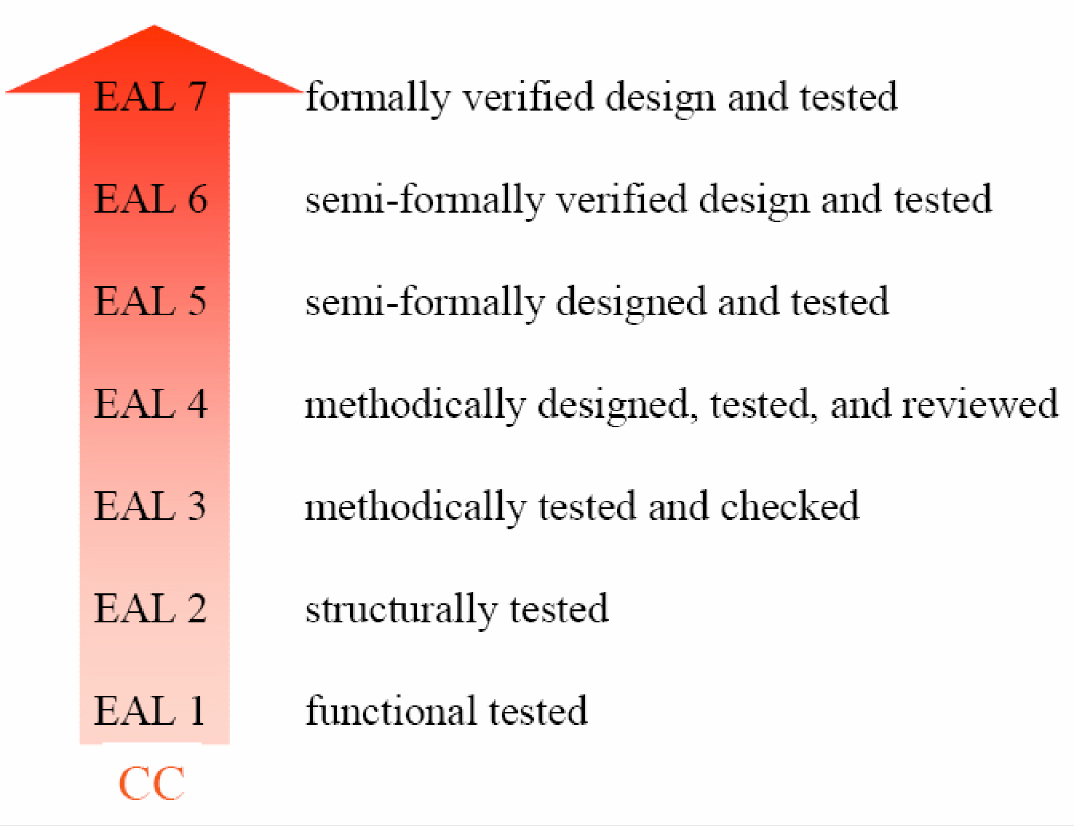
- Protection Profiles
  - What is needed in a security solution
  - User oriented, simple language
  - PP says what the system has to do

- Security Target
  - Created by developer
  - Contains IT security objectives and requirements of a specific identified TOE
  - Basis over which an evaluation is performed
  - Identify security capabilities of a particular product

Certification of Hardware and Software

- Security Issues
- Certification
- CC
  - ✓ PP
  - ✓ ST
  - ✓ EALs
- Product Certification
  - Examples
  - Formal methods application
- Conclusion

- Evaluation Assurance Levels
  - Trustworthiness, reliability
  - hierarchy level increases with increasing security assurance.



EAL 7	formally verified design and tested
EAL 6	semi-formally verified design and tested
EAL 5	semi-formally designed and tested
EAL 4	methodically designed, tested, and reviewed
EAL 3	methodically tested and checked
EAL 2	structurally tested
EAL 1	functional tested

Certification of Hardware and Software

- Evaluation Assurance Levels
  - High-level design: decomposes system into modules (subsystems) providing functionality described in fuctional specification.
  - Low-level design: provide specification of the internal workings of each module.

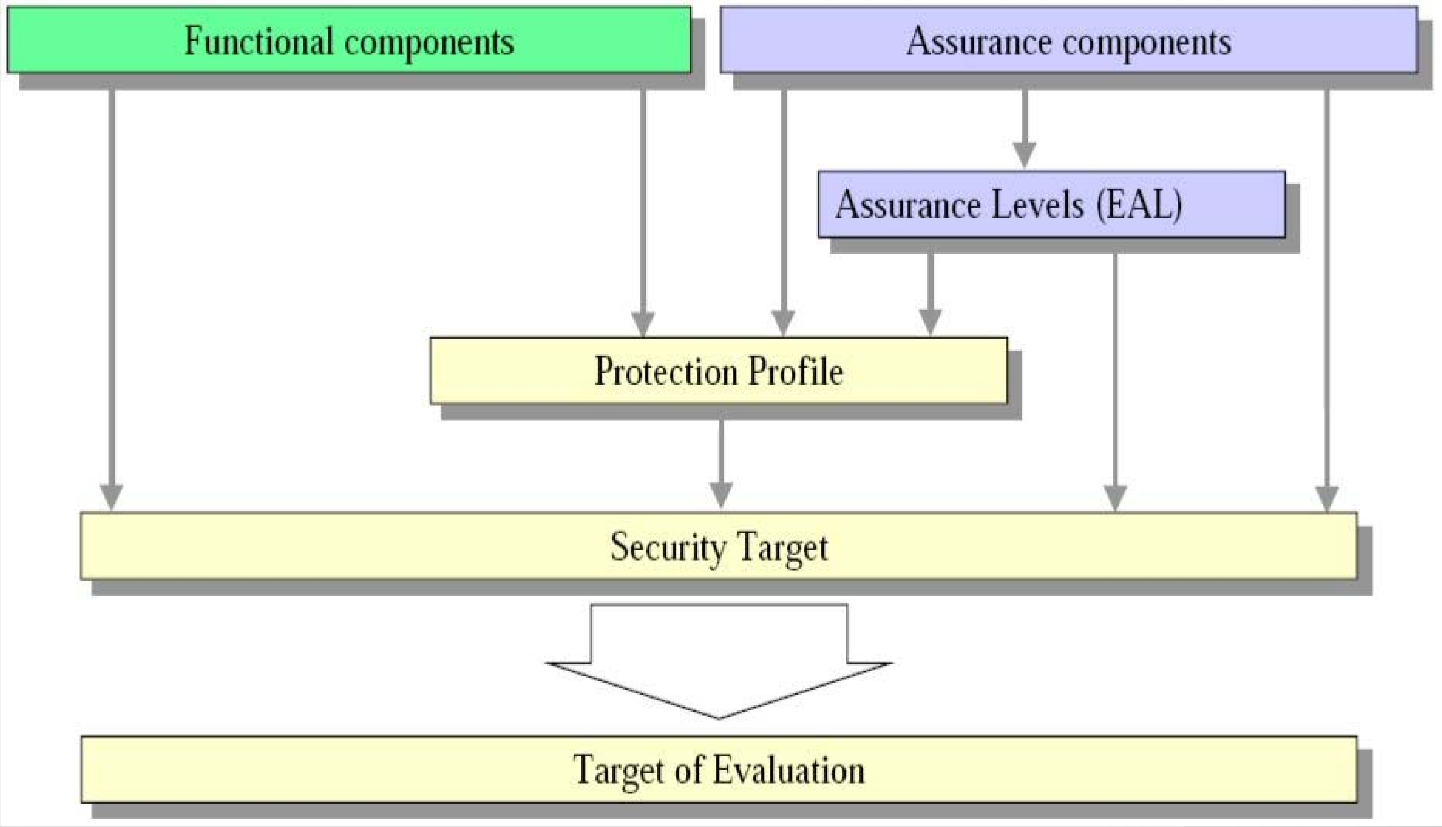
	low-level design	high-level design
EAL 1	Informal	Informal
EAL 2	Informal	Informal
EAL 3	Informal	Informal
EAL 4	Informal	Informal
EAL 5	Semi-formal	Semi-formal
EAL 6	Semi-formal	Semi-formal
EAL 7	Semi-formal	Formal

- **Security Issues**
- **Certification**
- **CC**
  - ✓ **PP**
  - ✓ **ST**
  - ✓ EALs
- **Product Certification**
  - Examples
  - Formal methods application
- **Conclusion**

- **Security Issues**
- **Certification**
- **CC**
  - ✓ **PP**
  - ✓ **ST**
  - ✓ EALs
- **Product Certification**
  - Examples
  - Formal methods application
- **Conclusion**

Certification of Hardware and Software

- Summary of correlation between CC components



- **Target Of Evaluation - TOE:** an IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation. Defines assets to protect. -> satisfies the ST

Certification of Hardware and Software

- **Security Issues**
- **Certification**
- **CC**
  - ✓ **PP**
  - ✓ **ST**
  - ✓ EALs
- **Product Certification**
  - Examples
  - Formal methods application
- **Conclusion**

- Certified products

Integrated circuits : Microcontrollers
ST Micro, Samsung Electronics, Infineon Technologies, AMTEL smartcards, .. EAL4+ (most of them)

Smart Cards : Operating Systems
ST Micro , Axalto, Infineon Technologies, Oberthur Card, Philips, Gemplus, IBM, .. EAL1+, .., EAL4+. Some EAL 5 e.g. Sun JavaCard.

Network Products : Firewalls
Bull, EADS Telecom, EAL2+

Certification of Hardware and Software

- **Security Issues**
- **Certification**
- **CC**
  - ✓ **PP**
  - ✓ **ST**
  - ✓ EALs
- **Product Certification**
  - Examples
  - Formal methods application
- **Conclusion**

- Suse Linux Enterprise Server v.8
  - evaluated and obtained an EAL3 rating
  - no code re-engineering, no interruption of development process, but more costs.
  - TOE: operating system, running and tested on the hardware and firmware specified in the ST.
  - design of test only to verify correct operation of security related user programs, DB-files and systems calls.
  - testing for system availability in a stress environment
  - no formal methods application: EAL 4 would be next.
  - system works in an normal environment.

Certification of Hardware and Software

- **Security Issues**
- **Certification**
- **CC**
  - ✓ **PP**
  - ✓ **ST**
  - ✓ EALs
- **Product Certification**
  - Examples
  - Formal methods application
- **Conclusion**

- Java Card Virtual Machine (JCVM)

  - developed by Sun Microsystems.
  - surrogate to Smartcard

    -> used to secure data storage and authentification.
  - based on a collection of Java applets.
    - widely used in banking and telecom sector.
    - may run on platform independent virtual machines.
    - interaction with systems through APIs – Application Programming Interfaces.

Certification of Hardware and Software

- Java Card Virtual Machine (JCVM)
  - Evaluated and obtained EAL 4 and EAL 5+ rating.
  - **TOE**:
    - processor chip and IC for software - drivers.
    - Card Operating System
    - JavaCard Runtime Environment
    - Card manager e.g. Global Platform Envir. (OPEN)
  - **Semi-formal (formal) models:** description for each representation level (SPM, FSP, HLD)
    -> Assurance Development Class (ADV)

- **Security Issues**
- **Certification**
- **CC**
  - ✓ **PP**
  - ✓ **ST**
  - ✓ EALs
- **Product Certification**
  - Examples
  - Formal methods application
- **Conclusion**

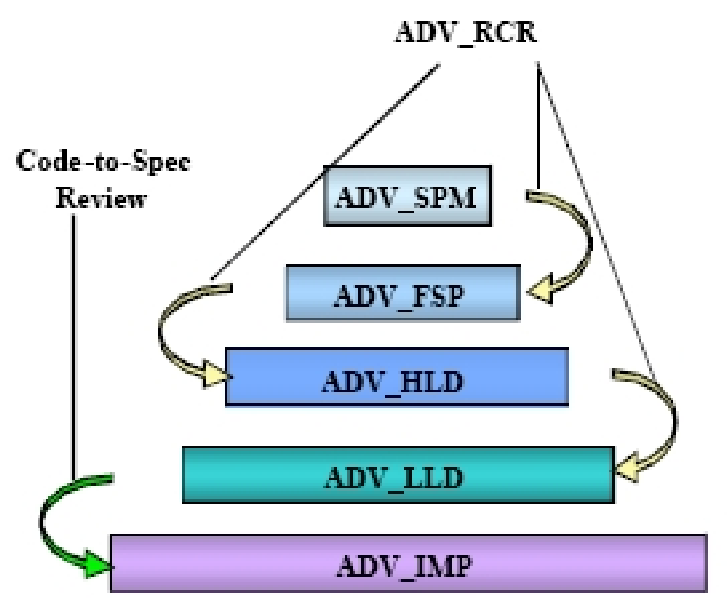
Certification of Hardware and Software

- **Security Issues**
- **Certification**
- **CC**
  - ✓ **PP**
  - ✓ **ST**
  - ✓ EALs
- **Product Certification**
  - Examples
  - Formal methods application
- **Conclusion**

- Java Card Virtual Machine (JCVM)

- What should be semi-formally described?

  - SPM: security rules (TOE security policy model)
  - FSP : external interfaces (functional specification)
  - HLD: subsystems and interactions (high-level design)
  - RCR: correspondence relations (between FSP and HLD)



Code-Spec-Review > compare Low Level Design (LLD) model to implementation as demo of their correspondence.

Certification of Hardware and Software

- **Security Issues**
- **Certification**
- **CC**
  - **PP**
  - **ST**
  - EALs
- **Product Certification**
  - Examples
  - Formal methods application
- **Conclusion**

- JCVM specification formalizing with B-Method
  - formalizing for CC evaluation.
  - applies semi-formal and formal models which specify, design and code high risk systems.
  - covers the whole system life-cycle i.e. from specification to executable code.
  - Refinement process to obtain the implementation of the B specification.

- **Security Issues**
- **Certification**
- **CC**
  - ✓ **PP**
  - ✓ **ST**
  - ✓ EALs
- **Product Certification**
  - Examples
  - Formal methods application
- **Conclusion**

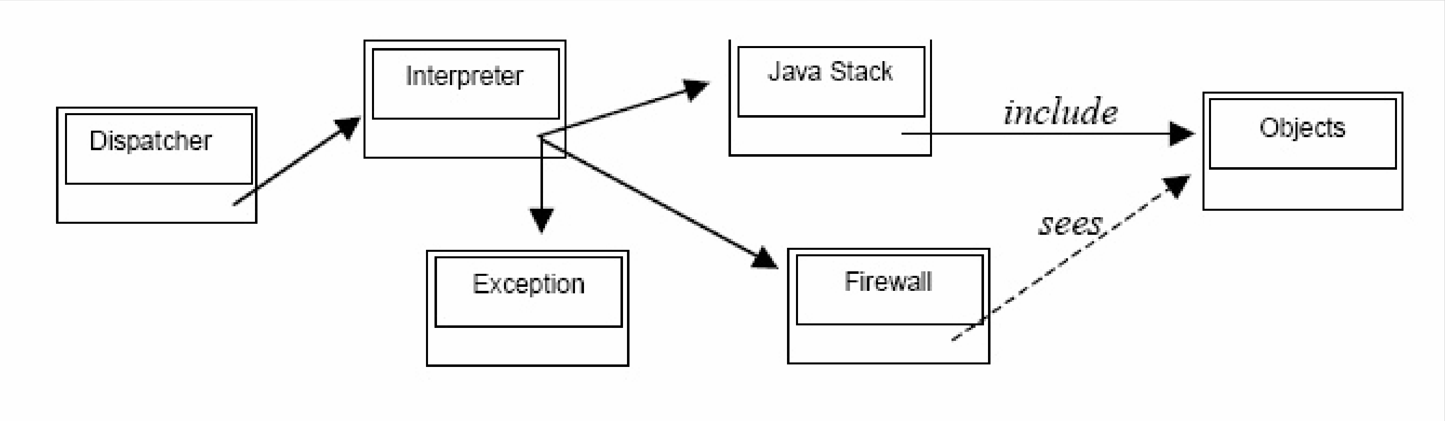
Certification of Hardware and Software

- JCVM specification formalizing with B-Method
  - Protection Profile
    - life-cycle management
    - Authen. Mechanism for loading applications
    - logical separation of data between applications
    - security services for applications
  - Security Target
    - integrity and confidentiality of assets,
    - protection of the TOE during its active life, that with active security functions,
    - protection of the TOE development environment and delivery process.

Certification of Hardware and Software

- **Security Issues**
- **Certification**
- **CC**
  - ✓ **PP**
  - ✓ **ST**
  - ✓ EALs
- **Product Certification**
  - Examples
  - Formal methods application
- **Conclusion**

- JCVM issues
  - what happens if part on which one applet is defective?
  - will problem spread to other applets? Detection?
  - solution through a firewall.
    - integrated in the VM.
    - every time access to resource, check.
    - if not allowed, return security exception.



- JCVM modules: dispatcher, interpreter, firewall, java stack, exception manager and the memory.

Certification of Hardware and Software

- **Security Issues**
- **Certification**
- **CC**
  - ✓ **PP**
  - ✓ **ST**
  - ✓ EALs
- **Product Certification**
  - Examples
  - Formal methods application
- **Conclusion**

Conclusion

- **Certification issues:**
  - other certification ways: Schleswig-Holstein
  - probably no IT systems evaluated in EAL 6 or EAL 7.
  - most operating systems obtained level 4 (Windows 2000, Linux Server v.9., Novell NetWare)
- **What speaks for formal methods?**
  - may be analysed mathematically and finally demonstrating their consistency and completeness.
  - they might become compulsory in the future.
  - may be processed using software tools. e.g. Model Checker

Certification of Hardware and Software

- **Security Issues**
- **Certification**
- **CC**
  - ✓ **PP**
  - ✓ **ST**
  - ✓ EALs
- **Product Certification**
  - Examples
  - Formal methods application
- **Conclusion**

- Conclusion
  - **What speaks against formal methods?**
    - To achieve a higher security, the system features and components has to be kept to the minimum.
    - Developer will need a lot of time and resources. More developers? More costs? More time?
    - Lack of market: but there's hope, EAL 4 products survived.
    - Formal methods are man-made and are too prone to mistakes.
- ..finally
  - no absolute security, not even with formal methods.
  - security market rising => bright future for formal methods?