RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

NECESSARY STATIC CODE ANALYSIS FOR HIGHEST LEVEL OF CERTIFICATION

FRAMA-C DAYS
14/06/2024

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Agenda

1. Certification

2.Code analysis

3.Formal methods

1. CERTIFICATION

ANSSI

- Agence nationale de la sécurité des systèmes d'information (French Cybersecurity Agency) created in 2009
- National authority for cybersecurity and cyber defence
- Government organisation that reports to the General Secretariat for Defence and National Security (SGDSN)
- Defensive mission (not offensive)
- Role: to protect the nation from cyber attacks
- Primary targets: Operators of critical national infrastructures ("OIV"), operators of essential services ("OES") and administrations

Certification

- Goals:
  - Give confidence (on a level achieved)
  - Obtain recognition (by an authority, on a sectorial domain, on a geographical domain)
  - Comply to regulatory/contractual requirements
  - Allow a common ground between different stakeholders (users/customers/suppliers)
- Definitions from the ISO/IEC 17000:
  - Conformity assessment: « demonstration that specified requirements relating to a product, process, system, person or body are fulfilled »
  - Conformity assessment can be based on a self-assessment (statement of conformity) or third party assessment (certification)

Certification at ANSSI

- Certification established by law: Decree N°2002-535

  -> for products in cybersecurity

- Main stakeholders:
  - Manufacturer (developper)
  - Laboratory in charge of the assessment (of the product or more precisely of the Target of Evaluation)
  - Certification body in charge of the certification
  - Sponsor

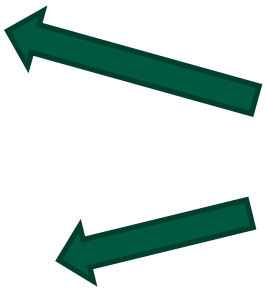
Product certification at ANSSI

- Certification de sécurité de premier niveau (CSPN)
  - Fixed time
  - « Low » Cost
  - Only one assurance level
  - National recognition (with a BSI agreement)
  - Based on the vulnerability assessment
- Common Criteria(CC)
  - No time constraint
  - High cost
  - Several assurance levels
  - International standard and recognition
  - Based on a conformity analysis and a vulnerability assessment

Assurance levels for CC certification

Code analysis

Formal methods



EAL1 – Functionally Tested
EAL2 – Structurally Tested
EAL3 - Methodically Tested and Checked
EAL4 – Methodically Designed, Tested and Reviewed
EAL5 – Semiformally Verified Designed and Tested
EAL6 – Semiformally Verified Design and Tested
EAL7 – Formally Verified Design and Tested

2. CODE ANALYSIS

CC requirements for code analysis

- Depending on the assurance level, the code analysis is mandatory:
  - Partial or full delivery of the source code needed for the assessment
  - As an entry point for the vulnerability analysis
  - No specific means mandatory (manual, automatic, static, dynamic, …)
    - Til the Note 26 – French interpretation for this code analysis

CC requir code analysis

- Depending or
  - Partial or fu
  - As an entry poin
  - No specific means mandat
    - Til the Note 26 – French interpretation for this code analysis

> "The main requirement of this note comes from the return of experience of the French certification body, with regard to manual static analysis and dynamic analysis (automated or not). It was observed that as a general rule, manual static analysis and dynamic analysis are always likely to miss significant vulnerabilities, even when reviewing small codebases"

CC requirements for code analysis

- Depending on the assurance level, the code analysis is mandatory:
  - Partial or full delivery of the source code needed for the assessment
  - As an entry point for the vulnerability analysis
  - No specific means mandatory (manual, automatic, static, dynamic, …)
    - Til the Note 26 – French interpretation for this code analysis
- Needs:
  - Efficient and complete analysis
  - Repeatable and verifiable analysis

Static code analysis

Note 26

- French specificity mandatory for:
  - CC evaluation and products assessed for the level AVA-VAN.3 (or above)

- Content of the Note 26:
  - Automated static analysis mandatory
  - To find vulnerabilities introduced by a bad use, or a limitation, of the implementation technology itself (programming language, compiler..)
  - Based on the source code (fully or partially) (including compilation directives)
  - Registered in a methodology of the laboratory (validated by ANSSI)

Static code analysis

Note 26

- Implementation
  - Development of a methodology by the laboratory
  - Run of this methodology on a pilot project (regular process for the licensing of the laboratories)
  - Follow-up with our internal software security laboratory

- Constraints
  - Manufacturer : white box approach and delivery of the source code
  - Laboratory : methodology and tooling
  - ANSSI : close cooperation with the laboratory
  - Various programming languages to take into account

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

2. FORMAL METHODS

Formal methods

Formal modeling of the security goals of a target of evaluation

- Depending on the assurance level, from EAL6
  - Related to component CC ADV_SPM.1
  - Based on functions and goals defined in the security target

- Goals
  - Formal representation of the security functions
  - Formal proof to validate security goals implemented in the security functions

Formal methods

Note 12

- CC are not prescriptive on the formal methods

- French note published in 2008 to define:
  - Goals for ANSSI
  - Expected furnitures
  - Interpretation of the CC
  - (not specific tools identified)

3. CONCLUSION

Conclusion

- Static code analysis necessary thanks to the following properties:
  - Efficiency
  - Repeatabilty
  - Verifiability
  - Comparability
- Formal methods are as well required from a specific EAL
- Both static code analysis and formal methods raise the level of security of the prodocut but it requires strong skills and good tools

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Questions ?

Franck Sadmi
Head of the French certification body

Franck.sadmi[a]ssi.gouv.fr