

Predictive Assurance Update on Lead Nation Project

Bundesamt für Sicherheit in der Informationstechnik (BSI)
(Federal Office for Information Security)

11 ICCC / September 2010

Irmela Ruhrmann

Head of Division Certification, Approval and Conformity Testing



Outline

- ❑ Project Overview
- ❑ CC Opportunities
- ❑ Predictive Assurance – Draft Concept
- ❑ Planned Action



Project Overview

Background

Presented at 9 ICCC in Jeju

- ❑ **Problem:** product certificate is frequently obsolete at, or shortly after, the certification date:
 - evaluated configuration no longer available on the market
 - need to operate product in other than the evaluated configuration
 - patches issued since certification date
- ❑ **Solution:** greater emphasis on the developer's development process including the update and flaw remediation process
- ❑ **Goal:** Provide a degree of 'predictive assurance' where the conclusions of an evaluation report could remain valid for a much more realistic and usable length of time



Project Overview

Project Progression (1)

- ❑ Initiated in March 2008 as Lead Nation Project by CCDB
- ❑ Initial plan presented at 9 ICCC in Jeju, Korea
Lead: GE
Contributing Nations: UK, US, SP, KR, NO, SE
- ❑ First Concept drafted
- ❑ Questionnaire distributed to vendors, CCRA Schemes
- ❑ Feedback from Questionnaire analysed and compiled
- ❑ Update on project presented at 10 ICCC in Tromsø, Norway



Project Overview

Project Progression (2)

- ❑ February 2010: Development of expanded version of the concept completed
- ❑ March 2010: Presentation of concept to CCDB
- ❑ June 2010: Presentation of revised concept at Lead Nation Meeting
- ❑ June/July 2010: Invitation for comments to CCRA Schemes, interested vendors
Comment period up to end of August 2010
- ❑ September 2010: Progress Report at 11 ICCC in Antalya, Turkey



CC Opportunities

Enhancements

CC could be enhanced by development process aspects to increase assurance, e.g.

- ❑ Developer design and code reviews
- ❑ Developer documentation and coding standards
- ❑ Static and dynamic code analysis performed by the developer
- ❑ Automated test generation and test execution (e. g. fuzzy testing)
- ❑ Developer threat and vulnerability analysis / penetration testing

Predictive Assurance needs to address, among others, these aspects.



CC Opportunities

Existing CC definitions and proposed enhancements

- ❑ assurance requirements
 - objectives to be identified
- ❑ requirements for developer evidence
 - methods to produce evidence to be defined
- ❑ evaluator actions
 - developer actions and
 - assurance activities for developer to be defined

Result:

Effectiveness of a developer in producing „secure products“ can be determined



CC Opportunities

Developer assurance measures

- ❑ Developer needs to describe his assurance measures and explain their effectiveness
 - Effective means assurance measures lead to a product with no or only limited security problems

Result:

Predictive assurance takes into account assurance measures performed by the developer as part of his development process



Predictive Assurance – Draft Concept

Proposal

❑ Steps to be taken

- Check for development process aspects that provide assurance
- Map them to the assurance objectives related to CC assurance requirements
- Evaluate the effectiveness of those assurance measures
- Determine the assurance that can be reasonably predicted for changes made by the developer
- Determine the type of changes the developer is allowed to perform without a need for re-evaluation

❑ Appropriate methodology to be developed



Predictive Assurance – Draft Concept

Additional evidence is required for

- ❑ The assurance measures applied by the developer
- ❑ The purpose of each measure
- ❑ Demonstration that the measure is effective for the purpose defined
- ❑ Evidence that the measure has been applied



Predictive Assurance – Draft Concept

The Assurance Target

- Developer and evaluator develop during the initial product evaluation an Assurance Target document that contains:
 - A description of all development process activities considered to provide assurance including:
 - their general objective
 - the methodology or tools used
 - the way the results of the activity are documented
 - how the results of the activity are being used in the TOE development
 - how the developer has assessed the effectiveness of the activity
 - A mapping of these activities to
 - CC assurance objectives and
 - security objectives of the product
 - An assessment how far these objectives are addressed by performing these activities



Predictive Assurance – Draft Concept

Structure of the Assurance Target

Chapter 1:

Overview of the development process and assurance methods

Chapter 2:

Mapping of assurance measures to the CC assurance objectives

Chapter 3:

Mapping of assurance measures to the security objectives of the product

Chapter 4:

Analysis of flaws in previous versions of the product

Chapter 5:

Evaluation approach for the development process on the basis of agreed methodology



Predictive Assurance – Draft Concept

Essential Aspects

- Documentation should refer to existing development documentation
- Analysis and reporting of flaws required
- Mitigation of flaws should be documented
- Effectiveness and extent of contribution of assurance measures should be described
- Usage of Tools should be documented



Planned Action

- ❑ Review comments received
- ❑ Discuss open issues with interested parties (CCRA Schemes, vendors)
- ❑ Revise concept
- ❑ Provide concept for second round of comments
- ❑ Incorporate results from other lead nation projects
- ❑ Plan trial evaluations



Kontakt



Bundesamt für Sicherheit in der
Informationstechnik (BSI)
(Federal Office for Information Security)

Irmela Ruhrmann
Godesberger Allee 185 - 189
53175 Bonn

zerti@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de