

Predictive Assurance Update on Lead Nation Project

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

10 ICCC / September 2009

Irmela Ruhrmann
Head of Division Certification, Approval and Conformity Testing

Overview

- ❑ Introduction
- ❑ Initial Steps of Project
- ❑ Feedback on Questionnaire
- ❑ First Concept
- ❑ Further Proceeding

Introduction

- ❑ Lead Nation Project “Predictive Assurance”
- ❑ Lead: GE
Contributing Nations: UK, US, SP, KR, NO, SE

Introduction

- Problem definition: product certificate is frequently obsolete at, or shortly after, the certification date:
 - evaluated configuration no longer purchasable
 - need to operate product in another than in the evaluated configuration
 - patches issued since certification date
- Solution: greater emphasis on the developer's original development process and 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

Introduction

- ❑ Initial focus on software products
 - patches are released more often than with hardware

- ❑ Feasibility for other product categories to be considered in a later step

Initial Steps of Project

- ❑ Draft general approach
- ❑ Compile Questionnaire
 - Questionnaire contains general approach on „predictive assurance process“ and seven questions
- ❑ Provide Questionnaire to vendors, CCRA Schemes
 - Questionnaire allows developers to express their needs and provide potential input for the „predictive assurance“ project
- ❑ Analyse and compile feedback from Questionnaire

Initial Steps of Project

- ❑ Feedback on Questionnaire was received from
 - ❑ Common Criteria Vendors Forum (CCVF)
 - ❑ International Security Certification Initiative (ISCI, WG1)
 - ❑ German vendors
 - ❑ Spanish Scheme (CB, ITSEF, vendors)
 - ❑ Korean Scheme (CB, ITSEF, vendors)
- ❑ General tendency of the feedback was positive and constructive

Feedback on Questionnaire

What are the typical types of product you submit for evaluations?

- ❑ Large variety of products:
 - complex operating systems
 - specific security products
 - hardware components

Do you see the need for a „predictive assurance process“?

- ❑ Most responders stated a clear need for a formalized and internationally recognized procedure

What are your main reasons for the need?

- ❑ „Time to market“ seems to be the most relevant issue
- ❑ Developers of products with short shipping cycles see a major problem in the discrepancy between the evaluated („old“) versions and the current versions of a product, including patches or new functionality

Feedback on Questionnaire

[...] Do you have such kind of procedure already in place and/or do you have recommendations for existing/standardized procedures to use here?

- ❑ All participating vendors have internal processes in place which provide assurance for secure development and change management
- ❑ Process for „predictive assurance“ should not require to follow external standards or to use mandatory tools
- ❑ Process for „predictive assurance“ should state feasible criteria, usable in conjunction with existing development processes

Feedback on Questionnaire

Is the general model of a „predictive assurance process“ and key elements adequate or do you have other suggestions?

- ❑ General model is supported in principle
- ❑ questions on details and criteria for decision making during the process Numerous
- ❑ Adequate „threshold value“ for the distinction between the two cases
 - vendor decides that a change can be applied
 - decision is made by CBis seen as crucial for success

Feedback on Questionnaire

Do you have additional suggestions or input for the planned Lead Nation project?

- Several different ideas
 - completely separate product evaluation from secure development process, e.g. include in site certification process
 - „threshold value“ dependent on product type,
 - etc...

Do you wish to participate in a trial for the „predictive assurance process“?

- Some potential participants – more information needed before commitment

Feedback on Questionnaire

Conclusion

- ❑ General response regarding „predictive assurance“ was positive
- ❑ More details needed before committing to actively participate in a trial
- ❑ Supportive to further proceeding

First Concept

- ❑ Initial evaluation is performed
- ❑ In parallel, specific activities are performed
 - developer provides concept for „predictive assurance process“
 - concept includes the following items:
 1. Tools, procedures and best practices to gain security of products
 2. Security awareness training of development personal
 3. Basic steps of „predictive assurance process“
 4. Procedures for information of customers
 5. Procedures to keep evaluation evidence up to date
 6. Definition of „impact criteria“ – severity of modification
 7. Definition of appropriate test suite:
 - regression testing, procedures to adapt

First Concept

Following the issuance of the certificate the „predictive assurance process“, takes place when developing further versions (patches, updates):

- ❑ External audits may take place
- ❑ Apply impact criteria for each product change
 - various models need to be discussed
- ❑ Developer to produce evidence defined by „predictive assurance process“
 - subject to review by evaluator at certain intervals
- ❑ Developer to apply test suite as defined by „predictive assurance process“

Further Proceeding

Project phases	Target date for completion
Develop an expanded version of the concept Take into account: <ul style="list-style-type: none">- Feedback on questionnaire- Input from CCRA Schemes (Contributing Nations)CCRA principles	January 2010
Conduct trial projects for a „predictive assurance process“	December 2010
Evaluation of trials	April 2011
Consider feedback of process description and trials to finalize concept, e.g. as supporting document, change proposal for CC and CEM	June 2011

Contact



Federal Office for Information Security
(BSI)

Irmela Ruhrmann
Godesberger Allee 185 – 189
53175 Bonn

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