Application of Engineering "Best" Practices in Common Criteria

Pulei Xiong, PhD
EWA-Canada
September 12th, 2013

Your Trusted Partner

Outline

- Introduction
- Model-Driven CC Analysis Tool
- Structured & Guided CC VA Framework
- Threat-Driven MD PP Development
- Conclusions

Your Trusted Partner

Introduction

- Long-standing concerns in CC:
  - the **reliability** (consistency) of evaluation results
  - the **cost-efficiency and effectiveness** of evaluation process
  - the **applicability** of CC certificates

- These issues in general are commonly addressed in the relevant engineering disciplines, such as:
  - Software Engineering
  - Quality Engineering
  - Security Engineering

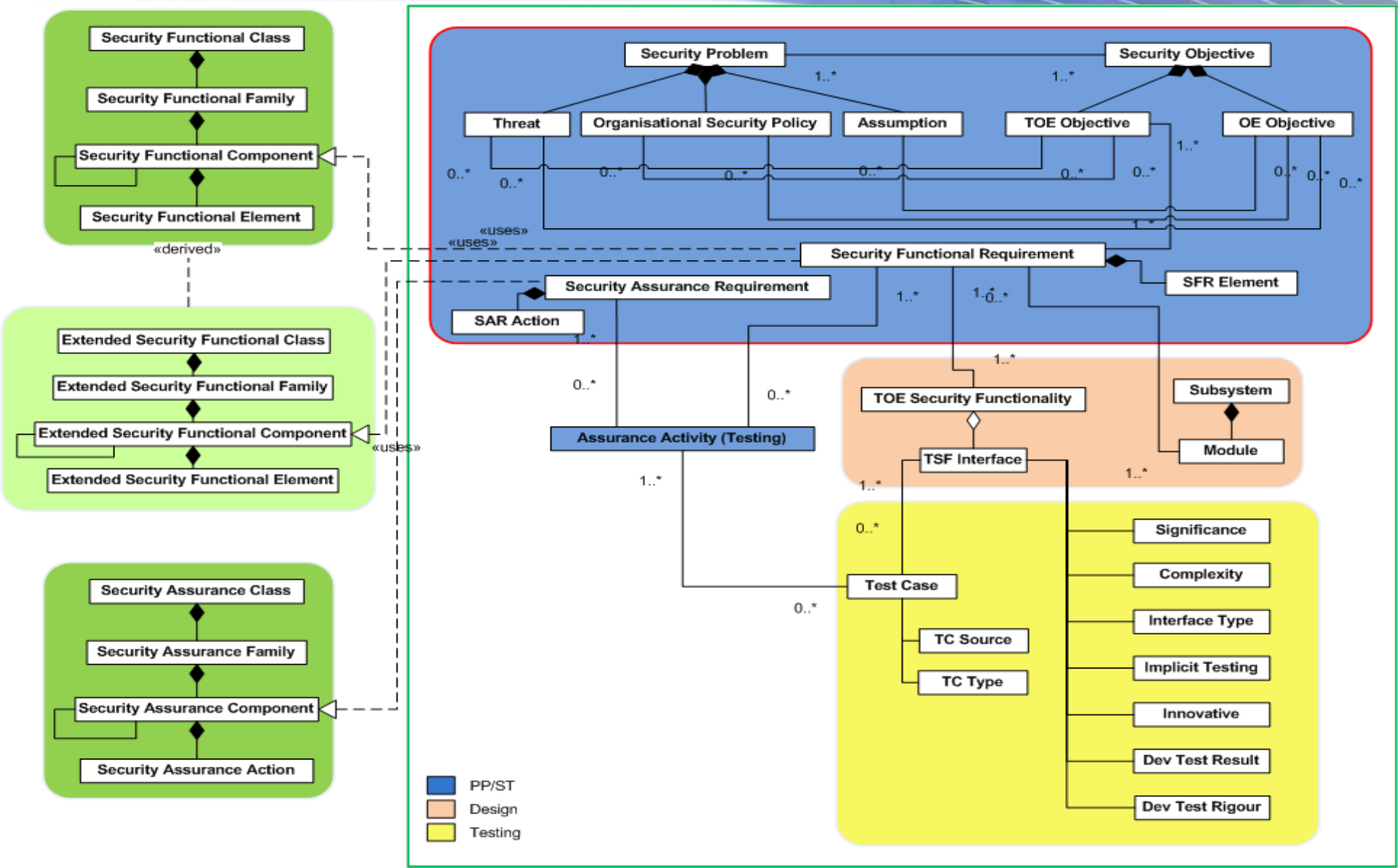
- In this presentation, we will share our recent efforts on applying engineering “best” practices in CC

Model-Driven CC Analysis Tool

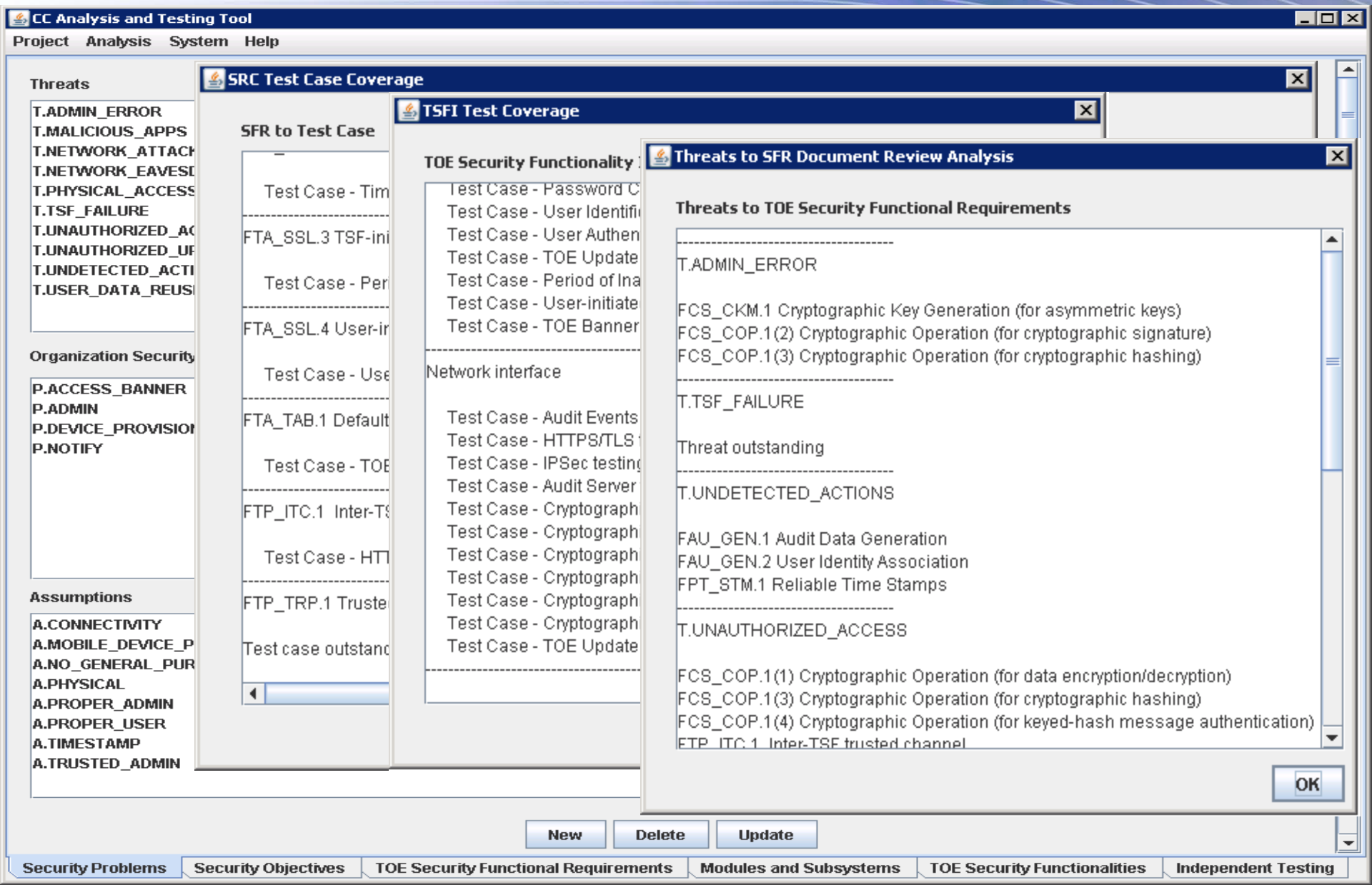
- An EWA-Canada IR&D project initiated in 2011 to support CC evaluation
  - Document review (Validation)
  - Test analysis (Validation & Verification)
- **Model-Driven approach** to CC analysis
  - Formalization of Evaluation Evidence
  - Tool Support
- A Java program tool and a backend database built upon the CC model

Your Trusted Partner

Common Criteria Evaluation Model



Java Program Screenshots

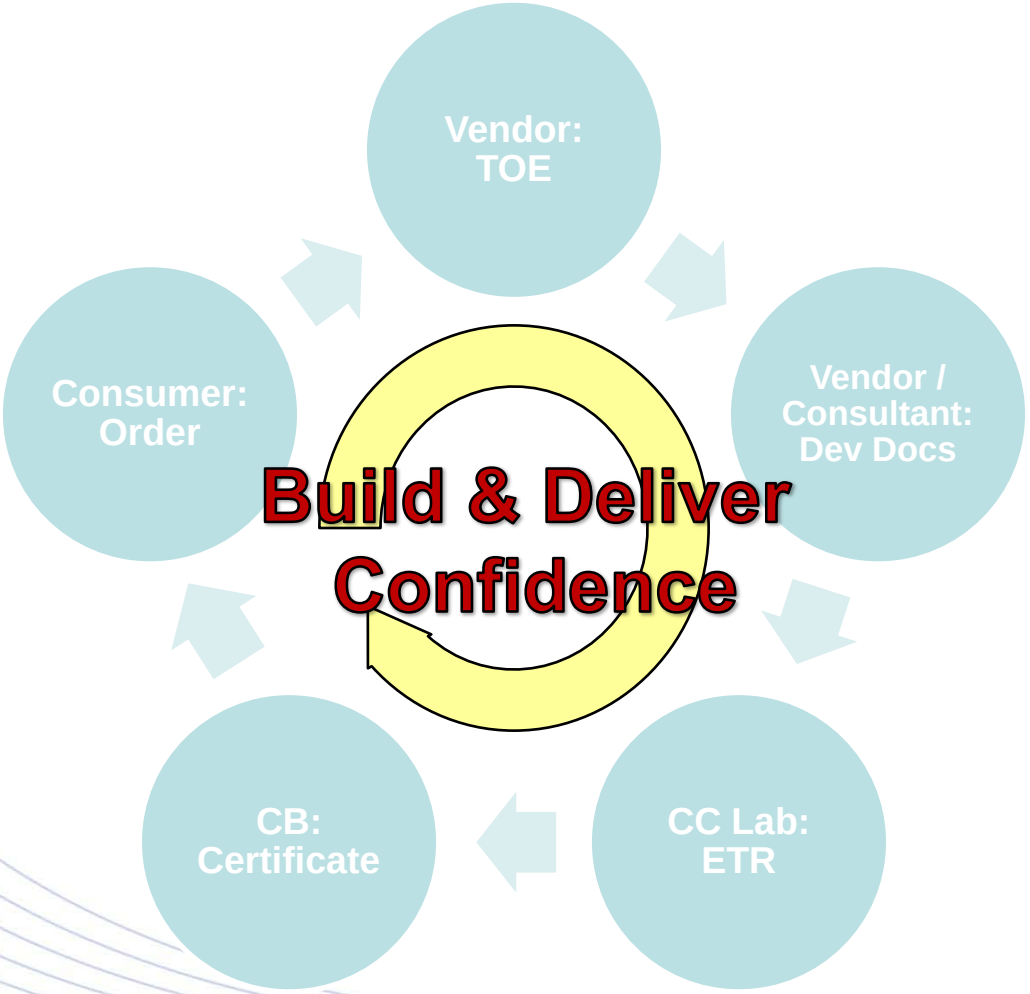


Usage of the Tool

- Document Review
  - **"Syntax" check** of a large number of associations, e.g. consistency & dependency, that need to be kept correct among the artifacts
  - Assist with **"semantic" validation** of the key artifacts, e.g. it can generate a view of threat vs. SFRs to help assess if a threat has been sufficiently countered by the SFR(s)

- Test Analysis
  - Leverage test analysis for **strategic test sampling**
  - Test coverage analysis against assurance activities
  - Test coverage analysis against TSFI, SFR, Threat …

A Bigger View: Tool Support in CC Eco-System



Tool Support for **All Stakeholders** in the **Entire CC Life Cycle**:

- ✓ Better documents quality → Shorter certification cycle
- ✓ Well-structured evidences → Appropriate test sampling
- ✓ Used for PP development & evaluation

Your Trusted Partner

Outline

- ✓ Introduction
- ✓ Model-Driven CC Analysis Tool
- ➢ **Structured & Guided CC VA Framework**
- ➢ Threat-Driven MD PP Development
- ➢ Conclusions

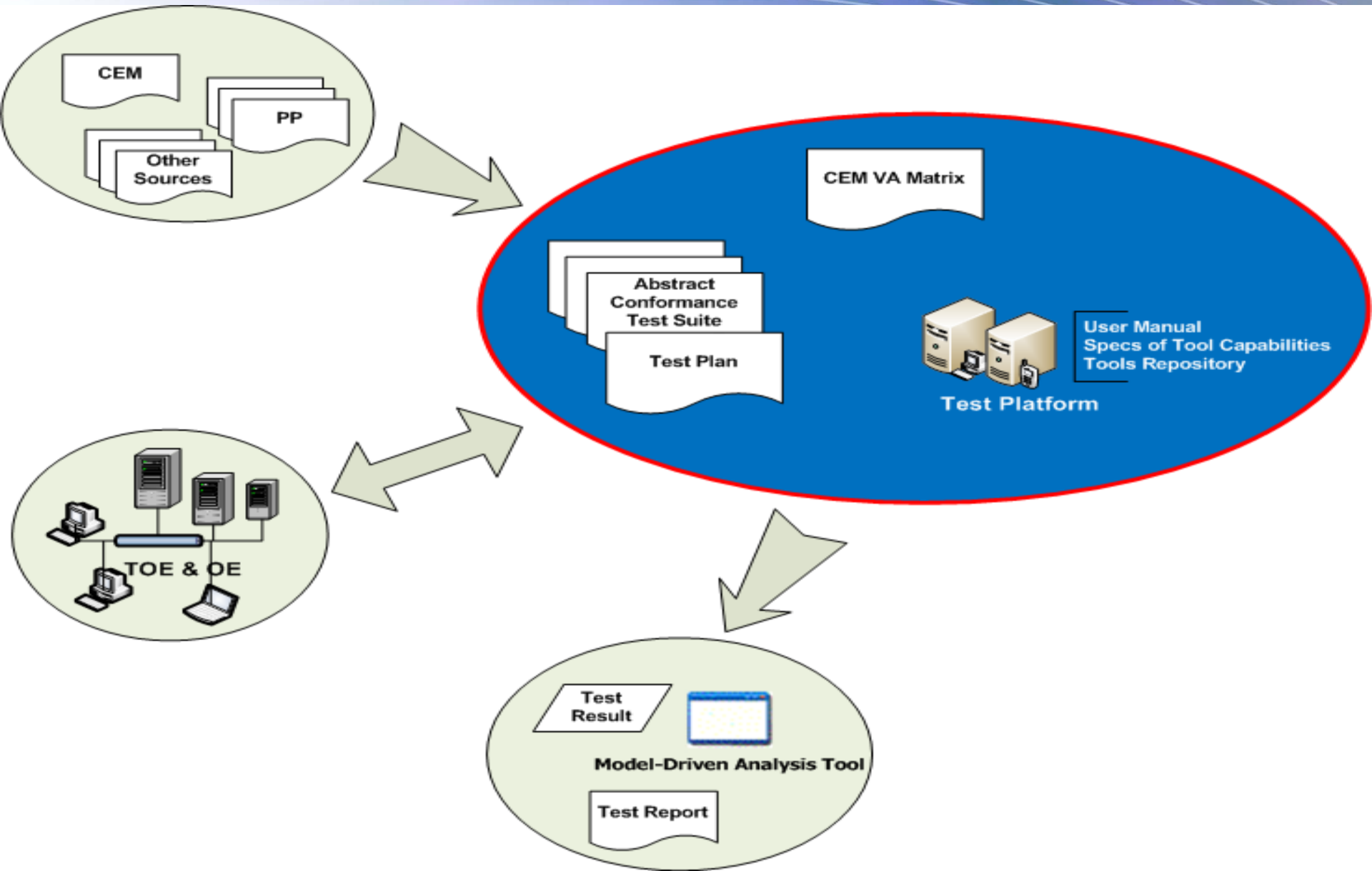
Your Trusted Partner

Structured & Guided CC VA Framework

- An EWA-Canada IR&D project to support VA in CC lab
  - focusing on **what** to test & **how** to test
- Presented at the 4th CCUF-CCDB Workshop
- "Structured" and "Guided"
  - Structured: Methodology vs. Goal, to achieve **repeatable** & **consistent** results
  - Guided: Compliant to CC (limited scope, conditional conclusions); to provide "**Ready-to-Use**" support
- A **Two-Layer** Structure
  - Conceptual Architecture
  - TOE Technology-specific implementation

Your Trusted Partner

CC VA Framework (Conceptual)



Implementation: CC VA for MD

- Generic vs. TOE Technology-specific
  - Generic: CEM VA Matrix
  - **TOE specific**: Test Requirements, Test Cases, Test Platform
- Defined Test Requirements
  - Source: CEM, MD PP, Web researches
  - Scope: **TOE**, and don't forget **OE**!
- **Abstract Test Suite** for mobile devices
  - Mobile OS & Firmware
  - Applications: native, Web-based
  - Network communications

Your Trusted Partner

Implementation: CC VA for MD (Cont'd)

- **Test Lab** for mobile device security testing
  - Based on open source technologies
  - **Capabilities**
    - Explore the file system on a mobile device
    - Intercept & manipulate web application traffic
    - Attack WiFi network, e.g. WPA dictionary attack, MITM attack
    - Static code analysis (reverse engineering)
    - and more …
- Structured & Guided: Test Requirement → **Test Design → Test Execution** → Test Analysis

Your Trusted Partner

Outline

- ✓ Introduction
- ✓ Model-Driven CC Analysis Tool
- ✓ Structured & Guided CC VA Framework
- ➢ **Threat-Driven MD PP Development**
- ➢ Conclusions

Your Trusted Partner

Threat-Driven MD PP Development

- The **Mobile Device PP TC** was established ~ **Nov 2010**
  - Consisting of a number of CBs, vendors, consultants, and labs
- The MD PP was under active development until the end of 2012
  - The latest **version 1.8** was internally released in Nov 2012
- It was then taken as the basis of the NIAP MD PP
- A Mobile "Space" Meeting was held at the 3rd CCUF-CCDB Workshop (May 2013, Ottawa Canada)

Your Trusted Partner

Threat-Driven MD PP Dev (Cont'd)

- Essentially, PP development is a practice of **Requirements Engineering**
  - **Elicit**: security problems, security requirements
  - **Analyze**: to clarify, classify & validate
  - **Specify**: using CC SFRs

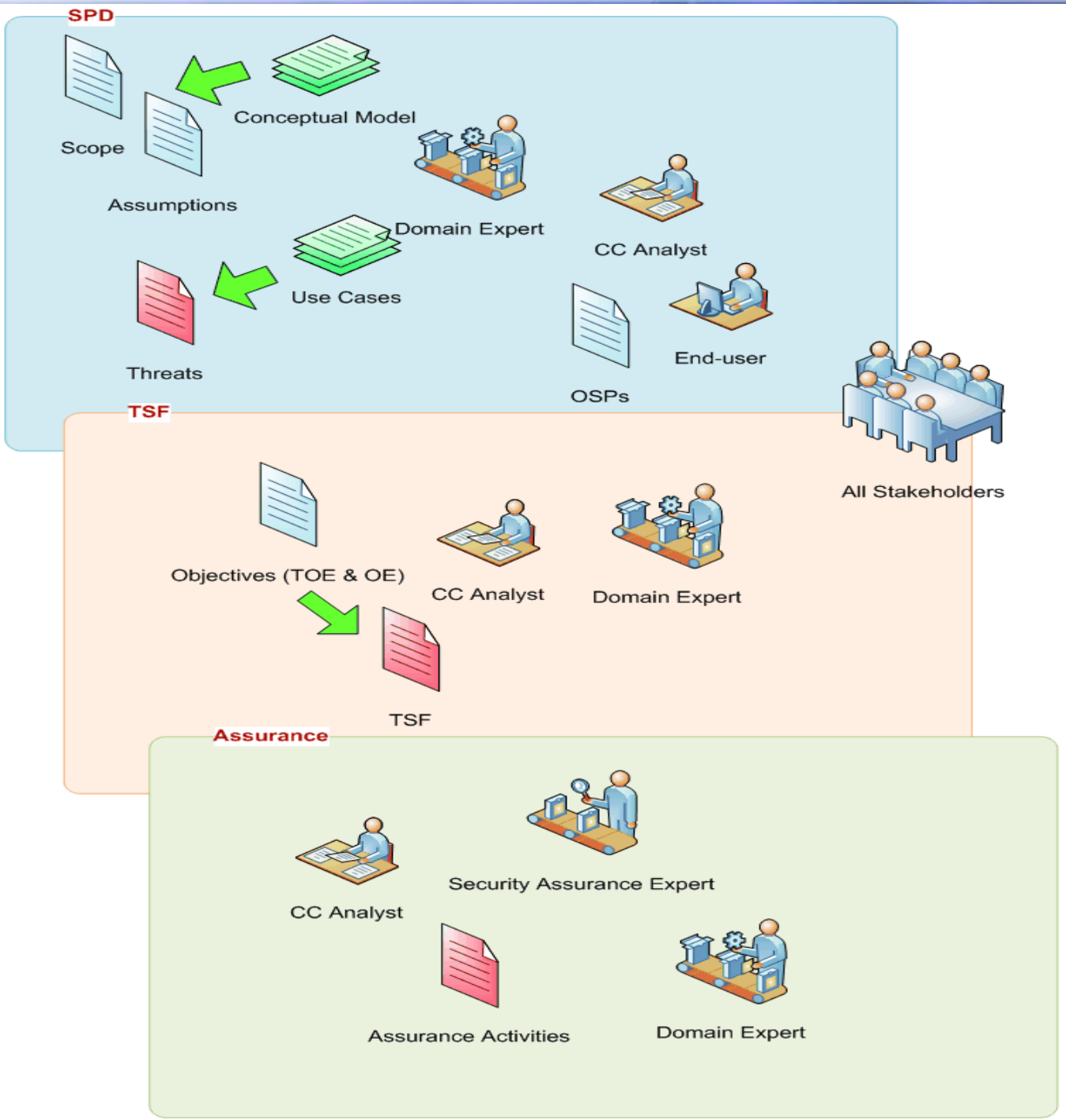
- **Particular challenges** to PP development
  - **Diversities** in a TC: different opinions
  - Obstacles to efficient **communication**
  - Limited **resources**: volunteer-based

Threat-Driven MD PP Dev (Cont'd)

- Understand the **Quality Criteria** for PPs: Consistent (Traceable), Self-justified (Rationale), Applicable & Feasible
- Identify **Key Artifacts** and their **Associations** in a PP
- **Conceptual Model**: establish **context** (scope, entities & relationships, assumptions) for problem domain
- **Use/Misuse Cases**: an efficient tool for system analysis: **elicit the threats** to the TOE and the protected assets
- **Threat-Driven Approach**: to **develop & justify SFRs**
- Specification of **Cryptographic SFRs** in a **CC scheme agnostic** way: acceptable to more nations

Enabling a More Secure Future

Process Artifacts Roles



Conclusions

- While CC & CEM provides a well-engineered framework for IT security evaluation, to date the application of engineering practices in CC cannot be considered adequate
- Shared our recent efforts in such engineering research & practices to address the long-standing concerns, in terms of:
  - **Formalization of Evaluation Evidence**
  - **Tool Support**
  - **Process Optimization**
- To provoke insightful thoughts and discussions in CC community; collaborate to pursue opportunities of further studies and practices in this field

Comments?

Contacts

Pulei Xiong, PhD
EWA-Canada
613-230-6067 x 1243
pxiong@ewa-canada.com

Mark Gauvreau
CC Lab Manager
EWA-Canada
613-230-6067 x 1222
mgauvreau@ewa-canada.com

Erin Connor
Director
EWA-Canada
613-230-6067 x 1214
econnor@ewa-canada.com

Your Trusted Partner