

# Application of Engineering “Best” Practices in Common Criteria

Pulei Xiong, PhD  
EWA-Canada  
September 12<sup>th</sup>, 2013

*Your Trusted Partner*

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

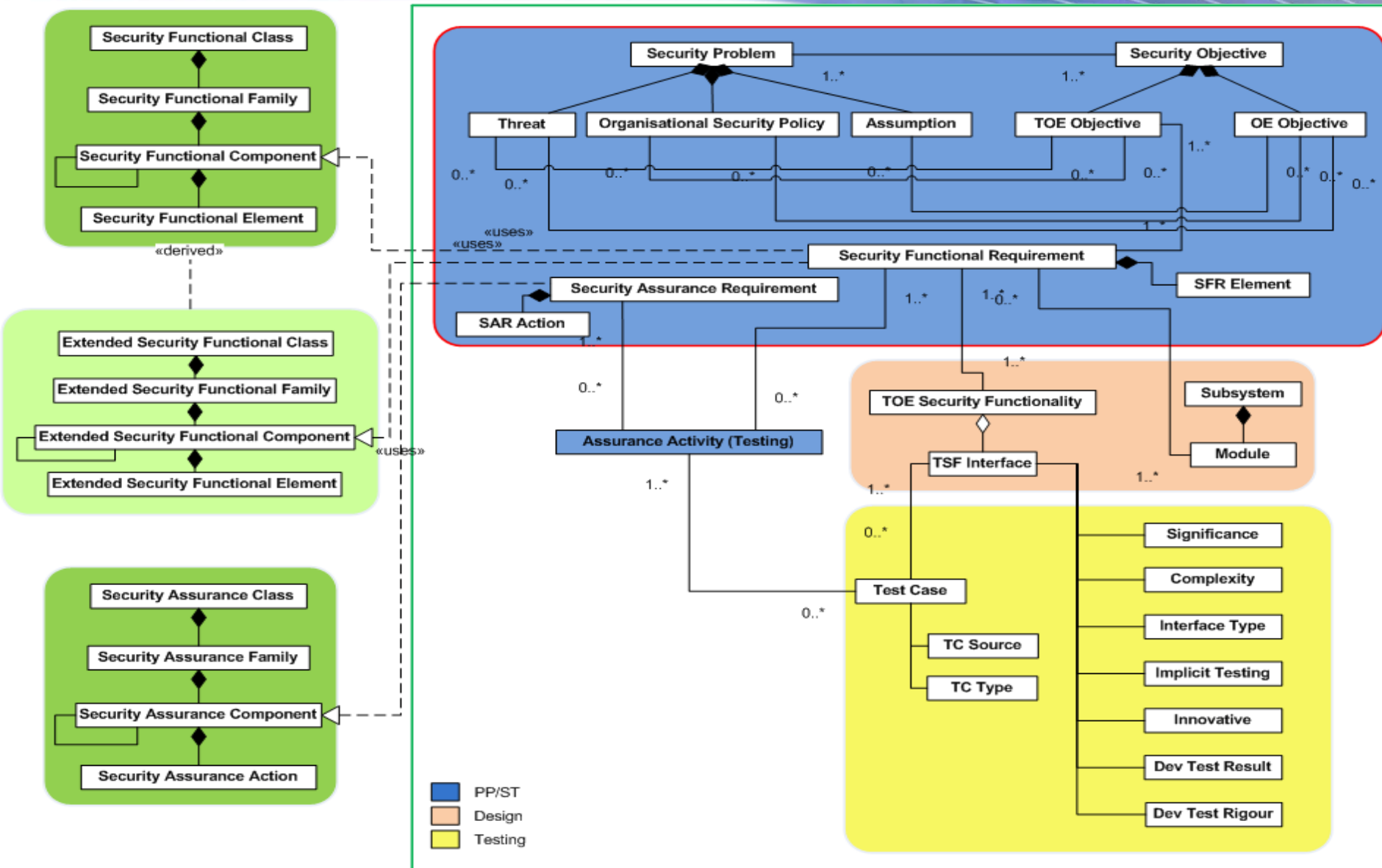
# Introduction

- 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

*Your Trusted Partner*

- 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

# Common Criteria Evaluation Model



# Java Program Screenshots

**CC Analysis and Testing Tool** [Project] [Analysis] [System] [Help]

**Threats**

- T.ADMIN\_ERROR
- T.MALICIOUS\_APPS
- T.NETWORK\_ATTACH
- T.NETWORK\_EAVESDI
- T.PHYSICAL\_ACCESS
- T.TSF\_FAILURE
- T.UNAUTHORIZED\_AC
- T.UNAUTHORIZED\_UF
- T.UNDETECTED\_ACTI
- T.USER\_DATA\_REUS

**Organization Security**

- P.ACCESS\_BANNER
- P.ADMIN
- P.DEVICE\_PROVISION
- P.NOTIFY

**Assumptions**

- A.CONNECTMITY
- A.MOBILE\_DEVICE\_P
- A.NO\_GENERAL\_PUR
- A.PHYSICAL
- A.PROPER\_ADMIN
- A.PROPER\_USER
- A.TIMESTAMP
- A.TRUSTED\_ADMIN

**SRC Test Case Coverage**

SFR to Test Case

Test Case - Tim
FTA_SSL.3 TSF-ini
Test Case - Per
FTA_SSL.4 User-ir
Test Case - Use
FTA_TAB.1 Default
Test Case - TOE
FTP_ITC.1 Inter-T
Test Case - HTI
FTP_TRP.1 Truste
Test case outstand

**TSFI Test Coverage**

TOE Security Functionality:

Test Case - Password C	
Test Case - User Identifi	
Test Case - User Authen	
Test Case - TOE Update	
Test Case - Period of Ina	
Test Case - User-initiate	
Test Case - TOE Banner	
Network interface	
Test Case - Audit Events	
Test Case - HTTPS/TLS	
Test Case - IPsec testing	
Test Case - Audit Server	
Test Case - Cryptograph	
Test Case - Cryptograph	
Test Case - Cryptograph	
Test Case - Cryptograph	
Test Case - Cryptograph	
Test Case - Cryptograph	
Test Case - TOE Update	

**Threats to SFR Document Review Analysis**

**Threats to TOE Security Functional Requirements**

T.ADMIN\_ERROR

FCS\_CKM.1 Cryptographic Key Generation (for asymmetric keys)

FCS\_COP.1(2) Cryptographic Operation (for cryptographic signature)

FCS\_COP.1(3) Cryptographic Operation (for cryptographic hashing)

T.TSF\_FAILURE

Threat outstanding

T.UNDETECTED\_ACTIONS

FAU\_GEN.1 Audit Data Generation

FAU\_GEN.2 User Identity Association

FPT\_STM.1 Reliable Time Stamps

T.UNAUTHORIZED\_ACCESS

FCS\_COP.1(1) Cryptographic Operation (for data encryption/decryption)

FCS\_COP.1(3) Cryptographic Operation (for cryptographic hashing)

FCS\_COP.1(4) Cryptographic Operation (for keyed-hash message authentication)

ETP\_ITC.1 Inter-TSF trusted channel

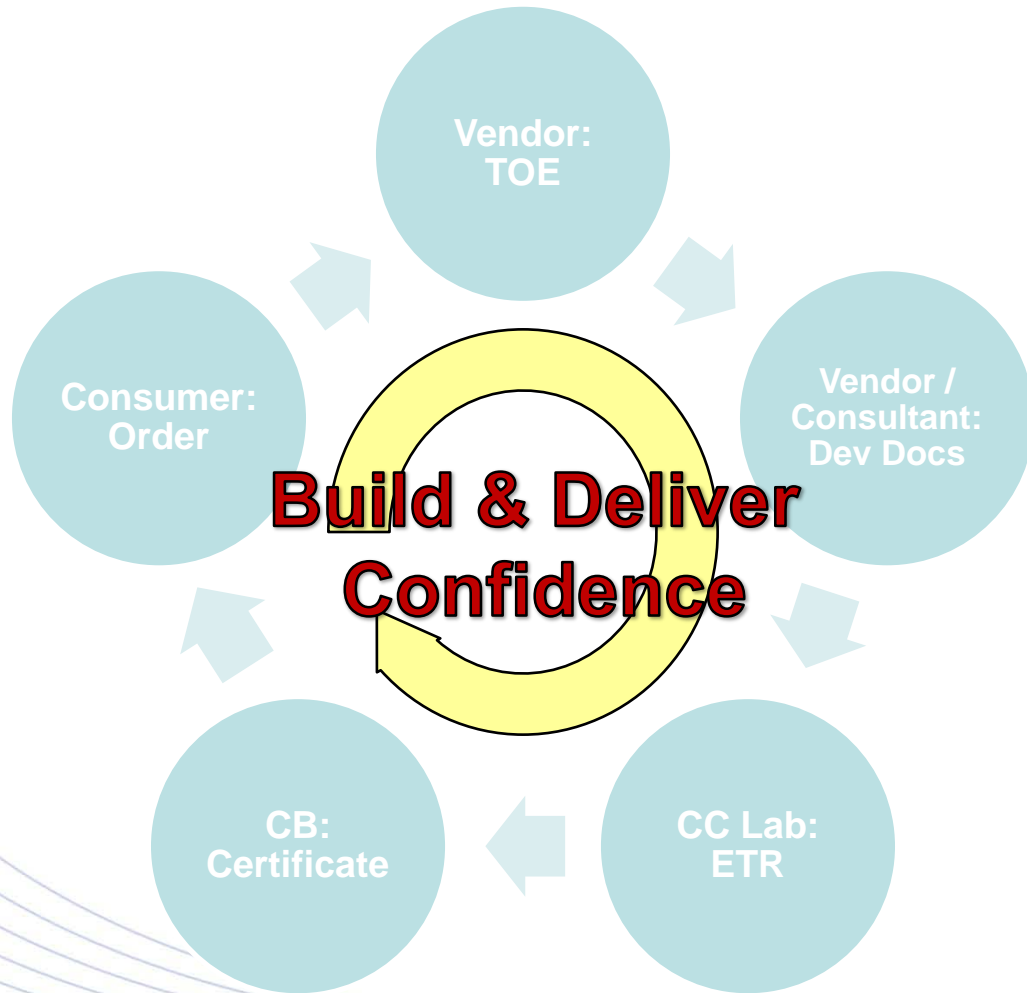
Security Problems | Security Objectives | TOE Security Functional Requirements | Modules and Subsystems | TOE Security Functionalities | Independent Testing

# 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 ...

*Your Trusted Partner*

# 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*



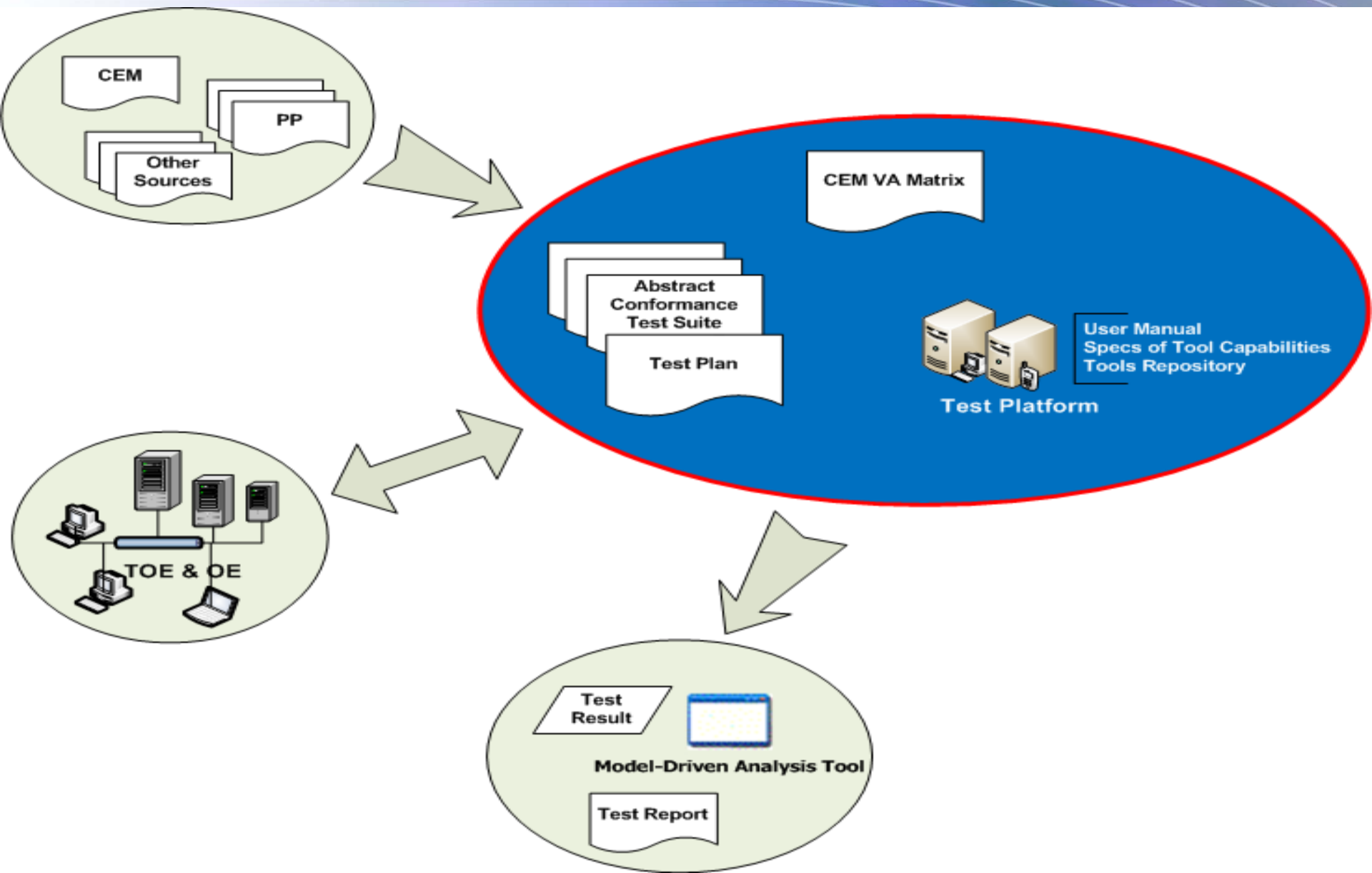
- ✓ Introduction
- ✓ Model-Driven CC Analysis Tool
- **Structured & Guided CC VA Framework**
- Threat-Driven MD PP Development
- Conclusions

# 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 4<sup>th</sup> 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)



- 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

- **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**

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

# 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 3<sup>rd</sup> CCUF-CCDB Workshop (May 2013, Ottawa Canada)

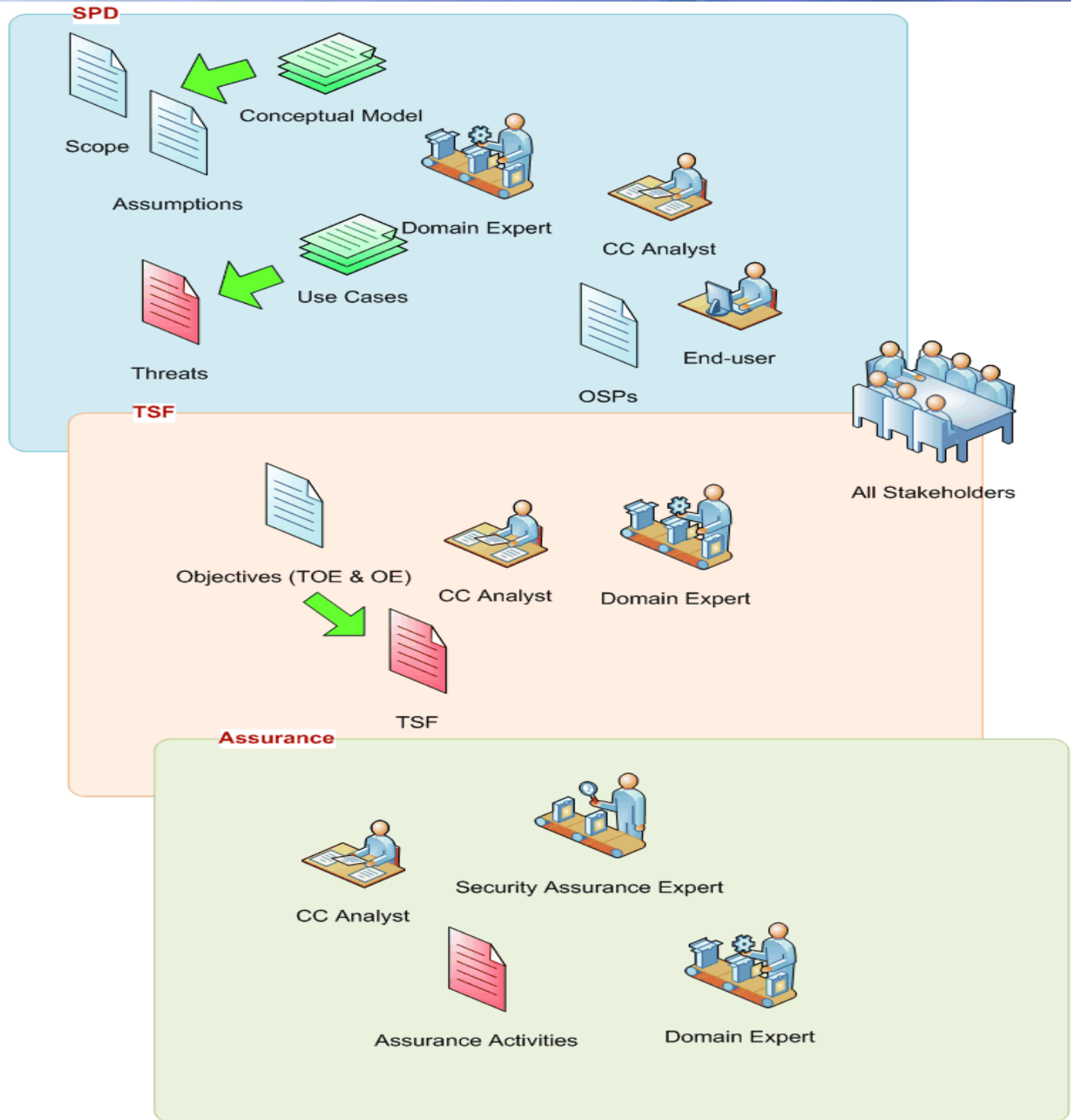
*Your Trusted Partner*

- 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



- 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

# 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](mailto:pxiong@ewa-canada.com)

### **Mark Gauvreau**

CC Lab Manager

EWA-Canada

613-230-6067 x 1222

[mgauvreau@ewa-canada.com](mailto:mgauvreau@ewa-canada.com)

### **Erin Connor**

Director

EWA-Canada

613-230-6067 x 1214

[econnor@ewa-canada.com](mailto:econnor@ewa-canada.com)

*Your Trusted Partner*