A Proposal for a COTS Assurance Package

Wesley H. Higaki

9th International Common Criteria Conference

Agenda

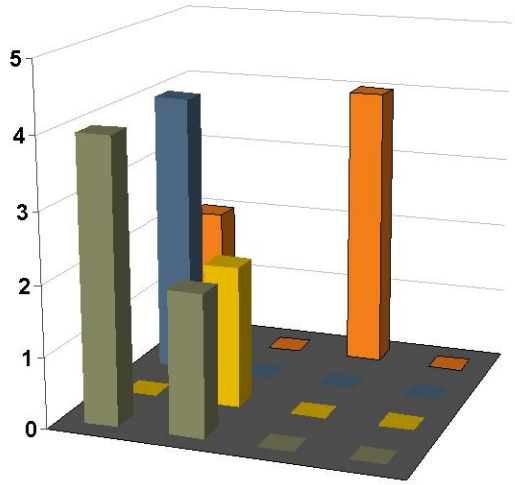
1. Background
2. Goals
3. Proposed Solution – COTS AP
4. Conclusions

Background

- Commercial off the shelf (COTS) products are frequently used in many critical information infrastructure systems
- Only a small percentage of those products undergo Common Criteria (CC) evaluation because…
  - Government mandates have not been effective in driving broader adoption
  - COTS vendors are driven by the commercial mass market
  - Mass market customers see no value in CC certification because it does not address their key issues

Greater Overall Assurance

Current

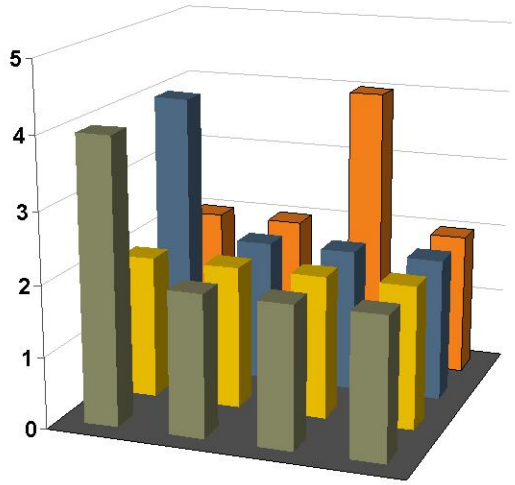


Today, few products are CC evaluated

$$\sum A_i = X$$

With lower total assurance

COTS AP



COTS AP offers more coverage

$$\sum A_i = Y$$

With greater total assurance

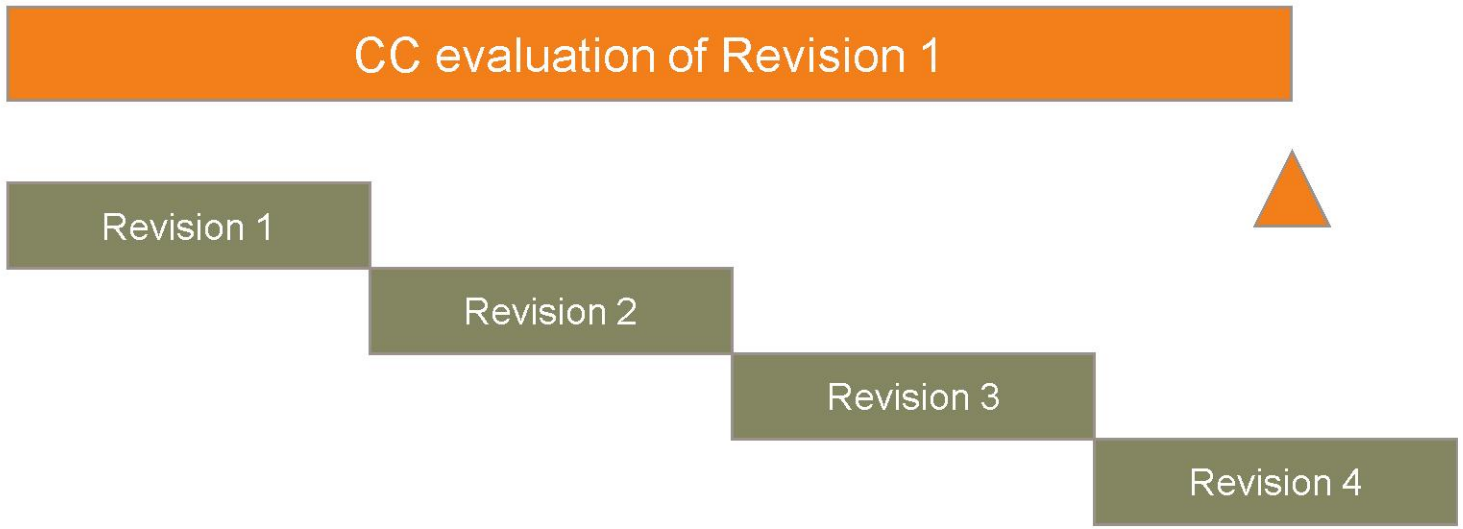
$$X << Y$$

Hypothesis

- If commercial mass market needs are addressed in CC evaluations
  - There would be greater demand for certifications and
  - More vendors would be motivated to submit products for evaluation
- Commercial mass market customers are concerned with:
  - Product code vulnerabilities exploitable by viruses, worms.
  - Software security patching
  - Product features that protect their data, systems and networks
- **CC evaluations need to address these concerns**

CC evaluations take too long

- CC evaluations take too long relative to product development cycles
- Products become obsolete by the time they are certified
- Not all product versions are able to be evaluated
- **Need to shorten evaluation time**



Goals of this Proposal

- Use the existing CC evaluation framework
  - International mutual recognition is a key benefit of CC
- Directly address the commercial mass market product security confidence concerns
- Significantly reduce the CC evaluation time and effort

Proposal

- Create a “COTS Assurance Package” including components from the following standard assurance classes:
  - ASE ST Evaluation
  - ALC Life-cycle support
  - ADV Development
  - AGD Guidance documents
  - ATE Tests
  - AVA Vulnerability analysis
- Modify the Common Evaluation Methodology (CEM) to focus evaluator efforts
- Introduce a new assurance class to address secure development
  - ASD Secure development

Why an Assurance Package?

- Provides the ability to combine assurance classes to address commercial customer needs
- Provides the opportunity to shorten evaluation times
- Allows augmentation to higher assurance
- **Consistent with existing CC framework**

COTS Assurance Package

- Starts with CC v3.1 EAL 2 as baseline
  - 52 work units unchanged
- 35 work units changed from “Examine” to “Check”
- 58 work units eliminated including:
  - ASE_ECD.1
  - ADV_FSP.2
  - ATE_IND.2
- Work units added include:
  - ALC_FLR.2
  - ASD_xxx
- Two levels developed
  - Basic
  - Augmented

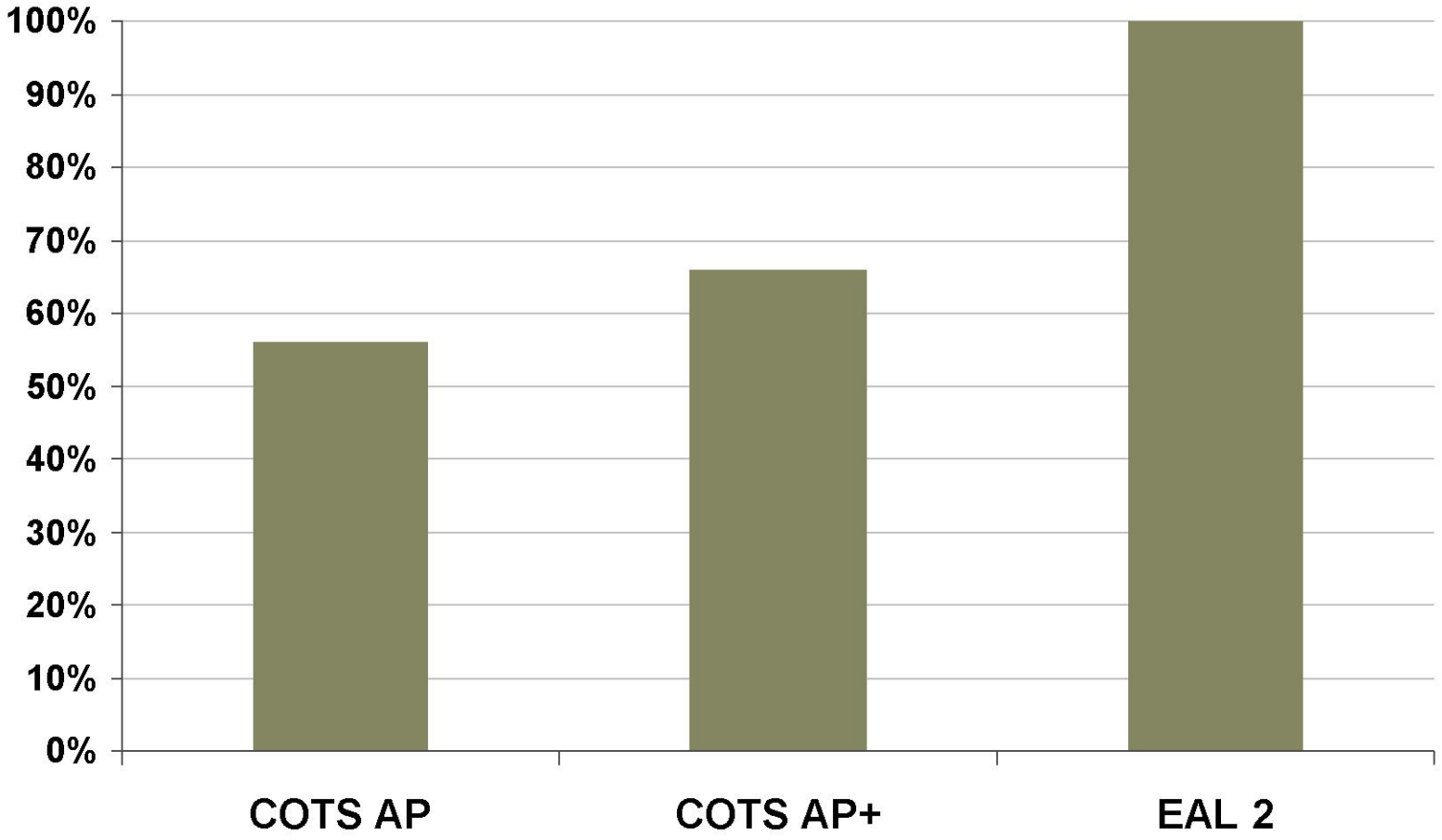
Modify Common Evaluation Methodology

- Reduce evaluator efforts to reduce time and effort
- Focus evaluator efforts on areas recognized as important to commercial customers
- Evaluator does not assess the quality of the vendor assurance measures
  - Quality is the role of the assurance class definition
  - Shifting emphasis in areas from “examine” to “check”

ASD Class

- The following assurance class is added to evaluate the secure software development processes:
  - ASD_TRA Security Training
  - ASD_REQ Security Requirements
  - ASD_DES Secure Design
  - ASD_IMP Secure Implementation
  - ASD_TST Security Testing
- Evaluation work units are added to cover this class
- **Addresses the mass market concerns for security**

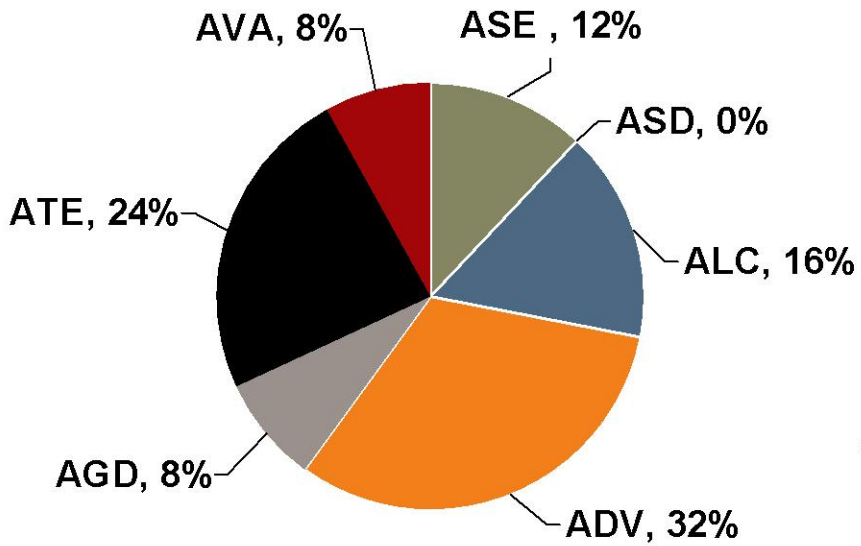
Relative Effort



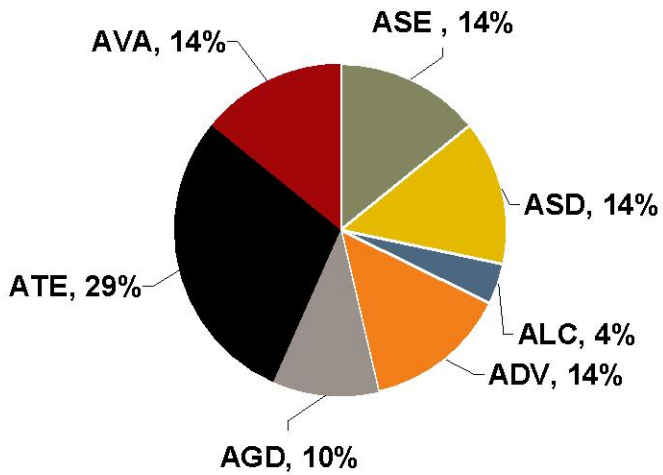
Reduces the evaluation time and effort

Evaluation Effort Comparison

EAL 2



COTS AP



Conclusions

- Addresses the needs of a broader customer base
- Encourages greater vendor participation
- Reduces evaluation time and effort
- Aligns evaluation timescale with product development
- Remains consistent with CC framework

Acknowledgements:

EWA-Canada

- Erin Connor
- Mark Gauvreau
- Grant Gibbs

Apex Assurance

- Ray Potter

Thank You!

Wesley H. Higaki

whigaki@symantec.com

+1 (650) 527-4701

Backup Slides

COTS AP Basic Details

1. ASE ST Evaluation
2. ASD Secure Development
   a) ASD_TRA Security Training [ASD_TRA.1]
   b) ASD_REQ Security Requirement [ASD_REQ.1]
   c) ASD_DES Secure Design [ASD_DES.1]
   d) ASD_IMP Secure Implementation [ASD_IMP.1]
   e) ASD_TST Security Testing [ASD_TST.1]
3. ALC Life-cycle support
   a) ALC_FLR Flaw remediation [ALC_FLR.2]
4. ADV Development
   a) ADV FSP Functional Specification [ADV_FSP.2]
5. AGD Guidance documents
   a) AGD_OPE Operational user guidance [AGD_OPE.1]
   b) AGD_PRE Preparative procedures [AGD_PRE.1]
6. ATE Tests
   a) ATE_COV Coverage [ATE_COV.1]
   b) ATE_FUN Functional testing [ATE_FUN.1]
   c) ATE_ IND Independent testing [ATE_IND.2]
7. AVA Vulnerability analysis
   a) AVA_VAN Vulnerability analysis [AVA_VAN.2]

COTS AP+ Details

1. ASE ST Evaluation
2. ASD Secure Development
   a) ASD_TRA Security Training [ASD_TRA.1]
   b) ASD_TRA Security Training Improvement [ASD_TRA.2]
   c) ASD_REQ Security Requirement [ASD_REQ.1]
   d) ASD_DES Secure Design Procedures [ASD_DES.1]
   e) ASD_DES Attack Surface Analysis [ASD_DES.2]
   f) ASD_DES Threat Modeling [ASD_DES.3]
   g) ASD_DES Risk Assessment [ASD_DES.4]
   h) ASD_DES Cryptographic Usage[ASD_DES.5]
   i) ASD_IMP Secure Implementation Procedures [ASD_IMP.1]
   j) ASD_IMP Secure Language [ASD_IMP.2]
   k) ASD_IMP Static Analysis [ASD_IMP.3]
   l) ASD_TST Security Test Procedures[ASD_TST.1]
   m) ASD_TST Fuzz Testing [ASD_TST.2]
   n) ASD_TST Penetration Testing [ASD_TST.3]

COTS AP+ Details (cont.)

3. ALC Life-cycle support
   a) ALC_FLR Flaw remediation: Flaw reporting procedures [ALC_FLR.2]
   b) ALC_CMC CM capabilities: Use of a CM system [ALC_CMC.2]
   c) ALC_CMS CM scope: Parts if the TOE CM coverage [ALC_CMS.2]
   d) ALC_DEL Delivery: Delivery procedures [ALC_DEL.1]
   e) ALC_DVS Development security: Identification of security measures [ALC_DVS.1]
   f) 3.6 f. ALC_TAT Tools & Techniques: Well-defined development tools [ALC_TAT.1]
4. ADV Development
   a) ADV-ARC Security Architecture: Security architecture description [ADV_ARC.1]
   b) ADV FSP Functional Specification [ADV_FSP.2]
   c) ADV_TDS TOE design: Basic design [ADV_TDS.1]
5. AGD Guidance documents
   a) AGD_OPE Operational user guidance [AGD_OPE.1]
   b) AGD_PRE Preparative procedures [AGD_PRE.1]
6. ATE Tests
   a) ATE_COV Coverage [ATE_COV.1]
   b) ATE_FUN Functional testing [ATE_FUN.1]
   c) ATE_ IND Independent testing [ATE_IND.2]
7. AVA Vulnerability analysis
   a) AVA_VAN Vulnerability analysis [AVA_VAN.2]

Evaluation Effort Comparison