



Composed TOE Lessons Learned

11th ICCC Turkey

Eric Winterton
CCTL Director
21 September 2010

This document is confidential and is intended solely for the use and information of the client to whom it is addressed.

Table Of Contents

- ▶ Background
- ▶ Issues
- ▶ Results
- ▶ Recommendations

Background

- ▶ Background
- ▶ Issues
- ▶ Results
- ▶ Recommendations

Definition of ACO

- ▶ Common Criteria Part 3 v3.1r3, July 2009 Paragraph 469
 - *“...Involves taking two or more IT entities successfully evaluated ... and combining them for use, with no further development of either IT entity.”*

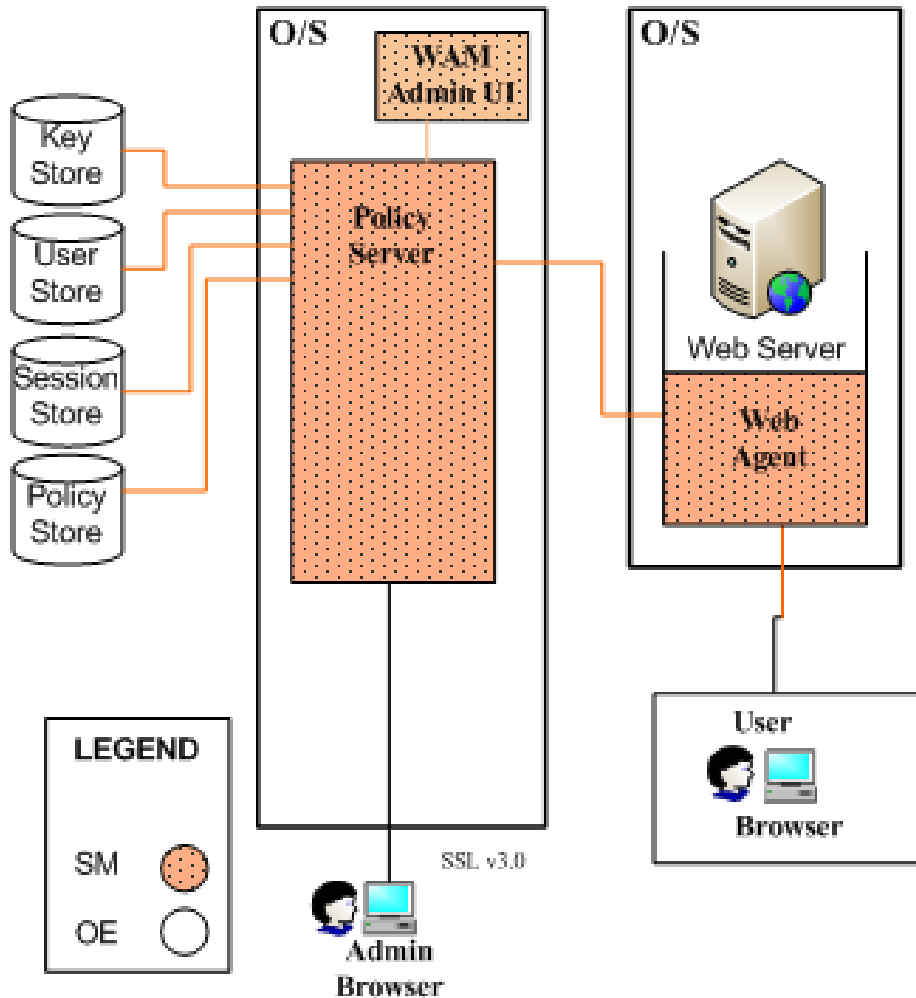
- ▶ Common Criteria Part 3 v3.1r3, July 2009 Paragraph 470
 - *“Provides a ... method ... to gain confidence in a TOE that is the combination of two or more successfully evaluated components without having to re-evaluate the composite TSF”*

- ▶ Common Criteria Part 3 v3.1r3, July 2009 Paragraph 471
 - *“...Reuse can be made of the component TOE evaluation results...”*

- ▶ TCSEC, *“Turning Multiple Evaluated Products into Trusted Systems”* July 1994
 - *“Assurance that modified mechanisms and interfaces perform as intended and that the overall security has not been diminished”*

Common Criteria Part 3 v3.1r3, July 2009

Base Component - CA Siteminder Web Access Manager r12 SP1-CR3



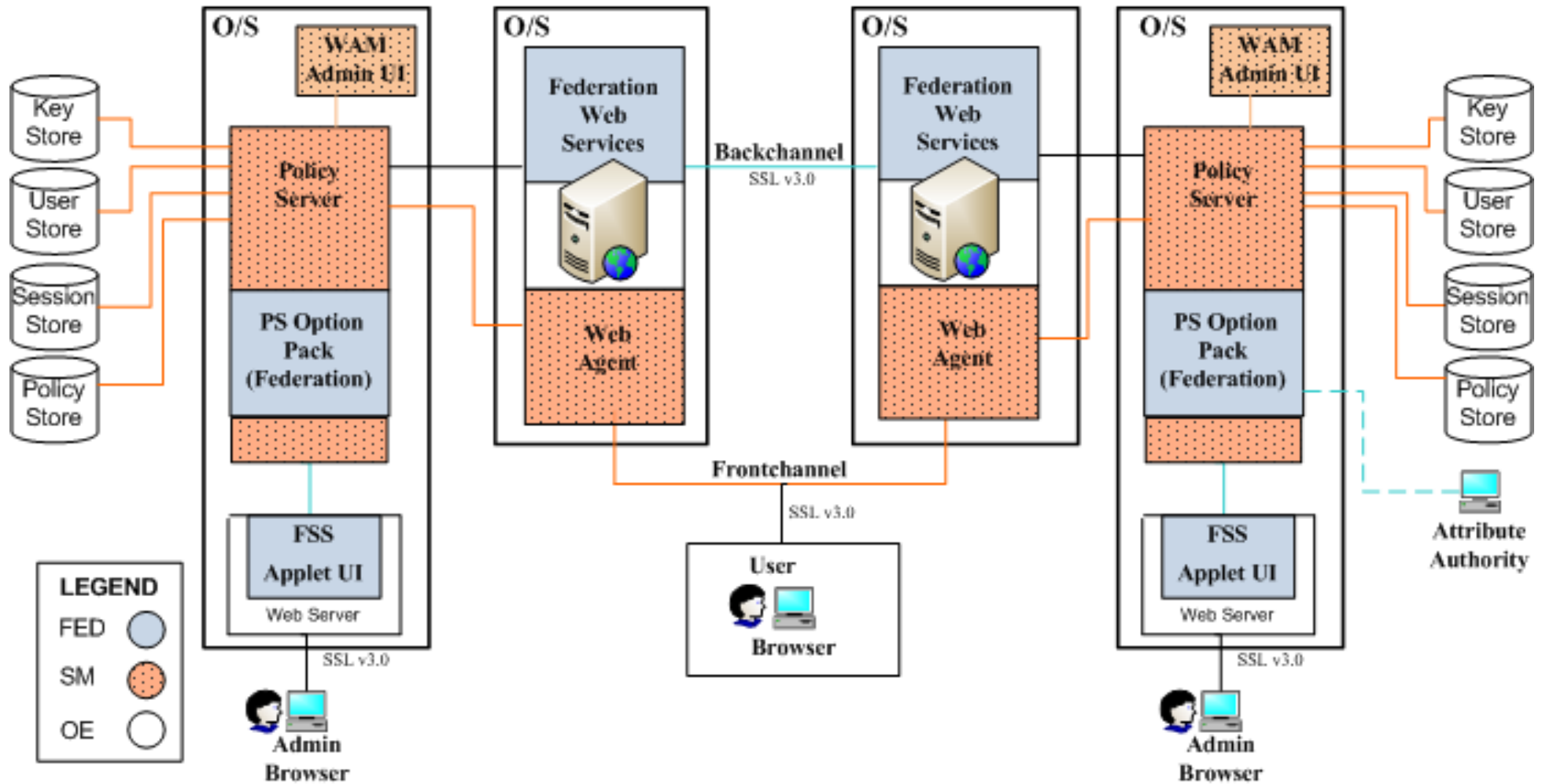
CA SiteMinder Federation Security Services r12 sp1 CR3

Asserting Party

Service Provider/Consumer

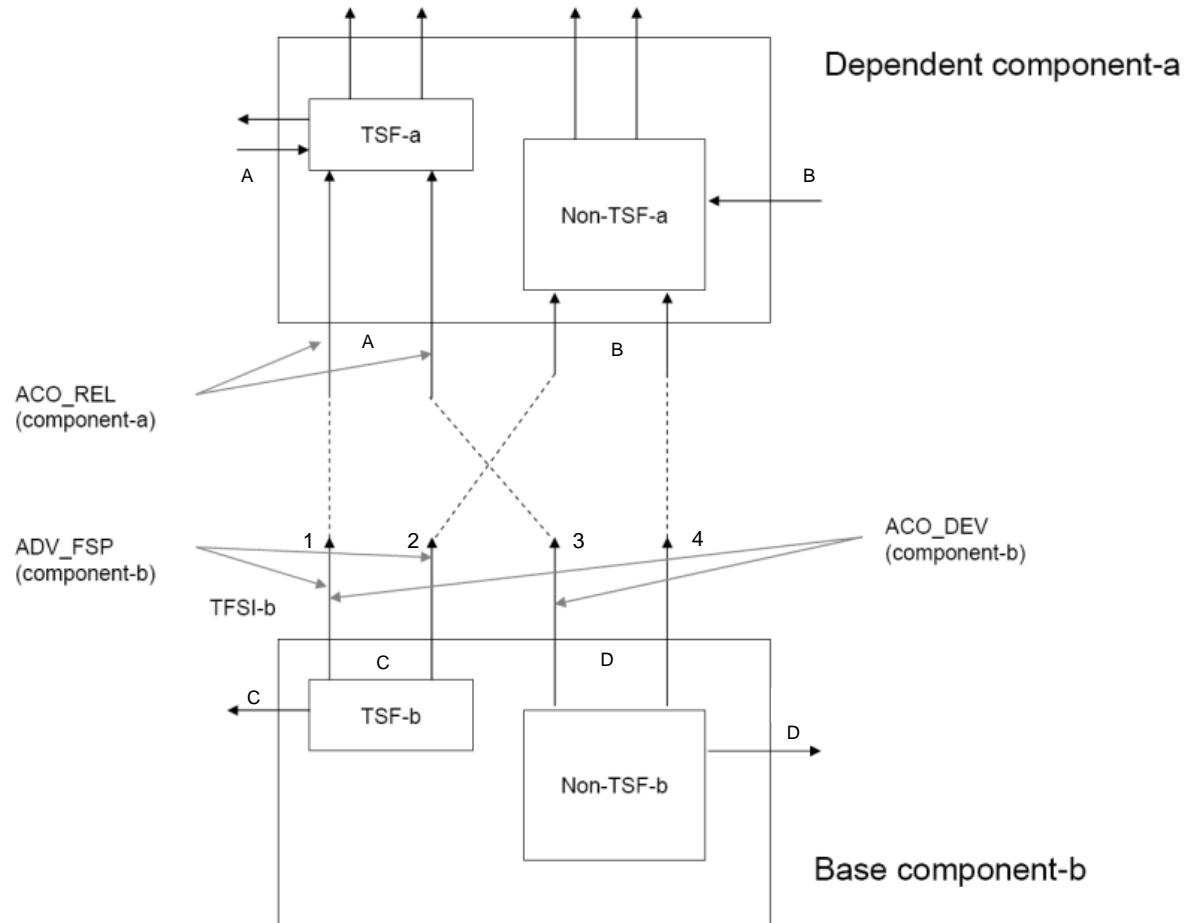
Relying Party

Identity Provider/Producer



ACO treats internal interfaces like external interfaces

- ▶ ACO_REL similar to ADV_FSP
- ▶ ACO_DEV similar to ADV_TDS
- ▶ ACO_CTT similar to ATE
- ▶ ACO_VUL similar to AVA



Issues

- ▶ Background
- ▶ Issues
- ▶ Results
- ▶ Recommendations

Two Types of Composed TOE's

- ▶ Two entities that can function independently of each other
 - The expectation of Composition is that both entities have already been evaluated as independent TOEs
 - The entities combination as a composed TOE will now validate that the additional functionality and interfaces provided as a combined evaluation will be in itself secure, and will not invalidate the previous evaluations.
 - Validate the configurations for the individual TOEs have not changed
 - Validate composite of the TOEs does not introduce any vulnerabilities
 - E.g., sensor/scanner (base component) and an analyzer (dependent component) in an IDS/IPS

- ▶ Two entities where one entity (dependent component) cannot function without the other entity (base component)

Issues with two entities where one depends on the other

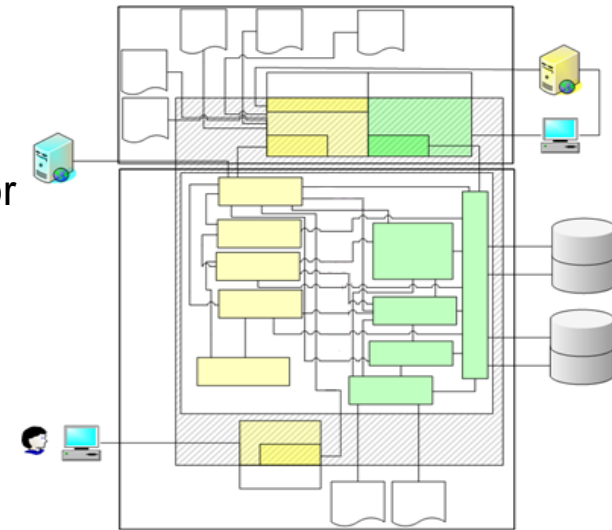
- ▶ Cannot validate the dependent component independently
- ▶ Current ACO requirements do not support this type of evaluation.
- ▶ ACO_DEV: Doesn't handle case of dependent component injecting data into the base component data flow. Had to map these composite interfaces to SFR's, and test cases.
- ▶ Still focused on external interfaces but had to extend:
 - SFR's/TSS description
 - Test Cases

Results

- ▶ Background
- ▶ Issues
- ▶ Results
- ▶ Recommendations

CA SiteMinder Federation Security Services r12 sp1 CR3 Evaluation Results

- ▶ Increased composition documentation and “composite” interface descriptions had notable cost and schedule impact
- ▶ Client expectation that they would be rewarded for base component certification did not materialize
 - ADV evaluation, while relying on the base component evidence for a large portion, required a substantial amount of changes to incorporate ACO_DEV requirements
 - Base component tests needed to be re-executed because ACO_CTT required assurance that adding the dependent component did not “break” the original validated TOE
- ▶ Testing is repetitive



Recommendations

- ▶ Background

- ▶ Issues

- ▶ Results

- ▶ Recommendations

What do we really want from ACO?

- ▶ Ability to evaluate extended functionality of a vendors product
 - Maximizing reuse
 - Without retesting the old product again
 - Analysis to support overall security
- ▶ System evaluation for use by Common Criteria customers (i.e., System Integrators and Certification & Accreditation professionals)

OPTION 1: Modify the ACO requirements to evaluate extended product functionality

- ▶ No new vulnerabilities were discovered by performing ACO work units
- ▶ Modify existing policies to allow for these types of evaluations without adding additional burden to the vendor's
 - Do not retest base component (only deltas)
 - Treat interfaces to base component like FSP interfaces
 - Proper analysis and SFR mapping should minimize cost

OPTION 2: Modify ACO requirements to complement C&A Processes

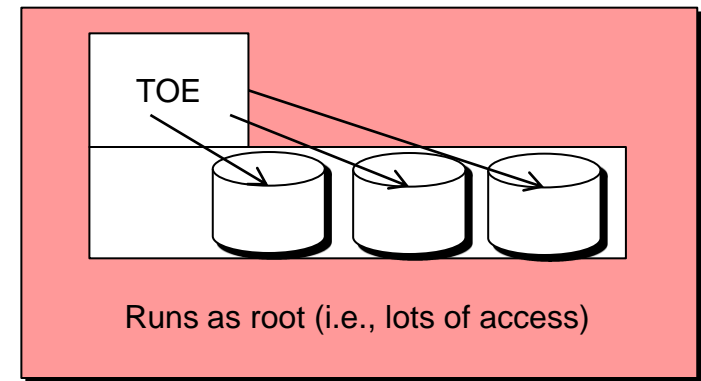
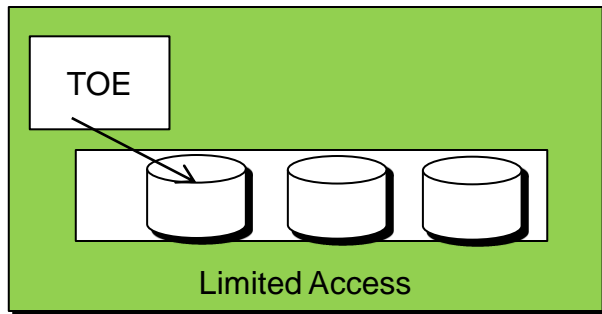
- ▶ Focus on risk
 - TCSEC states, “Security testing of the system, as with all assurance activities, is performed to support a certification and accreditation, and not an evaluation, of the system.”
 - In other words what is the risk of using this product
- ▶ Give credit to Vendor’s for using architectures and implementations that are less risky
- ▶ Create new architecture requirements that are consistent with accreditation risk models. (i.e., create a risk rating instead of a pass/fail)

Running At Reduced Permissions

- Software developers commonly require their software to be given permissions not needed to fulfill its intended function.

e.g., run as root

- Administrators often grant software these permissions during install to avoid potential software conflicts
- Software running at high permissions introduces greater risk if it is somehow subverted
- Least privilege should apply to software as well as users
- SW should not be assumed to always behave properly



In Conclusion

- ▶ ACO is a good idea just not in it's current implementation
- ▶ Current ACO requirements don't achieve documented goals as is:
 - Little reuse was achieved
 - Further development of base component was necessary to meet requirements of ACO
 - Significant focus was put on composite TSF
- ▶ Need to revise ACO
 - OPTION 1: Modify ACO requirements to evaluate extended product functionality
 - OPTION 2: Modify ACO requirements to complement C&A Processes
- ▶ Is there an OPTION 3?
- ▶ The Common Criteria Community should create a working group to suggest revisions to the ACO requirements to help the Government clients who buy CC products.

Questions

