APPLYING COMMON CRITERIA TO SERVICE ORIENTED ARCHITECTURES

Samuel Paul Kaluvuri
(SAP)

Michele Bezzi
(SAP)

Antonino Sabetta
(SAP)

Yves Roudier
(Eurecom)

Renato Menicocci
(FUB)

Vittorio Bagini
(FUB)

Alessandro Riccardi
(FUB)

Massimiliano Orazi
(FUB)

INTERNATIONAL COMMON CRITERIA CONFERENCE 2012, PARIS

AGENDA

- Changes in software provisioning models based on SOA
- Challenges in Applying CC to the new software provisioning models
  - Assurance of Operational Environment
- Proposed Solution
  - Assurance of IT Parts of Operational Environment
  - Assurance of Non-IT Parts of the Operational Environment
- Conclusions
- Future Work

AGENDA

- **Changes in software provisioning models based on SOA**
- Challenges in Applying CC to the new software provisioning models
  - Assurance of Operational Environment
- Proposed Solution
  - Assurance of IT Parts of Operational Environment
  - Assurance of Non-IT Parts of the Operational Environment
- Conclusions
- Future Work

CONTEXT

- Paradigm shift in software provisioning and consumption models
- Facilitated by Service Oriented Architectures (SOA)
  - Gmail, Dropbox, SAP ByDesign enjoy immense popularity
  - Offer enormous benefits to consumers and providers
  - Offers large scale inter-organizational inter-operability
- However, Security concerns are hampering a much wider adoption of SOA based solutions
- Common Criteria Certification can provide the required security assurance, however there are some challenges in applying CC certification to SOA

TRADITIONAL SOFTWARE PROVISIONING MODEL

- How is software consumed until now?
  - An organization that needs an IT solution delegates the responsibility to the IT department
  - The IT department searches for a suitable IT product from available solutions
  - Deploys the Software Product in its IT Infrastructure
- In this Model:
  - The Software Consumer has control over the IT infrastructure of an organization
  - The Software Consumer has control over the IT related processes that are put in place in an organization

COMMON CRITERIA IN TRADITIONAL SOFTWARE PROVISIONING MODELS

- How is software consumed until now?
  - An organization that needs an IT solution delegates the responsibility to the IT department
  - The IT department searches for a suitable IT product from available CC certified solutions
  - Deploys the Software Product in its IT Infrastructure
  - Realizes an operational environment consistent with the security target of the CC certified product (by configuring the IT infrastructure and the IT related processes and other

SERVICE ORIENTED ARCHITECTURES

- Software provided as “service”
- Facilitates on-demand, off-premise software solutions
- Services consumed through interfaces that are exposed – hides the internal dynamics of the software and its underlying architecture
- Consumers are relieved of the complexity of procuring and maintaining IT infrastructures

SOA BASED SOFTWARE PROVISIONING MODEL

- ❑ How can a service be consumed?
  - ❑ An organization that needs an IT solution delegates the responsibility to the IT department
  - ❑ The IT department searches for a suitable service from available services
  - ❑ Uses a thin client (application) to consume that particular service
- ❑ In this Model, the service consumer:
  - ❑ **Does not own** the IT infrastructure of a service provider
  - ❑ **Cannot control** IT related processes that are put in place by the service provider

COMMON CRITERIA IN SOA BASED PROVISIONING MODELS

- How is service consumed?
  - An organization that needs an IT solution delegates the responsibility to the IT department
  - The IT department searches for a suitable service from available CC certified services
  - Uses a thin client (application) to consume that particular service
  - However, it **CANNOT** realize an operational environment consistent with the security target of the CC certified product (since it can **NEITHER** configure the IT infrastructure **NOR** the IT related processes nor other)

AGENDA

- Changes in software provisioning models based on SOA
- **Challenges in Applying CC to the new software provisioning models**
  - **Assurance of Operational Environment**
- Proposed Solution
  - Assurance of IT Parts of Operational Environment
  - Assurance of Non-IT Parts of the Operational Environment
- Conclusions
- Future Work

CHALLENGES IN APPLYING CC TO SOA

- No Common Criteria certified services available
- Some of the major reasons are :
  - CC certification is expensive and does not justify the Return of Investment (ROI) for service based applications – as of now
  - Does not tackle the service-specific needs
- Few of the service specific requirements for applying CC are:
  - Contribute to provide assurance for the correctness Operational Environment of a service
  - Adapting to Dynamic Landscapes where Service Environments could change frequently

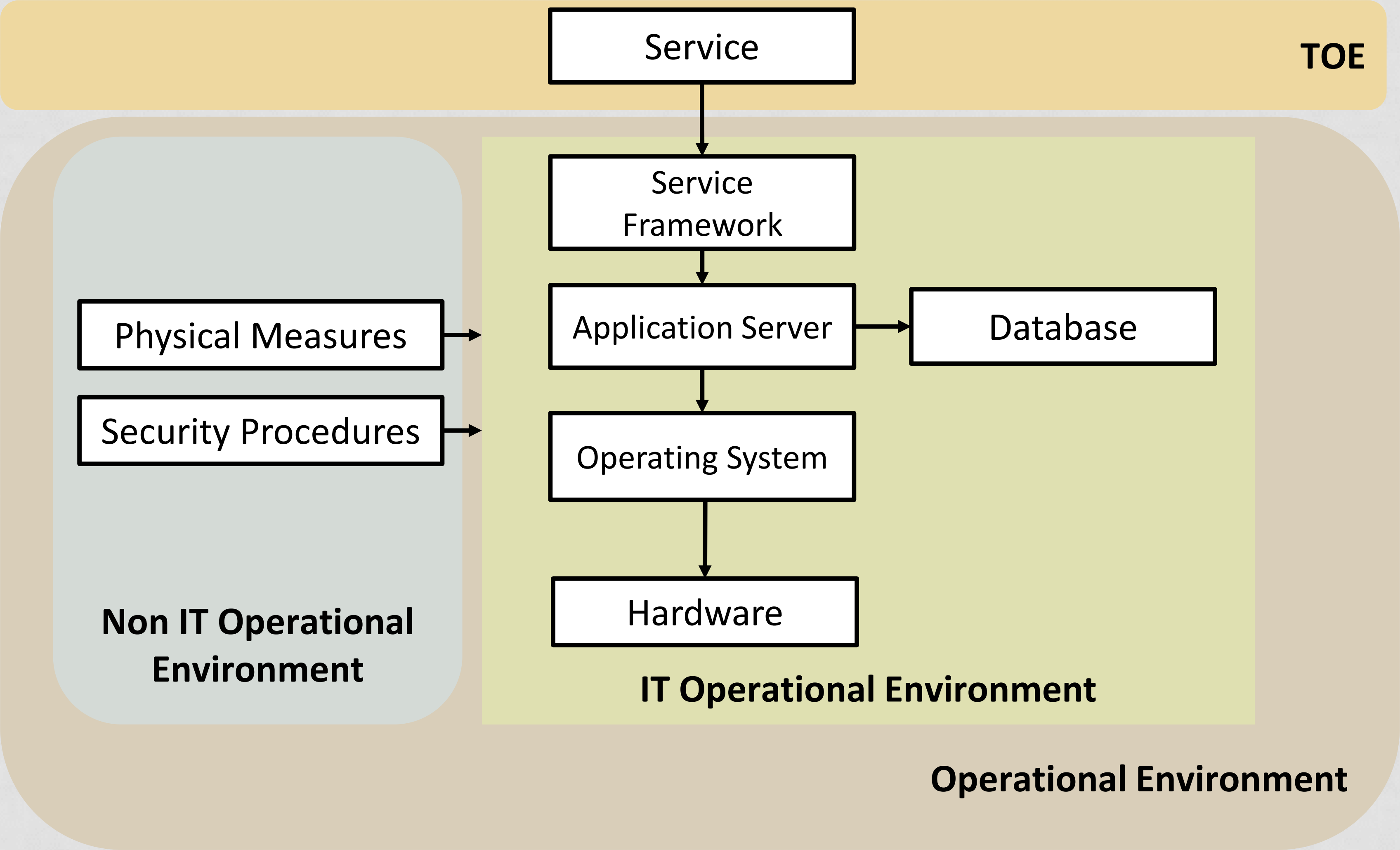
CHALLENGES IN APPLYING CC TO SOA

- No Common Criteria certified services available
- Some of the major reasons are :
  - CC certification is expensive for on-demand, off-premise solutions, whose market does not make it viable to spend hundreds of thousands of euros to acquire certification
  - Does not tackle the service-specific needs
- Few of the service specific requirements for applying CC are:
  - Contribute to provide assurance for the correctness Operational Environment of a service
  - Adapting to Dynamic Landscapes where Service Environments could change frequently *(outside the scope of this presentation)*

OPERATIONAL ENVIRONMENT OF A SERVICE

- Operational Environment
  - Environment in which the TOE is operated [CCp1]
  - Assumed to be a 100% correct instantiation of the security objectives for the operational environment [CCp1]
  - Correctness verification is left to the consumer
- IT Operational Environment: HW/SW/FW components that realize the IT part of the SO for the OE
  - For the rest of the presentation we assume that the non-TOE required HW/SW/FW contains all the components needed to realize the IT portion of the SO for the OE
- Non-IT Operational Environment: Security procedures and physical measures put in place to realize the non-IT part of the SO for the OE

OPERATIONAL ENVIRONMENT – SIMPLIFIED EXAMPLE



TOE

Service

Service Framework

Physical Measures

Application Server

Database

Security Procedures

Operating System

Hardware

Non IT Operational Environment

IT Operational Environment

Operational Environment

AGENDA

- Changes in software provisioning models based on SOA
- Challenges in Applying CC to the new software provisioning models
  - Assurance of Operational Environment
- **Proposed Solution**
  - **Assurance of IT Parts of Operational Environment**
  - **Assurance of Non-IT Parts of the Operational Environment**
- Conclusions
- Future Work

PROPOSED SOLUTION

- Provide meaningful security assurance to the service consumer for both:
  - The Service
  - And the **correctness** of its Operational Environment that includes both:
    - IT part of the OE
    - Non IT part of the OE

PROPOSED SOLUTION

- Provide meaningful security assurance to the service consumer for both:
  - **The Service**
  - And the **correctness** of its Operational Environment that includes both:
    - IT part of the OE
    - Non IT part of the OE

SECURITY ASSURANCE OF THE SERVICE

- ❑ The "service" corresponds to the CC-TOE
- ❑ The Security Functional Requirements (SFR) that are prescribed in the Common Criteria V3.1 might be sufficient to provide the required assurance on the CC-TOE
- ❑ A deeper analysis should be performed to evaluate if extended SFRs (foreseen by CC) need to be introduced specifically for services
- ❑ For the rest of the discussion, we assume that the current set of SFRs are sufficient

PROPOSED SOLUTION

- Provide meaningful security assurance to the service consumer for both:
  - The Service
  - And the **correctness** of its Operational Environment that includes both:
    - IT part of the OE
    - Non IT part of the OE

ASPECTS TO CONSIDER TO MAKE CC PROVIDING ASSURANCE ON THE OE CORRECTNESS

Conceptual

- ❑ CC tailored for traditional software provisioning models, where consumer has control over OE
- ❑ Non IT security processes are outside the scope of CC certification
- ❑ Since CC Security Objectives for OE and for the TOE are stated in a ad-hoc manner, there is no common vocabulary

Application

- ❑ CC Security Objectives for OE are expressed in natural language and hence:
  - ❑ Difficult to identify key elements such as assets, actions etc.,
  - ❑ Difficult to compare SO's coming from different Security Targets (Such as the Security Target of a Service with the Security Target of a part of the service's IT Operational Environment)

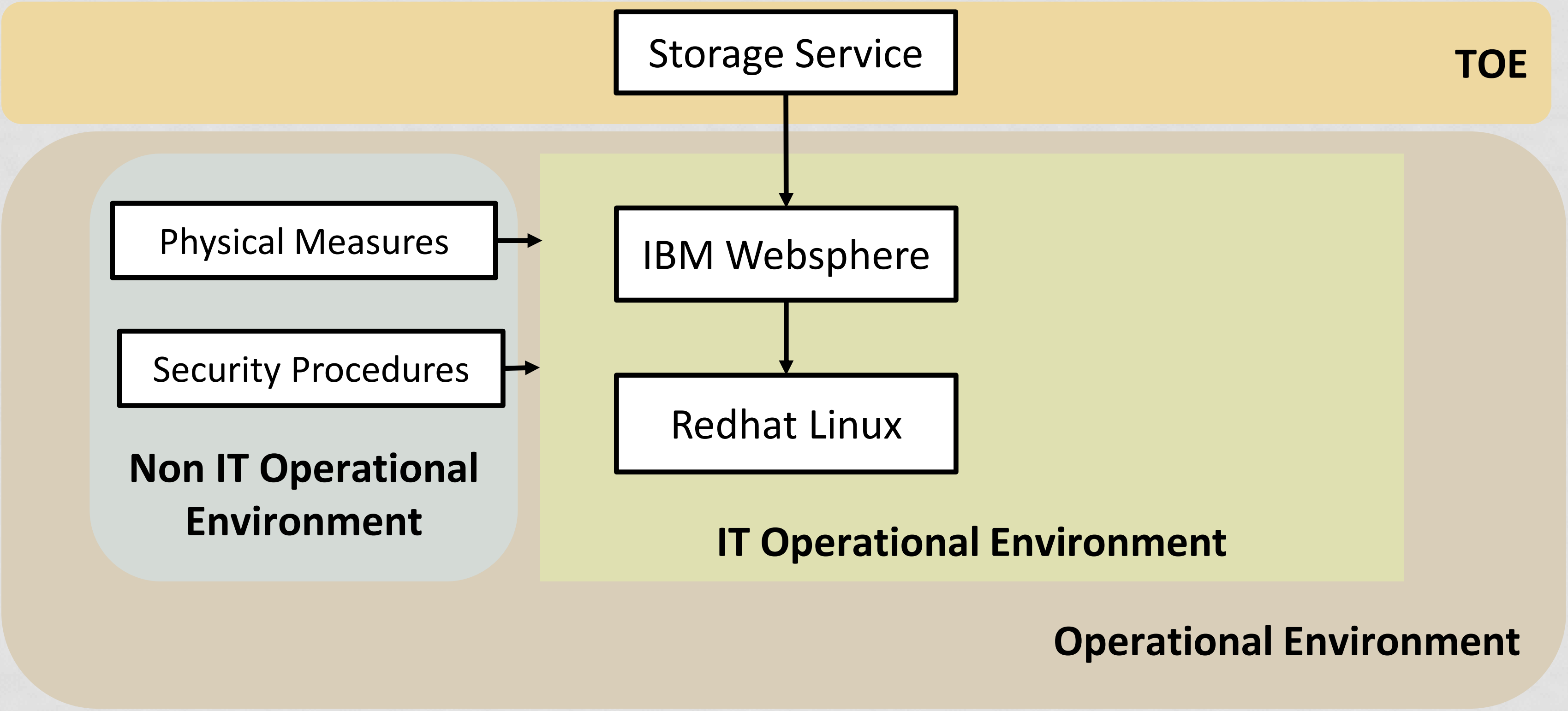
PROPOSED SOLUTION

- Provide meaningful security assurance to the service consumer for both:
  - The Service
  - And the **correctness** of its Operational Environment that includes both:
    - IT part of the OE
    - Non IT part of the OE

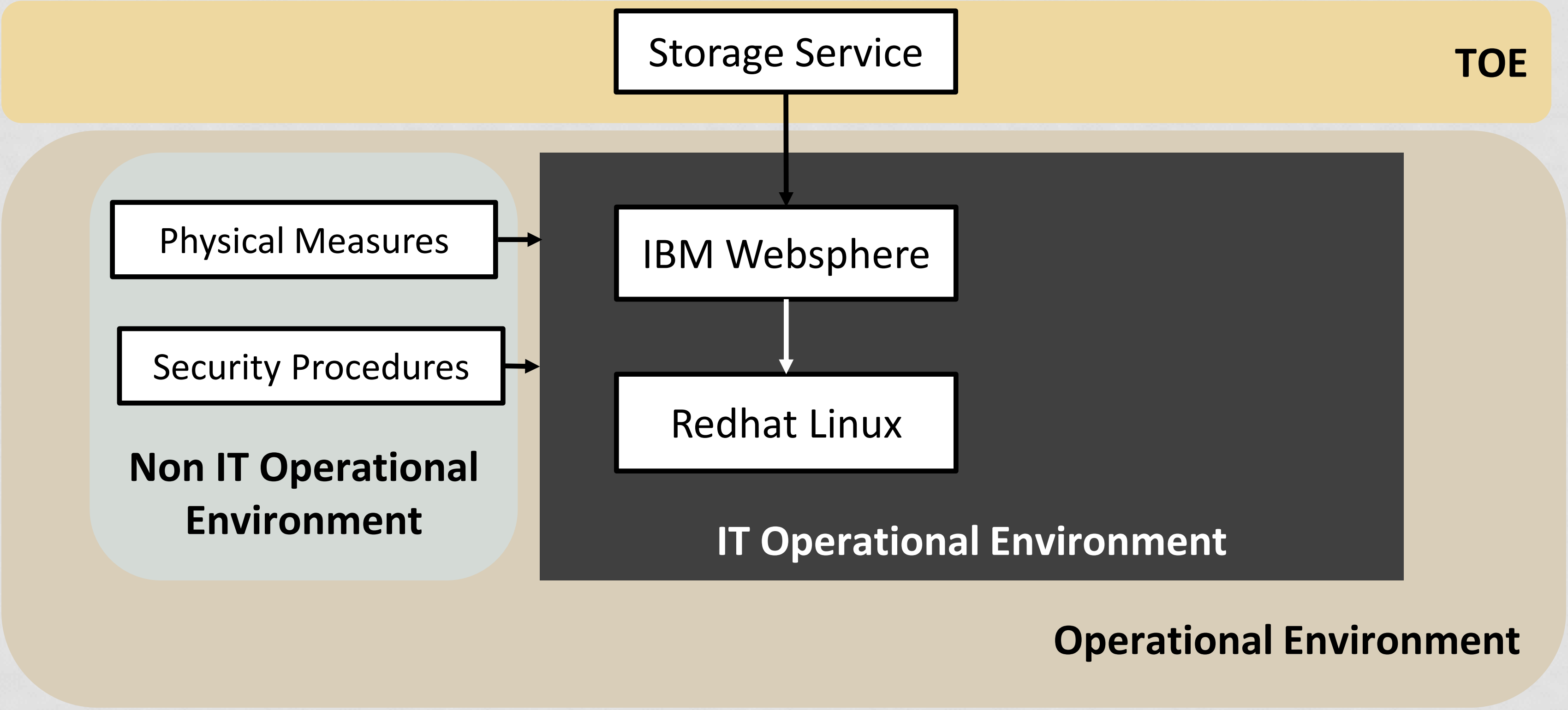
ASSURANCE FOR IT OE – FIRST STEPS

- What should be done?
  - Structured representation of the CC Security Objectives instead of natural language
- Why it should be done?
  - Provide support for the correctness verification of the OE for a given TOE
  - Provide solutions in the direction of machine processability of Security Targets

EXAMPLE : SIMPLIFIED USE CASE OF A STORAGE SERVICE



EXAMPLE : SIMPLIFIED USE CASE OF A STORAGE SERVICE



IBM WEBSPHERE – SECURITY OBJECTIVES (OE)

O.ADMIN	Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
O.PROTECT	Those responsible for the TOE must ensure that procedures exist to ensure that data transferred between workstations is secured from disclosure, interruption or tampering
O.ATTR	The IT Environment shall maintain User and Group mappings for clients.
O.RECOVER	Those responsible for the TOE must ensure that procedures are provided to ensure that after system failure or other discontinuity, recovery without a security compromise is obtained.

REDHAT LINUX – SECURITY OBJECTIVES (TOE)

O.HIERARCHICAL	(LSPP mode only) The TOE must allow hierarchical definitions of roles. Hierarchical definition of roles means the ability to define roles in terms of other roles. This saves time and allows for more convenient administration of the TOE.
O.ROLE	(LSPP mode only) The TOE must prevent users from gaining access to and performing operations on its resources/objects unless they have been granted access by the resource/object owner or they have been assigned to a role (by an authorized administrator) which permits those operations.

COMPARISON OF SECURITY OBJECTIVES

- ❑ Since security objectives are defined in an unstructured (ad-hoc) manner and there is no common vocabulary, it is:
- ❑ Difficult to understand that two security targets contain/have the same security objectives
- ❑ Difficult to compare them, as they are expressed in natural language and needs a manual inspection – can lead to subjectivity

STRUCTURED REPRESENTATION OF SO

- It is difficult to provide a universal structure
- Proposed structure
  - Fits to CC definition: statement of an intent to counter identified threats [CCpart1]
  - Contains the reference to the asset that is going to be protected with that SO – so that a consumer knows **WHAT** exactly is being protected or secured through a particular security objective
  - Contains the (high-level) action to be performed wrt a security property of the asset – so that a consumer knows **HOW** an asset is secured
  - Contains the subject which is in charge to perform the given action – so that a consumer knows **WHO** is responsible for meeting the Security Objective

STRUCTURED REPRESENTATION OF SECURITY OBJECTIVES

- ***SO : <subject> <qualifier> <action> <asset> <context specification>***

- <subject> ({TOE,OE})
- <qualifier> : {must, shall, will}
- <action>: e.g., *keep confidential*
- <asset>: e.g., *files transmitted by the TOE*
- <context specification> e.g. “according to policy X” (OPTIONAL)

- **SO Identifier: O.<subject>_<action>_<asset>_<context>**

IBM WEBSPHERE – SECURITY OBJECTIVES FOR TOE

O.ACCESS	The TOE must ensure that only those clients with the correct authority are able to access an object.

- Can be translated into SOs talking about Confidentiality and Integrity in order to fit into the defined structure
  - O. TOE_CONFIDENTIALITY_RESOURCE
    - <subject> = The TOE
    - <qualifier> = shall
    - <action> = preserve the confidentiality of
    - <asset> = TOE resources
  - O.TOE_INTEGRITY_RESOURCE
    - <subject> = The TOE
    - <qualifier> = shall
    - <action> = preserve the integrity of
    - <asset> = TOE resources

IBM WEBSPHERE – SECURITY OBJECTIVES FOR OE

O.ATTR	The IT Environment shall maintain User and Group mappings for clients.

- O. OE_ROLE_CLIENT
  - <subject> = The OE
  - <qualifier> = shall
  - <action> = maintain User and Group mapping (ROLE)
  - <asset> = CLIENT

REDHAT LINUX– SECURITY OBJECTIVES FOR OE

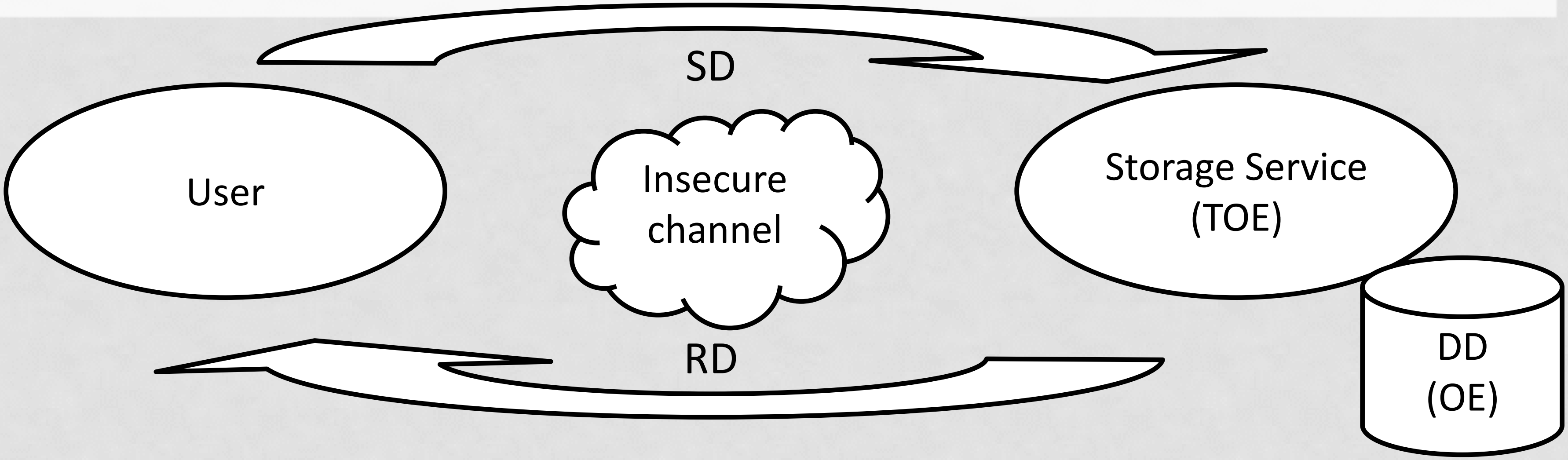
O.HIERARCHICAL	(LSPP mode only) The TOE must allow hierarchical definitions of roles. Hierarchical definition of roles means the ability to define roles in terms of other roles. This saves time and allows for more convenient administration of the TOE.

- O. TOE_ROLE_CLIENT
  - <subject> = The TOE
  - <qualifier> = shall
  - <action> = maintain hierarchical definitions of roles
  - <asset> = CLIENT

SO OF IBM WEBSPHERE (OE) – SO OF REDHAT LINUX (TOE) COMPARISON

IBM Websphere OE	**Redhat Linux TOE**
O. OE_ROLE_CLIENT	*O. TOE_ROLE_CLIENT*
<subject> = The OE	<subject> = The TOE
<qualifier> = shall	<qualifier> = shall
<action> = maintain User and Group mapping (ROLE)	<action> = maintain hierarchical definitions of roles
<asset> = CLIENT	<asset> = CLIENT

STORAGE SERVICE EXAMPLE



- ❑ We could try to define elements of vocabularies for <action> and <asset> based on a model for the TOE of interest (service)
- ❑ **SD**: file to be stored
- ❑ **DD**: file stored in a DB which is part of the OE (and also of the non-TOE HW/SW/FW)
- ❑ **RD**: the data returned to the User

TRANSLATING EXISTING SO TO STRUCTURED SO

- In the general case is necessary to
  - Read the whole set of SOs
  - Read the whole SPD
  - Reword the SOs to identify the key elements of the structured SOs
- It can be useful to define structured threats
  - To better understand SOs
  - To increase machine readability of the whole ST
  - The structure to be used could come directly from CCp1 recommendations, containing the 3 main elements: “threat agent”, “adverse action” and “asset”

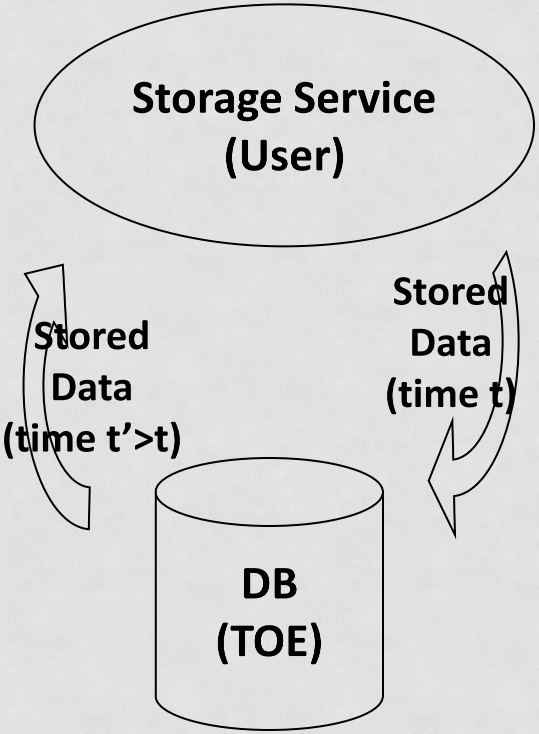
Storage Service example: THREATS – SO MAPPING

T.MALICIOUS_VIOLATION_SD (Malicious users can intentionally read/modify/destroy in an unauthorized way SD)	O.TOE_INTEGRITY_SD O.TOE_CONFIDENTIALITY_SD
T.MALICIOUS_VIOLATION_DD (Malicious users can intentionally read/modify/destoy in an unauthorized way DD)	O.TOE_CONFIDENTIALITY_DD O.OE_INTEGRITY_DD
T.MALICIOUS_VIOLATION_RD (Malicious users can intentionally read/modify/destroy in an unauthorized way RD)	O.TOE_INTEGRITY_RD O.TOE_CONFIDENTIALITY_RD
T.USERS_VIOLATION_DD (TOE users can accidentally read/modify/destroy in an unauthorized way DD)	O.TOE_CONFIDENTIALITY_DD O.OE_INTEGRITY_DD

- No need to express the “full” version of the SO or of the Threat once the structure is well-defined
- Any service that can be consistent with the model of the Storage Service can reuse its SPD and SO (a catalogue of SPD, SO and rationales can be produced, a sort of PP)

Storage Service example: OE Correctness

- In the Storage Service example the OE should be a DB that provides integrity of data stored in it
- We can imagine that
  - The DB could be the TOE of another ST, conforming to the model on the right
  - One of its SOs could be O.TOE_INTEGRITY_STOREDDATA
- In this case it is easier to verify the correctness of this TOE for being the OE of Storage Service (once verified that Stored Data is equivalent to DD)



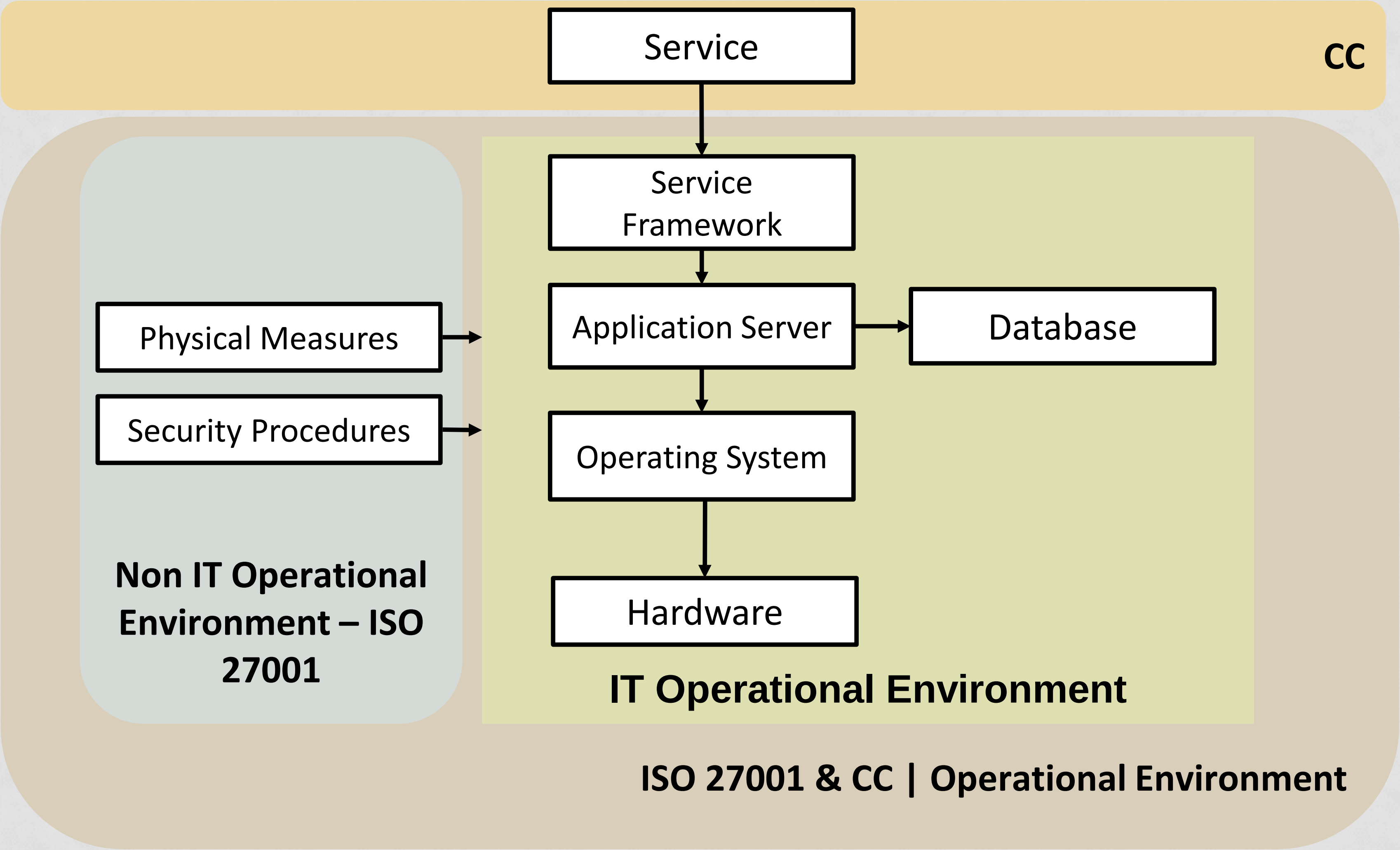
PROPOSED SOLUTION

- ❑ Provide meaningful security assurance to the service consumer for both:
  - ❑ The Service
  - ❑ And the **correctness** of its Operational Environment that includes both:
    - ❑ IT part of the OE
    - ❑ Non IT part of the OE

LACK OF ASSURANCE OF NON IT
Preliminary Analysis

- ❑ The non IT OE environment is maintained by organizations that provide the service and the service consumer has no control over this.
- ❑ Common Criteria does NOT certify the security processes in place in an organization
- ❑ However, there are process based security certifications that are well accepted such as ISO 27001
- ❑ We present a quick summary of the boundaries for these different certification schemes

BOUNDARIES OF CERTIFICATION SCHEMES



Service

CC

Service Framework

Physical Measures

Application Server

Database

Security Procedures

Operating System

Non IT Operational Environment – ISO 27001

Hardware

IT Operational Environment

ISO 27001 & CC | Operational Environment

CC – ISO 27001

- ISO 27001/ ISO 27002 standards are used mainly to certify the security processes that are in place in an organization
- Major cloud service providers have an ISO 27001 certification
  - E.g., Amazon S3, Microsoft Azure..
- ISO 27001allows an organization to define their control objectives that are then evaluated by the Authorized Certification Authorities
  - The results of the certification, the specific control objectives are not disclosed publicly

ASSURANCE OF NON IT OE THROUGH ISO 27001

- ❑ We propose to use the ISO 27001 certified OE as a means to provide the required Assurance
- ❑ A competent authority can then verify that the Security Objectives stated for the non-IT OE are backed up by corresponding control objectives in the ISO 27001 certificate

CC SO FOR OE – ISO 27001 CONTROL OBJECTIVES

Common Criteria Security Objective for OE	**ISO 27001 Control Objectives**
O.ADMIN	A.8 Human resources security
Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.	A.8.1 Prior to employment
	A.8.2 During employment
	A.8.3 Termination or change of employment

CC SO FOR OE – ISO 27001 CONTROL OBJECTIVES

Common Criteria Security Objective for OE	ISO 27001 Control Objectives
O.RECOVER	A.10 Communications and operations management
Those responsible for the TOE must ensure that procedures are provided to ensure that after system failure or other discontinuity, recovery without a security compromise is obtained.	A.10.3 System planning and acceptance

AGENDA

- Changes in software provisioning models based on SOA
- Challenges in Applying CC to the new software provisioning models
  - Assurance of Operational Environment
- Proposed Solution
  - Assurance of IT Parts of Operational Environment
  - Assurance of Non-IT Parts of the Operational Environment
- **Conclusions**
- Future Work

CONCLUSIONS

- We presented a structured approach to represent the security objectives for the IT part of the OE:
  - It is easier to verify the correctness of the OE
  - Certified products with similar functionalities are more comparable
  - Structured SO are machine readable making it possible for consumers to search for
- We presented how we can make use of process certifications as evidence for Non-IT Operational Environment security objectives in CC
- Disadvantages
  - Additional effort in writing ST, but CC community could produce catalogue of SPDs, SOs and rationales

AGENDA

- Changes in software provisioning models based on SOA
- Challenges in Applying CC to the new software provisioning models
  - Assurance of Operational Environment
- Proposed Solution
  - Assurance of IT Parts of Operational Environment
  - Assurance of Non-IT Parts of the Operational Environment
- Conclusions
- **Future Work**

FUTURE WORK

- To consider also OSPs and assumptions
- To build up a full ST for a real service with structured SPD and SOs
- To define a catalogue of SOs (collecting a large number of ST of already certified products)
- To make the Security Targets machine processable