Challenges and Solutions of Distributed Systems Composition

TELECOM TECHNOLOGY CENTER

Tsui, Tsun-Te / Dr. Jeng, Albert B.
Telecom Technology Center

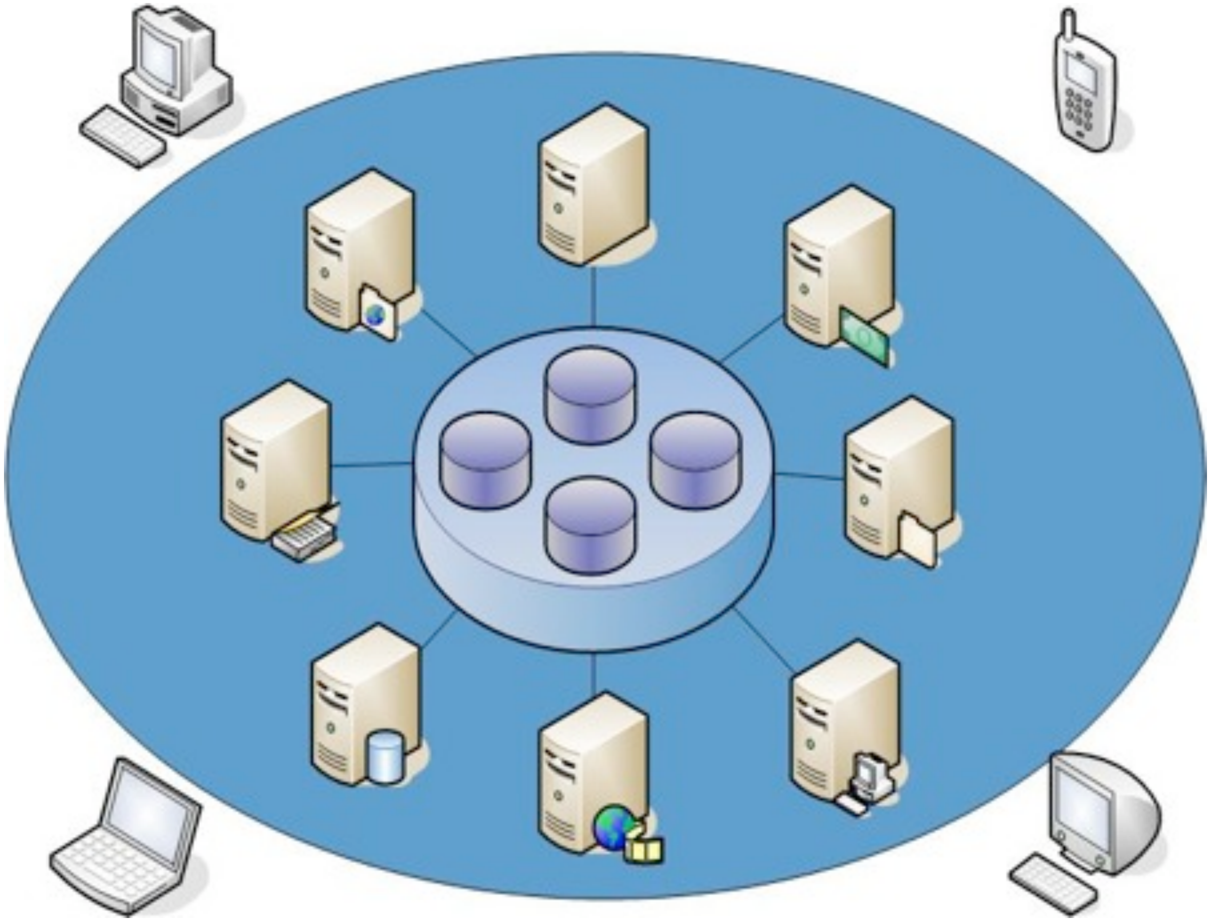
Outline

- Introduction
- Distributed Systems Overview
- How CC Address the Composition Problem
- Challenges in Distributed Systems Composition
- Recommended Solution for Distributed Systems Composition
- Conclusion

Introduction

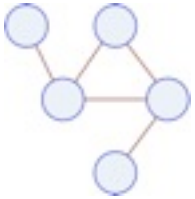
- A Distributed System
  - consists of cross-platform resources which may lead to great difficulties for providing trustworthy security assurance
  - composition of large-scale security mechanisms into a coherent system-wide security assurance is a major challenge
- In CC v3.1
  - class ACO on composition was developed to address the issue
  - fails to address the composition problem including technical criteria for judging the trustworthiness of interconnected information system or distributed systems
- Recommendation on how CC should address distributed systems composition problem based on the most recent research results

Distributed Systems Overview

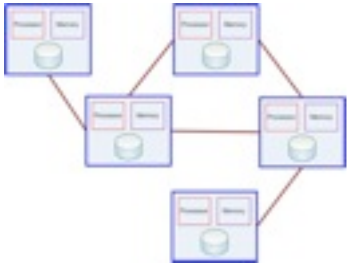


Distributed Systems

- An integration of system services, presenting a **transparent** view of a multiple computer system with **distributed resources and controls**



- A collection of independent computers that appear to the users of the system as a single computer



- Examples
  - Massively multiplayer online games and virtual reality communities
  - A large bank with hundreds of branch offices all over the world
  - DNS, Search engine (e.g. Google), Web mail (e.g. hotmail)

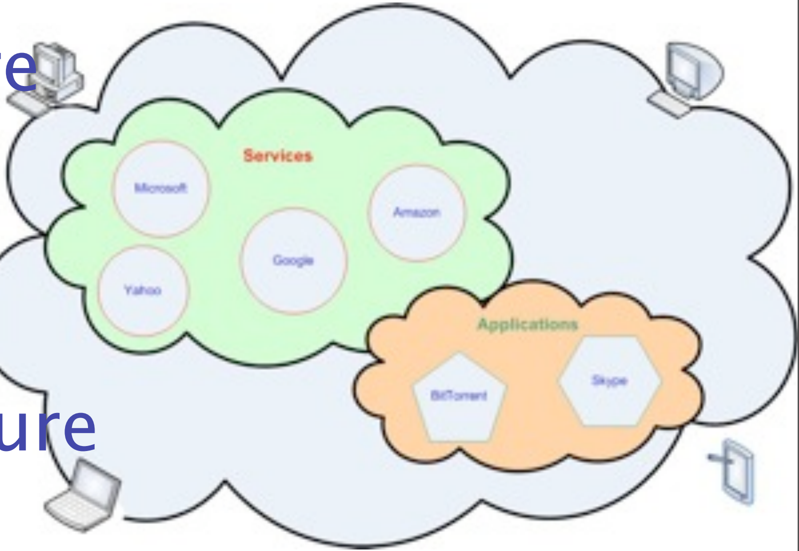
Distributed System Design Issues

- A distributed system consists of **concurrent processes** accessing **distributed resources** through message passing in a network environment that may be unreliable and contain un-trusted components

- Design issues
  - Setup model and identify components
  - Arrange the interaction among components
  - Assure components communication
  - Protect components and system security
- A recent hot paradigm is **Cloud Computing**

Principal Characteristics of Cloud Computing

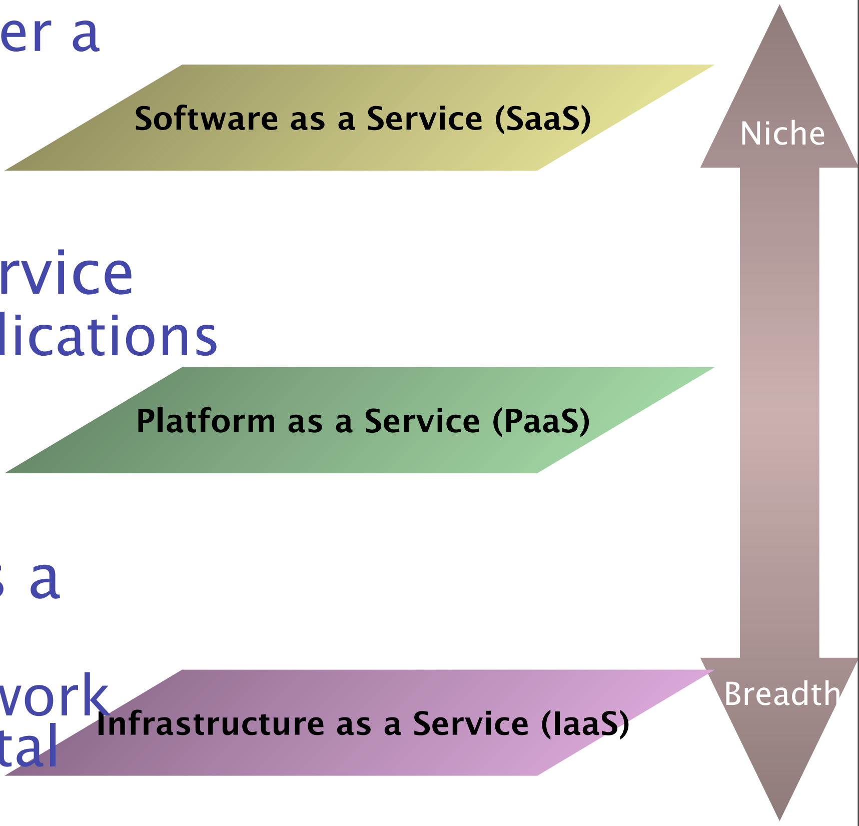
- Abstraction of Infrastructure
- Resource Democratization
- Services Oriented Architecture
- Elasticity/Dynamism of Resources
- Utility model of Consumption & Allocation



(Source: Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing”, April 2009)

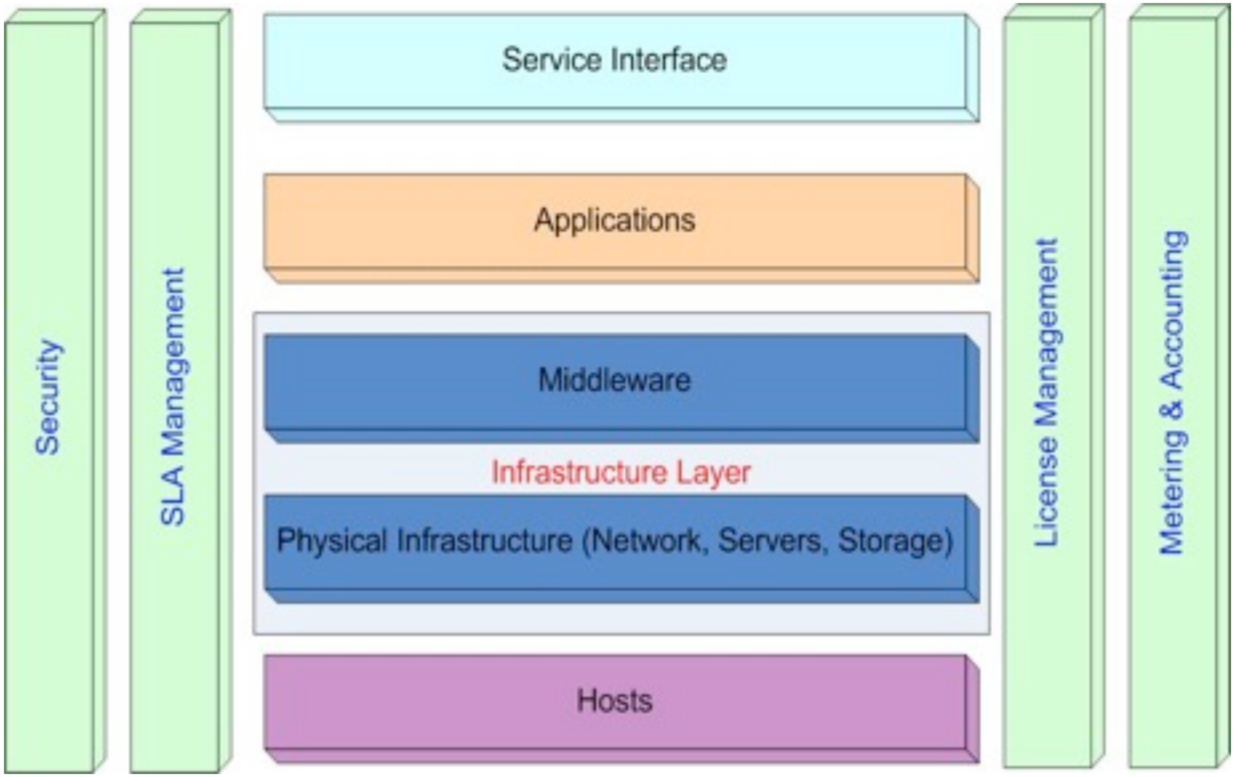
Cloud Service Delivery Models

- SaaS – Cloud **Software** as a Service
  - Use provider's applications over a network
- PaaS – Cloud **Platform** as a Service
  - Deploy customer-created applications to a cloud
- IaaS – Cloud **Infrastructure** as a Service
  - Rent processing, storage, network capacity, and other fundamental computing resources


Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Niche
Breadth

Distributed Systems Security

- Hosts
  - Manageability
  - Metering
  - Security
- Infrastructure
  - Physical
  - Middleware
- Applications
- Services



財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

Cloud Computing Security Issues

- Some key issues:
  - **Trust, Multi-tenancy, Encryption, Compliance**

- Cloud computing contains massively **complex systems** can be reduced to **simple primitives** that are replicated thousands of times and **common functional units**

- Cloud computing security is a tractable problem
  - There are both advantages and challenges

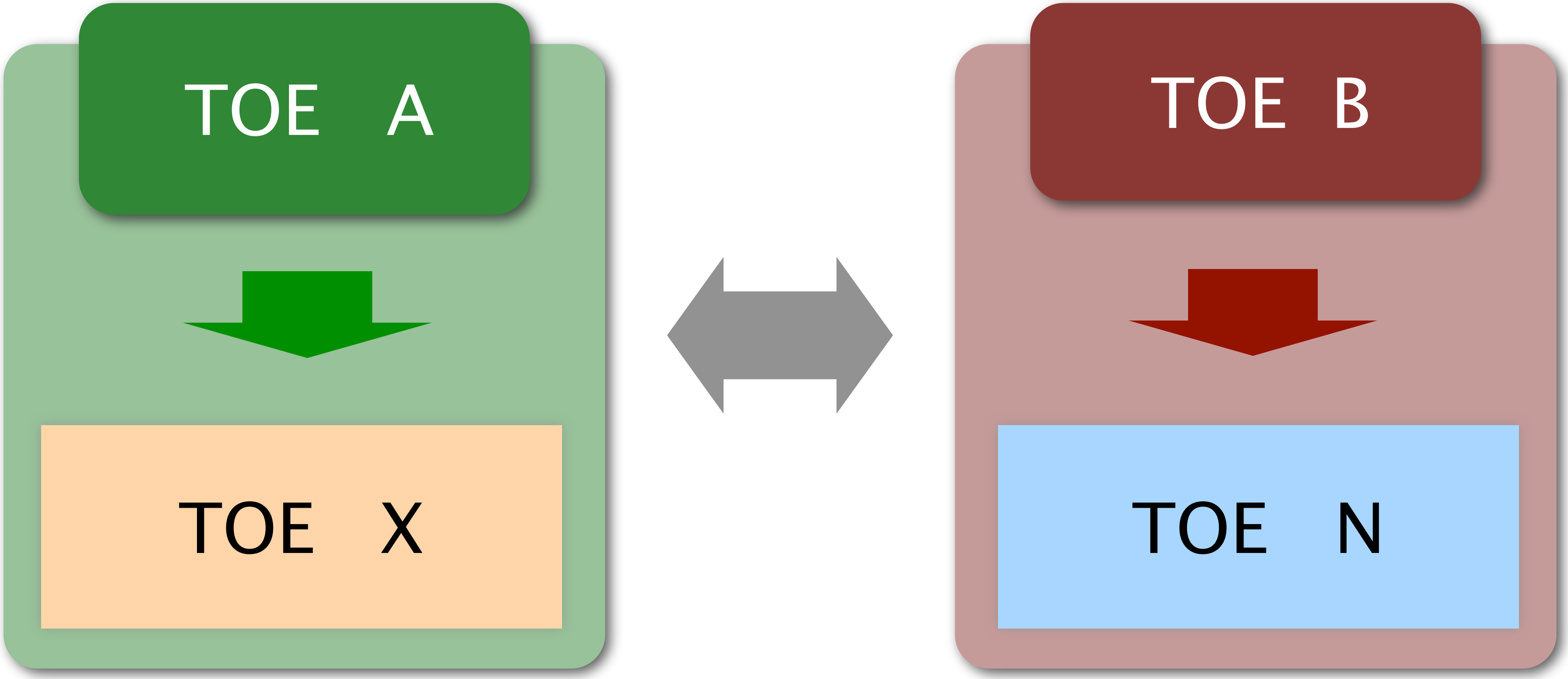
(Source: P. Mell & T. Grance, “Effectively and Securely Using the Cloud Computing Paradigm”, NIST, Information Technology Laboratory, August 2009)

General Cloud Computing Security Challenges

- Trusting vendor’s security model
- Customer inability to respond to audit findings
- Obtaining support for investigations
- Indirect administrator accountability
- Proprietary implementations can’t be examined
- Loss of physical control

(Source: P. Mell & T. Grance, “Effectively and Securely Using the Cloud Computing Paradigm”, NIST,

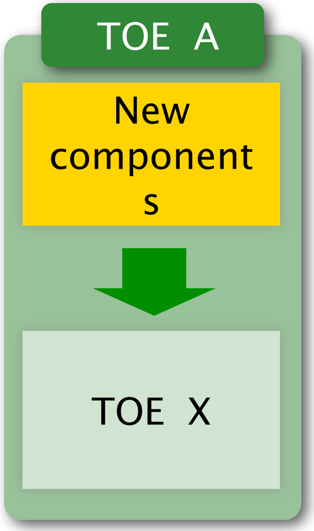
How CC Address the Composition Problem



財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

CC Composition Scenario

- Composition scenario
  - Assume **Component X** has been evaluated
  - Assume **Component A** shall be evaluated
  - Making use of the evaluation of X
    - What can be reused and how?
    - What needs to be re-done?



- The CC Composition Class ACO provides a solution to the practical issues of leveraging off the results of existing CC evaluation
  - Example: A TOE composed of Java applet and smart card controller which have been evaluated separately before

CC Composite Evaluation

- **Composite Evaluation** refers to the evaluation of a system or product that is composed of components—some of which have already been evaluated
- Reduced risk of incompatibility problems in a very late evaluation stage
- ST, ETR-Lite, Certification Report, and evaluation evidence are indispensable in composite evaluations
- Composite evaluations are of significant interest in the smartcard

Composite Evaluation in CC v2.x

- Supporting document
  - [CCDB-2007-09-01] Composite product evaluation for Smartcards and similar devices v1-0 Mandatory
    - Additional security assurance families: **ASE_COMP, ACM_COMP, ADO_COMP, ADV_COMP, ATE_COMP, AVA_COMP**
  - [CCDB-2007-09-02] ETR-template lite for composition v1-0 Guidance

- Composition guidelines mainly focus on smart card (IC + COS + Application)

Composite Evaluation in CC v3.1

ACO: composition class

- Composition rationale (ACO_COR)
- Development evidence (ACO_DEV)
- Reliance of dependent component (ACO_REL)
- Composed TOE testing (ACO_CTT)
- Composition vulnerability analysis (ACO_VUL)

Challenges in Distributed Systems Composition

The Generic Composition Problems

- What happens when putting together the results of two individual component TOEs for operational use, with no further development?
- How to determine assurance of the composed TOE?
- How can a composed product be evaluated?
- How much can be reused from the evaluation of individual components and what needs to be considered when reusing evaluation results?

Challenges in Distributed Systems Composite Evaluation (1/2)

- CC could be used for distributed systems certification/evaluation but it is not readily usable

- Evaluation for system/distributed system lacks
  - Experience in developing system Protection Profiles and Security Targets (except smart card)
  - Functional requirements for non-IT security controls (e.g., physical security, security administration, personnel security, disaster recovery)
  - Criteria to address cross domain issues
  - Criteria to address distributed resources and controls under various administrations and policies
  - Operational maintenance measures

Challenges in Distributed Systems Composite Evaluation (2/2)

- CC doesn’t provide evidence that risk analysis was adequate
- CC and CEM need new/different assurance requirements and lack integration information of components
  - Systems need to be evaluated in their environment taking into account technical and management controls
- The IT security community does not have agreed approach/methodology to evaluate systems composed of evaluated products
- CC evaluation laboratories not accredited to perform system evaluation

Recommended Solution for Distributed Systems Composition

Recommended Solution for Distributed Systems Composition

- Evaluation for Individual components/products
- Learn from early/experimental use of “system level” PPs & use of the CC for system evaluation (e.g., UK, US DoD)
- Turn to system Certification and Accreditation (SAOS, NIST SP 800 series)

System Certification & Accreditation

- System Security **Certification**
  - a process that ensures the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system
- System Security **Accreditation**
  - the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls
- C&A provides assurances that the system residual risk reduced by the IT and non-IT security controls are acceptable to the accreditation official
  - Configuration Management
  - Guidance documentation
  - Life cycle controls
  - Maintenance

Future CC for Distributed Systems Evaluation (1/2)

- Reports/evidence from CC evaluated products used in systems integration could provide useful information for system security certification – if better tailored for that function
  - Current CC evaluation reports/evidence not intended for this purpose
- Develop CC for systems
  - System PP/ST development
  - System CEM development

Future CC for Distributed Systems Evaluation (2/2)

- Expansion of CC to include:
  - Cryptography (NIST FIPS 140)
  - Non-IT functional requirements of the operational environment (e.g., physical, administrative, procedural, personnel) as found in ISO 17799 and other control documents
  - New technical controls + assurance requirements / packages
  - ISO/IEC JTC 1/SC 27 WG3 Work Item: Security Evaluation Criteria
- Expansion of CEM to include assessment methods for the non-IT functional requirements of the operational environment
- Accreditation of labs to perform limited CC-based system evaluations (e.g., smart card)

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

Conclusion

- Anticipation for future CC
  - Output from CC v4 working group: **Implementation Assurance**
    - New approach aimed at large software products
  - Focus on smart card composite evaluations
  - Develop an upgraded CC for system / distributed system composite evaluation

- CC Labs only perform limited CC-based system evaluations for the composed product evaluation

- The general system or distributed system composite evaluation is a significant research problem and beyond the reach of CC without a major overhaul on CC

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

Thank you

TELECOM TECHNOLOGY CENTER

Tsui, Tsun-Te tttsui@ttc.org.tw

Dr. Jeng, Albert albertjeng@hotmail.com