

Cloud and the Common Criteria

Sunil J. Trivedi
The MITRE Corporation



September 2010

Here is a Test... 😊

■ Who has the biggest cloud on this planet?

- Google?
- Microsoft?
- Amazon?
- Name a Government?



■ Reference:

- <http://www.cloudtweaks.com/2010/03/the-biggest-cloud-on-the-planet-is-owned-by-the-crooks/>

Why Cloud Computing?

- **Sacrifice some physical and administrative control to gain efficiency, agility, and reduced infrastructure costs**
- **Getting popular in commercial sectors; drawing attention from Government and Defense sectors**
- **Cloud management tools and techniques are still under construction**
- **Cloud security issues are not new, but mitigation could be a challenge**

NIST Definition

(National Institute of Standards and Technology)

- **Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction**

Cloud Abstraction

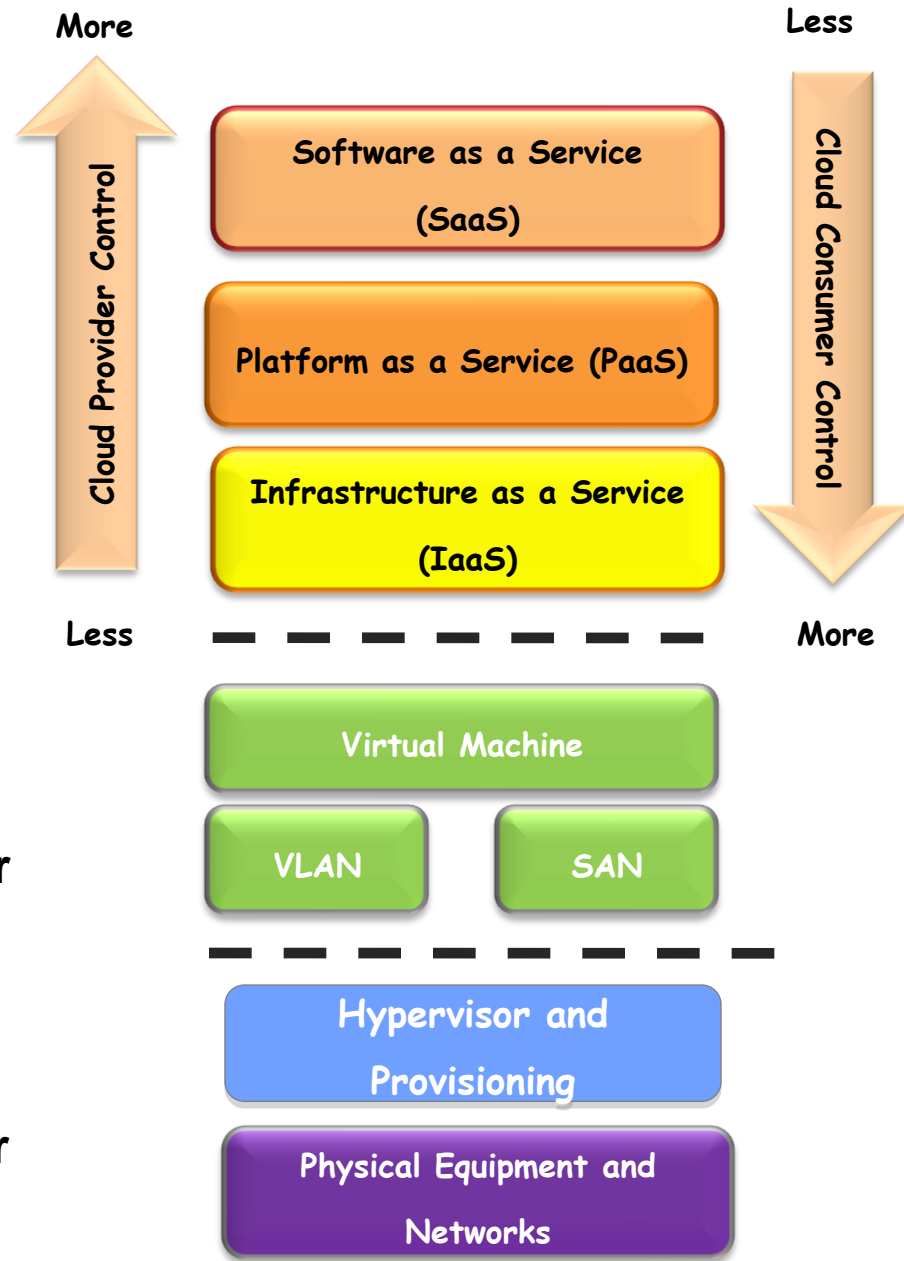
**“Applications to Order”
Software Layer**

**“Virtual Servers to Order”
Platform Layer**

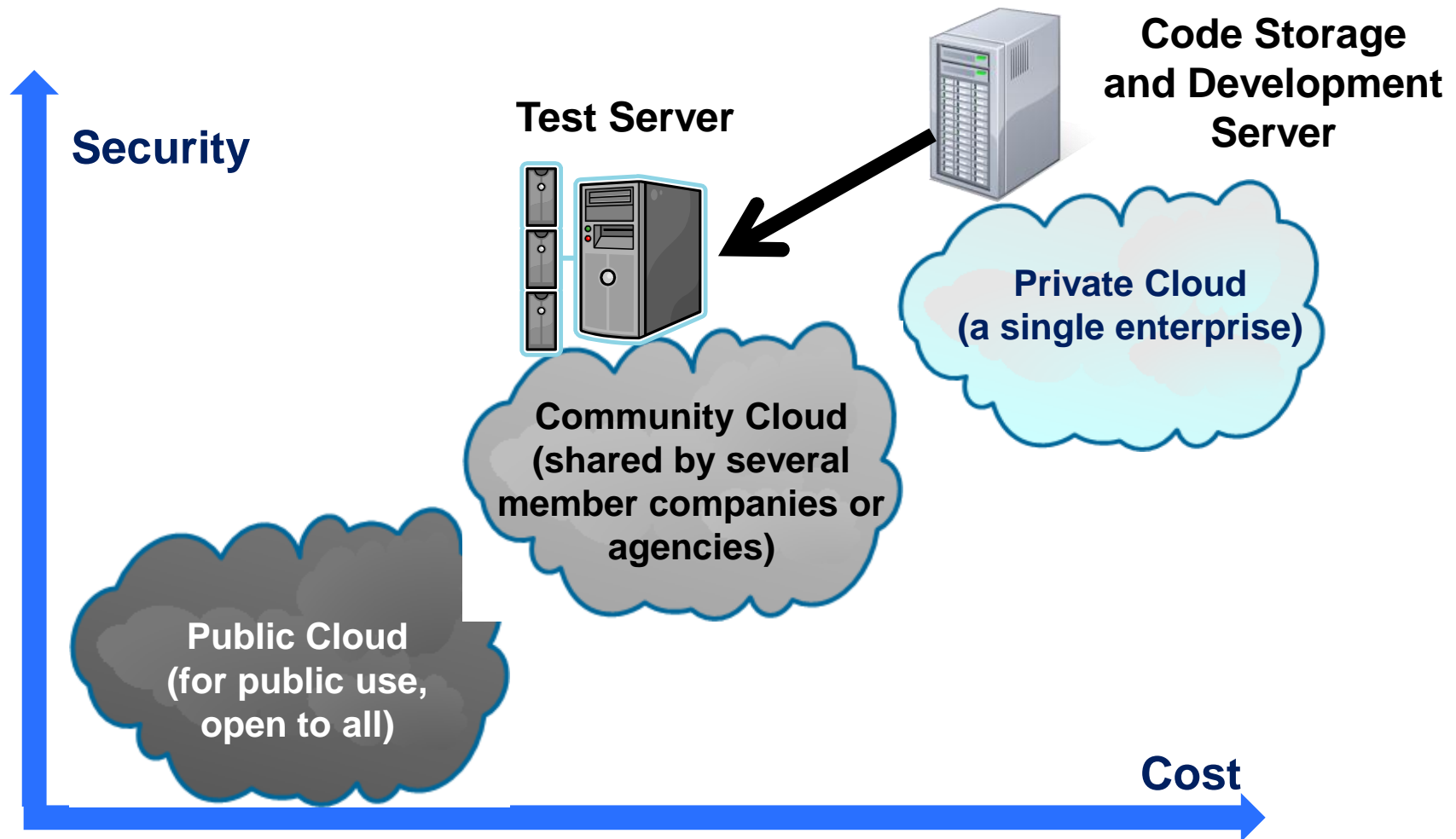
**“Processing, Storage,
and Bandwidth for hire”
Infrastructure Layer**

**Virtual Layer
Managed for the Consumer**

**Physical Layer
Hidden from the Consumer**



Security vs. Cost



The New Challenge

- **The Cloud: A Dynamic Hosting Environment**
 - **Cloud as a Target of Evaluation (TOE)**
 - **Physical Layer may not be under customer control**
 - **Lack of control over vendor software changes**
 - **Does not align well with Common Criteria (CC) evaluation model**

- **As services are delivered globally, complex compliance requirements may need to be considered**

Cloud Security Issues

- Consider “Cloud as a Product”
- Issues are:

Confidentiality

Availability

Trust & Assurance

Legal Concerns



Integrity

Privacy

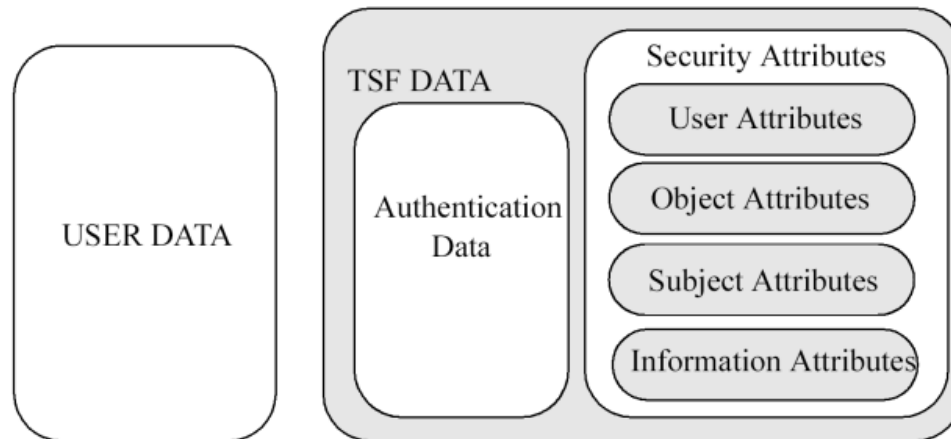
Security Audit

Cloud Abuse

Confidentiality and Common Criteria - 1

- Addressed by Class FDP, User Data Protection
 - Inter-TSF user data confidentiality transfer protection, FDP_UCT
- Addressed by Class FPT, Protection of TSF Data
 - Confidentiality of exposed TSF Data
- Cryptographic functionality may be used to meet objectives specified in these classes

TOE DATA



Confidentiality and Common Criteria – 2

- **Observations:**
 - Traditionally, CC SFRs have addressed data-in-transit
 - Currently, no reference to encrypting data-at-rest
- **In the cloud, stored data must be encrypted with a readily available local backup copy**
 - BP oil spill example
- **Operations become expensive on encrypted data, especially on a remote store**

Challenge:

Adapting CC SFRs for protecting data-at-rest

Integrity and Common Criteria - 1

- **Addressed by Class FDP, User Data Protection**
 - **Stored data integrity (FDP_SDI)**
 - **Inter-TSF user data integrity transfer protection (FDP_UIT)**
 - **Internal TOE transfer (FDP_ITT)**
 - **Integrity Protection, Error, and Monitoring**
 - **Rollback (FDP_ROL)**
 - **Rollback to preserve the integrity of the user data**
- **Addressed by Class FPT, Protection of TSF**
 - **Integrity of exported TSF data (FPT_ITI)**
 - **Internal TOE TSF data Transfer (FPT_ITT)**
 - **monitor and identify integrity errors**
 - **TSF Self Test (FPT_TST)**
 - **verify the integrity of TSF data and TSF itself**

Integrity and Common Criteria - 2

■ Observations

- FDP: Focuses on user data protection
- FPT: Focuses on protection of the TSF data
- FIA specifies components to protect attributes associated with the user
- Data exchange integrity implying data-in-transit
- Encryption is not required/expected on the stored data

Challenge:

Adapting CC SFRs for protecting data-at-rest

Privacy and Common Criteria

- **Addressed by Class FPR, Privacy requirements**
 - Provide a user protection against discovery and misuse of identity by other users
 - A PP/ST author might consider it appropriate not to require protection of the privacy of users against a suitably authorized user
- **The current CC is not very clear here**
 - According to FAU_GEN.2 User identity association, there is a potential conflict between the audit and privacy requirements
- **Observations:**
 - What if the authorized user or the auditor is a third party cloud admin/auditor?
 - Audit by an admin on a local physical drive may not be available at a virtual level

Challenge:

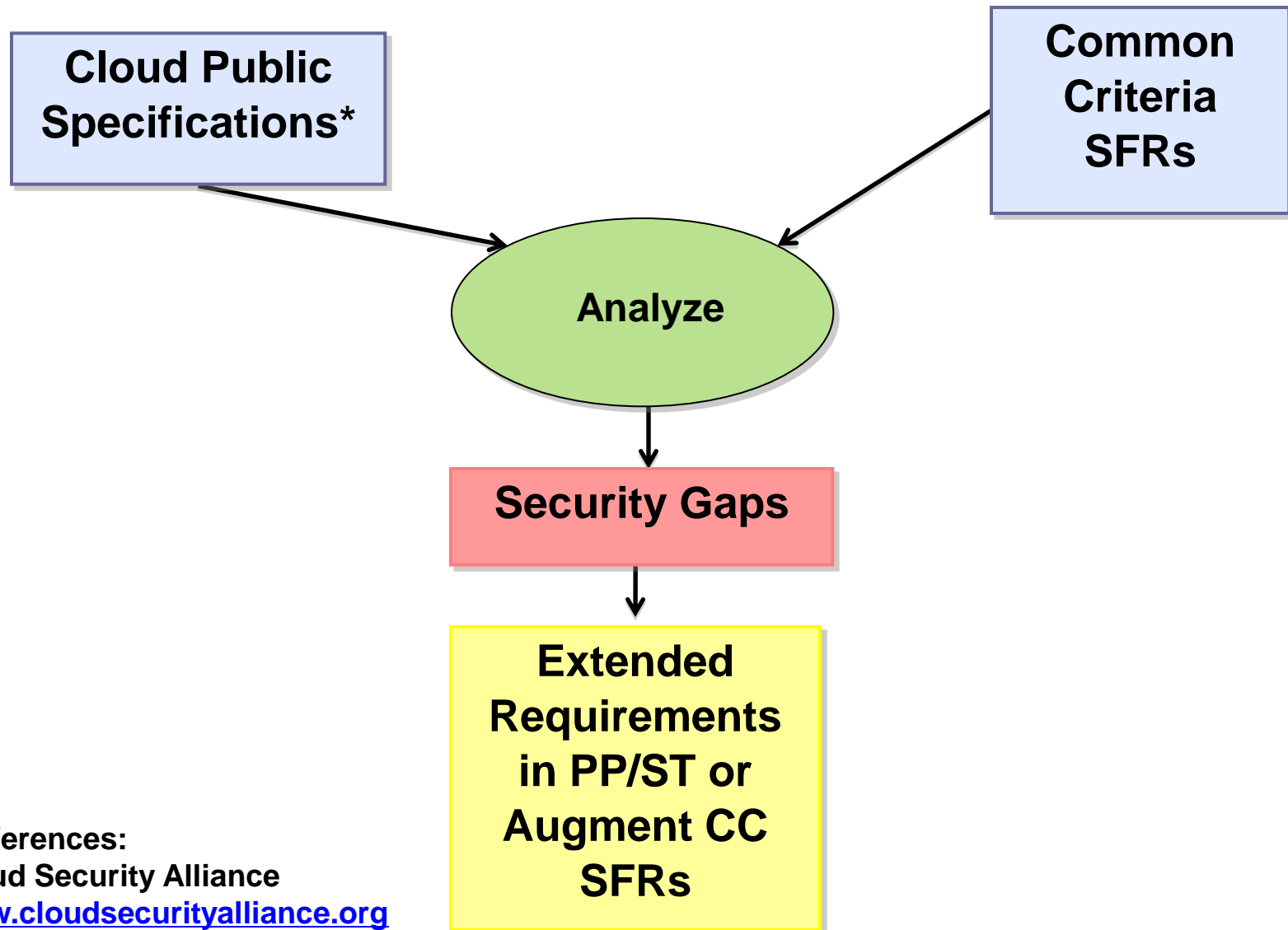
Clarify current CC to address ambiguity regarding Privacy

Availability and Common Criteria

- Addressed by Class FPT, Protection of TSF
 - Availability of exported TSF data (FPT_ITA)
- Addressed by Security audit event storage, FAU_STG
 - Guarantees of audit data availability, FAU_STG.2
- Addressed by Class FRU, Resource utilization
 - Supports the availability of required resources such as processing capability and/or storage capacity
- Observations:
 - Typically, in a cloud, clients have no control over
 - Data (may get accidentally lost or written over)
 - Data Corruption
 - Resources (important customer may get priority)

Challenge: Introduce SFRs mandating an up-to-date backup copy, in case cloud fails to provide one

Developing Cloud Security Requirements for CC



*References:
Cloud Security Alliance
www.cloudsecurityalliance.org

Cloud - CC Security Functions

- A TOE is essentially a set of software, firmware, and/or hardware accompanied by a set of guidelines
 - Useful set of testable assertions
 - Virtual Server Technology
 - Web Applications Technology
 - Software Applications
 - Physical layer not under customer control
 - But is any software really under customer control?
- Cloud can also be an environment supporting layered applications

US Government Cloud Projects

- DISA RACE

- <http://www.disa.mil/race/>

- GSA Apps.Gov

- https://www.apps.gov/cloud/advantage/main/start_page.do/

- DoI National Business Center (NBC)

- <http://cloud.nbc.gov/>

- And more....

Cloud Vendor Listing (not exhaustive)

Software as a Service

- Google Apps
- Microsoft Azure
- NetSuite
- Salesforce

Platform as a Service

- Amazon Web Services
- GoGrid Platform
- Google AppEngine
- Rackspace
- Salesforce

Infrastructure as a Service

- Amazon
- Rackspace

Other Players

- AT&T – application hosting
- Enomaly – integration software
- Rightscale – support sw

Conclusions

- To consider the “cloud as TOE,” some CC changes will be required as explored in this presentation
 - For CC, Evaluating a Private Cloud, might be a manageable task
- Lack of control over physical layer in a Public Cloud will require considerably more changes for the CC and evaluation practice in general
 - This is a discussion for another time

Questions

