OWASP Cloud Top 10

Top 10 Cloud Security Risks

DRAFT

Ludovic Petit

SFR

Chapter Leader OWASP France

OWASP Global Connections Committee

Ludovic.Petit@owasp.org

About me

- Group Fraud & Information Security Adviser at SFR
- Member OWASP Global Connections Committee
- Translator of the OWASP Top Ten
- Chapter Leader OWASP France
- Contributions & Reviews
  - OWASP Secure Coding Practices - Quick Reference Guide
  - OWASP Mobile Security Project
  - OWASP Cloud Top10 Project

Agenda

- Motivation
- Cloud Top 10 Security Risks
- Summary & Conclusion
- Q&A

Motivation

Develop and maintain Top 10 Risks with Cloud

Serve as a Quick List of Top Risks with Cloud adoption

Provide Guidelines on Mitigating the Risks

Building Trust in the Cloud

Data Protection in Large Scale Cross-Organizational Syste

Cloud Top 10 Risks

- R1. Accountability & Data Risk
- R2. User Identity Federation
- R3. Legal & Regulatory Compliance
- R4. Business Continuity & Resiliency
- R5. User Privacy & Secondary Usage of Data
- R6. Service & Data Integration
- R7. Multi-tenancy & Physical Security
- R8. Incidence Analysis & Forensics
- R9. Infrastructure Security
- R10. Non-production Environment Exposure

R1. Accountability & Data Risk

ditional data center of an organization is under complete control of that organization.

organization logically and physically protects the data it owns.

rganization that chooses to use a public cloud for hosting its business service loses control o

poses critical security risks that the organization needs to carefully consider and mitigate.

must ensure about the guarantee of recovering Data:

- Once the data entrusted to a third operator, what are the guarantees that you will recover information?
- What about the backups performed by the operator of Cloud?

R2. User Identity Federation

very important for the enterprises to keep control over user identities as they move services
cations to the different cloud providers.

er than letting Cloud providers create multiple islands of identities that become too comple
ge down the line.

s should be uniquely identifiable with a federated authentication (e.g. SAML) that works acros
providers.

experience is enhanced when he/she does not manage multiple userids and credentials. This a
r back-end data integrations between cloud provides.

R3. Legal & Regulatory Compliance

plex to demonstrate Regulatory compliance.

that is perceived to be secure in one country may not be perceived secure in another du
ent regulatory laws across countries or regions.

nstance, European Union has very strict privacy laws and hence data stored in US may not co
those EU laws.

R4. Business Continuity & Resilency

ess Continuity is an activity an IT organization performs to ensure that the business ca
ucted in a disaster situation.

se of an organization that uses cloud, the responsibility of business continuity gets delegated t
provider.

creates a risk to the organization of not having appropriate business continuity.

t Service Continuity and QoS, one have to ensure about

- the contractual solutions proposed by the Operator of Cloud,
- the Service Level Agreement as well

R5. User Privacy & Secondary Usage of Data

s personal data gets stored in the cloud as users start using social web sites. Most of the social
ague about how they will handle users personal data.

ionally most of the social sites go with the default share all (least restrictive) setup for the user.
nkedIn, Twitter, Facebook it is very easy to deduct personal details of the users.

need to ensure with your Cloud providers what data can or cannot be used by them for secon
oses.

cludes data that can be mined directly from user data by providers or indirectly based on
vior (clicks, incoming outgoing URLs, etc.).

social application providers mine user data for secondary usage e.g. directed advertising
ler when many of us use their personal gmail/hotmail or yahoo account to tell a friend your vac
and immediately you start seeing advertisements on hotels/flights near your destination.

R6. Service & Data Integration

nizations must be sure that their proprietary data is adequately protected as it is transfe
een the end user and the cloud data center.

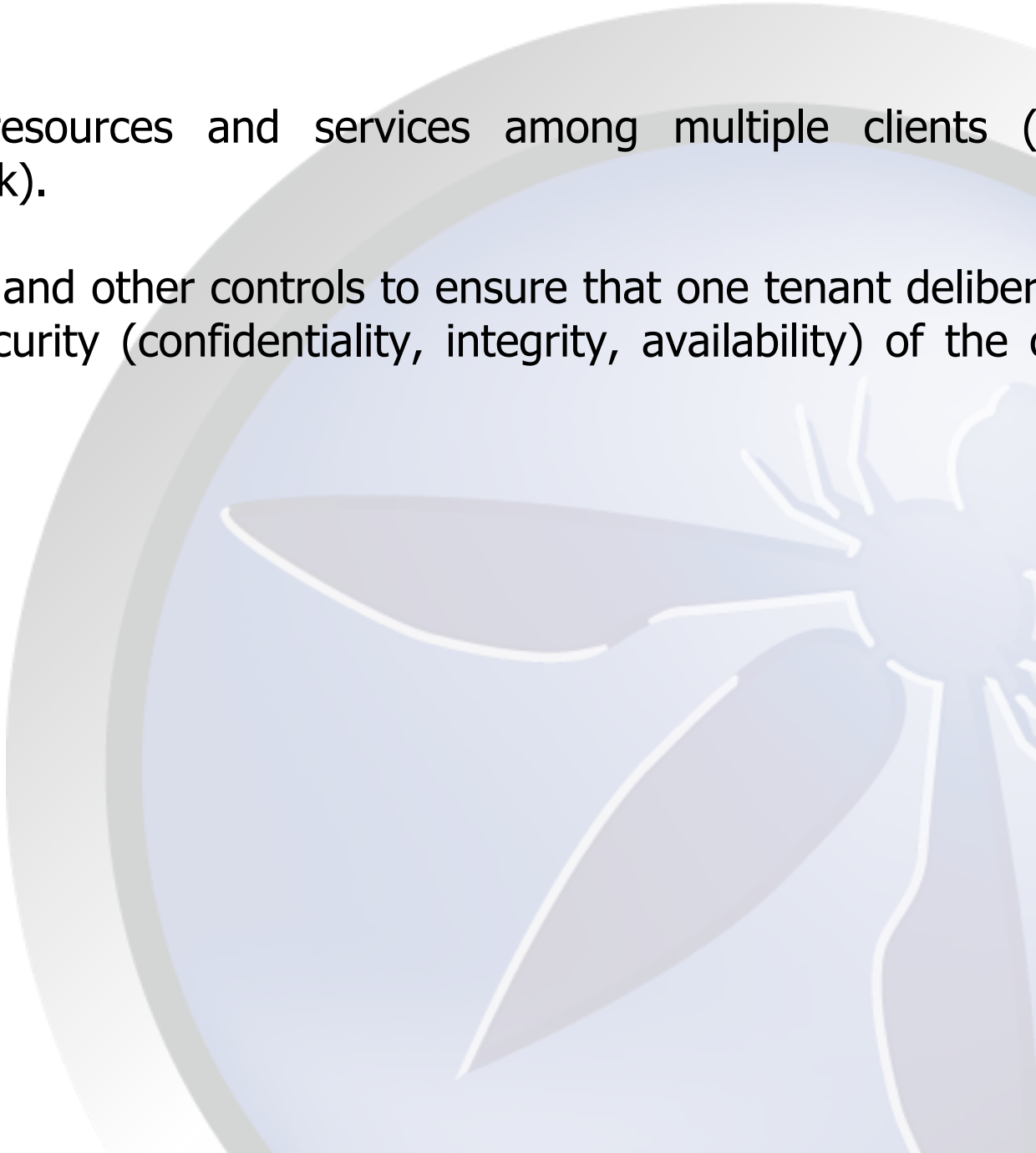
e interception of data in transit should be of concern to every organization, the risk is much gr
rganizations utilizing a Cloud computing model, where data is transmitted over the Internet.

cured data is susceptible to interception and compromise during transmission.

R7. Multi-tenancy & Physical Security

-tenancy in Cloud means sharing of resources and services among multiple clients (
orking, storage/databases, application stack).

reases dependence on logical segregation and other controls to ensure that one tenant deliber
advertently can not interfere with the security (confidentiality, integrity, availability) of the
nts.



R8. Incidence Analysis & Forensics

e event of a security incident, applications and services hosted at a Cloud provider are difficu
tigate as logging may be distributed across multiple hosts and data centers which could be loc
rious countries and hence governed by different laws.

along with log files, data belonging to multiple customers may be co-located on the same hard
storage devices and hence a concern for law enforcing agencies for forensic recovery.

R9. Infrastructure Security

frastructure must be hardened and configured securely, and the hardening/configuration base
d be based on Industry Best Practices.

cations, Systems and Networks must be architected and configured with tiering and security zo
access must be configured to only allow required network and application protocols.

nistrative access must be role-based, and granted on a need-to-know basis. Regular
ssments must be done, preferably by an independent party.

licy and process must be in place for patching/security updates, and can based on risk/th
ssments of new security issues.

ugh the fine details of the items above must be regarded as highly sensitive information,
nable to expect a customer to want to see at least the high-level details.

Provider must be willing to provide this.

R10. Non-production Environment Exposure

T organization that develops software applications internally employs a set of non-produ
onments for design, development, and test activities.

non-production environments are generally not secured to the same extent as the produ
onment.

organization uses a Cloud provider for such non-production environment, then there is a high
authorized access, information modification, and information theft.

Summary & Conclusion

Summary

oud computing is a new way of delivering computing resources, not a new technology.

puting services (ranging from data storage and processing to software, such as email handling
available instantly, commitment-free and on-demand.

checklist should provide a means for customers to

- Assess the risk of adopting Cloud Services
- Compare different Cloud provider offerings
- Obtain assurance from selected Cloud providers
- Reduce the assurance burden on Cloud providers

Q&A

Want to contribute or provide feedback?

Ludovic.Petit@owasp.org

The OWASP Cloud Top 10 Project

ps://www.owasp.org/index.php/Projects/OWASP_Cloud_%E2%80%90_10_Proj