Cloud Security – Revision Notes

Cloud Security - Revision Notes for MCQ

New Risks in Cloud
- **Trust and Dependence**: Customers must trust providers to protect data privacy and computation integrity.
- **Multi-tenancy**: VMs from different customers share physical hardware → introduces security risks like **side-channel attacks**.

Multi-tenancy Risks
- **VM Co-residency**: No control over which server your VM resides on.
- **Side-channel Exploits**: Leakage via CPU cache → **RSA/AES keys can be extracted**.
- **VM Isolation Failure**: VMs can escape to **hypervisor level** (hypervisor escape attack).

Attack Model
- **Goal**: Demonstrate cross-VM attacks are **practical in real-world clouds** like **Amazon EC2**.
- **Two Phases**:
  1. **Placement**: Adversary lands VM on same host as victim.
  2. **Extraction**: Uses **side-channels** to steal info.

Threat Model
- **Trusted**: Cloud provider + infrastructure.
- **Not Considered**: Admin subversion, hypervisor bugs.
- **Adversary**: Malicious cloud customers.
- **Victim**: Users with confidential services.
- **Goal**: Show how new cloud features expand the **attack surface**.

Amazon EC2 Overview
- **IaaS** with **Xen hypervisor**, region & availability zone based.
- Adversary can run up to **20 instances** → potential for co-residency.

Key Questions
1. **Q1**: Can you locate an instance in the cloud? → **Yes, via cloud cartography**.
2. **Q2**: Can co-residency be detected? → **Yes, via internal IP + SYN traceroute**.
3. **Q3**: Can attacker force co-residency? → **Yes, via brute-force or timed launches**.
4. **Q4**: Can attacker exploit co-residency? → **Yes, via side-channel (e.g., cache attack)**.

Cloud Cartography & Network Probing
- **Cloud cartography**: Maps IPs to instance types/zones.
- **Probing**: Internal (VM→VM), External (outside→VM).
- **WHOIS** used to ID IP ranges of EC2.

Effective Co-residency Check
- Compare **internal IPs** → if close, do **TCP SYN traceroute**.
- Just 2 packets, very stealthy.

Achieving Co-residency
- **Brute-force**: Launch many VMs and probe.
- 8.4% co-residency achieved on 1686 targets.
- **Fresh instance attack**: New VMs often placed together.

Exploiting Co-residency
- **Keystroke timing attack**:
  - Measures **inter-keystroke time** via **cache load**.
  - Can recover passwords typed in SSH sessions.

Preventive Measures
- Detect: **Mapping**, **Co-residence checks**.
- Protect: Prevent **co-location** & **side-channel leakage**.

SaaS Cloud-based Collaboration

Types of Collaboration
- **Tightly-coupled** (Federated).
- **Loosely-coupled** → more **vulnerable**, harder to secure.

Problem Statement
- Choose ideal **SaaS cloud provider** and **secure loosely-coupled collaborations**.

🔑 **Trust Models in Cloud**

- Trust models often **lack mathematical validation**.
- Web services evaluated using **QoS + Trust** metrics.

🔐 **Risk-based Access Control (RAC)**

- Allows **access despite lack of full permissions**.
- **Balances risk vs. sharing**.
- More flexible than strict **Multi-Level Security (MLS)**.
- **Challenges**:
  - No method to compute **security uncertainty**.
  - **Operational need** is not quantified → valid requests discarded.

🔁 **Inter-Domain Role Mapping (IDRM)**

- Finds **minimal role set** covering required permissions.
- **No polynomial time solution** → use **heuristics**.
- **Variants**:
  - **IDRM-Safety**
  - **IDRM-Availability**
- **Goal**: minimize **extra permissions** needed.

⚔️ **Conflict Detection & Removal**

🔑 **Conflict Detection**

- **Inheritance conflict**:
  - Need at least **one exit role**.
  - Detected if entry role is **senior** to exit role.
- **SoD (Separation of Duty) Conflict**:
  - If entry & exit roles are **conflicting pair**.

🖌️ **Conflict Removal**

🌀 **Cyclic Inheritance:**

- **Matched roles**: Replace IA with A-relation.
- **Unmatched**: Add **virtual role**.

🚫 **SoD Conflict:**

- Identify **conflicting permissions**.
- Remove from **collaborating role's permission set**.

☑️ **Quick Recap (Key Terms)**

Term	Definition
Multi-tenancy	Sharing hardware among users via VMs.
Co-residency	Two VMs on same physical machine.
Side-channel attack	Leaking data via shared resource behavior.
Cloud cartography	Mapping the cloud's IP to determine instance location.
RAC	Risk-based access control system.
IDRM	Mapping roles across domains securely.
SoD	Separation of Duty – no single user should perform conflicting tasks.