Cloud Applications Architecture

Course 9 - Infrastructure Security

Security

Why is Security Important?

More data (value) than ever (higher stakes)

- Data is the new oil

We do more (especially sensitive) things online.

Stricter regulations.

- More concerning fines

CIA Triad

Confidentiality

- only the authorized entities (people and/or systems) have access to the data

Integrity

- only the authorized entities can modify the data through well-defined procedures

Availability

- there is no point in having a well-guarded system if no one can use it.
- Also, earthquakes tend to overrule highly sophisticated security measures

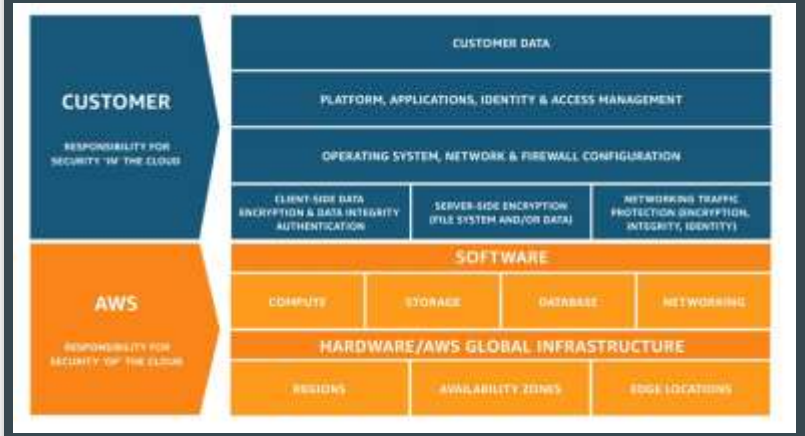
Standards

Many cloud services are certified making your product also compliant

- CSA (Cloud Security Alliance) - Best practices for cloud security
- ISO 27001 - Information Security Management
- ISO 27017 - 27001 in the context of cloud
- ISO 27018 - Personal data protection in cloud
- PCI DSS - Card payments security
- HIPAA - Health information protection

Shared Responsibility Model

Azure Model



AWS Model

Infrastructure Security

(as opposed to application security)

Concerned with:

- Network architecture
- Cloud users (as opposed to application users)
- Application/system permissions
- Resource access permissions

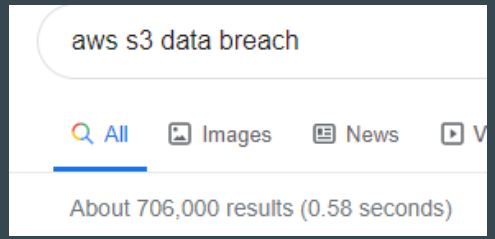
An entirely different paradigm compared to traditional approaches, main difference being the **user** concept.

Infrastructure Security - Common Issues

Unauthorized access

- Mine bitcoin while someone else is paying
- My AWS account was hacked and I have a $50,000 bill

Leaky buckets - examples



Secure by Design

- Not something you add later
  - DevSecOps approach
- Least privilege principle
  - Allow users and applications to perform only what they have to and no more
  - Avoid using root/admin accounts
- Reduced attack surface
  - Keep the number of publicly available resources as low as possible
  - Remove redundant users and policies (e.g. after an employee leaves)
- Multi-factor authentication
  - Most (if not all) providers support this, but it has to be enabled
- Zero trust architecture [Azure][Cloudflare]
  - Basically add security at each layer (not only at the edge)

Secure by Design

Cloud enables us to make security part of the architecture.

- Networks and firewalls/security groups are resources just like any other.
- Users, roles and services accounts are also resources.
- Fine-grained authorization controls/policies are enforced immediately and are also resources in most cases.
- Whitelist approach - e.g. by default, a new user cannot do anything
- Most services behave similar to users
    - If a service must use another service, explicit permission must given.
- In cloud, most requests are HTTP based - each request is evaluated

User Access and Permissions

IAM

Most providers offer an IAM (Identity and Access Management) service:

- AWS IAM
- Google Cloud IAM
- Azure Active Directory

This service facilitates authentication and authorization to the cloud infrastructure

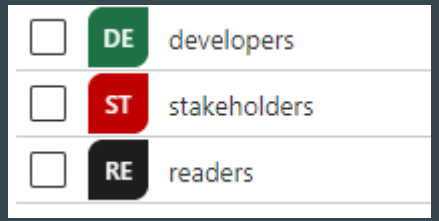
Users

Most providers allow multiple users within one account.

These are usually developers or other stakeholders (DBAs, consultants, auditors).

Some providers also offer **groups**.

- Common examples



User Permissions

Managed through roles and/or policies

- Might also be assigned at the group level
- A user might be part of multiple groups

Least privilege principle

- Operations that require elevated privileges should leverage just in time privileges
  - AWS enables users to assume certain roles
  - Azure AD Privileged Identity Management

Can (should) vary based on environment

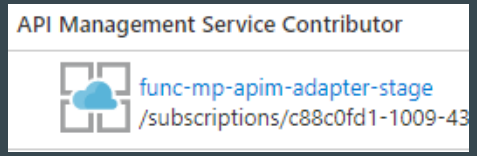
- E.g. a developer might have access to the database service in the development environment, but should not have access in the production environment

Application Permissions

(Enable/allow a service to call another service)

Highly dependant on the provider. E.g.:

- In Azure, each service has its own roles (e.g. API Management Contributor) to which applications can be added.
- In Google Cloud, applications use service accounts through keys (one service account can have multiple keys).



Logging & Monitoring

Since all actions in cloud are HTTP calls performed by a certain identity, they can be monitored - e.g. AWS CloudTrail

- Send notifications on certain events (e.g. VM creation)
- Help with audits
- Detect anomalies

Confidentiality

- Enforce and democratize **encryption**
  - Facilitated by key management services: Google CKM, AWS KMS, Azure Key Vault
  - At least for sensitive and/or PII data
- Social engineering is still a risk nowadays
  - MFA and short lived access tokens help
- Most managed database services will offer encryption at rest by default.

Integrity

Highly relevant especially in the context of distributed systems which are most likely eventual consistent.

Availability

Attacks

- DDoS: Krebs (620 Gbps), Mirai, Dyn, Project Shield (saved Krebs), AWS Shield (02.2020, 2.3 Tbps), Github (1.3 Tbps, memcache) -

Plan with availability in mind:

- Use dedicated services (that also make high availability easier to achieve
- Leverage protection services/offerings (several network services from main providers offer DDoS protection by default) - e.g. Azure CDN.
- Attacks from today are just the normal traffic from tomorrow.

Further Readings

CNCF Security Whitepaper (focuses on containers)

AWS Well-Architected Framework - Security Chapter

Google Architecture Framework - Security, Privacy, and Compliance

Azure Well-Architected Framework - Security Chapter