Comparison of Cloud-Specific Applications Security Frameworks and Standards

Nicole Takam Madjo Epse Ketchiozo

CYBR 691 – Special Topics in Cybersecurity

Spring 2023 - UMBC

Outline:

Introduction

Many organizations are turning to cybersecurity frameworks to implement a baseline of their security roadmap. With the adoption of cloud computing and the migration of many applications to the cloud, it becomes important to review some of the most used frameworks, and how to apply them to enforce security principles.

We will do a quick review of the challenges of cloud environments before diving into frameworks. We will end up with a use case scenario on how AWS leverages on these frameworks for their clients.

1. Cloud Computing and application security challenges

Before we jump into security frameworks and standards that a specific to cloud computing, it is important to understand what it is and the security challenges faced by the deployment of cloud applications.

1.1 Introduction to Cloud Computing

Cloud computing is defined by AWS [1] as the "the on-demand delivery of compute power, database, storage, applications, and other IT resources through a cloud services platform through the internet with pay-as-you-go pricing." In our context, we can rephrase this as providing on-demand services that are necessary to deploy an application using a cloud service platform through the internet, and only paying for the services that are needed, as the need arises throughout the SDLC stages. The three major cloud service providers (CSPs) are AWS, Google Cloud, and Microsoft Azure.

Many enterprises are moving their applications to the cloud because there are several advantages:

- Pricing model: pay-as-you-go allows to pay only for services needed and used;
- Benefit from massive economies of scale: this becomes very useful when dealing with security challenges. Cloud providers offer various robust tools and services, and invest to keep their customers;
- Increase speed and agility: resources take a minute to be deployed;
- Stop guessing capacity before-hand: you can start small, and grow as need arise. With auto-scaling, you can scale up your resources capacity to accommodate to your need during peak time and scale down when things slow down, without managing unused resources;
- Ease to automate processes: cloud computing has enabled new tools and practices like DevOps, that help automate most processes like security, build, test, deployment and administration of applications.

Some challenges related to Cloud Computing include:

- Vendor locking: experience has shown that a multi-cloud strategy is the best approach, but this is challenging given that vendors don't always offer compatible resources;
- Skills set: cloud computing is relatively new, there is a lack of trained professionals;
- Cost management: after migrating to the cloud, most enterprises focus on modernization and cost optimization. The reality check is that going to the cloud is not always cheaper than running application on premises. Most enterprise need to resist to urge to move everything to the cloud and select the right strategy for their use cases.
- Security: It is the highest priority for clients and CSP as more people embrace cloud's scalability and flexibility. We will talk more about it in the following section.

It is also important to understand the three different cloud services models summarized on figure 1.1, and the level of control and flexibility they offer:

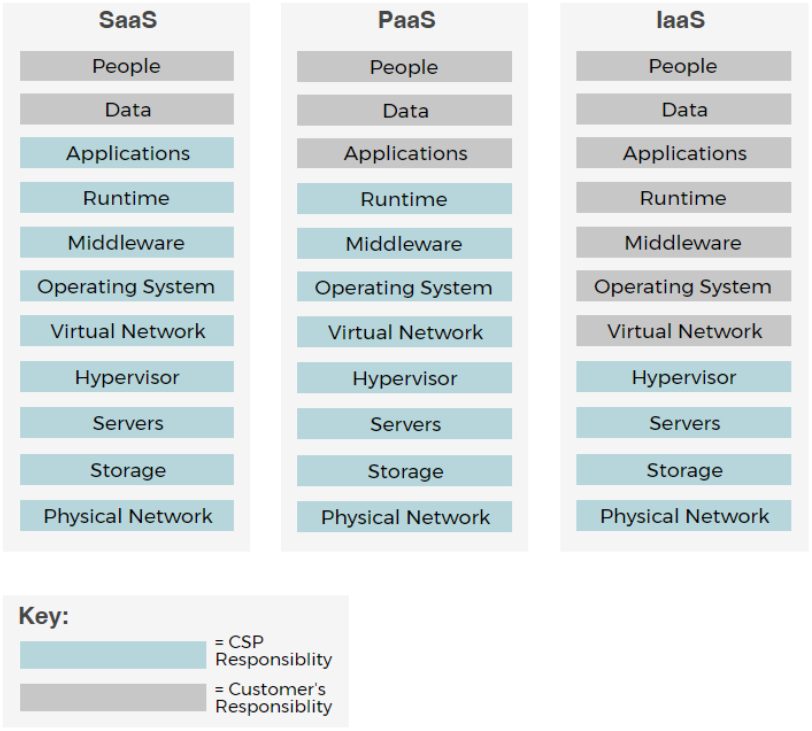

Figure 1: *Cloud Service Models [2]*

- Infrastructure as a Service (IaaS): Cloud Services Providers(CSP) offer clients direct access to their servers and storage, and control over their infrastructure just as on premises. Provides

the highest level of flexibility and allows automated deployments.

- Platform as a Service (PaaS): Through this model CSP offer clients a platform on which they can develop and deploy software without managing the underlying cloud infrastructure. It is the model most used for cloud application development, increasing developer productivity and utilization rates while decreasing application's time to market.
- Software as a Service (SaaS): Most familiar model or end-user applications known by consumers, who do not handle software management, its deployment or the underlying cloud infrastructure. They are managed by a third-party. Familiar examples include Dropbox or Google Apps.

When deploying an application to the cloud, there are the following deployment models: Private Cloud, Community Cloud, Public Cloud, and Hybrid Cloud. These models define the boundaries of the cloud infrastructure and determine access to the resources.

1.2 Cloud-based application security challenges

There are growing security challenges related to the adoption of cloud services. As business grow, they need to keep up with visibility, compliance and regulatory requirements. As infrastructure becomes more diverse, it becomes challenging to ensure adequate protection of resources and data across diverse platforms. Attacks have become more sophisticated, more frequent, and growing in intensity. CSP providers do not always keep up with the pace and need to provide adequate protective services. Given the existing shortage of skilled professional in cybersecurity in general, it becomes more challenging to find those specialized in Cloud Computing.

To add to the above challenges, cloud security is a shared-responsibility between the CSP and the client. It varies from one CSP to the other, by the cloud services and deployment models adopted by an organization, as summarized by U.S. National Security Agency (NSA) [3] in the figure below:

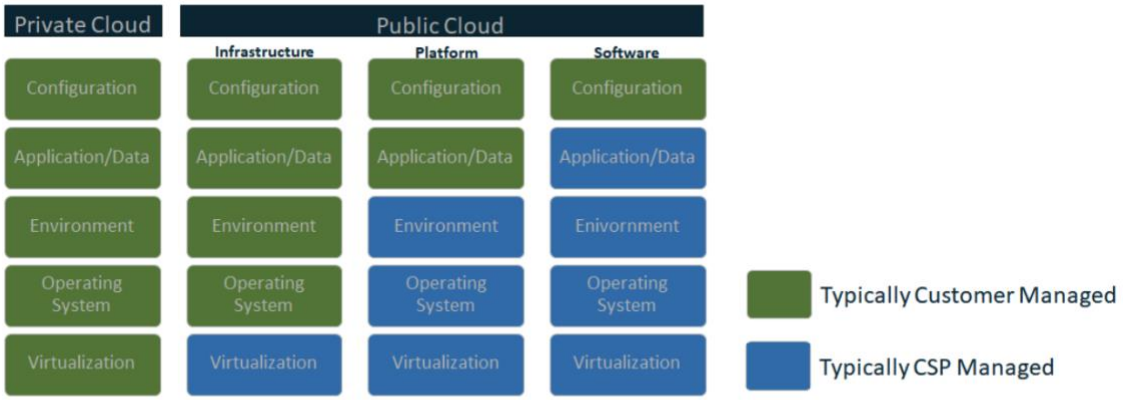

Figure 1: Cloud Shared Responsibility Model

Figure 2: *Cloud Shared Responsibility Model*

The 2023 Cloud Security Trends Whitepaper by the SANS [4], reveals that unauthorized access to cloud resources by outsiders, poorly configured interfaces and cloud assets, and the lack of visibility into what is going on within the cloud are organizations top concerns. On the other-hand, Cloud-centric attacks and breaches were mostly due to account compromise or poor configuration of cloud services and resources.

2. Cloud-specific security frameworks and standards

Given the peculiarity of Cloud Computing and the security challenges associated with its adoption, the U.S. Government and private organization have developed some specific frameworks to guide all stakeholders in their cloud journey. In the sections below, we will present some of these frameworks, and identify some common recommendations and controls that apply the principle of least privilege.

2.1. National Institute of Standards and Technology – NIST

There are two frameworks developed by NIST [5] that directly apply to security of cloud-based applications: NIST SP 800-37 and NIST SP 800-53. They holistically cover all major concerns for security risks for any information systems and can be tailored to address cloud application security needs.

NIST SP 800-37 Rev.2 - Risk Management Framework (RMF) for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy – describes and provides guidelines for applying the RMF to information systems and organizations. Particularly, the RMF incorporates security and privacy into application and systems development life cycle.

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Table 1: *Security and Privacy Control Families*

NIST SP 800-53 Rev.5 - Security and Privacy Controls for Information Systems and Organizations – provides a catalog of flexible and customizable security and privacy controls for information systems and organizations. These controls are the starting point to determine the functional or operational requirement for securing low, moderate and high impact federal information systems and now all organizations (as specified by Rev.5. NIST SP 800-53 identifies the security controls families listed on Table 1. The implementation of these controls for a cloud-based application are mostly influenced by the CSP and the cloud model adopted by the organization.

If we take as hypothesis the AC and IA families, they are mostly implemented through Identity and Access Management with AWS, and the corresponding service for Azure is a combination of Azure Active Directory and Azure Role Based Access Control. In this scenario, the CSP provides the services, and the shared-responsibility model will guide clients in the implementation of the controls using the available services. CSP and their market place partners also offer some tools that will help to verify compliance with NIST 800-53 security controls.

Let us for examine how the security principle of least privilege is implemented with this framework. AC-Access Control- family includes subfamily AC-6 – least privilege. The purpose of the control is stated: "Employ the principle of least privilege, allowing only authorized users (processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks". The frameworks details steps to fully implement this control, and gives a list of related controls sub-families: AC-2, AC-3, AC-5, AC-16, CM-5,

CM-11, PL-2, PM-12, SA-8, SA-15, SA-17, SC-38. This helps to further re-inforce the principle in all stages of the SSDL.

2.2. The Federal Risk and Authorization Management Program – FedRAMP

FedRAMP is "a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies." [6] It is a framework that leverages on basic NIST SP 800-53 Rev. 5 controls, and includes additional controls to address the unique elements of cloud computing with the ultimate goal of ensuring that all data (federal) is secured in cloud environments.

FedRAMP provides categorization template for CSPs and their client to use analyze data hosted on their systems and to categorize system based on the types of information processed, stored, and transmitted on their systems. Cloud Services Offerings (CSOs) are categorized into Low, Moderate and High impact levels, across confidentiality, integrity and availability (CIA) security objectives.
Federal Agencies and CSO go through an assessment program using standardized authorization packages to be able to operate.
FedRAMP Security Controls Baseline provides the catalog of High, Moderate, Low, and Tailored LI-Saas baseline security controls with additional guidance and requirements.
If we take again the hypothesis of AC – Access Control families, AC-06 "Least Privilege" is categorized as a high baseline control with recommendations (01),(02),(03), (07),(08) that are specified as required for an application to be authorized as a high Impact Level. While AC-06 – (02) is a required moderate baseline control for Moderate Impact Authorization, and there is no AC-06 requirement in Low Baseline Controls and Tailored Li-Saas.

2.3. Cloud Security Alliance – CSA STAR

The Cloud Security Alliance (CSA) provides the Security, Trust, Assurance, and Risk (STAR) registry which is a publicly accessible registry that documents security and privacy controls provided by CSPs [7].

Figure 3: *CSA CCM Technology Domains.*

STAR uses the Cloud Controls Matrix (CCM) as a framework to outline key principles of transparency, rigorous auditing, and standards for cloud technology. CSA CCM has 197 control objectives structured in 17 cloud technology domains. Organizations use it to evaluate and document their security controls. There are two levels of STAR: level 1 – self-Assessment - mostly used for cloud-based applications, and Level 2 of STAR - Third-Party Audit - used to build other industry certifications and standards. In addition to the CCM, the Consensus Assessment Initiative Questionnaire CAIQ provides a set of "yes or no" questions based on security controls in the CCM.

For our hypothesis, of least privilege, we have control domain "Identity & Access Management - IAM".
CCM control title "least privilege" with control ID IAM 05. Other related controls ID related IAM 08 - "User Access Review", IAM 14 – "Strong Authentication", CEK-18 – "Key Archival".
The lease privilege is also addressed by the CAIQ question ID "IAM-05.1 "Is the least privilege principle employed when implementing information system access?" Other related CAIQ IAM-08.1, IAM-08.1 include "Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance?" guide in the implementation of the principle.

2.4. The OWASP 10 for the Cloud

The Open Worldwide Application Security Project® (OWASP) has published the Cloud-Native Application Security Top 10 [8] to address the new set of challenges raised by the adoption of cloud computing. This document provides information about prominent security risk for cloud -native applications, as well as the challenges involved and how to overcome them.

The OWASP Cloud-Native Top 10 list include:

- CNAS-1: Insecure cloud, container or orchestration configuration
- CNAS-2: Injection flaws (app layer, cloud events, cloud services)
- CNAS-3: Improper authentication & authorization
- CNAS-4: CI/CD pipeline & software supply chain flaws

- CNAS-5: Insecure secrets storage
- CNAS-6: Over-permissive or insecure network policies
- CNAS-7: Using components with known vulnerabilities
- CNAS-8: Improper assets management
- CNAS-9: Inadequate 'compute' resource quota limits
- CNAS-10: Ineffective logging & monitoring (e.g. runtime activity)

The project is still under development. The least privilege principle is address under CNAS-3, with Over-permissive cloud IAM roles as an example of risk that will violate this principle. CNAS-1 and CNAS-6 have related risks.

3. Use Case Scenario: AWS

Amazon Web Service (AWS) holds most of the market in Cloud Computing. This CSP offers a lot of services for the security of cloud-applications. The benefits of AWS security include data protection, compliance, cost saving and ability to quickly scale. In terms of security and compliance, they support the implementation of several frameworks including FedRAMP and NIST 800-53 through the shared-responsibility model.

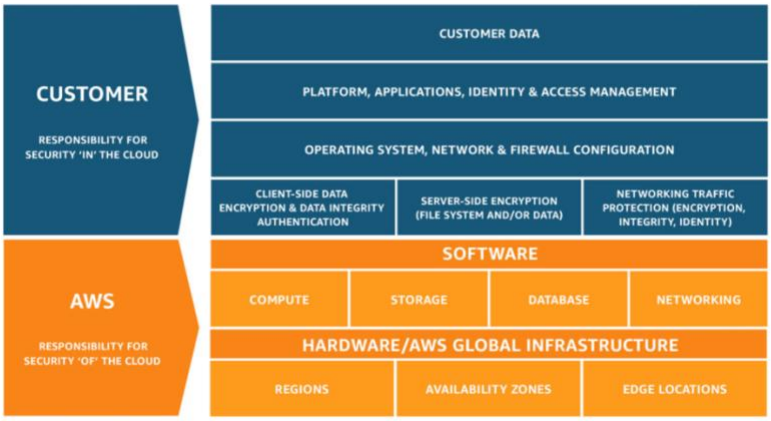

Figure 4 – *AWS Shared-Responsibility Model.*

The customer inherits some controls from AWS, while other controls implementation is a common responsibility. But most controls related to application deployment are specific to customers. That is when the AWS Well-Architected Framework become a handy free tool to guide clients in securing their cloud-based applications.

The security pillar of the AWS Well-Architected Framework [9] emphasizes on the principle of least privilege as necessary to implement a strong identity foundation: "User access should be granted using a least-privilege approach with best practices including

password requirements and MFA enforced. Programmatic access, including API calls to AWS services, should be performed using temporary and limited-privilege credentials, such as those issued by the AWS Security Token Service." It then lists some best practices under identity and access management that clients can follow. The questions provide a guidance in the process.

Conclusion

In this project, we reviewed cloud computing concepts and how some frameworks could be leveraged to implement cybersecurity principles for cloud-based applications.

There are other frameworks like Center for Internet Security (CIS) Benchmarks, SOC2, and ISO/IEC 27001 Standard, and market place tools that we wished we had enough time to cover. We hope that our study will serve as a starting point in implementing robust security for cloud-based applications.

References:

1. Amazon Web Services. AWS Cloud Essentials. https://aws.amazon.com/getting-started/cloud-essentials/?intClick=dc navbar. 05/15/2023
2. U.S. Department of the Interior. Cloud Service Models. https://www.doi.gov/cloud/service.05/15/2023
3. National Security Agency. Mitigating Cloud Vulnerabilities. https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF. 05/15/2023
4. Dave Shackleford. ebook 2023 Cloud Security Trends. https://pages.awscloud.com/rs/amazonwebservicesm2/images/awsmp-attboHXrE3jtzA6BS-awsmp-adhoc-sec-2023-security-trends-ebook.pdf?aliId=eyJpIjoieVwvNjRzVVdncnoydFhldWoiLCJ0IjoiVlpoT09KRWlDTVcycGt6cjVQZnNNZz09In0%253D. 05/15/2023
5. NIST. Computer Security Resource Center - Publications. https://csrc.nist.gov/publications/.05/15/2023
6. FedRAMP. Securing Cloud Services for the Federal Government. https://www.fedramp.gov/.05/15/2023
7. Cloud Security Alliance. https://cloudsecurityalliance.org/.05/15/2023
8. OWASP. OWASP Cloud-Native Application Security Top 10. https://owasp.org/www-project-cloud-native-application-security-top-10/. 05/15/2023
9. Amazon Web Services. Security Pillar – AWS Well-Architected Model.

https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html. 05/15/2023

Tables and Figures