

CSCI 5409 Adv Topic in Cloud Computing – Fall, 2023
Week 10 – Lecture 2 (Nov 10, 2023)

Security – Part 2

Dr. Lu Yang
Faculty of Computer Science
Dalhousie University
luyang@dal.ca

Housekeeping and Feedback

- Start recording
- Starting working on the term project. Ask Purvesh and Rahul questions.
- The final covers contents before (30%) and after (70%) the midterm.

Objectives

- Understand cloud security mechanisms
- Understand the best practices of the AWS Well-Architected Framework security pillar


Contents

- Section 1.** Cloud Security Mechanisms
- Section 2.** AWS Well-Architected Security Pillar and Best Practices



1

Cloud Security Mechanisms

1. Encryption
 2. Transport Layer Security (TLS)
 3. Hashing
 4. Public Key Infrastructure
 5. Hardened Virtual Server Images
 6. Single Sign-On (SSO)
 7. Cloud-Based Security Groups
- 

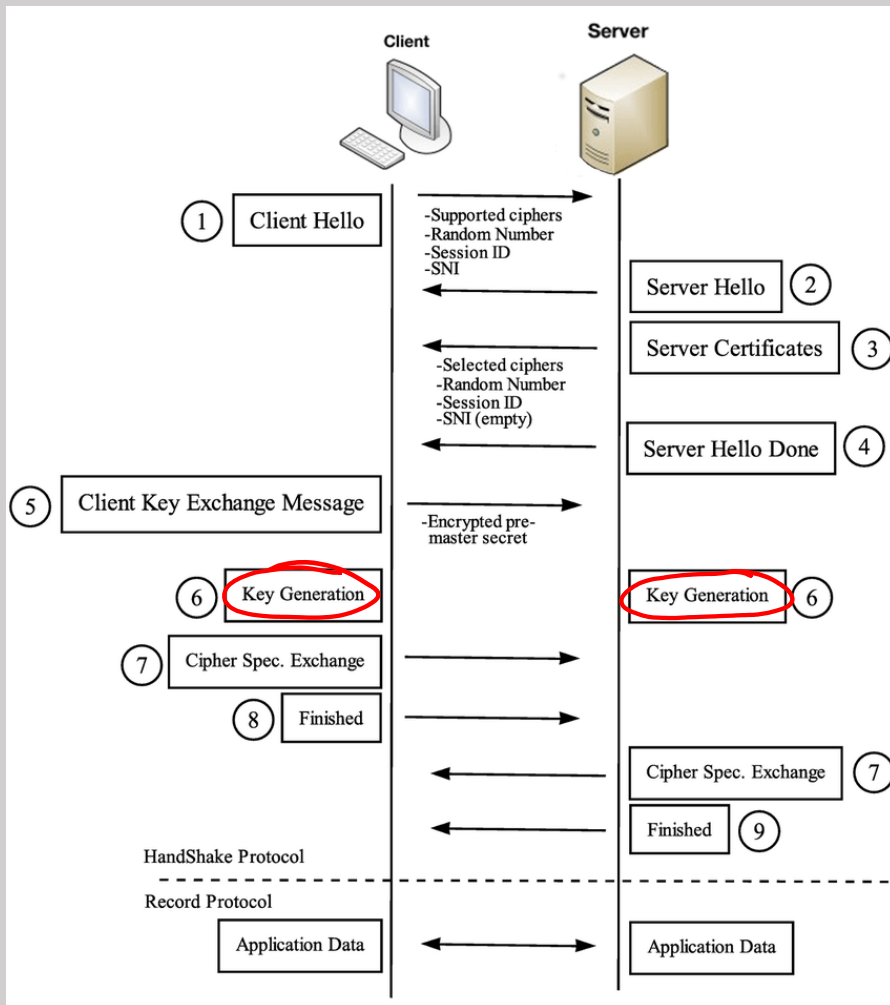
Encryption

- These are related mechanisms we use to achieve security in all layers
- They are also ideally our mechanisms used to establish **non-repudiation**, that you are who you say you are and cannot deny it
- Two types of encryption [1]:
 - Symmetric:
 - **Fast**
 - Asymmetric (public key cryptography):
 - **Slow**

Symmetric Encryption	Asymmetric Encryption
It is a type of encryption that uses a <u>single key</u> to both encrypt (encode) and decrypt (decode) data or information.	It is a type of encryption that uses <u>two keys</u> , a <u>private</u> and a <u>public key</u> , to encrypt and decrypt data.
The same <u>private key</u> is used for both <u>encoding</u> and <u>decoding</u> information.	The <u>public key</u> is only used to <u>encrypt</u> the data and the <u>private key</u> is used to <u>decrypt</u> the data.
This type of encryption is mostly used in modern computer systems to protect user <u>privacy</u> and <u>enhance</u> security.	This type of encryption is widely used for <u>sharing</u> of information or data <u>between</u> organizations and to <u>secure</u> online transactions.
<u>AES</u> is a standard symmetric encryption algorithm.	<u>RSA</u> is a standard asymmetric encryption algorithm.
The widely used symmetric encryption algorithms are <u>AES-128</u> , <u>AES-192</u> , and <u>AES-256</u> .	The widely used asymmetric encryption algorithms are <u>Diffie-Hellman</u> , <u>ECC</u> , <u>ElGamal</u> , <u>DSA</u> , <u>Elliptic curve cryptography (ECC)</u> , etc.

[1] Cloud Computing (T. Erl, Z. Mahmoud, R. Puttini / 2013) pg. 231 – 232

Transport Layer Security (TLS)



- Transport Layer Security (TLS) replaces the now-deprecated predecessor Secure Sockets Layer (SSL)^[1]
 - A cryptographic protocol designed to provide communications security over a computer network
 - There are several versions of the protocol, but **HTTPS** is the most publicly visible
- This is the mechanism we use to secure data as it leaves the cloud consumer organization's trust boundary, crosses the open internet and lands in the cloud provider's systems
- TLS uses the Public Key Infrastructure and digital certificates to secure web transactions^[2]
- All of this happens in ~100 milliseconds

[1]: https://en.wikipedia.org/wiki/Transport_Layer_Security

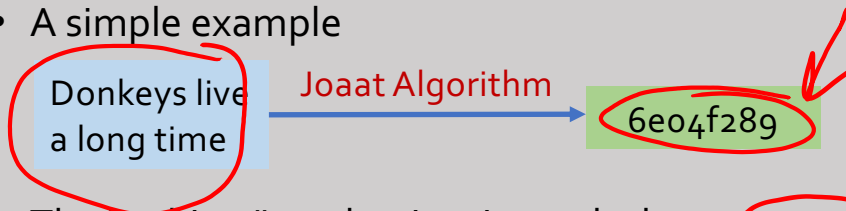
[2]: <https://www.ssl2buy.com/wiki/ssh-vs-ssl-tls>

Figure: https://www.researchgate.net/figure/TLS-handshake-protocol_fig1_298065605

Hashing (1/2)

- Why do we need hashing?

- A simple example



- The hashing "mechanism is used when a one-way, non-reversible form of data protection is required. Once hashing has been applied to a message, it is locked, and no key is provided for the message to be unlocked." [1]

- **Irreversibility**

- Irreversibility points to the fact that once you hash something, there is no way back.

- **Uniqueness**

- Unique, because no two hash values are ever the same for two different pieces of data.

- Use cases

- Hash passwords, credit card #s, and whatever important

- Identify or compare files or databases

- Rather than comparing the data in its original form, it's much easier for computers to compare the hash values.

- Benefits

- Hashing protects data while in storage, mitigates malicious intermediary threats, and limits the severity of exposed data

Hashing (2/2)

Hashing Algorithm

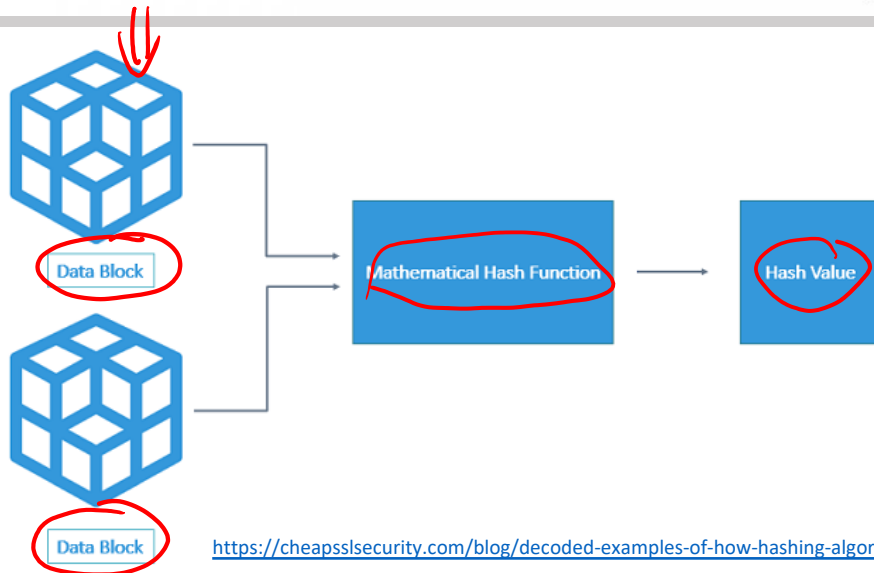


Hashing Function

"Behind every successful man, there is a great woman." — Groucho Marx

"Behind every successful hash algorithm, there is a great hash function."

A hash function is a mathematical function that converts an input value into a compressed numerical value – a hash or hash value. Basically, it's a processing unit that takes in data of arbitrary length and gives you the output of a fixed length – the hash value.



<https://cheapsslsecurity.com/blog/decoded-examples-of-how-hashing-algorithms-work/>

Image: Hash Function Structure

How Hashing Works?

To get the hash value of a pre-set length, you first need to divide the input data into fixed sized blocks. This is because a hash function takes in data at a fixed-length. These blocks are called 'data blocks.' The size of the data block(s) differs from one algorithm to another. But for a particular algorithm, it remains the same. For example, SHA-1 takes in the message/data in blocks of 512-bit only. So, if the message is exactly of 512-bit length, the hash function runs only once.

Popular Hashing Algorithms

- Message Digest (MD) Algorithm
- Secure Hash Algorithm (SHA)
- RACE Integrity Primitives Evaluation Message Digest (RIPEMD)
- Whirlpool
- RSA

Public Key Infrastructure (1/2)

Recall...

- We've seen public key encryption and authentication when doing things like setting up EC2 instances, but these are issued by a trusted source (AWS).

/home/manan/.ssh/public key

But now...

- How do we know whether to trust servers on the internet like facebook.com?
- **PKI** (or Public Key Infrastructure) is the framework of encryption and cybersecurity that protects communications between the server (your website) and the client (the users).
- Three key components *https*
 - Digital certificates
 - A digital certificate is like a drivers license — it's a form of electronic identification for websites and organizations.
 - Certificate authority
 - Digital certificates are usually digitally signed by a third-party certificate authority (CA), like Verisign and Comodo
 - Registration authority
 - Registration Authority (RA), which is authorized by the Certificate Authority to provide digital certificates to users on a case-by-case basis.
- These certificates are key to authentication and non-repudiation and are our major defense against **malicious intermediaries**

Public Key Infrastructure (2/2)

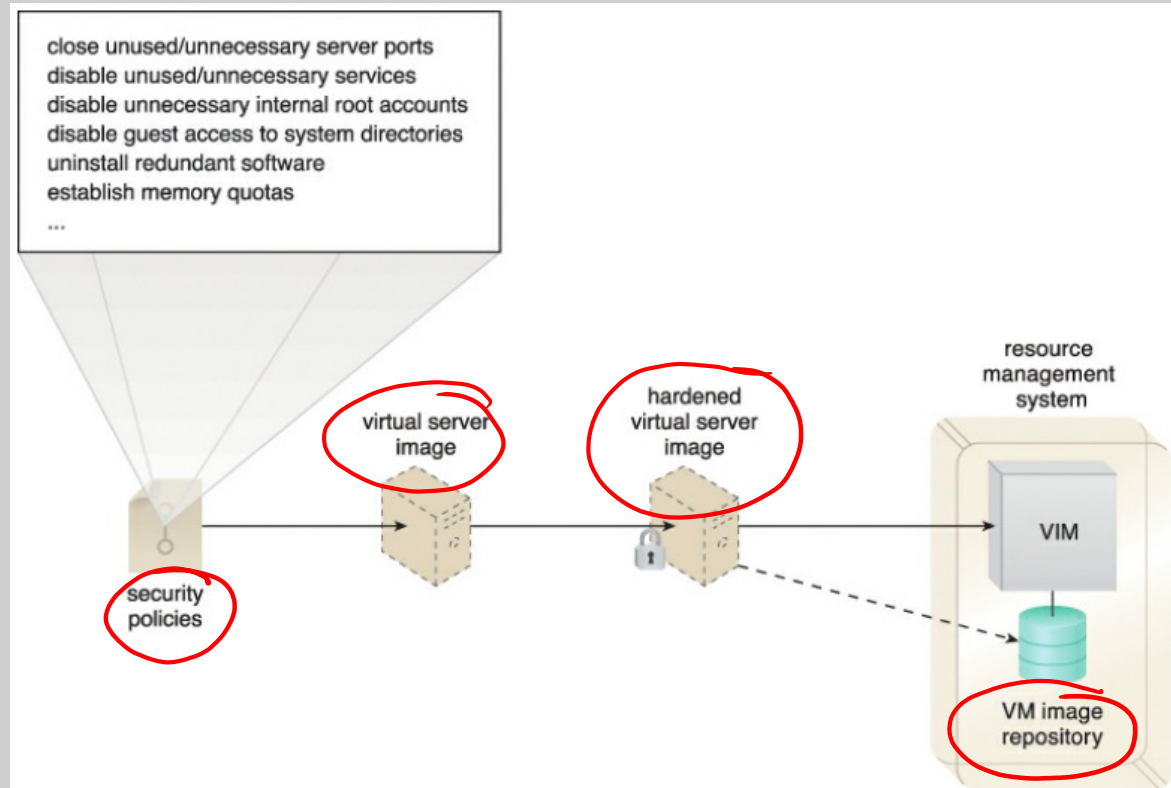
- **Public key:**
 - The public key is available to any user that connects with the website
- **Private key:**
 - The private key is a unique key generated when a connection is made, and it is kept secret
- **When communicating ...**
 - The client uses the public key to encrypt and decrypt, and the server uses the private key

Now let's watch this:

https://www.youtube.com/watch?v=Q_LD54YuZcc

Hardened Virtual Server Images

- As previously discussed in architecture lecture, we often create virtual machines from template configurations
- "Hardening is the process of stripping unnecessary software from a system to limit potential vulnerabilities that can be exploited by attackers." [1]
- Hardening examples:
 - Removing redundant programs
 - Closing unnecessary server ports
 - Disabling all unused services, internal root accounts, and guest access
- This can be done for you by the cloud provider, or you can perform this process yourself through your own security policy

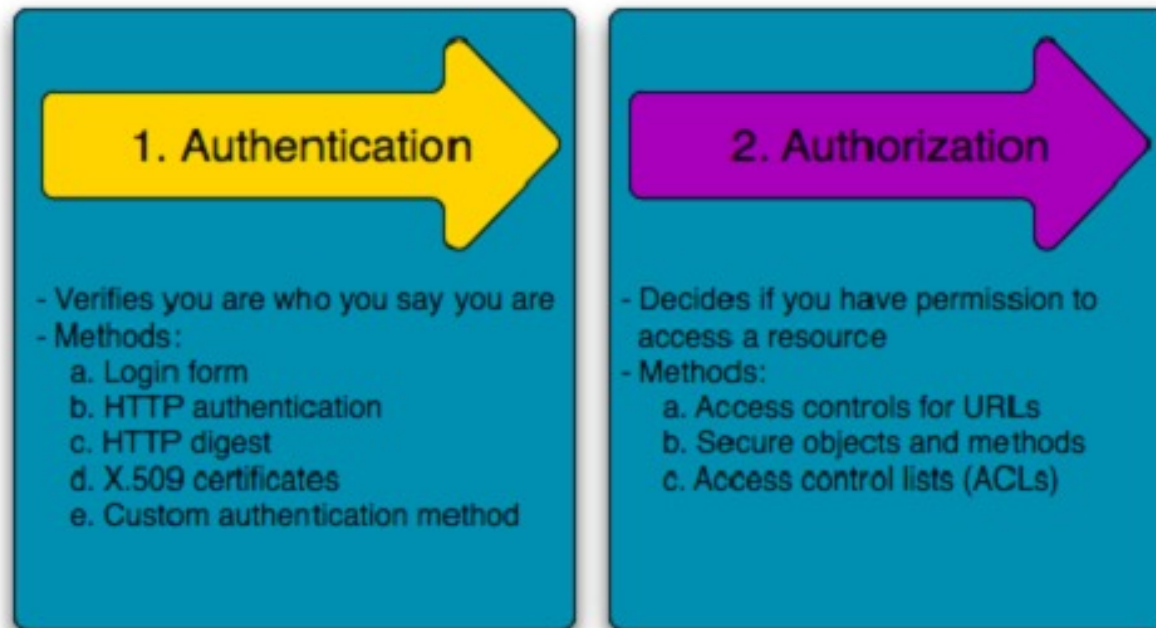


A cloud provider applies its security policies to harden its standard virtual server images. The hardened image template is saved in the VM images repository as part of a resource management system.

Single Sign-On (SSO) (1/2)

- Challenges

- Propagate the authentication and authorization information for a cloud service consumer across multiple cloud services can be a challenge, especially if numerous cloud services or cloud-based IT resources need to be invoked as part of the same overall runtime activity.

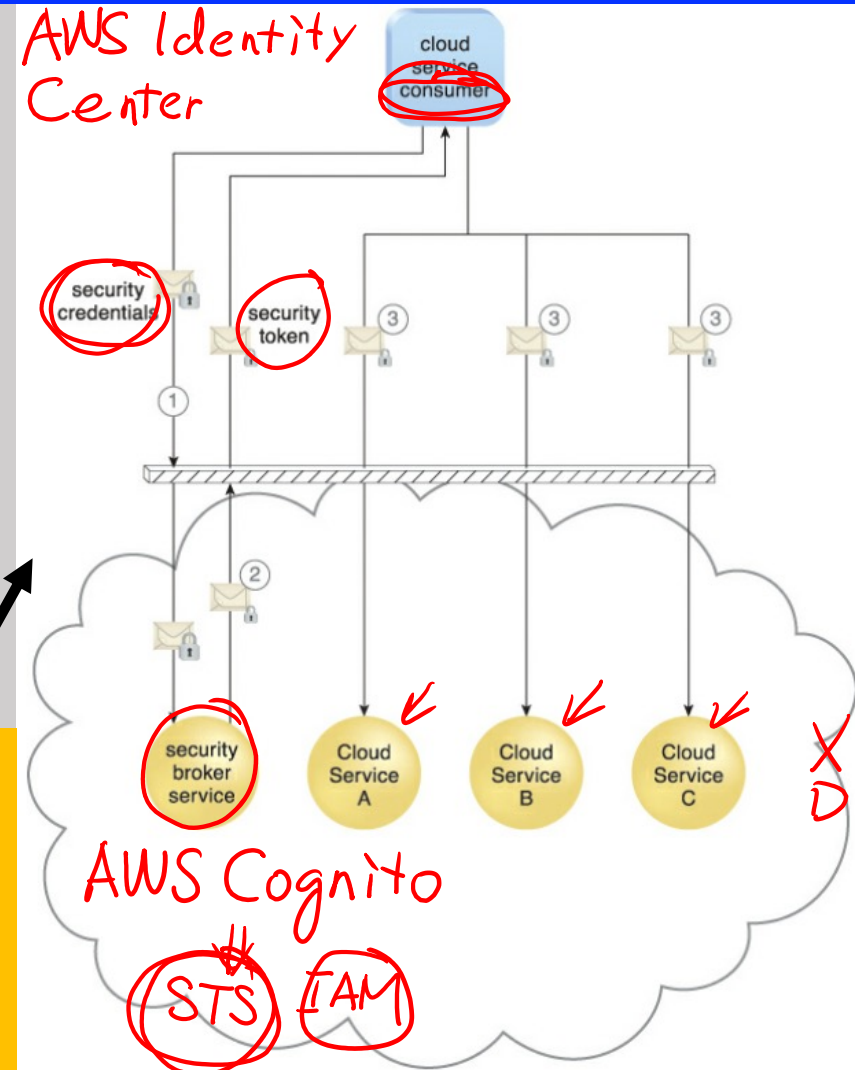


Single Sign-On (SSO) (2/2)

- SSO is a mechanism by which architectures with multiple services allow the user to seamlessly transition from one service to another while maintaining authentication
 - Single Sign-On doesn't eliminate threats, your architecture still requires a robust authentication mechanism
 - Since it is essentially a **mandatory** feature of any modern suite of web apps it's important to ensure you implement single sign-on properly with industry standards like OAuth, OpenAM or the mechanisms provided by your modern cloud provider
- The logo for OpenAM, featuring the word "Open" in orange and "AM" in dark blue, with a red underline. Below it is the tagline "Authenticate - Authorise - Federate". To the right is a grey, 3D-style icon of a hexagonal shape.
- A circular logo for OAuth 2.0. The word "OAUTH" is written in a semi-circle at the top, and "2" is in the center. The word "OAUTH" is also written in a semi-circle at the bottom. The logo has a metallic, 3D appearance.



- (1) A cloud service consumer provides the security broker with login credentials.
- (2) The security broker responds with an authentication token (message with small lock symbol) upon successful authentication, which contains cloud service consumer identity information
- (3) The identity information is used to automatically authenticate the cloud service consumer by Cloud Services A, B, and C.





2

AWS Well-Architected Security Pillar

1. Revisit
2. Security Pillar Best Practices

AWS Well-Architected Security Pillar – Revisit (1/2)

- "The **Security pillar** encompasses the ability to protect data, systems, and assets to take advantage of cloud technologies to improve your security." [1]
- **Principles:**
 1. Implement a strong identity foundation (principle of least privilege and separation of duties/authorization)
 2. Enable traceability (monitor, alert and audit) *AWS Config AWS CloudTrail*
 3. Apply security at all layers (not just the gate into the system)
 4. Automate security best practices (improves ability to scale, reduces human error)
 5. Protect data in transit and at rest
 6. Keep people away from data (eliminate need for direct access or manual processing)
 7. Prepare for security events (have an incident management policy and processes)

[1] <https://docs.aws.amazon.com/wellarchitected/latest/framework/security.html>
<https://cloudtweaks.com/2019/04/pillars-of-aws-well-architected-framework/>

AWS Well-Architected Security Pillar – Revisit (2/2)

Best Practices

Security

To operate your workload securely, you must apply overarching best practices to every area of security. Take requirements and processes that you have defined in operational excellence at an organizational and workload level, and apply them to all areas.

Identity and Access Management

Identity and access management are key parts of an information security program, ensuring that only authorized and authenticated users and components are able to access your resources, and only in a manner that you intend.

Detection

You can use detective controls to identify a potential security threat or incident. They are an essential part of governance frameworks and can be used to support a quality process, a legal or compliance obligation, and for threat identification and response efforts.

Infrastructure Protection

Infrastructure protection encompasses control methodologies, such as defense in depth, necessary to meet best practices and organizational or regulatory obligations.

Data Protection

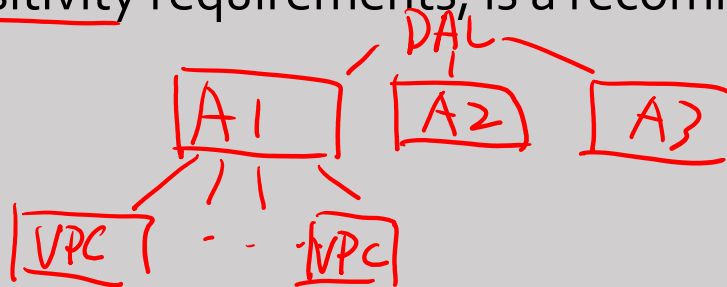
Before architecting any system, foundational practices that influence security should be in place. For example, data classification provides a way to categorize organizational data based on levels of sensitivity, and encryption protects data by way of rendering it unintelligible to unauthorized access. These tools and techniques are important because they support objectives such as preventing financial loss or complying with regulatory obligations.

Incident Response

Even with extremely mature preventive and detective controls, your organization should still put processes in place to respond to and mitigate the potential impact of security incidents.

Security Pillar Best Practices – Security

- We must apply overarching best practices to every area of security
- Take requirements and processes that you have defined in operational excellence at an organizational and workload level, and apply them to all areas
- Staying up to date with AWS and industry recommendations and threat intelligence helps you evolve your threat model and control objectives.
- Automating security processes, testing, and validation allow you to scale your security operations.
- In AWS, segregating different workloads by account, based on their function and compliance or data sensitivity requirements, is a recommended approach



Security Pillar Best Practices – IAM

- The **identity and access management (IAM)** "mechanism encompasses the components and policies necessary to control and track user identities and access privileges for IT resources, environments, and systems."^[1]
- Privilege-management elements form the **core** of **authentication** and **authorization**
 - Define principals: accounts, users, roles, and services that can perform actions in your account
 - Build out policies aligned with these principals, and implement strong credential management
- Four main components:
 - **Authentication**: Username and password, MFA, etc.
 - **Authorization**: What the role has access to or permission to perform
 - **User Management**: The ability to create and manage groups and users
 - **Credential Management**: Pairing credentials (e.g. keys) to authenticated accounts
- In AWS, privilege management is primarily supported by the **AWS Identity and Access Management (IAM)** service, which allows you to control user and programmatic access to AWS services and resources.

Security Pillar Best Practices – Detection

- Use detective controls to identify a potential security threat or incident. For example:
 - Conducting an inventory of assets and their detailed attributes promotes more effective decision making (and lifecycle controls) to help establish operational baselines.
 - You can also use internal auditing, an examination of controls related to information systems, to ensure that practices meet policies and requirements and that you have set the correct automated alerting notifications based on defined conditions
- Through logs, alerts and monitors provided by your own application and cloud provider services you can detect:
(1) Potential Misconfigurations (2) Threats (3) Unexpected Behavior (4) Exploits
- May even be required for legal or compliance obligations
- Use these steps:
 - 1) **Configure**: Configure active and passive monitoring systems, spend high here to create highly available and secure systems
 - 2) **Investigate**: Regularly monitor, set up alerting, investigate and actively look for problems, automate when possible (e.g. blacklisting)
- In AWS, you can implement detective controls by processing logs, events, and monitoring that allows for auditing, automated analysis, and alarming
 - **CloudTrail logs** and **CloudWatch** provide monitoring of metrics with alarming
 - **AWS Config** provides configuration history
 - **Amazon GuardDuty** is a managed threat detection service
 - **Service-level logs** are also available, e.g., Amazon Simple Storage Service (Amazon S3) logs access requests

Security Pillar Best Practices – Infrastructure Protection

- Infrastructure protection encompasses control methodologies, such as defense in depth, necessary to meet best practices and organizational or regulatory obligations.
- This your architecture, how have you designed your application to use security mechanisms to protect your data and IT infrastructure in all layers

Protecting Networks:

1. Create network layers (subnets), use this to restrict access
2. Control all traffic between layers
3. Implement inspection and protection (firewalls and gateways)
4. Automate self-defending network based on threat intelligence and anomaly detection (e.g. intrusion detection)

Protecting Compute Resources:

1. Perform vulnerability management (keep track of libraries, tools, APIs used, monitor for vulnerability reports and patch), your cloud service provider may do this for you
2. Reduce attack surface (hardening!)
3. Enable people to perform actions at a distance (i.e. reduce manual error through automation)
4. Implement managed services
5. Validate software integrity (code signing)

- In AWS,
 - You should use **Amazon VPC** to create a private, secured, and scalable environment
 - AWS customers are able to tailor, or harden, the configuration of an AWS EC2, ECS, or Elastic Beanstalk instance, and persist this configuration to an immutable Amazon Machine Image (AMI)
 - Then, whether triggered by Auto Scaling or launched manually, all new virtual servers (instances) launched with this AMI receive the hardened configuration

<https://docs.aws.amazon.com/wellarchitected/latest/framework/wellarchitected-framework.pdf>

Security Pillar Best Practices – Data Protection

- Before architecting any system, foundational practices that influence security should be in place, for example:
 - Data classification provides a way to categorize organizational data based on levels of sensitivity
 - Data encryption protects data by way of rendering it unintelligible to unauthorized access
- Best Practices:
 - Identify the data within your workload (what needs protecting)
 - Define data protection controls (give yourself ways to protect it)
 - Define data lifecycle management (retention policies, access management, sharing, etc.)
 - Automate identifying and classifying
 - Implement secure key management and enforce encryption at rest
 - Enforce IAM, without this everything else is pointless
 - Use and enforce the use of mechanisms (IAM, hashing, encryption) to keep people away from data
- In AWS,
 - As an AWS customer you maintain full control over your data.
 - AWS makes it easier for you to encrypt your data and manage keys, including regular key rotation, which can be easily automated by AWS or maintained by you.
 - Detailed logging that contains important content, such as file access and changes, is available.
 - AWS has designed storage systems for exceptional resiliency.
 - Versioning, which can be part of a larger data lifecycle management process, can protect against accidental overwrites, deletes, and similar harm.
 - AWS never initiates the movement of data between Regions.
 - AWS provides multiple means for encrypting data at rest and in transit

Security Pillar Best Practices – Incident Response

- No programmer and no technology is perfect, an incident will happen
- Contain spread, limit exposure, reduce severity by being prepared to respond:
 - Establish the goal or response objectives (containing, mitigating, recovering, etc.)
 - Document plans
 - Know what you have and what you need (in terms of logs, snapshots and evidence)
 - Automate where possible
 - Choose scalable solutions
 - Educate your team
 - Pre-deploy disaster recovery IT resources
 - Simulate disaster scenarios and evaluate your response through "game days"
 - Continuously iterate, learn and improve your process when problems happen
- In AWS,
 - Detailed logging is available that contains important content, such as file access and changes.
 - Events can be automatically processed and trigger tools that automate responses through the use of AWS APIs.
 - You can pre-provision tooling and a "clean room" using AWS CloudFormation. This allows you to carry out forensics in a safe, isolated environment.

The background of the image is a stylized world map divided into four quadrants by a vertical and a horizontal line. The top-left quadrant is red, the top-right is blue, the bottom-left is yellow, and the bottom-right is green. The word "Kahoot!" is written in a large, white, bold, sans-serif font across the center of the image, spanning all four quadrants.

Kahoot!