LEE JIHU

34061648

ICT379 assignment part2

**Table of Contents**

**Discussion of Security Problems**

* **Who Could be the Potential Adversaries?**
* **What Could be the Security Requirements?**

**Description of Security Architecture**

* **How AWS Works**
* **How to Achieve the Security Requirements**

**Analysis of Limitations**

**References**

**Discussion of Security Problems**

Who Could be the Potential Adversaries?

Potential adversaries that may threaten Amazon Web Service (AWS) may include adversaries with malicious intentions or users who may threaten purely incompetence within an organization. One particular threat AWS users may face, for example, is user access control called identity and access management (IAM), which could seriously damage the service if the company allows users to access more resources than they need. For example, users who are granted access may accidentally delete data from the database, resulting in months or years of work disappearing. *(Alsmadi & Karabatis & Aleroud. 2017)* Data deletion by companies can have extreme consequences for AWS system client users to remove account data and lose their accounts. If this happens on a large scale, many client users will also lose all progress in their work. IAM security threats are generally (not always) related to enemies who have no malicious intentions but cause problems due to incompetence. Therefore, users must be granted access only if they are trusted users. Another security problem with AWS is loose security group policy. Instead of configuring permissions for each individual user, it is easy for administrators to create group policies only for user groups. However, this can lead to security defects that can be exploited by malicious-intentioned attackers. Few group policies have a good understanding of how AWS security works, so AWS resources can be accessed. These malicious attackers can use a bot to run scripts and attack open ports. Attacking an open port allows an attacker to take advantage of a bug that may be in an application running on that open port. Attackers can access data, install malware, damage applications, or gain control rights. *(Dieter Gollmann. 2011)* For example, AWS workloads may have an open port 25 (SMTP). If this port is unused and does not need to be opened, an attacker can search for a port to see the version of that port application and find a known vulnerability. Based on the vulnerability found, an attacker can use it to inject malware or anything he or she wants. The reason why opposition can occur is that an employee of a company has been fired and wants revenge on the company. However, the most common reason is that data is stolen and sold, or encrypted using ransomware to maintain data ransom, and victims have to pay to decrypt the data.

What Could be the Security Requirements?

AWS uses four key security strategies which include *(Albert Anthony. 2018)*:

* Prevent

Prevention includes user-assigned authority definition, infrastructure protection, and data protection. Preventing security breaches in AWS is critical because it prevents potential enemies from unauthorized access to cloud systems and causing previously mentioned problems. The best result in terms of security is to prevent as many security breaches as possible. If the attack is blocked, no further action is required, but if the attack is not blocked, further action is required.

* Detect

There should be a system that can detect security breaches. Cloud computing systems always have vulnerabilities somewhere, so they must have detection systems that can detect potential threats from cloud systems. Rapid detection of security threats can prevent system damage by stopping attacks faster. This means that faster detection speed increases response speed.

* Respond

After detecting a security breach, the next step is to respond to it. AWS response works with automated incident response and recovery to help security teams focus on finding the root cause of the attack. It is important to find the root cause of the security breach, as it can strengthen the security of AWS systems and prevent future attacks that can occur in the same way. Looking at an example of an open port, if the open port is attacked and the security system detects an attack, the port must be closed to prevent further attacks from occurring on that port. However, some security violations may not be as simple as attacking open ports, which can make it harder to detect more complex attacks and find root causes.

* Remediate

If the root cause of the security breach is found, the next step is to recover from the attack and solve the security problem. AWS solves security issues by implementing an automated system called CloudEndure Disaster Recovery so that continuous replication of AWS systems can return to the original state of the attack. For example, if the user is given more privileges than IAM requires and the user clears the entire data load from the system, CloudEndure allows the system to return to its state before a disaster occurs.

Other security requirements that AWS and many other cloud computing systems follow include:

* Authenticity – confirming a user’s permissions and access to a system. AWS uses I AM for this.
* Confidentiality – ensuring that only intended users have access to data
* Integrity – ensuring that data is not changed or manipulated unless needed to by an authenticated database administrator.
* Availability – ensures that all AWS systems are available to those that need it

**Description of Security Architecture**

How AWS works.

AWS is a platform that provides flexible, reliable, scalable, easy-to-use, and cost-effective cloud computing services. AWS provides three services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Being a cloud computing service means that AWS users do not have to have things like their own data center or software. For example, if a user of AWS tries to have his or her own set of virtual machines (e.g., Windows 2016 server with many other Windows OS VMs), AWS can provide resources without having to own the host of that virtual machine and the hardware it needs to run. To explain in more detail what IaaS. AWS can do, Netflix, a video streaming service, is an example of a large company using AWS. Netflix uses AWS to store customer data, analysis, and transcoding of engines and videos that recommend videos to customers. AWS' PaaS eliminates the need for organizations to focus on resources, software maintenance, capacity planning and patching of products, allowing them to focus on application deployment and management. SaaS provides users with complete software managed by AWS. *(Albert Anthony. 2018)*

How to Achieve the Security Requirements

AWS' first security requirement is to prevent security threats. One way is to define user rights using IAM. The best way is to give IAM users the minimum rights they need to complete the task. For example, if the operation of the IAM user/process is reading data, the IAM user/process is only authorized to read from that data and does not have the right to modify that data. This prevents data changes and maintains data integrity. IAM users authorized to modify data must be trusted users. Otherwise, an internal attack may occur.

The second security requirement is to detect security threats. AWS uses VPN to detect potential security threats from outsiders. One example of suspicious behavior is when a series of login attempts for a single IP address fails, which is usually a signal for an attacker to access the system. The opponent may be doing this through indiscriminate attacks or preceding attacks. VPN scans can be used to detect these potential security threats. Search terms can search for failed login attempts and sort results by source IP, destination IP, user, source type, and number. You can find failed login attempts using the same search terms as 'fail\* password | stat count by src, dest, user, sourcetype | sort – count > 2'.

The third security requirement is to respond to security threats. For example, an appropriate response to a series of login attempt failures is to prevent the source IP from attempting login any more. AWS can do this through Virtual Private Cloud (VPC). You can configure a network access control list (ACL) using the VPC dashboard. In this case, it is recommended to create an ACL that blocks suspicious IPs. The fourth security requirement is to modify it. If you use this example again, you may need to change only the password of the attack/attack system if the suspicious IP is blocked. Encryption security is enhanced because passwords can be complicated enough by combining numbers, symbols, and case letters. Hash encryption schemes such as SHA1 or SHA256 ensure password security, so it is not recommended to store passwords in plain text.

IAM allows AWS to meet authentication security requirements and ensure data integrity with minimal privileges to users. In terms of confidentiality, encrypted data that is idle or in transit is best. AWS uses a hardware security module (HSM) to store encryption keys, which is called AWS CloudHSM. If the key needs to be stored in-house, HSM is also used, and you can access the key by connecting directly to IPSec *(James S. Tiller .2001)* via IPSec VPN, Amazon VPC, or AWS. For availability, AWS uses technologies such as firewalls, security groups, initial session restrictions, and ACLs to protect against DoS/DDoS attacks. For example, AWS uses an initial (half-open) session limit to prevent flooding of TCP SYN packets. If the initial TCP SYN connection amount exceeds the normal size, delete additional TCP SYN packets from the source IP to prevent packet flooding.

**Analysis of Limitations**

One of AWS' security restrictions is VPC. One drawback of VPC is that IP control may not be sufficiently subdivided when filtering network traffic because it is based only on IP range, protocol type, and port range. The ACL of the VPC allows only 18 application protocols, and users must implement their software security applications if they want to go one step further. *(Messaoud Benantar.2006)* Another security limitation of AWS is key circulation in the Key Management System (KMS). Since there is little control over key circulation and AWS KMS has key circulation time (once a year), it cannot force key circulation provided by AWS users. Key circulation is not allowed in the key circulation schedule if the user wants to perform key circulation faster. The user can import the key himself, but the user can manually and fully control the imported key, and the KMS of AWS does not touch the imported key. In other words, the user must establish key circulation and decrypt/re-encrypt data for the imported key. *(Roger A. Grimes.2021)*

**Reference**

Izzat M Alsmadi & George Karabatis & Ahmed Aleroud. 2017. Information Fusion for Cyber-Security Analytics. SPRINGER

Dieter Gollmann. 2011. Computer Security (3rd ed)

Albert Anthony. 2018. AWS: Security Best Practices on AWS: Learn to secure your data, servers, and applications with AWS. Packt publishing

 James S. Tiller. 2001. A Technical Guide to IPSec Virtual Private Networks. CRC press

Messaoud Benantar.2006. Access Control Systems: Security, Identity Management and Trust Models. SPRINGER

Roger A. Grimes.2021. Hacking multifactor authentication. WILEY