SECURITY ON AWS
By Max Ellsberry

AWS Security Standards

- The IT infrastructure that AWS provides has been designed and managed in alignment with the best practices and meets a variety of standards. Below are some of the standards Amazon has listed.
- Service Organization Control (SOC) 1: Statement on Standards for Attestation Engagements (SSAE) 16: International Standards for Assurance No. 3402 (ISAE 3402) formerly Statement on auditing Standards (SAS) 70
- SOC 2
- SOC 3
- (FISMA) - Federal Information Security Management Act

MORE...

- (DDM) Department of Defense
- (IATMP) Information Assurance Certification and Accreditation Process
- (FedRAMP) Federal Risk and Authorization Management Program
- C午后 Computing Security Requirements Guide (SRG) Levels 2 and 4
- Payment Card Industry Data Security Standard (PCI DSS) Level 1
- International Organization for Standardization (ISO) 9001 and 27001
- International Traffic in Arms Regulations (ITAR)
- Federal Information Processing Standard (FIPS) 140-2
Some Industry Specific Standards

- (CJIS) Criminal Justice Information Services
- (CSA) Cloud Security Alliance
- (FERPA) Family Educational Rights and Privacy Acts
- (HIPAA) Health Insurance Portability and Accountability Act
- (MPAA) Motion Picture Association of America

AWS Global Infrastructure

- **Physical and Environmental Security** - The data centers that Amazon houses are state of the art using architectural and engineering. Amazon has had experience with operating large scale data centers for years. Physical access to facilities is strictly controlled by security staff. Amazon only provides data center access and information to employees and contractors who have legitimate business and need such privileges.

- **Fire Detection and Suppression** - AWS data centers have an automatic fire detection and suppression to reduce risk. The fire detection system consists of mechanical and electrical infrastructural spaces, chiller rooms and generator rooms. These areas are also protected by wet pipe, double interlocked pre-action, or gaseous sprinkler system.

AWS Global Infrastructure Continued...

- **Power** - AWS data centers power systems are designed to be redundant and maintainable with an impact to operations 24/7. (UPS) Uninterruptible power supply in the event of electrical failure and essential loads in the facility.

- **Climate and Temperatures** - Climate control is required to prevent the over heating of servers and other hardware to reduce the risk of outages. AWS facilities have personnel and system monitors that maintain temperatures and humidity at appropriate levels.

- **Management** - AWS monitors electrical, mechanical, and life support systems and other equipment so that any issue is identified immediately. The AWS staff performs preventive maintenance to maintain operability of equipment.

- **Storage Device Decommissioning** - When a storage device reaches the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals.
Business Continuity Management

Amazon’s infrastructure has a high level of availability and provides customers with the features to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal impact to the customer.

- **Availability** - Data centers are built in clusters in various global regions. All Amazon data centers are online and serving customers. In case of any failures traffic is directed away from the affected area. Core applications are deployed in a N+1 configuration so that in an event of failure there is sufficient capacity to enable traffic to be load balanced to remaining sites.

AWS provides customers with flexibility to place instance and store data in different geographic regions and across different availability zones within each region. Each AZ is designed as an independent failure zone.

Incident Response

- The Amazon Incident Management team employs industry standard diagnostic procedures to drive resolution of business impacting events. Staff operates 24/7 with 365 days of coverage to detect incidents.
Communication

- AWS has implemented an internal communication method at a global level to help employees understand their respectful role and to communicate significant events in a timely manner. Such methods are orientations, job training, and video conferences, etc., via Amazon intranet.
- AWS has implemented a strong external communication method to support its customer base and community. A Service Health Dashboard is available and maintained to alert customers of issues that may be of broad impact.

Network Security

- The AWS network has been architected to permit you to select the level of security and resiliency appropriate for your workload. To enable you to build geographically dispersed, fault-tolerant web architectures with cloud resources, AWS has implemented a world-class network infrastructure that is carefully monitored and managed.
- Network devices, including firewalls and other boundary devices, are in place to monitor and control communications. These boundary devices employ rule sets, access control lists, and configurations to enforce the flow of information to specific information systems services.
- ACLs, or traffic flow policies, are established on each interface, which manage and enforce the flow of traffic. ACL policies are approved by Information Security. These policies are automatically pushed to ensure these managed interfaces have the most up-to-date ACLs.
Secure Access Points

- AWS have strategically placed limited access points to the cloud. Customer can access these access points called APIs endpoints, and they permit secure HTTP access that allow you to create a communication session with AWS. To support customers with Federal Information Processing Standard (FIPS) cryptographic requirements, the Secure Sockets Layer (SSL) terminating load balancers in AWS GovCloud (US) are FIPS 140-2 compliant.
- AWS has implemented network devices that are dedicated to managing interfacing communications with internet service providers.

Transmission Protection

- You can connect to an AWS access point via HTTP or HTTPS using SSL, a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery. For those who need extra layers of network security, AWS offers Amazon Virtual Private Cloud which provides a private subnet with the AWS cloud and the ability to use IPSec Virtual Private Network (VPN) device to provide an encrypted tunnel.

Network Monitoring and Protection

- Distributed Denial of Service (DDoS) Attacks - All AWS APIs endpoints are hosted on a large internet scale and built on the same infrastructure that Amazon was built on. Proprietary DDoS mitigation techniques are used.
- Man In The Middle (MITM) Attacks - All of AWS APIs are available via SSL protected endpoints that provide secure authentication. Amazon EC2 AMIs automatically generate new secure shells (SSH) host certificates on first boot and log them to the instances console.
- IP spoofing - Amazon EC2 cannot send spoof network traffic. The AWS firewall will not permit an instance to send traffic with a source IP or MAC address other than its own.
Network Monitoring and Protection

- **Port Spoofing** - Unauthorized ports scans by Amazon EC2 customers are a violation of AWS Acceptable Use Policy. Violations of the AWS AUP are taken seriously and every reported violation is investigated. When detected that port is stopped and closed. You can request conduct vulnerability scans as required to meet your compliance requirements. These scans are limited to your own instances and must not violate Amazon AUP.

- **Packet Sniffing by Other Teams** - While Amazon does not provide ample protection against one customer inadvertently or maliciously attempting to view another customer's data as a standard practice you should encrypt sensitive traffic.

AWS Account Security Features

- Amazon provides many tools and features that you can use to keep your AWS account and resources safe from unauthorized use.

Credentials

- AWS uses several credentials for authentications.
AWS Cloud Service-Specific Security

- **Compute Services** - AWS provides a variety of cloud-based computing services that include a wide selection of compute instances that can scale up or down automatically.
- **EC2 Security** - Consists of multiple levels of security: The hypervisor, instance isolation, host operating system, system and guest operating system, API access, Amazon EBS Security.

Networking

- AWS provides a range of networking services that enable you to create a logically isolated network that you define, establish a private network connection to AWS cloud use a highly available and scalable DNS service, and deliver content to your end user with low latency at high data transfer speeds.

Elastic Load Balancing Security

- Takes over the encryption and decryption work from the Amazon EC2 instances and manages it centrally on the load balancer.
- Offers clients a single point of contact, and can also serve as the final line of defense against attacks on your network.
- When used in an Amazon VPC, supports creation and management of security groups associated with your ELB to provide additional networking and security options.
- Supports end-to-end traffic encryption using TLS (previously SSL) on those networks that use secure HTTP (HTTPS) connections.
Amazon VPC Security

- We have already seen in earlier chapters how we can make our Amazon Virtual Private Cloud more secure by using the following security options:
  API Access, Subnets and Route Tables, and Security Groups (Firewall)