Cloud Security Overview

Murat Kantarcioglu

Outline

- Current cloud security techniques
  - Amazon Web services
  - Microsoft Azure
- Cloud Security Challengers

Amazon Security Overview

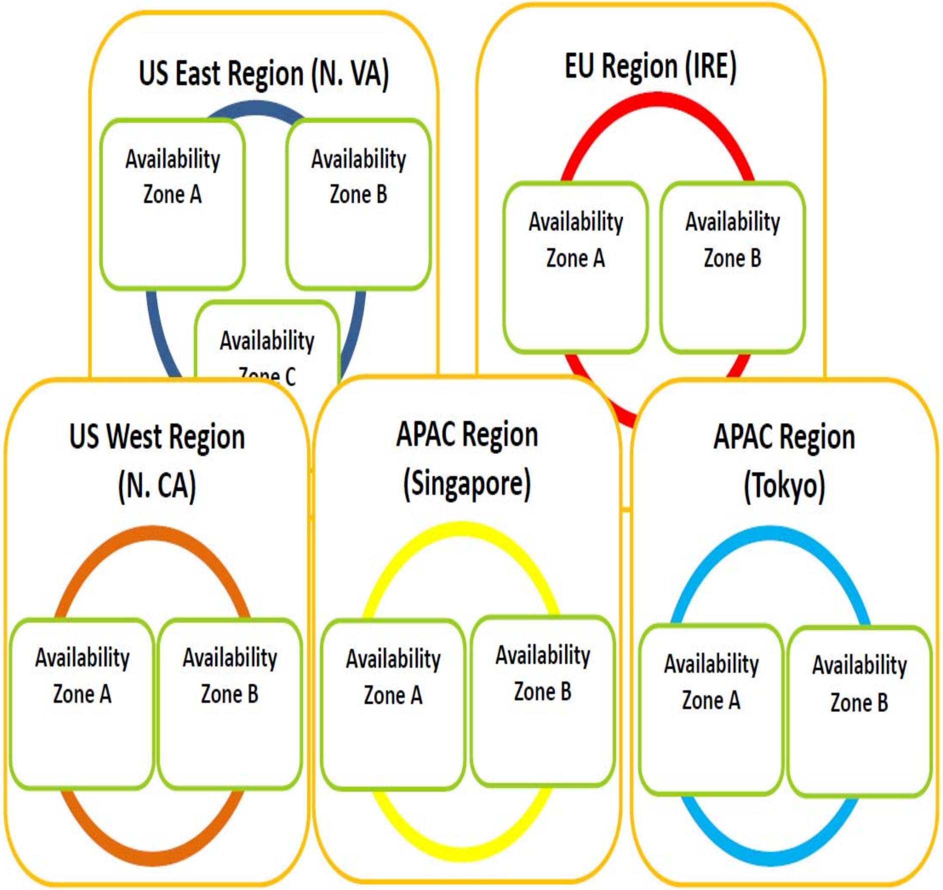
- AWS is compliant with various security certifications
  - E.g., FISMA (Federal Information Security Management Act)- Low Level
  - Internal information, communication and employee lifecycle management to increase security

AWS Physical Security

- Data centers are protected by many security features and safe guards
  - Two factor authentication, security force etc.
  - Fire Detection and suppression
  - Power
  - Climate and Temperature safeguards

AWS Configuration and Continuity Management

- Changes are reviewed, tested, and approved before rolled out.
- Different availability zones to separate faults
  - Different regions could be selected for regulatory compliance or increasing reliability.
- 24x7 incident response team
- Backups for stored data
- Physical devices are erased using DoD or NIST media sanitization techniques



AWS Identity and Access Management

- For each AWS account, you can create multiple users with different credentials
- For each user, you can give different rights
  - More details on this when we cover Identity management and cloud.
- Multi-factor authentication based on hardware tokens
- Key and Certificate Rotation for increased security

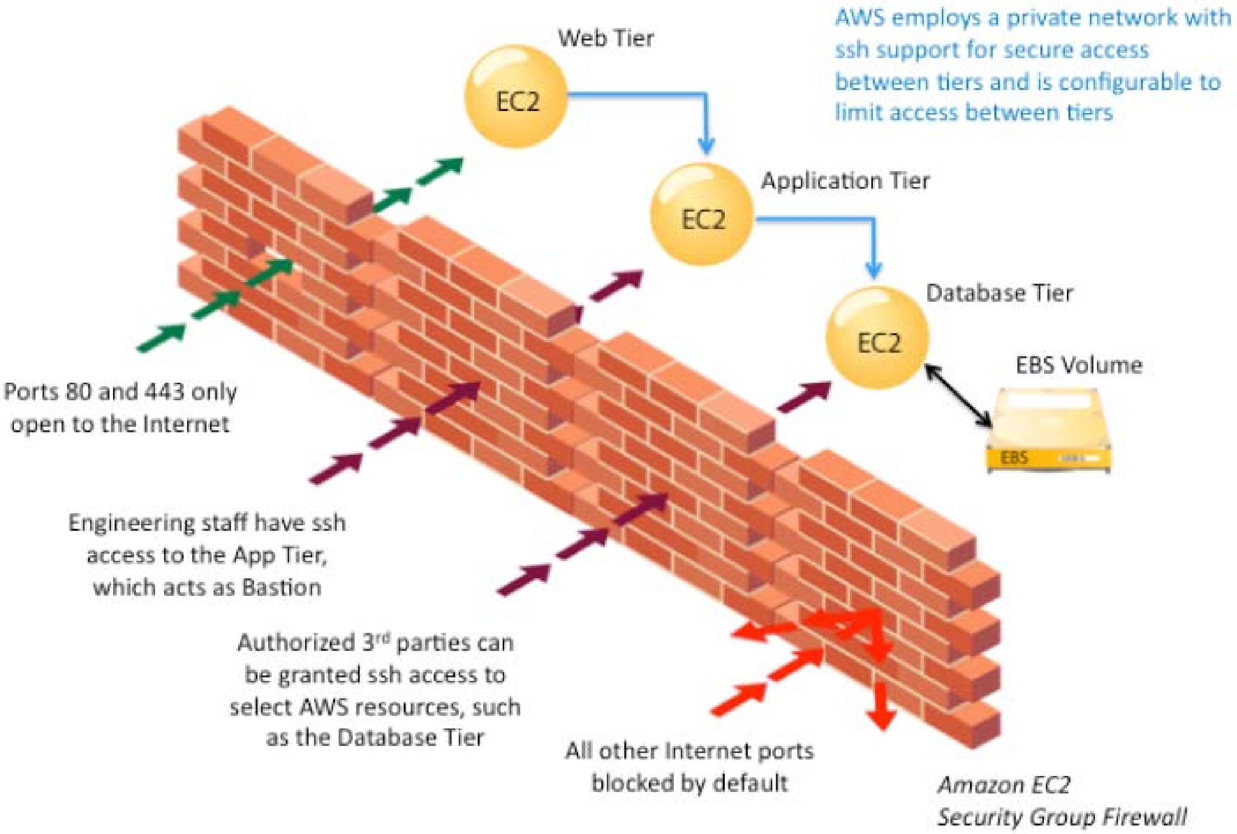
AWS Network Security Features

- Increased reliability against DDOS
- SSL based access to almost all resources to prevent man in the middle attacks
- All EC2 instances needs to use their actual IPs and MAC addresses.
- Packet Sniffing by other tenants are prevented by Hypervisor
  - We will talk about Hypervisor’s in detail later.
- You can create Virtual Private Clouds that are distinct, isolated network within cloud.

EC2 Security

- Host operating systems are protected
  - Two factor authentication
  - Auditing
- Guest operating systems must be controlled by users
- Firewalls

EC2 Firewall

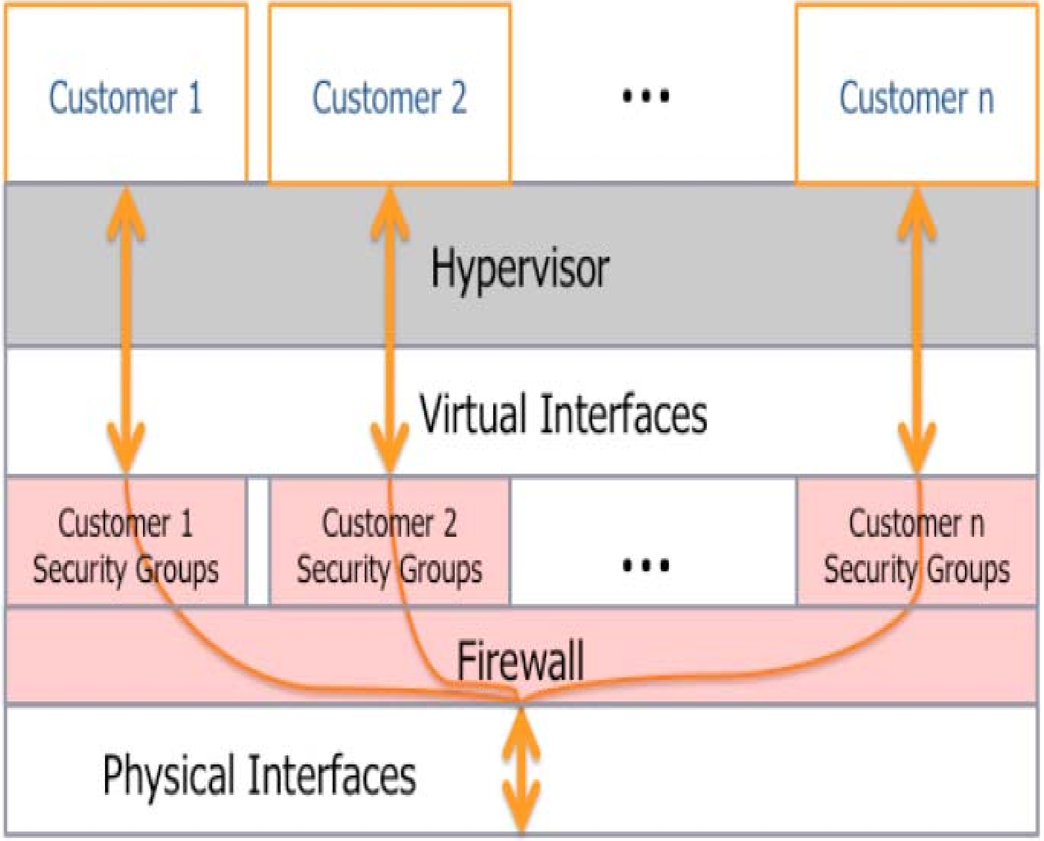

Web Tier
EC2
AWS employs a private network with ssh support for secure access between tiers and is configurable to limit access between tiers
EC2
Application Tier
Database Tier
EC2
EBS Volume
EBS
Ports 80 and 443 only open to the Internet
Engineering staff have ssh access to the App Tier, which acts as Bastion
Authorized 3rd parties can be granted ssh access to select AWS resources, such as the Database Tier
All other Internet ports blocked by default
Amazon EC2 Security Group Firewall

EC2 Firewall Features

- Firewall is not controlled through Guest operating system
  - X.509 certificates and keys are needed to authenticate with the firewall
- Guest OS level firewalls could be added for additional security

Hypervisor based Isolation and Security

- Hypervisors are used to limit access to resources and to maintain isolation between instances
- Prevents access to raw hard disks



Storage Systems (EBS, S3 etc.)

- SSL based secure APIs
- Authentication based on HMAC or public key crypto
- Security groups
- Possible Access logging
- Data can be encrypted by the customer

Microsoft Azure Overview

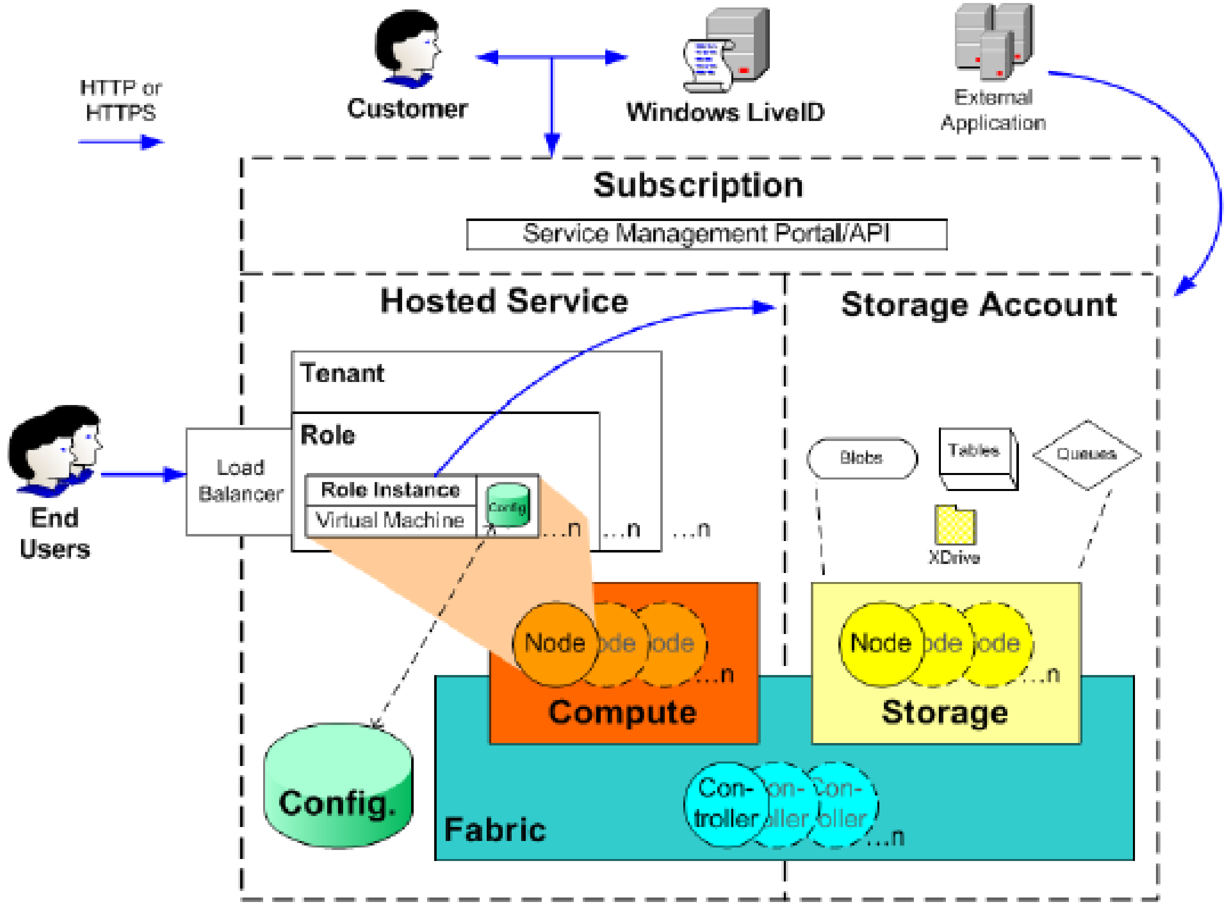


Figure 2: More granular illustration of Windows Azure components and relationships.

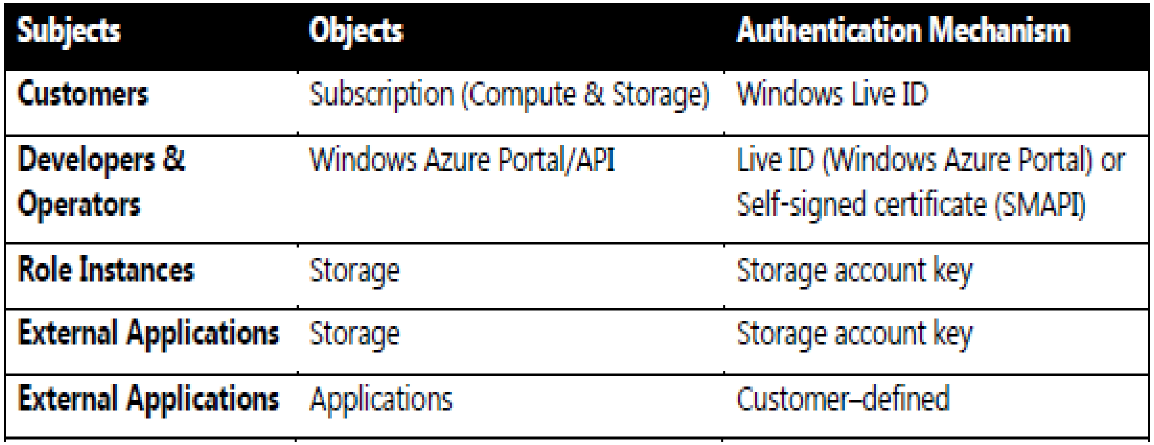
Azure Structure

- Each role instance is a new VM
- VMs run on Microsoft Azure Hypervisor
- One VM is special
  - Runs “hardened” root OS
  - Hosts Fabric Agent (FA)
- FAs manage Guest agents within Guest OSes on customer VMs.
- FAs manage storage nodes
- The collection of Hypervisor, VMs, FA and customer VMs comprises compute node.

Microsoft Azure Authentication

- SMAPI is a REST protocol for web services
  - Runs over SSL using self-signed certificates
- Certificates and keys store separately by Azure
  - Encrypts the keys and stores some secret location
- Fabric Controller keeps separate master key and authentication keys to authenticate with hardware devices

Table 1 - A summary of Windows Azure authentication mechanisms.



Subjects	Objects	Authentication Mechanism
Customers	Subscription (Compute & Storage)	Windows Live ID
Developers & Operators	Windows Azure Portal/API	Live ID (Windows Azure Portal) or Self-signed certificate (SMAPI)
Role Instances	Storage	Storage account key
External Applications	Storage	Storage account key
External Applications	Applications	Customer–defined

Access Control In Azure Storage

- User can create multiple accounts
- Each account has a storage key
- Given a storage key, you can access all the data related to storage key.
  - No fine grained access control !
- Data can be made publicly readable
- User can sign query templates using storage account key
  - Container lever access policies are also possible
- Two keys could be valid at any given time to allow key updates

Azure Isolation

- Hypervisors used for isolation
- Isolation of FC are achieved by limiting communication with FA
  - Unidirectional communication to FAs
    - FAs reply requests
  - All incoming messages assume to be untrusted
  - If possible some FCs are put on separate VLANs

Azure Packet Filtering

- Root OS and Hypervisor filters packets to prevent spoofed and unauthorized traffic.
- Customer access to VMs is limited
  - E.g., no remote terminal connection
- Connection between different applications is considered internet connection.
-

Other Azure Security and Reliability Features

- Cryptographic tools for data encryption
- Data deletion for disposed hardware
- Integrity checks for data
- Backups to increase availability
- Monitoring agents gather data from FCs and root OSs to create audit logs
- Personnel policies, physical security similar to Amazon

Main Cloud Security Problems

- VM- level attacks
  - Exploit potential vulnerabilities in hypervisor
- Cloud provider vulnerabilities
  - E.g. cross-site scripting vulnerability in Salesforce.com
  - Phishing
- Integrating cloud authentication with company authentication mechanisms
- Availability
- Single point of Failure
- Assurance of computational integrity by cloud provider

Issues with moving data to cloud providers

- Will cloud provider fight against a subpoena?
- Do you trust Azure logs to show gross negligence on Microsoft part?
- Contractual obligations?
- If you can hack one place for espionage Gmail could be a good starting point?
- Data lock-in

What is new in cloud computing security?

- Too big to fail?
  - What if Amazon hardware is confiscated?
  - What if Amazon fails?
- Hiding activity patterns
- Using cloud for crime?
- Secure cloud auditing
  - Mutual auditability

Quiz

- In Microsoft Azure Storage, for a given storage account, how would you enable fine grained access control? Your answer should be less than 30 words.