SEG4135 - Lecture 8

Cloud Security

Definitions

Authentication

- Are you the person you claim to be

Authorization

- Are you able to perform a specific action

Security of Data at Rest

- Security of data when it is sitting in the same space

Security of Data in Motion

- Ensuring data is secure when moving from point A to point B

Integrity

- Ensuring data has not changed in transit

Auditing

- Who has done what action.

CSA Cloud Security Architecture

CSA provides a trusted cloud initiative (TCI) reference architecture

TCi is a methodology and a set of tools that enable cloud application developers and security architects to assess where their internal IT and their cloud providers are in terms of security, capabilities, and to plan a roadmap to meet the security needs of their business.

- Governance, risk management, and compliance
    - Compliance management
    - Policy management
    - Vendor management
- Information security management
    - Capability mapping
    - Risk portfolio
    - Personal risk management
    - Risk Dashboard
        - Risk can be quantified by the damage a threat could do
- Privilege Management Infrastructure
    - Identity management
    - Authorization services
    - Authentication services
- Threat and vulnerability management
    - Compliance testing
    - Vulnerability management
    - Penetration testing
- Infrastructure protection services
    - Server
    - Network
    - Application
- Data protection
    - Data Lifecycle Management
        - Keeping track of the number of users that access the data
        - Levels of security and protection can change
    - Cryptographic services
    - Data loss protection
- Policies and standards
    - Operation security baselines
    - Information Security policies
    - Jobs and Guidelines

Authentication

- Easiest way to do this is via a secret that only one user has.

SSO

- Sign on to the identity management server once.
- Multiple styles
    - SAML-Token
    - Kerberos

OTP - One Time Password

- The user receives a password that can be used one time.

Authorization

OAuth

- A standard for authorization that allows resource owners to share their private resources stored on one site from another
- Sign in with google/facebook

IAM

- Federated Identity management
- RBAC

Encryption Levels for Data at Rest

- Application
- Host
- Network
- Device

Wide Area VM Migration

- Why create a backbone?
    - For energy efficiency
    - We don’t want hotspots in a datacenter

Recall: Manycast

- We have unicast, one to one.
- We have multicast, one to many
- For datacenter migrations, we have to use Anycast or Manycast
- Anycast
    - We want to hit one node in a set of nodes, doesn't matter which one we hit but we have to hit one.
- Manycast
    - We want to hit a subset of nodes that exist in a set of nodes, hit as many as possible

System settings and assumptions

- Transport mediums in the cloud backbone
- IP/WDM network; each node is associated with a data center
    - IP Wavelength division multiplexing
    - Allows more users to take advantage of a fiber line

Demand types

- Upstream
- Downstream
- Regular network traffic
- Energy consumption overhead of heach demand is known in advance

Data centers

- Physical hosts
- VMs
- CPU Capacity per VM
- Memory Capacity per VM

Motivation

We want to be able to predict the demand profile in the Cloud. Is it possible to have a holistic scheme which

- Reconfigures the cloud network
- Maps Vms onto the physical hosts in the data entes and backbone with the objectives of minimum data center and transport energy consumption.

Problem Formulation

- Minimize the total power consumption in each node

$$DC_i + \sum_{j \in N_i^v} P_r \cdot C_{ij} + \sum_{j \in N_i^p} (P_t \cdot W_{ij} + S_{ij} \cdot P_{edfa} \cdot f_{ij})$$

Objectives

- Minimize delay for three types of traffics
- Routing over G' (Physical topology mapping)
    - Assign pre-computed shortest distances as virtual link costs
- Routing over G (Virtual topology mapping)
    - Shortest path, basically

Power-Minimized Provisioning (PoMiP)

- The cost of a virtual link from i to j is
    - We add up the physical link hosts and we divide it by the remaining capacity
- The cost he a physical link
    - The cost of an EDFA times the amount of EDFAs plus the Cost of an amplifier times the number of amplifiers
- Select the datacenter that is the min of the power consumption in terms of cooling and the increase in cooling

Delay and Power-Minimized provisioning (PePoMiP)

- For the virtual link cost
    - Select the virtual link with the lowest sum of its physical links
- For the physical cost
    - (Total power of EDFAs * total power of transponders) * fiber length
- Select half data centers w.r.t. PoMiP Ranking
- Select half data centers w.r.t. The shortest precomputed distances