Cloud security

Security For The Virtualization Product

- Cloud provider is responsible for security of virtualization software.
- The virtual machines come with an OS such as Microsoft Windows, Linux or a Unix variant.
- Customers have no access or control of the virtualization software.
- Zero day vulnerability is a flaw
- The hackers obtain root access to the operating system and delete large portions of the customer data.

Security For The Virtualization Product continue..

- Early problem detection techniques IPS and IDS used to protect against intrusion, virtual LANs with IPsec to protect in-transit messages, and NAC to prevent rogue users or machines from gaining access to underlying infrastructure.

- Since mobile access to the cloud is becoming ubiquitous, cloud providers must use schemes such as WiFi Protected Access to defend against wireless-based attacks on the hypervisor, OS, and applications.

Security For The Virtualization Product continue..

- Wi-Fi Protected Access(WPA) provides a more sophisticated data encryption and user authentication than Wired Equivalent Privacy(WEP).
- WPA uses Temporal Key Integrity Protocol(TKIP) for stronger encryption and includes a per-packet mixing function, a message integrity check, an extended initialization vector, and a re-keying mechanism.

Host security

Host Security

- Physical machine
- Threats:
  - Weak access control to hypervisor
  - VM escape problem are prone to threats
  - VM have many nodes, so any threats is easy to amplify, called velocity of attack

Host Security For SaaS

- For SaaS services, the provider owns and manages the servers, network and applications.
- The provider often refuses to provide details on OS, patches, implemented security measures, hypervisor, etc.
- This is to keep the information away from hackers who might then exploit the data to intrude into hosts.
- SaaS access hides the operating system from the user.

Host Security For Software As A Service(SaaS)

- The following are some ways to get assurance of the degree of security implemented by the SaaS provider:

1. Customers can ask for detailed security status after signing a Non-Disclosure Agreement(NDA) with the provider.
2. Customers can ask if the provider has a security assessment report such as SAS70 or the SysTrust report.
3. Customers can also ask for security certifications such as ISO 27002.

Host Security For Infrastructure As A Service (IaaS)

- In IaaS, users have complete access to the server OS, its resources such as the CPU, memory, network ports, bandwidth and storage, along with root or administrator password.
- To protect from attacks, users must implement strategies to limit the access.

Host Security For IaaS continue..

- The following are some ways to tighten host-level security in an IaaS cloud:

1. Users should create their own OS image to be installed on virtual servers, thus protecting users integrity.
2. Block ports that are not used such as and SMTP. NetBIOS is the single most dangerous port on the internet.

Host Security For Infrastructure As A Service (IaaS) continue..

3. Customise the hosts to run services required by the application on the host.
4. Install host-based IPS and IDS services to monitor and analyse the OS and log files.
5. Enforce strong passwords for users.
6. Enable event logging, set up automated alerts, review log files for security breaches.
7. Protect the encryption keys. After the processing is over, it is best to remove the keys from the cloud.
8. Users are required to type passwords for sudo access to gain root-level rights for Unix hosts.

Host Security For Platform As A Service(PaaS)

- PaaS provides an environment to develop products, customers have an access to libraries and kernel-level parameters but do not have root or administration-level privileges.
- The cloud provider gives a number of APIs, which are used by the PaaS users to indirectly access the abstraction layer, that hides the OS.
- The host administration in PaaS is the responsibility of the cloud provider.

Data security

Data security in cloud

- Data stored in cloud faces following issues
  - Data availability
  - Data performance
  - Price
  - Flexibility
  - Underlying complexity
  - Data security
  - Data integrity

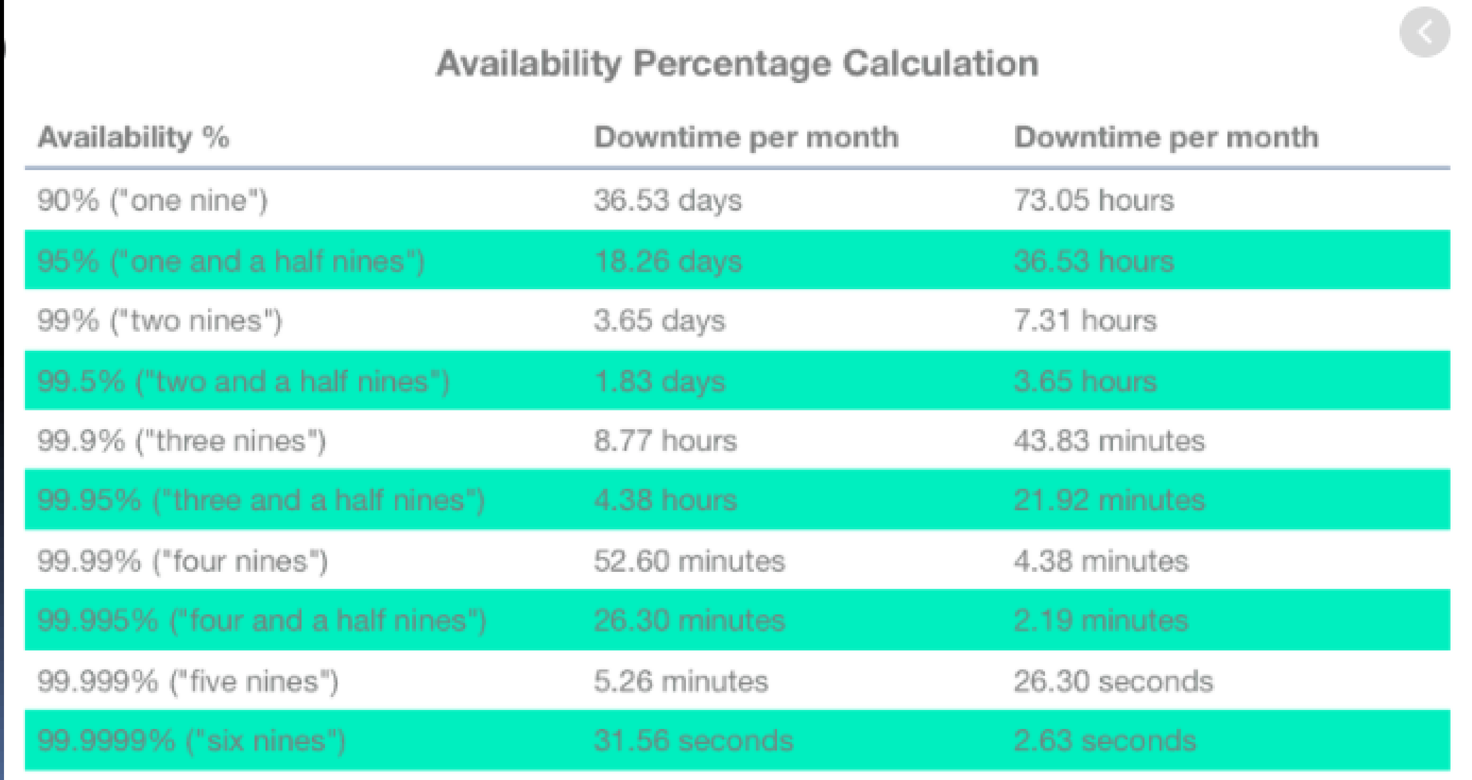
Challenges to data security in clouds

DATA SECURITY CHALLENGES

- Security Risk: due to multitenancy
  - Snooping: access to each tenant should be limited to his/her own data
  - Unauthorized Discovery: Data should be visible only to owner
  - Spoofing: no tenant can assume the identity of another tenant
  - Accidental/ Malicious deletion
  - Denial of service Attack
- Quality of Service: performance, long response time
- Availability
- Confidentiality & encryption
- Integrity
- Cloud data management

Data Availability

- Data availability makes sure that user can access data when they want to.
- Unexpected downtime



Availability Percentage Calculation

Availability %	Downtime per month	Downtime per month
90% ("one nine")	36.53 days	73.05 hours
95% ("one and a half nines")	18.26 days	36.53 hours
99% ("two nines")	3.65 days	7.31 hours
99.5% ("two and a half nines")	1.83 days	3.65 hours
99.9% ("three nines")	8.77 hours	43.83 minutes
99.95% ("three and a half nines")	4.38 hours	21.92 minutes
99.99% ("four nines")	52.60 minutes	4.38 minutes
99.995% ("four and a half nines")	26.30 minutes	2.19 minutes
99.999% ("five nines")	5.26 minutes	26.30 seconds
99.9999% ("six nines")	31.56 seconds	2.63 seconds

Data Availability

- Cloud services are not visible to users, so hard to track problems
- No control by cloud consumer
- Virtualized pool makes it difficult to track location of resources and enforce security policies
- Multitenancy, security breach created by one customer impacts the other customer.

DATA CONFIDENTIALITY AND ENCRYPTION

- Data confidentiality makes sure that the data in the cloud cannot be read by the unauthorized user.
- Protect data from unintended users.
- Cloud data is encrypted using an algorithm and key.
- There are two ways to encrypt data:

1. Symmetric Encryption
2. Asymmetric Encryption
   - Sender uses public key of receiver
   - Receiver uses own private key

Key Protection

- The problem with exchanging shared key, especially in a large multi tenant cloud is that others in the cloud can gain access to the key and thus can decrypt unauthorized documents.
- Also relying on the cloud provider for key management is hazardous.
- Solutions:

1. So encrypt the key itself!! How???
2. Change the key at regular intervals.
3. Cloud users should manage their own Encryption keys.

User should keep at least two set of encryption keys in case lost or deleted.

Algorithms used for Cloud Data Encryption

- **RSA Algorithm:**

  The algorithm selects Two large prime numbers and uses their product to form the required keys to encrypt the data.

- **3DES Algorithm**:

  3DES encrypts the data thrice using a different unique key at least in one of the three passes.

- **International Data Encryption Algorithm:**

  It uses same secret key of 128 bits for encryption/decryption. It is fast and operates on 64 bits block at a time.

Algorithms used for Cloud Data Encryption

- **Blowfish Algorithm:**

  It is another symmetric block-cipher(like DES and IDEA)

  It is designed to use keys of length from 32-448 bits. It is a strong and fast algorithm.

- **RC4 Algorithm:**

  It can use keys upto 2048 bits. It works by creating a stream of random bytes and XORing those bytes with the text. It is useful when you need a new key for each message.

- **Software-Optimized Encryption Algorithm(SEAL):**

  It is a stream cipher algorithm in which data is continuously encrypted. It uses 160 bit key for encryption.

Data Integrity

- Encrypted data in the cloud should not be modified or tampered by unauthorized party. If it gets intercepted, data lacks integrity.
- Man-in-the-middle attack can replace the bits in transit within the cloud. The receiver decrypts the message but without data origin authentication, the receiver does not become aware that the data received is different.
- So what to do???

Proactive Measures Taken to Ensure Data Integrity.

- Cloud provider must control the access to data using RBAC mechanism.
- Cloud provider must design and implement user interfaces that prevent input of invalid data.
- Cloud provider must use error detection and correction software when transmitting data within or outside the cloud.
- Cloud provider must make sure that data storage is protected using Data Integrity Field (DIF). It is important that users have cloud data on disks and arrays that implement DIF. This ensures that right data is not available at wrong location.

CLOUD DATA MANAGEMENT
CLOUD STORAGE GATEWAY (CSG)

- CSG is an appliance residing in customers premises and provide data protection before moving the data to a cloud.
- CSG could be:
- Hardware appliance

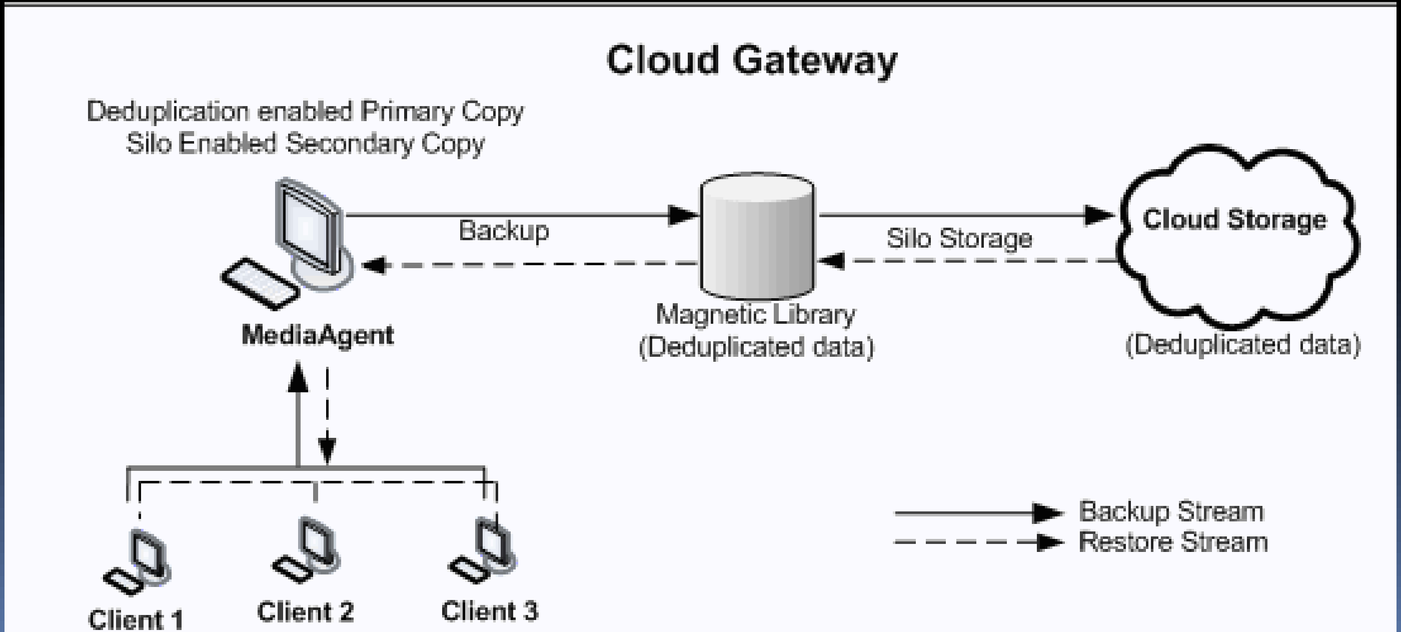
  Cache is installed within corporate office or data center.
- Downloadable software program:

  Download CSG software and configure cache.

  CSG supports various formats and facilitated data backup eliminating the issue of vendor lock-in.

CSG continue…

- Customer contacts CSG vendor to get credentials for each cloud provider a user makes use of and for call-home features.
- Call-home features allows CSG to automatically report issues, status, problems and diagnostic reports to CSG vendor.



CSG CONTINUE…

- CSG provides data protection in four steps:

1. The CSG cache accelerates I/O rates and enables a convenient replication procedure.
2. Files that are to be copied to the cloud are first stored in CSG cache.
3. After certain pre-set time interval the cache data is pushed in the cloud.
4. Data that is read from the cloud is copied to cache.

Features of CSG

- **Caching Algorithm**

  Cache provides a buffer of vital data to speed access and reads instead of reaching original servers. CSG must use certain algorithms such as LRU algorithm to enhance cache hit rate.

- **Intelligent Pre-fetching Algorithm**

  CSG must monitor read patterns and intelligently pre-fetch data from cloud to cache before the user requests the data. CSG must mesure its success rate and regulate its algorithm in real time to improve cache hit rate.

- **Caching time periods**

  CSG allows user to set up a caching time duration which would remove old cache data in preference to newly cached data.

- **Synchronous Snapshots**

  CSG must take synchronous snapshots of user file tree and data. It allows CSG to identify new and modified data.

Features of CSG

- **Data replication process**

  CSG must have efficient data transfer mechanism. Data should be de-duplicated, compressed and encrypted before sending to cloud.

- **End-to-end Encryption**

  This protects data from being read by unauthorized users and hackers.

- **Secure Channel**

  Ideally the data in transit between CSG and the cloud is encrypted twice. Once before it is transmitted and other when it sent over a Virtual Private Network(VPN) tunnel to the cloud.

- **Data Compression**

  It helps to reduce bandwidth and storage space utilization.

- **CSG Tuning Parameters**

  CSG must allow its administrator to tune certain parameters during certain time period and cache push intervals.

  CSG can be tuned to create new instances of virtual machine and data copies to meet peak loads in real time.

Advantages of CSG

- Facilitate the use of unlimited storage space in the cloud.
- No longer need to plan or purchase storage for expansion(eg:hard disk)
- Pay-per –use cloud billing.
- Backup of data is easier with faster access, enhanced security and snapshot based protection.

Cloud Firewall

- It is a network firewall appliance, explicitly built to work with other cloud-based security solutions.
- It serves the same purpose as traditional firewalls but is different under following three aspects:

1. Scalability
2. Availability
3. Extensibility

https://www.cloudflare.com/en-in/learning/cloud/what-is-a-cloud-firewall/

Virtual Firewall(VF)

- A VF is a network firewall service running entirely within a virtual environment.
- It provides the usual packet filtering and monitoring.
- It provides an easy way to decrease investment expenses by consolidating multiple logical firewalls onto a single platform.
- https://searchcloudsecurity.techtarget.com/definition/virtual-firewall

VF CONTINUE…

- Depending on the point of deployment, VF can operate in two different modes:

1. **Bridge mode:**

   The firewall acts like a physical firewall that works with a physical or virtual switch to intercept network traffic destined for other network segments.

2. **Hypervisor mode:**

   The firewall service resides in the virtualization hypervisor where it can capture, monitor and filter all the activities of all the virtual machines and logical resources.

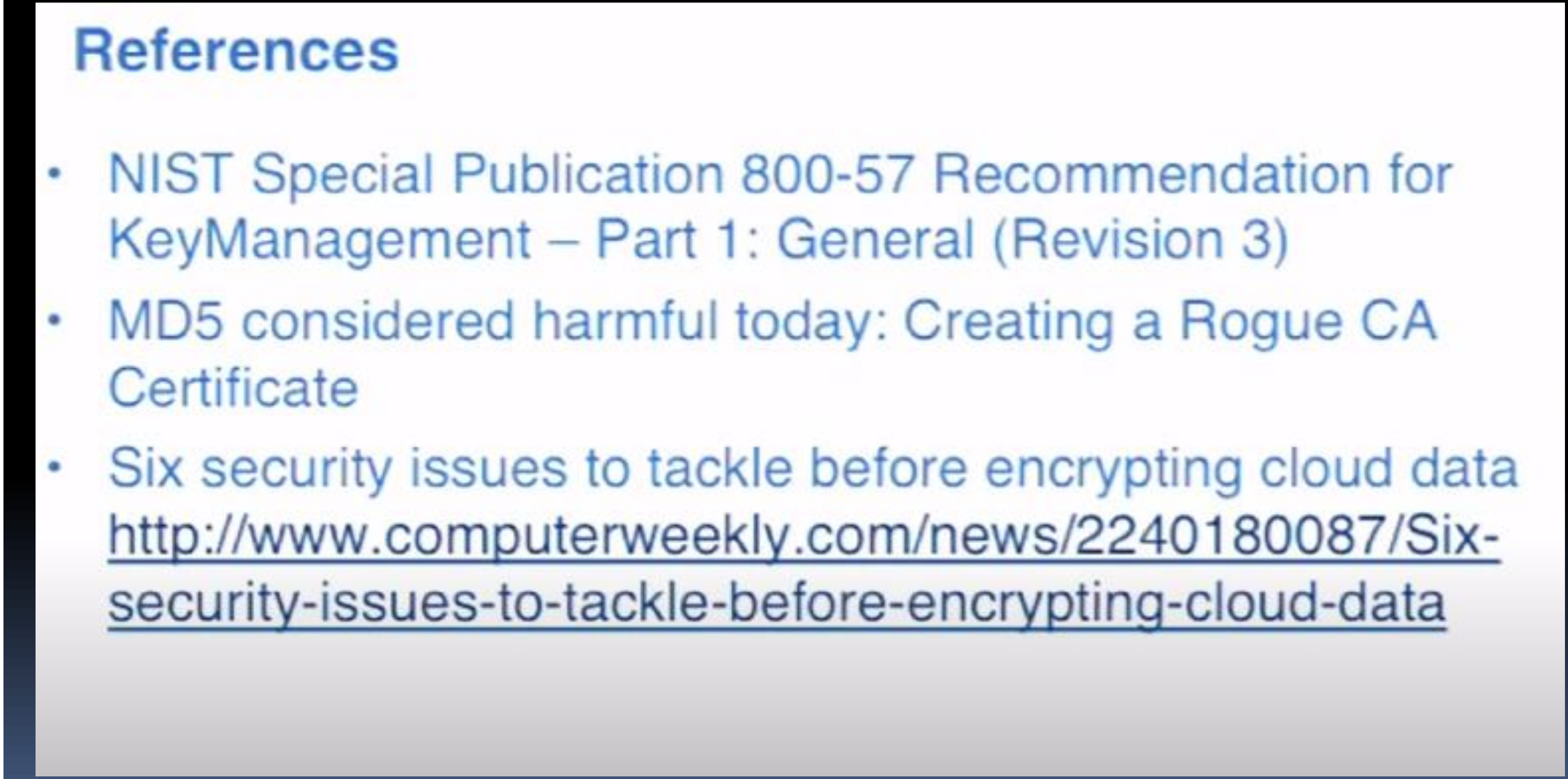
References

1. Cloud computing Black Book, Kailash Jayaswal

2. Data Security Essentials https://www.youtube.com/watch?v=9WckTTqpD_M

3. How to Implement Top 10 AWS Security Best Practices in 2021? https://www.youtube.com/watch?v=QCMQYlopxoU

References



References

- NIST Special Publication 800-57 Recommendation for KeyManagement – Part 1: General (Revision 3)
- MD5 considered harmful today: Creating a Rogue CA Certificate
- Six security issues to tackle before encrypting cloud data http://www.computerweekly.com/news/2240180087/Six-security-issues-to-tackle-before-encrypting-cloud-data