Cisco Networking Academy
Mind Wide Open

Security in the Cloud

Lokesh Pidawekar
Application Security Engineer

December 10, 2015

Webinar Series

- What is Cloud? How will it affect me and my network? Tony Rice (Nov 24th)
- **Security in the Cloud – (Dec 10th) Lokesh Pidawekar**
- Open Stack—what is it? Connecting ACI to Open Stack - (Jan 19th)

… whoami?

- Application Security Engineer
  Cisco Critical Business Security Services
- Master of Science in Information Assurance from Northeastern University, Boston (MA)
- CISSP, CCNA, MCITP (Virtualization Administrator)

Why learn this?

http://www.wordstream.com/images/attention-economy-zoidberg-why.png

Cloud is becoming ubiquitous

Cloud Computing

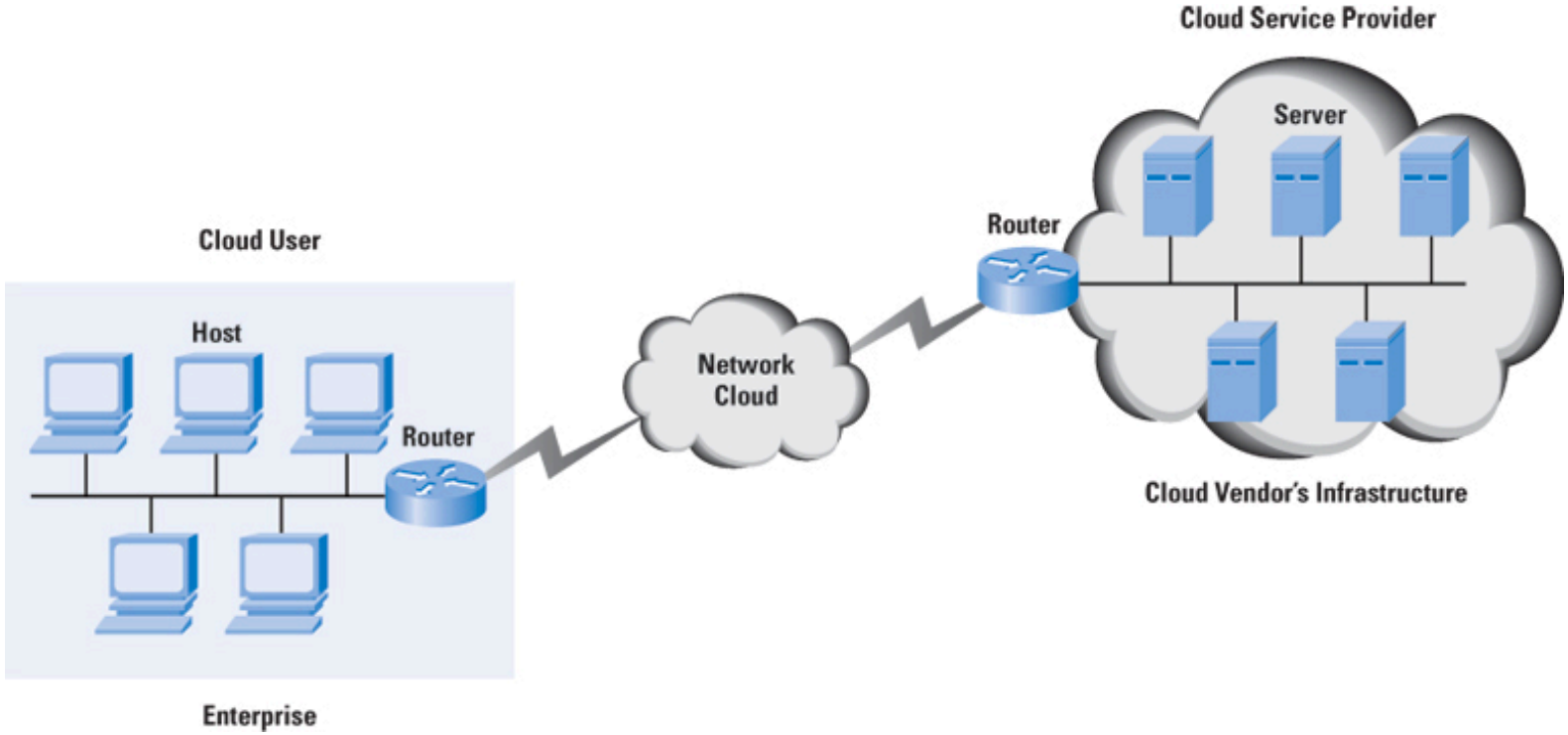
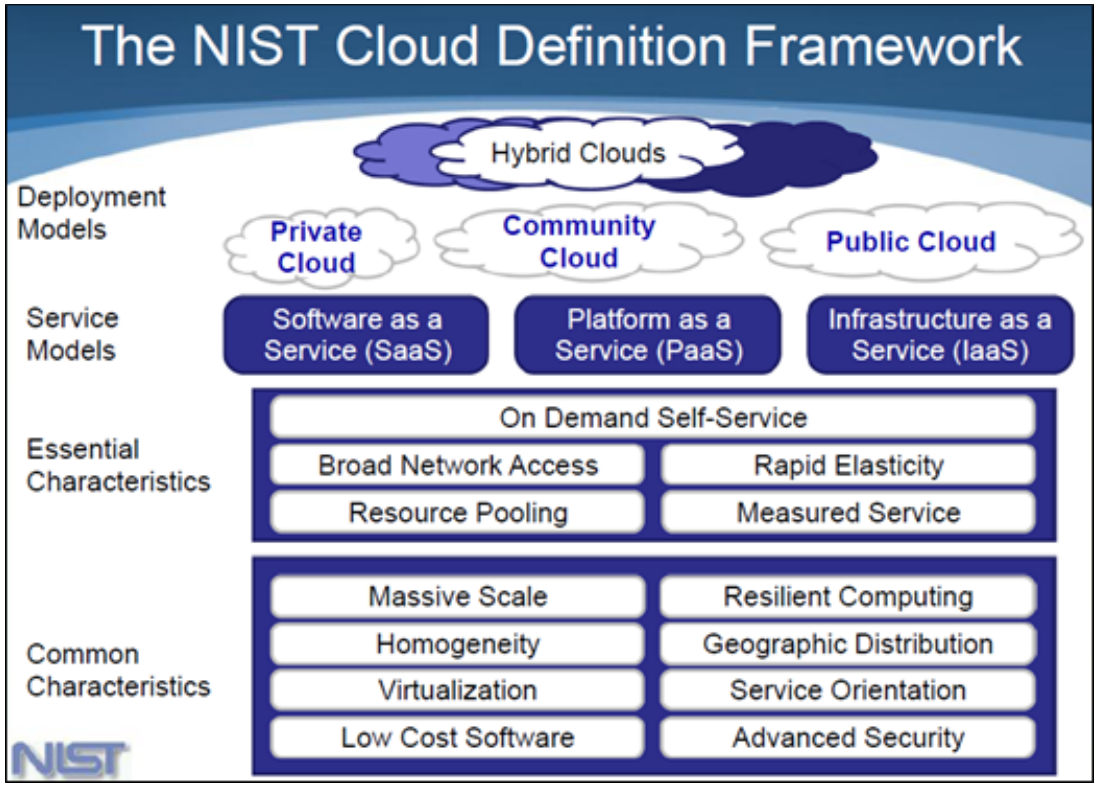


Image Credit: T. Sridhar

Reasons for popularity of cloud

- Pay per use
- Rapid provisioning
- Increases efficiency
- Less maintenance
- Scalability

Service and Deployment Models



Types of cloud services

- Software as a Service - LinkedIn, Facebook, Dropbox, Citrix, Evernote
- Platform as a Service – Azure, Google App Engine, Heroku
- Infrastructure as a Service - Amazon, Rackspace, Cisco

Cloud providers news

iCloud – Stores backup of photo library, app data and documents

Considered to be breached in mid 2014 and private pictures of celebrities were posted online on Aug 31, 2014

News continues

Snapchat – Messaging app to share photos and videos

An anonymous group exploited vulnerability to expose 4.6 million usernames and phone numbers

Reference - http://techcrunch.com/2013/12/31/hackers-claim-to-publish-list-of-4-6m-snapchat-usernames-and-numbers/

Why Security is important

- There is no perimeter around the cloud
- We do not know where will the data be physically hosted
- We do not know if the cloud service provider takes security seriously
- Shared tenancy and dynamic in nature

Safeguarding the cloud

- Identity and Access Management
- Data Security
- Vulnerability Management
- Monitoring
- Logging
- Incident Response

Identity and Access Management

- Administrator accounts
  - Shared admin credentials
  - Login from untrusted devices
  - Multi Factor authentication
  - No session time out
- User authentication and account management
  - Multi Factor authentication
  - Single Sign on
- Granular Permission Model
  - Segregation of duties

Data Security

- Security of Data in transit
  - SSL/TLS encryption
- Security of Data at rest
  - Full Disk Encryption
  - Database level encryption
  - Secure storage of cryptographic keys
- Data backup
  - Secure data backup at offsite
- Data Destruction
  - Traditional methods like purging, destroying might not be sufficient
  - Encryption

Vulnerability Management

- Regular network and application vulnerability scanning
- Rapid patching
- Hardening critical components
- Periodic third party penetration testing

Monitoring

- For abuse of admin accounts
- For unauthorized operation
- Should be automated and alert
- Anomaly detection

Logging

- Enabled for critical service and components
- Should not be limited to login/logout but for all activities performed
- Logs should be collected on centralized location
- Periodic review of audit logs
- Log Management

E.g. CloudTrail by Amazon

Incident Response

- Conventional Forensics methods may not be useful due to lack of physical access to device
- Data collection will depend on Cloud Service Provider
- Multi-tenancy and huge infrastructure
- Scaling and transient nature of cloud

API security

API related security vulnerability was responsible for Snapchat breach that impacted 4.6 million users – It was easy to retrieve user information as some static token were used

- API should be authenticated and authorized
- API keys should be treated as credentials and should not be exposed publicly
- Access should be restricted

Reference - http://gibsonsec.org/snapchat/fulldisclosure/

Compliance challenges

- Sarbanes-Oxley Act of 2002 (SoX)
- PCI-DSS
- HIPAA

Conclusion

- Security is shared responsibility of Cloud provider and consumer
- Traditional methods need to be tailored for cloud
- Security controls should not be overlooked
- The cloud is someone else's computer

Questions?

- Cloud Computing *National Institute of Standards and Technology:*
  http://www.nist.gov/itl/cloud/
- Security of Cloud Computing: Seeing Through the Fog
  http://www.satnac.org.za/proceedings/2011/papers/Internet_Services_and_Applications/178.pdf
- CSA Security Guidance Version 3
  https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/

MaverickRocky02

lpidawek@cisco.com