PennState

CSE543 Computer Security

Module: Cloud Security

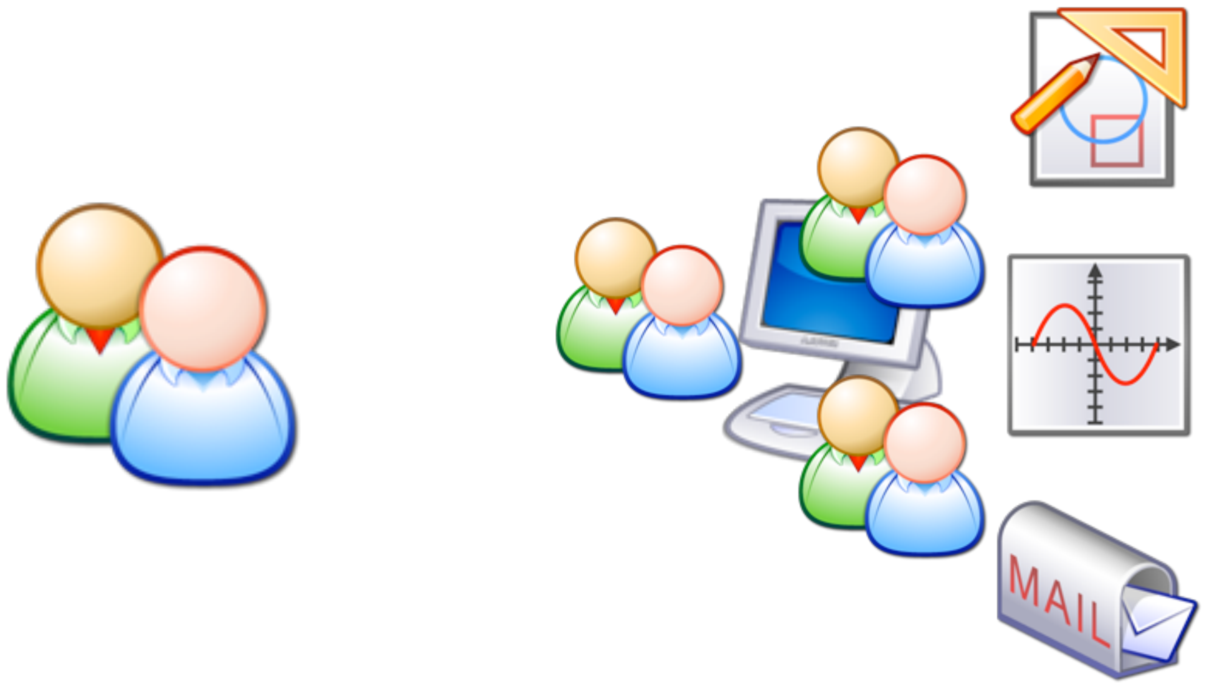
Asst. Prof. Syed Rafiul Hussain
Department of Computer Science and Engineering

Cloud Computing Is Here

rackspace® HOSTING

vmware®

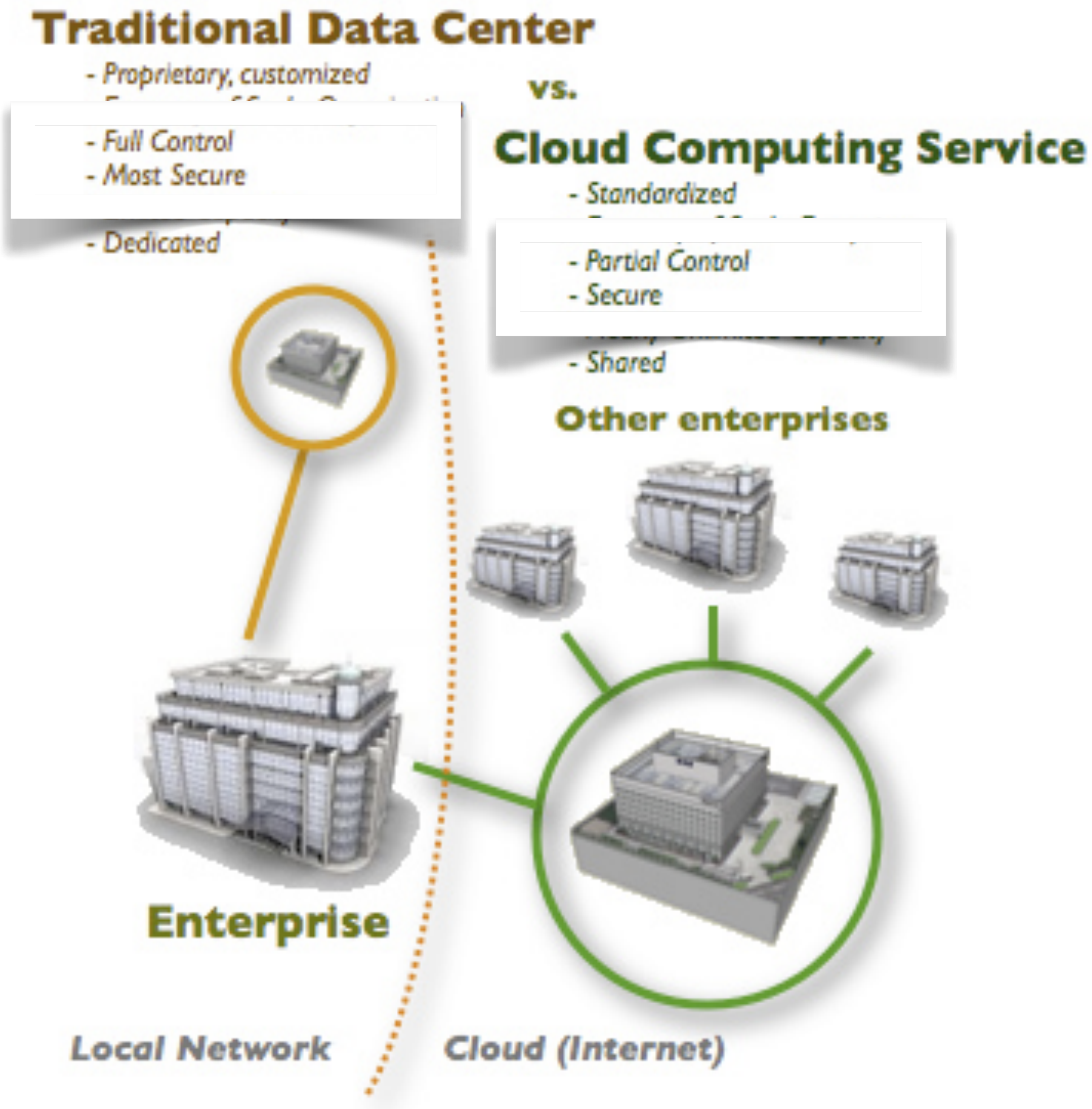
amazon web services™



Why not use it?

What’s Happening in There?

From Data Center to Cloud



Traditional Data Center

- Proprietary, customized
- Full Control
- Most Secure
- Dedicated

vs.

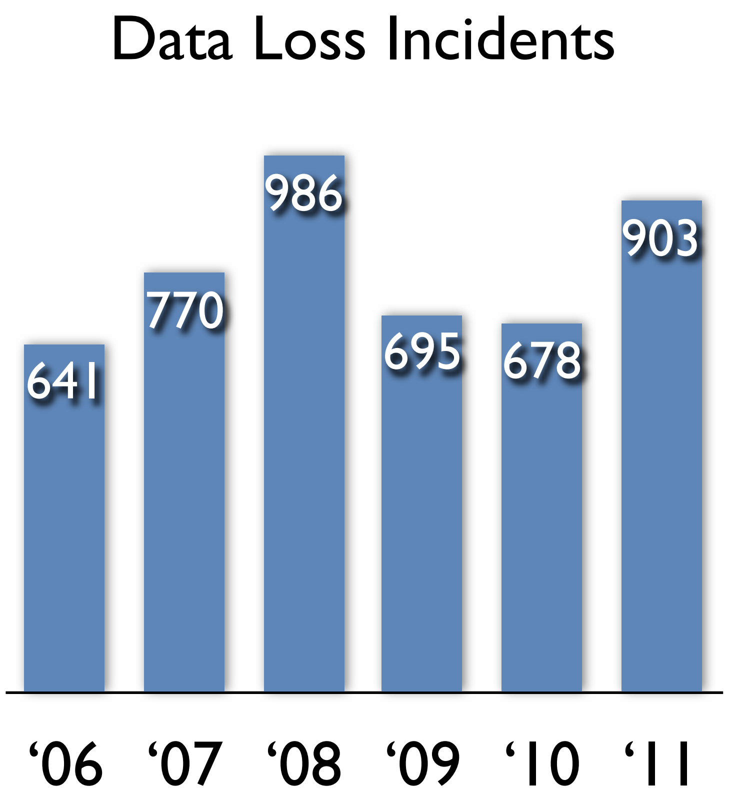
Cloud Computing Service

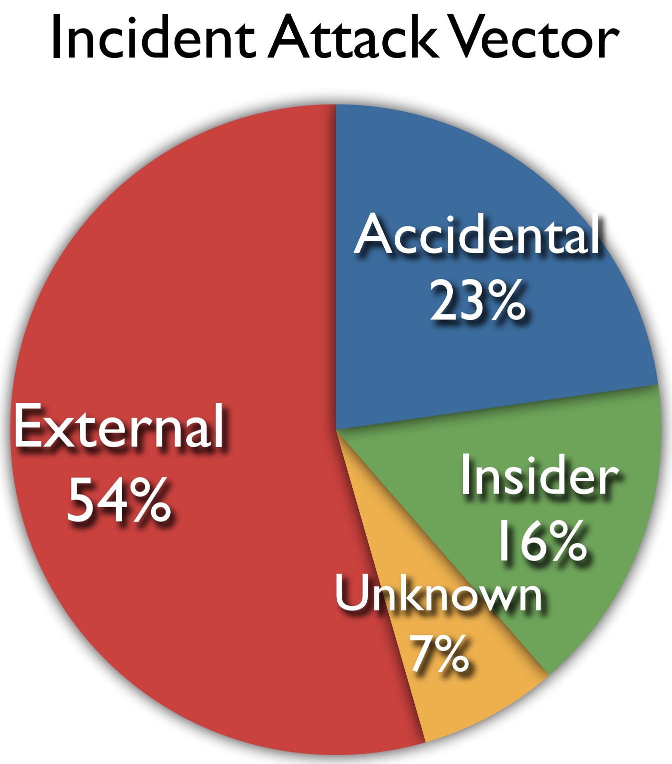
- Standardized
- Partial Control
- Secure
- Shared

From http://blogs.zdnet.com/Hinchcliffe

Reasons to Doubt

- History has shown they are vulnerable to attack
  - SLAs, audits, and armed guards offer few guarantees
  - Insiders can subvert even hardened systems





Credit: The Open Security Foundation datalossdb.org

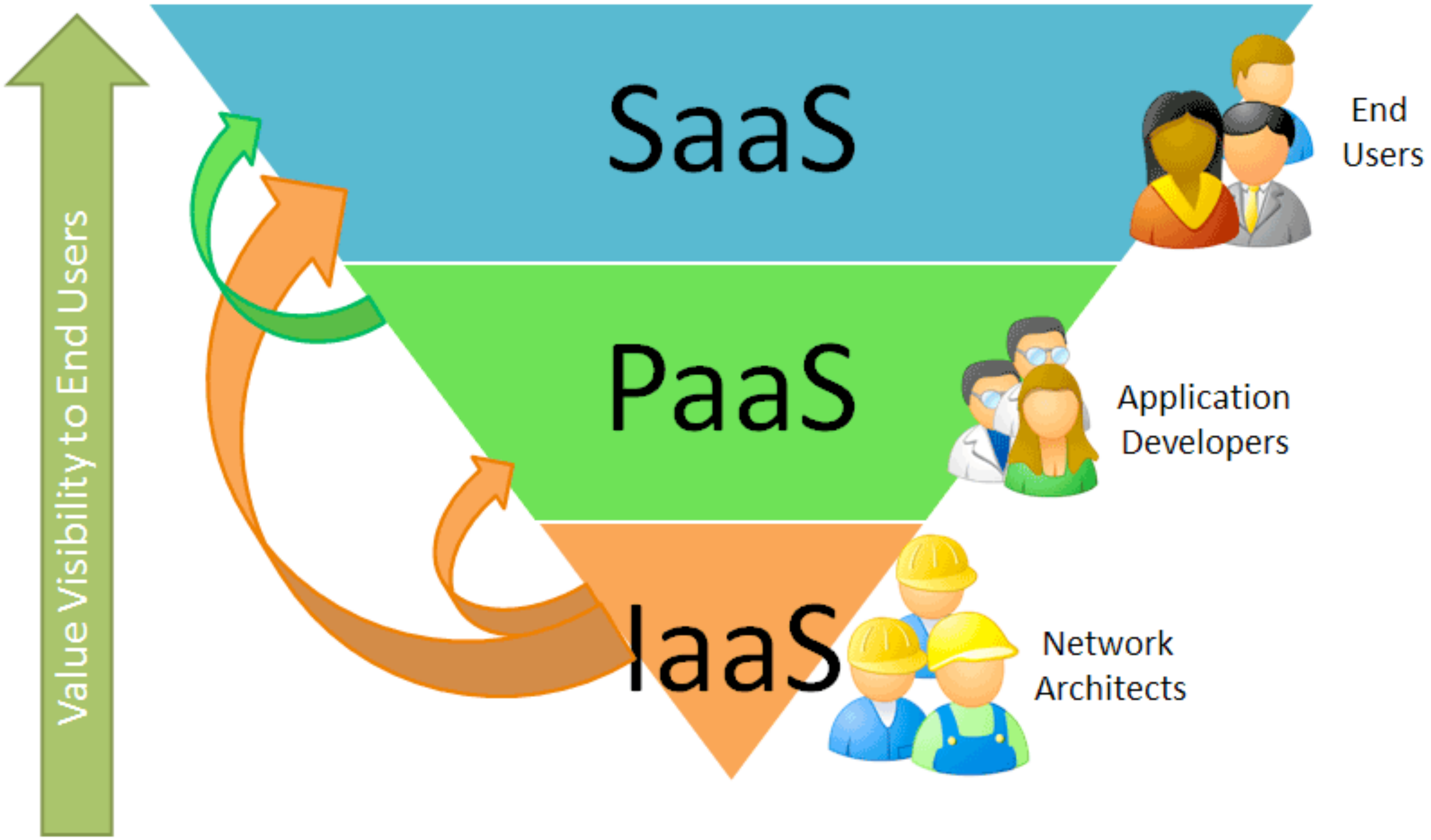
Cloudy Future

- New problem or new solution?
  - New challenges brought on by the cloud (plus old ones)
  - Utility could provide a foundation for solving such challenges

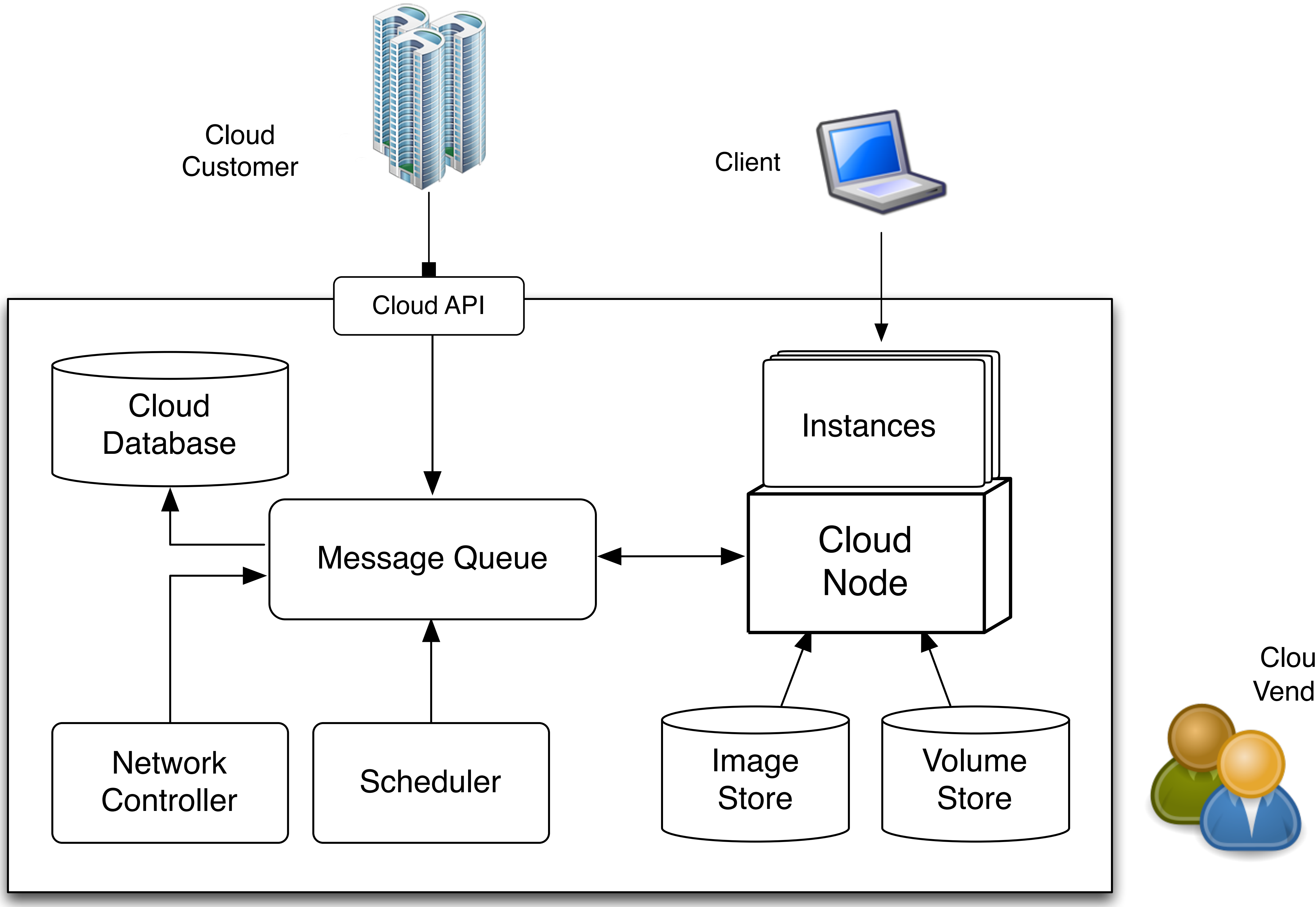
What is Cloud Computing?

- Cloud vendor provides managed computing resources for rent by customers
- What do you want to rent?
  - (Virtualized) Hosts (Infrastructure as a Service)
    - Rent cycles: *Amazon EC2, Rackspace Cloud Servers, OpenStack*
  - Environment (Platform as a Service)
    - Rent instances: *Microsoft Azure, Google App Engine*
  - Programs (Software as a Service)
    - Rent services: *Salesforce, Google Docs*
- Other variations can be rented

What is Cloud Computing?



IaaS Platform: OpenStack



How to Build an IaaS Cloud?

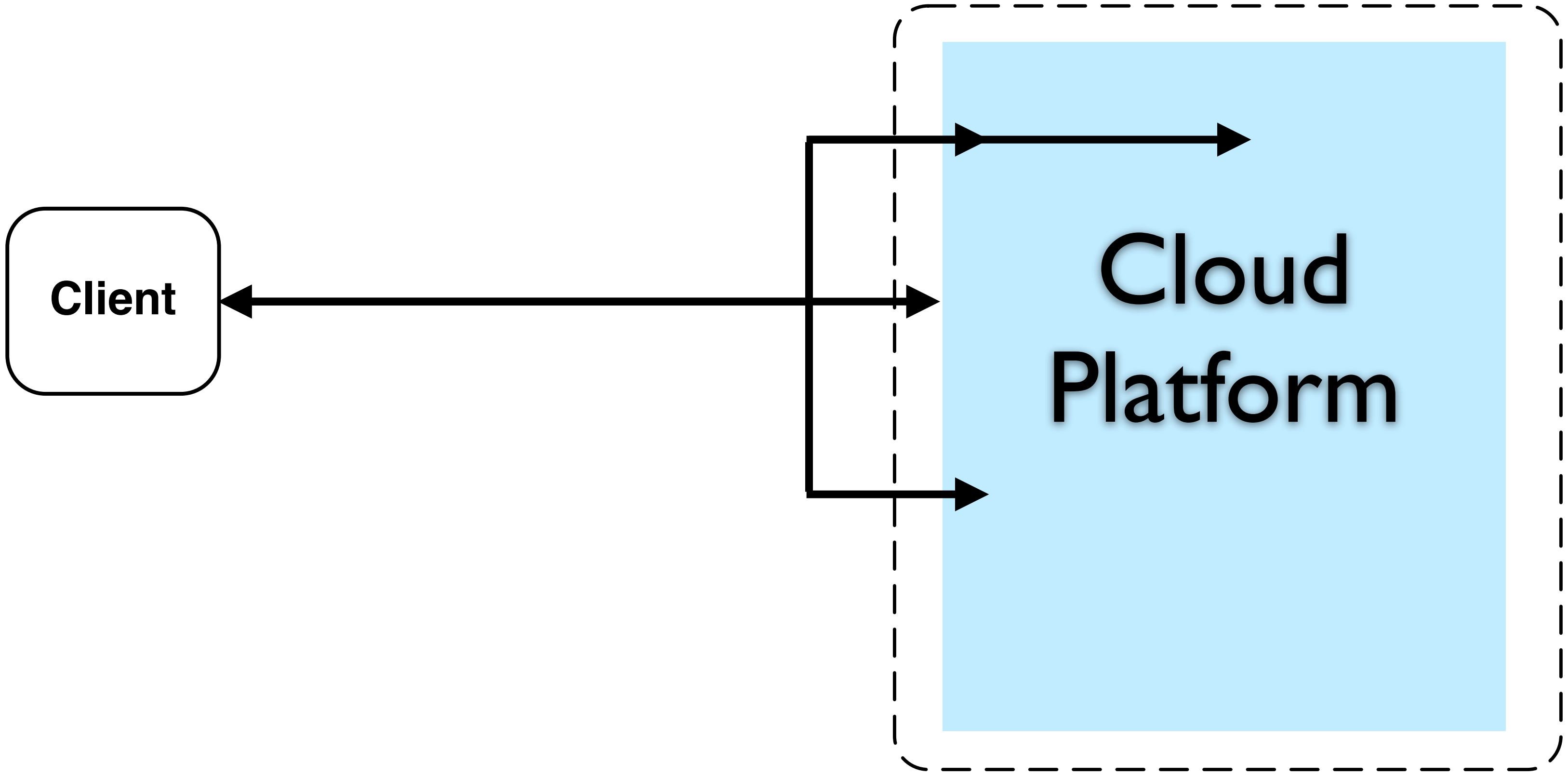
- Vendors obtain hardware resources for
  - Various cloud services: API, Messages, Storage, Network, ...
  - Compute nodes for running customer workloads
- Install your hardware
  - Need to choose software configurations specific for services and compute nodes
- Start your hosts
  - Join the cloud - services and available compute nodes
- Now your cloud is running
  - Have fun! Customers are ready to use your services and nodes

How to Use an IaaS Cloud?

- Customers choose an OS distribution
  - These are published by the cloud vendor and others
  - Obtain cloud storage necessary to store these and your data
- Configure your instance (VM)
  - Prior to starting - enable you to login and others to access the instance's services
- Start your instance
  - Boots the chosen OS distribution with the configurations
- Now your instance is running
  - Have fun! Login via SSH or ready for your clients

Cloud Complexity

- Cloud environment challenges
  - Opaque, Complex, Dynamic
  - Insiders, Instances, Co-hosting

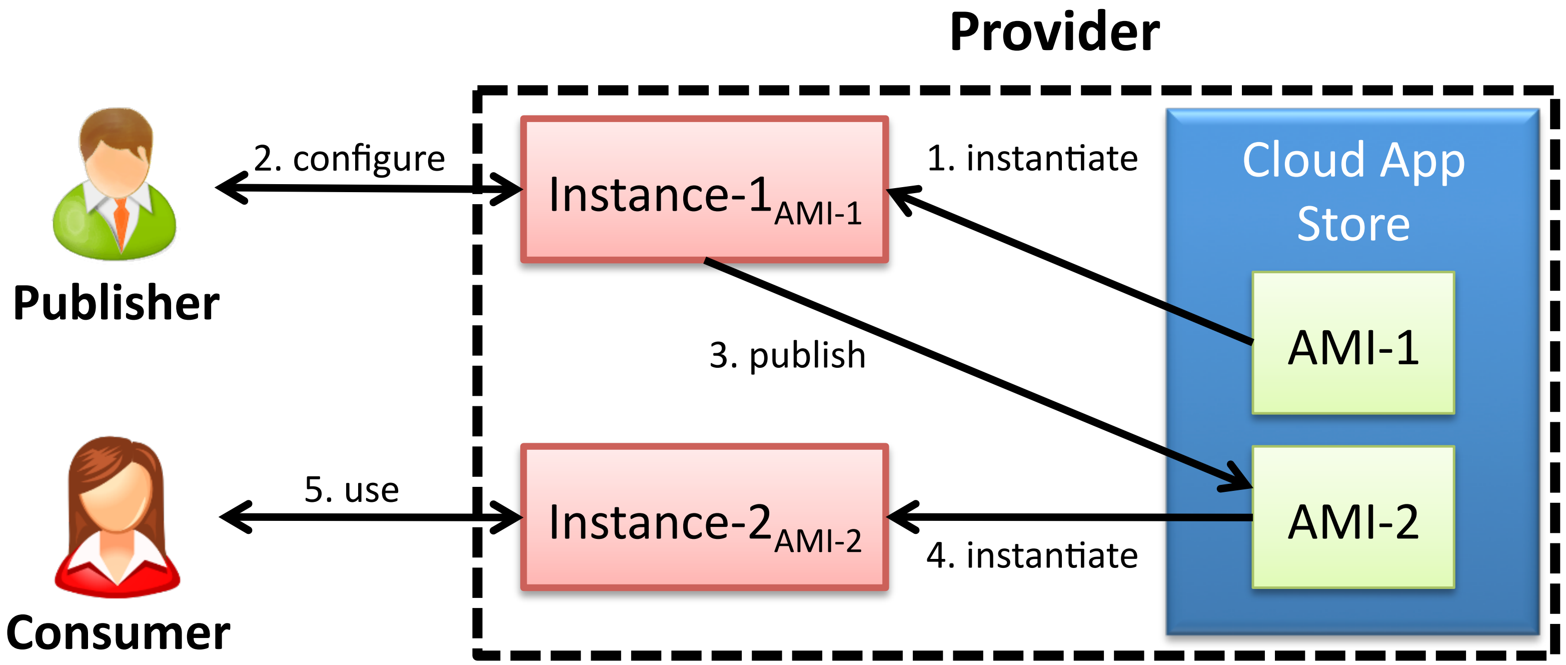


What Could Go Wrong?

- What do customers depend on from the cloud?
  - Trust Model
  - Are those parties worthy of our trust?
- Who are potential adversaries in the cloud?
  - Threat Model
  - Are customers protected from their threats?
- What would be ideal from a security standpoint?
  - Ideal Security Model
  - How many trusted parties and how many threats?

Published Instances

Consumers use published instances



Who do you trust? What are threats?

SSH Study *[AmazonIA]*

- Publisher left an SSH user authentication key in their AMI
- Fortunately, Amazon agreed that this is a violation
  - Unfortunately, it was not an isolated problem
    - 30% of 1100 AMIs checked contained such a key
  - Also, pre-configured AMIs had SSH host keys
    - Thus, all instances use the *same host key pair*
    - Implications?

Security Configuration

- Zillions of security-relevant configurations for instances
  - Do you have the right code and data installed?
  - Are you running the expected code?
  - Discretionary access control
  - Firewalls
  - Mandatory access control
    - SELinux, AppArmor, TrustedBSD, Trusted Solaris, MIC
  - Application policies (e.g., Database, Apache)
  - Pluggable Authentication Modules (PAM)
  - Application configuration files
- Plus new configuration tasks for the cloud - e.g., storage

Insiders

- Although the vendor may have a good reputation, not every employee may

Insider Threats

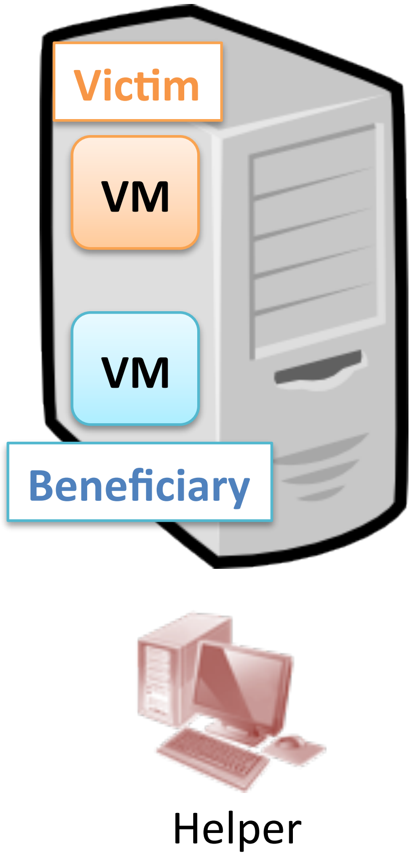
- May trust the cloud vendor company
  - But, do you trust all its employees?
- Insiders can control platform
  - Determine what software runs consumers' code
- Insiders can monitor execution
  - Log instance operation from remote
- Insiders may have physical access
  - Can monitor hardware, access physical memory, and tamper secure co-processors

Co-Hosting Threats

- An instance co-hosted on the same physical platform could launch attacks against your instance
- Co-hosted instances share resources
  - Computer
    - CPU, Cache, Memory, Network, etc.
- Shared resources may be used as *side channels* to learn information about resource or impact its behavior

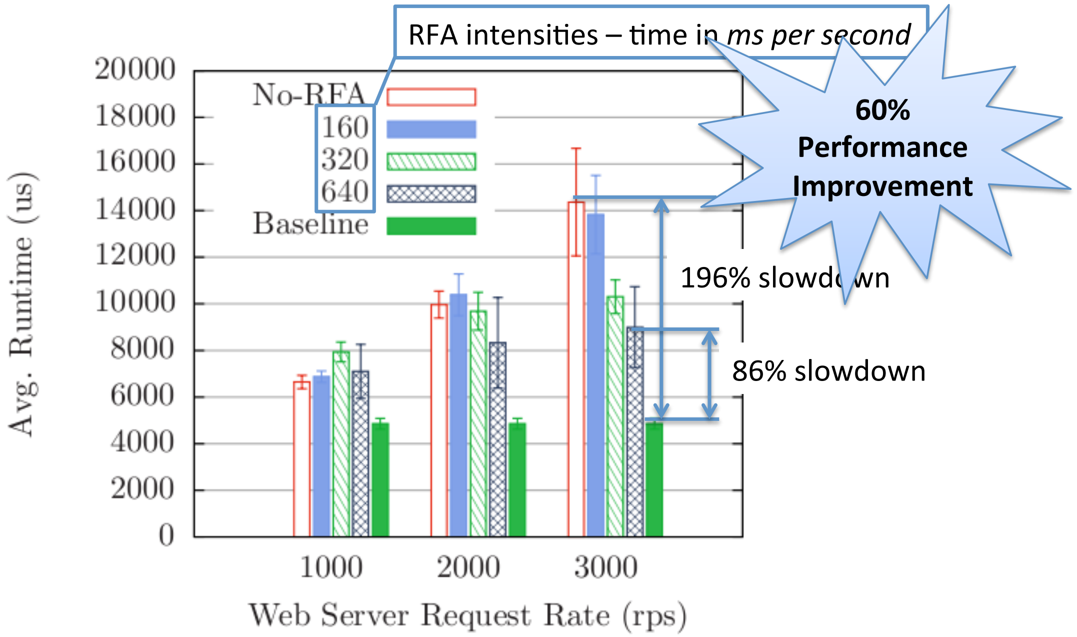
Resource Freeing Attacks

- Setup
- Victims
  - One or more VMs with public interface
- Beneficiary
  - VM whose performance we want to improve (*contend over target resource*)
- Helper
  - Mounts attack using public interface



Resource Freeing Attacks

- Resource contention over the CPU
  - Schedule beneficiary more frequently
- Attack: shift resource usage via public interface
  - Helper can choose requests to send to victim
  - Approach lower scheduling priority
    - Make victim appear *CPU-bound*

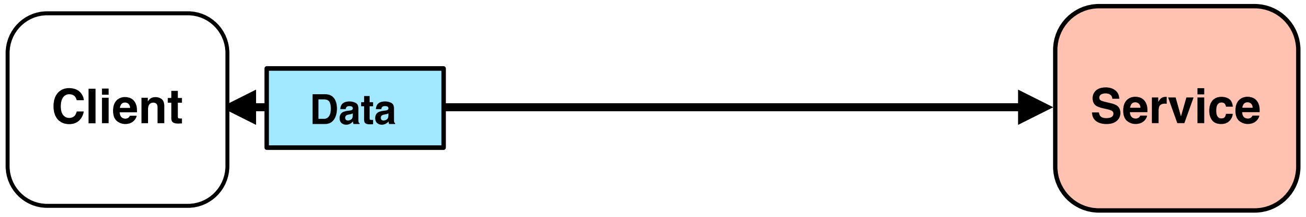


Preventing Vulnerabilities

- How would you prevent these threats?
  - Misconfigured instances
  - Compromised cloud services
  - Insiders
  - Side channels

Verifiable Computation

- Your services are black boxes - to the cloud!
  - Send a program and encrypted data
  - Program computes over encrypted data
  - Scheme: KeyGen (for Program), Compute (Program), Verify



Depends on heavy crypto - homomorphic encryption

Take Away

- Cloud computing is here to stay
  - In some form
- May be a solution or a problem or both
  - Introduces new types of vulnerabilities into systems we ran on data centers - which had vulnerabilities to begin with
- Ultimately, have to improve service providers' jobs
  - Make it easy to ensure that systems perform as expected
- Two possible methods
  - Verifiable computation and instance monitoring