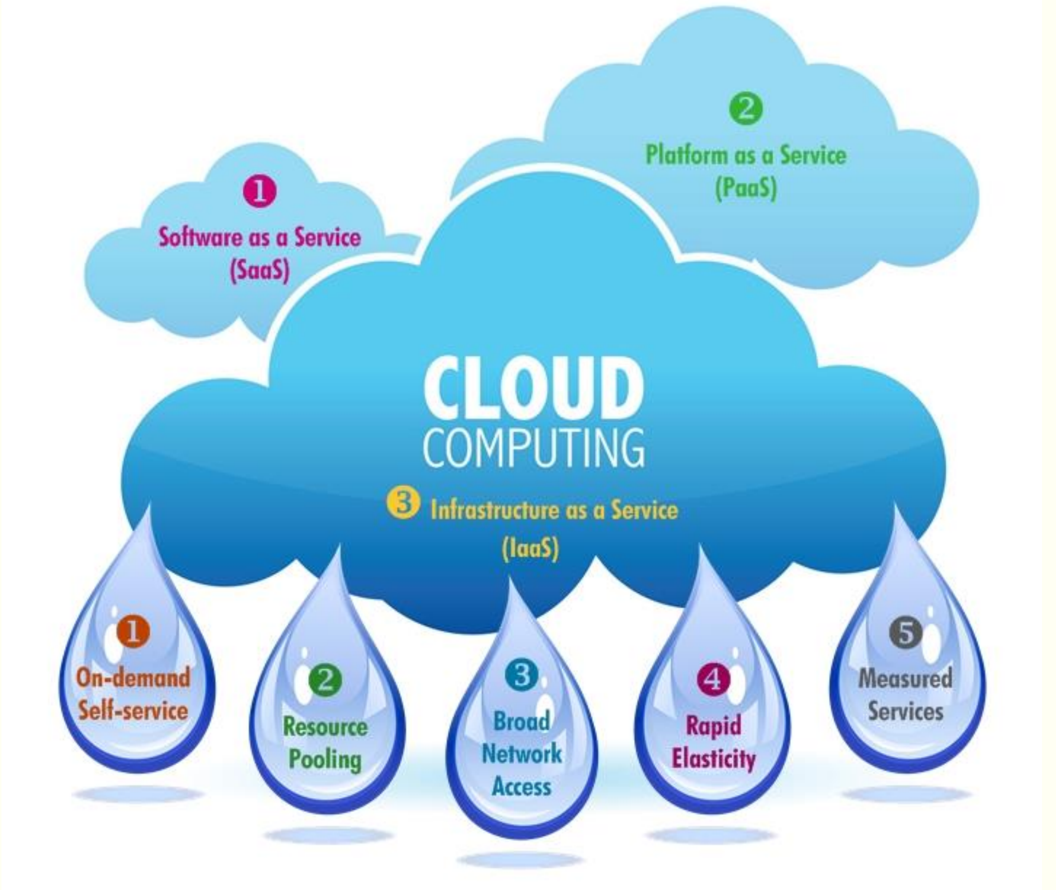
CLOUD COMPUTING

This session Cloud Security Issues & Solution



Today's Topics

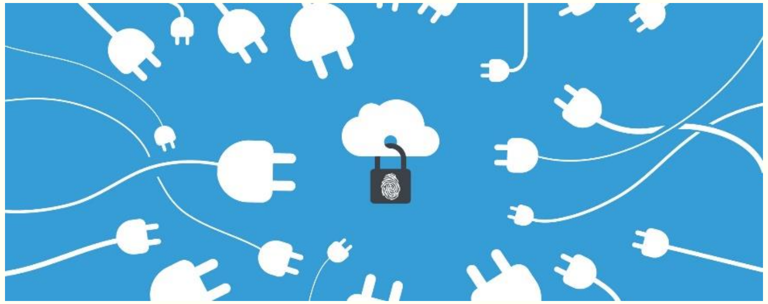
- Cloud Security Issues

SECURITY

Cloud Security Issues : Introduction

Introduction

- Cloud Ecosystem : A massive scale of Virtual Resources
- Also a massive concentration of risk
  - expected loss from a single breach can be significantly larger
  - concentration of “users” represents a concentration of threats



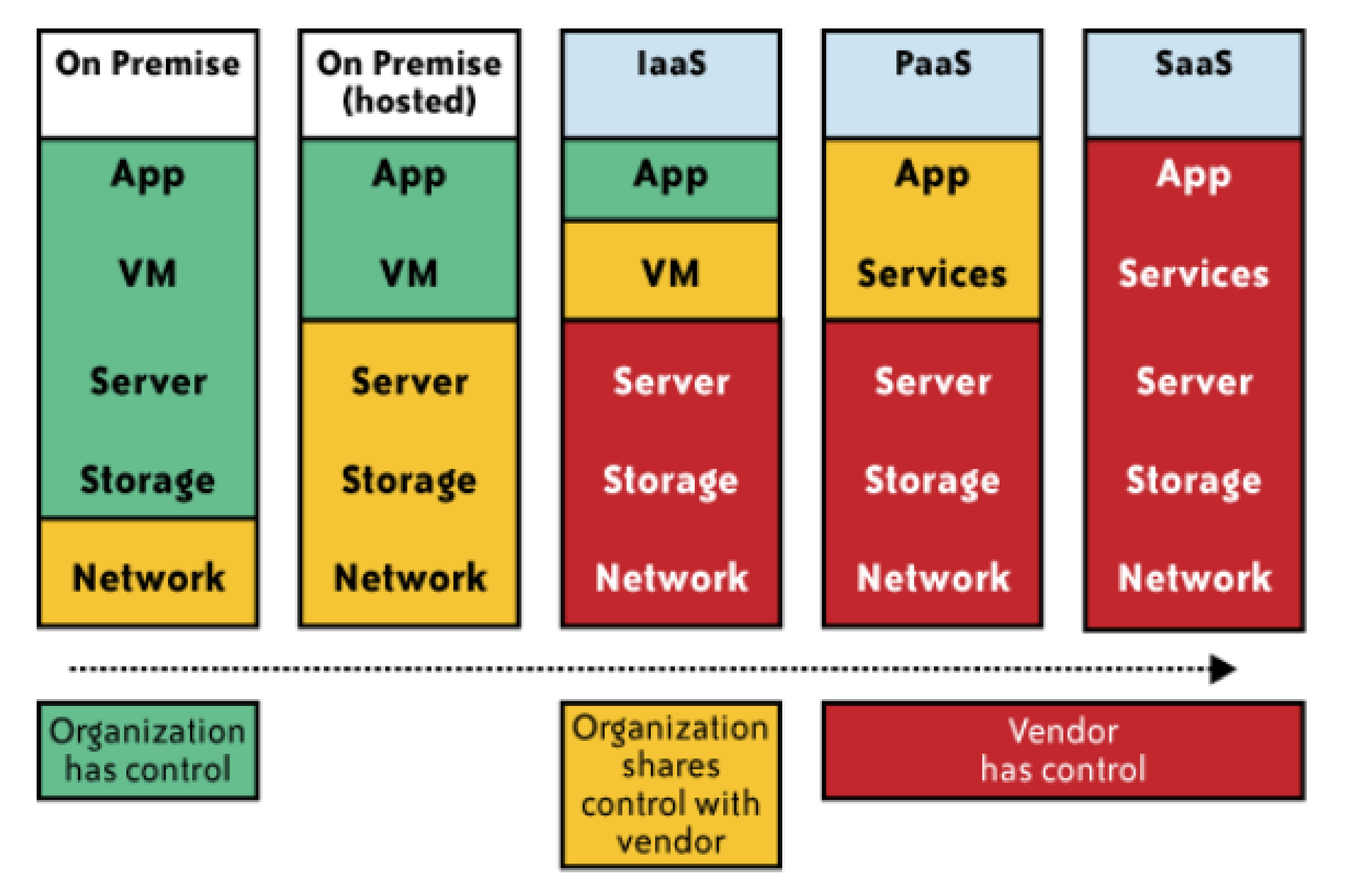
- “Ultimately, you can outsource responsibility but you can’t outsource accountability.”

Cloud Computing: Security Analysis?

- Cloud computing definitely makes sense if your own security is weak, missing features, or below average.
- Ultimately, if
  - the cloud provider's security people are "better" than yours (and leveraged at least as efficiently),
  - the web-services interfaces don't introduce too many new vulnerabilities, and
  - the cloud provider aims at least as high as you do, at security goals,
- then cloud computing has better security.

From [2] John McDermott, ACSAC 09

Impact of cloud on the governance structure of IT organizations

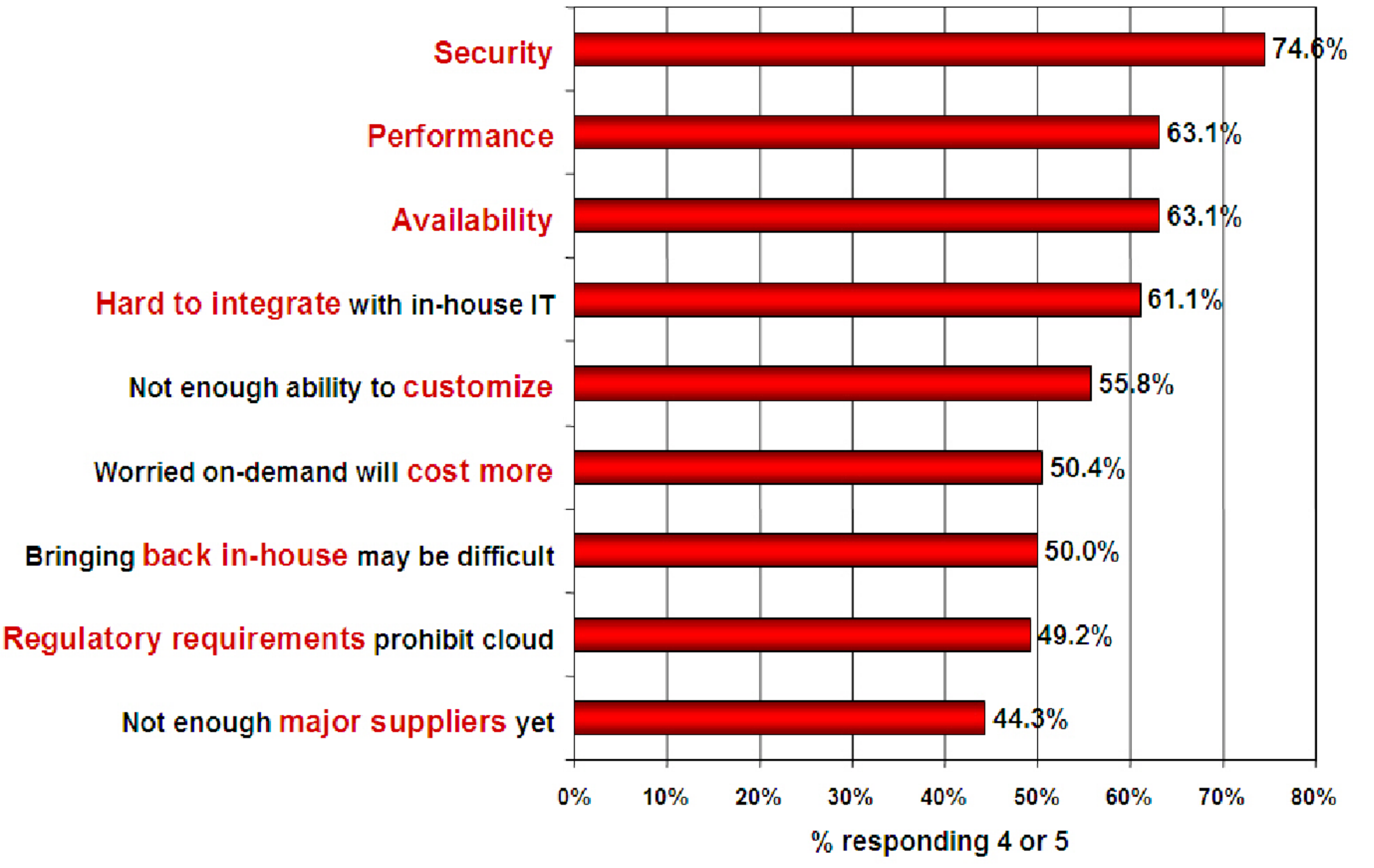


From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Cloud Adoption : Reluctance

- The cloud acts as a big black box, nothing inside the cloud is visible to the clients
- Clients have no idea or control over what happens inside a cloud
- Even if the cloud provider is honest, it can have malicious system admins who can tamper with the VMs and violate confidentiality and integrity
- Clouds are still subject to traditional data confidentiality, integrity, availability, and privacy issues, plus some additional attacks

Companies are afraid to use clouds



Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model

(1=not significant, 5=very significant)

Source: IDC Enterprise Panel, August 2008 n=244

[Chow09ccsw]

Cloud Security Issues

Most security problems stem from:

- Loss of control
- Lack of trust (mechanisms)
- Multi-tenancy

These problems exist mainly in 3rd party management models

- Self-managed clouds still have security issues, but not related to above

[**Chow09ccsw**]

Loss of Control in the Cloud

- Consumer’s loss of control
  - Data, applications, resources are located with provider
  - User identity management is handled by the cloud
  - User access control rules, security policies and enforcement are managed by the cloud provider
  - Consumer relies on provider to ensure
    - Data security and privacy
    - Resource availability
    - Monitoring and repairing of services/resources

Lack of Trust in the Cloud

- Trusting a third party requires taking risks
- Defining trust and risk
  - Opposite sides of the same coin (J. Camp)
  - People only trust when it pays (Economist's view)
  - Need for trust arises only in risky situations
- Defunct third party management schemes
  - Hard to balance trust and risk
  - e.g. Key Escrow (Clipper chip)
  - Is the cloud headed toward the same path?

Multi-tenancy Issues in the Cloud

- Conflict between tenants' opposing goals
  - Tenants share a pool of resources and have opposing goals
- How does multi-tenancy deal with conflict of interest?
  - Can tenants get along together and 'play nicely' ?
  - If they can't, can we isolate them?
- How to provide separation between tenants?
- Cloud Computing brings new threats
  - Multiple independent users share the same physical infrastructure
  - Thus an attacker can legitimately be in the same physical machine as the target

Taxonomy of Fear - CIA

- Confidentiality
  - Fear of loss of control over data
    - Will the sensitive data stored on a cloud remain confidential?
    - Will cloud compromises leak confidential client data
  - Will the cloud provider itself be honest and won't peek into the data?
- Integrity
  - How do I know that the cloud provider is doing the computations correctly?
  - How do I ensure that the cloud provider really stored my data without tampering with it?
- Availability
  - Will critical systems go down at the client, if the provider is attacked in a Denial of Service attack?
  - What happens if cloud provider goes out of business?
  - Would cloud scale well-enough?
  - Often-voiced concern
    - Although cloud providers argue their downtime compares well with cloud user's own data centers

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

Taxonomy of Fear (cont.)

- Privacy issues raised via massive data mining
  - Cloud now stores data from a lot of clients, and can run data mining algorithms to get large amounts of information on clients
- Increased attack surface
  - Entity outside the organization now stores and computes data, and s
  - Attackers can now target the communication link between cloud provider and client
  - Cloud provider employees can be phished

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

Taxonomy of Fear (cont.)

- Auditability and forensics (out of control of data)
  - Difficult to audit data held outside organization in a cloud
  - Forensics also made difficult since now clients don't maintain data locally
- Legal dilemma and transitive trust issues
  - Who is responsible for complying with regulations?
    - e.g., SOX, HIPAA, GLBA ?
  - If cloud provider subcontracts to third party clouds, will the data still be secure?

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

Threat Model

- A threat model helps in analyzing a security problem, design mitigation strategies, and evaluate solutions

- Steps:
  - Identify attackers, assets, threats and other components
  - Rank the threats
  - Choose mitigation strategies
  - Build solutions based on the strategies

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

Threat Model

- Basic components
    - Attacker modeling
        - Choose what attacker to consider
            - insider vs. outsider?
            - single vs. collaborator?
        - Attacker motivation and capabilities
    - Attacker goals
    - Vulnerabilities / threats

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

What is the issue?

- The core issue here is the levels of trust
  - Many cloud computing providers trust their customers
  - Each customer is physically commingling its data with data from anybody else using the cloud while logically and virtually you have your own space
  - The way that the cloud provider implements security is typically focused on they fact that those outside of their cloud are evil, and those inside are good.
- But what if those inside are also evil?

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

Attacker Capability: Malicious Insiders

- At client
  - Learn passwords/authentication information
  - Gain control of the VMs
- At cloud provider
  - Log client communication
  - Can read unencrypted data
  - Can possibly peek into VMs, or make copies of VMs
  - Can monitor network communication, application patterns
  - Why?
    - Gain information about client data
    - Gain information on client behavior
    - Sell the information or use itself

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

Attacker Capability: Outside attacker

- What?
  - Listen to network traffic (passive)
  - Insert malicious traffic (active)
  - Probe cloud structure (active)
  - Launch DoS
- Goal?
  - Intrusion
  - Network analysis
  - Man in the middle
  - Cartography

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

Challenges for the attacker

- How to find out where the target is located?
- How to be co-located with the target in the same (physical) machine?
- How to gather information about the target?

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

PART II: SECURITY AND PRIVACY ISSUES IN CLOUD COMPUTING - BIG PICTURE

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Data Security and Storage

- Several aspects of data security, including:
  - Data-in-transit
    - Confidentiality + integrity using secured protocol
    - Confidentiality with non-secured protocol and encryption
  - Data-at-rest
    - Generally, not encrypted , since data is commingled with other users' data
    - Encryption if it is not associated with applications?
      - But how about indexing and searching?
  - Processing of data, including multitenancy
    - For any application to process data

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

What is Privacy?

- The concept of privacy varies widely among (and sometimes within) countries, cultures, and jurisdictions.
- It is shaped by public expectations and legal interpretations;
  - as such, a concise definition is elusive if not impossible.
- Privacy rights or obligations are related to the collection, use, disclosure, storage, and destruction of personal data
- At the end of the day, privacy is about the accountability of organizations to data subjects, as well as the transparency to an organization's practice around personal information.

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

PART III. POSSIBLE SOLUTIONS

Security Issues in the Cloud

- In theory, minimizing any of the issues would help Third Party Cloud Computing
  - Loss of Control
    - Take back control
      - Data and apps may still need to be on the cloud
      - But can they be managed in some way by the consumer?
  - Lack of trust
    - Increase trust (mechanisms)
      - Technology
      - Policy, regulation
      - Contracts (incentives)
  - Multi-tenancy
    - Private cloud
      - Takes away the reasons to use a cloud in the first place
    - VPC: its still not a separate system
    - Strong separation

Minimize Lack of Trust: Policy Language

- Consumers have specific security needs but don’t have a say-so in how they are handled
  - Currently consumers cannot dictate their requirements to the provider (SLAs are one-sided)
- Standard language to convey one’s policies and expectations
  - Agreed upon and upheld by both parties
  - Standard language for representing SLAs
- Create policy language with the following characteristics:
  - Machine-understandable (or at least processable),
  - Easy to combine/merge and compare

Minimize Lack of Trust: Certification

- Certification
  - Some form of reputable, independent, comparable assessment and description of security features and assurance
    - Sarbanes-Oxley, DIACAP, DISTCAP, etc

- Risk assessment
  - Performed by certified third parties
  - Provides consumers with additional assurance

Minimize Loss of Control: Monitoring

- Cloud consumer needs situational awareness for critical applications
  - When underlying components fail, what is the effect of the failure to the mission logic
  - What recovery measures can be taken
    - by provider and consumer

- Requires an application-specific run-time monitoring and management tool for the consumer
  - The cloud consumer and cloud provider have different views of the system
  - Enable both the provider and tenants to monitor the components in the cloud that are under their control

Minimize Loss of Control: Monitoring (Cont.)

- Provide mechanisms that enable the provider to act on attacks he can handle.
  - infrastructure remapping
    - create new or move existing fault domains
  - shutting down offending components or targets
    - and assisting tenants with porting if necessary
  - Repairs
- Provide mechanisms that enable the consumer to act on attacks that he can handle
  - application-level monitoring
  - RAdAC (Risk-adaptable Access Control)
  - VM porting with remote attestation of target physical host
  - Provide ability to move the user's application to another cloud

Minimize Loss of Control:Utilize Different Clouds

- The concept of 'Don't put all your eggs in one basket'
  - Consumer may use services from different clouds through an intra-cloud or multi-cloud architecture
  - A multi-cloud or intra-cloud architecture in which consumers
    - Spread the risk
    - Increase redundancy (per-task or per-application)
    - Increase chance of mission completion for critical applications
  - Possible issues to consider:
    - Policy incompatibility (combined, what is the overarching policy?)
    - Data dependency between clouds
    - Differing data semantics across clouds
    - Knowing when to utilize the redundancy feature
      - monitoring technology
    - Is it worth it to spread your sensitive data across multiple clouds?
      - Redundancy could increase risk of exposure

Minimize Loss of Control: Access Control

- Many possible layers of access control
    - E.g. access to the cloud, access to servers, access to services, access to databases (direct and queries via web services), access to VMs, and access to objects within a VM
    - Depending on the deployment model used, some of these will be controlled by the provider and others by the consumer

- Regardless of deployment model, provider needs to manage the user authentication and access control procedures (to the cloud)
    - Federated Identity Management: access control management burden still lies with the provider
    - Requires user to place a large amount of trust on the provider in terms of security, management, and maintenance of access control policies.
        - This can be burdensome when numerous users from different organizations with different access control policies, are involved

Minimize Multi-tenancy

- Can’t really force the provider to accept less tenants
  - Can try to increase isolation between tenants
    - Strong isolation techniques (VPC to some degree)
    - QoS requirements need to be met
    - Policy specification
  - Can try to increase trust in the tenants
    - Who’s the insider, where’s the security boundary? Who can I trust?
    - Use SLAs to enforce trusted behavior

Conclusion

- Cloud computing is sometimes viewed as a reincarnation of the classic mainframe client-server model
  - However, resources are ubiquitous, scalable, highly virtualized
  - Contains all the traditional threats, as well as new ones

- In developing solutions to cloud computing security issues it may be helpful to identify the problems and approaches in terms of
  - Loss of control
  - Lack of trust
  - Multi-tenancy problems

?
Q
&
A
!