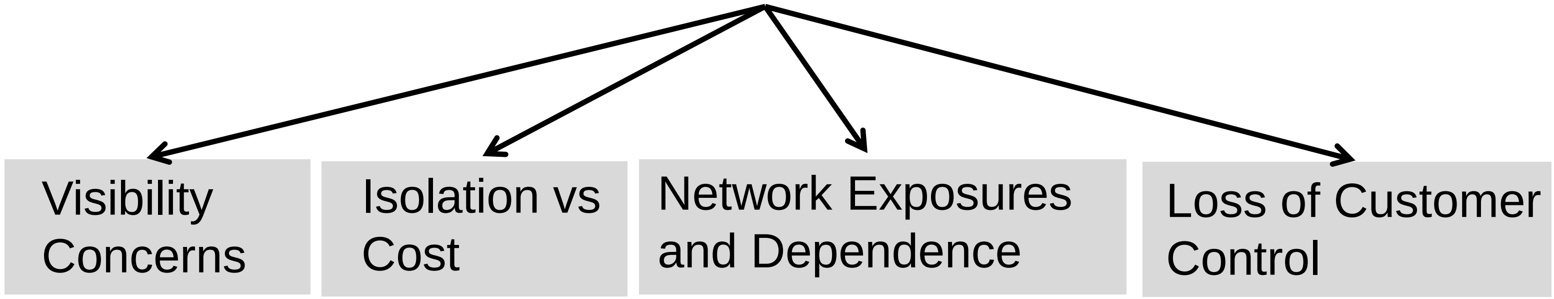
Cloud Security Report Out

4 subgroups



Visibility Concerns

Isolation vs Cost

Network Exposures and Dependence

Loss of Customer Control

Ron Knode

(and everyone in track 3)

General

- We need to include attack modeling in our system descriptions.
- Operational monitoring/checking is important as well as static evaluations.
- A focus on low hanging fruit only may prevent us from getting where we need to be: principled protection of data, security engineered/evaluated systems.
- Can highly sensitive data and applications be supported in cloud processing?
- Cloud data centers appear to be physically well guarded.

Visibility Concerns

- Visibility objective is verifiable transparency
  - Is whatever is claimed be happening really happening ... and nothing else
- What are the elements of information that need to be made “visible” (i.e., “transparent)
  - technical (e.g., configuration, architecture, ...)
  - operational
  - others ??
  - are there “families” or “templates” of such items
- What granularity and timeliness needed

Visibility (continued)

- What's the relationship between the elements needed for visibility/transparency and control frameworks (e.g., FISMA, SAS70, ...)
- How do we benchmark the initial status of elements we care about?
- Is there any difference in the needs for transparency (visibility) between
  - IaaS, PaaS, SaaS
  - public, private, community, hybrid
- What is the linkage between transparency/visibility and contract terms and SLA's?
- Enforcement mechanisms on visibility?

Isolation vs Cost

- We are back to the future
  - Utility computing model, time sharing
- True segmentation is pseudo-science
- However low and moderate systems are the target of evaluation
- Subversion is not truly mitigatable in a cloud
  - too man unknowns
- Risk acceptance versus cost, not isolation versus cost
- SLAs are critical for cloud service

Isolation versus Cost

It comes down to “trying” the low hanging fruit and seeing what the realities are for security

Last consideration was the idea of evaluating the implementation of the cloud itself, not just the “software, platform, or Infrastructure”. The “cloud control system” must be A&A (deep technical analysis, ongoing visibility, etc)

Network Exposures and Dependencies

- Border has changed from perimeter to requiring internal protection
  - Cloud systems amplify this issue
- Adversaries: Need to model the adversaries and include internal and external threats
- Operational: Logic behind the network.
  - Exposing configuration of network to tenants
- Greater dependency on network resiliance
  - Cloud systems by design rely on networked resources
- Security Controls: Need to be closer to the data

Network Exposures and Dependencies

- Legacy System Access
  - User access protected by two factor authentication,
  - but legacy system access interfaces single factor
- Benefits
  - Centralized patch administration
  - SAAS configured by vendor to be secure and protect against misconfigurations causing vulnerablities

Loss of Customer Control

- New consumer security oblgiations
  - e.g., need for a change in Data Labelling/marking
- privileged access to the data
- access by foreign nationals
- ensure data deletion is real
- if you encrypt, then the keys should be in the customers control
- the key generation process shoudl be driven by some trusted third party
- how to ensrue compliance of regulated data

Loss of Customer Control

- does the service provider support muti-tenant audit logging
- vulnerability of other tenants data or applications
- doing dynamic real-time continuous monitoring
- data location
- malicious insiders from service providers
- need for legal and acquisition partners in writing SLAs
- capability of doing data segmentation