Security and the Cloud

Dr. Clifford Neuman, Director
USC Center for Computer Systems Security
Information Sciences Institute
University of Southern California

USC Viterbi
School of Engineering

UNIVERSITY OF SOUTHERN CALIFORNIA
INFORMATION SCIENCES INSTITUTE

CENIC 2010
Monterey, California
10 March 2010

Defining The Cloud

The cloud is many things to many people

- Software as a service and hosted applications
- Processing as a utility
- Storage as a utility
- Remotely hosted servers
- Anything beyond the network card

Clouds are hosted in different ways

- Private Clouds
- Public Clouds
- Hosted Private Clouds
- Hybrid Clouds
- Clouds for federated enterprises

The Cloud is Federated

Securing the cloud will requires some form of

- Federated Identity Management
- Federated Policy Management

Today these federations as ad-hoc

- Pair-wise coordination or
- Multiple registration
- How do we coordinate while still maintaining local control.

Risks of Cloud Computing

Reliability

- Must ensure provider's ability to meet demand and to run reliably

Confidentiality and Integrity

- Service provider must have their own mechanisms in place to protect data.
- The physical machines are not under your control.

Back channel into own systems

- Hybrid clouds provide a channel into ones own enterprise

Less control over software stack

- Software on cloud may not be under your enterprise control

Harder to enforce policy

- Once data leaves your hands

Defining Policy

Characterize Risk

- What are the consequences of failure for different functions

Characterize Data

- What are the consequences of integrity and confidentiality breaches

Mitigate Risks

- Can the problem be recast so that some data is less critical.
  - Redundancy
  - De-identification
- Control data migration within the cloud

Controlling Migration

Characterize Node Capabilities

- Security Characteristics
  - Accreditation of the software for managing nodes and data
- Legal and Geographic Characteristics
  - Includes data on managing organizations and contractors
- Need language to characterize
- Need endorsers to certify

Define Migration Policies

- Who is authorized to handle data
- Any geographic constraints
- Necessary accreditation for servers and software
  - Each node that accepts data must be capable for enforcing policy before data can be redistributed.
- Languages needed to describe

Enforcing Constraints

With accredited participants

- Tag data and service requests with constraints
- Each component must apply constraints when selecting partners
  - Sort of inverting the typical access control model

When not all participants are accredited

- Callbacks for tracking compliance
- Trusted computing to create safe containers within unaccredited systems.

Summary

Great potential for cloud computing

- Economies of scale for managing servers
- Computation and storage can be distributed along lines of a virtual enterprise.
- Ability to pay for normal capacity, with short term capacity purchases to handle peak needs.

What needs to be addressed

- Forces better assessment of security requirements for process and data.
- Accreditation of providers and systems is a must.
- Our models of the above must support automated resolution of the two.

For More Information

For updates and related information

- http://clifford.neuman.name/presentations/2010/20100310-neuman-cenic/
- http://clifford.neuman.name/
- http://ccss.usc.edu/