Cloud Security

Christoph Schuba
Christoph.Schuba@Sun.COM
http://blogs.sun.com/schuba

Cloud Computing

- Evolution:

  ...
  Public Utility Computing
  Grid Computing
  Cloud Computing
  ...

- Enterprise ready. Example:
  - > New York times converting 11M articles/images to PDF
  - > in house IT Dept: 7 weeks
  - > in the cloud: < 24h for < $300

Cloud Computing...

- ...is not for everyone
  - traditional data center architectures
- ...is not for everything
  - some workloads are not for the cloud

- Cloud security is

  different things for different uses

Cloud Users and Uses

- Users
  - > Internet startups
  - > Research projects
  - > Web 2.0 developers
  - > Niche players
- Uses
  - > Development and Testing
  - > Functional offloading
  - > Augmentation (accommodate peak loads)
  - > Experimenting

Cloud Architectural Services

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Cloud types

- Public Cloud
  - Run by third parties
  - Many different customers
  - Mixing of servers, storage systems, other infrastructure
- Private Cloud
  - Good option for companies dealing with data protection and service-level issues
  - Alternative data center architecture
- Hybrid Cloud
  - Controlled way of sharing private and public clouds

Public Cloud Anecdote Lack for Demand for Security

- In Grid computing: 95% of customers opt out of security services
  - Secure grid option exists
  - Informed decision
  - Certificate management overhead too high?
  - Greater security threads already accepted elsewhere?

Complex Cloud Security Map

Public Cloud
Private Cloud
Hybrid Clouds

Authentication
Authorization
Integrity
Availability
Non Repudiation
Audit

Compute
Storage
Communication

*

Startups
Research Projects
Web 2.0 developers
Niche Players

Development and Testing
Functional Offloading
Augmentation
Experimenting

Cornerstone Technologies

- Virtualization technologies
  - OS v12n
  - Type-1/2 hypervisors
  - Network virtualization

  -> Availability/disaster recovery/business continuity
- High-bandwidth networking
- File system support
- Architectural patterns

Cloud Security Mechanisms

- Identity Management and Provisioning
- Network security services
- Secure by default
- User/process rights management
  - Fine-grained application privileges
  - Role-based access control (RBAC) for administration
- Multi-level security and Mandatory Access Control
- Cryptographic service

Security on Many Levels

- Host Operating System
- Guest Operating System
- Firewall
- APIs - very much in flux
- Instance isolation: compute and storage

Security on Many Levels (cont.)

- Network security
  - > DDoS attacks
    - > standard techniques and constant attention
  - > Man In the Middle (MITM) attacks
    - > SSL, SSH, certificate management
  - > IP spoofing
  - > Port scanning
  - > Packet sniffing
    - > Tenant sniffing inside public cloud

Security on Many Levels (cont.)

- Storage security
  - Pool and object-level scrubbing
  - Redundant storage w/o backup?
  - Encrypted storage

Challenges

- New paradigm has unknown failure modes
- Transfer/abandon familiar tools and processes
- Early adoption vs. mission critical use
- Management complexity
  - user, system provisioning, monitoring

Thank you.
Questions?

Christoph Schuba
Christoph.Schuba@Sun.COM
http://blogs.sun.com/schuba