Securing Services in Clouds

Steve Hanna, Juniper Networks

Cloud Computing Defined

- **Dynamically scalable shared IT resources accessed over a network**
  - May include storage, software, platform, etc.
  - Often shared with other customers
  - Often accessed over the Internet
  - Often billed on a usage basis

- **Notes**
  - Similar to Timesharing
    - Rent IT resources vs. buy
  - New term – definition still being developed

Cloud Computing Drivers and Inhibitors

- **Drivers**
  - Lower fixed costs (capital and operating)
  - Greater scalability
  - Faster time to roll out new services

- **Inhibitors**
  - Loss of control
  - Security concerns
  - Availability concerns

Cloud Computing Security

- **Information Security Principles Unchanged**
  - Confidentiality
    - Prevent unauthorized disclosure
  - Integrity
    - Preserve information integrity
  - Availability
    - Ensure information is available when needed

Security Challenges of Cloud Computing

- Loss of control
- Sharing resources with untrusted parties
- Availability issues
- Legal and regulatory issues
- Perimeter model broken
- Integrating provider and customer security systems

Loss of Control

- **Threats**
  - Provider controls servers, network, etc.
  - Customer must trust provider's security
  - Failures may violate CIA principles
- **Countermeasures**
  - Verify and monitor provider's security
- **Notes**
  - Outside verification may suffice
  - For SMB, provider security may exceed customer security

Sharing Resources with Untrusted Parties

- **Threats**
  - Provider resources shared with untrusted parties
    - CPU, storage, network
  - Customer data must be separated
  - Failures will violate CIA principles

- **Countermeasures**
  - Hypervisors for compute separation
  - MPLS, VPNs, VLANs, firewalls for network separation
  - Cryptography (strong)
  - Application-layer separation (less strong)

Availability Issues

- **Threats**
  - Clouds may be less available than in-house IT
    - Complexity increases chance of failure
    - Clouds are prominent attack targets
    - Internet reliability is spotty
    - Shared resources may provide attack vectors
    - BUT cloud providers focus on availability
- **Countermeasures**
  - Evaluate provider measures to ensure availability
  - Monitor availability carefully
  - Plan for downtime
  - Use public clouds for less essential applications

Legal and Regulatory Issues

- **Threats**
  - Laws and regulations may prevent cloud computing
    - Requirement to retain control
    - Certification requirements not met by provider
    - Geographical limitations – EU Data Privacy
  - New locations may trigger new laws and regulations

- **Countermeasures**
  - Evaluate legal issues
  - Require provider compliance with laws and regulations
  - Restrict geography as needed

Perimeter Model Broken (Again)

- **Threats**
  - Including the cloud in your perimeter
    - Lets attackers past the moat
    - Prevents mobile users from accessing the cloud
  - Not including the cloud in your perimeter
    - Essential services aren't trusted
    - No access controls on cloud

- **Countermeasures**
  - Drop the perimeter model!

Integrating Provider and Customer Security

- **Threat**
  - Disconnected provider and customer security systems
    - Fired employee retains access to cloud
    - Misbehavior in cloud not reported to customer
- **Countermeasures**
  - At least, integrate identity management
    - Consistent access controls
  - Better, integrate monitoring and notifications
- **Notes**
  - Can use SAML, LDAP, RADIUS, XACML, IF-MAP, etc.

Bottom Line on Cloud Computing Security

- **Weigh risks and benefits in each case**
- **For small and medium organizations**
  - Cloud security may be a big improvement!
  - Cost savings may be large (economies of scale)
- **For large organizations**
  - Already have large, secure data centers
  - Main sweet spots:
    - Elastic services
    - Internet-facing services
- **Employ countermeasures listed above**