Cloud Access Control Delegation

David Slik
NetApp, Inc.
Cloud Risks & Rewards

- The use of cloud-based data storage has significant technical and business value:
  - Economic “as-a-service” consumption
  - Geographic diversity & mobility
  - Proximity to cloud compute resources

- However, cloud-based data storage introduces significant legal and operational risks:
  - Maintaining data ownership and controls
  - Preventing unauthorized data access
Cloud Risks & Rewards

- These areas of concern have limited the adoption of cloud-based data storage outside situations where:
  - Data is already public
  - Unauthorized disclosure has little economic or political consequence
  - Unauthorized disclosure can be blamed on or consequences transferred to other actors (such as the cloud provider)
  - Costs of avoiding risks are higher than costs of the consequences of the risks
Cloud Risks & Rewards

- Encrypting data before storing it into the cloud resolves governance and access control concerns, but introduces significant new issues:
  - Need to build an entirely new access control and key management system (KMS) + key distribution infrastructure, and modify clients to use these
  - Cloud resources can no longer access data directly, and data needs to flow through custom code that talks with the KMS and decrypts data
Cloud Risks & Rewards

- Ideally, a solution to these trade-offs would involve:
  - Not significantly increasing costs, as this would negate economic benefits of cloud-based data storage
  - Not requiring modifications to cloud infrastructure, which is often not possible because it is controlled by third-parties
  - Require limited or no modifications to applications
Introducing SNIA DAC

DAC – Delegated Access Control

- Standardizes a simple challenge/response protocol for delegating access control decisions and key distribution for HTTP-based storage
- Started as CDMI extension, but works with S3, Swift, etc.

- Can be integrated into any HTTP-based storage protocol
  - Allows use by unmodified clients
  - Allows transparent integration with cloud computing
- Can be used directly by clients
  - Allows use with clouds that don’t support DAC
Introducing SNIA DAC
Integrated with Cloud Server

- Storage Client
  - GET
  - Plaintext

- Cloud Server
  - GET
  - Plaintext
  - DAC Request

- DAC Provider
  - Key
  - Key Read

- KMS

Cloud Compute

OR

Administrative Boundary
Introducing SNIA DAC
Integrated with Storage Client

Cloud Server $\rightarrow$ GET $\rightarrow$ Storage Client $\rightarrow$ DAC Request $\rightarrow$ DAC Response $\rightarrow$ DAC Provider $\rightarrow$ KMS

- Ciphertext $\rightarrow$ Cloud Server
- Key Read $\leftarrow$ KMS
- Administrative Boundary

Integrated with Storage Client
Trustworthy Cloud

- A cloud service that provides assurances (Legal, technical, reputation, audit, etc) that directives on data governance and access control will be honored.
  - Cloud permitted to access to the decryption keys
  - Cloud can thus access data plaintext

- Advantages
  - Allows unmodified clients
  - Allows cloud-driven data processing

- Disadvantages
  - Does not protect against a malicious cloud
  - Does not protect against a compromised cloud
Untrustworthy Cloud

- A cloud service that is known, suspected or capable of violating data governance and access control directives due to technical, financial or personnel issues.
  - Cloud not permitted to access decryption keys
  - Cloud cannot access data plaintext

- Advantages
  - Does not require modifications to cloud
  - Protects against malicious and compromised clouds

- Disadvantages
  - Requires client modifications or proxy
  - Does not support cloud-driven data processing
Delegated Access Control Landscape

<table>
<thead>
<tr>
<th>Untrustworthy Cloud</th>
<th>Trustworthy Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td></td>
</tr>
<tr>
<td>Client DAC</td>
<td>Server DAC</td>
</tr>
<tr>
<td>Required for Trust</td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td>Client DAC</td>
</tr>
<tr>
<td></td>
<td>Required for Trust</td>
</tr>
</tbody>
</table>

Support for Delegated Access Control

AWS KMS

Amazom S3

Microsoft Azure

Additional Integration Points

- Cloud Integration
  - Requires participation of cloud provider

- Client Integration
  - Requires modifications to application

- Web Application Integration
  - Requires less invasive modifications to web apps

- Proxy Integration
  - Requires no modifications to applications
Web Application Integration
Where cloud supports Delegated Access Control

- Javascript library added to web application that intercepts all AJAX calls
  - Library adds headers to cloud HTTP(S) operations
  - Cloud forwards request to Delegated Access Control system
  - Delegated Access Control system makes access determination decision based on client headers
  - Ciphertext returned with access headers
  - Library decrypts access headers
  - Library uses access headers to transparently decrypt ciphertext
Web Application Integration
Where cloud does not support Delegated Access Control

- Javascript library added to web application that intercepts all AJAX calls
  - Library gets ciphertext from cloud HTTP(S) operation
  - Library makes Delegated Access Control request directly to Delegated Access Control system
  - Delegated Access Control system makes access determination decision based on client headers
  - Library decrypts access headers
  - Library uses access headers to transparently decrypt ciphertext
Native Protocol Proxy Integration
Where cloud supports Delegated Access Control

- Proxy added between application and cloud provider
  - Proxy receives application HTTP(S) operation
  - Proxy adds headers to cloud operations
  - Cloud forwards request to Delegated Access Control system
- Delegated Access Control system makes access determination decision based on client headers
- Ciphertext returned with access headers to proxy
- Proxy decrypts access headers
- Proxy uses access headers to transparently decrypt ciphertext, and returns plaintext to application
Native Protocol Proxy Integration
Where cloud does not support Delegated Access Control

- Proxy added between application and cloud provider
  - Proxy receives application HTTP(S) operation
  - Proxy gets ciphertext from cloud
  - Proxy makes Delegated Access Control request directly to Delegated Access Control system
- Delegated Access Control system makes access determination decision based on client headers
- Proxy decrypts access headers
- Proxy uses access headers to transparently decrypt ciphertext, and returns plaintext to application
JavaScript/CDMI Client Demonstration
Call for Participation

- SNIA is widening work on DAC to take it beyond CDMI
- Looking at creating a stand-alone standard for DAC
- If you’re working with object/cloud storage, and want to participate, contact us and join the Cloud technical working group (TWG)
  - Weekly Wednesday calls
  - Bi-monthly face-to-face meetings
  - Quarterly plugfests

- Join us at the Plugfest being held at SDC!
Thank you!

Questions

dslik@netapp.com