Safe Deduplication and Message-Locked Encryption

Vinson Young
Eswar Natarajan
Motivation

- Secure Storage on Cloud
  - Encryption
- Memory-efficient Storage on Cloud
  - Deduplication
- Caveat:
  - Per-user encryption destroys reduces deduplication
  - Current implementations trade security vs. storage
- Important for secure Cloud / Infrastructure-as-a-service for user / provider
Proposal Overview

- Evaluate current encryption + deduplication methods
- Create new system based on shortcomings of current ideas
Background

- Memory Deduplication
  - Identical memory blocks/pages combined
  - Significant space saving
  - Many identical pages between users running same OS
Background (cont’d)

- Encryption
  - Encrypt(Plaintext, Key+IV) = Ciphertext
  - Ciphertext ideally looks random
  - Key storage / generation changes security properties
Overview -- Current Techniques

- Message-locked Encryption
  - Key based on hash of full message
  - Identical message -> Identical cipher for dedup

- Where is hashing for key done?
  - Client-side
  - Server-side
  - Separate Trusted Server
    - ClouDedup - separate server + block-based
    - DupLESS - separate server + message-based
Proposal

- By November 1st: Set up own server with encryption+deduplication
- By November 10th: Evaluate current proposals (client-side, server-side, and trusted-server)
- By November 20th: Come up with new idea and implement
- By Dec 1: Ready presentation
Evaluation Methodology

- Test reference framework for expected side-channel leaks (client-side and server-side) and potential other leaks
- Test potential proposal against leaks seen in prior proposals