Preserving Privacy in Policy-Based Content Dissemination
Mohamed Nabeel, Ning Shang, Elisa Bertino (Purdue University)

What is policy based content dissemination?

A simplistic approach using encryption

Only one encryption per node!

Issue #1: Privacy of the users is not preserved

Issue #2: The key management does not scale

Building blocks: OCBE and BGKM Schemes

OCBE: Oblivious Commitment Based Envelope

An encrypted message

Commitment (I am a doctor)

Envelope (Here are the secrets to Medical Records)

Publisher

Subscriber

* Publisher does not learn credentials
* User can open the envelope only if her credential satisfies the condition

BGKM: Broadcast Group Key Management

Each row is constructed with

a random vector from the n-th space of A

ACV - Access Control Vector

Some selected experimental results

Average computation time for running one round of GE-OCBE protocol

Time to generate an ACV for different user configurations

Key decryption time for different user configurations

ACV generation and key decryption for different number of conditions per policy