Flexible End-to-End Security in CCN

Christopher A. Wood[1][2]   Ersin Uzun[2]

[1] Department of Computer Science
UC Irvine

[2] Computer Science Laboratory
PARC

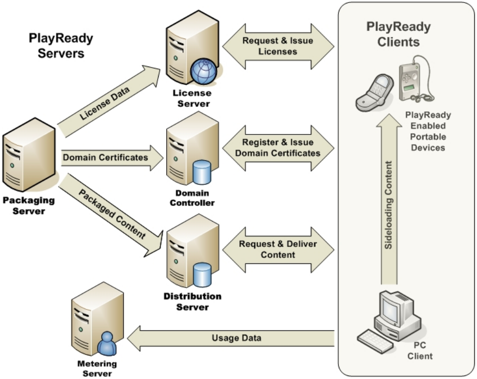
IEEE Consumer Communications and Networking Conference, 2014
Special Session: Information Centric Networking

Outline

1. Problem Statement and Motivation
2. Proxy Re-Encryption (PRE) for Content Protection
3. PRE-Based Architecture
4. Wrapping Up

Overview of General DRM Solutions

- Content is encrypted with a randomly generated (content) key
- Content key is encrypted with target consumer's public key and embedded in licenses
    - Licenses individualize content for a single consumer
- Inherent hybrid approach for encrypting content

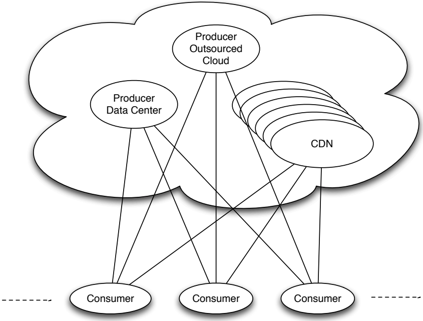


Source:

http://www.microsoft.com/playready/documents/

Technical Landscape: Cheap Storage and Expensive Bandwidth

- Common constraint:
  - Storage space is cheaper than bandwidth
- Content delivery infrastructure:
  - CDNs (old) or CCN (new)
  - Efficient distribution and scalability



CCN-Specific Content Delivery

- Solution #1: consumers ask for media directly over a secure tunnel

CCN-Specific Content Delivery

- Solution #1: consumers ask for media directly over a secure tunnel
- Problem #1:
  - We want to utilize storage/cache in the network and avoid unnecessary round-trip messages

CCN-Specific Content Delivery

- Solution #1: consumers ask for media directly over a secure tunnel
- Problem #1:
  - We want to utilize storage/cache in the network and avoid unnecessary round-trip messages
- Solution #2: encrypt content with one key, cache in the network, force consumers to get key online

CCN-Specific Content Delivery

- Solution #1: consumers ask for media directly over a secure tunnel
- Problem #1:
  - We want to utilize storage/cache in the network and avoid unnecessary round-trip messages
- Solution #2: encrypt content with one key, cache in the network, force consumers to get key online
- Problem #2:
  - We don't want a dishonest user to publish symmetric keys that enable others to bypass DRM protection

CCN-Specific Content Delivery

- Solution #1: consumers ask for media directly over a secure tunnel
- Problem #1:
  - We want to utilize storage/cache in the network and avoid unnecessary round-trip messages
- Solution #2: encrypt content with one key, cache in the network, force consumers to get key online
- Problem #2:
  - We don't want a dishonest user to publish symmetric keys that enable others to bypass DRM protection

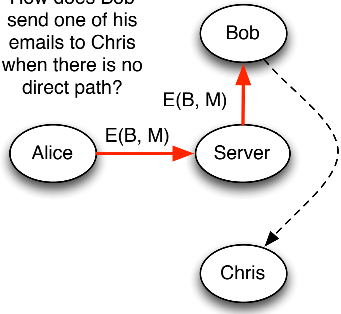
Main question: How can we leverage network caches without sacrificing content security and individualization?

Proxy Re-Encryption

Enter Proxy Re-Encryption

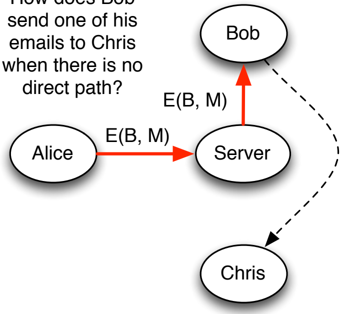
Proxy Re-Encryption Overview

How does Bob send one of his emails to Chris when there is no direct path?

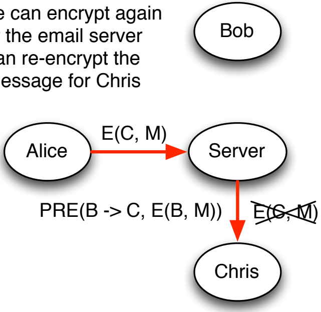


Proxy Re-Encryption Overview

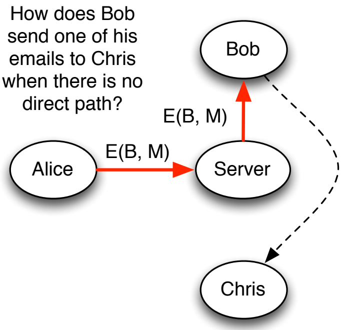
How does Bob send one of his emails to Chris when there is no direct path?



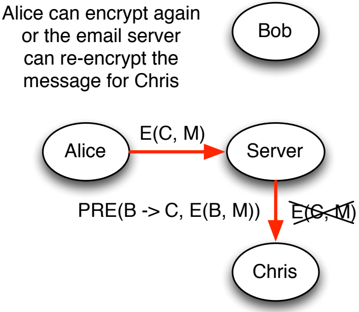
Alice can encrypt again or the email server can re-encrypt the message for Chris



Proxy Re-Encryption Overview



How does Bob send one of his emails to Chris when there is no direct path?



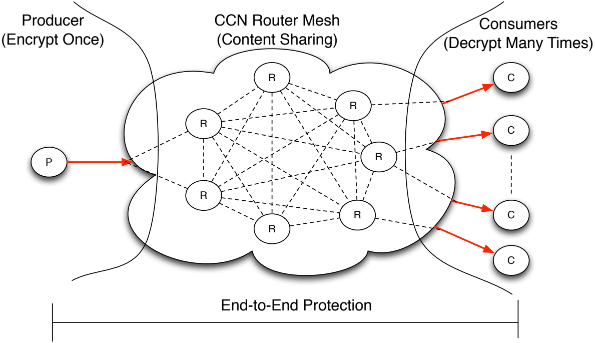
Alice can encrypt again or the email server can re-encrypt the message for Chris

- Email server transforms ciphertext encrypted by Bob's public key to a new ciphertext encrypted by Chris's public key
- Ideal properties of a PRE scheme:
    - Unidirectional, non-interactive, single- or multi-hop, etc.

PRE Application Motivation

DRM technology based solely on PRE for content security enables:

- End-to-end content security
- No risk of shared key leakage
- Full usage of network caches



Flavors of PRE

There exists many constructions of PRE schemes:

- Identity-based constructions (Green and Ateniese)
- ElGamal encryption and Schnorr signature combinations (Chow, Weng, Yang, and Deng)
- And more...

Flavors of PRE

There exists many constructions of PRE schemes:

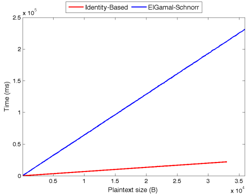
- Identity-based constructions (Green and Ateniese)
- ElGamal encryption and Schnorr signature combinations (Chow, Weng, Yang, and Deng)
- And more...

Our application architecture is concerned with the following properties.

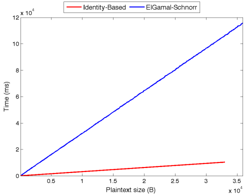
PRE Property	*Identity-Based* [1]	*ElGamal-Schnorr* [2]
1. Unidirectional	✓	✓
2. Non-interactive	✓	✓
3. Non-transitivity	✓	✓

Single- or multi-hop re-encryption depends on the use case!

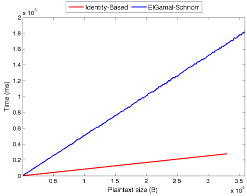
PRE in Practice (single-hop)



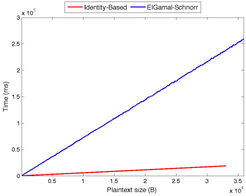
(a) Encrypt() times



(b) ReKeyGen() times



(c) ReEncrypt() times



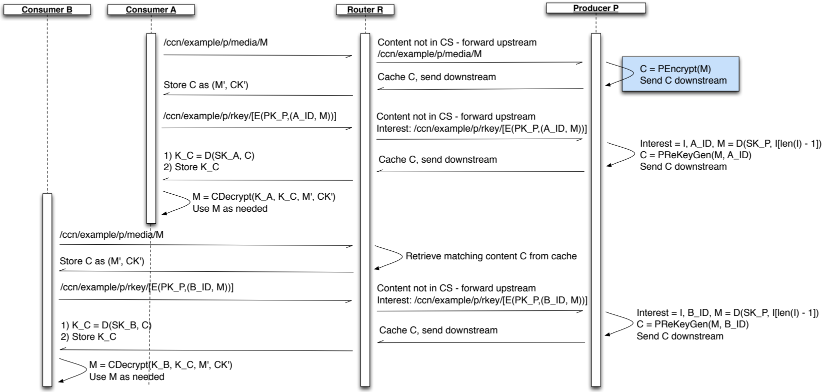
(d) Decrypt() times

(*Based on Java implementations using JPBC library and native BigInteger class*)

Content Retrieval Overview

1. (Setup) Consumer i is issued a secret key sk_i by the producer
   - Issued by the master key manager in the identity-based setting
2. (Online) Consumer i asynchronously requests content encrypted C_p under a producer-owned public key and re-encryption key $\mathrm{rk}_{P \rightarrow C}$
3. Upon receipt of both:
   1. Re-encrypt the encrypted content C using $\mathrm{rk}_{P \rightarrow C}$ to obtain C_i
   2. Decrypt C_i using sk_i

Content Retrieval Message Flow



/ccn/example/p/media/M

Content not in CS - forward upstream
/ccn/example/p/media/M

C = PEncrypt(M)
Send C downstream

Cache C, send downstream

Store C as (M', CK')

/ccn/example/p/rkey/[E(PK_P,(A_ID, M))]

Content not in CS - forward upstream
Interest: /ccn/example/p/rkey/[E(PK_P,(A_ID, M))]

Interest = I, A_ID, M = D(SK_P, I[len(I) - 1])
C = PReKeyGen(M, A_ID)
Send C downstream

Cache C, send downstream

1) K_C = D(SK_A, C)
2) Store K_C

M = CDecrypt(K_A, K_C, M', CK')
Use M as needed

/ccn/example/p/media/M

Retrieve matching content C from cache

Store C as (M', CK')

/ccn/example/p/rkey/[E(PK_P,(B_ID, M))]

Content not in CS - forward upstream
Interest: /ccn/example/p/rkey/[E(PK_P,(B_ID, M))]

Interest = I, B_ID, M = D(SK_P, I[len(I) - 1])
C = PReKeyGen(M, B_ID)
Send C downstream

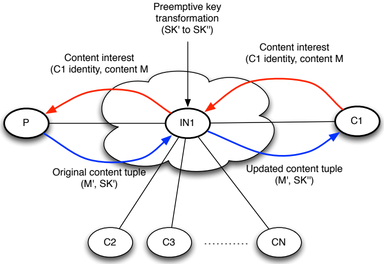
Cache C, send downstream

1) K_C = D(SK_B, C)
2) Store K_C

M = CDecrypt(K_B, K_C, M', CK')
Use M as needed

In-Network Transformations

- Preemptively request consumer re-encryption keys to enable access when producer is offline
- Re-encrypt content at (application layer of) routers/proxies to save consumer decryption overhead
    - This feature requires a multi-hop PRE scheme
- Full PRE scheme can be deployed if routers/proxies can spare extra cycles


Preemptive key transformation (SK' to SK")
Content interest (C1 identity, content M
Content interest (C1 identity, content M
P
IN1
C1
Original content tuple (M', SK')
Updated content tuple (M', SK")
C2
C3
....
CN

Implementation Discussion

Implementation notes:

- Producers and consumers implemented as Java programs and tested over CCNx
- PRE setup phase done offline and relevant keys are stored in local files
- Java objects are serialized and embedded in interests before sent through the network

Future plan: Release code as CCNx application

Preliminary Evaluation (Benefits)

- End-to-end encryption from producer to consumer application
- Strong content security with individualized encryption keys
- Full utilization of caching in CCN
- Few round-trip messages between producers
- Compatible with existing business models and flexible enough to accommodate in-network transformation proxies
- Significantly simplified key management (i.e., one private key per user to decrypt various content)

Preliminary Evaluation (Drawbacks)

- Known PRE constructions are prohibitively expensive to use for large content objects
    - Hybrid encryption approach required

Preliminary Evaluation (Drawbacks)

- Known PRE constructions are prohibitively expensive to use for large content objects
  - Hybrid encryption approach required
- Hybrid encryption requires content to be encrypted with the same symmetric key
  - *No better than current PKI-based DRM solutions*

Review

- PRE-based content delivery provides the best of both worlds:
  1. End-to-end content protection and individualization
  2. Complete usage of in-network storage and caches
- Supports appealing business models for content delivery:
  - Proxy-based decryption to save client computational resources
- Enables flexible client key management

Questions

Thank you for your attention!

Questions? Fire away!

References I

M. Green and G. Ateniese. Identity-Based Proxy Re-Encryption. *Applied Cryptography and Network Security. Springer Berlin Heidelberg* (2007).

S. Chow, J. Weng, Y. Yang, and R. Deng. Efficient Unidirectional Proxy Re-Encryption. *Progress in Cryptology - AFRICACRYPT 2010*. Springer Berlin Heidelberg (2010), 316-332.