Content-Base Confidentiality

lessons learned in the past year

Yingdi Yu
UCLA
What is content-based confidentiality?

- Confidentiality stays with content
  - independent from where the content is
  - independent from how it is delivered
  - content are produced in encrypted format
  - only authorized consumers are able to access the content

- Application-level end-to-end confidentiality
  - not just the end of a connection
  - multi-party communication
Req. on confidentiality

• Once encrypted, hard to change
  • encrypted content is sealed by digital signature

• Encryption requires careful design
  • fine granularity
    • different content may be visible to different consumers
  • flexibility
    • retain the ability of changing confidentiality without re-encryption
  • scalability
    • keep reasonable number of encryption keys
    • avoid unnecessary re-encryption/signing
  • forward secrecy
    • make encryption keys less dependent on other keys

• Content encryption should not block data production
Application driven approach

- Two pilot applications
  - EBAMS, open mHealth
  - distributed production
    - a group of producers under the same name space
- differential confidentiality
  - different consumers may access different content
- Online data sharing
Granularity

- minimum granularity is necessary unless content redesigning is feasible

- content is encrypted directly using key with minimum granularity

- coarse granularity is expressed as a combination of keys with smaller granularity
Flexibility

• grant new consumers the access to content
  • re-encrypt keys rather than re-encrypt content

• revoke consumers’ access to content
  • for content yet to be produced
    • give each decryption key a limited scope (e.g., time interval)
    • prevent a consumer from acquiring access to further content
  • for content has been produced
    • make decryption keys unavailable if consumer has not got the key yet
    • still an open question about how to revoke access if consumer has got the decryption key
Scalability

• producers <-> consumers
  • it may not scale if each producer has to know every potential consumer
  • need an indirection (namespace manager)
    • present single encryption instruction to producers
    • distribute decryption credentials to consumers

• content production <-> access control
  • content should be encrypted without knowing the access control information
  • need an indirection
    • content is encrypted using a key created by content producer
    • content encryption key is encrypted by another key that represents access scope
Name-based access control

• Namespace manager publishes encryption instructions in terms of a named public key (group encryption key)
  • `/alice/health/read/activity/E-KEY/20150928080000/20150928180000`
  • encrypt Alice’s activity data produced during 8am to 6pm on Sep. 28th, 2015

• Namespace manager publishes decryption credentials in terms of encrypted private key (group decryption key)
  • encrypted using each authorized consumer’s public key
  • `/alice/health/read/activity/D-KEY/20150928080000/20150928180000/FOR/bob`
Content production/consuming

- Producer create a symmetric key (content key) to encrypt content
  - content key has the minimum granularity, e.g. one hour
  - `/alice/health/samples/activity/steps/C-KEY/20150928080000/20150928090000`
- Producer retrieves group encryption key from namespace manager
  - encrypt content key using a group encryption key if the content key name falls into the scope of the group encryption key
  - `/alice/health/samples/activity/steps/C-KEY/20150928080000/20150928090000/FOR/alice/health/read/activity`

- Consumer decrypts content by constructing a decryption key chain
  - retrieve encrypted content, encrypted content key, encrypted group decryption key

- Application library will be available in next NDN platform release
Open questions

• Revoke access that has been granted
  • controlled functional encryption

• Avoid key exchange between namespace manager and producers
  • identity-based encryption, attribute-based encryption

• Enable forward secrecy: decouple consumer private key with content key
  • minimize the damage when a private key is compromised later

• Read auditing

• Secure multi-party computing
Summary

• Content-based confidentiality makes confidentiality of content location-independent

• Content should be carefully encrypted to achieve flexible and scalable access control at fine granularity

• Expressive NDN name can be leveraged for efficient access control

• More encryption schemes need to be explored to address remaining issues