UCLA ENGINEERING
Henry Samueli School of Engineering and Applied Science
Birthplace of the Internet

NAC: Named-Based Access Control in NDN

Zhiyi Zhang (UCLA), Yingdi Yu (UCLA), Alexander Afanasyev (Florida International University), Jeff Burke (UCLA), Lixia Zhang (UCLA)

Internet Research Laboratory

Introduction

Data-centric confidentiality by encryption requires an **easy-to-use key management mechanism**

- Only authorized parties can access protected data.
- Support fine granularity

NAC

- Using **NDN naming conventions** to systematically name encrypted data and keys
- Automated decryption key retrieval for legitimate consumers

NAC-ABE

- Supporting **attribute-based encryption** to achieve higher flexibility and lower overhead

Name-based Access Control (NAC)

Naming Convention

- Interest packet uses the prefix (in gray box) to fetch the data packet
- **ENCRYPTED-BY** as a special component
- Data packet's name carries, as a suffix, the name of the key used to encrypt its content

Content Data Name /<OriginalContentName>/**ENCRYPTED-BY**/<CKName>

CK Data Name /<CKName>/**ENCRYPTED-BY**/<CredPrefix>/**KEK**/…

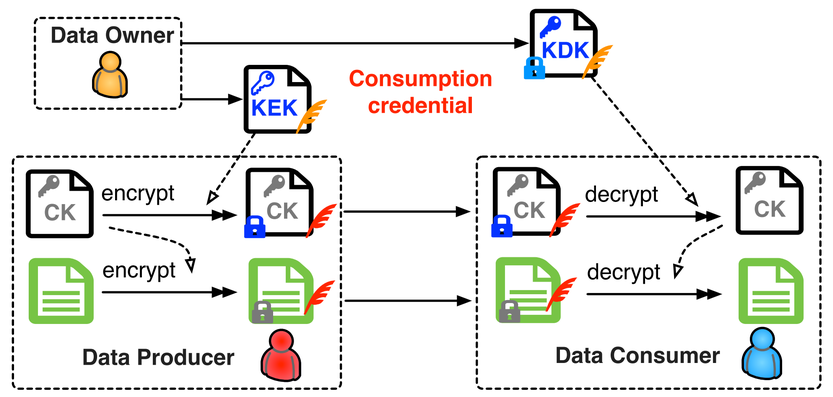
KDK Data Name /<CredPrefix>/**KDK**/…/**ENCRYPTED-BY**/<ConsName>/**KEY**/…

<CredPrefix> Credentials inferred from content name prefix

<ConsName> Identity name from consumer's own certificate

Entities

- Data Owner* controls user's access to content
- Data Producer* produces content and encrypt content
- Data Consumer decrypts content



* can be the same entity

NAC with Attribute-based Encryption Extensions (NAC-ABE)

Attribute-based Encryption

- Use readable plain-text **attribute policy** as the encryption key (e.g. "*UCLA and student*", "*register-year > 2014*")
- Users with **necessary attributes** can decrypt the content, e.g., key for {"UCLA", "student"} attribute set can decrypt the content encrypted by "UCLA and student" policy

Naming Convention

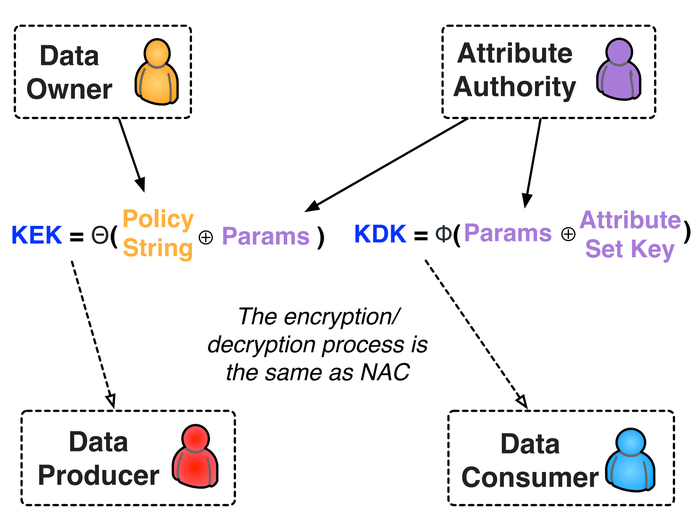
CK Data Name /<CKName>/**ENCRYPTED-BY**/<AttrPolicy>

KDK Data Name /<Authority>/**DKEY**/<AttrSet>/**ENCRYPTED-BY**/<ConsName>

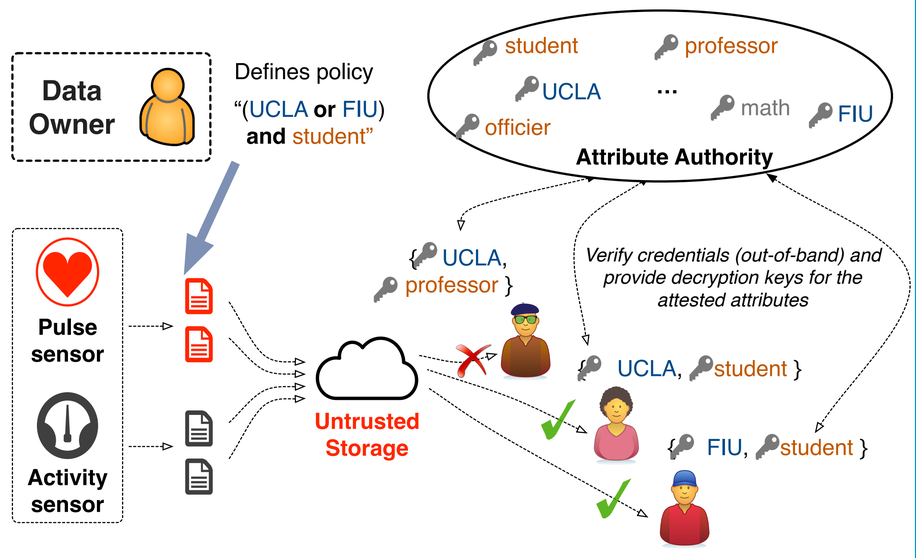
<AttrPolicy> The policy defined by the data owner

<AttrSet> A set of attributes represented by the crypto key

Attribute authority as a level of indirection

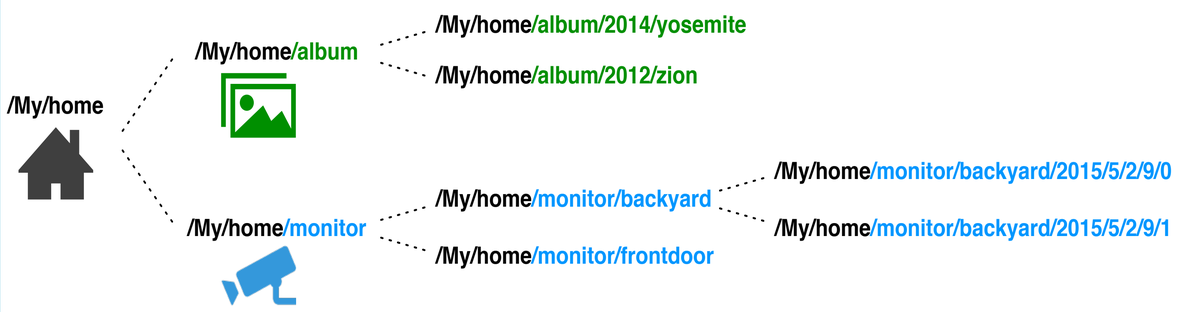


Named attributes and attribute policy

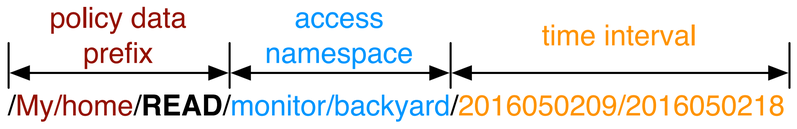


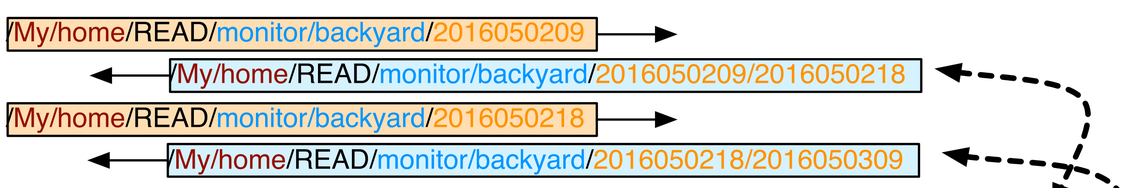
Fine-grained Access Control

1. Hierarchical naming structure



2. Naming convention





In addition to the hierarchical naming structure, **timestamp components** can be added to the data and key names to control data access by specific time periods.

May 2nd 9AM-4PM
/<prefid>/C-KEY/**2016050209/2016050210**

May 2nd 4PM- May 3rd 9AM
/<prefid>/C-KEY/**2016050216/2016050309**

May 3rd 9AM-4PM
/<prefid>/C-KEY/**2016050309/2016050316**

3. Named attributes and attribute policies of NAC-ABE

Future Work

- **Access rights revocation**: It is possible that the data owner may want to revoke a consumer's access before the end of the time interval.
- **Name confidentiality**: The name of the data packet and interest packet conveys rich information.
- **Forward secrecy**: Forward secrecy requires past communication to be free from compromise of a long lived key.

References & Code bases

[1] L. Zhang, A. Afanasyev, et al., "Named Data Networking," ACM SIGCOMM Computer Communication Review, 2014.

[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. of Conference on the Theory and Applications of Cryptographic Techniques, 2005, pp. 457–473.

[3] Y. Yu, A. Afanasyev, and L. Zhang, "Name-based access control," Technical Report NDN-0034, Revision 2, 2016.

[4] M. Ion, J. Zhang, and E. M. Schooler, "Toward content-centric privacy in icn: Attribute-based encryption and routing," in Proceedings of the 3rd ACM SIGCOMM Workshop on Information-centric Networking, 2013

NDN-CCL https://github.com/named-data/ NDN-CCL-API
NAC-ABE https://github.com/Zhiyi-Zhang/NAC-ABE

This material is based upon work supported by the National Science Foundation under contract No. CNS-1345318 and CNS-1629922