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

# NAC: Automating Access Control via Named Data

Zhiyi Zhang (UCLA), Yingdi Yu (UCLA), Sanjeev Kaushik Ramani (FIU),
Alexander Afanasyev (FIU), Lixia Zhang (UCLA)

Internet Research Laboratory

## Motivation & Introduction

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

- Only authorized parties are given the access to protected data.
- Fine granularity

**NAC**

- Using **NDN naming conventions** to systematically name encrypted data and keys
- Legitimate consumers can securely retrieve keys only by names

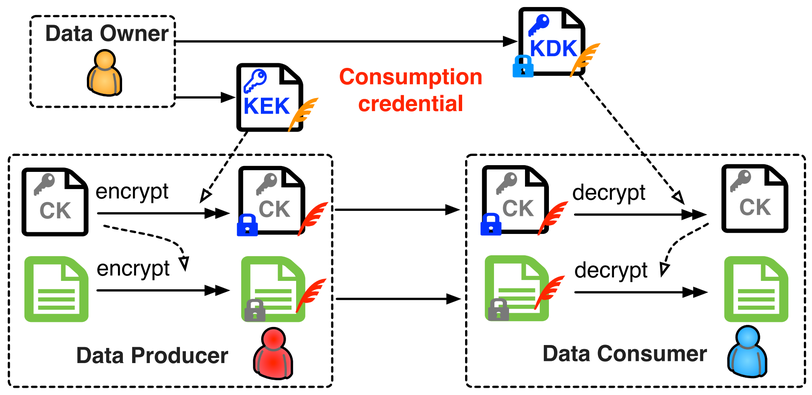
**NAC-ABE** also

- Take use of **attribute-based encryption** to achieve higher scalability and lower overhead

## Name-based Access Control (NAC)

### Naming Convention

- Interest packet uses the prefix 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




### Work Flow of NAC

**Content Data** /military/air/aircraftA/info
Extract CK name from Data Content

**CK Interest** /military/air/aircraftA/**CK**/<CK-id>

**CK Data** /military/air/aircraftA/**CK**/<CK-id>
**/ENCRYPTED-BY**
/military/control/**NAC**/military/air/aircraft/**KEK**/<Key-id>
Extract KDK name from Data name

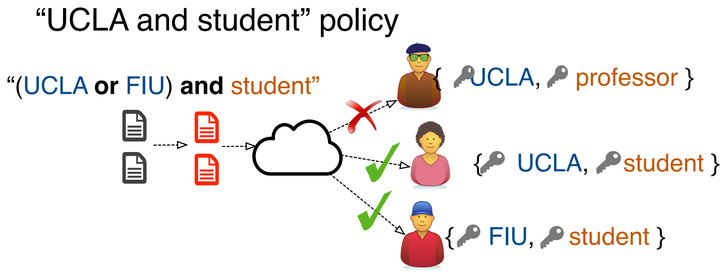
**KDK Interest** /military/control/**NAC**/military/air/aircraft/**KDK**/<Key-id>
**/ENCRYPTED-BY**
/militay/ground/squardA/soldier1/KEY/<Key-id>

**KDK Data** /military/control/**NAC**/military/air/aircraft/**KDK**/<Key-id>
**/ENCRYPTED-BY**
/militay/ground/squardA/soldier1/**KEY**/<Key-id>

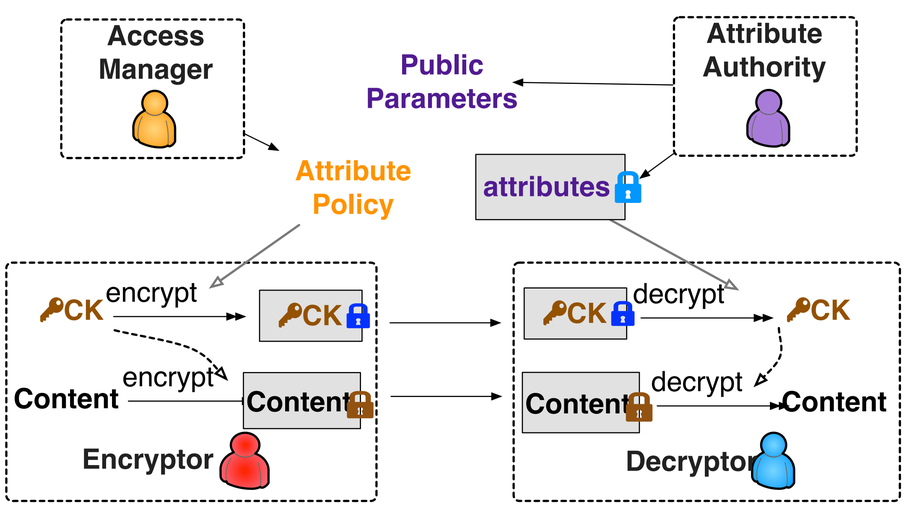
## NAC with Attribute-based Encryption Extensions (NAC-ABE)

### Attribute-based Encryption

- Use readable plain-text attribute policy as the encryption key, such as "UCLA and student", "register-year > 2014"
- Users who have sufficient attributes can decrypt the content, e.g., key for {"UCLA", "student"} attribute set can decrypt the content encrypted by "UCLA and student" policy




### Attribute authority as a level of indirection




### KEK (Policy) Fetching and CK Encryption

**KEK Interest** /military/control/**NAC**/military/air/aircraftA/**KEK**

**KEK Data** /military/control/**NAC**/military/air/aircraftA/**KEK**
**/(**"Soldier" AND "SquadA") OR "General"

CK ("Soldier" AND "SquadA") OR "General" CK

### Naming Convention

**Content Data** /military/air/aircraftA/info
Extract CK name from Data Content

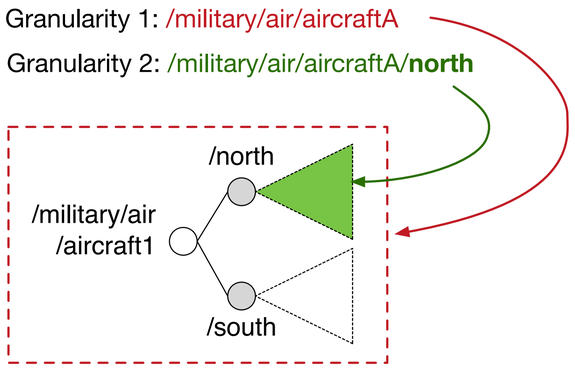
**CK Interest** /military/air/aircraftA/**CK**/<CK-id>

**CK Data** /military/air/aircraftA/**CK**/<CK-id>
**/ENCRYPTED-BY**
/military/control/**NAC**/military/air/aircraftA/**KEK**/
**(**"Soldier" AND "Squad A") or "General"

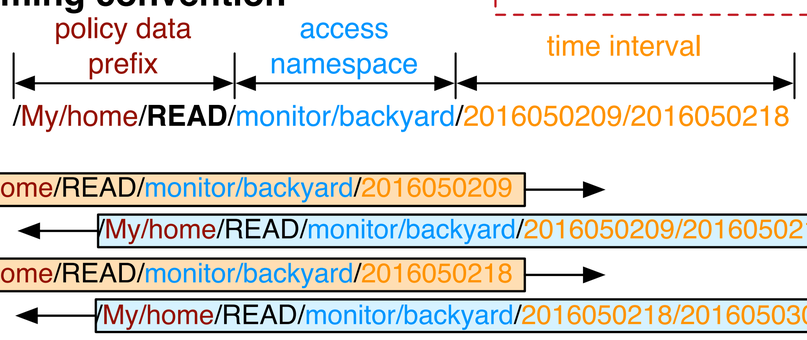
## Fine-grained Access Control

### 1. Hierarchical naming structure

The hierarchical naming helps to establish the access control granularity in a natural way.




### 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

With attribute-based access control, the system can define the attributes based on the granularity need of the system.

## Security Assessment

**Threats mitigation by NAC**

- Eavesdropping: All sensitive data is encrypted and thus makes no sense for attackers, even though attackers can collect these data from the broadcast media or cache.
- Device Compromise: Short-lived KEK-KDK pairs to reduce the information leakage. Access manager can also initiatively notify producers to do re-encryption.

**Threat Mitigation by NDN**

- Man-in-the-Middle Attack: All data in NDN is signed.
- Denial of Service Attack: When attackers flood the Interest packets for the content or keys, the cache can stop these Interests. If attackers use forged Interest packets (e.g., append randomness to a valid prefix), mechanism proposed and mentioned in previous papers (https://named-data.net/publications/) can mitigate such attacks.

## 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] Zhiyi Zhang, et al., "NAC: Automating Access Control via Named Data", in Proc. of Conference on IEEE Milcom 2018 Track 2 - Networking Protocols and Performance.
[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

NAC https://github.com/named-data/ name-based-access-control
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-1719403

## Named Data Networking (NDN): A New Internet Archi