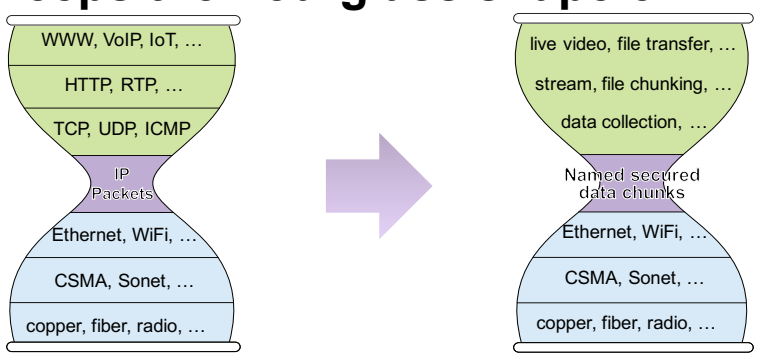
NAC
Name-Based Access Control in NDN

Zhiyi Zhang (UCLA), **Yingdi Yu** (UCLA),
Alexander Afanasyev (UCLA), **Lixia Zhang** (UCLA)

Named Data Networking (NDN): A New Internet Architecture

Keeps the hourglass shape of IP



Fundamentally changes the narrow waist

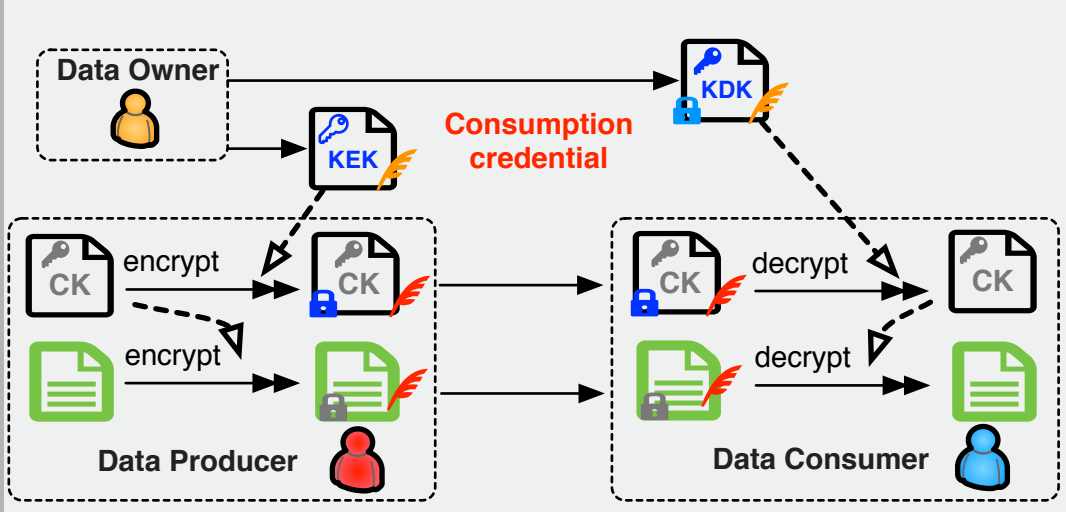
Delivering packets to given destination addresses → Fetching data identified by given names

Makes Possible

- Transparent data retrieval via any available channels, or from storage or analytics engines
- Data is signed and, when needed, encrypted at data production time
- Resilient, efficient, and scalable data distribution
  - Built-in multicast support, loop-free multi-path retrieval, request aggregation
  - Adaptive routing and forwarding with quick detection and avoidance of failures

Name-based Access Control (NAC)

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



Content Data Name

/<OriginalContentName>/**ENCRYPTED-BY**/<CKName>

CK Data Name

/<CKName>/**ENCRYPTED-BY**/<CredPrefix>/**KEK**/…

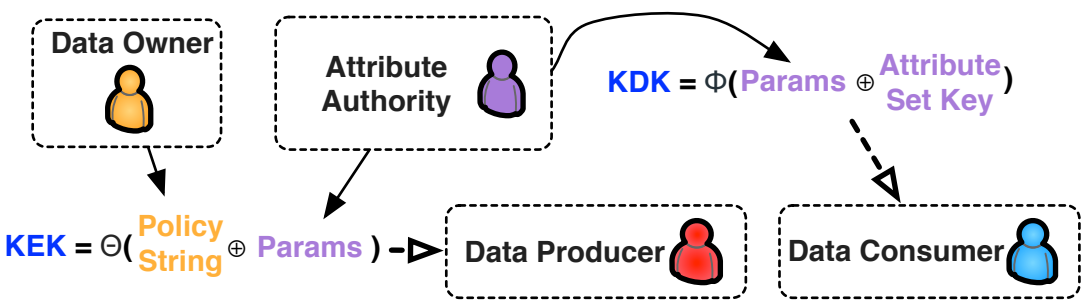
KDK Data Name

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

<CredPrefix> Credentials inferred from content name prefix

<ConsName> Identity name from consumer's own certificate

Attribute-based Encryption Extensions (NAC-ABE)



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

- Data owners define data access attributes
- Consumers obtain sets of attributes as decryption keys from the attribute authority after a vetting process

NAC is a general framework for user-friendly data confidentiality and access control management

Distributed Analytics and Information Science International Technology Alliance
Annual Fall Meeting, September 2017