# Toward Content-Centric Privacy in ICN: Attribute-based Encryption and Routing

Mihaela Ion
University of Trento/CREATE-NET
Via Alla Cascata 56D
Trento, Italy 38123
mihaela.ion2005@gmail.com

Jianqing Zhang
Intel Labs
3600 Juliette Lane
Santa Clara, CA, USA 95054
jianqing.zhang@intel.com

Eve M. Schooler
Intel Labs
3600 Juliette Lane
Santa Clara, CA, USA 95054
eve.m.schooler@intel.com

## ABSTRACT
We design a content-centric privacy scheme for Information-Centric Networking (ICN). We enhance ICN's ability to support data confidentiality by introducing attribute-based encryption into ICN and making it specific to the data attributes. Our approach is unusual in that it preserves ICN's goal to decouple publishers and subscribers for greater data accessibility, scalable multiparty communication and efficient data distribution. Inspired by application-layer publish-subscribe, we enable fine-grained access control with more expressive policies. Moreover, we propose an attribute-based routing scheme that offers interest confidentiality. A prototype system is implemented based on CCNx, a popular open source version of ICN, to showcase privacy preservation in Smart Neighborhood and Smart City applications.

## Categories and Subject Descriptors
C.2.1 [**Computer-Communications Networks**]: Network Architecture and Design

## General Terms
Design, Security

## Keywords
ICN, Security, Privacy, Attribute-based Encryption

## 1. INFORMATION CENTRIC NETWORKS
With the predominant usage of the Internet having shifted toward the distribution of content, many efforts are underway to rethink how content should be distributed and stored in the Internet. One promising approach is Information Centric Networking (ICN), a candidate next generation Internet architecture [1]. Increasingly, content dissemination is to multiple recipients versus part of a point-to-point interaction, and requestors care less about the original address of the data source and more about if the data simply can be found somewhere in the network.

Key features of ICN include name-based routing, general purpose distributed caching in the network and self-securing data. These characteristics are appealing to the future Internet of Things, with application to Smart Homes, Neighborhoods and Cities, where devices are increasingly mobile, intermittently connected and/or in sleep mode, because data remains accessible regardless of the circumstances of the original data source. In addition, ICN focuses on securing the data rather than the communication channels. It aims to provide content-based security from the time of data creation and to embed security into each data unit, making the data security self-contained.


*ICN'13,* August 12, 2013, Hong Kong, China.
ACM 978-1-4503-2179-2/13/08.

## 2. CHALLENGE: CONFIDENTIALITY
Most existing ICN implementations ensure data integrity (data has not been tampered with) as well as authentication (data is from who it says it is from) by signing data at creation [1]. However, confidentiality (the desire to keep data private among those authorized) is often addressed by symmetric encryption [2, 3] or not supported at all. We argue that such approaches do not align completely with ICN's content-centric principles, nor ICN's philosophy to decouple publishers and subscribers of data.

One challenge with confidentiality is how to present and enforce access control policies, which are usually enforced by a trusted third party or by the data owner. Yet in ICN, data is likely replicated and disseminated in the network, making it difficult for the owner to continue to control the data. Another challenge is how to reduce the burden of key management. Security solutions using symmetric-key encryption [2, 3] solutions require publishers and subscribers to share secrets, which tightly couples publishers and subscribers, making the solutions impractical for large-scale deployments, with large numbers of devices and high group dynamics.

## 3. CONTENT-BASED CONFIDENTIALITY
To address these challenges, our research enhances the way ICN describes, encrypts and routes information, drawing inspiration from application-layer publish-subscribe. The basic ideas are (1) attach access control policies to the data itself, (2) enforce the policies in a distributed manner upon delivery and (3) specify policies in terms of the content.

### 3.1 Of Naming, Attributes, Subscriptions
We enrich ICN with a pub-sub layer that is based on attributes rather than strictly names. As a result, users are able to express more complex Interests, by combining ICN names with Boolean expressions of constraints on attribute values and meta-data. This enhancement enables the network to filter undesired content at the earliest vs. latest point of delivery. Figure 1 and Table 1 illustrate the construction of subscriptions based on names vs. attributes.

### 3.2 Attribute-based Encryption
We introduce Attribute-based Encryption (ABE) into ICN, because of its many advantages over symmetric key encryption. Senders and receivers do not need to share secret keys, thus meeting an ICN objective to decouple senders and receivers and simplifying key management for large-scale dynamic applications though a Key Authority is needed. With ABE, a receiver can

decrypt data only if its decryption key satisfies the access control policies embedded in the cipher-text or the key itself. Thus, the policies are enforced by the data and the keys without requiring a third party to enforce them on data delivery. Because keys are generated by data or receivers' attributes, ABE allows the definition of highly flexible, fine-grained access control policies.

**Table 1. Name-based vs. Attribute-based Subscriptions.**

| Subscription | Name-based | Attribute-based |
|---|---|---|
| All Trento data | $T_4$, $T_6$, $T_7$ | Trento |
| All Trento temperature since 2008 | $T_4$ (super-set) | Temperature and Trento and Year > 2008 |
| All Trento air quality with Air Quality Index (AQI) > 50 | $T_7$ (super-set) | Air Quality Index and Trento and AQI > 50 |

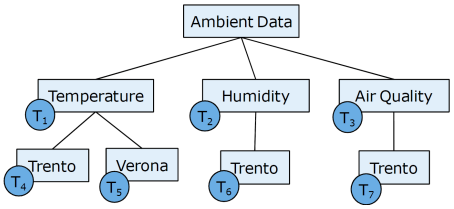


**Figure 1. Hierarchical Subscriptions.**

We leverage two types of ABE: Key-Policy (KP-ABE) [4] and Ciphertext-Policy (CP-ABE) [5]. In KP-ABE, the sender encrypts data using an encryption key, which is derived from the attributes of the data, and the access policy is embedded in the decryption key. A Key Authority issues receivers the decryption keys that describe what they can read (e.g., temperature data between certain dates). In CP-ABE, attributes are used to describe receivers and the policy is attached to the cipher-text. The sender defines the policy (e.g., only the utility company can read the data). In this case, a Key Authority issues each receiver a key that is derived from the receiver's attributes.

## 3.3 Integration with CCNx

CCNx [2], a popular open source ICN variant, has two main message types: *Interest* messages are used to request data by name and *Content* are used to supply data in response to a matching Interest. We employ the Java interface of CCNx to read/write messages encrypted by KP-ABE or CP-ABE. Figure 2 shows the architecture of the KP-ABE implementation over CCNx. We validate our approach by implementing privacy-preserving applications that collect EV charging information across homes in the Smart Neighborhood and environmental sensor data in the Smart City. We demonstrate the re-usability of our middleware-agnostic security and privacy library through its integration with multiple pub-sub systems (CCNx and PADRES[7]).

## 3.4 Attribute-based Routing

Because ICN's name-based routing can be too restrictive at times, we create a Broker to work alongside of CCNx to enable attribute-based routing, which allows expressing constraints on the attributes of the data and restricts the forwarding of data that does not match the constraints.

Because subscriptions can reveal user's privacy (personal preferences or interests), we encrypt the attribute constraints in subscriptions as in [7] using Searchable Data Encryption (SDE) [6]. SDE leverages a proxy server and does not require publishers and subscribers to share keys, and thus maintains the decoupling of them. We re-use our attribute-based routing Broker as the proxy server to verify if a particular filter, which is encrypted by one user, is matched to a request from another user by a computation trapdoor without leaking the filter keywords.

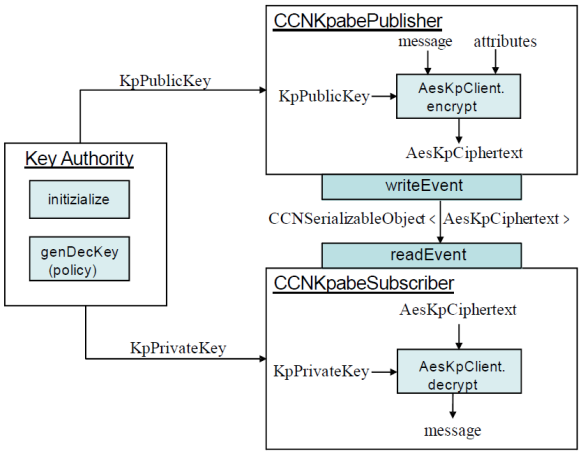


**Figure 2. KP-ABE over CCNx.**

# 4. CONTRIBUTIONS

We make several contributions to the way ICN describes, encrypts and routes information. An ABE and SDE based encryption scheme is proposed for content-centric data privacy in ICN with fine-grained access control policies. The scheme supports large-scale applications by decoupling publishers and subscribers with no need to share keys. We enrich ICN with a pub-sub routing scheme that uses expressive subscription filters based on attributes constraints. We preserve users' privacy by encrypting subscription interests while still allowing routers to forward encrypted data to subscribers. Finally, we implement a middleware-agnostic library to support CCNx, as well as other pub-sub systems.

# 5. REFERENCES


[1] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman. A Survey of Information-Centric Networking. *IEEE Communications Magazine* 50(7):26-36, July 2012.

[2] Palo Alto Research Center (PARC). Content Centric Networking (CCNx). https://www.ccnx.org/.

[3] J. Zhang, Q. Li, and E. M. Schooler. iHEMS: An Information-Centric Approach to Secure Home Energy Management. In *3rd IEEE Conf. SmartGridComm,* Nov 2012.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *The 13th ACM Conf. CCS,* Oct 2006.

[5] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy*, pp. 321-334, 2007.

[6] C. Dong, G. Russello, and N. Dulay. Shared and Searchable Encrypted Data for Untrusted Servers. *Journal Computer Security*, 19(3):367-397, 2011.

[7] M. Ion, G. Russello, and B. Crispo. Design and Implementation of a Confidentiliaty and Access Control Solution for Publish/Subscribe Systems. Computer Network, 56(7):2014-2037, May 2012.