Attribute-Based Encryption on a Resource Constrained Sensor in an Information-Centric Network

Adeel Mohammad Malik
Ericsson
adeel.mohammad.malik@ericsson.com

Joakim Borgh
Ericsson
joakim.borgh@ericsson.com

Börje Ohlman
Ericsson
borje.ohlman@ericsson.com

ABSTRACT

The Information-Centric Networking (ICN) paradigm is drastically different from traditional host-centric IP networking. As a consequence of the disparity between the two, the security models are also very different. The security model for IP is based on securing the end-to-end communication link between the communicating nodes whereas the ICN security model is based on securing data objects often termed as Object Security. Just like the traditional security model, Object security also poses a challenge of key management. This is especially concerning for ICN as data cached in its encrypted form should be usable by several different users. Attribute-Based Encryption (ABE) alleviates this problem by enabling data to be encrypted under a policy that suits several different types of users. Users with different sets of attributes can potentially decrypt the data hence eliminating the need to encrypt the data separately for each type of user. ABE is a more processing intensive task compared to traditional public key encryption methods hence posing a challenge for resource constrained environments with devices that have low memory and battery power. In this demo we show ABE encryption carried out on a resource constrained sensor platform. Encrypted data is transported over an ICN network and is decrypted only by clients that have the correct set of attributes.

Keywords

Attribute-Based Encryption (ABE), Information-Centric Network (ICN), Content-Centric Network (CCN), Internet-of-Things (IoT), Sensor Networks, RIOT OS, CCN-lite

1. INTRODUCTION

The Internet-of-Things (IoT) is a fast evolving trend with the total number of connected devices expected to be around 16 billion by 2021 [1]. The IoT is expected to have a huge impact in the Information and Communication Technology (ICT) arena giving birth to new technology and business opportunities such as smart cities, smart buildings, industry automation, autonomous cars etc. IoT devices are usually resource constrained for practical reasons such as limiting the energy consumption to have increased battery lifetime and limiting the size of the device for easy installation.

Emerging technology trends such as the IoT also inspire the need for more efficient networks that can deliver content faster with minimal overhead while at the same time ensuring foolproof data security. Information-Centric Networking (ICN) is a new networking paradigm where the communication is based on named content unlike traditional host-centric IP networking where it is based on named hosts. Amongst the many features that ICN offers, ubiquitous caching is one. Though caching is a widely used concept in traditional host-centric networks, it becomes even more relevant in ICN where content is treated as a primitive. Every node in an ICN network is a potential cache that serves cached data objects to several users.

To conserve energy on resource constrained IoT devices, data produced by them is typically cached in networks they are attached to. If the same data is requested more than once it can be served from the caches hence eliminating the need for the sensor to retransmit the data. ICN complements this very well with ubiquitous caching. However, in ICN nodes in the network are not trusted and therefore sensitive data needs to be protected before it can be cached in the network. Traditional encryption schemes secure a communication link end-to-end hence encrypting data for a specific user. This undermines the usefulness of ICN where a cached copy of an encrypted data object should be usable by several different users.

Attribute-Based Encryption (ABE) alleviates the problem described above by allowing data to be encrypted for several different types of users without knowing their exact identity. The encryptor uses descriptive attributes to specify who can access the data. With ABE a data object is encrypted only once regardless of the number of recipients. Cached copies of this encrypted data object are therefore usable by several users. The associated tradeoff of this is computational efficiency. ABE is processing intensive and hence a challenge to interwork with resource constrained IoT devices.

2. BACKGROUND

ABE is a form of public-key encryption where data is described with attributes as meta-data. The attributes decide how the data is encrypted and only the entities with the corresponding keys should be able to access the content. There are two types of ABE: Key-Policy ABE (KP-ABE) [2] and Ciphertext-Policy ABE (CP-ABE) [3]. In this demo we will use CP-ABE. In CP-ABE the users in the system have keys which are a collection of attributes typically describing the user. The ciphertext, the encrypted data, is associated with an access policy based upon such attributes. A user can decrypt the encrypted data if the attributes of the user's private key satisfies the access policy specified in the ciphertext.

The collections of attributes which constitutes the private keys are distributed to the users by a trusted third party called an authority. This authority can decrypt all the data objects in the system as it can generate any private key. In an attempt to circumvent this researchers have proposed multi-authority (MA) ABE systems [4,

ICN'16 September 26-28, 2016, Kyoto, Japan

ACM ISBN 978-1-4503-4467-8/16/09.

DOI: http://dx.doi.org/10.1145/2984356.2985229

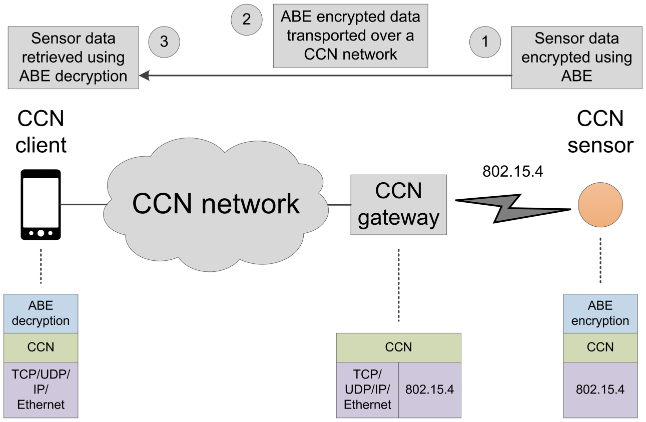

Figure 1: Demo setup

5]. In such systems the trust is distributed among the authorities and a single authority can not compromise the entire system. The encryption and decryption operations of ABE scale linearly with the number of attributes there are in the policy. An important property of ABE systems is collusion resistance. This means that two users which can not individually decrypt an object, should not be able to decrypt it if they collude.

ABE offers expressive access control on the expense of computational efficiency. The operations of ABE are substantially more expensive than traditional public key encryption operations such as RSA. This is not an issue for workstations or even smart phones [6] (depending on security strength and complexity of policy), but when considering resource constrained devices such as sensors this becomes a problem.

3. DEMO DESCRIPTION

The demo highlights two main features, ABE encryption on sensor devices and transport of sensor data over an ICN network, in this case CCN. Using ABE over ICN makes our system agnostic to the lower layers in the stack as there is no need to establish a secure end-to-end connection such as TLS. In addition the store-and-forward characteristics of ICN make it possible to support Delay Tolerant Networking (DTN) scenarios where it might never be possible to establish an end-to-end connection between the sensor and the client.

Figure 1 shows the demo setup that includes a CCN client, some nodes forming the CCN network, a CCN gateway and a CCN sensor. The CCN sensor will encrypt data using ABE and send it towards the CCN network. Between the gateway and the sensor CCN runs directly over 802.15.4 radio. CCN faces are defined using the next hop 802.15.4 MAC address (64 bit). Running CCN directly over 802.15.4 link layer saves RAM/Flash capacity on the constrained sensor which can instead be used for more sophisticated ABE policies to encrypt data on the sensor.

Between the client and the gateway, CCN can run either on TCP/UDP/IP over Ethernet or directly over Ethernet. In the former case the CCN faces are defined using the next hop IP address and the TCP/UDP port number. In the latter case the CCN faces are defined using the Ethernet MAC address and the Ethertype. CCN faces and routes are statically configured in all the nodes.

At the sensor data is encrypted using different ABE policies. The client application offers a way to generate keys that correspond to a particular set of ABE attributes. Using the right set of ABE attributes the user can decrypt the sensor data. In order to demonstrate the ABE concept the client application offers a way to generate keys locally to decrypt the data. However, in a real world scenario these keys will be generated by an authority responsible for its respective attributes. The demo also shows Multiple Authority-ABE (MA-ABE) which is briefly mentioned in section 2.

The hardware platform used for the sensor and the gateway is the STM32F4DISCOVERY board that has a STM32F407 MCU featuring an ARM Cortex-M4 32-bit core, 1 MB Flash memory and 192 KB RAM. The STM32F4DISCOVERY board is connected to the Atmel AT86RF233 802.15.4 radio transceiver. The sensor and the gateway run the RIOT OS [7] and its CCN-lite [8] port. The CCN network and the client use the vanilla version of CCN-lite.

4. DISCUSSION & FUTURE WORK

With this demo we show that ABE can be carried out on a resource constrained device such as a sensor. The processing load increases linearly with the increasing number of attributes in the policy. Running ABE on a resource constrained device under a larger and more complex policy can be a challenge.

The security level employed also affects the overall processing load of ABE. In the current implementation we use a security level of 128 bits. Lowering the security level reduces the encryption time and the needed memory resources, essentially making larger policies viable. Using the right level of security for an application is important to ensure that the encryption is foolproof and also that there is significant leeway to design a suitable policy.

The implementation for this demo is not exhaustively optimized in terms of RAM usage. This applies to both the CCN stack running on the sensor platform and the ABE encryption code. The CCN stack uses malloc() calls predominantly which use up space in the very limited amount of RAM on the sensor platform. The current implementation supports only a handful of attributes in each policy. With some effort on code optimizations we expect that even larger policies will be possible to support.

To draw further conclusions on the feasibility of ABE on battery-powered resource constrained devices it is critical to take into account the energy consumption of ABE. Therefore in the future we would like to perform experiments of the energy consumption of ABE encryption on the sensors.

5. REFERENCES

[1] *Ericsson Mobility Report*, June 2016.

[2] V. Goyal, O. Pandey, A. Sahai, B. Waters, *Attribute Based Encryption for Fine-Grained Access Control of Encrypted Data*, In ACM conference on Computer and Communications Security (ACM CCS), 2006.

[3] J. Bethencourt, A. Sahai, B. Waters, *Ciphertext-Policy Attribute-Based Encryption*, In: IEEE Symposium on Security and Privacy, pp. 321-334 (2007).

[4] M. Chase, S.M. Chow, *Improving privacy and security in multi-authority attribute-based encryption*, ACM conference on Computer and communications security (CCS 2009), pp. 121–130. ACM, New York (2009).

[5] A. Lewko, B. Waters, *Decentralizing Attribute-Based Encryption*, Cryptology ePrint Archive Report 2010/351 (2010), http://eprint.iacr.org/

[6] M. Ambrosin, M. Conti, T. Dargahi, *On the Feasibility of Attribute-Based Encryption on Smartphone Devices*, arXiv:1504.00619

[7] *RIOT OS for the Internet-of-Things*, https://www.riot-os.org/

[8] *CCN-lite: Lightweight implementation of the CCNx protocol of XEROX PARC*, http://www.ccn-lite.net/