Thesis topic: Attribute based encryption for information centric networking

Background
With the predominant usage of the Internet having shifted toward the distribution of content. New Internet architecture designs are underway to rethink how content should be distributed and stored in the Internet. One promising approach is Information Centric Networking (ICN), a candidate of next generation Internet architecture. The main idea of ICN is to supports content-based data dissemination through in-network caching and interested based content retrieval. Data objects can be cached in ICN routers, so that the requests can necessarily obtain the data from the original sources. This architecture design is different from traditional host-based end-to-end communication. It is more scalable and efficient in the distribution of data objects.

Description
ICN decouples data from the source and allows data objects to be stored anywhere. This in-network caching property can reduce network traffic load and data delay. Since the data objects can be obtained anywhere, enforcing access control of the data objects in the network is a challenge. We will explore access control scheme for ICN in this thesis project. One interesting problem with confidentiality is on how to present and enforce access control policies. Confidentiality is usually addressed by a trusted third party or by the data owner in traditional Internet architecture. Yet in ICN, data is likely replicated and disseminated in the network, making it difficult for the owner to continue to control the data.

To address this challenge, a new idea has come up which suggests attaching access control policies to the data content itself. The advantage of specifying policies in terms of data content enables the policies to be enforced in a distributed manner upon delivery. Attribute-based Encryption (ABE) has recently been suggested for providing data object security in ICN. With ABE, 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. 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. Since keys are generated by data or receivers’ attributes, ABE allows the definition of highly flexible, fine-grained access control policies. However, the research is still in its early stage. Many open questions remain to be discussed and further investigated.
The main goal of this thesis work is to gain better understanding of how ABE can provide access control in ICN network. We will also compare different ABE schemes with other access control mechanisms. The work will be carried in a number of phases.

1. Perform a literature study to find out the state of the art for access control in ICN.
2. Select appropriate cryptographic algorithms and implement ABE for ICN.
3. Study if it is necessary to have an authority server with ABE and explore the possibility of a distributed approach
4. Evaluate the computation and communication overhead of ABE for ICN, and compare with other access control mechanism (encryption based or interest-based, etc.).
5. Investigate how revocation can be performed in ABE for ICN and study other possible extensions.

**Description of the work**

- Preparations and reading: information centric networking (ICN), attribute based encryption (ABE)
- Investigation of which cryptographic algorithm to be used and possibility of a distributed ABE implementation
- Evaluate the performance of the implemented ABE mechanism for ICN by experiments and compare with other approaches
- Performance and security analysis on ABE for ICN
- Report writing
- Code documentation and packaging

**Qualifications**

You should be self-motivated and used to working with others in project teams. The positions also require you to be fluent in English, both written and spoken. In return, you will get to perform you thesis work with cutting-edge technology in a stimulating learning environment with a friendly atmosphere.

You should have good programming skills. Likely programming environment include Linux, C, etc.

The Thesis is for a Master of Science Degree in Electrical Engineering, Computer Science or equivalent.
Contact Information

Edith Ngai
+46 70 167 9160

Börje Ohlman
+46 10 717 8095

Schedule  Full-time
Number of Openings  1

Company Description:
Ericsson is shaping the future of mobile communications and broadband Internet, providing innovative solutions in over 140 countries. More than half of Ericsson's employees worldwide are university graduates and over a quarter of our research staff have technology PhDs.

Ericsson Research provides Ericsson with system concepts, technology and methodology, to secure long term competitive product provisioning. World-class innovation is achieved through cooperation within Ericsson and with partners, customers, universities and research institutes.

Our research branch is working with the latest technology in network caching, network features, security and advanced multimedia delivery. We are regularly offering interesting master or diploma thesis and internships. Together with our research staff, you will have the opportunity to work on the exciting future of computer systems and communications technologies.