On the Secure Distribution of Information in Health Care Context

Zoltán Csajbók, University of Debrecen

The security of health care information systems, in the most general meaning, has a large number of aspects. See its short but exhaustive discussion, e.g., in [5]. This talk, however, is only about the secure communication in hospital environment, in other words, roughly speaking, it is only about the encryption in hospital information systems.

Hospital information systems have several very special properties, such as [2], [3]:

- Confidential message might be sent without knowing a priori who the final receiver is. In addition, in the real-life practice, if the receiver is known his/her public ID might not be known for sure, although it would be needed immediately.
- A hospital information system has to work *in extreme dynamic contexts*, where people's roles and rights change frequently.
- The system has to allow users to flexibly specify policies to constrain the disclosure of the confidential information but *these policies have to be controlled by medical protocols*.
- From the previous considerations it follows that the generation of a *decryption key has to be postponed in time*, i.e., it has to be generated after the correspondent encryption key was created.

These properties have strong implications on how a hospital information system has to support the late-binding mechanism for roles and even for health care professionals. The Identity Based Cryptography (IBC) [1] is really good for realizing an information system with the late-binding mechanism and it can be flexibly used *to adjust cryptographic schemes to functional requirements*.

It seems, in a more general context, the cryptographic primitives of the IBC are such strong means that they can provide the possibility to change the paradigm in the cryptography. We think of the change from the 'technology-driven' approach to the 'applications-driven' approach.

Applications-driven approach means that we can develop information systems and cryptographic schemes at the same time and the cryptographic schemes are able to fit with the requirements of the information system.

In our talk we show a cryptographic scheme in health care context based on disclosure policy which is given in the terms of a logical formula [6] and the attribute based authorization control [4]. Referring to the former discussion, it is not a general scheme but it is built from strong cryptographic primitives to satisfy the required considerations of the secure communication within hospital information systems.

References

[1] D. Boneh, M. Franklin, *Identity-Based Encryption from the Weil Pairing*, Proceedings of CRYPTO 2001, LNCS 2139, pages 213-229, Springer-Verlag, 2001.

[2] M. Casassa Mont, P. Bramhall, and C. R. Dalton, *A Flexible Role-based Secure Messaging Service: Exploiting IBE Technology in a Health Care Trial*, HP Laboratories Bristol, HPL-2003-21, 2003

[3] M. Casassa Mont, P. Bramhall, *IBE Applied to Privacy and Identity Management*, HP Laboratories Bristol, HPL-2003-1001, 2003

[4] G. Inman, D. W. Chadwick, and N. Klingenstein, *Authorisation using attribute from multiple authorities - a study of requirements*. In Proceedings of HCSIT Summit - ePortfolio International Conference, Maastricht, The Netherlands, October 2007.

[5] D. Mundy, D. W. Chadwick, *Secure knowledge management*, In J.N.D.Gupta & S.K.Sharma. Wickramasinghe, editor, Creating Knowledge Based Health Care Organizations, pages 321-337. Idea Publishing Group, February 2004.

[6] N. P. Smart, *Access Control Using Pairing Based Cryptography*. In M. Joyce (Ed.): CT RSA 2003, LNCS 2612, pp. 111-121, 2003. Springer-Verlag Berlin Heidelberg 2003.