Accepted Manuscript

Attribute-based handshake protocol for mobile healthcare social networks

Yi Liu, Hao Wang, Tong Li, Ping Li, Jie Ling

PII: S0167-739X(16)30749-X
DOI: http://dx.doi.org/10.1016/j.future.2016.12.010
Reference: FUTURE 3251

To appear in: *Future Generation Computer Systems*

Received date: 15 September 2016
Revised date: 6 December 2016
Accepted date: 8 December 2016

Please cite this article as: Y. Liu, H. Wang, T. Li, P. Li, J. Ling, Attribute-based handshake protocol for mobile healthcare social networks, *Future Generation Computer Systems* (2016), http://dx.doi.org/10.1016/j.future.2016.12.010

Attribute-based Handshake Protocol for Mobile Healthcare Social Networks

Yi Liu[a], Hao Wang*[b], Tong Li[c], Ping Li[d], Jie Ling[a]

[a]*School of Computer Science and Technology, Guangdong University of Technology, Guangzhou, China*
[b]*School of Information Science and Engineering, Shandong Normal University, Jinan, China*
[c]*College of Computer and Control Engineering, Nankai University, Tianjin, China*
[d]*School of Computer Science, Guangzhou University, Guangzhou, China*

Abstract

In this paper, we study the privacy protection problem of handshake protocol for mobile healthcare social network, and introduce the concept of attribute-based handshake (ABH) protocol. Using ABH, users in mobile healthcare social network can make a handshake to authenticate each other and obtain a common session key without exposing their privacy when their attributes meet the social needs of each other. Then, we provide the formal definition and security model of ABH protocol with a specific construction proving its security in the standard model. Finally, we introduce how to deploy our ABH protocol in the mobile healthcare social network.

Keywords: attribute-based, handshake protocol, mobile social network, healthcare

1. Introduction

With the rapid development of mobile Internet industry, people pay more and more attention to that the Internet brings them. Especially with the emergence and spread of the mobile social network and intelligent mobile phones, it has attracted numerous groups to use mobile social network to carry on the various social activities. Mobile social network (MSN) is social network where individuals with similar interests converse and connect with one another through their mobile phone and/or tablet. Much like web-based social network, mobile social network occurs in virtual communities. A current trend for social network websites, such as Facebook, is to create mobile apps to give their users instant and real-time access from their device. In turn, native mobile social networks have been created