Journal of Network and Computer Applications 34 (2011) 1131–1137

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

An efficient anonymous authentication protocol for mobile pay-TV

Tien-Ho Chen *, Yen-Chiu Chen, Wei-Kuan Shih, Hsin-Wen Wei

Department of Computer Science, National Tsing Hua University, No. 101, Kuang Fu Road, Section 2, 300 HsingChu, Taiwan, ROC

ARTICLE INFO

Article history:
Received 31 May 2010
Received in revised form
23 September 2010
Accepted 18 November 2010
Available online 26 November 2010

Keywords:
Mobile pay-TV
Authentication
ECC
Smart card
Dynamic ID
STB

ABSTRACT

In terms of convenience requirements, mobility has been one of the most important services for pay-TV systems. In 2009, Yang and Chang proposed an authentication protocol for mobile devices using elliptic curves cryptography (ECC) and claimed that their mechanism is secure and efficient using in mobile pay-TV systems. In this paper, we demonstrate that their protocol still is insecure for authentication without password protection and performs inefficiently. Therefore, we offer an anonymous authentication protocol (AAP) to solve the performance issue and insecure risks. In addition, we present an analysis of our protocol to show that our protocol suits better for applications with higher security requirements and low power-consuming devices.

1. Introduction

With the integration of wireless communication and pay-TV, mobile broadcast TV technologies have advanced noticeably in recent years (Allamandri et al., 2007; ETSI, 2004, 2005; Fabio et al., 2007; Faria et al., 2006; Gallery and Tomlinson, 2005; Gardikis et al., 2008; Kornfeld and May, 2007; Lee et al., 2000; Ollikainen, 2006; Song and Korba, 2003; Sun and Leu, 2009). Especially, how to promise authorized subscribers a secure access and keep unauthorized subscribers from illegitimate accesses in mobile broadcast TV services has become an important issue. Typically, Conditional Access System (CAS) supports this mechanism. There are two main parts in CAS: (1) head end system (HES) and (2) numerous receivers. The structure of CAS is shown in Fig. 1 and the statements are described as follows:

- *Head end system* (*HES*): HES is a system sending broadcast TV services to receivers.
- *Receiver*: A receiver is a subscriber device with a CAS module used for access control.
- *SAS/SMS*: Subscriber Authorization System and Subscriber Management System are subsystems responsible for subscriber authorization and management; its works include key management, user authentication, entitlement messages delivery, subscriber information management and rights management.
- *Encrypter/decrypter*: Encrypter is a component for enciphering Control Word (CW), keys, or sensitive information, and Decrypter employs the reverse engineering of encrypter.
- *Multiplexer (MUX)/Demultiplexer (DEMUX)*: MUX is a component for multiplexing A/V, data or IP into MPEG-2 transport stream, and DEMUX employs the reverse engineering of MUX.
- *Scrambler/Descrambler*: Scrambler is a component for signal scrambling, and descrambler employs the reverse engineering of Scrambler.
- *Transmitter (TX)/Receiving module (RX):* TX is a subsystem for signal transmission, and RX is a subsystem for signal receiving.
- *ECM/EMM*: ECM and EMM are defined by DVB (ETSI, 2004) as two conditional access messages, namely Entitlement Control Message (ECM) and Entitlement Management Message.

Pay-TV systems supply receivers with many different services. The CAS generally performs these services in two modes, namely broadcast and interactive mode. In the broadcast mode, A HES broadcasts the service messages via a SAS/SMS, Encrypter, MUX, Scrambler and Transmitter to subscriber devices periodically, and the receiver listens to the messages constantly. In the interactive mode, a subscriber's receiver must be authenticated first to obtain the entitlement service. While he/she wants to obtain a service, his/her device sends a subscription and authentication messages to a HES. After the authentication and subscription being validated, HES delivers the service messages which include rights codes and authentication messages via a SAS/SMS, Encrypter, MUX, Scrambler and Transmitter to this subscriber device. Then, the subscriber can use his/her private key, authentication key and entitlement data to obtain the service.

* Corresponding author. Tel.: +886 35715131x42808; fax: +886 35723694.
E-mail addresses: riverchen@rtlab.cs.nthu.edu.tw (T.-H. Chen), ycchen@rtlab.cs.nthu.edu.tw (Y.-C. Chen), wshih@rtlab.cs.nthu.edu.tw (W.-K. Shih), hwwei@iis.sincia.edu.tw (H.-W. Wei).

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.11.005