On the Security of a Pay-TV Scheme of ICON 2001

Antionette W.-T. Goh\(^1\)  Rafael C.-W. Phan  Lawan A. Mohammed
Information Security Research (iSECURES) Lab  Swinburne University of Technology (Sarawak Campus)
Kuching, Malaysia

\texttt{tinette\_goh@yahoo.com}  \texttt{rphan\@swinburne.edu.my}  \texttt{lmohammed\@swinburne.edu.my}

Abstract — In this paper\(^2\), the security of a conditional access system (CAS) for digital television proposed at ICON 2001 is studied. The authors claim to have designed a scrambling and key distribution scheme that is able to thwart attackers from practicing smart card cloning and also the McCormac Hack. However, we show that the key distribution scheme is particularly insecure, hence allowing as much as three attacks to be carried out. Our attacks allow unauthorized access to Pay-TV systems by bypassing certain operations in the authentication scheme carried out between the decoder box and the smart card. We further suggest countermeasures to secure the CAS against our attacks.

Keywords: Conditional access system (CAS), scrambling, key distribution, smart card, decoder box.

1 Introduction

In Pay-TV systems, the service provided relies much on the operation of the Conditional Access System (CAS) [2], which uses scrambling [also called encryption] as a security measure. This is to prevent viewers from accessing unauthorized video streams or more simply put, viewing transmissions they have not paid for.

At the IEEE International Conference on Networks (ICON) 2001 [3], Kanjunarin and Amnouraksa outlined a scrambling scheme for digital video information, and a scrambling key distribution scheme. Firstly, the scheme proposes a block encryption method for digital video scrambling. Secondly, it proposes a reliable key distribution scheme that is claimed to detect any possible fraud in the decoder box, thus also claiming to eliminate the occurrence of smart card cloning and the McCormac Hack [3]. The key extraction component of this key distribution scheme is built into the decoder box and allows the decoder to authenticate the smart card and decoder box to receive the proper scrambling key to descramble any scrambled video stream.

However, we show that the key distribution scheme fails to ensure full security. In particular, we show that an attacker can actually tap off valuable information generated in a smart card, allowing him to use a cloned smart card with any intended decoder box, even when the key distribution scheme and authentication scheme is fully operating in the decoder box. We present three attacks which will be further discussed in this paper. Our results will show that the CAS system proposed is susceptible to smart card cloning and the McCormac Hack, contrary to its designers’ claims. We also further suggest countermeasures to secure the CAS against our attacks.

2 Conditional Access System (CAS)

The CAS scheme for Pay-TVs proposed in [3] is divided in two parts: scrambling scheme for digital video streams and key distribution scheme. The scrambling scheme only requires a certain portion of the entire video stream to be encrypted, in an effort to reduce processing time. Meanwhile, the key distribution scheme provides the descrambling key and other descrambling parameters to the decoder box and smart card. All descrambling parameters are hidden in the broadcast message (\(X\)) to the subscriber.

2.1 Scrambling scheme

The scrambling scheme consists of three major stages: separation of bit streams, masking and encryption.

The video stream is first separated into \(n\) fixed size blocks before they are put through a six-step masking process, which is unkeyed and hence does not really contribute to its security.

\(1\) The first author acknowledges the Swinburne Sarawak internal grant.
\(2\) A preliminary version of this work was presented as a poster at the ICCSA 2005 conference and an abstract was included in its proceedings [1].