An Efficient Monitoring Method of a Network Protocol for Downloadable CAS

*Youngho Jeong *Ohyung Kwon *Chunghyun Ahn *Jinwoo Hong

*Electronics and Telecommunications Research Institute

*yhcheong@etri.re.kr

Abstract

This paper presents an efficient monitoring method of a network protocol for a downloadable conditional access system (DCAS) that can securely transmit conditional access software via a bi-directional communication channel. In order to guarantee a secure channel based on mutual authentication between a DCAS head end server and set-top boxes, DCAS messages are encrypted and digitally signed. Owing to applied cryptographic algorithms, it is impossible to get information from messages directly without additional processing. Through categorizing DCAS messages into several groups, the proposed monitoring method can efficiently parse and trace DCAS messages in real-time. In order to verify the stability and effectiveness of the proposed monitoring method, we implement a DCAS monitoring system capable of capturing and parsing all DCAS messages. The experimental results show that the proposed monitoring method is well designed.

1. Introudction

In order to solve the existing problems of an embedded conditional access system (CAS) and CableCARDs, a study of a downloadable conditional access system (DCAS) began in the Next-Generation Network Architecture (NGNA) project. DCAS uses a secure microprocessor (SM) soldered onto a circuit board instead of a removable card [1], [2]. Because the downloaded conditional access (CA) software runs on an SM, DCAS is much more cost-effective and easier than the previous CAS solutions for deployment and replacement. DCAS can remove the lock-in issue for CAS or STB vendors, and it is also much more flexible and easier to manage and distribute a CAS module onto an STB.

Among the core technologies in DCAS, a network protocol is very important for guaranteeing system security. To securely download CA software, a network protocol defines a series of messages to be transferred between a DCAS headend and SM. Mutual authentication and encryption key sharing should also be included in a network protocol [3]-[5]. If a DCAS service is launched, service operators need to trace and check message sequences based on the network protocol in order to maintain the stability of the DCAS headend servers and cable network.

However, DCAS messages are encrypted and digitally signed. Owing to the applied cryptographic algorithms for security, it is impossible to receive information from the captured messages directly. Therefore, efficient monitoring of the DCAS network protocol without degrading the original security level is required.

2. DCAS Network Protocol

To mutually authenticate and share an encryption key (EK) for downloading a CA code, the headend and SM conform to a novel DCAS protocol proposed by ETRI, as shown in Fig. 1.

If downloading a CA code is required through parsing a message in an announcement protocol, the SM begins keying the protocol to generate an EK. The SM sends a message to receive the seed value needed to derive the EK in the keying protocol. The authentication proxy (AP) forwards a unique value received from the SM to a trusted authority (TA) that checks if it is a pre-assigned value. If it is validated, the TA sends a seed value for the SM and intermediate values for AP that are needed to generate an EK.

Before the authentication protocol begins, the SM generates an EK using unique values stored in it, along with a seed value received from the TA. Then, the SM sends the message containing additional values used to generate the EK in the AP. Using intermediate values from the TA and additional values from the SM, the AP can also generate an identical EK produced in the SM. Exchanging succeeding messages, the AP and SM each verify the equality of the other's generated EK.

In order to download a CA code, the AP transfers a message containing the download mechanism, download server's IP address, target file name, and so on. Receiving information related to the code download, the SM downloads the CA code and installs it in secure memory according to directives provided by the AP. After downloading and installing the CA code, the SM sends a final message to the AP indicating the download status for the CA code.

The first author, Youngho Jeong, is with the Broadcasting & Telecommunications Convergence Future Technology Research Department, ETRI, Daejeon, Rep. of Korea.

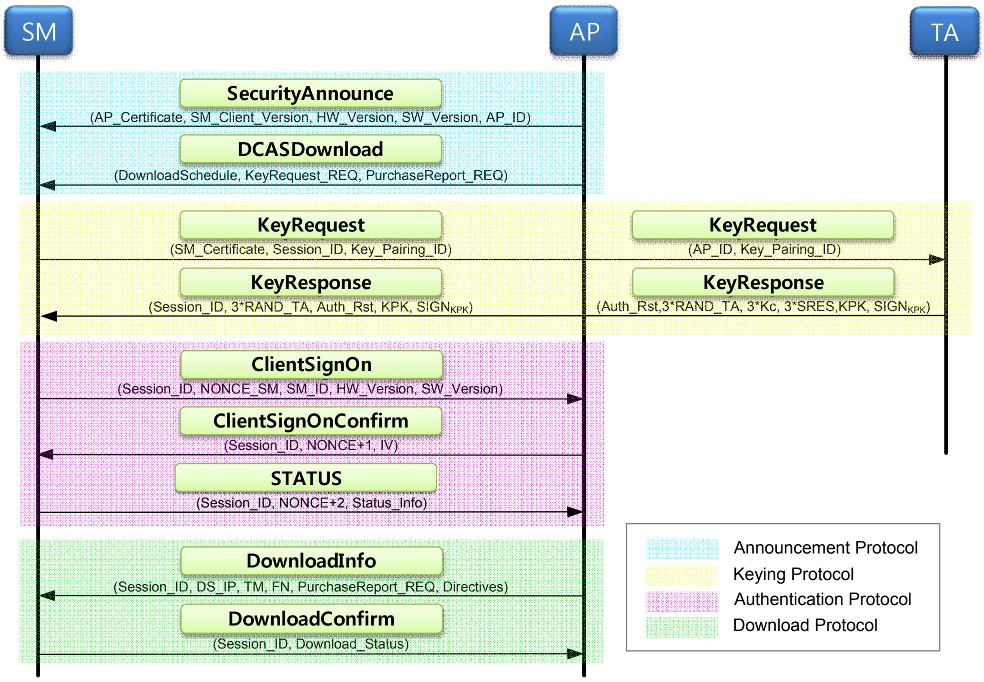
SM
AP
TA
SecurityAnnounce
(AP_Certificate, SM_Client_Version, HW_Version, SW_Version, AP_ID)
DCASDownload
(DownloadSchedule, KeyRequest_REQ, PurchaseReport_REQ)
KeyRequest
(SM_Certificate, Session_ID, Key_Pairing_ID)
KeyRequest
(AP_ID, Key_Pairing_ID)
KeyResponse
(Session_ID, 3*RAND_TA, Auth_Rst, KPK, $SIGN_{KPK}$)
KeyResponse
(Auth_Rst,3*RAND_TA, 3*Kc, 3*SRES,KPK, $SIGN_{KPK}$)
ClientSignOn
(Session_ID, NONCE_SM, SM_ID, HW_Version, SW_Version)
ClientSignOnConfirm
(Session_ID, NONCE+1, IV)
STATUS
(Session_ID, NONCE+2, Status_Info)
DownloadInfo
(Session_ID, DS_IP, TM, FN, PurchaseReport_REQ, Directives)
DownloadConfirm
(Session_ID, Download_Status)
Announcement Protocol
Keying Protocol
Authentication Protocol
Download Protocol

Fig. 1. DCAS network protocol.

3. Proposed Monitoring Method

For monitoring and analyzing the DCAS protocol effectively, we classify DCAS messages into five groups according to their process type as shown in Fig. 2. Message groups (1) and (2) are captured directly in the network and can be parsed as follows. In message group (1), because message contents are not encrypted, they can be parsed after only verifying the digital signature by the public key of the AP. However, messages belonging to message group (2) are required to be decrypted by the private key of the AP. For the private and public keys of the AP, because monitoring and headed systems are operated by an identical service operator, key sharing between two systems is possible.

In message group (3), parsing messages between the AP and TA is impossible as they are encrypted by symmetric keys generated in the transport layer security (TLS) protocol. To solve this, the AP transmits newly constructed messages, encrypted and signed by the sharing keys, to the monitoring system when a message is sent or received between the AP and TA. The message format of the AP for message group (3) is as follows.

- H || E(Pub(AP), M) || S(Prv(AP), M))

M represents the header and message contents transmitted between the AP and TA, which are not encrypted by keys generated in the TLS protocol. H is a newly defined header for transmitting messages from the AP to the monitoring system, and it includes information on the message type, length, and so on. The merit of this message format is to reuse an existing message process module implemented in the AP.

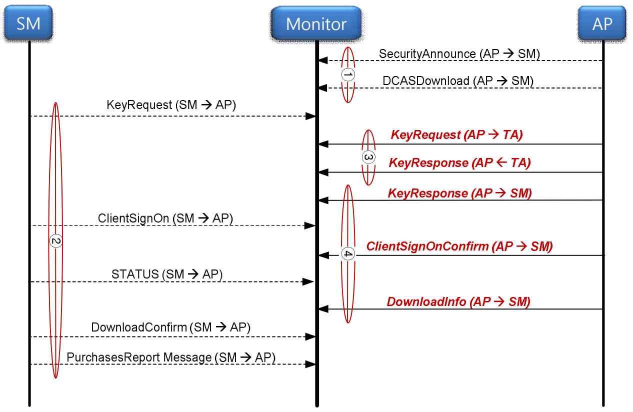

Fig. 2. Message group according to process type.

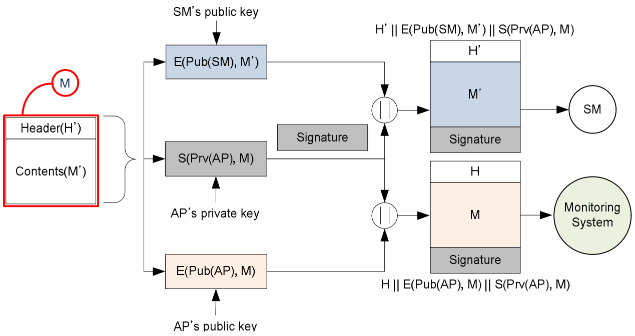

Fig. 3. Message monitoring process in AP.

The private key of the SM is essential to parse messages belonging to message group (4). However, service operators operating a monitoring system cannot obtain the private key of an SM owing to the DCAS design premise for guaranteeing security. This problem is also solved by the message process in the AP, as shown in Fig. 3. Message contents transmitted to the monitoring system are encrypted by the public key of the AP, and the digital signature for M is concatenated. Then, the same digital signature attached in the original DCAS message to be transmitted to the SM can be used because M, an object of the digital signature, is not changed. Finally, a new message header is added and a newly generated message is transmitted to the monitoring system. After decrypting the received message using shared keys, the monitoring system checks the digital signature to verify the authenticity of the message and receives the original message contents.

The functional architecture of the monitoring system is shown in Fig. 4. The monitoring system consists of five major function modules and a database. The capture module gathers DCAS and TFTP messages related to a CA code download in real-time and stores it in the database. DCAS message groups (1) and (2), along with TFTP messages, are collected directly in the network, and message groups (3) and (4) are received from the AP. The cryptography module decrypts the received messages and verifies their digital signature. The monitoring module provides several functions such as searching, filtering, and tracing for DCAS messages. The statistical analysis module gives service operators a variety of information required for effective network management.

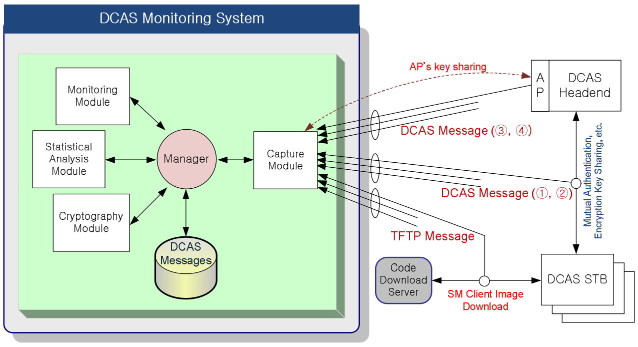

Fig. 4. Functional architecture of monitoring system.

4. Experimental Results

To verify the effectiveness of the proposed monitoring method, we implemented the monitoring system and constructed a test-bed using DCAS head end servers and an STB in a laboratory. An AP located in the DCAS headend transmits DCAS messages to the SM, built into an STB, via a cable modem termination system (CMTS) with a Data-Over-Cable Service Interface Specification (DOCSIS) set-top gateway (DSG) tunnel on a DOCSIS channel. A clear audio/video stream is scrambled by a control word generated in a CAS server and is transmitted to the STB through a cable network. To descramble the received audio/video stream, an entitlement management message and entitlement control message generated by the CAS server are transferred to the STB in the DSG channel and MPEG transport stream (TS), respectively. In a virgin state, the STB starts to communicate with the AP according to the DCAS protocol automatically and downloads the CA code from the head end securely. Then, the DCAS monitoring system analyzes and monitors the captured messages in the cable network.

Through a real-time statistical analysis for DCAS messages, the monitoring system shows results such as the ratio of DCAS packets to other packets, error ratio for received messages, etc. in (1) of Fig. 5. The filtering module in (2) searches the related messages for specific parameter values, the results of which are shown in (3) and (4), where (3) represents a message sequence chart according to the transaction between an AP and SM. When a specific message is selected, its detailed information is shown in (4). The session duration and processing times for each DCAS message are shown in (2). The network configuration for monitoring the DCAS protocol is set in (5).

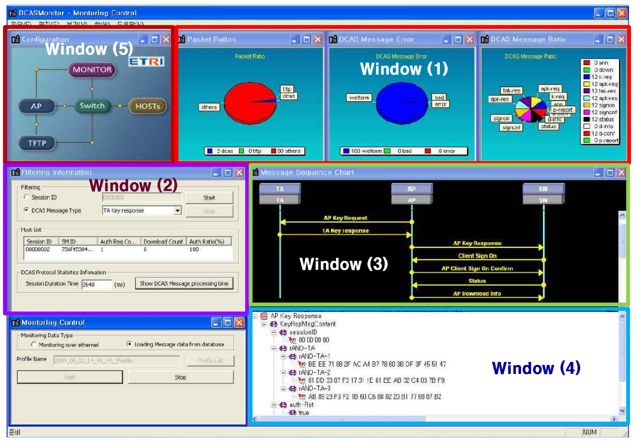

Fig. 5. Test results of DCAS monitoring system.

5. Conclusion

In this paper, we proposed an efficient monitoring method for a DCAS network protocol designed for downloading a CA code securely via a bi-directional communication channel. To overcome monitoring problems on a network protocol based on cryptographic functions, we classified DCAS messages into four groups, and proposed adequate methods for each message group. The merit of the proposed method is reusing the message process module, implemented in an AP, and the digital signature. Through experimental results, we confirmed that the proposed monitoring method can operate stably, securely, and effectively.

References

[1] ITU-T, Rec. J.290, Next Generation Set-Top Box Core Architecture, ITU-T Rec. J. 290, Nov. 2006

[2] T. Lookabaugh &and J. Fahrny, “Openness and Secrecy in Security Systems: PolyCipher Downloadable Conditional Access,” The Cable Show Conf., May 2007.

[3] B.S. Choi, et al., “A Tool Pack Mechanism for DRM Interoperability,” ETRI Journal, vol. 29, no.4, Aug. 2007, pp. 539-541.

[4] D.K. Kim, et al., “Design and Performance Analysis of Electronic Seal Protection Systems Based on AES,” ETRI Journal, vol. 29, no. 6, Dec. 2007, pp. 755-768.

[5] B.S. Koo, et al, “Design and Implementation of Unified Hardware for 128-Bit Block Ciphers ARIA and AES,” ETRI Journal, vol. 29, no. 6, Dec. 2007, pp. 820-822.