HDCP IIA over 1722a Discussion

Dave Olsen 6/25/2012
There are three elements of the content protection system. Each element plays a specific role in the system. First, there is the authentication protocol, through which the HDCP Transmitter verifies that a given HDCP Receiver is licensed to receive HDCP Content. The authentication protocol is implemented between the HDCP Transmitter and its corresponding downstream HDCP Receiver.

With the legitimacy of the HDCP Receiver determined, encrypted HDCP Content is transmitted between the two devices based on shared secrets established during the authentication protocol. This prevents eavesdropping devices from utilizing the content. Finally, in the event that legitimate devices are compromised to permit unauthorized use of HDCP Content, renewability allows an HDCP Transmitter to identify such compromised devices and prevent the transmission of HDCP Content.

This document contains chapters describing in detail the requirements of each of these elements. In addition, a chapter is devoted to describing the cipher structure that is used in the encryption of HDCP Content.

1.4 Terminology

Throughout this specification, names that appear in italic refer to values that are exchanged during the HDCP cryptographic protocol. C-style notation is used throughout the state diagrams and protocol diagrams, although the logic functions AND, OR, and XOR are written out where a textual description would be more clear.

This specification uses the big-endian notation to represent bit strings so that the most significant bit in the representation is stored in the left-most bit position. The concatenation operator ‘||’ combines two values into one. For eight-bit values \( a \) and \( b \), the result of \( (a || b) \) is a 16-bit value, with the value \( a \) in the most significant eight bits and \( b \) in the least significant eight bits.

1.5 References


Requirements

- Authentication and Key Exchange (AKE) – The HDCP Receiver’s public key certificate is verified by the HDCP Transmitter. A Master Key $km$ is exchanged.

- Locality Check – The HDCP Transmitter enforces locality on the content by requiring that the Round Trip Time (RTT) between a pair of messages is not more than 7 ms.

- Session Key Exchange (SKE) – The HDCP Transmitter exchanges Session Key $ks$ with the HDCP Receiver.

- Authentication with Repeaters – The step is performed by the HDCP Transmitter only with HDCP Repeaters. In this step, the repeater assembles downstream topology information and forwards it to the upstream HDCP Transmitter.
Requirements

- A reliable, bidirectional packet protocol (e.g., TCP/IP) is used to transport messages used for the HDCP authentication protocol from the HDCP Transmitter to the HDCP Receiver, and vice versa.

- Each packet must contain exactly one message. Each packet payload commences with a `msg_id` specifying the message type, followed by parameters specific to each message.

- In the case of TCP/IP, packets use an IP address and port number determined by procedures above the HDCP layer. Also, parameter values spanning more than one byte follow the convention in [5] of sending the most-significant byte first.
Reliable Protocol Discussion
Locality Check Discussion
Addressing