HARMAN

1722 Content Protection

Harman Corporate Technology Group

Jeff Hutchings – 4/5/2011

AKG by HARMAN harman/kardon by HARMAN Infinity by HARMAN JBL by HARMAN Lexicon by HARMAN Mark Levinson by HARMAN

Agenda

HARMAN

- Content protection and Digital Rights Management
- Introduction to content protection
- DTCP Overview
- HDCP Overview
- 1722 Content Protection
- What we need from 1722
- Conclusions

Content Protection and DRM

HARMAN

- **DRM (Digital Rights Management)**
  - Group of technologies that are used to determine and manage legal rights to view, copy (or not), or distribute (or not) digital audiovisual content
  - Available access rights are set by artists, studios, etc.
- **Content Protection**
  - Content protection is just one part of DRM
  - Content protection is used to protect authorized content from illegal copying, distribution, etc., as it is transmitted across various links or stored on media.
- **Example**
  - Purchasing a valid BluRay disk grants you legal access to view it on a valid BluRay player
  - Content protection is used to insure you or someone else can't illegally copy and distribute it

Content Protection Overview

HARMAN

- **Many, many different types of content protection**
  - Media (DVDs, Files, BluRay, CDs, etc)
  - Link (HDMI, MOST, IP, WiFi, etc)
- **Media Examples**
  - Content Scrambing System (CSS) - DVD
  - Advanced Access Content System (AACS) - BluRay
- **Link Examples**
  - Digital Transmission Content Protection (DTCP)
    - Originally developed with 1394 in mind, already plays well with 1722 as a result
  - High-Bandwidth Digital Content Protection (HDCP)
    - Originally developed for HDMI/DVI links. Now has IIA (Interface Independent Adaptation) for any transmission interface technology

DTCP Overview (1 of 2)

HARMAN

- **DTLA (Digital Transmission License Authority) History**
  - DTLA: “The 5C”: Hitachi, Intel, Panasonic, Sony, Toshiba
  - Released by DTCP in 1999, widely adopted by many content providers
- **What is DTCP?**
  - “Link Protection”
    - Using authentication and encryption, DTCP protects content from tampering, unauthorized copying, or retransmission, during transport on networks.
  - Copy Protection
    - DTCP enables content providers to enable/disable various levels of copy protection/access
      - Copy once
      - No more copies
      - Copy Never
      - Copy freely

DTCP Overview (2 of 2)

HARMAN

- **What is DTCP? (continued)**
  - System Renewability
    - Compromised or rogue devices can have authentication “revoked”
    - Robustness of system is improved
    - Better long term integrity

HDCP Overview (1 of 2)

HARMAN

- **DCP LLC - Digital Content Protection, LLC**
  - Intel Subsidiary for license management of HDCP technology
  - Similar function to DTLA but for HDCP
  - Originally developed for HDMI, DVI, now interface independent
  - **No Approved Retransmission Technologies (ART)**
    - **Example:**
      - **HDCP protected content cannot be retransmitted with DTCP. Must be transmitted using HDCP again. This may be an issue for 1722 as it does not inherently support HDCP and DTCP simultaneously.**

HDCP Overview (2 of 2)

HARMAN

- **What is HDCP?**
  - "Link Protection"
    - Using authentication and encryption, HDCP protects content from tampering, copying, or retransmission, during transport on networks.
  - Copy Protection
    - By definition, HDCP has only one copy protection mode:
      - No copies. Period.
  - System Renewability
    - Compromised or rogue devices can have authentication "revoked"
    - Robustness of system is improved
    - Better long term integrity

1722 Content Protection Necessary

HARMAN

- **Link Protection Needed**
  - Content from protected sources must be protected when transported on 1722 network
  - Protection scheme is determined by content providers and license administrators (DTLA, DCP, etc)
  - Example 1: 1722-enabled BluRay player to 1722-enabled Monitor
    - AACS→DTCP→1722 Transport→DTCP→Display
      - Supported using existing 61883 defined formats
      - Valid use case supported by DTLA and AACSLA
  - Example 2: HDMI BluRay player to 1722-enabled Monitor
    - AACS→HDCP→1722 Transport→HDCP→Display
      - HDCP not currently supported by 1722, but valid HDCP use case
    - AACS→HDCP→DTCP→1722 Transport→DTCP→Display
      - NOT ALLOWED BY DTLA OR DCP. No approved ART for HDCP

1722 and DTCP

HARMAN

- **Underlying Support**
  - DTCP evolved with IEEE-1394 in mind
  - 61883 formats are compatible with DTCP
    - SYN bit fields define encryption and copy protection modes
- **Open Issues**
  - Must still implement protocol for authentication and key exchange, system renewability
  - DTCP Supplement E Mapping DTCP to IP exists and is valid
  - No formal definition of DTCP supplemental mapping for 1722
    - 1722 is network layer 2, IP is network layer 3
    - May still be able to use Supplement E “as is”, this is under investigation
  - Currently no way in 1722 bit fields to support multiple protection types
    - HDCP and DTCP for example

1722 and HDCP

HARMAN

- **Underlying Support**
  - HDCP 2.0 IIA (Interface Independent Adaptation)
    - Enables HDCP usage on links other than HDMI, DVI.
  - Native support for transport streams such as IEC13818 outside of IEC 61883-4
- **Open Issues**
  - Must implement protocol for authentication and key exchange, system renewability
  - Currently no way in 1722 bit fields to support multiple protection types
    - No HDCP ART, must support both DTCP and HDCP
  - Could also choose not to support HDCP content on 1722

DTCP versus HDCP (1 of 2)

HARMAN

- **Similarities**
  - High level authentication and key exchange (AKE)
  - System Renewability Messaging (SRM)
  - Base encryption cipher: AES-128
- **Differences**
  - Underlying cryptographic functions
    - DTCP: SHA-1, Elliptic-Curve Cryptography (ECC), Diffie-Helman (EC-DH), Digital Signature Algorithm (EC-DSA)
    - HDCP: SHA-256, RSA, RSAASA-PKCS1
  - AKE Protocol
    - HDCP requires additional locality check (maximum RTT of 7mS)

DTCP versus HDCP (2 of 2)

HARMAN

- **Differences (continued)**
  - AES-128 cipher operating mode
    - DTCP: Cipher Block Chaining
    - HDCP: Counter (sometimes called Integer Counter)
    - To support both requires a multi-context cryptographic engine capable of both modes. There are commercial devices with supporting software that do this already.
  - Stream startup
    - DTCP allows protected content transmission before AKE
    - HDCP requires AKE first, then content transmission

What is needed from 1722

HARMAN

- **DTCP**
  - Explore whether or not DTCP-IP can be used “as is”
  - Implement as needed, or pursue further definition with DTLA (yuck)
    - Formal statement from 1722 regarding DTCP support?
      - Support is implied via existing SY bits in 61883 formats, and for transport streams.
- **Should 1722 support multiple content protection schemes?**
  - If yes:
    - Identify which to support initially
    - Define additional bit fields, packet formats, etc., as needed for
      - Content protection ID
      - Encryption modes
      - Copy protection modes
      - Future proofing

More Information

HARMAN

- **DTLA**
  - http://www.dtcp.com/
- **Informational DTCP specifications**
  - http://www.dtcp.com/specifications.aspx
  - Note: Full specifications only available in hardcopy from the DTLA to DTCP licensees.
- **DCP and HDCP IIA 2.0 Specification**
  - http://www.digital-cp.com/
  - Link to specification about halfway down the page.
- **AACS**
  - http://www.aacsla.com/home

WHERE SOUND MATTERS

AKG by HARMAN harman/kardon by HARMAN Infinity by HARMAN JBL by HARMAN Lexicon by HARMAN Mark Levinson by HARMAN