1722a Content Protection

Dave Olsen 4/17/2012
Agenda

- Content Protection and DRM
- DTCP Overview
- HDCP Overview
- DTCP versus HDCP Similarities
- DTCP versus HDCP Differences
- Next Steps
Content Protection and DRM

- **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 and DRM

- Digital rights management is outside the scope of 1722a
- 1722a is really only concerned about content link protection

Link Protection

- Digital Transmission Content Protection (DTCP)
  - Originally developed with 1394/61883 in mind
- 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)

- **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
What is DTCP? (continued)

- System Renewability
  - Compromised or rogue devices can have authentication “revoked”
  - Robustness of system is improved
  - Better long term integrity
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.
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
DTCP versus HDCP Similarities

- High level authentication and key exchange (AKE)
- System Renewability Messaging (SRM)
- Base encryption cipher: AES-128
- Implementations are self certified by the manufacturer
- Interoperability can be verified at a test house
DTCP versus HDCP 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)
  - Stream startup
    - DTCP allows protected content transmission before AKE
    - HDCP requires AKE first, then content transmission
DTCP versus HDCP Differences

- **Protocol Support**
  - DTCP evolved with IEEE-1394 in mind
    - All 61883 formats are compatible with DTCP
      - SYN bit fields define encryption and copy protection modes
  - HDCP evolved from HDMI
    - HDCP IIA supports Transport Stream Data – 61883-4
    - Currently no bit in 1722 to indicate HDCP
DTCP versus HDCP Differences

- **Approved Retransmission**
  - DTCP can be transmitted as HDCP
  - HDCP has no approved retransmission technology
    - Any content that originates on HDMI or MHL must use HDCP
DTCP versus HDCP Differences

- **Copy Modes**
  - DTCP has multiple copy modes
    - Copy once, No more copies, Copy Never, Copy freely
  - HDCP has one copy mode
    - Copy Never
DTCP versus HDCP Differences

- **Approved methods**
  - DTCP requires a DTLA approved supplement
    - Incomplete informational docs are available online
    - Complete docs are available for purchase, subject to license agreement
    - Supplement for DTCP over 1722 has to be reviewed and approved by the DTLA
  - HDCP provides IIA
    - Documents are available for free online
    - Specification for HDCP over 1722 using the IIA needs no approval
    - Could be included as an annex in 1722a
Next Steps?

- **Does HDCP support all use cases?**
  - HDMI/MHL input is a requirement
  - DTCP can be retransmitted by HDCP
  - HDCP does not require documents to be purchased by each workgroup member
  - HDCP only supports Transport Streams with the IIA
  - Define HDCP bit

- **Does DTCP support all use cases?**
  - Satellite/Digital TV typically support DTCP
  - DLNA supports DTCP
  - Are DTCP copy modes important
Next Steps?

- Do we need to support both DTCP and HDCP?

- Possibility of reusing DTCP-IP if we had an alternate 1722 format that includes an IP header
More Information

- **DTLA**

- **Informational DTCP specifications**
  - Note: Full specifications only available in hardcopy from the DTLA to DTCP licensees.

- **DCP and HDCP IIA 2.0 Specification**
HARMAN
WHERE SOUND MATTERS