Two Issues in HDCP/HDMI

CEA/DCP Plugfest

April, 2005

Gary Graunke, DCP Technical Support

Consumer Electronics Association

DIGITAL CONTENT PROTECTION, LLC
digital-cp.com

Agenda

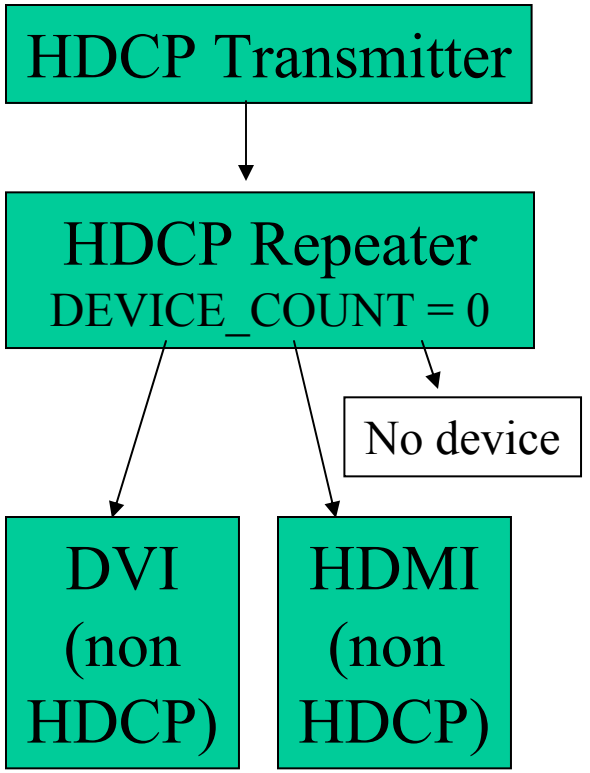
- Preface
- Repeaters with Zero DEVICE_COUNT
  - Problem statement
  - Content protection requirements
  - Existing device behavior requested
  - Interoperability concerns
  - Workaround, Solution recommendations requested
- AVMUTE difficulties
  - Problem statement
  - Workaround, Solution recommendations?
- Summary and next steps

Preface

- Compliant devices may sometimes nevertheless not interoperate
- Understanding differences in implementation is the first step
- Workarounds for fielded legacy devices
- Incorporate consensus recommendation into future spec revisions

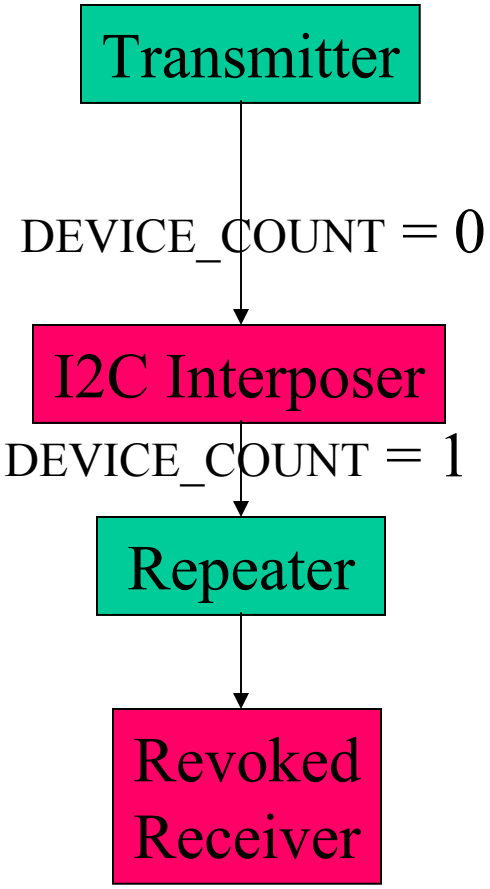
Repeater with Zero DEVICE_COUNT

- What happens when an HDCP Repeater has no downstream HDCP devices?
- Can have DVI, HDMI devices without HDCP
- Or simply no devices
- Repeater may desire protected content (has display/audio capabilities)



Clarifying Requirements

- Upstream transmitter cannot skip second phase of authentication for downstream repeater
  - DEVICE_COUNT is easy to spoof
  - Key-based V computation match enables trust in DEVICE_COUNT
- Repeater cannot send protected content to non-HDCP downstream devices



Repeaters with No Downstream HDCP Devices

- Downstream repeater behavior varies
  - Case A: Repeater authenticates as repeater
    - Computes V' over empty KSV list, sets READY
    - May expect to receive protected content
  - Case B: Repeater authenticates as receiver
    - No second phase of authentication
    - Will receive protected content as normal receiver
  - More cases?

Upstream Transmitter Behavior

- Upstream transmitter sees downstream repeater with zero DEVICE_COUNT
  - Case A: Transmitter includes repeater in authentication, completes 2nd phase
    - Computes V with empty KSV list
    - Transmitter sends protected content as usual
  - Case B: Transmitter excludes repeater from authentication
    - No protected content sent to repeater
  - More cases???

Interoperability Concern

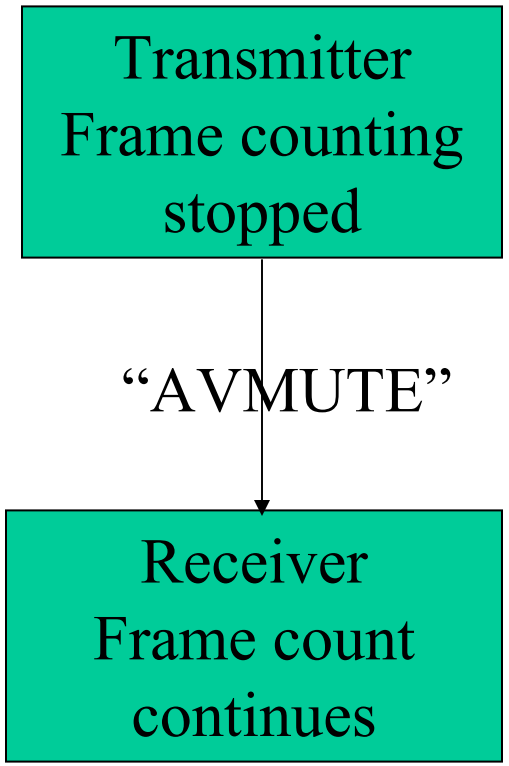
- Case B transmitter, Case A repeater at bottom level of repeater tree
  - Transmitter does not send protected content
  - Repeater wants to function as receiver
    - has display or speakers
- Non-problems
  - Repeater does not need display content
  - Top, interior repeaters have non-zero device count
  - For bottom two levels, repeaters are same type (A/B)
- Others?

Possible Workarounds / Solutions

- Short-term Workaround
  - Add repeater KSV to KSV_FIFO when otherwise empty
    - Redundant, adds one more device to list
- Long-term alternatives
  - Transmitters move to Case A
    - Be able to compute V of empty list
  - Repeaters that display content move to Case B
    - Be able to authenticate as receiver
- Others??? Comments???

AVMUTE Problem

- HDMI GCP (including AVMUTE) is optional
  - AVMUTE is a case of General Control Packet
  - Receivers may not interpret AVMUTE GCP
- Optional HDCP Advance Cipher AC mode
  - Supported by receiver, enabled by transmitter
  - Transmitter may expect receiver to stop cipher during AVMUTE
  - Loss of synchronization during AVMUTE



Possible Solutions

- Workarounds
  - Do nothing--normal loss of synchronization detection will cause re-authentication
  - HDCP transmitter enabling 1.1 options and sending AVMUTE always re-authenticates after sending AVMUTE
- Longer Term Solutions
  - Add BCaps bit if receiver recognizes AVMUTE?
- Others???

Summary and Next Steps

- Compliant devices may sometimes nevertheless not interoperate
- We are gathering information during plugfest and following weeks
- Soon: Point out problem, suggest optional workarounds in final 1.1 clarification/errata
- Longer-term: Assuming concensus, drive toward common solution(s) in future spec