Protecting Against Unauthorized Redistribution of Digital Broadcast Content

Presentation to the CPTWG

Intel, Hitachi, Matsushita, Sony and Toshiba

Problem Statement

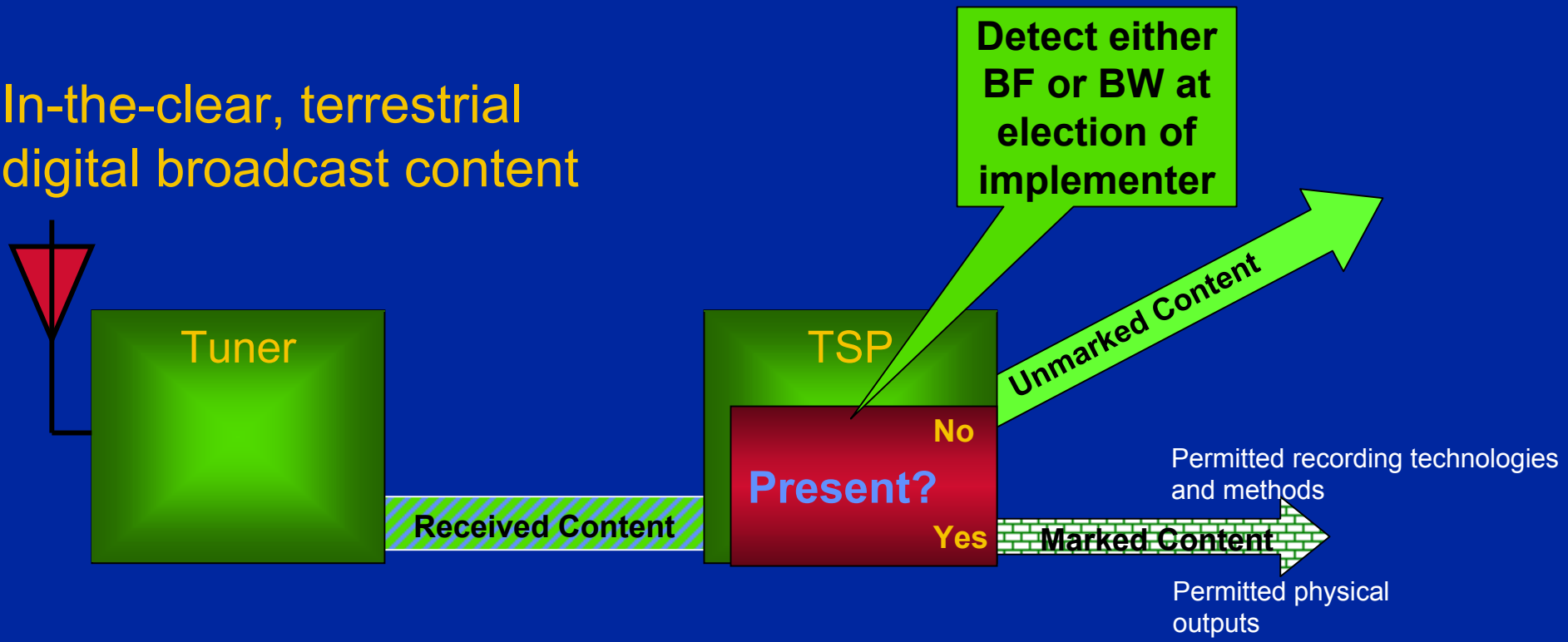
- Currently, there is no enforceable technical means to prevent unauthorized redistribution of unencrypted digital terrestrial broadcasts.
- A solution for such content is needed that would:
  - Enable content owners to signal application of content protection.
  - Avoid deletion or alteration of such signaling means.
  - Prevent unauthorized routing of protected content to unprotected digital outputs and unauthorized recording technologies.
  - Not interfere with lawful consumer recording and enjoyment of broadcast content.

Challenges

- Achieve consensus on signaling means - broadcast flag (BF, ATSC flag for US use) and broadcast watermark (BW, the consensus watermark) - to signal application of protection against unauthorized redistribution for unencrypted digital terrestrial broadcast content.
- Develop compliance and robustness rules to govern the secure handling of unencrypted digital terrestrial broadcast content received by CE and IT products.
  - From tuner through to authorized outputs and recording technologies.

Technical Proposal

In-the-clear, terrestrial digital broadcast content



Definitions

- “Received Content” is digital terrestrial broadcast content that has been processed by a digital demodulator.
- “Marked Content” is Received Content that has been screened for either the BF or BW and determined to contain such signaling means.
- “Unmarked Content” is Received Content that has been screened for either the BF or BW and determined not to contain such signaling means.

Compliance Rules Summary

Compliant Products:

- Must comply with specified robustness rules (see next slide).
- Must ensure Received Content is screened for either the BF or BW at the election of the implementer.
- Must ensure Marked Content leaves the product only by:
  - Authorized outputs (e.g., IEEE1394 w/DTCP, DVI w/HDCP, analog, etc.).
  - Removable media that implement secure recording means (e.g., CPRM, D-VHS, etc.).
- Subject to the robustness rules, have no limitations concerning the internal
  - display,
  - processing or
  - secure buffering or lawful storage

  of Received Content.
- Have no requirements concerning Unmarked Content.

Robustness Rules Summary

Compliant Products must:

- Not have functions that defeat the compliance or robustness rules.
- Be designed and manufactured in a manner that provides a specified level of protection against unauthorized routing of Received Content, and against interference with the BF or BW, prior to screening for either of such signaling means.
- Be designed and manufactured in a manner that provides a specified level of protection against unauthorized routing of Marked Content.

Proposed Next Steps:

- Multi-industry participation is invited for a technical discussion of issues related to the proposed solution.
- Make expeditious progress:
  - Technical and enforcement solutions
  - Substantial completion by Q1, '02
- Meeting following CPTWG today:
  - Further review and discuss this technical proposal
  - Organize group and set intermediate milestones and logistics for next series of meetings