Content Protection for Streaming Media - Why using HDCP 2.2 Pro is not the solution

White Paper

Tripleplay
Rapier House
40-46 Lamb's Conduit Street
London
WC1N 3LJ

www.tripleplay.tv

1 Introduction

Protecting content when streaming over a LAN or WAN is crucial for many content providers. This paper explores the use of HDCP 2.2 Pro as a technology to accomplish that and highlights the deficiencies of that approach.

Summary:

- HDCP 2.2 Pro is not a DRM system.
- HDCP 2.2 Pro cannot be used with many common client devices, including PCs, mobile and System on Chip (SoC) displays.
- HDCP 2.2 Pro restricts who can deploy systems using it.
- HDCP 2.2 Pro restricts where systems can be deployed.
- HDCP 2.2 Pro requires public Internet access.
- HDCP 2.2 pro is suitable for a very limited set of use cases.
- HDCP 2.2 pro will not be allowed by US broadcasters.

2 HDCP 2.2 Pro

HDCP has been used as a copy protection mechanism for HD TVs for many years. This started as protecting the link between the source (e.g. a Sky Set Top Box) and the sink (TV). More recently HDCP was extended so that it can be used over an IP LAN to protect content, this was introduced in HDCP 2.0. The main limitation of HDCP 2.0 was that the number of keys per source was limited to 32 so making it impracticable for medium to large deployments.

HDCP 2.2 Pro was introduced to lift the restriction on the number of clients (32) that had been a problem for systems using HDCP 2.2 for IP media streaming. That's about the only good thing it does, and it is worth noting that one vendor still has a limit of 1000 end points per source.

There are however major downsides to using HDCP 2.2 Pro; The range of client devices that can be used is seriously limited and that using HDCP 2.2 Pro ties the end user and installers to a very restrictive set of procedures and processes.

Client device support is limited

The biggest downside of using HDCP for content protection remains, that every client device which needs access to the HDCP signal will need to include support for HDCP 2.2 Pro, so PCs, smart TVs, mobile devices and SoC devices are going to be a problem as they don't currently support this protocol.

For example, many popular SoC display devices (e.g. Samsung SSP, LG WebOS) do not support HDCP 2.2 Pro over the LAN, disqualifying these devices from being used where content protection is needed using HDCP 2.2 Pro.

This means that systems using HDCP 2.2 Pro will always be tied to proprietary hardware.

Added to that, there are many TV devices already deployed since 2013 which do not, and never will, support HDCP 2.2, so further limiting the range of client devices supported.

Restricted customer deployments

The location at which an HDCP 2.2 Pro system is installed must be authorised by the DCP (the body that controls how and where HDCP 2.2 Pro is deployed), and must be present on the DCP website: http://www.digital-cp.com/HDCP_Pro_Authorized_Locations

The DCP also prohibits certain types of deployments. In particular, it cannot be used in MDUs (Multiple Dwelling Units) such as college dormitories, duplexes, apartment blocks etc, again, restricting for installers of the technology.

Deployment gotchas

Deploying HDCP 2.2 Pro also has some hidden overheads that have not been fully owned up to.

https://www.digital-cp.com/HDCP_Professional_Information

The main points are;

- Licensed HDCP Pro repeaters will be required.
- Only authorised installers will be allowed to buy and integrate them – and the authorisation has to come from DCP (the Digital Content Protection LLC organisation).
- Systems with Pro repeaters will require updating four times per year to keep their configurations up to date, presenting a hidden cost and time implication for the end user and the installer.

What this means in practice is that where any HDMI routing is taking place, for example in a redundant headend where the source needs to be split, or where a client device is fanning out to multiple display devices, specialist equipment will be needed.

The requirement that only authorised installers will be allowed to install and maintain the equipment means additional staff costs, training and registration will be needed. This will be an obstacle to many smaller AV companies. With the general industry move for AV to be run by IT departments, this will also be a burden to IT departments with many end users.

Every four months the device SRMs (System Renewability Messages) must be updated. If the update does not take place, then the system reverts to regular HDCP 2.2 with the 32 device limit until the SRM has been updated. The SRM updates are carried out over the public Internet, meaning that for secured networks found in many enterprises this will pose a big problem as external internet access is often restricted, particularly in the finance and government sectors.

HDCP 2.2 Pro is not a DRM

Protecting content is crucial for streaming media, but that is not the only requirement placed on a comprehensive protection scheme. In addition to the encryption, there must be a mechanism to control which clients are authorised to decrypt the content. HDCP encrypts the content between a source and one or more sinks. This has an important consequence; other than issuing new SRMs, there are no mechanisms to authorise/de-authorise individual client devices, making this at best a secure way of transmitting AV over a LAN to a restricted set of client devices. It does not allow, for example, removing or subsequently restoring an individual client's rights to view protected content.

For this level of functionality additional software and DRM encryption will need to be installed and activated.

In contrast, all professional DRMs and their associated middleware systems, including the Tripleplay system, have the ability to control client authorisations down to individual devices.

3 Conclusions

Tripleplay's broadcast standards based software encryption tools do not have the inflexibility of very limited client support so we can always integrate new devices using appropriate encryption methods.

There are no specialised or expensive approvals needed for staff installing and maintaining systems with standard DRMs. In addition, customers and installers don't need to get approvals from the DCP before anyone can install and use our systems.

Tripleplay already supports a range of client devices with SECUREMEDIA, Samsung LYNK DRM, Philips VSECURE and AES128, all approved by major studios and broadcasters.

Existing investments that customers have already made in TV and other client devices are protected.

In summary, HDCP 2.2 Pro;

- Is not a DRM.
- Has very restricted client device support.
- Seriously limits who can install systems using HDCP 2.2 Pro.

Feature Comparison

Feature	Tripleplay	HDCP 2.2 Pro
Support Amino x5x	Y[1]	N
Support Philips SoC	Y[2]	N
Support Samsung SSP SoC	Y[3]	N
Support HLS	Y[4]	N
Support Desktop media players	Y[5]	N
Protection for non-HDCP 2.2 sources – eg DVB, QAM, direct IP	Y	N
Encrypts Video at ES level	Y	Y
Full DRM functionality	Y	N
Clients	Unlimited	1000
Approved by major broadcasters in US	Y	N
Approved by broadcasters in Australia	Y	N
Approved by broadcasters in Africa	Y	N
Approved by Sky	Y[6]	Y
Requires registered installers	N	Y
Can operate without Internet access	Y	N
Restricts the types of installation	N	Y

1 Uses the Arris SECUREMEDIA DRM or VERIMATRIX for content protection
2 Uses the Philips VSECURE DRM
3 Uses the Samsung LYNK DRM
4 Uses AES128 and the HLS standard
5 Uses AES128 and the CSA
6 Using the Sky Brightbox