Proximity control based on IEEE802.1AS

Eric H.S. Ryu

eric_ryu@samsung.com
Samsung Electronics

IEEE 802.1 Interim Meeting, York
September 2006

One of problems on the contents networking

❑There is no end-to-end accurate distance measurement mechanism in IEEE802 network

❑There are some proposal to use the current RTT mechanisms but it is not accurate enough for privacy and contents protection.

- ▪DTCP over IP specifies a 7ms end-to-end delay limit and a 3 hop limit for RTT; the latter provides the hop count but not the actual link distance between the server and renderer.

- ▪An electrical signal can travel more than 100 meters in 1 μs; therefore, the granularity is greater than several hundred meters. A delay limit of 7ms is equivalent to hundreds of kilometers.
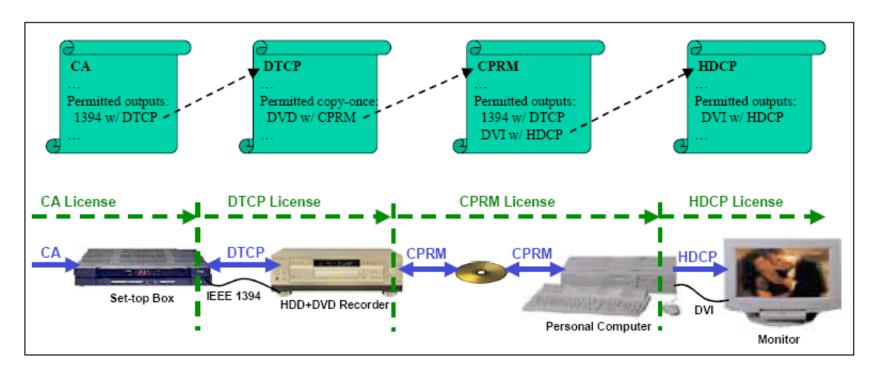
Chain of different copy protection mechanisms

Figure 3: Content protection chain example

If we have a homogeneous copy protection mechanism…

Content Protection in the Digital Home

Michael Ripley, Corporate Technology Group, Intel Corporation
C. Brendan S. Traw, Corporate Technology Group, Intel Corporation
Steve Balogh, Corporate Technology Group, Intel Corporation
Michael Reed, Corporate Technology Group, Intel Corporation

Analysis of security proposals in DLNA usage scenarios

Top Category	2nd Category	3rd Category	Scenario Number	Sum
Device Authentication	Wired/Wireless	In-band/out-of-band	2.1.1v2, 2.1.7	2
		In-band	2.7.12a, 1.8.1, 1.8.3, 1.8.4, 1.2.17	5
		Out-of-band	2.1.2, 2.1.3, 2.1.4, 2.7.13	4
		Blue-tooth	2.1.5	1
		DTCP/IP	1.6.12, 1.6.18	2
	Wireless only	In-band/out-of-band	2.7.7, 2.7.8, 2.7.12	3
		Out-of-band	2.7.9, 2.7.10, 2.7.11, 1.6.5, 1.6.36a, 1.6.37a, 1.6.38, 1.6.39, 1.6.40, 2.1.13, 2.1.14	11
		Security controller	2.7.1, 2.7.2, 2.7.3	3
		UPnP device security	1.8.8, 1.8.9,	2
		Wi-fi Protected Access (WPA)	2.7.4, 2.7.5, 2.7.6	3
Content Authentication	Wired/Wireless	General DRM	1.6.7a, 1.6.10, 1.6.24, 1.6.25, 1.6.31, 1.6.32, 1.6.34a, 1.6.35,	8
		CORAL DRM	1.6.11,	1
		OMA DRM	1.6.12	1
		WMDRM	1.6.26,	1
DRM interoperability and guest device in home case			1.6.1, 1.6.19, 1.6.20, 1.6.21, 1.6.22, 1.6.23, 1.6.27, 1.6.28, 1.6.29a, 1.6.30	10
Total				57

DLNA usage scenarios: Wire/Wireless Device Authentication

S-Number	Company name / Author name	Scenario Title and/or Description
2.1.1v2	Intel / Paul Sorenson	… It automatically detects wireless network and exchanges Discovery data… needed password, USB flash, etc
2.1.7	Nokia / Jose Costa	… User utilizes the Control Point to access the Access Point configuration page to set up the link layer security…
2.1.2	Philips- Samsung / Armand Lelkens, et al	John simply touches the new device with the home EZ setup registrar. The media player now is part of the wireless network without know anything about SSID, keys etc. …
2.1.3	Philips- Samsung / Armand Lelkens, et al	Rekeying a network … smart card , NFC, USB stick. The trigger for the AP to generate new settings can be a push button on the AP
2.1.4	Philips- Samsung / Armand Lelkens, et al	Guest device entering and leaving a home
2.1.5	Philips / Armand Lelkens	… She touches the TV with the mobile phone. The picture on the phone is transferred to the TV.
2.7.12a	Nokia / Jose Costa-Requena	Secured Content Sharing
2.7.13	Samsung / Jooyeol Lee	Guest device controls home network devices and vice versa
1.8.1	LGE / KyungJu(Kalen) Lee	Parental control over media access … When John's children are present, he deselects adult mode …
1.8.3	Intel / Paul Sorenson	Parental control over media access … Not knowing the PIN, Billy clicks the 'Skip' button … All movies that appear in the listings are rated G or PG.
1.8.4	Lenovo / Austin Luo	The Administrator classifies and organizes content according to different user settings, each with different access privileges
1.6.12	Sony Corporation / Bruce Fairman	Portable Player as a Secure Server
1.2.17	EchoStar / Communications Corp. John Card II	TV Ratings for DVR recording … After 2 hours, content is blocked by the HDTV and the user is prompted to enter permission information to continue…
1.6.18	Panasonic / Hiroki Yamauchi	Move the Protected Content FROM another Storage Server

DLNA usage scenarios : Wireless Device Authentication (1)

S-Number	Company name / Author name	Scenario Title and/or Description
2.7.1	Intel / Paul Sorenson	A Mobile Device attempting to join the home network is not given access unless proper guest credentials are presented.
2.7.2	Intel / Paul Sorenson	A new Mobile Device attempting to join the home network is not given access unless proper credentials are presented
2.7.3	Intel / Paul Sorenson	A user can define a restricted set of operations for a device that are available to guest users on the network
2.7.4	HP / Bob Taylor	The owners grant the device access to the network, but only to the specified sub-set of content in the repository
2.7.5	HP / Bob Taylor	Attack from within the Home
2.7.6	HP / Bob Taylor	Attack from the Internet
2.7.7,	HP / Bob Taylor	Authenticated Identity is the Key to Content Anywhere-Anytime; Identity Authentication: Biometric, token, password
2.7.8,	HP / Bob Taylor	Privacy of Identifiable Information that can be tied to a specific person; Identity Authentication: Biometric, token, password
2.7.9	Philips / Wim Bronnenberg, et al	Initial set-up of a secured network
2.7.10	Philips / Wim Bronnenberg, et al	Introduction of a new device to a network that is already secured
2.7.11	Philips / Wim Bronnenberg, et al	Giving access permissions to a Control Point
2.7.12	Nokia / Jose Costa	Secured Content Sharing

DLNA usage scenarios : Wireless Device Authentication (2)

S-Number	Company name / Author name	Scenario Title and/or Description
1.6.5	Philips / Martin Rosner, at al	Authorized Domain/ Using content via non-Authorized Domain devices
1.6.36a	Philips-Samsung / Martin Rosner, at al	Authorized Domain/ Adding Devices to the AD
1.6.37a	Philips-Samsung / Martin Rosner, at al	Authorized Domain/ Removing Devices from the AD
1.6.38	Samsun-Philips / Jooyeol Lee. Et al	Authorized Domain/ Accessing another user's content as a Guest
1.6.39	Philips / Martin Rosner, at al	Authorized Domain / Setting up and Using an Authorized Domain
1.6.40	Philips / Martin Rosner, at al	Authorized Domain/ Remote access to an Authorized Domain
2.1.13	Microsoft / David Roberts	Automatic Wireless & WAN Configuration
2.1.14	MS / David Roberts	A new device is connected to the home network & needs temporary access to a service The homeowner uses an out of band interface to transfer permission to a device to access service
1.8.8	Fujitsu / Takuya Sakamoto	Access Control in home domain (a guest device that has authorization can share the host content)
1.8.9	Fujitsu / Takuya Sakamoto	Access Control for device authentication (prohibit specific content from being used by a specific user group)

DLNA usage scenarios : Content Authentication

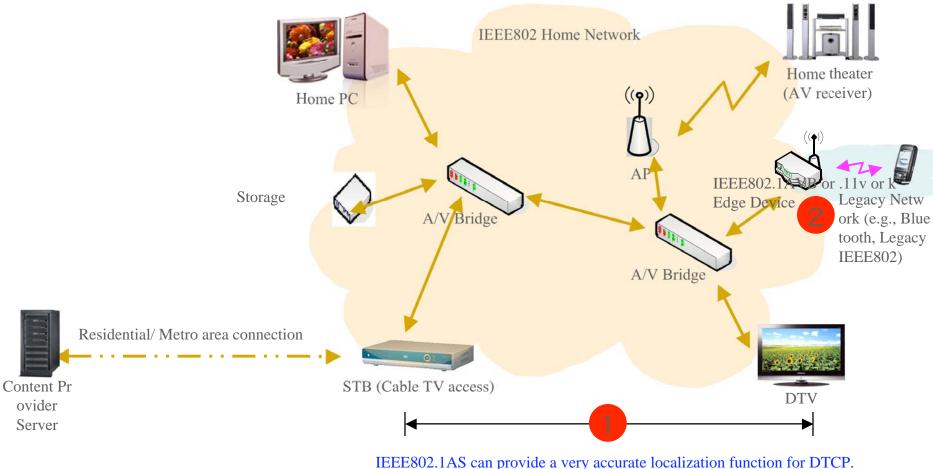| S-number	Company name / Author name	Scenario Title and/or Description
1.6.7a	Dolby Laboratories / Brian Link, at al	Download and Play/Export Commercial Content
1.6.10	Sony Corporation / Bruce Fairman	Content migration with DRM interoperability
1.6.11	Philips-UMG / Martin Rosner, at al	Digital Rights Management Interoperability between different mobile devices
1.6.12	Sony Corporation / Bruce Fairman	Portable Player as a Secure Server
1.6.24	Sony Corporation / Bruce Fairman	Protected Contents Synchronize between portable DMP and DMS
1.6.25	MS / Florian Pestoni	Device to Device Copy/ This scenario requires direct content exchange between two portable players over an IP connection
1.6.26	MS / Florian Pestoni	Content License Acquisition for portable device
1.6.31	Huawei / Lixianghui	Content Playcount management Across DLNA Devices
1.6.32	HP / Mirjana Spasojevic	Protect personal media using a DRM system
1.6.34a	CableLabs / Ralph Brown	Protected content that is stored on STB is moved to media server
1.6.35	CableLabs / Ralph Brown	Protected content that is stored on STB-PVR is streamed to DMA

DLNA use-cases: DRM interoperability and guest device treatment

S-number	Company name / Author name	Scenario Title and/or Description
1.6.1	HP/ Bob Steigerwald, at al	Content Protected IPTV 1.6.1 / Content is redirected to different devices
1.6.19	UMG-Philips / Dmitry Radbel, at al	Remote Access to the Home Network – Content Download
1.6.20	UMG-Philips / Dmitry Radbel, at al	Remote Access to the Home Network – Content Streaming
1.6.21	UMG-Philips / Dmitry Radbel, at al	Using Content from a "Guest Device" in a Home Network
1.6.22	UMG-Philips / Dmitry Radbel, at al	Moving a Device with Content between Home Networks
1.6.23	UMG-Philips / Dmitry Radbel, at al	Exporting Protected Content from Home Network to Storage Device
1.6.27	MS / Florian Pestoni	CP4-Sync to DMS/Stream to DMR
1.6.28	MS / Florian Pestoni	CP5-Secure Managed Copy
1.6.29a	MS-Samsung/ Florian Pestoni, at al	Burn/Copy to Removable Media
1.6.30	MS / Florian Pestoni	Home domain (definition of home domain, including car)

Summary of security proposals

❑Secure Domain Selection

❑Content Transferring

❑DRM Interoperability

❑Usage regulation

❑Temporary allowance

Digital content service environment

IEEE802.1AS can provide a very accurate localization function for DTCP.

Using IEEE802.1AS accurate localization, content providers can more easily control the physical span of their content distribution compared to using DTCP controls

Note: IEEE802.1 AVB, IEEE802.11k, IEEE802.11v can be thought as a homogeneous domain

Service domain segmentation

Case1: Single proximity control domain

- Single proximity control mechanism works in small area.

Case2: Mixed proximity control domain

- Multiple proximity control mechanisms are combined in the domain

Case 3: Proximity control with the remote STB certified by content provider

- For the network-based content delivery case.
- The proximity control point can be an STB or other device authorized by contents provider

Assumptions

❑ **For the single proximity control domain (SPC)**

- Network elements have a common link distance measurement method
- For example, IEEE802.1AS, IEEE802.11v, IEEE802.11k, IEEE802.xx have the same functionality
- With accurate timing/synchronization capability, the IEEE802 technology can achieve the service domain boundary (end-to-end) within TBD feet. (the current target value is around 30 feet but it needs verification through hardware prototype tests).

❑ **For mixed proximity control domain (MPC)**

- IEEE802.1 wired and wireless interfaces that do not support new standardized network timing/synchronization technology.
- Also, non-IEEE802 families, such as IEEE1394, Bluetooth, USB, Wireless USB, Wireless IEEE1394, etc
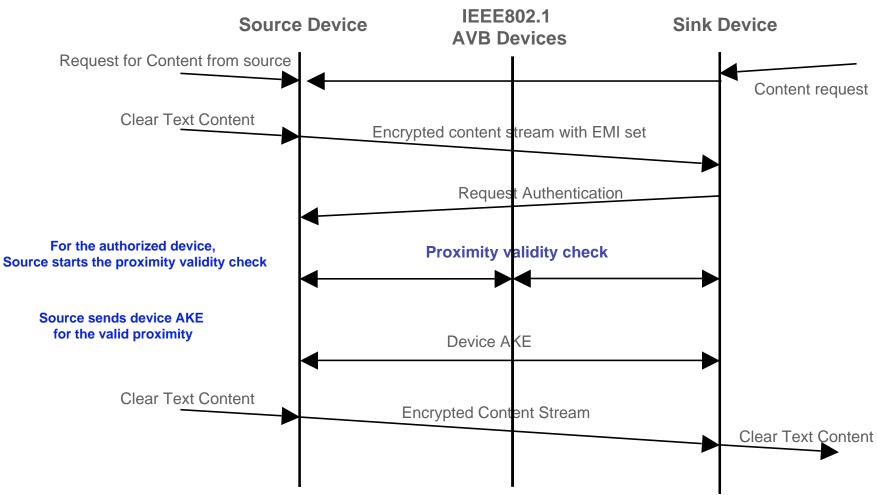
Assumptions (2)

❑ For the SPC domain

- Since IEEE802.1 AVB assumes the switched network case, the two separated devices are connected as logically point-to-point.

- What we need to add for this case is that proximity parameter, i.e. the physical distance.

- DTCP over IP can be an initial reference model for DTCP over IEEE802 AVB

- DTCP over IEEE802 AVB can have IEEE802.1x wireless in one of its domains if it has layer 2 proximity capability.

❑ For different DRMs and connectivities

- As indicated in many of the DLNA usage cases, we can conditionally extend the proximity control mechanism to those regions.

- If there is a new activity for new connectivity or related DRM, the current proposal can be ported, and the SPC domain can include non-IEEE802 technology in the future for a full homogeneous control mechanism.
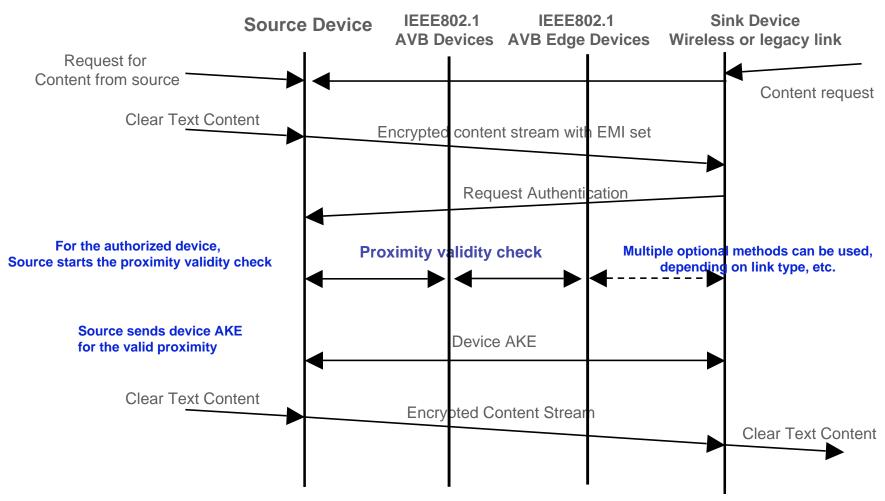
Case 1: For a Single proximity control domain

As an Example…

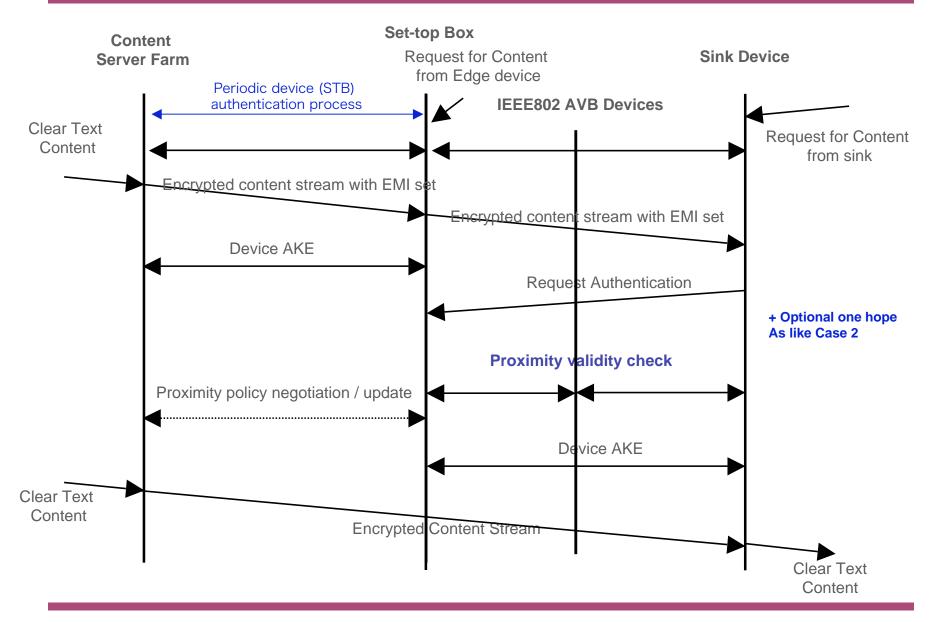# Case 2: For multiple proximity control domain

As an Example…

Case 3: For the Network based service

❑Approach

▪The authorized set-top box is under the control of the service provider

▪The first link is longer than the home domain size; it may be difficult to include the IEEE802.1AS functionality in this link.

▪The set-top box is an intermediate control point for proximity control. For the first time delay, between the content server and set-top in the home, the link distance need not be considered if the set-top is certified and is provided with a suitable authentication method by the content provider.

▪Two or three domains can exist in this scenario

Case 3: For the Network based service

Content Server Farm

Set-top Box
Request for Content from Edge device

Sink Device

Periodic device (STB) authentication process

IEEE802 AVB Devices

Clear Text Content

Request for Content from sink

Encrypted content stream with EMI set

Encrypted content stream with EMI set

Device AKE

Request Authentication

+ Optional one hope As like Case 2

Proximity validity check

Proximity policy negotiation / update

Device AKE

Clear Text Content

Encrypted Content Stream

Clear Text Content

Summary

❑ IEEE802.1AS separately measures the propagation delay and processing delay, and it can be used for proximity control at the reasonable accuracy.

❑ We propose to consider a standard procedure in IEEE802.1 for proximity controlling.