

Blu-Ray Media Decryption on MAGIK Board based on I.MX6 Processor

Revathi.S* and Chaitra.C**

*PG Student, Dept of E&I, SIT, Tumakuru, India

E-mail: revathiprk9@gmail.com

**Assistant Professor, Dept of E&I, SIT, Tumakuru, India

E-mail: Chaitra_chtr@yahoo.co.in

Abstract: The digital optical storage device that is currently supporting high definition format is Blu-ray disc. Blu-ray disc, mostly preferred by major Hollywood movie studios to store their high definition content is protected from unauthorized access, by digital rights management technology. Digital rights management restricts the use of discs by imposing several encryption techniques in which Advanced Access Control System, Blu-ray disc+ are among them. In order to remove the protection, many ripping tools are available in the internet. Instead of paying for the softwares, a method of removing protection from Blu-ray is explained here. In this paper, decryption and streaming of Blu-ray video on MAGIK board is accomplished using the libraries provided by Videolan organization. The MAGIK (Media Accelerated Graphics Innovation Kit) board is a computer on module based on NXP's i.MX6 processor. Dynamic link libraries are obtained by cross compiling the VLC libraries. Finally with the help of these DLL's, Blu-ray decryption and playback is accomplished.

Keywords: Blu-ray, Advanced Access Content System, Blu-ray disc+, MAGIK board, VLC libraries.

Introduction

Digital rights management aims at securing copyrighted data from unauthorized access. The existing protection mechanisms like encryption, cryptography, watermarking, licenses and contracts such as license agreements are the means of digital rights management techniques that are implemented on copyrighted content. By the introduction of this technology, owners of copyrighted data are in the gain of profit. However, the legal users are not able to enjoy their purchased content resulting in limit of fair use [1]. Restrictions such as limited number of copies, disturbance during playback is not tolerable since an authorized user has the rights to do anything with their purchased content. This paper aims at removing the protection employed on Blu-ray discs so that the legal user can make several copies of it and view the Movie later. Although many softwares are available in the Internet which can remove protection, they are all licensed and paid softwares. Without paying for the softwares, we can accomplish this job using VLC libraries. Compiling and Building these libraries results in dynamic linked libraries that can be placed inside the VLC folder in Program files path of "C" drive. Along with the many companies who adopted Digital rights management technology, Blu-ray disc association also started to use Digital rights management techniques to fight against piracy issue. Advanced Access Content System and BD+ are the 2 methods that need to be concentrated.

In Advanced Access Content System, 128 bit keys generated by the Advanced Encryption Standard are used. The content owner provides the content to Advanced Access Content System licensing organization in the form of titles, which can be simply the movie name itself. These titles are encrypted using the 128-bit title key that is subsequently encrypted by media key. Media key is stored in Media key block which is unique for each licensed player. Unique serial numbers are embedded on pre-recorded discs that cannot be duplicated on user's recordable media [2] [3].

Blu-ray disc+, at its core, is a virtual machine running on playback engine based on Self protecting digital content concept. Security keys are issued to every Blu-ray disc+ licensed player. The content code is executed every time when a Blu-ray disc+ protected disc is inserted into Blu-ray player [2].

MAGIK Platform

The hardware implementation involves MAGIK platform consisting of a carrier board and system on module board. MAGIK is a computer on module based on Smart Mobility Architecture (SMARC) standard specified by Standardization Group of Embedded Technologies. SMARC specification aims at building computer on modules with low power consumption. The system on module (SOM) board can be referred to as system on chip (SOC) since it contains all the necessary functional units of a system. SOM board of MAGIK platform contains i.MX6 processor as its core processor and memory blocks as shown in Fig.1. To access the use of peripherals and connectors, Carrier board is deployed together with the SOM boards to

function as an embedded computer on a single circuit board. Carrier board consists of interfaces such as HDMI, LCD, Camera, and USB as shown in figure 2. The SOM board is placed on the carrier board shown in Fig. 2, finally forming an embedded system for multimedia applications.



Figure 1. MAGIK2 Carrier board

I.MX6 Processor

The i.MX6 series processors are based on ARM Cortex-A9 processors with solo, dual and quad core. It incorporates several dedicated hardware accelerators to achieve the targeted multimedia high performance. Main application areas where i.MX6 processors are used extensively includes infotainment systems, human machine interface systems, video processing and audio playback systems. Because of the advanced security feature provided by these processors [4] i.MX6 processor is being used on our SOM board as depicted in Fig.2. Using MAGIK board an infotainment system is built for Blu-ray video streaming.

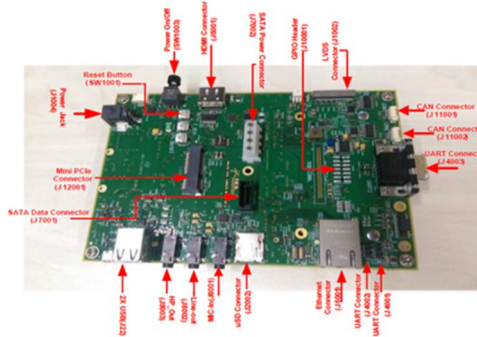


Figure 2. I.MX6 Processor based MAGIK SOM board

Proposed Work

Infotainment system refers to the combination of information and entertainment. Basically, it is an embedded system mainly focused to support multimedia distribution among users. Using MAGIK SOM board and Carrier board with the necessary interfaces being enabled, an infotainment system is built as shown in Fig.3. Blu-ray decryption is done in the Test PC followed by the streaming of video to HDMI display.

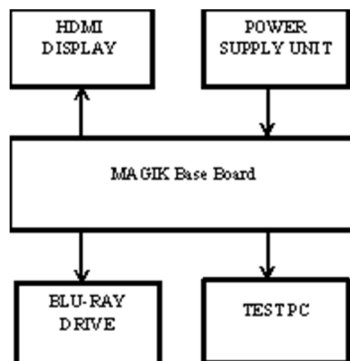


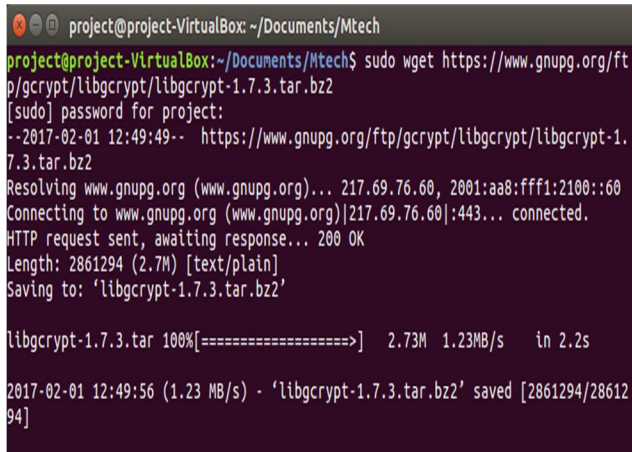
Figure 3. MAGIK based Infotainment system

Decrypting Blu-ray

The libraries necessary to decrypt the encrypted Blu-ray can be obtained in the Videolan website as mentioned in [5]. Libbluray, Libbdplus and Libaacs are the libraries that are necessary for decryption. Along with these, the dependency libraries such as libgrypt, libpgg-error, zlib, libxml2 and libpng are required. Linux platform is used to carry out the compiling process since compiling in Windows platform is a tedious process. Using the basic linux commands we have obtained the dynamic linked libraries. The commands used here are,

```
$ sudo apt-get install
$ ./configure
$ sudo make install
```

Before starting compilation process, we have created a folder wherein all the resulting files will be saved. The following figures show commands in linux terminal window for a single library file compilation. The same has to be followed for all the other libraries. Fig.4 and Fig.5 shows the terminal window in linux platform for downloading the VLC libraries in zip format and extracting it.

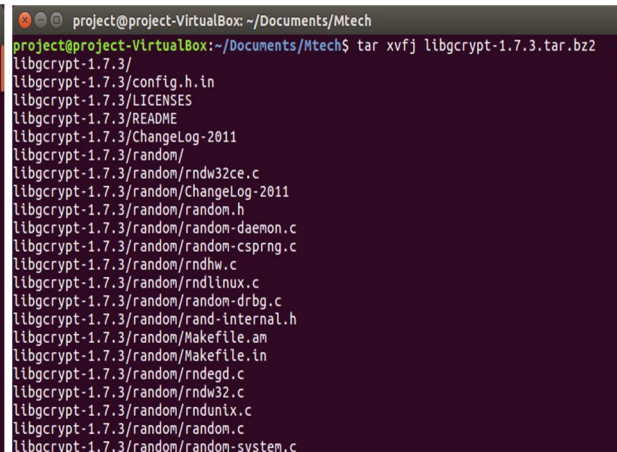


```
project@project-VirtualBox: ~/Documents/Mtech
project@project-VirtualBox:~/Documents/Mtech$ sudo wget https://www.gnupg.org/ftp/gcrypt/libgrypt/libgrypt-1.7.3.tar.bz2
[sudo] password for project:
--2017-02-01 12:49:49-- https://www.gnupg.org/ftp/gcrypt/libgrypt/libgrypt-1.7.3.tar.bz2
Resolving www.gnupg.org (www.gnupg.org)... 217.69.76.60, 2001:aa8:fff1:2100::60
Connecting to www.gnupg.org (www.gnupg.org)|217.69.76.60|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2861294 (2.7M) [text/plain]
Saving to: 'libgrypt-1.7.3.tar.bz2'

libgrypt-1.7.3.tar 100%[=====] 2.73M 1.23MB/s in 2.2s

2017-02-01 12:49:56 (1.23 MB/s) - 'libgrypt-1.7.3.tar.bz2' saved [2861294/2861294]
```

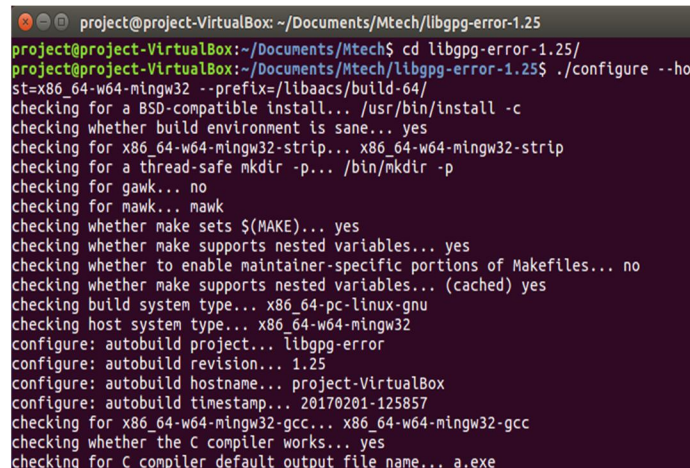
Figure 4: Command to download the library files



```
project@project-VirtualBox: ~/Documents/Mtech
project@project-VirtualBox:~/Documents/Mtech$ tar xvfj libgrypt-1.7.3.tar.bz2
libgrypt-1.7.3/
libgrypt-1.7.3/config.h.in
libgrypt-1.7.3/LICENSES
libgrypt-1.7.3/README
libgrypt-1.7.3/ChangeLog-2011
libgrypt-1.7.3/random/
libgrypt-1.7.3/random/rndw32ce.c
libgrypt-1.7.3/random/ChangeLog-2011
libgrypt-1.7.3/random/random.h
libgrypt-1.7.3/random/random-daemon.c
libgrypt-1.7.3/random/random-csprng.c
libgrypt-1.7.3/random/rndhw.c
libgrypt-1.7.3/random/rndlinux.c
libgrypt-1.7.3/random/random-drbg.c
libgrypt-1.7.3/random/rand-internal.h
libgrypt-1.7.3/random/Makefile.am
libgrypt-1.7.3/random/Makefile.in
libgrypt-1.7.3/random/rndegd.c
libgrypt-1.7.3/random/rndw32.c
libgrypt-1.7.3/random/rndunix.c
libgrypt-1.7.3/random/random.c
libgrypt-1.7.3/random/random-system.c
```

Figure 4: Command for extracting the library file

In Fig.6 and Fig.7, the command for cross compilation and building the libraries is shown in terminal windows.



```
project@project-VirtualBox: ~/Documents/Mtech/libpgg-error-1.25
project@project-VirtualBox:~/Documents/Mtech$ cd libpgg-error-1.25/
project@project-VirtualBox:~/Documents/Mtech/libpgg-error-1.25$ ./configure --host=x86_64-w64-mingw32 --prefix=/libaacs/build-64/
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for x86_64-w64-mingw32-strip... x86_64-w64-mingw32-strip
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking whether to enable maintainer-specific portions of Makefiles... no
checking whether make supports nested variables... (cached) yes
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-w64-mingw32
configure: autobuild project... libpgg-error
configure: autobuild revision... 1.25
configure: autobuild hostname... project-VirtualBox
configure: autobuild timestamp... 20170201-125857
checking for x86_64-w64-mingw32-gcc... x86_64-w64-mingw32-gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.exe
```

Figure 5: Command for configuring the libraries with respect to the host processor x86

The obtained DLL file after compilation process is present in the same folder where we created in the starting process as mentioned before. It can be seen in Fig. 8. The final output i.e. libaacs.dll, libbdplus.dll and libbluray.dll is placed inside VLC folder as shown in Fig. 9.

```

project@project-VirtualBox: ~/Documents/Mtech/libgpg-error-1.25
config.status: creating src/Makefile
config.status: creating tests/Makefile
config.status: creating lang/Makefile
config.status: creating lang/cl/Makefile
config.status: creating lang/cl/gpg-error.asd
config.status: creating src/versioninfo.rc
config.status: creating src/gpg-error.w32-manifest
config.status: creating src/gpg-error-config
config.status: creating config.h
config.status: executing depfiles commands
config.status: executing libtool commands
config.status: executing po-directories commands
config.status: creating po/POTFILES
config.status: creating po/Makefile

libgpg-error-1.25 prepared for make

Revision: 6d834f8 (28035)
Platform: x86_64-w64-mingw32

project@project-VirtualBox:~/Documents/Mtech/libgpg-error-1.25$ make
make all-recursive
    
```

Figure 6. Command for building the libraries

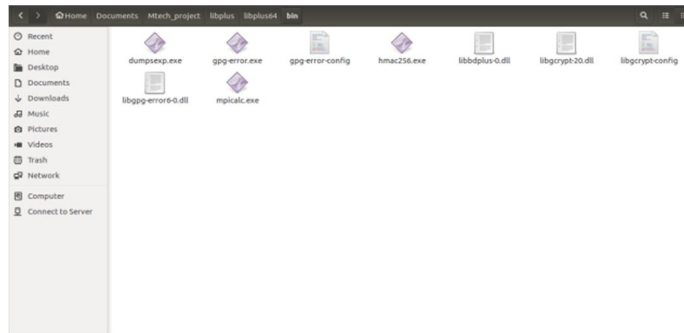


Figure 7. DLL files after compilation process

Name	Date modified	Type	Size
Unspecified (18)			
plugins	23-09-2016 10:58	File folder	
skins	10-10-2016 12:01	File folder	
AUTHORS	10-10-2016 12:01	Text Document	17 KB
COPYING	10-10-2016 12:01	Text Document	18 KB
libaacs.dll	16-04-2016 01:47	Application extens...	34 KB
libbluray.dll	16-04-2016 01:47	Application extens...	34 KB
libdplus.dll	16-04-2016 01:47	Application extens...	34 KB
libmmbd.dll	16-04-2016 01:47	Application extens...	34 KB
libvlc.dll	10-10-2016 12:01	Application extens...	147 KB
libvlc.dll.manifest	10-10-2016 12:01	MANIFEST File	1 KB
libvlccore.dll	10-10-2016 12:01	Application extens...	2,617 KB
NEWS	10-10-2016 12:01	Text Document	167 KB
README	10-10-2016 12:01	Text Document	3 KB
THANKS	10-10-2016 12:01	Text Document	6 KB
vlc	10-10-2016 12:01	Application	132 KB
vlc.exe.manifest	10-10-2016 12:01	MANIFEST File	2 KB
vlc	10-10-2016 12:01	IconView ICO File	72 KB
vlc-cache-gen	10-10-2016 12:01	Application	120 KB

Figure 8. DLLs placed inside VLC folder

Conclusion

An infotainment system built using MAGIK2 SOM and Carrier board in order to stream Blu-ray videos is discussed in this paper. Considering the advanced features supported by I.MX6 processor family, we have used it on our infotainment system. Coming to the decryption part, without the use of third party software, decrypting the Blu-ray using VLC libraries is discussed along with the obtained results. Once the Blu-ray is decrypted, the purchased user can make several copies of it, as a back-up. Paying for third party software’s license is avoided and also the cross compiling process is simple.

References

- [1] Amber Sami Kubesch and Stephen Wicker, "Digital Rights Management: The Cost to Consumers," IEEE Proceedings, vol. 103, no. 5, pp. 726-733, May. 2015.
- [2] Dell (2006) "Blu-ray Disc™ Next Generation Optical Storage: Protecting Content on the BD-ROM" Available <http://www.dell.com/downloads/global/vectors/brcp.pdf>
- [3] DaeYoub Kim and MiSuk Huh, "Improved AAC3 Framework for Private Digital Contents," in Digest of Technical papers on International Conference on Consumer Electronics, 2009, paper 6.4-2, pp 1-2.
- [4] NXP Semiconductors, "i.MX 6Solo/6DualLite Automotive and Infotainment Applications Processors Data Sheet", IMX6SDLAEC, Rev.7 Nov.2016
- [5] Videolan Projects, Available <http://www.videolan.org/projects/>