

Encryption for camera's

A study to encrypt pictures, clips and more

A study by: NovemberBravo

Date: 24 December 2016

Table of Contents

Introduction.....	2
The Question of this study.....	3
My solutions.....	3
Solution 1: Special firmware on the camera's.....	3
Solution 2: Special firmware on a SD card AkA Self Encrypting SD cards.....	4
Solution 3: A special SD to Mirco SD adapter.....	5
Solution 4: External Encrypting Device.....	6
Conclusion.....	6
References.....	7

Introduction

A few days before writing this study I came [across this](#) article on Vice Motherboard NL. The article tells about an open letter 150 journalists wrote to camera manufactures to urge them to build in encryption into their camera's. This because allot the earlier mentioned journalists go to countries which don't have freedom of speech.

In the open letter they write the following:

“Without encryption capabilities, photographs and footage that we take can be examined and searched by the police, military, and border agents in countries where we operate and travel, and the consequences can be dire.

We work in some of the most dangerous parts of the world, often attempting to uncover wrongdoing in the interests of justice. On countless occasions, filmmakers and photojournalists have seen their footage seized by authoritarian governments or criminals all over the world. Because [the contents](#) of their cameras are not and cannot be encrypted, there is no way to protect any of the footage once it has been taken. This puts ourselves, our sources, and our work at risk.

Many technology companies have in recent years embraced encryption technology, often including it in their products and enabling it by default. Indeed, encryption has, in some sectors, become an industry-best practice. Apple's iPhones encrypt all data stored on them by default, as do many phones running Google's Android operating system; text messages and voice calls made with WhatsApp, iMessage, FaceTime, and Signal are all protected using end-to-end encryption technology; and laptops and desktop computers running modern versions of Microsoft Windows and macOS encrypt all data stored by default too.

However, we face a critical gap between the moment we shoot our footage and the first opportunity to get that footage onto more secure devices.” (Timm, 2016)

As you can read in the part of the letter above [here](#) they are facing authoritarian governments, police, terrorists and other people that don't want that the journalists do their work. They also talk about some devices like the iPhone that have encrypted drives by default.

In the last sentence they talk about “a gap”. That gap is the time between making the content and transferring the content onto a secure device that has encryption. They want the camera manufactures to solve that gap problem but apparently they don't see it as a problem. Now since the camera manufactures won't do something about it maybe I can think of some way to help the journalists. And that is what this paper is about. Find a way for the journalists to help them secure there footage.

Now I must admit up front that my I.T. and hacking skills at the moment of writing this aren't up to par with what other hackers can do I think it will be mostly suggestions in this study, not concrete solutions.

The Question of this study

The question of this study is:

How can the content created by journalists be stored encrypted onto a saving medium with the technology we have right now?

My solutions

Now I think there are a few ways to fix the 'gap' problem. The following pages contain my solutions for the problem.

Solution 1: Special firmware on the camera's

On some camera's these days you can put special firmware. With this firmware you can unlock special features on the camera's. For instance for Canon camera's you got Magic Lantern.

“Magic Lantern is a software enhancement that offers increased functionality to the excellent Canon DSLR cameras. We have created an open framework, licensed under GPL, for developing extensions to the official firmware.

Magic Lantern is not a "hack", or a modified firmware, it is an independent program that runs alongside Canon's own software. Each time you start your camera, Magic Lantern is loaded from your memory card. Our only modification was to enable the ability to run software from the memory card.

ML is being developed by photo and video enthusiasts, adding functionality such as: HDR images and video, timelapse, motion detection, focus assist tools, manual audio controls much more.” (Magic Lantern, 2013)

The Magic Lantern firmware is an add-on to the standard Canon firmware that is running on the camera's. It has features that the Canon camera's don't have out of the box. Features that include encryption of footage.

I came across a post on the Magic Lantern forums.

“io_crypt is a module which automatically encrypts .CR2 and .JPG while you shoot them.

The original file content is never written to card, so there is no way to restore the image content by reading the raw sectors etc.

You can choose between different modes and security levels.

This was formerly discussed there and was requested already a few times.” (g3gg0 , 2014)

In the post a member of the forum explains a piece of software that he has created. The software is called io-crypt. With io_crypt you can encrypt all your footage while you shoot it.

Solution 2: Special firmware on a SD card Aka Self Encrypting SD cards

Another possibility is to hack the firmware on the SD card to encrypt the contents. It can be done. Some SD cards are hackable. They have small micro controller some of which can be hacked and can run some code. I don't know if the micro controllers are powerful enough to run encryption function. Also not everybody is techsavvy enough to start hacking SD cards. Off course you could ask a hacker or a SD card manufacturer to make Self Encrypting SD cards.

Solution 3: A special SD to Micro SD adapter

One other way is to do something with SD to Micro SD adapters.

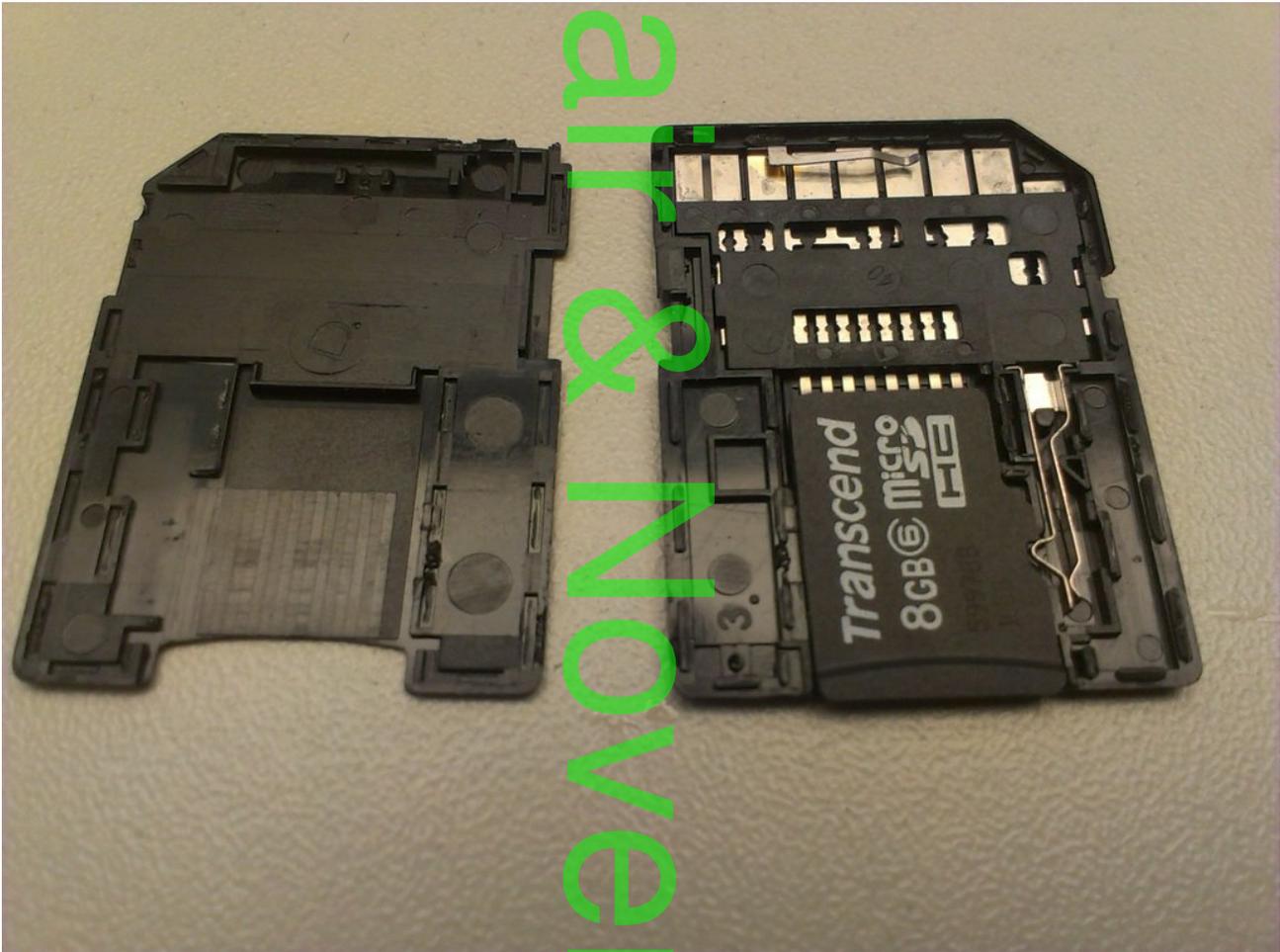


Illustration 1: The insides of a typical SD to Micro SD adapter. (noq2, 2013)

As you can see above there isn't much in the adapter. The big leads from the SD just get smaller into leads for the Micro SD card size. This means there is space for a little circuit board. On this circuit board you can place a micro controller that encrypts the data that comes in. With this idea you could use normal Micro SD cards that are wide spread in the world. A problem with this is that the Micro SD cards probably can't write fast enough to handle the huge amounts of data.

Solution 4: External Encrypting Device

This is a solution I have been brainstorming amount the most. My idea/solution is the following: We need a SD adapter that is wired up to a micro controller. On that micro controller is an encryption functionality that encrypts the data that is being written onto the SD card. The adapter is inserted into the camera SD slot so that it can extract the contents of that camera.

I want to try to make a prototype to test this idea. For more about this prototype see the chapter Prototypes.

Conclusion

The conclusion of the study is the following:

To solve the problem of the journalists and do it the way they want it the best way is to install the Magic Lantern and io_crypt firmware. This way they can shoot their footage and don't worry about any authoritarian governments that don't want the footage out there. For now I think this is the best solution for the journalists to do.

References

Timm, T. (2016, 14 december). *Over 150 filmmakers and photojournalists call on major camera manufacturers to build encryption into their cameras*. Accessed on 25 december 2016, from <https://freedom.press/news/over-150-filmmakers-and-photojournalists-call-major-camera-manufacturers-build-encryption-their-cameras/>

noq2. (2013, 12 december). *Micro SD card adapter surgery...* [Online image] Download on 28 december 2016 from <https://blog.noq2.net/micro-sd-card-adapter-surgery.html>

Magic Lantern. (2013) *About Magic Lantern*. Accessed on 30 december from <http://www.magiclantern.fm/about.html>

g3gg0. (2014, 2 february). *io_crypt - encrypt your photos while you shoot them*. Accessed on 30 december 2016 from <http://www.magiclantern.fm/forum/index.php?topic=10279.0>