Report Exercise 1

Software Security

Gabor Szivos – 1227443

188.959 – SS 2017

May 7, 2017

Contents

1 Introduction

2 Related Work

As it is likely when getting in touch with state of the art technology, the number of related scientific papers seems to be limited. The most important research done on this field that could have been obtained is briefly described in this section, to give readers a short introduction on the existing literature. The most outstanding work related to the topic examined in this state of the art report is titled "A VHDL Architecture for Auto Encrypting SD Cards" and was published by the University of Gothenburg in November 2016 [DR16]. To summarize, the students working on this master's thesis designed an encrypted SD-card for journalists.

The approach was based on a hardware solution. An SD-Card adapter was designed, that applies to the SD-card standard, in other words, the auto-encrypting SD had the size and shape of a usual SD card. Inside this seemingly normal SD-card there was an encryption hardware module, based around a FPGA and a publicly available intellectual property core, which was used for encryption.

A speciality about this approach is that the design aims the SD-card to be used by journalists, who work in "destabilized areas". By this the authors of the thesis mean countries, where a journalists takes big risks when taking photographs and trying to get these photographs out of the country. This is the point, where plausible deniability takes effect: When a new photograph is saved, it first is encrypted and then hidden on the file system, so no traces of the photographs may be found and the journalists are safe.

The encryption of the data is realised with a ChaCha20 algorithm that is implemented in the used FPGA. For the encryption a pair of public and private keys is created outside of the SD card. The public key gets stored on the SD card afterwards. The decryption

is performed outside of the SD with the use of the private key. It is important here to notice, that previewing the photographs is possible as long as the SD card is powered up.

What is missing in the described approach is a hardware implementation. All of the work that was done to achieve what was achieved in this project was carried out on a simulator. Even though the writers of this thesis achieved all of their goals it is inevitable to thoroughly test this solution as a fully developed hardware platform to proof the applicability of the proposed solution.

An issue that has not been addressed completely in our opinion is the plausible deniability. Even though the proposed solution "hides previously created encrypted files from the camera", it is not assured that this file hiding is sufficient towards forensic analysis.

Another approach to this issue, especially focused on plausible deniability was developed by Adam Skillen and Mohammad Mannan at the Concordia University in Montreal, Canada [SM13]. This solution is basically an app ("Mobiflage") that stores photographs on a deniable file system, which means hiding encrypted volumes within random data on the external storage of a mobile device. The paper was published in 2013.

Google's Android operating system was used for the prototypic implementation of Mobiflage. A precondition for the application of Mobiflage is the existence of an external memory (SD-card), as the proposed solution does not support internal memory. Two separate volumes are created on the volumes of the SD-card:

1. An userdata volume, used for settings and application data

2. An auxillary volume, where the photos will be persisted

Mobiflage achieves plausible deniability through plausible deniable encryption (PDE) this technique enables the output of different reasonable and innocuous plaintexts from a given ciphertext. The original plaintext (or the image data) is only revealed if the correct key is entered. This makes the decrypted data seem correct for unauthorized individuals trying to force the disclosure of the encrypted information. As Skillen et. al states, there is a file system for Linux called "Rubberhose" which features PDE. Mobiflage features two modes for saving images:

1. Standard Mode In this mode the so called "decoy" password is entered at boot time and non-sensitive data is displayed. The storage medium is mounted as Mobiflage isn't installed.

2. PDE mode In the PDE mode the user enters the "trust" password at boot time and the hidden data may be accessed on the SD-card.

The most important aspect here is that the source of the image is a smartphone or tablet and not a DSLR or any other kind of camera. This fact reduces the time from the capture of the image to the secure persistence on the memory drastically. From the other point of view it might not be sufficient enough for a journalist to take pictures with a smartphone, instead he relies on professional equipment like a DSLR to achieve the desired quality of work.

What is missing in this approach is the universality of the solution. The clear advantage of the approach of Davidsson et. al [DR16] is that the SD-card may be used in any device, regardless of DSLR or smartphone.

presentation of existing overview literature / state of the art literature in the field

what was presented there? what were the main results?

is something open/missing?

3 Method

4 Results

5 Discussion

6 Conclusion

References

[DR16] Alexander Davidsson and Torbjörn Rasmusson. A vhdl architecture for auto encrypting sd cards. Master's thesis, 2016. 36.

[SM13] Adam Skillen and Mohammad Mannan. On implementing deniable storage encryption for mobile devices. 2013.