Report Exercise 1

Software Security

Gabor Szivos – 1227443

188.959 – SS 2017

May 6, 2017

Contents

ABSTRACT

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. 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 thorougly test this solution as a fully developed hardware platform to proof the applicability of the proposed solution. [DR16]

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.