Multifactor, multiple people. Authentication approach for unlocking encrypted fies.

Yuri Gorokhov *, **Lars Noergaard Nielsen** *

*University of California, San Diego

Submitted as part of graduate security course CSE227.

Proposal of a system to authenticate access to encrypted files using both Multifactor and multiple people, across different locations. Making sure that files are only accessible with the consent of all involved participants.

Multifactor | Encryption

Introduction

Controlling who has access to files is often a requirement in industry and various other contexts. Systems for dealing with information that only is accessible with multiple peoples consent is therefore interesting to investigate. Software for file access control purposes include Dell Identity Manager[2], User Lock Access Manager [1] and native OS support such as an Access Control List. These systems is not adressing security as such, as not providing encryption capabilities. Common for these solutions is that file access is administered centrally by a administrator. We propose an approach were users actively set file permissions by agreeing to encrypt files by their common consent, only allowing access to these files when all parties has responded to the access request. The latter step is additionally secured by Mulfifactor Authentication.

System Description

The proposed system is composed of a user client, harddrive client and a verification server.

A benefit from this central point of contol is that the server can deny access to a file, even though participants grant access, which might be useful in some access schemes.

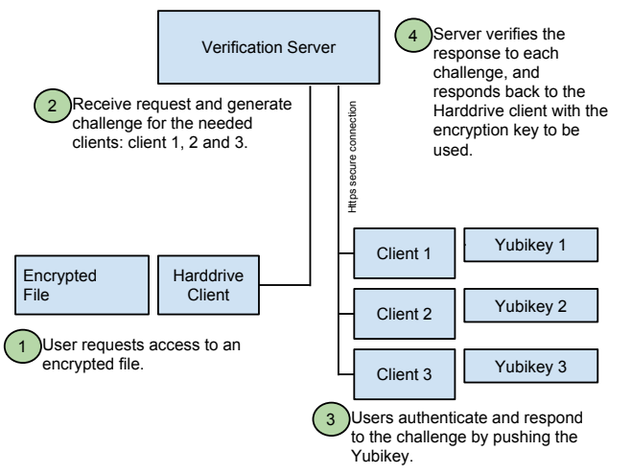

Fig. 1. System components and interaction. 4 major steps to grant access.

Multifactor authorization: Yubikey

In this work we choose Yubikey for Multifactor authentication for several reasons: It provides a simple procedure for the user - only a physical touch on the device is neccesary to allow the device to respond to the presented challenge.

Encryption scheme

This sections presents the encryption scheme used, to ensure that decryption of the file is only possible when responses from all participants and their Yubikey challenges are retrieved.

Discussion

Discussion on strenghts and weaknesses of the solution

ACKNOWLEDGMENTS. This work was supported by..

1. **http://www.isdecisions.com/lp/userlock/userlock-windows-network-security.htm?gclid=CMfPI-rqisQCFciBfgodhxwAmQ**

2. **http://software.dell.com/products/identity-manager-data-governance/**

Reserved for Publication Footnotes

Table 1. Table caption

Treatments	Response 1	Response 2
Treatment 1	0.0003262	0.562
Treatment 2	0.0015681	0.910
Treatment 3	0.0009271	0.296