Technische Universität München
Chair for Network Architectures and Services
Prof. Dr.-Ing. Georg Carle

MA/BA

Privacy Preserving Multi User Network File System

Introduction

Cooperation between humans typically requires file sharing. In corporate environments this is often implemented by services like Samba. Privateers, however, use Cloud services like Dropbox. An important feature of every file sharing solution is access control, i.e., the capability to restrict access to individual files or folders to a user or a user group.

Problem

One common problem is that administrative personnel can easily bypass „conventional" access control mechanisms based on, e.g., access control lists and spy on the data. Access control can also be implemented using cryptography. However, emulating quite complex access control policies by encryption is challenging. A quite novel encryption mechanism designed to solve this issue is Attribute-based Encryption (ABE). Here, a central entity creates decryption keys with embedded attributes for users, e.g., the name of a user group the key owner is member of. For the encryption of files a different key is used. A specific features of ABE is that an access policy can be cryptographically embedded into cipher text. Later, only those users with matching attributes in their decryption key can decrypt the data. Unfortunately, the central ABE key ussuer is still able to bypass ABE access control when she issues a key with required attributes to herself.

Task Description

In the beginning of this thesis thorough analyses of requirements on file sharing services and properties of ABE need to be done and the question answered how well suited ABE is for file sharing. Furthermore, different attackers models need to be defined and the attacker's ability to break the access control assessed. Especially Master's students need to investigate the question for an alternative to ABE. Some features of ABE can be emulated by conventional symmetric and asymmetric cryptography. This creates a distributed solution in contrast to the centralized ABE approach. Which advantages and disadvantages has such a system compared to ABE? A proof of concept implementation of the privacy-preserving and secure file sharing featuring the selected cryptographic approach needs to be done as well.

Requirements

This thesis requires knowledge concerning cryptography as well as operation systems (Linux), as the prototype function needs to be embedded into the OS, e.g., using FUSE.

Miscellaneous

This thesis can be performed in German or English.





Further Information: Dr. Holger Kinkelin und Marcel von Maltitz
(lastname@net.in.tum.de)
Chair for Network Architectures and Services