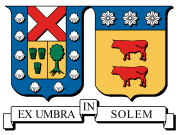
UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
VALPARAÍSO, CHILE



P2P USER IDENTIFICATION: USERNAME/PASSWORD

Memoria presentada como requerimiento parcial
para optar al título profesional de
INGENIERO CIVIL EN INFORMÁTICA
por

Rodrigo German Fernández Gaete

Comisión Evaluadora:
Xavier Bonnaire
Horst von Brand

JUNIO 2013

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
VALPARAÍSO, CHILE

TÍTULO DE LA TESIS:
P2P USER IDENTIFICATION: USERNAME/PASSWORD

AUTOR:
RODRIGO GERMAN FERNÁNDEZ GAETE

Memoria presentada como requerimiento parcial para optar al título profesional de **Ingeniero Civil en Informática** de la Universidad Técnica Federico Santa María.

Profesor Guía _____
Xavier Bonnaire

Profesor Correferente _____
Horst von Brand

Junio 2013.
Valparaíso, Chile.

...

Índice general

Índice de figuras

Thanks

Abstract

With more than 1,5 billion active users, social networks are one of the most popular Internet services. The problem is that social networks services of today are not scalable, having very high maintenance costs. On the other hand, P2P services are robust, scalable and self-organized by nature, but have a complete different architecture with new problems and unique requirements. Therefore, this document focus on finding the existing problems in the implementation of a P2P social networking service. We thoroughly investigate the requirements and features of social networks, along with the challenges facing a P2P implementation. The main features discussed are (a) the users login, (b) users posts, (c) users contacts list, (d) groups and organizations among users, (e) privacy settings and (f) integration with other services and applications. After the analyzis of these features with their current solutions, we discuss the problems that hinder the satisfaction of the system requirements, ending with the identification of today's main challenges. Among the problems identified are (1) deficiencies in the implementation of complex search, which do not allow real-time feedback and need to improve the quality and accuracy of the results obtained, (2) lack of proposals for enhanced security system for these systems, especially related to selfish users control and encryption systems, and (3) vulnerabilities in the entry mechanisms of the system and (4) management of selfish users.

Keywords: Social networks, p2p.

Chapter 1

Introduction

The subject of securely establishing stable identities in P2P systems has been previously studied, for instance by Aberer, Datta and Hauswirth [5]. The need for identities mainly arose from technical concerns, such as handling dynamic IP address assignment, or avoiding Sybil attacks [6]. Authentication of a node is done via a signature key, automatically generated and stored on the node.

Traditionally, P2P networks identified the different nodes that compose the system, but not the user behind each one of them as a different being. As P2P systems grow in funciontalities, the need to identify users inside the network arose.

P2P networks are conformed by nodes with unique identifiers that map to their own IP address. That way is easy to differenciate them between each others, but it is not enough to handle user identities. To let an user log in to the network using different nodes, a user identity *proof* is needed. That is because all nodes the P2P networks shares the same functionalities, so anybode can identify as an user if it can prove it for the other peers. For this to work, the proof of identity need to be:

Unique asdasd

As P2P systems began providing more complex functional- ity [2], [3], [4], [7], the need to authenticate users, rather than nodes, arose. It seems that often, authentication via a signature key has been carried over to this problem. While a solution of automatic identification of a node is preferable as long as users use a single device, equating a node with a user fails as users increasingly access services from multiple devices. Illustrative is the case of backup systems, where an impor- tant use case is to restore data on a different system from where it was backed up. Here, two different approaches to authen- tication have been taken. All approaches build on encrypting backed up content, and the approaches vary in whether the keys are randomly derived [7], or derived from a password [8]. In the former case, a user must manually back the keys up, as these keys are required to restore the backup. The systems deriving a key from a password are related to our proposed protocol, and use some related techniques. However, to the best of our knowledge, they do not consider the additional protocols required surrounding password authentication, such as remembered logins, and recovering lost passwords. Some P2P storage systems also use techniques which

are related to ours. For example, the DHT-based systems GNUnet and Freenet use keyword strings to derive a public-private key pair whose private key is used to sign data and the hash of the public key to identify the data in the storage. Both of these systems use a keyword string as a seed to a pseudo- random number generator that produces the key pair [9], [10]. Knowing only the memorable keyword string the user can store and retrieve information. Related to forgotten passwords, recovery of information in a P2P scenario has been studied by Vu et al. [11] who proposed a combination of threshold-based secret sharing with delegate selection and encrypting shares with passwords. Frykholm and Juels [12] proposed a password-recovery mechanism based on security questions very similar to our protocol for the same task. They offer better, information- theoretic security properties, something not applicable to our scenario. We treat the subject of password change, which is not applicable to their scenario, although their proposal could be extended to support password change using our techniques.

Chapter 2

P2P Networks

Chapter 3

P2P Identification Schemes

Chapter 4

Conclusions

Bibliography