Chapter 13
Entity Authentication and Trust Validation in PKI Using Petname Systems

Md. Sadek Ferdous
University of Glasgow, UK

Audun Jøsang
University of Oslo, Norway

ABSTRACT

Recognition of identities and certainty about identity ownership are crucial factors for secure communication in digital environments. Identity Management Systems have been designed to aid users as well as organisations to manage different user identities. However, traditional Identity Management Systems are primarily designed to facilitate the management of identities from the perspective of the service provider, but provide little support on the user side to manage organisational identities. Public Key Infrastructures (PKI) is the primary tool in aiding users to manage such identities on their sides as well as to establish trust during online transactions. Nevertheless, the complexities and difficulties involved in managing and understanding such certificates from the general public's point of view are overlooked. This causes vulnerabilities that open up for serious attacks such as identity theft and Phishing. Petname Systems have been proposed for managing organisational identities on the user side in order to improve the user friendliness and to strengthen security. This chapter provides an analysis of the Petname Model by describing its history and background, properties, application domains, and usability issues, and explains how a Petname System can be effectively combined with the PKI to recognise identities and impose certainty by validating the user trust on those identities. The chapter also presents an analysis on two applications that integrate the Public Key Infrastructure with the Petname Model.

DOI: 10.4018/978-1-4666-4030-6.ch013

INTRODUCTION

Entity identification and trust are two important factors that help people decide whether or not to engage in transaction with other people in the real world. We humans inherit these qualities as part of our human endeavours in the society, and as our boundary of social interactions expand over time so does our ability to utilise those qualities to our benefit. But trust can misleads us while engaging in transactions with other human beings due to the complex and unpredictable nature of human behaviour, and when expectation does not meet in transaction, it results in erosion of trust. With the ever growing expansion of the Internet, technologies have enabled us to engage in transactions much like the way we transact in real world. However, with the absence of the face-to-face interaction, trust assessment through the Internet is typically much more challenging. At the initial growing stage of the Internet, the web and web-based services were not foreseen in its current form and the necessity of formal verification of entity identities was not felt. This led to the omission of the much needed Identity Layer. This causes the identification of entities to be very difficult in online world which in turn makes it difficult to establish and validate trust with other entities.

Authentication was subsequently added for verifying the correctness of claimed and assumed identities. Authentication requires prior registration of identities, and is based on a set of security mechanisms combined with a credential or security token. As authentication became necessary for accessing many online services, more and more identities and credentials were issued, and their management became problematic, both for service providers and for users. Identity Management (IdM, in short) Systems were introduced by the industry to facilitate the server-side management of user identities. Initially, the client-side management of user identities was not considered to be an issue. However, many people currently feel overloaded with identities and passwords that security policies require them to memorise. The growing number of identities that users need to handle and the inability of users to comply with credential management policies now makes client (user) side IdM a critical issue. It is important to consider that users need to manage their own identities as well as SP (Service Provider) identities. The latter aspect of IdM has received relatively little attention. Users have been provided with only PKI and digital certificates for identifying and authenticating SPs. In practice PKI on the Internet is used for automatic authentication of SP entities through their domain names. Although technically sound, PKI suffers from serious usability issues which make it difficult for general people to use it effectively and efficiently. This creates precisely the vulnerability that makes phishing attacks potent and successful. Petname Systems can be an effective solution against such threats. In this chapter we highlight the shortcomings of PKI and show how a Petname System can effectively be used to improve security and usability.

An essential part of an IdM is the namespace which provides a set of unique names (identifiers) for all entities it deals with. Different types of namespaces will have different properties. It is desirable that the namespace enables names to be 1) Global, 2) Memorable and 3) Unique (Called "Secure" in Wilcox, 2001). Unfortunately, no single namespace have all the three properties simultaneously (Wilcox, 2001). However, by combining a global namespace with a local namespace, all three properties can be combined (Miller, 2000). A so-called Petname System is a solution for achieving this. The combination of IdM and Petname Systems therefore seems to be an ideal choice for client-side Identity Management.

In this chapter, we present an extensive elaboration of our previous work on Petname Systems that can be found in (Ferdous et al., 2009). In addition, we focus on PKI and show how a Petname System