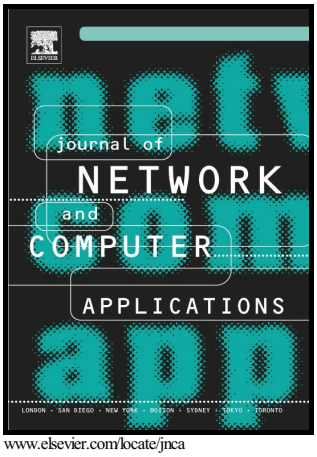
Proxy Re-Encryption: Analysis of Constructions and its Application to Secure Access Delegation

David Nuñez, Isaac Agudo, Javier Lopez



www.elsevier.com/locate/jnca

PII: S1084-8045(17)30107-8
DOI: http://dx.doi.org/10.1016/j.jnca.2017.03.005
Reference: YJNCA1877

To appear in: *Journal of Network and Computer Applications*

Received date: 11 October 2016
Revised date: 17 January 2017
Accepted date: 6 March 2017

Cite this article as: David Nuñez, Isaac Agudo and Javier Lopez, Proxy Re Encryption: Analysis of Constructions and its Application to Secure Acces Delegation, *Journal of Network and Computer Applications* http://dx.doi.org/10.1016/j.jnca.2017.03.005

Proxy Re-Encryption: Analysis of Constructions and its Application to Secure Access Delegation

David Nuñez, Isaac Agudo, Javier Lopez

Network, Information and Computer Security Laboratory (NICS Lab)
Universidad de Málaga, Spain
Email: {dnunez, isaac, jlm}@lcc.uma.es

Abstract

This paper analyzes the secure access delegation problem, which occurs naturally in the cloud, and postulate that Proxy Re-Encryption is a feasible cryptographic solution, both from the functional and efficiency perspectives. Proxy re-encryption is a special type of public-key encryption that permits a proxy to transform ciphertexts from one public key to another, without the proxy being able to learn any information about the original message. Thus, it serves as a means for delegating decryption rights, opening up many possible applications that require of delegated access to encrypted data. In particular, sharing information in the cloud is a prime example. In this paper, we review the main proxy re-encryption schemes so far, and provide a detailed analysis of their characteristics. Additionally, we also study the efficiency of selected schemes, both theoretically and empirically, based on our own implementation. Finally, we discuss some applications of proxy re-encryption, with a focus on secure access delegation in the cloud.

Keywords: Proxy Re-Encryption, Cloud Computing, Access Delegation, Cryptography

1. Introduction

The materialization of the cloud computing paradigm has raised great expectations regarding performance, simplification of business processes, and, foremost, cost reduction. At the same time, these expectations come with new security and privacy risks. Threat scenarios radically change when moving from resources fully controlled by the data owner to resources administrated by third party entities like public clouds. Nowadays, the great majority of cloud systems base their security on preventing potential attackers from accessing internal servers and databases, where users' data is stored. To this end, there is a great variety of measures, with access control systems and network defense techniques being the most prominent. However, the premise of this approach is that the attackers should not be able to break a predetermined security perimeter, where the protected assets (e.g., users' data) reside. These types of measures, although crucial, are often not enough. In addition to external attackers, which may include not only "hackers" but also nation-scale adversaries, accidental data disclosures and insider attacks are also a menacing possibility.

Countermeasures to these threats include the establishment of internal security policies and governance rules, and the reinforcement of access control strategies, but these simply reduce the situation to a trust problem. That is, in the end, there are no actual mechanisms that prevent cloud providers from breaking these measures, either by accident or intentionally, and, in most cases, there is almost no risk of being discovered accessing users' information without their consent. An interesting conflict appears in this scenario – users want to go to the cloud for its benefits, but at the same time, they are unwilling to provide their data to entities that they do not necessarily trust. The adoption of cloud services has been slowed by this dichotomy from the beginning. The introduction of more advanced security mechanisms that enable users to benefit from cloud services and still ensure the confidentiality of their information could help to reduce the trust assumptions in the cloud, and hence, to break the aforementioned dichotomy.

Therefore, it is necessary to depart from the traditional premise that shapes current cloud security and to assume that the measures defined above can be bypassed. A more realistic premise is to assume that the attackers have potential access to users' data [1]. Under this assumption, the only plausible solution is the use of cryptography, so outsourced data is stored in encrypted form. Thus, when traditional security measures fail, attackers will only obtain encrypted data. In a way, the deployed encryption mechanisms become the ultimate safeguard of data confidentiality. A critical principle of this solution is to design the system in such a way that even the provider itself does not have access to the corresponding decryption key; not doing this would again imply a strong trust assumption on the provider. However, a naive combination of this principle with traditional encryption primitives, both symmetric and asymmetric, can hinder the proper processing and sharing of outsourced information and negatively impact the functionality of the system. Therefore, this requirement implies the use of cryptographic primitives that transcend traditional ones, so data confidentiality can be guaranteed, but functionality still remain unaffected.