Securing cloud authentication

Andrea Huszti[a], **Norbert Oláh**[b]

[a]Faculty of Informatics
University of Debrecen
Debrecen, Hungary
huszti.andrea@inf.unideb.hu

[b]Faculty of Informatics
University of Debrecen
Debrecen, Hungary
onorbi@hotmail.com

Abstract

Cloud computing is becoming more and more important in the field of information technology, which faces many security challenges. One of the most important issues is to achieve secure users' authentication.

Several cloud service providers use the well-known password-based technology which requires only a user name and a password, however many known successful attacks have been implemented showing the weakness of this technology. There are some service providers who also require a one-time password, thereby increasing the safety of the system or the password-based system is completed with a cryptographic application running on a certain smart card.

In our proposed two-factor authentication system a person uses a static password and a one-time password for verification. The protocol's main goal was to operate shared resources and shared control among the cloud servers instead of the single server control. The static password is different in case of every cloud server and the one-time password is shared on the provider's side. Since the static password differs in case of every cloud server and none of the servers are familiar with the whole one-time password, we provide protection against internal attackers. Our system is based on the generalization of hash chains - the so-called Merkle tree, where leaves represent the secret shares known by the different cloud servers. In case of external attacks we carried out a security analysis in the Dolev-Yao model and the internal adversaries are seen as malicious, but cautious attackers. By having avoided the asymmetric cryptography we have achieved good efficiency results in our system.

Keywords: Cloud computing, two-factor authentication, internal attackers

MSC: 94A62,94A60