Identity-based Password Registration for Clouds*

Andrea Huszti[a], **Norbert Oláh** [b]

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

[b] University of Debrecen, Doctoral School of Informatics
olah.norbert@inf.unideb.hu

Abstract

Nowadays, we apply various distributed systems (cloud, fog) which consist of multiple, autonomous resources that communicate through a network. These systems are very popular, however, have to face many security challenges. One of the most significant challenges is the secure user authentication. If it is breached, confidentiality and integrity of the data or services may be compromised. In the case of Software as a Service model, the cloud service provider takes responsibility for securing all the data from unauthorized access.

The password usage is an especially common and widespread form of user authentication. Several types of suggestions and solutions exist (i.e. password-authenticated key exchange), as there are several known vulnerabilities as well. These vulnerabilities include various key loggers, dictionary attacks, phishing attacks or stolen passwords from the server.

Boneh and Franklin [1] formalized the notion of Identity-Based Encryption (IBE), which uses bilinear pairings over elliptic curve groups. In IBE setting, the public key of a user can be any arbitrary string, typically the e-mail address. There is no need for Bob to go to the Certificate Authority to verify the public key of Alice. In this way an IBE can greatly simplify certificate management.

The proposed protocol is a secure key exchange protocol where the entity authentication is provided by the identity-based key pair. The registration results in users exchanging password-based long-lived keys with the servers of the provider. Our proposed registration phase is an ideal choice for multi-server authentication. Each server stores the bilinear map of a password

*The presented research has been partially supported by the SETIT Project (no. 2018-1.2.1-NKP-2018-00004), which has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the 2018-1.2.1-NKP funding scheme and supported by the European Union, co-financed by the European Social Fund (EFOP-3.6.2-16-2017-00015).

share, hence if a server is compromised on provider's side real passwords are not revealed. A formal security analysis is also provided. Security of the proposed registration protocol is based on the assumptions that MAC is existentially unforgeable under an adaptive chosen-message attack and Bilinear Diffie-Hellman problem is computationally infeasible in the Random Oracle Model.

Keywords: identity-based cryptography, long-lived key exchange, password, registration

References

[1] Dan Boneh and Matthew K. Franklin, Identity-based encryption from the Weil pairing, *SIAM J. Comput.*, 32 (2003), 586–615.