Identity-based password Registration for Distributed Systems

Andrea Huszti, Norbert Oláh

University of Debrecen
Faculty of Informatics
Department of Computer Science

Budapest
2019.11.08.

Content

Motivation

Definition

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Solutions in practice

OpenStack Identity service (for clouds):

- user name and password (OneLogin)
- Kerberos (Golden Ticket Attack (2015))

Scientific literature

Two-factor-based, centralized:

- 2011 A. J. Choudhury, P. Kumar M. Sain: A Strong User Authentication Framework for Cloud Computing
- 2014 N. Chen, R. Jiang: Security Analysis and Improvement of User Authentication Framework for Cloud Computing

Concept of multiple-server model:

- 2003 J. Brainard, A. Juels, B. Kaliski, M. Szydlo: A New Two-Server Approach for Authentication with Short Secrets (TLS-based)
- 2011 Sood, Sandeep K., Anil K. Sarje, and Kuldip Singh, A secure dynamic identity based authentication protocol for multi-server architecture
- 2016 A. Huszti, N. Olah: A simple authentication scheme for clouds

Our goal

- Distributed system (multi-server authentication)
  1. Robustness
  2. Greater availability
- Mutual key authentication as well as mutual key confirmation (AKC)
- Efficiency
  1. MAC, xor operations and symmetric encryption
  2. ECDH key exchange

Properties

- Identity-based protocol
- no PKI
- Identity-based key pair on both sides, and a key pair for PKG.

Motivation

- bilinear map based (necessary for verifying securely stored passwords)
- instead of TLS like connection (with key exchange and encryption, or signature and encryption), special, optimized messages
- augmented PAKE: server securely stores password, not only a hash, but salted bilinear map of the password
  - slowing down the dictionary attack
- Enable authentication of user and server for multiple servers, with x different keys
- good for automatic long-lived key update (password won't change, just the key)
- security proof in BPR model

Proposed protocol I

User (U)	$P, \gamma P, xP$	Server (S_i)
$Q_U = H_1(ID_U), \gamma Q_U$		$Q_{S_i} = H_1(ID_{S_i}, x_i P, \gamma Q_{S_i}, x_i$
$t, r \in \mathbb{Z}_q^*$ random, $z = H(t)$		
$psw \mapsto (s_1, \ldots, s_n)$ password		
$M_i = \hat{e}(Q_{S_i}, z x_i P + \gamma Q_U)\hat{e}(zP, s_i P)$		
$K_i = \hat{e}(zP, s_i P)$		
	$\xrightarrow{Q_U, zP, M_i, Enc_{K_i}(r)}$	
		$\frac{M_i}{\hat{e}(\gamma Q_{S_i}, Q_U)\hat{e}(Q_{S_i}, x_i zP)} = \hat{e}(zP, s_i P)\ (K_i')$
		$Dec_{K_i'}(Enc_{K_i}(r))$
		$Mac_{K_i'}(r)$
	$\xleftarrow{Q_{S_i}, Mac_{K_i'}(r)}$	
$Mac_{K_i}(r) \stackrel{?}{=} Mac_{K_i'}(r)$		
		Store: $Q_U, \hat{e}(zP, s_i P), zP$

NEMZETI KUTATÁSI, FEJLESZTÉSI
ÉS INNOVÁCIÓS HIVATAL

AZ INNOVÁCIÓ LENDÜLETE

AZ NKFI ALAPBÓL
MEGVALÓSULÓ PROJEKT

This research was 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.

Thank you for your attention!