Securing Cloud Authentication

HU-MATHS-IN
Hungarian Service Network for Mathematics in Industry and Innovations

CHALLENGES

Secure societies – Protecting freedom and security of Europe and its citizens

The Industrial Problem

Cloud computing is a promising technology in the healthcare industry. However handling sensitive health data is challenging. One of the most important issues is the secure entity authentication. If it is breached, confidentiality and integrity of the data or services may be compromised. A secure mutual entity authentication protocol for a cloud environment is required.

Research group

DECRYPT

DECRYPT
UNIVERSITY OF DEBRECEN

Design and provide provable security analysis of cryptographic algorithms and protocols

Company

CCLAB

CCLAB

Common criteria evaluation, Web Application Security, Swiss smart mete
Fido certification

SZÉCHENYI 2020
MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Strukturális és Beruházási Alapok
BEFEKTETÉS A JÖVŐBE

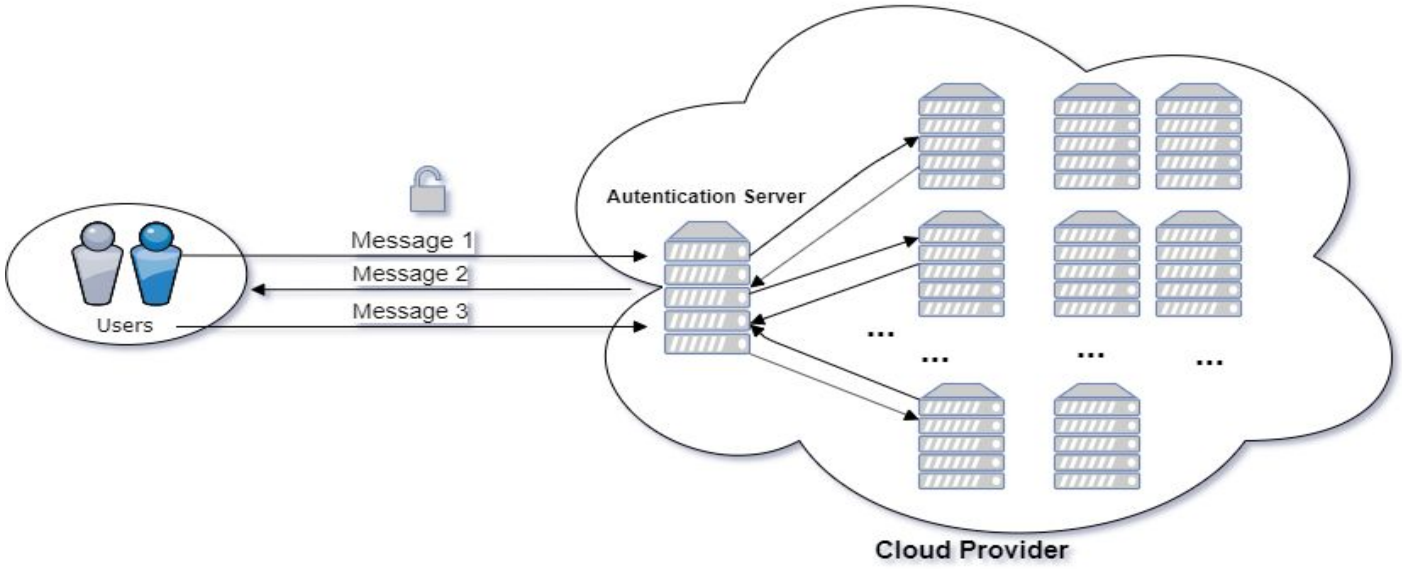
Securing Cloud Authentication

HU-MATHS-IN
Hungarian Service Network for Mathematics in Industry and Innovations

Challenges & Goals

Prevalent single-server solutions might result in single point of failure and vulnerable against offline dictionary attacks. Multiple-server schemes are most of the cases not scalable. Goals are

- to take advantage of distributed systems and apply multiple-server authentication
- to provide robustness, scalability and greater availability
- to provide a security proof of the protocol
- to minimize computational costs by using fast cryptographic operations



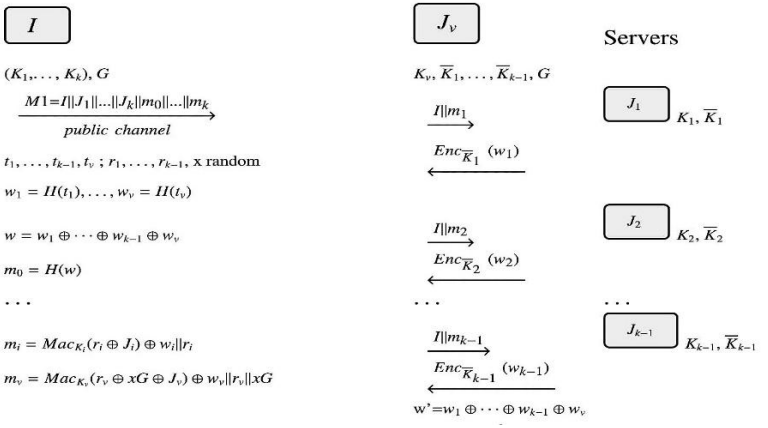
Authentication protocol for the cloud

Securing Cloud Authentication

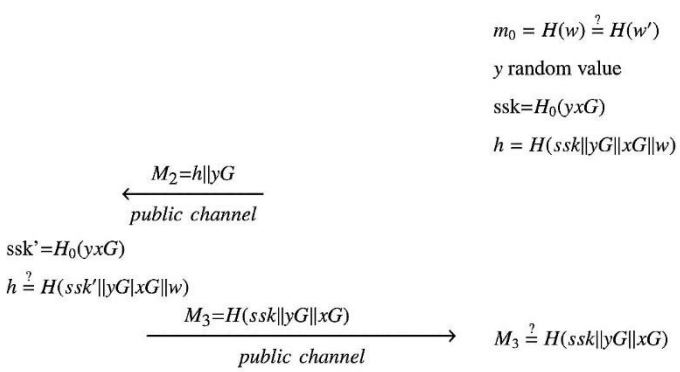
HU-MATHS-IN
Hungarian Service Network for Mathematics in Industry and Innovations

Mathematical and computational methods and techniques applied

- Design an advanced key exchange cryptographic protocol with key confirmation.
- The protocol is analyzed according to the extended Bellare-Rogaway model.
- A complexity theoretic reduction is given which turns an adversary against the protocol into an adversary against a cryptographic primitive.
- Java implementation is created and tested on Microsoft Azure environment.



The formalized protocol I.



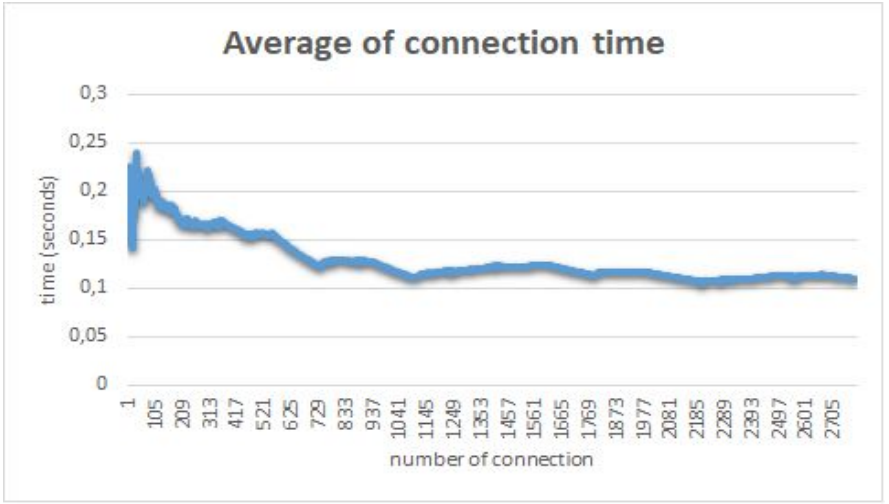
The formalized protocol II.

Securing Cloud Authentication

HU-MATHS-IN
Hungarian Service Network for Mathematics in Industry and Innovations

Results & Benefits to the company

- A new mutual entity authentication protocol with key agreement is given.
- Identity verification is executed by multiple servers on the provider's side.
- The protocol is provably secure in the threshold hybrid corruption model.
- The implementation is tested, good efficiency results are achieved. This design provides a higher security level for users and handles the case of corrupt servers. The construction ensures the scability by apply the Keyed Key Derivation Function and the robustness of authentication as well.



Efficiency analysis of the implementation

The company has a multi-server mutual entity authentication system for clouds.