Provably Secure Scalable Distributed Authentication for Clouds

Andrea Huszti, Norbert Oláh

University of Debrecen

Online
14 December 2020

Motivation of the paper

- Cloud computing is a significant technology
- There are some challenges and problems in cloud providers::
  - Servers are compromised and the secrets are vulnerable to theft.
  - Secure user authentication is an important issue of cloud services
    If authentication is breached, confidentiality and integrity of the data or services may be compromised

Practical solution for user authentication

OpenStack Identity service (for clouds):

- username and password
- Lightweight Directory Access Protocol
- Kerberos
- TLS/SSL

Incidents and issues

- Weak passwords (dictionary and rainbow table attacks)
- Poor maintenance and implementation (side channel attacks)
- OneLogin
- Golden Ticket Attack

Scientific approaches

Multi-server environment

- Brainard, J., Juels, A., Kaliski, B., Szydlo, M.: A new two-server approach for authentication with short secrets.

Password-authenticated key exchange

- Boyen, X.: HPAKE: password authentication secure against cross-site user impersonation.
- Katz, J., Ostrovsky, R., Yung, M.: Efficient password-authenticated key exchange using human-memorable passwords.

Treshold solutions

- Isler, D., Küpcü, A: Distributed Single Password Protocol Framework.
- Di Raimondo, M., Gennaro, R.: Provably secure threshold password-authenticated key exchange.

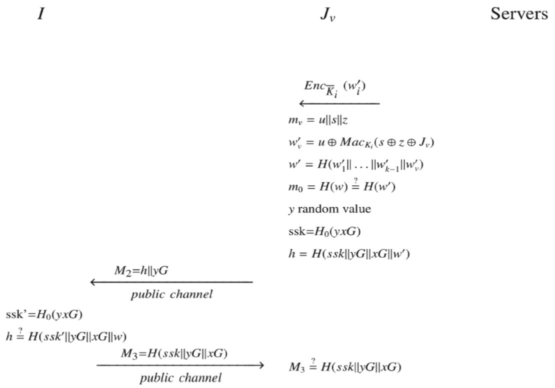
Our contribution

- Shared secret key between two or more entities
- Take advantages of the distributed system — distributed authentication
  - Robustness, scalability and greater availability
- Authentication:
  - Password-based
  - Key agreement and key confirmation between the parties
  - Provably secure protocol
  - Efficiency

Proposed protocol

I	J_v	Servers
$(K_1, \dots, K_k), G$	K_v, G	
$K_i = KKDF^{c+i}_{key}(psw)$, where $key = H(salt \| psw)$	$\overline{K}_1, \dots, \overline{K}_{k-1}$ short-lived keys	
$K_n = KKDF_{key}(psw) \oplus \dots \oplus KKDF^{c+n-2}{}_{key}(psw)$		
$t_1, \dots, t_{k-1}, t_v\, ;\, r_1, \dots, r_{k-1}$, x random		
$w_1 = H(t_1), \dots, w_v = H(t_v)$		
$w = H(w_1 \| \dots \| w_{k-1} \| w_v)$		
$m_0 = H(w)$		
$m_i = (Mac_{K_i}(r_i \oplus J_i) \oplus w_i) \| r_i$		
$m_v = (Mac_{K_v}(r_v \oplus xG \oplus J_v) \oplus w_v) \| r_v \| xG$		
$\xrightarrow[\textit{public channel}]{M_1 = I \| J_1 \| \dots \| J_k \| m_0 \| \dots \| m_k}$		
	$\xrightarrow{I \| m_i}$	J_i
		$K_i, \overline{K}_i$
		$m_i = p \| q$
		$w_i' = p \oplus Mac_{K_i}(q \oplus J_i)$

Proposed protocol



Security goals

- **Correctness**
- **Key secrecy**
- **Known-key security** (Freshness)
- **Mutual authentication**
- **(Perfect) Forward-secrecy**

Bellare-Rogaway model - Indirect proof

- Each participant is modelled by an oracle
- Oracles keep transcripts and answer the questions on the tape in one step.
- It is assumed that the attacker is able to create queries. Each query models some type of attack.

Theorem

Theorem

The proposed protocol is a secure AKC protocol in the random oracle model, assuming MAC is existentially unforgeable under an adaptive chosen-message attack and symmetric encryption scheme is indistinguishable under chosen plaintext attack, moreover ECCDH assumption holds in the elliptic curve group.

Proof Consider an adversary $\mathcal{A}$ and suppose that

$$Pr[\texttt{No-Matching}^{\mathcal{A}}(\kappa)]$$

is non-negligible. There are two cases: either the edge or the client oracle is accepted.

Security assumption of the symmetric encryption

- $n_C(\kappa)$ indicates the probability of an event that the attacker is successful
- Suppose that a client oracle is accepted — a server oracle is impersonated by the attacker
- Generating an $\mathcal{F}$ polynomial-time algorithm to break the symmetric encryption scheme is *indistinguishable under chosen plaintext attack*

$$\xi_2(\kappa) = \frac{n_C(\kappa)}{T_1(\kappa)\,T_2(\kappa)\binom{T_2(\kappa)-1}{k-1}\,T_3(\kappa)} - \lambda(\kappa),$$

- It contradicts the security assumption of the symmetric encryption

NEMZETI KUTATÁSI, FEJLESZTÉSI
ÉS INNOVÁCIÓS HIVATAL

AZ INNOVÁCIÓ LENDÜLETE

AZ NKFI ALAPBÓL
MEGVALÓSULÓ PROJEKT

Project ID: 2018-1.2.1-NKP-2018-00004

Thank you for your attention!