Designing secure multiple-server authentication schemes

Norbert Oláh

University of Debrecen

23. Gyires Béla Informatikai Nap
11 December 2020
Motivations

Distributed Authentication

One-Time Password Authentication and Key Exchange for Cloud Environment

Identity-based cryptography

Provably Secure Scalable Distributed Authentication for Clouds
- **Internet of Things (IoT)**
  2018 $772 billions are spent on IoT devices

- **Edge computing**
  Edge computing broadly as all computing outside the cloud happening at the edge of the network, and more specifically in applications where realtime processing of data is required.

- **Cloud computing**
  Several advantages (cost savings, scalability, robustness, etc.)

- **Smart home, city**
  Savings, safety, convenience, and control.
Security challenges

Fears of internal and external attackers

- Data is available to service providers - clouds
- "Optimizing" production at the expense of security - IoT
  Resource constrained devices
- Human risks
  - Poor security
    Most devices use weak or default passwords.
  - Poor maintenance
    After the initial setup, users do not use the devices properly (update).
- These systems and devices are common targets of cyber attackers.
  - Different types of external attacks
  - Zombie networks, DoS attacks, MITM, Brute Force, etc.
  - Several incidents: Mirai and other Botnets (dictionary attack)
Definitions

- **Entity authentication**
The protocol by which one entity is assured of the identity of a second entity.


- **Cryptographic protocol**
It is a system of rules that allow two or more entities of a communications system to transmit information via any kind of variation of a physical quantity and accomplish one or more security goals.

- **Mutual authentication**
In mutual authentication parties who engage in a conversation in which each gains confidence that it is the other with whom he speaks.

- **Key agreement**
Both entities contribute to the joint secret key by providing information from which the key is derived.

- **Authenticated key agreement protocol**
A key exchange protocol that provides mutual implicit key authentication is called an authenticated key agreement protocol (AK protocol).
Concept of Distributed Authentication

Centralized structure

- There are fears about the centralized structure
- Central databases are primary targets for hackers
- If these databases are compromised it cause huge damage.
- A single point of failure occurs typically in single-server solutions.
  If the server is unavailable, the provider usually needs to ensure replication to tackle the failure of their servers.
- Golden Ticket Attack, OneLogin attack

Distributed Authentication

- External attackers have to attack multiple servers simultaneously, which increases the attack cost.
- If one or more servers break down or become corrupt, the service provider is able to service and authenticate the users securely.
Security goals designing authenticated key agreement protocol

- **Correctness**: Participants will always accept the same symmetric key.

- **Key secrecy**: In the presence of an active attacker, the symmetric key can be calculated only by the participants.

- **Known-key security** (Freshness): Each protocol run results in a unique secret symmetric key. A compromised symmetric key is not able to provide information about other symmetric keys.

- **Mutual authentication**: Mutual authentication prevents an attacker from impersonating a legitimate participant and illegally accessing user information.

- **(Perfect) Forward-secrecy**: It holds if long-term secrets of one or more entities are compromised and the secrecy of previous session keys is not affected.
One-Time Password Authentication and Key Exchange for Cloud Environment

- Two-factor authentication
  static password + one-time password
- Malicious insiders
  distributed authentication among cloud servers, one-time password is stored distributed
- MAC key exchange
  providing data origin integrity
- Improving efficiency
Merkle-tree
One-Time Password Authentication and Key Exchange for Cloud Environment


Identity-based cryptography

- Certificate-based:

- Identity-based:

  ![Certificate-based diagram](image1)
  ![Identity-based diagram](image2)
Bilinear map

Definition

Let $G_1$ and $G_2$ be two groups of order $q$ for some large prime $q$. A map $e : G_1 \times G_1 \rightarrow G_2$ is an admissible bilinear map if it satisfies the following properties:

1. Bilinear: We say that a map $e : G_1 \times G_1 \rightarrow G_2$ is bilinear if $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1$ and all $a, b \in \mathbb{Z}$.

2. Non-degenerate: The map does not send all pairs in $G_1 \times G_1$ to the identity in $G_2$. Since $G_1, G_2$ are groups of prime order, if $P$ is a generator of $G_1$ then $e(P, P)$ is a generator of $G_2$.

3. Computable: There is an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in G_1$. 
Bilinear Diffie-Hellman Problem

Definition

Let $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear map on $(G_1, G_2)$ and $a, b, c \in Z_q^*$. Given $(P, aP, bP, cP)$, compute $e(P, P)^{abc}$. 
Identity-based cryptography

- Gábor Kovács and Attila Pethő. "Személyre szabott titkosítási rendszerek megvalósítása" (2014)
- Szilárd Dávid Szürti and Botond Mezei "Attribute-based Encryption WASI-alapú platformfüggetlen implementációja" - TDK (2020) (SETIT project)

Supervisors: Attila Bagossy and Ádám Vécsi
Provably Secure Scalable Distributed Authentication for Clouds

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

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

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

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 $F$ polynomial-time algorithm to break the symmetric encryption scheme is \textit{indistinguishable under chosen plaintext attack}.

\[
\xi_2(\kappa) = \frac{n_C(\kappa)}{T_1(\kappa) T_2(\kappa) \left( \frac{T_2(\kappa)}{k-1} \right) T_3(\kappa)} - \lambda(\kappa),
\]

- It contradicts the security assumption of the symmetric encryption.


https://doi.org/10.1007/978-3-030-65411-5_10
Motivations

Distributed Authentication

One-Time Password Authentication and Key Exchange for Cloud Environment

Identity-based cryptography

Provably Secure Scalable Distributed Authentication for Clouds

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

Norbert Oláh

Designing secure multiple-server authentication schemes
Thank you for your attention!
Identity-based encryption

**IBE**: \((\text{SetUp}, \text{Key}, \text{Enc}, \text{Dec})\)

- **SetUp**
  
  output: \((PP, msk)\),
  
  \(PP = (\mathcal{P}, \mathcal{C}, \mathcal{I}, mpk)\) public parameters and \(msk\) a master secret key

- **Key**
  
  input: \(id \in \mathcal{I}\) public key, \(PP, msk\)
  
  output: \(d_{id}\) secret key

- **Enc**
  
  input: \(id \in \mathcal{I}, m \in \mathcal{P}, PP\)
  
  output: \(c \in \mathcal{C}\)

- **Dec**
  
  input: \(c \in \mathcal{C}, id \in \mathcal{I}, d_{id}, PP\)
  
  output: \(m \in \mathcal{P}\)