Identity-based Password Registration for Clouds

Andrea Huszti, Norbert Oláh

University of Debrecen
Doctoral School of Informatics

Eger
01. 29. 2020.

Content

Motivation

New technologies are coming

- Cloud computing
  Fog computing
- Internet of things
- Autonomous vehicles

In their rush to penetrate the market, many device vendors neglect security in favor of user-friendliness and usability.

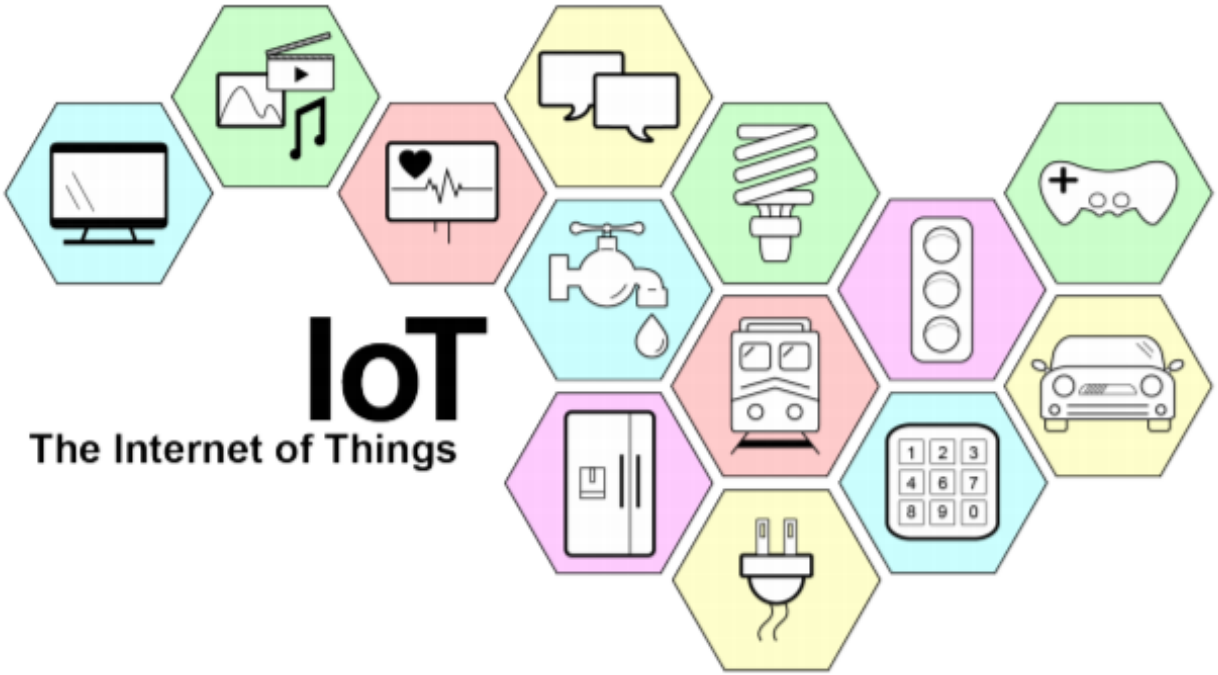
Motivation

There are some problems of the user's devices:

- Feeble protection
  Most devices uses weak or default passwords.
- Poor maintenance
  After initially setting them up, users forget about them unless they stop working properly.
- Increasing influence
  For example: The ubiquity and increasing popularity of the Internet of Things (IoT) have made IoT devices a powerful amplifying platform for cyberattacks.

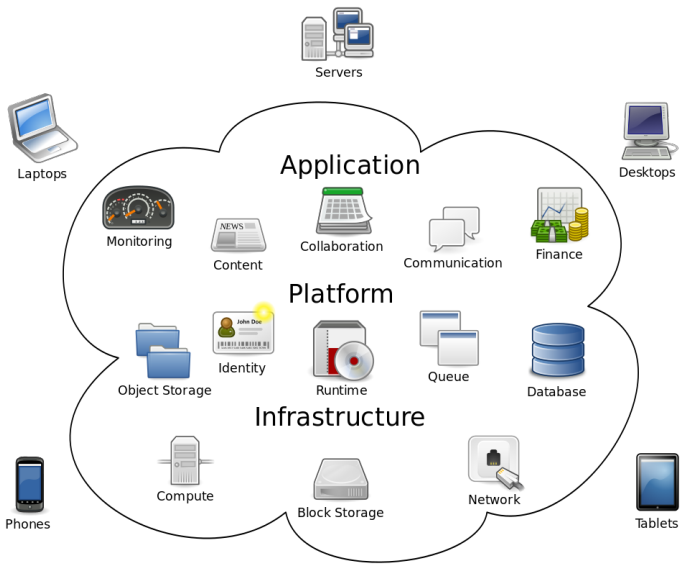
Internet of Things

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.



Cloud computing

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.



Identity-based cryptography

- Certificate-based:

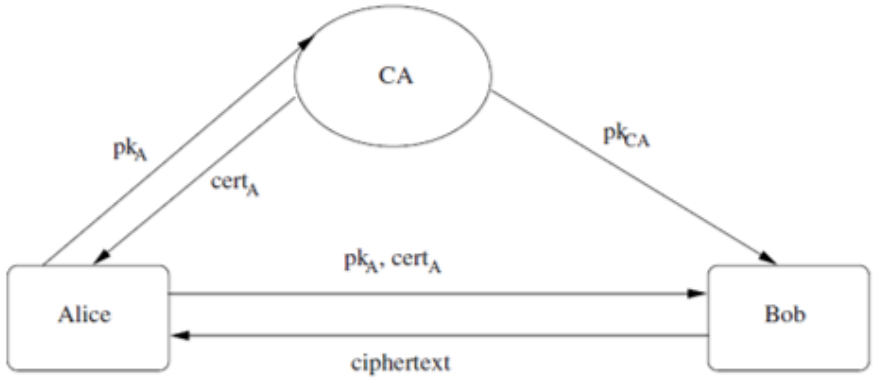


Fig. 1.9 Certifying authority and trust in public key.

- Identity-based:

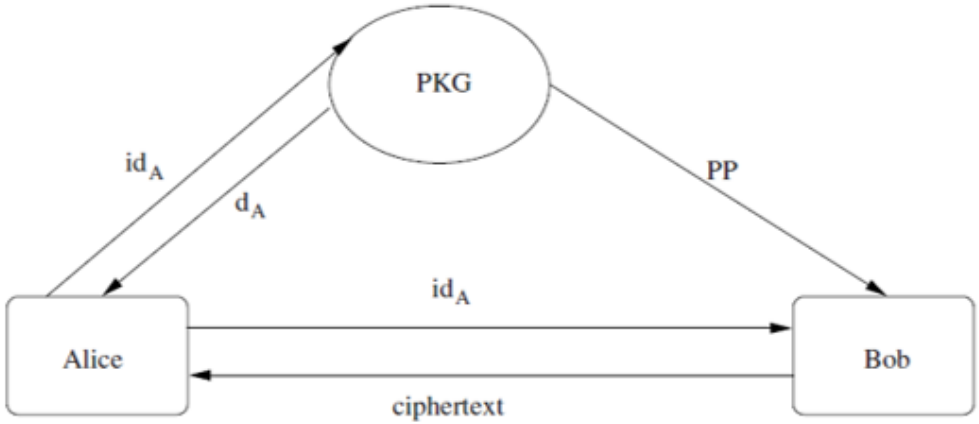


Fig. 1.10 An overview of an IBE scheme.

Security challenges

Fears of internal and external attackers

- Data is available to service providers.
  Intentionally or unintentionally disclose customer information or disclose it to the authority upon request.
- Human risks
- Different types of external attacks

Several incidents in practice

- Golden Ticket attack (authentication)
- Ashley Madison data breach (weak cryptography)
- Mirai and other Botnets (brute force, dictionary attack)

CIA security requirements

Our goal

- Registration: Identity-based long-lived key exchange with password registration
- Identity-based cryptography
- Formal security analysis
- Applications

Proposed registration

User (U)	$P, \gamma P$	Server (S)
$Q_U = H_1(ID_U)$		$Q_S = H_1(ID_S)$, $x\gamma P$
γQ_U		γQ_S, x
$t \in \mathbb{Z}_q^*$ random		
$z = H(t)$		
psw password		
$s = H(psw)$		
$m_1 = \hat{e}(Q_S, zx\gamma P + \gamma Q_U)\hat{e}(zP, sP)$		
$K = H_0(\hat{e}(zP, sP))$		
$V_1 = H_2(\hat{e}(Q_S, zx\gamma P + \gamma Q_U), K)$		
	$\xrightarrow{Q_U, zP, m_1, V_1}$	
		$\frac{m_1}{\hat{e}(\gamma Q_S, xzP + Q_U)} =$
		$K' = H_0(\hat{e}(zP, sP))$
		$V_1 \stackrel{?}{=} H_2(\hat{e}(\gamma Q_S, xzP + Q_U), K')$
		$r_S \in \mathbb{Z}_q^*$ random
		$Mac_{K'}(r_S)$
	$\xleftarrow{Q_S, Mac_{K'}(r_S), r_S}$	
$Mac_K(r_S) \stackrel{?}{=} Mac_{K'}(r_S)$		
		Store: $Q_U, \hat{e}(zP, sP), zP$

Security goals

- **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 run of the protocol results in a unique secret symmetric key. A compromised symmetric key cannot provide information about other symmetric keys.
- **Mutual authentication**: Mutual authentication prevents an attacker from impersonating a legitimate participant and illegally accessing user information.

Oracle

Fix a nonempty set ID of participants

- $Client = \{1, 2, \ldots, T_1(\kappa)\}$
- $Server = \{1, 2, \ldots, n = T_2(\kappa)\}$
- Each participant is modelled by an oracle $\prod^{l}_{I,J}$, which simulates a participant I executing a registration in the belief that it is communicating with another participant J for the lth time, where $l \in \{1, \ldots, T_3(\kappa)\}$ for some polynomial function T_3.

Oracles keep transcripts, which contain all messages they have sent and received and the queries they have answered.

Adversarial model

Definition

We assume that $\mathcal{A} \notin ID$, *i.e.* neither a client nor a server. $\mathcal{A}$ is a probabilistic polynomial time Turing Machine with an access to the participants' oracles, *i.e.* it has a query tape where oracle queries and their answers are written. $\mathcal{A}$ is able to relay, modify, delay or delete messages. We assume that $\mathcal{A}$ is allowed to make the following queries. Each query models some kind of adversarial attack.

Adversarial model

- $\texttt{Send}(\prod_{I,J}^{i}, M)$
- $\texttt{Reveal}(\prod_{I,J}^{i})$
- $\texttt{Corrupt}(\prod_{I,J})$:
- $\texttt{Test}(\prod_{I,J}^{i})$:

We define $\mathcal{A}$'s advantage, the probability that $\mathcal{A}$ can distinguish the long-lived key held by the queried oracle from a random string, as follows:

$$Adv^{\mathcal{A}}(\kappa) = |Pr[\text{guess correct}] - 1/2|.$$

No-Matching

Definition

$\texttt{No-Matching}^{\mathcal{A}}(\kappa)$ denotes an event when in a protocol P in the presence of an adversary $\mathcal{A}$ assuming there exist a client oracle $\prod^{s}_{I,J}$ which is accepted, but there is no server oracle $\prod^{t}_{J,I}$ having a matching conversation with $\prod^{s}_{I,J}$.

Secure AKC protocol

Definition

A protocol is a *secure AKC protocol* if for every adversary $\mathcal{A}$,

1. There is a client oracle having matching conversations with a server oracle and vice versa and they always accept holding the same long-lived key K_{IJ}, and this key is distributed uniformly at random on $\{0,1\}^{\kappa}$.
2. The probability of $\texttt{No-Matching}^{\mathcal{A}}(\kappa)$ is negligible.
3. If the tested oracle is fresh, then $Adv^{\mathcal{A}}(\kappa)$ is negligible.

Bilinear Diffie-Hellman Problems

Definition

Bilinear Diffie-Hellman Problem. 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 $e(P, P)^{abc}$.

Definition

Multiplication of Bilinear Diffie Hellman. Given aP, bP, cP, dP, eP and calculate $e(P, P)^{abc} * e(P, P)^{bde}$.

MAC unforgeable

Consider the experiment for a message authentication code (Key, Mac, Ver), an adversary $\mathcal{A}$, and security parameter κ, as follows. The message authentication experiment $Exp_{Mac}^{eforge}(\mathcal{A})$:

1. A random key K is generated by running $Key(1^{\kappa})$.
2. The adversary $\mathcal{A}$ is given input 1^{κ} and oracle access to $Mac_K(.)$. The adversary eventually outputs a pair (m, t).
3. The output of the experiment is defined to be 1 if and only if $Ver_K(m, t) = 1$ and m was never asked from the oracle $Mac_K(.)$ before.

Security proof

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, moreover Bilinear Diffie Hellman and Multiplication of Bilinear Diffie Hellman is computationally infeasible in the Random Oracle Model.

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 server, or the client oracle is accepted.

Bilinear Diffie Hellman

Let $\mathcal{A}$ succeeds denote the event that in $\mathcal{A}$'s experiment there is a server oracle $\prod_{J,I}^{t}$ that is *accepted*, but there is no client oracle $\prod_{I,J}$ having matching conversation to $\prod_{J,I}^{t}$. We construct a polynomial time adversary $\mathcal{F}$ that for given aP, bP, cP, P calculates $BDH(aP, bP, cP, P) = e(P, P)^{abc}$.

$$\xi_1(\kappa) = \frac{n_S(\kappa)}{T_1(\kappa)T_2(\kappa)T_3(\kappa)},$$

where $\xi_1(\kappa)$ is non-negligible, if $n_S(\kappa)$ is non-negligible, $T_i(\kappa)(i = 1, \ldots, 3)$ is polynomial in κ. That contradicts the security assumption of the BDH problem, hence $n_S(\kappa)$ must be negligible.

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.

Thank you for your attention!

Universal security requirements

- Entity authentication
  Lack of strong authentication can lead to unauthorized access to users account on a provider.
- Data integrity
  Data is not modified.
- Confidentiality
  The data may be accessed and used only by authorized persons.
- Access Management
  The data owner needs to make a flexible and scalable access control policy, so that only the authorized users can access.

MAC

Let $\mathcal{A}$ succeeds denote the event that in $\mathcal{A}$'s experiment there is a client oracle $\prod_{I,J}^{t}$ that is *accepted*, but there is no server oracle $\prod_{J,I}$ having matching conversation to $\prod_{I,J}^{t}$. We assume that $Pr[\mathcal{A} \text{ succeeds}] = n_{C_1}(\kappa)$, where $n_{C_1}(\kappa)$ is non-negligible. We construct a polynomial time adversary $\mathcal{F}$ that is able to proceed an existential forgery against MAC under an adaptive chosen message attack.

$$\xi_2(\kappa) \geq \frac{n_{C_1}(\kappa)}{T_1(\kappa)T_2(\kappa)T_3(\kappa)} - \lambda(\kappa),$$

where $\lambda(\kappa)$ denotes the probability that $\mathcal{F}$ previously calculated the flow. Since $n_{C_1}(\kappa)$ is non-negligible, $T_i(\kappa)$ (i=1,...,3) is polynomial in κ and $\lambda(\kappa)$ is negligible, thus $\xi_2(\kappa)$ is non-negligible. That contradicts the security assumption of MAC, hence $n_{C_1}(\kappa)$ must be negligible.

Multiplication of Bilinear Diffie-Hellman Problem

Let see the other case of $\mathcal{A}$ experiment in which there is a client oracle $\prod_{I,J}^{t}$ that is *accepted*, but there is no server oracle $\prod_{J,I}$ having matching conversation to $\prod_{I,J}^{t}$. We assume that

$$Pr[\mathcal{A} \text{ succeeds}] = n_{C_2}(\kappa),$$

where $n_{C_2}(\kappa)$ is non-negligible. In this case we can construct a polynomial time adversary that for given aP, bP, cP, dP, eP, P calculates $mBDH(aP, bP, cP, dP, eP) = e(P, P)^{abc} * e(P, P)^{bde}$.

$$\xi_3(\kappa) = \frac{n_{C_2}(\kappa)}{T_1(\kappa)T_2(\kappa)T_3(\kappa)T_4(\kappa)} - \lambda(\kappa),$$

where $\lambda(\kappa)$ denotes the probability that $\mathcal{F}$ previously calculated the flow. Similarly to Case 1. $\xi_3(\kappa)$ is non-negligible, if $n_{C_2}(\kappa)$ is non-negligible, $T_i(\kappa)$ (i=1,. . . ,4) is polynomial in κ and $\lambda(\kappa)$ is negligible. That contradicts the assumption of M Bilinear Diffie Hellman, hence $n_{C_2}(\kappa)$ must be negligible.