Course Project Report: Identity-Based Encrpytion

Name: CHE Yulin, Student#: 20292673

Q1

What is the motivation for proposing the identity-based encryption?

Definition

Identity-Based Encryption (IBE) is defined as a public-key encryption scheme where any valid string, which uniquely identifies a user, is the public key of the user.

Original Motivation

The original motivation for identity-based cryptography was to simplify certificate management and thus eliminate the need for Certification Authorities.

Challenge in Traditional PKI

With traditional public key cryptography, the generation of the keys, the publication of the associations between parties and their public keys and the management of all this require a dedicated secure infrastructure. Such an infrastructure is expensive, complex, does not scale well to large sizes, and does not easily extend to manage parties' attributes, e.g., their roles and rights.

Comparison with Traditional PKI

In traditional Public-Key Infrastructure (PKI), a public-key certificate is required to bind the key to its user. However, certificates are not required in IBE, because each user has a unique identity to which they are intrinsically bound. Instead, IBE requires a trusted central authority called a Private-Key Generator(PKG) for generation and distribution of private keys to registered users.

Simplicity of IBE

IBE offers a much simpler solution for many applications, solving the above challenge and meeting the original motivation. And two reasons are elaborated as follows.

First Resaon for Simplicity

Because the encryption key can be any bit string, it can be chosen by the encrypting party. The encrypting party can base its choice of bit string on the needs of the application. First choice is something simple, e.g, the email address of the receiving party, a digital photograph of the receiving party, a URL. Second choice is something more complex, e.g, the role of the receiving party, expressed by a list of attributes he must have, a set of conditions the receiving party must meet, a policy that the receiving party must conform to, executable program code.

Expressing these requirements in the encryption key relieves the supporting infrastructure from managing them, thus enabling the infrastructure to be simpler.

Second Reason for Simplicity

Because the decryption key does not need to be generated at the same time, or by the same entity, as the encryption key, the trusted third party can delay generating it until the receiving party has demonstrated its right to have it.

So, there is no need for any party to store keys, thus, easing the management problem considerably, reducing the risk of inadvertently exposed keys compromising the secrecy of the protected content.

Benefit & Application

Thus, IBE removes several difficulties associated with traditional PKI such as certificate lookup, life-cycle management, Certificate Revocation Lists and cross-certification issues giving a greatly-simplified public-key encryption and signature scheme. Besides, IBE is suitable for the following applications, revocation of public keys, managing user credentials, delegations of decryption keys, forward secure encryption schemes.

Q2

What are the advantages and disadvantages of the IBE over the traditional certificate-based public-key encryption?

There are many disadvantages in IBE, while advantages of IBE could be achieved by slightly modifying traditional certificate-based public-key encryption schema. Thus, disadvantages are elaborated first, and advantages are elaborated second.

Disadvantages

PKG PR-Key Compromise Cost Problem

We must also trust that the PKG/CA private key is known only to the PKG/CA. Compromise of the PKG private key compromises the private keys of all users in that domain. In contrast, compromise of the CA private key enables the attacker to sign and publish new compromised public keys, tricking senders into encrypting new messages to these public keys, though it does not compromise existing private keys or messages encrypted to those keys.

Revocation of PU-Key Incurred Problem

IBE must use short-lived keys to support revocation, as there is no revocation method for IBE analogous to X.509's CRLs or OCSP. So, in practice, the PKG must remain online, with the associated increased risk of compromise. Thus, in this aspect, IBE requires stronger trust assumptions than RSA, requiring a fully-trusted, online entity (the PKG), as opposed to a partially-trusted (with respect to secrecy of user private keys), offline entity (the CA).

Users' PR-Key Transmission Problem

We also require a trustworthy process by which recipients obtain and manage their private keys. For modern RSA PKIs, recipients typically generate and maintain sole control over their private keys. As part of the certificate request and issuance process, the CA requires the key holder to authenticate and prove posession of the private key, typically by signing the certificate request. For IBE, the PKG generates the private key and sends it to the recipient via a private, authenticated channel. Thus, in both cases, we must trust the user authentication to the PKG or CA, so private keys are not associated with the wrong recipients. For IBE, however, we must also trust that the private key is not compromised at the PKG or on the network. Again, IBE requires stronger trust assumptions than RSA.

Key Escrow

It is well understood that IBE includes a type of key escrow, because the PKG generates the user's private keys, which causes the following two bad effects, namely PKG as a possible man-in-the-middle and no non-repudiation guarantee.

Key Escrow Problem 1: PKG as a Possible Man-in-the-Middle

The PKG is a fully-trusted entity that could decrypt all messages in the domain, unlike a traditional CA which has no access to user private keys. IBE provides a weaker form of end-to-end security for encryption than traditional RSA-based PKIs, with the PKG as a possible man-in-the-middle. Thus, we can consider IBE trust assumptions to be in between solutions that provide strong end-to-end security and gateway-based systems, where the sender must trust the recipient's domain administrators to properly handle encrypted messages.

Key Escrow Problem 2: No Non-Repudiation Guarantee

It is well understood that IBE includes a type of key escrow, because the PKG generates the user's private keys. PKG is able to sign users' message, thus, non-repudiation is not guaranteed in IBE. A user could repudiate that the message
is signed by PKG.

Advantages

Elimination of User Key Distribution

In IBE once the sender obtains the parameters of a particular domain's PKG, he can compute the public key of any user in that
domain. That is, instead of requiring one online (public) key fetch operation per recipient as in RSA, IBE only requires one online key fetch operation per domain (the PKG's key). By effectively eliminating the need to distribute end user public keys, IBE addresses a major hurdle in widespread deployment and use of secure email. This is perhaps the most important benefit of IBE.

Elimination of Certificate and CA

Digital certificate and certification authorities are not needed here. Because receiver's identifier information is used, sender needn't to retrieve receiver's public key. Thus, CA is not required to issue public keys.

Policy Based Encryption

Using IBE the sender can associate arbitrary policies with the encrypted email message. It can do so by concatenating the policy with the recipient's ID prior to computing the public key. When the message is encrypted using this key, the PKG can enforce the sender's policy regarding the release of the private key. For example, the sender can postdate the message by including a specific date in the encryption key, and the PKG will then release the corresponding key only on or after that date. This benefit is beginning to gain value as email messaging is being used increasingly for formal communication and is being incorporated into workflow systems.

Implicit client mobility

In IBE the receiver can contact the PKG whenever it needs a private key. Therefore, as long as the receiver can contact the PKG, IBE provides seamless client mobility as the recipient can use any device from any location to access private keys for email decryption. This benefit is very valuable as users often check email using a variety of devices such as PDAs and laptops and do so from a variety of locations. In RSA users can utilize smart cards or online credential repositories to provide client mobility but this benefit is not provided implicitly.

Q3

Can an IBE system be used for signing digital documents? If yes, can the digital signature be used for non-repudiation?

Can an IBE system be used for signing digital documents?

If the PKG is trusty and its private key has not been compromised, which means it will not commit man-in-the-middle attacks then the answer is yes, else not. Attention please, here is a strong assumption that PKG is fully trusty and its private key has not been compromised.

To prove it can provide the functionality of signing digital documents, we need to prove it can provide sender authentication and message integrity. The specific key generation and key usage is as follows, where PKG is the private key generator, Alice is the message sender, Bob is the message receiver.

- Initialization Phase:
  PKG creates its private and public key pair, denoted as sk_{PKG} and pk_{PKG} , where sk stands for secret key and pk stands for public key.
- Authentication Phase:
  Alice authenticates herself to PKG and obtains a private key $sk_{ID_{Alice}}$, which is associated with her identity ID_{Alice} .
- Signing Phase:
  Alice create a signature sig , using her private key $sk_{ID_{Alice}}$ on the message msg , and then sends $msg||sig$ to Bob.
- Check Sender Authentication and Data Integrity Phase:
  - Bob receives $msg'||sig'$ and then splits them. Then bob verify by using ID_{Alcie} and pk_{PKG} set up before to confirm the sender authentication and data integrity.
  - The verifier hashes msg' , getting $hash(msg')$, and then use (ID_{Alcie}, pk_{PKG}) as Alice's public key decrpts sig' , then compare $D_{(ID_{Alcie}, pk_{PKG})}(sig')$ with $hash(msg')$. If they are met then sender authentication is met sicne only PKG and Alice have Alice's private key, data integrity is also met since the hashed message is the same as the hash value from Alcie.

If yes, can the digital signature be used for non-repudiation?

Of course not.

Unfortunately, all identity-based cryptographic schemes have inherent weakness, a "key escrow" property. Recall that in IBE and IBS schemes, the PKG issues private keys for user using its master secret key. As a result, the PKG is able to decrypt or sign any messages.

However, non-repudiation means that only an entity which possesses a signing key can create a signature, here there are indeed two entities PKG and Alice to create a signature. Thus, non-repudiation is not guaranteed.

Q4

Do you think IBE will be widely used? Please justify your conclusion.

From available resources, I think IBE will not be widely used.

Advantages vs Disadvantages

From Q1, we know the original motivation of introducing IBE is to simplify certificate management and thus eliminate the need for Certification AuthoritiesHowever, advantages of IBE could also be achieved by slightly modifying traditional certificate-based public-key encryption schema. The detail explanation could be found in paper `Khurana H, Basney J. On the risks of IBE[C]//International Workshop on Applied PKC. 2006: 1-10.`

Thus, the advantages elaborated in Q2 are not significant, compared with disadvantages and built-in flaws in IBE design. The elimination of user key distribution, certificate, certificate authorities, flexibility of policy-based encryption, implicitly client mobility are not hard to achieve with some modifications of traditional certificate-based public key cryptography systems such as secure email systems S/MIME.

Important Weakness

The disadvantages are hard to resolve. I list the most important ones.

PKG PR-Key Compromise Cost Problem

The compromise of PKG's private key will make the whole system insecure. Compromise of the PKG private key compromises the private keys of all users in that domain. There is a lack of proper efficient mechanism to cope with this difficulty.

Key Escrow Problem

Non-repudiation and higher confidentiality are important properties of a good cryptography system. However, in IBE these two properties are hard to gain. To resolve the key escrow problem, there are some attempts. Boneh and Franklin suggested that
the master secret key of the PKG be distributed using Shamir's secret sharing technique into a number of PKGs. The user then obtains partial private key shares associated with his identity from the multiple PKGs and reconstruct a whole private key. But this "multiple PKG" method impose heavy loads on users since they should authenticate themselves to the multiple PKGs, which takes big communication and computational cost.

Revocation of PU-Key Problem

There is a situation as follows. Suppose that Bob wants others to use his email address to encrypt messages. But, suppose that
the private key associated with Bob's email address has been compromised, so he cannot use his email address as a public key any more. In order to tackle these problems, we have to use short-lived keys, which incurs overhead and complexity. Thus,whether the time period should not be too short or too long, which makes security policy management complicated. Short-lived keys makes PKG keys has to be always online, making it easier to be attacked.

Complexity Analysis

Identity-based cryptographic schemes proposed so far in the literature can be categorized into two classes: "Pairing-
based schemes" and "Factoring-based schemes". The latter mainly refers to the IBE scheme pro-
posed by Cocks. However, because of efficiency, the former "Pairing-based schemes" have been focused on by many cryptographers. Recently, cryptographic schemes that have some different structures. Even though these schemes still use
the bilinear pairing, they turn out to be more efficient than previous schemes. (Note that although the techniques for speeding up the bilinear pairing computation have been developed by Barreto et al., the computational cost for the pairing computation is still expensive compared to a single or double exponentiation in the finite field.)