Faculteit
Ingenieurswetenschappen

Departement
Elektrotechniek – ESAT

KATHOLIEKE
UNIVERSITEIT
LEUVEN

# Identity-based Broadcast Encryption for OSNs

## Defining a security model

**Stijn Meul**

Promotor:
Prof. Dr. Ir. Bart Preneel
Prof. Dr. Ir. Vincent Rijmen
Daily supervisor:
Ir. Filipe Beato

2013—2014

# 1 Security Model

## 1.1 Parties in the Model

Different parties can be distinguished in the security model of an Anonymous Identity Based Broadcast Encryption scheme for Online Social Networks (OSNs):

**User** A user is defined to be any identity that has a profile on the OSN and is thus identifiable by a unqiue $ID$.

**Sender** The sender is a user of the OSN who wants to broadcast messages to sets of varying intended receivers. The sender broadcasts these messages using the infrastructure provided by the OSN. The set of intended receivers consists of a subset $\mathcal{S}$ of people that are part of the OSN.

**OSN** The OSN can be considered as an unsafe communication infrastructure. On the one hand the OSN offers a communication channel that allows sending messages. On the other hand the OSN offers an interface for storing user defined content (profile information) and lists of users that are connected to each other as friends. The communication infrastructure provided by the OSN is considered unsafe because the sender has to trust the OSN completely with his content. As the OSNs store all the sender's messages as well as his profile information, the OSN has full access to all the data that is sent over its infrastructure. This will be a motivation for the user to encrypt his data to prevent the OSN from having access to the plain text data. In our practical implementation of IBE for OSNs, the OSN will be Facebook.

**PKG** A Public Key Generator (PKG) is a third party that can be partially trusted. A PKG is needed in identity-based encryption schemes to allow using any string as a public key. PKGs announce their public keys $pk_{PKG}$ to all users of the OSN. Furthermore PKGs generate private keys $sk_{ID}$ corresponding to any public string that uniquely identifies a sender of the OSN. As in an OSN virtually any user can broadcast messages over its network, any user of the OSN can request a private key $sk_{ID}$ associated to his identity $ID$. Note that as the PKGs generate the private key $sk_{ID}$ for every user, key escrow is implicitly present in IBE schemes. This means that the trust is shifted from the OSN to the PKGs. To prevent the undesired key escrow property a threshold secret sharing technique should be used. This means that the information of a minimum number of PKGs should be combined by the user to derive his $sk_{ID}$ such that $sk_{ID}$ can only be known to this minimum number of PKGs if they collaborate. It is therefore required that PKGs are hosted by different parties that have no motivation to collaborate.

**Friends of the sender** Friends of the sender are other users of the OSN that are connected to the sender. The group of all friends associated to a user identity $ID$ will be called $\mathcal{F}_{ID}$. $\mathcal{F}_{ID}$ is stored on the servers of the OSN and can be seen by all parties that are given access to a users profile information i.e. every member of $\mathcal{A}_{ID}$.

**Parties that are given access to the OSN** Every party that is given access to services of the OSN is part of the access group $\mathcal{A}$. Any virtual or real world party can be part of $\mathcal{A}$ i.e. users, advertising companies, system administrators of the OSN, software applications

specifically developed for the OSN, etc. Note that these parties do not have to be users neither real life persons. Companies or software code can be part of $\mathcal{A}$ as well. The members of $\mathcal{A}$ are all defined by the OSN. The user thus has no control in who is a member of $\mathcal{A}$.

**Parties that are given access to user content** Every party that is given access to content from a user $ID$ of the OSN is part of an access group $\mathcal{A}_{ID}$. The user has partial control on who has access to his user content as he decides which users of the OSN are considered friends. Namely, $\mathcal{F}_{ID} \subseteq \mathcal{A}_{ID} \subseteq \mathcal{A}$. The OSN however can still define extra parties that are member of $\mathcal{A}_{ID}$ without being part of $\mathcal{F}_{ID}$.

**Intended receivers** The group of intended receivers $\mathcal{S}$ is a list of user $ID$s that are allowed to have access to a particular message. It is the sender who determines the members of $\mathcal{S}$. Any user in $\mathcal{A}_{ID}$ will then be able to see the ciphertext although only the members of $\mathcal{S}$ will be able to decrypt the message. Thus $\mathcal{S} \subseteq \mathcal{A}_{ID}$. Note however that not every member of $\mathcal{S}$ has to be a friend of user $ID$. Mathematically this means that if $\exists s \in \mathcal{S} : s \notin \mathcal{F}_{ID}$ then $s \in \mathcal{A}_{ID} \backslash \{\mathcal{F}_{ID}\}$. This concept is required to enable users to encrypt messages to other users than their friends.

## 1.2 Desired Requirements of the Architecture

### 1.2.1 Requirements on $\mathcal{S}$

One of the main goals of the designed architecture should be to **let the user granulary define his own privacy**. That is that the access rights are no longer defined by the OSN as the members of $\mathcal{A}_{ID}$ but by the users as the list of intended receivers $\mathcal{S}$ on a per message basis. To ensure that only the receivers in $\mathcal{S}$ are able to read a certain message, this message should be encrypted such that only these receivers are able to decrypt this message.

To leak as less information as possible the **group of intended receivers should be anonymous to any user in $\mathcal{A}$ that is not in $\mathcal{S}$**. Based on interactions between users a lot of information can be infered by making $\mathcal{S}$ public. For example by just analysing the frequency at which users are communicating with their connections, one can conclude whether they are friends in real life as well. Making $\mathcal{S}$ public for every message would therefore violate the users privacy.

Note however that although receivers being secret to unintended other users is desirable, it might be useful on a social network that **the members of the set $\mathcal{S}$ know each other**. Suppose for example that Alice posts a Facebook update on her profile page intended to Bob and Dylan. This means that $Bob, Dylan \in \mathcal{S}$. As a reaction to Alice's Facebook update, Bob wants to write a reply to start a discussion. However, as Bob does not know which other users are allowed to see Alice's update, he can now only encrypt his reply to Alice thereby preventing Dylan from joining the discussion. However, this discussion could have been useful to Dylan as well because otherwise Alice would not have included Dylan as a recipient in $\mathcal{S}$ in the first place.

### 1.2.2 Requirements on PKG

- PKG should not be able to know $sk_{ID}$ completely i.e. PKG only knows a share of the secret $sk_{ID}$

- PKG should be trusted not to collaborate with other PKGs
- PKG should not publish its share of the secret $sk_{ID}$
- A minimum threshold number of PKGs should be online in order for the protocol to work
- This threshold number of PKGs should be connected by the sender before he is able to derive his secret key $sk_{ID}$
- Only a threshold number of PKGs should be online to enable IBE
- PKG should not have an advantage when trying to find $sk_{ID}$ over any other party that does not know a share of the secret

## 1.3 Adversaries

### 1.3.1 Passive Adversaries

Passive attacks focus on uncovering secret information without affecting the functionality of any resource in the architecture.

**OSN** Although the OSN has access to all messages posted over its infrastructure, the OSN can only see the encrypted messages. If encryption is done correctly, a ciphertext can not be distinguished from a complete random string. The OSN is therefore no longer able to see plain text data posted by its users.

**PKG** There should not be any form of key escrow in the proposed architecture. This means that the PKG is not allowed to know the complete secret key of a user $sk_{ID}$. As secure secret sharing is used, the PKG has no more information than any other third party that is not in $\mathcal{A}$. Even if the PKG and the OSN collaborate such that PKG $\in \mathcal{A}_{ID}$, the PKG can not decrypt the messages sent on the OSN infrastructure. Only if multiple PKGs would be collaborating such that the number of collaborating PKGs equals the threshold of the secret sharing scheme, decryption by these PKGs would be possible. It is therefore important that PKGs can be trusted that they not collaborate with other PKGs neither share secret user keys $sk_{ID}$ with other parties.[1]

**Other parties** Other parties than the PKG or the OSN have no additional information whether they are in $\mathcal{A}, \mathcal{A}_{ID}$ or even in $\mathcal{F}$. Only users that are in $\mathcal{S}$ will have all the required information to decrypt the corresponding message.

### 1.3.2 Active Adversaries

Active adversaries try to alter system resources to affect their operation or actively take part in the protocol to derive more information from the secret data than actually is allowed.

[1] http://www.cypherpunks.ca/ iang/pubs/DPKG-SCN10.pdf mentions something about secret sharing not being possible for IBE schemes, however http://www.argreenhouse.com/society/wcan06/wcan06s4p3.pdf proposes such a secret sharing IBE scheme...

**OSN** Nothing can be done to prevent the OSN from actively altering its own resources to bring down the proposed IBE architecture. If a user of IBE for OSNs gets blocked for using encryption on the OSN infrastructure, this can not be prevented by the proposed architecture. When messages get deleted by the OSN because they are encrypted, this can not be prevented either. Altering of messages by the OSN can be prevented by requiring the user to concatenate an HMAC.

**PKG** The PKG should not be able to bring down the proposed IBE architecture as a threshold secret sharing technique between multiple PKGs is used. This means that when the PKG actively brings down its servers, the proposed IBE architecture can still be supported because there are still enough other PKGs that offer their services. However it can not be circumvented that the PKG actively generates wrong information e.g. wrong $sk_{ID}$ or $pk_{PKG}$ values to sabotage the system. However, when a user notices a malicious PKG sabotaging the infrastructure for IBE on OSNs, he can still decide to try another PKG as a threshold secret sharing technique is used.

**Other parties actively attacking the OSN** Any other party than the OSN or the PKG has a hard time trying to actively alter resources of the architecture. The OSN can not allow any party being able to shut down or alter its service. If the OSN goes down this has a negative impact on the faith of the users and the investors of the OSN. It can be assumed this is enough motivitation for the OSN to prevent external parties from bringing the OSN environment down or altering its behaviour. The OSN therefore has complete responsibility for the availability of its services.

**Other parties actively attacking the PKG** Parties that are not associated with the PKG should not be able to alter resources of the PKG. The PKG should be highly secure to prevent external parties from undesirably changing its behaviour. Denial-of-service attacks are difficult to circumvent by one PKG. However, the total number of available PKGs should be large enough such that bringing down all these PKGs at once is hard. Denying the service of one PKG then does not suffice to bring down the complete architecture because a secret sharing technique is used.

**Other parties actively attacking a user** Note that the protocol guarantees that the senders messages can be only decrypted by the profiles associated to the $ID$ strings in $\mathcal{S}$. It thereby implicitly assumes that the user knows which real life person is corresponding to the user $ID$s in $\mathcal{S}$. A malicious user can still pretend to be someone else by creating a fake profile of someone who is familiar to the sender. This, however, is a practical problem that is inherently present in OSNs and therefore is not in the scope of this protocol. Also users in $\mathcal{S}$ that are careless with their OSN login could be a thread to the confidentiality of a message. These type of active attacks can not be circumvented by any protocol or architecture because they are based on users of the OSN that are being careless and uncritical. It therefore is assumed that a user who is motivated to use IBE on OSNs, is also critical enough to know the consequences of careless behaviour on his privacy.

**Intended receivers breaking the social contract** Another problem arises when an intended receiver in $\mathcal{S}$ decrypts a message and then broadcasts the plain text to all his connections in $\mathcal{A}_{ID}$ or sells this information to third parties. This would be a compromise of the social contract between the sender and the intended receiver. It is therefore assumed that every sender can trust any intended receiver in $\mathcal{S}$ such that no violation of the social contract neither careless behaviour by the receiver will ever take place.