Survey on forward and post-compromise security notions for PKI, (H)IBE, and RBE

HiWi position/Bachelor's Thesis

To realize public-key encryption, the encrypting/sending party, say Alice, needs to somehow learn the public key of the receiving party, say Bob. In practice, this is realized through a **public key infrastructure (PKI)**. However, there are alternatives that are especially interesting for large organizations:

- **(Hierarchical) identity-based encryption ((H)IBE):** In IBE, a trusted party generates a *master public key* mpk (and *master secret key* msk). Given msk and an identity id (say `bob@big.org`), the trusted party can derive a user secret key $\mathrm{usk}_{\mathrm{id}}$ for id. Given only mpk and an identity id, any party can encrypt directly for id. Thus, a single mpk replaces the whole PKI, but a trusted party is required to hold msk and can derive all user secret keys. This leads to key-escrow problem and a single point of failure.
- **Registration based encryption (RBE):** To resolve the key-escrow problem, RBE was proposed. In RBE, a *key aggregator* compresses a public list $(\mathrm{pk}_1, \mathrm{id}_1), \ldots, (\mathrm{pk}_N, \mathrm{id}_N)$ of public keys and identity strings into one digest key dpk. Now, dpk plays the role of the IBE mpk.

These three approaches, PKI, (H)IBE, and RBE offer different tradeoffs. For example:

- **PKI:** Retrieving the public key(s) for an identity by interacting/querying the PKI.
  - Pros: Simple and high security. Delivery of pks is the only single point of failure.
  - Cons: Need PKI infrastructure, need to download keys for ("unknown") identities. Need to trust PKI.
- **(H)IBE:** Given the master public key (of an organization), we can encrypt to any identity.
  - Pros: One public key per organization is enough to encrypt to all identities (even "unknown" ones).
  - Cons: Key-escrow problem. Single point of failure.
- **RBE:** Publicly computable aggegrate "master public key". Can encrypt to any aggegrated identity.
  - Pros: Solves key-escrow problem and single point of failure of (H)IBE.
  - Cons: Current schemes are completely impractical and it's unlikely they can compete with optimized (H)IBE. Need to trust aggregator, but have small aggregate dpk.

Scope of the work

The goal of this work is to compare the approaches that PKI, (H)IBE, and RBE especially w.r.t. forward security that they (can) offer. Here, forward security ensures that "past" ciphertexts hide the message, even if the secret key of a user is leaked in the future. In particular, this entails

- a literature review about existing notions of forward security;
- a categorization of these as well as the threat models;
- an evaluation of their suitability within the context of approaches (PKE, (H)IBE, RBE);
- and a comparison between the approaches.

If no suitable notions or threat models exist, or existing notions fail to appropriately capture the setting, then fixes or new notions should be proposed. and post-compromise

Requirements

Given the breadth of notions, this is a long-term HiWi topic or a very challenging bachelor's thesis. Following prior knowledge is helpful.[1]

- Theoretical foundations of cryptography and provable security are essential.
- A good grasp of security notions and modelling is important.
- Prior knowledge of advanced encryption notions is helpful, e.g., IBE is introduced in the lecture "Authentifizierung und Verschlüsselung".
- Detailed knowledge of inner workings of (H)IBE and RBE is not required, but basic familiarity may be necessary for systematization.

[1] It is customary to *cite the published versions* but **read the full version** of conference publications, found e.g., directly at the Cryptology ePprint Archive, via dblp, or other search engines. The shortened conference versions can be hard to follow.

Contact

In case of interest or for further information, please contact Michael Klooß, michael.klooss@kit.edu.