Practically usable IBE for Online Social Networks

Online sharing platforms are becoming an important means of communication, replacing for instance email and IRC chat. Users disclose intimate thoughts on Facebook, blog about their political views, upload holiday pictures to Google Plus, and publish their current activities on Twitter. Currently users have to rely on those service providers if they want to limit the access to their data. This is not always ideal as the access control settings are usually difficult to configure correctly, or they produce leakages due to system bugs. Sometimes data is even leaked on purpose (sold) to third parties. These issues make users sensitive to data privacy leaks.

Systems like Scramble! propose cryptographic techniques as a solution to address privacy issues in online platforms. Instead of publishing content in clear, Scramble! allows the user to publish the encryption version. In this way, only the people the user wants, have access to the content, leaving others oblivious. However, Scramble! doesn't solve the difficult problem of key management.

Goal: The expected work for this project is to explore a better key management and encryption protocol for social networks, such as Identity Based Encryption (IBE). The student should evaluate and implement IBE within Scramble! and social networks like Facebook. Additionally, an evaluation of the security and efficiency levels of the application and used algorithms should be performed. In the end, the final application should become an easy to use (and easy to install) open source project, efficient enough for daily use by non-experts.

Requirements: The student(s) should have notions of scripting programming as well as cryptography, and be willing to develop these skills during the project.

More information can be found at `https://www.cosic.esat.kuleuven.be/scramble`.

Practicalities

Promotor:	Bart Preneel
	Vincent Rijmen
Daily supervision:	Filipe Beato filipe.beato@esat.kuleuven.be office 01.65
Nature of the work:	30% literature, 30% theoretical work, 40% software
Number of students:	1 or 2

