Crypto-Book: Privacy Preserving Online Identities

John Maheswaran (PhD student), David Wolinsky, Bryan Ford
Yale University

Social networking sites are popular and users find it convenient to use the identities from these sites for cross-site authentication however this creates privacy and tracking risks.

We propose *Crypto-Book*[1], a new architecture combining social networking, public key cryptography and ring signatures to provide a framework for usable, privacy preserving online identity management. Our architecture leverages existing social network identities, but augments them with one or more additional *key servers* that convert the social network identities into public/private keypairs and enable users to use those keypairs in anonymity preserving ways through the use of ring signatures [2, 1]. Additionally we propose a secure, anonymous private key pickup protocol along with an implementation based on email.

System Architecture: Figure 1 shows the overall system architecture. The client user logs into their online social networking site such as Facebook and is provided with an OAuth token by the Facebook (or other social networking site) API.

The client securely sends their OAuth token to each of the key servers. Each keyserver is tasked with maintaining a public/private keypair associated with each social network identity. On receipt of the client's Facebook OAuth token, each keyserver obtains that client's private key part and returns it to the client over the secure connection, the client combining the private keys to form their composite private key.

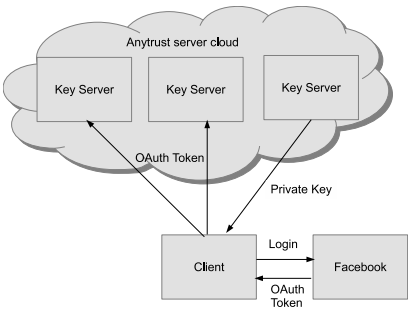

Figure 1: Overall System Architecture

Once a client has obtained their own private key and a list of public keys corresponding to other Facebook identities, the client constructs a ring signature [2, 1] with all the Facebook identities as the anonymity set. A ring signature has the property that a third party can verify using only the public keys that the signature was created by one of the members of the anonymity set. However they cannot determine which person in the anonymity set specifically created the signature.

The ring signature is now used by the user as a form of anonymous online identity and could be used in a multitude of different scenarios. For example the user could anonymously sign a document to give a credible leak, join an anonymous chat group open only to a specific set of users, or anonymously comment on blog posts.

Anonymous Key Pickup: We propose a protocol that allows Alice to collect her private key part from a key server without the key server knowing Alice has picked up her private key. Alice securely connects through an anonymity network to the key server. Alice supplies a list of email addresses including her email along that form the anonymity set. The server generates a private key for each email address and encrypts it using the same single symmetric key. The server securely sends to Alice the symmetric encryption key along.

Each key is attached to an email and sent out such that each email address only receives their own encrypted private key. Alice then decrypts her private key part received via email. Alice has anonymously got her private key, the server cannot identify who collected their key.

[1] `http://www.crypto-book.com/`

References

[1] R. Rivest, A. Shamir, and Y. Tauman. How to leak a secret: Theory and applications of ring signatures. In *Essays in Memory of Shimon Even*, pages 164–186, 2006.

[2] R. L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In *Advances in Cryptology - ASIACRYPT 2001*, pages 552–565. Springer, 2001.