Distributed Public-Key Infrastructure With Short Keys

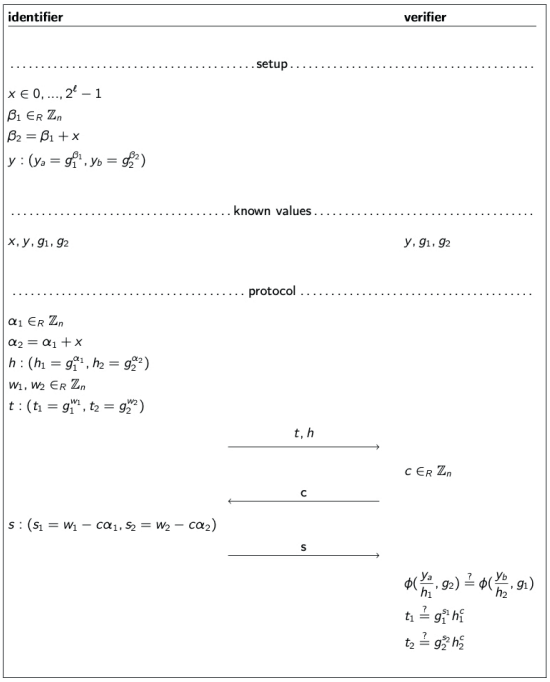
Degree programme: BSc in Computer Science | Specialisation: IT Security
Thesis advisor: Prof. Dr. Rolf Haenni
Expert: Jean-Marie Leclerc

We present an identification protocol based on pairing-based cryptography over elliptic curves. With this protocol, it is possible to generate sufficiently short keys, which can be entered by human users on a regular keyboard, that is without requiring special hardware. An implementation of this protocol into a real-world usecase is realized as well.

Problem

User identification is one of the most widely implemented processes on the internet. There is nearly no website without a login form. Almost every website offers a possibility to identify a user on their sites. Usually, the identification is done by entering an user ID and the corresponding password, making it the most common way to digitally identify someone.

However, time has shown that an identification via password has many security-relevant flaws. For this reasons, security specialists have developed new alternatives to securely identify entities over the internet. Unfortunately, they have a common denominator called hardware. They need for example a token to securely safe the certificate or a reader to scan the biometric information. Hardware-based solutions are expensive and also require suitable interfaces, which makes them to a disadvantage. Here is where this work comes into play.



Interactive PBC Identification Scheme

Solution

In this project we designed and implemented an identification scheme that allows a user-friendly key transportation solution which is independent of formats, operating systems, network, hardware and more. This scheme uses bilinear mapping with pairing based cryptography (PBC) over elliptic curves.

A huge advantage of our PBC identification scheme is, that the same security strength can be reached as other cryptographic systems by using much shorter keys. It was possible to reach the same security requirements with only a 112-bit key instead of a 2048-bit key like in RSA. By using a base32 encoding, a 112-bit key consists at most of 23 symbols. That is only 7 character longer than a credit card number. Hardware is no longer required to save the private key. The user can just easily retype it from a piece of paper.

We implemented this scheme into three use cases to show the possible domains where it can be used. Our most advanced solution is use case 3. It has a distributed key generation that publishes the partial public keys to a trusted certification authority and sends the partial private keys to the recipients. The final private key is calculated by the recipient and therefore only visible to the recipient during the whole time. Even if a private key gets lost with the post order, nothing can be done with that key.

We recommend the idea of this scheme for solutions needing a high security level and who does not want to depend on any hardware for key distribution or key storage. It is also not recommended to use this scheme on platforms that need a frequently identification because of the cumbersome manual retyping of the key.

Bruno Miguel Fernandez Dinis

Mathew Thekkekara