Contribution ID: **75** Type: **Presentation**

Asymmetric Cryptography Hands-On

Tuesday 15 April 2014 12:20 (1 hour)

Symmetric cryptography uses the same key for encryption and decryption of a message and implies that all communicating parties know the key, which itself must have been exchanged over a secure channel.

Asymmetric cryptography mechanisms use two different keys: one for encryption and another for decryption, and this means that everything that has been encrypted with one key can only be decrypted with the other. Making one of the keys known to the public - the "public"key –means that any system can encrypt the message with the public key of the key holder (receiver), prior to sending.

I explore the mathematical background, security analysis, possible various attacks and explain why asymmetric algorithms cannot substitute symmetric ones, but just complement each other. The presentation gives hands on experience with digital signatures, certificates and Single Sign On (SSO) - a mechanism permitting users to access multiple Information Systems with a single user authentication action.

Primary author: PATER, Lukasz Piotr (CERN)

Presenter: PATER, Lukasz Piotr (CERN)

Track Classification: Information Security