

## **Smartphone authentication for mobile users using untrusted computers**

Anna Vapen, PhD student, Linköping University, 2009-04-30

Prof. Nahid Shahmehri

Users of web applications are mobile in the sense that they use different computers, for example at work, at home or at an Internet café. These computers can be considered untrusted since they can contain keyloggers and malware. When a user logs in to use a web application there is a need for an authentication method that is secure even if the computer cannot be trusted, and that can be used on any computer anywhere.

Normally usernames and passwords are used in simple authentication solutions. The problem is that users need to remember a large variety of different usernames and passwords. For a password to be secure it needs to be relatively complex which makes it difficult to remember. To use complex passwords there is a need for secure storage of the passwords, or an alternative method such as using one-time passwords and challenge-response where the user is presented with a challenge that only this user can give the correct response to.

Both for storage of passwords and for running a cryptographic application that calculates a response we need a trusted environment that can be reached by the mobile user. Many security-conscious organizations, specifically in the areas of e-commerce and online banking, use hardware security tokens for authentication. The token can be for example a smartcard, a USB-stick or other hardware specific for the application. In recent years mobile phones have been used in authentication solutions and identity management. Because of their prevalence, mobile phones are an excellent platform for something the user wants to have available at all times.

Using a smartphone, an enhanced mobile phone similar to a PDA, we get access to a rich set of input channels (e.g. camera, voice, keypad, touch screen, accelerometers, GPS etc) and communication channels (long distance as GSM/WCDMA, WiFi etc and short distance as Bluetooth, NFC etc). They also contain trusted hardware in the form of a SIM or USIM card.

An interesting challenge with using a smartphone as a hardware security token is to explore its interactive features to be able to create a highly usable and fast authentication solution that can provide a high level of security in security critical settings as well as for simpler services like social networks, e-mail and blogs. One solution that we are investigating is the possibility of using optical input as part of an authentication process where the user has a smartphone as a hardware token.