Project Description:

Device Pairing for Mobile Devices

Application Scenario

It is sometimes required for people on the move to set-up temporary, or even permanent, connections between mobile devices. These connections require cryptographic keys to be established in an ad-hoc but secure manner, e.g. for transferring data, such as images or movies, between the two devices. The generation of such temporary keys cannot rely on external services, such as Key Distribution Centers or a PKI, but may instead rely on the sensing capabilities of the two smart devices, e.g. the reading from accelerometers if the two devices are shaken together or the ability of both devices to determine what network connections are available and possibly event to see if the two devices are observing the same network traffic (headers of packets sent over the network).

The sensor data simultaneous read by two devices at the same time may be used as input parameters for a key derivation function (KDF) on the two devices, thus generating the same key on the two devices to be used in a symmetric algorithm. It is important that both devices read the same sensor values at the same time and that nobody else are able to read or infer the parameter values that are intended to be used by the KDF.

Project Definition

Design, and evaluate a system for device pairing, i.e. simultaneous generation of a shared secret on two mobile devices that can be used to generate a shared secret-key for symmetric cryptography. Issues that *must* be addressed are:

- Identification of appropriate input parameters for a key derivation function that may be simultaneously generated on two devices at the same time.
- Identification of a suitable key derivation function for the chosen parameters.
- Risk analysis: What assets are at stake?
- Threat model; you should explicitly state what threats your system has been designed to handle, e.g., ballot box stuffing, vote selling, etc.
- Security: Make sure that your system protects against the security issues raised in the threat model, and clearly document the threats that you do not protect against.