Sense the Key: Key Management for Mobile Devices - Demo Proposal -

Christian Rohner, Fredrik Bjurefors, Henrik Andersson
Uppsala University

We approach secure key management on mobile devices by using sensor data to generate shared secrets. Under the assumption that two devices in proximity sense the environment sufficiently similar, we process the sensor data into (pseudo) random bit-strings used as input to a cryptographic key agreement algorithm. The attendees of our demo are invited to experiment with two different sensors, accelerometers and microphones.

We further present a novel approach to key exchange following the drag&drop paradigm: The user points with a camera equipped mobile phone to a visual code printed on a device, holds down a button, and releases it when pointing to the visual code of another device. The mobile phone uses the information encoded in the visual key to transfer the public key from one device to the other.

1 Key Generation for Mobile Devices

Attendees of our demo will be introduced to the idea of using sensor data to generate shared secrets: The information extracted from the sensors has to be both *random* and *similar enough* such that two devices can use it to agree on a common secret[1]. Achieving either of these properties is trivial, but it is non-trivial to achieve both at the same time. The visitor of our demo can experiment with two types of sensors and try the usefulness and stability of some of our algorithms:

- *Accelerometer:* Holding two devices equipped with accelerometers in one hand will generate a secret key based on the shaking pattern. This approach is usable with small mobile devices.
- *Microphones:* The perceived acoustics within a room is different at different locations. Noisy environments as the demo room might be particularly suited for that type of sensor.

The progress of the key agreement protocol and the randomness of the shared key is visualised in graphical form as the demo proceeds. The visualisation will be on two laptop computers to which the devices are connected to.

The technical contribution of the system is the extraction of relevant information from the sensor data.

[1] We use the key agreement protocol from Maurer [1] where the two devices can agree on a shared key by communicating over a public channel.

2 Drag&Drop Key Exchange

We use a camera equipped mobile phone (Nokia N70) to initiate secure communication between two devices. By decoding the visual code printed on the two devices, the mobile phone gets information about the public key and the Bluetooth address of the devices, authenticates them with a challenge-response protocol, and transfers the public keys to the respective other device. The protocol is implemented following the drag&drop paradigm – using the camera as a pointer – to make the usability as intuitive as possible.

The progress of the key exchange protocol is visualised on a laptop computer which is one of the devices to be initiated for secure communication. The current version of the demo uses simple colour codes and is a proof of concept. Bluetooth address and public key are not encoded on the visual code itself. However, the mobile phone recognises the colour code and requests the information from a repository.

Note to the Demo Organiser

The demo does not have special requirements other than a demo booth/table.

References

[1] Ueli Maurer. Secret key agreement by public discussion. *IEEE Transaction on Information Theory*, 39(3):733–742, May 1993.