Shake well before use: two implementations for implicit context authentication

Rene Mayrhofer and Hans Gellersen

Lancaster University, Computing Department, South Drive, Lancaster LA1 4WA, UK
{rene,hwg}@comp.lancs.ac.uk

Abstract. Secure device pairing is especially difficult for spontaneous interaction in ubiquitous computing environments because of wireless communication, lack of powerful user interfaces, and scalability issues. We demonstrate a method to address this problem for small, mobile devices that does not require explicit user interfaces like displays or key pads. By shaking devices together in one hand for a few seconds, they are securely paired. Device authentication happens implicitly as part of the pairing process without the need for explicit user interaction "just for security". Our method has been implemented in two variants: first, for high-quality data collection using wired accelerometers; second, using built-in accelerometers in standard Nokia 5500 mobile phones.

1 Introduction

Device pairing over wireless channels is insecure because of the possibility of man-in-the-middle and impersonation attacks. To safeguard against such threats, device-to-device communication needs to be authenticated. However, in the case of spontaneous interaction, only the user who initiates the interaction can distinguish between the intended target and other similar devices or malicious attackers. Such an authentication is difficult because of two reasons: many devices lack explicit user interfaces like displays and keypads that could be used to verify the device pairing, and explicit authentication does not scale when considering hundreds of spontaneous interactions a day.

Context-based authentication is one approach to address both issues, by using implicit sensory input and thus making authentication unobtrusive. Shaking two (or multiple) devices together is one option for device pairing. It has first been suggested by Holmquist et al. [1] as a possible user interaction method and subsequently been studied by others [2,3].

When devices are being shaken together, they will experience similar acceleration values. In addition to the user interaction for selecting devices to pair with, these sensor data streams can be used as input for secure authentication. Our demonstration applications build upon the authentication method introduced previously [4]. We present two specific implementations of this method. The first is used for high-quality data collection, interactive experimentation, and optimization of parameters and algorithms, and is based on wired accelerometers and laptop or desktop PCs. The second runs on off-the-shelf Nokia 5500 mobile phones and uses their embedded 3D accelerometers.

2 Authentication based on shaking

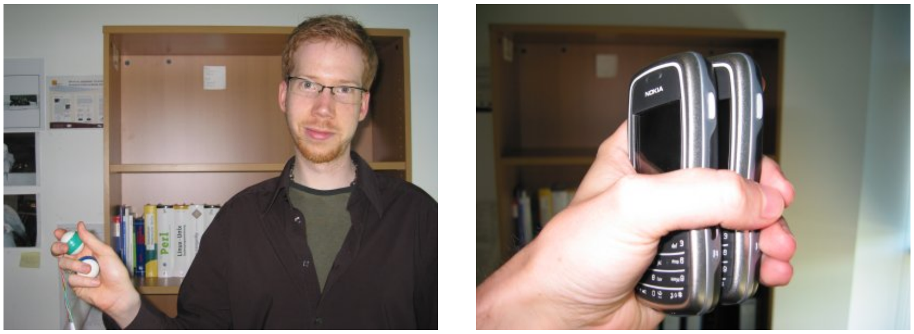
Our authentication method as described in detail in [4] consists of five tasks. The first three pre-processing tasks *sensor data acquisition*, *temporal alignment* and *spatial alignment* are executed locally and independently on each device and serve to extract and normalize *active segments*, which represent the accelerometer time series during shaking. Based on these active segments, the final two tasks *feature extraction* and *key generation* may interactively communicate with the remote device(s) over insecure wireless channels such as IEEE 802.11 wireless LAN or IEEE 802.15 Bluetooth to generate authenticated, secret shared keys on all devices shaken together.

We have proposed two different protocols for implementing the final two tasks. Both have the same aim of generating an authenticated, secret shared key from sensor time series, but achieve this with very different designs. The first protocol uses a conservative design and well-understood cryptographic primitives in two phases, key agreement and key verification. In the first phase, based on unauthenticated Diffie-Hellman key agreement, the devices agree to secret shared keys over the wireless channel. Using these keys in the second phase, they run an extended variant of the interlock protocol to exchange their recorded active segments in a way that detects man-in-the-middle attacks. Finally, the devices can locally and independently compare their local with the respective remote sensor data and verify if the pairing process should succeed or not. Our current implementation uses the coherence metric, but different devices can use different means of comparing active segments.

The second protocol is more unconventional and generates the secret shared key directly from sensor time series. To this end, the feature extraction task computes exponentially quantized, pairwise added FFT coefficient vectors over sliding windows of the active segments. These feature vectors are used as input to a *Candidate Key Protocol* (CKP) [5], which broadcasts one-way hashes of the vectors as so-called candidate key parts. If a receiving device can compute the same one-way hash, it has verified that its sensor input matches that of the sender without actually revealing it to eavesdroppers. After a sufficient number of such matching key parts have been collected, they are concatenated and hashed again to create a so-called candidate key, which is again broadcast. If one or multiple remote devices can generate the same key, it is acknowledged and can be used for subsequent secure communication. The second protocol is more dynamic and scalable, as it allows remote devices to "tune into" the key stream of another. On the other hand, the first protocol is more flexible in terms of using different methods of comparison and is considered more secure against offline attacks.

3 Implementation for data collection and experimentation

The sensor data acquisition task of our first implementation uses four ADXL202JE accelerometers, two per device mounted at an angle of 90° and set to output pulse-width modulation at about 600 Hz sample rate with a maximum acceleration of 2 g. The primitive sensor boards are fixed within ping-pong balls using



(a) Implementation 1: wired accelerometers for high-quality data collection

(b) Implementation 2: off-the-shelf Nokia 5500 mobile phones

Fig. 1. Two implementations of the "Shake well before use" authentication method

compressed foam so that they will remain constant inside the balls, but with arbitrary (and from the outside unknown) orientation (see Fig. 1a). All eight pulse-width modulated output channels are connected directly to a standard parallel port and polled at around 1 MHz, resulting in a resolution of around 10 bits per sample.

A simple ASCII coding of this sensor data stream acts as the interface to a Java-based implementation, where it is down-sampled to either 128 Hz or 256 Hz for the remaining two pre-processing tasks and implementations of both cryptographic authentication protocols. The first protocol uses TCP channels for communication, while the second one uses UDP multicast packets. Their respective results are displayed in a simple GUI to give immediate user feedback during interactive experimentation.

4 Implementation on off-the-shelf mobile phones

Our second implementation runs on off-the-shelf Nokia 5500 mobile phones, which feature an integrated 3D accelerometer (see Fig. 1b). A background Symbian application is started automatically and uses the Nokia Sensor API to access the accelerometer data at its pre-set sample rate of around 30 Hz [6]. It opens a TCP socket for streaming a binary coding upon request.

The remaining pre-processing tasks as well as an implementation of the first protocol using Bluetooth RFCOMM communication are contained within a Java MIDlet that connects to the TCP socket provided by the Symbian part. Bluetooth as a wireless communication channel poses two challenges for the implementation: there is no broad- or multicast, and inquiry as well as service discovery are slow for user interaction. Our implementation addresses this by performing the first phase of the protocol, namely Diffie-Hellman key agreement, opportunistically. Whenever a compatible device is found by the regular background inquiry process, an unauthenticated secret shared key is established with it. The second phase is started as soon as a valid active segment segment has been collected and exchanges it with all remote devices for which a shared key is already known. Those devices that have been shaken together will then verify that their respective active segments are similar enough and thereby authenticate the secret shared key.

5 Conclusions

We present a method for secure device pairing based on shaking devices together. Two different implementations show different aspects; while the first, wired implementation allows easier experimentation, rapid prototyping of new algorithms for comparing similarity of active segments, and high-quality data collection, the second one demonstrates that the method can be used on resource limited devices like mobile phones. Using Bluetooth as a communication channel poses new challenges, which are partially addressed by implementing opportunistic key agreement.

Our complete, open source implementations are available at http://www.openuat.org.

Acknowledgments

We gratefully acknowledge support by the Commission of the European Union under the FP6 Marie Curie Intra-European Fellowship program contract MEIF-CT-2006-042194 “CAPER”.

References

1. Holmquist, L.E., Mattern, F., Schiele, B., A., P., Beigl, M., Gellersen, H.W.: Smart-its friends: A technique for users to easily establish connections between smart artefacts. In: Proc. UbiComp 2001, Springer-Verlag (September 2001) 116–122
2. Lester, J., Hannaford, B., Borriello, G.: “Are you with me?” – Using accelerometers to determine if two devices are carried by the same person. In: Proc. Pervasive 2004, Springer-Verlag (April 2004) 33–50
3. Marin-Perianu, R., Marin-Perianu, M., Havinga, P., Scholten, H.: Movement-based group awareness with wireless sensor networks. In: Proc. Pervasive 2007, Springer-Verlag (May 2007) 298–315
4. Mayrhofer, R., Gellersen, H.: Shake well before use: Authentication based on accelerometer data. In: Proc. Pervasive 2007, Springer-Verlag (May 2007) 144–161
5. Mayrhofer, R.: The candidate key protocol for generating secret shared keys from similar sensor data streams. In: Proc. ESAS 2007, Springer-Verlag (July 2007) 1–15
6. Vajk, T., Bamford, W., Coulton, P., Edwards, R.: Using a mobile phone as a ’Wii like’ controller. In: Proc. CyberGames 2007. (September 2007) *to appear.*