Accepted Manuscript

LiReK: A lightweight and real-time key establishment scheme for wearable embedded devices by gestures or motions

Zitao Chen, Wei Ren, Yi Ren, Kim-Kwang Raymond Choo

PII: S0167-739X(17)30566-6
DOI: https://doi.org/10.1016/j.future.2017.10.008
Reference: FUTURE 3747

To appear in: *Future Generation Computer Systems*

Received date : 5 April 2017
Revised date : 7 August 2017
Accepted date : 5 October 2017

Please cite this article as: Z. Chen, W. Ren, Y. Ren, K.-W.R. Choo, LiReK: A lightweight and real-time key establishment scheme for wearable embedded devices by gestures or motions, *Future Generation Computer Systems* (2017), https://doi.org/10.1016/j.future.2017.10.008

LiReK: A Lightweight and Real-time Key Establishment Scheme for Wearable Embedded Devices by Gestures or Motions

Zitao Chen[a,e], Wei Ren[a,b,e], Yi Ren[c], Kim-Kwang Raymond Choo[d,a]

[a] *School of Computer Science, China University of Geoscience, Wuhan, P.R. China*
[b] *Hubei Key Laboratory of Intelligent Geo-Information Processing, China University of Geosciences (Wuhan), Wuhan, P.R. China*
[c] *School of Computer Science, University of East Anglia, Norwich, UK*
[d] *Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, USA*
[e] *Guizhou Provincial Key Laboratory of Public Big Data, GuiZhou University, Guizhou, P.R. China*

Abstract

With the recent trend in wearable technology adoption, the security of these wearable devices has been the subject of scrutiny. Traditional cryptographic schemes such as key establishment schemes are not practical for deployment on the (resource-constrained) wearable devices, due to the limitations in their computational capabilities (e.g. limited battery life). Thus, in this study, we propose a lightweight and real-time key establishment scheme for wearable devices by leveraging the integrated accelerometer. Specifically, we introduce a novel way for users to initialize a shared key using random shakes / movements on their wearable devices. Construction of the real-time key is based on the users' motion (e.g. walking), which does not require the data source for key construction in different devices worn by the same user to be matching. To address the known limitations on the regularity and predictability of gait, we propose a new quantization method to select data that involve noise and uncertain factors when generating secure random number. This enhances the security of the derived key. Our evaluations demonstrate that the matching rate of the shake-to-generate secret key is up to 91.00% and the corresponding generation rate is 2.027 bit/sec, and devices worn on human participant's chest, waist, wrist and carried in the participant's pocket can generate 4.405, 4.089, 6.089 and 3.204 bits random number per second for key generation, respectively.

Keywords: Lightweight; Key Management; Real-time; Body Sensor Networks; Embedded Devices

1. Introduction

Advances in both hardware (e.g. embedded wireless microelectronic components) and software have contributed to the popularity of wearable and embedded devices. These devices typically offer ubiquitous computing. For example, embedded sensors can be used to monitor the real-time physiological status of users and can be applied in a wide range of situations, such as in healthcare and allied health services (e.g. counting of steps, tracking of heart rate, and monitoring of glucose levels) [1, 2]. However, these devices are generally not designed with security in mind [3, 4, 5, 6]. The amount and nature of data and services these wearable devices can have access to (e.g. the user's private data), as well as the limitations of these devices (e.g. resource-constrained), require us to rethink how we design security solutions for wearable devices [7, 8, 9, 10].

Due to the limitations in the computational capability of the underlying hardware, a number of existing cryptographic solutions such as key establishment protocols may not be fit-for-purpose. For example, the Diffie–Hellman (DH) key exchange is usually employed in existing key management schemes. However, DH key exchange implementations require complex cryptography computations such as modular-exponentiation operation. Thus, the overheads may be beyond the existing capability of resource-constraint wearable devices.

It is important to be able to establish a secure session between two devices particularly those worn by the same user, as these wearable devices require frequent data exchange between devices (e.g. transmitting a user's health-related information such as glucose level and heartbeat counts between the smartwatch to a paired mobile device, so that the information can be sent to the hospital network). A successful compromise could have real-world implications. For example, if a malicious attacker successfully changes the glucose level or heartbeat counts of a particular user, this would result in delivery of the wrong medication or treatment plan and lead to fatality. Undeniably, security is an important factor to be considered in wearable devices, particularly those deployed in real-world applications. It is, therefore, unsurprising that designing lightweight and real-time cryptographic solutions such as key establishment protocols is of ongoing research interest [11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21].

One challenge in designing lightweight cryptographic solutions such as key establishment protocols is providing an optimal security assurance without incurring excessive en-