ARTICLE IN PRESS

Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

A variant of password authenticated key exchange protocol

Yuexin Zhang [a,b], Yang Xiang [a,b], Wei Wu [c,*], Abdulhameed Alelaiwi [d]

[a] Centre for Cyber Security Research, Deakin University, Geelong, VIC 3220, Australia

[b] The State Key Laboratory of Integrated Services Networks, Xidian University, China

[c] Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, 350117, China

[d] King Saud University, Riyadh, 11543, Saudi Arabia

HIGHLIGHTS

- The proposed protocol is a cross-layer design.
- Two users extract a short secrets at the physical layer.
- Using the extracted secrets, two users establish a secret key at higher layers.
- Comparing with other related protocols, the new protocol achieves a better performance.
- The protocol is proved secure in the standard model.

ARTICLE INFO

Article history:
Received 19 April 2016
Received in revised form
12 January 2017
Accepted 8 February 2017
Available online xxxx

Keywords:
Secret key
Password
Mobile devices
Physical layer
Higher layers
Internet of Things
Fog computing

ABSTRACT

Password authenticated key exchange (PAKE) protocols are designed for a pair of users to establish a secret session key over a public and unreliable network. In existing PAKE protocols, it is assumed that short passwords are pre-shared between users. This assumption, however, would be impractical in certain applications. For instance, in the Internet of Things and Fog computing, billions of devices will be wirelessly connected. In practice, the devices are produced by different factories, and it is not practical to assume that these devices are pre-loaded with passwords when they leave factories. As a result, existing PAKE protocols cannot be directly employed in these applications. Moreover, it is investigated that devices can extract secrets using the wireless fading channel. However, the key extraction rate at the physical layer is slow. Motivated by these observations, this paper presents a variant of password authenticated key exchange (vPAKE) protocol without the password sharing assumption. To obtain the passwords, wireless devices, such as mobile phones, tablets, and laptops, are used to extract short secrets at the physical layer. Using the extracted secrets, users can establish a secret key at higher layers. The performance analysis shows that comparing with other PAKE protocols (which are proved secure in the standard model), the communication and computation consumptions of our protocol are significantly reduced. Additionally, the proposed protocol is proved secure in the standard model.

1. Introduction

The "pay-as-you-go" Cloud computing model provides an efficient mechanism to enable ubiquitous, on-demand access to a shared pool of configurable computing resources, such as networks, servers, storage, applications, and services. In practical applications, an emerging wave of Internet deployments requires mobility support and location awareness. To meet these requirements, a new platform, i.e., Fog computing, is designed in [1]. Specifically, the Fog is a cloud close to the "ground", and it enables applications on billions of connected devices, which are already connected in the Internet of Things (IoT), to run directly at the network edge [2,3]. Fig. 1 shows a brief structure of Fog computing.

As shown in Fig. 1 that, Fog servers adopt certain wireless interfaces, e.g., WiFi and Bluetooth, to connect with mobile users. Furthermore, mobile users can wirelessly connected with each other. To secure the communications, cryptographic keys are needed to provide confidentiality, integrity, and authentication services [4].

* Corresponding author.
E-mail addresses: yuexinz@deakin.edu.au (Y. Zhang), yang.xiang@deakin.edu.au (Y. Xiang), weiwu@fjnu.edu.cn (W. Wu), aalelaiwi@ksu.edu.sa (A. Alelaiwi).

http://dx.doi.org/10.1016/j.future.2017.02.016
0167-739X/

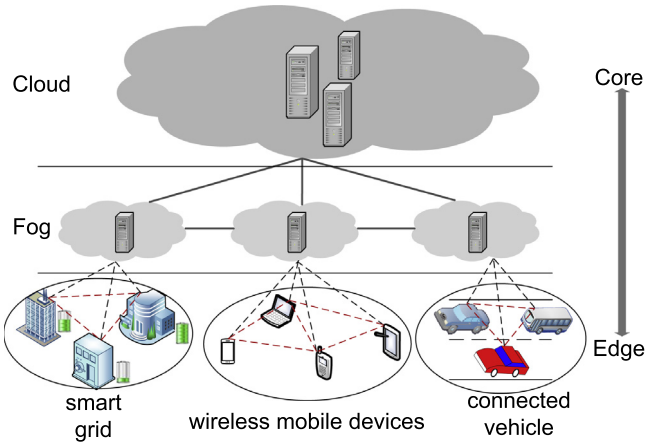

Fig. 1. A brief structure of Fog computing.

As one type of key establishment protocols, the password authenticated key exchange (PAKE) protocol has been widely studied.

Until now, many efforts have been devoted to the design of secure PAKE protocols. The seminal work in this area was proposed by Bellovin and Merritt (BM) in [5] (the so-called encrypted key exchange protocol). Then Bellare, Pointcheval, and Rogaway proved the security of BM protocol in the ideal-cipher model [6]. Due to its simplicity, the BM protocol became the basis of other protocols [7–10]. Though protocols [5–10] are quite efficient, the use of the ideal-cipher model is a strong assumption. To avoid using the ideal-cipher model, several PAKE protocols are designed and proved secure in the standard model. As the first practical PAKE protocol in the standard model, protocol [11] was proposed by Katz, Ostrovskky, and Yung (KOY) in 2001, and it was proved secure in the standard model under the decisional Diffie–Hellman (DDH) assumption. Inspired by this work, protocols [12–17] are proposed based on the KOY protocol. However, comparing with [5–10], protocols [11–17] consume considerable communication and computation resources (details of these protocols and performance comparison of them will be presented in Sections 2.1 and 6, respectively).

In existing PAKE protocols, it is assumed that short passwords are pre-shared between users. Using the pre-shared passwords, users can establish secret session keys over the public and unreliable network. However, the password sharing assumption may become impractical in certain applications. For instance, it is estimated that 50 to 100 billion devices will be wirelessly connected to the Internet of Things (IoT) by 2020 [18]. Specifically, the devices are produced by different factories, and they are integrated with different technologies. Thus, it is not a practical assumption that all these devices are pre-loaded with certain secrets when they leave factories. As a result, the password sharing assumption would not be practical in some situations.

Motivated by these observations, in this paper, we aim to design an efficient PAKE protocol without the password sharing assumption. To achieve this goal, we need to find a mechanism such that users can obtain short secrets without using any pre-shared secrets and the on-line trusted third party. Looking at our daily lives, we always have wireless devices, such as mobile phones, tablets, and laptops, at hand. Specifically, it is predicted by Cisco that the average connected devices per person will reach 6.58 in 2020 [19]. Thus, it is a desirable choice to obtain the secrets with the aid of these devices.

Recently, there is an increasing interest in extracting secret bits using the wireless fading channel. In the typical multipath environments, the wireless channel between two users Alice and Bob experiences a time-varying, stochastic fading between the transmitted and received signals. Specifically, the fading is unique, location-specific and reciprocal. Namely, it is invariant within the channel

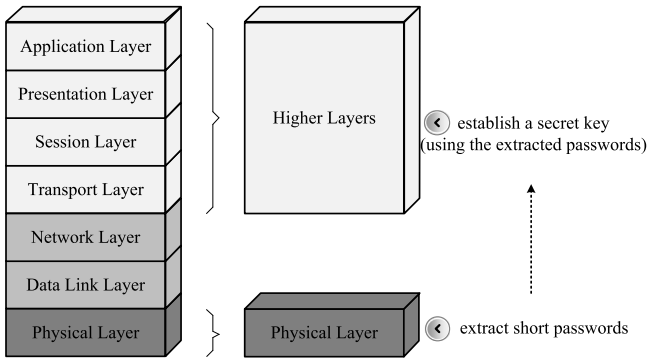

Fig. 2. The system model of our vPAKE protocol.

coherence time[1] whether the signals are transmitted from Alice to Bob or from Bob to Alice. However, the key extraction rate at the physical layer is quite slow (around 1 bit/s, please refer to Section 2.2 for details). Take AES-128 as an example, it needs more than 2 min to extract a secret key with 128 bits. In certain applications, this is unacceptable. However, it should be an acceptable trade-off to extract shorter secret bits (e.g. short "password") with less time consumptions.

Our contribution. In this paper, we present a variant of password authenticated key exchange (vPAKE) protocol without password sharing assumption. Specifically, our vPAKE protocol possesses the following properties:

1. Our protocol is specifically designed for assisting users, who do not pre-share any secrets and have no access to the on-line trusted third party, to establish a secret session key. Specifically, the proposed protocol is a cross-layer design. Namely, with the aid of wireless devices (e.g., mobile phones, tablets, and laptops), users in our protocol extract short passwords at the physical layer. Then, they establish a secret key at higher layers with light communication and computation consumptions. Fig. 2 shows the system model of our vPAKE protocol.
2. We compare our vPAKE protocol with other PAKE protocols (which are proved secure in the standard model). The comparison shows that in terms of communication and computation consumptions, the new protocol achieves a better performance than other PAKE protocols.
3. Under the assumptions that secret passwords can be extracted at the physical layer, and the DDH problem is hard in $\mathbb{G}$, the proposed protocol is proved secure in the standard model.

Organization of this paper. The remainder of this paper is organized as follows. We present a brief overview on the related work in Section 2. Section 3 reviews some preliminaries, i.e., the security model, the decisional Diffie–Hellman assumption, and the core idea of the key extraction algorithm. The proposed protocol is described in Section 4, and its security proof and performance comparison are provided in Sections 5 and 6, respectively. Section 7 concludes this paper.

2. Related work

This section reviews two types of key establishment protocols, i.e., password authenticated key exchange protocols (at higher layers), and key extraction protocols using the wireless fading channel (at the physical layer).

[1] In wireless communications, the channel coherence time is a statistical measure of the time duration over which the channel impulse response is essentially invariant.

Please cite this article in press as: Y. Zhang, et al., A variant of password authenticated key exchange protocol, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.02.016