一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
MoNA2017-5(2017-06)

デバイス共有のためのオンライン上の社会的関係性に基づいた認証制御の実証

稲垣　悠一† 　新熊　亮一†

† 京都大学大学院情報学研究科
〒 606-8501 京都府京都市左京区吉田本町
E-mail: †yinagaki@icn.cce.i.kyoto-u.ac.jp, ††shinkuma@i.kyoto-u.ac.jp

あらまし　近年，Airbnb や Uber に代表されるような，シェアリング・エコノミーと呼ばれる形態のサービスが成功を収めており，この市場の規模はさらに拡大を続けると予想されている．このような社会では，スマートフォンやセンサデバイス，自動運転車といったさまざまなデバイスが他者と共有されることになる．他者にデバイスを共有する際は，セキュリティの観点から，全くの他人には使用の権限を与えず親しい人ほど強い権限を与えるという認証の制御が行われることが望ましい．しかし，これらを個々のユーザに対してそれぞれ設定することは困難である．このような問題を解決するため，本稿では，オンラインの社会的関係性を利用することでデバイス共有時の認証を柔軟かつ効率的に制御するシステムを提案する．

キーワード　認証，デバイス共有，社会的関係性，受付制御

Feasibility Study on Authentication Control for Device Sharing Based on Online Social Relationships

Yuichi INAGAKI† and Ryoichi SHINKUMA†

† Graduate School of Informatics, Kyoto University
Yoshida-honmachi, Sakyo-ku, Kyoto-shi, Kyoto, 606-8501 Japan
E-mail: †yinagaki@icn.cce.i.kyoto-u.ac.jp, ††shinkuma@i.kyoto-u.ac.jp

Abstract　Services of a form called “sharing economy” as represented by Airbnb and Uber are expected to continue growing. In such a society, various devices, such as smartphones, sensors, and autonomous cars, will be shared with others. When sharing devices with others, device owners generally do not want to share their devices with strangers, while they want to grant stronger permission to their closer friends or family. However, manually configuring the permission level for each user is a great burden. Therefore, this report proposes a system that uses online social relationships for controlling authentication of device sharing.

Key words　Authentication, Device sharing, Social relationship, Admission control

1. Introduction

Over the past several years, we have witnessed great progress in wireless communications and digital electronics. These advances have enabled more and more devices, such as tablets, sensors, wearable devices, robots, and autonomous cars, to be connected to the Internet. Due to the spread of the Internet of Things (IoT) paradigm, even everyday things such as food packages, furniture, and report documents will be Internet nodes by 2025 [1]. In addition to this change, a global trend towards peer-to-peer sharing of personal assets has been suggested. This trend is called the “sharing economy” and is shown in services such as Airbnb, Uber, and Freecycle. In 2011, the sharing economy was nominated by Time as one of “10 ideas that will change the world” [2]. Furthermore, the global annual revenue of the sharing economy, which was $15 billion in 2015, is estimated to grow to $335 billion by 2025 [3].

In such a society, various devices will be shared with others. For example, in a global Wi-Fi sharing community called FON [4], members of the community share their Wi-Fi router with other members. Another example is a cloudlet [5]. By sharing computing resources with mobile devices, a cloudlet realizes mobile cloud computing and enables the mobile devices to offload computing tasks with low latency. Sensing devices in wireless sensor networks (WSNs) are also shared for various purposes. SenseWeb is an infrastructure for shared sensing, which provides greater understanding by collecting sensing data from multiple different networks [6]. Sharing airborne sensors helps efficient utilization of their spare sensing resources [7] [8]. A system called eShare enables energy exchange among shared sensors [9].

To share and utilize those devices efficiently, the permission level for each user should be able to be controlled flexibly. Device owners generally do not want to share their devices with strangers, while they want to grant stronger permission to their close friends. For example, when we share a Wi-Fi AP, we want our family to use the Wi-Fi AP longer than our friends, but we do not want to share the Wi-Fi AP with those who pass by our house. However, this flexible control is difficult because most conventional authentication methods focus on determining whether the user is trusted, not on how much the user is trusted by the device owner. Although the owner can manually configure the permission level for each user, it is a great burden.

Therefore, this report proposes a system that exploits online social relationships as a solution to the authentication problem when sharing devices. When a shared device receives an access request from a guest user, first the shared device identifies the guest user by her or his online social account. After the identification, an authentication server acquires the online social relationship between the owner and the guest user. Then, the authentication server evaluates the online social relationships and determines the permission level automatically.

The distinguishing feature of the proposed system is that online social relationships are exploited to solve the authentication problem when sharing devices. By acquiring and evaluating the online social relationship between a device owner and potential user, the proposed system automatically determines whether the user can access the shared device and her or his permission level. The owner can make efficient use of the shared device without worrying about complicated access configurations for users.

The purpose of this report is to examine the feasibility and effectiveness of the proposed system. To achieve this, this report presents a prototype system and measures the performance of the prototype system.

2. System Design

2.1 Definition of Online Social Relationship

One of the most common and familiar examples of online social relationships is found in online social networks (OSNs) [10]. OSNs are offered by social networking services (SNSs) such as Facebook, Twitter, Google+, and LinkedIn. OSNs consist of nodes and edges. Nodes represent users (more specifically, online social accounts of users) of OSNs, while edges represent social interactions among these users. The most basic social interactions that are represented by edges are friendships. Although some OSNs adopt undirected friendships and other OSNs adopt directed friendships, both types of friendships are included in online social relationships. Besides friendships, comments, messages, and reactions to other users are also examples of online social relationships.

2.2 System Architecture

2.2.1 Overview

The proposed system architecture (Fig. 1) consists of the following components: (a) authentication server, (b) shared devices, (c) owner and (d) guest user. The authentication server manages the shared devices and online social account information of the owners and guest users. According to the relationship between the owner and guest users, the authentication server decides which guest user can access which function or resource of the shared devices. A centralized architecture is adopted for the authentication server, so it can easily manage online social relationships between the owner and guest users. The shared devices are devices that can be accessed by guest users, such as tablets, sensors, wearable devices, robots, and autonomous cars. Each shared device belongs to one owner. The guest users are granted access to the shared devices according to the online social relationship with the owner of the shared device.

2.2.2 Device Registration

An owner registers devices on the authentication server before the owner starts to share the devices. When an owner registers a device, the authentication server issues a unique ID to the device. The authentication server associates the device ID with the owner's online social account information and records them in a database.

2.2.3 Authentication

The authentication flow of the proposed system is depicted in Fig. 2. Authentication consists of two phases: identification and authorization. In the identification phase (1.1–1.4), the authentication server identifies the guest users by their online social accounts. In the authorization phase (2.1–2.4), the authentication server acquires the online social relationships between the owner and the guest user, then, the shared devices control the access for the guest user based on the relationships.

Identification

(1.1) A guest user requests access to the shared device.

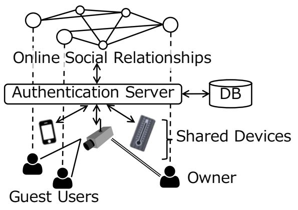

Fig. 1 Proposed system architecture

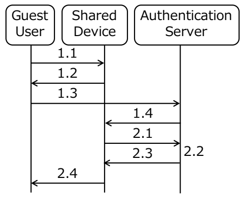

Fig. 2 Authentication flow

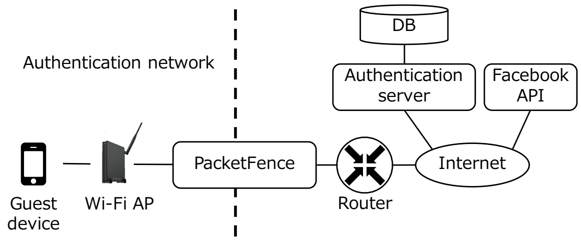

Fig. 3 Implemented prototype

(1.2) The shared device requests the guest user to sign in to the authentication server. (1.3) The guest user signs in to the authentication server with the guest user's online social account. (1.4) The authentication server notifies the shared device that the guest user has completed signing in to the authentication server.

Authorization

(2.1) The shared device requests the authentication server to authorize the guest user. (2.2) The authentication server acquires online social relationships between the owner and the guest user. Based on these relationships, the authentication server creates access control information that defines whether the guest user can access the shared device and the permission level for the guest user. (2.3) The authentication server issues the access control information to the shared device. (2.4) The shared device controls the access for the guest user based on the received information.

3. Prototype Implementation

3.1 Overview

To demonstrate a configuration example and evaluate the feasibility of the proposed system, this report presents a prototype implementation.

The architecture of the implemented prototype is illustrated in Fig. 3. The implemented prototype chooses the Wi-Fi access point (AP) as a shared device and uses the number of common friends on Facebook [11] as an indicator of online social relationships. According to the number of common friends, the authorized duration for guest users to access the Internet through the AP is controlled. To delegate guest user identification management to Facebook accounts, the OAuth [12] protocol is used. In addition, the implemented prototype adopts a system called PacketFence [13] to control the packet flow through the AP. PacketFence communicates with the authentication server and the guest device and performs access control on behalf of the shared Wi-Fi AP.

Like the proposed system, the authentication flow is composed of the identification phase and authorization phase. In the identification phase, the guest user requests access to the shared device and signs in to the authentication server with the guest user's Facebook account. The authentication server identifies the guest user by receiving the guest user's information from Facebook. The authentication server and PacketFence communicate with each other to exchange the guest user's pieces of information such as the guest user's name or email address. In the authorization phase, the authentication server obtains the number of common friends between the owner and the guest user and determines the authorized duration for the guest user to access the Wi-Fi AP. Due to the PacketFence's specification, the authorization phase is requested twice.

Under this configuration, the implemented prototype allows the guest users to connect to the Internet through the AP without entering complex Wi-Fi passwords as long as they have a Facebook account.

3.2 Performance Measurement

3.2.1 Metric

This report adopts the time required for authentication as a metric. However, the time consumed while the user enters her or his username and password on the signing in page of Facebook should not be included in the measurement because it varies from person to person. Therefore, this report assumes that the user usually uses Facebook with a browser on the user's device, i.e., the user has already signed in to Facebook and a Facebook credential has been stored in a browser cookie. Under this assumption, the signing in procedure is completed as soon as the user visits the signing in page of Facebook, and the time taken to enter the username and password is not included in the measurement.

3.2.2 Experimental Setup

The details of the experimental setup are listed in Table 1. PacketFence was installed on a CentOS machine. The authentication server was implemented as a Ruby on Rails web server and deployed on one of the most popular platforms as a service (PaaS) named Heroku.

The time required for authentication was extracted from timestamps in a log file of the authentication server. In this measurement, the time required for authentication is defined as the length of a period that begins with the first request to the sever and ends with the last response from the server. The measurement was made five times, and the average time

Table 1 Details of experimental setup

OS	CentOS 6.8
Memory	8 GB
CPU	Core i7-860 2.8 GHz × 8
No. of measurements	5
PacketFence version	6.3.0
Guest device	iPhone 6 iOS 10.2
Browser on guest device	Google Chrome
Authentication server	Ruby 2.3.1, Rails 4.2.7, on Heroku

Table 2 Time required for authentication

	Time from previous event [s]	
Event	Reference	Proposed
Request identification	-	-
Redirect	0.90	0.58
Response access_token	1.62	1.48
Response identification	0.30	0.23
Request token	2.38	2.38
Response token	0.05	0.16
Request username, email	0.80	0.80
Response username, email	0.02	0.01
Request authorization	0.89	1.01
Response authorization	0.02	0.17
Request authorization	0.79	0.78
Response authorization	0.02	0.14
Total	7.78	7.74

was calculated.

3. 2. 3 Reference Setup

The reference system does not consider online social relationships between a device owner and guest users. The authentication server in the reference system does not acquire and evaluate online social relationships on Facebook and allows all guest users to use the Wi-Fi AP for fixed duration.

3. 2. 4 Results

The results of the measurement are shown in Table 2. The results show that the proposed system can be fully implemented as an actual working system and the time required for authentication is within a realistic range. The dominant part in terms of required time was the Facebook sign-in because several redirects related to the Facebook sign-in procedure occurred in this part. It is hard to reduce the time consumed during these redirects because they are managed in Facebook. On the other hand, the time required for the authentication server to acquire the number of common friends from Facebook was not dominant. Thus, there is no big difference in required time for authentication between the reference system and the prototype system. Even if the system acquires and evaluates more complex online social relationships, the time required for the authentication would only be a little longer.

4. Conclusion

This report proposed an authentication control system that evaluates the online social relationships between the device owner and each user and determines the permission level for each user automatically. To evaluate the feasibility of the proposed system, a prototype system was implemented that enables users to share a Wi-Fi AP by evaluating the number of common Facebook friends between the owner and the guest user and determining the authorized access duration for each user. By measuring the required time for the authentication process using the implemented prototype, the feasibility of the proposed system was confirmed. As future work, utilization of other sources of online social relationships and applications other than Wi-Fi AP can be explored.

Acknowledgement

This work is supported in part by the KDDI Foundation.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol.54, no.15, pp.2787–2805, 2010.

[2] T. Teubner, "Thoughts on the sharing economy," Proceedings of the International Conference on e-Commerce, vol.11, pp.322–326, 2014.

[3] C.J. Martin, "The sharing economy: A pathway to sustainability or a nightmarish form of neoliberal capitalism?," Ecological Economics, vol.121, pp.149–159, 2016.

[4] FON, `https://fon.com/`.

[5] M. Chen, Y. Hao, Y. Li, C.-F. Lai, and D. Wu, "On the computation offloading at ad hoc cloudlet: architecture and service modes," IEEE Communications Magazine, vol.53, no.6, pp.18–24, 2015.

[6] A. Kansal, S. Nath, J. Liu, and F. Zhao, "Senseweb: An infrastructure for shared sensing," IEEE MultiMedia, vol.14, no.4, pp.8–13, Oct. 2007.

[7] J. Beal, K. Usbeck, J. Loyall, and J. Metzler, "Opportunistic sharing of airborne sensors," Distributed Computing in Sensor Systems (DCOSS), 2016 International Conference onIEEE, pp.25–32 2016.

[8] J. Beal, K. Usbeck, J. Loyall, M. Rowe, and J. Metzler, "Adaptive task reallocation for airborne sensor sharing," Foundations and Applications of Self* Systems, IEEE International Workshops onIEEE, pp.168–173 2016.

[9] T. Zhu, Y. Gu, T. He, and Z.-L. Zhang, "eshare: a capacitor-driven energy storage and sharing network for long-term operation," Proceedings of the 8th ACM Conference on Embedded Networked Sensor SystemsACM, pp.239–252 2010.

[10] L. Garton, C. Haythornthwaite, and B. Wellman, "Studying online social networks," Journal of Computer-Mediated Communication, vol.3, no.1, pp.0–0, 1997.

[11] T. Kaya and H. Bicen, "The effects of social media on students' behaviors; facebook as a case study," Computers in Human Behavior, vol.59, pp.374–379, 2016.

[12] D. Hardt, "The oauth 2.0 authorization framework," 2012.

[13] H. Annuar, B. Shanmugam, A. Ahmad, N.B. Idris, S.H. AlBakri, and G.N. Samy, "Enhancement and implementation of network access control architecture for virtualization environments," Sept. 2013.