Computers in Industry 82 (2016) 151–159

Contents lists available at ScienceDirect

Computers in Industry

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

VOAuth: A solution to protect OAuth against phishing

Min Xie[a,*], Wei Huang[b], Li Yang[a], Yixian Yang[a]

[a] Information Security Center, Beijing University of Posts and Telecommunications, China
[b] School of Computer Science, Communication University of China, China

ARTICLE INFO

Article history:
Received 21 July 2015
Received in revised form 13 May 2016
Accepted 21 June 2016
Available online xxx

Keywords:
Anti-phishing
OAuth
Validation system
Tripartite consultation

ABSTRACT

The OAuth protocol is designed for authorization which enables users to grant third-party applications to access their resources stored at a server. However, OAuth cannot prevent counterfeiting the *Authorization Server*, thus phishing attacks are usually encountered. Although the version 2.0 of OAuth has been widely used in web authorization services, counterfeiting problem remains unsolved. In this paper, VOAuth (Validation OAuth) is proposed as a novel solution to address this problem, which brings in a Validation System and optimizes the processes of OAuth. The Validation System including Validation Gateway and Validation Client can guarantee the authenticity of *Authorization Server* by taking tripartite consultation and one-time pad into account, hence users can be protected from phishing due to that passwords will not be stored or submitted for a long time. In order to prove that VOAuth can avoid phishing attacks especially counterfeiting *Authorization Server* effectively, countermeasures on phishing threat models and formal verification in VOAuth are shown with Alloy Analyzer. Finally, VOAuth is implemented in an actual mobile Internet application and has been on-line for more than two years with over 15 million users. So far, the leakage of user privacy data does not occur and there is no phished account reported, which provides further evidence of the effectiveness of VOAuth.

1. Introduction

OAuth [1] is one of the most popular authorization protocols which has been widely used by many leading enterprises such as Facebook, Twitter, etc. It reduces the technical threshold for users to connect up external data to the current site (or for services to provide protected data for third-party developers). Relying on the security of the transport layer, both OAuth 1.0 and OAuth 2.0 bring in effective security considerations for most threat models. Among these considerations, several mechanisms can prevent those phishing attacks launched by malicious clients (third-party applications), such as the strict examination mechanism to clients or clients' redirect URIs to avoid MITM (Man-in-the-Middle Attack) and State Parameter against CSRF (Cross-site Request Forgery). However, neither OAuth 1.0 nor 2.0 can verify the authenticity of the *Authorization Server* [1,2]. If users do not verify the authenticity of these websites before entering their Credentials by mistake, it will be possible for attackers to exploit negligence of users and steal their passwords. OAuth can inform users facing risks introduced by phishing attacks and make it easy for users to confirm the authenticity of their sites [3]. Unfortunately, this is a rough way to solve this problem, for it requires users to have adequate knowledge about HTTP/HTTPS and to pay enough attention on the features (e.g. domain, logo) of the authorization page. As is known to all, most of users cannot distinguish phishing attacks due to the lack of vigilance and security knowledge [4].

2. Related work

Many solutions have been proposed to address the problem. One solution provided by Twitter is that any consumer key registered on Twitter can only be able to use the so called out-of-band (OOB) authorization method, which does not rely on redirection [5]. However, it cannot protect from the circumstance of an attacker masquerading as a client that dose not realize the mechanism. Haitham S. Al-Sinani proposed a browser extension-based method to prevent clients from redirecting authorized page directly [6], however, due to the characteristics of mobile devices, malicious applications do not complete the authorization through the browser, so that any browser-extension based solutions cannot be effective on mobile devices.

In order to solve the problem of phishing especially counterfeiting *Authorization Server* on browsers and mobile devices,

* Corresponding author at: Room 1202, Unit 4, Building 9, No. 88 Fangfei Road, Fengtai, Beijing, China.
E-mail address: heaven2358@gmail.com (M. Xie).

http://dx.doi.org/10.1016/j.compind.2016.06.001
0166-3615/

VOAuth (Validation OAuth) is proposed in this paper, which is an effective solution and can be easily implemented with a strong anti-phishing capacity. Moreover, VOAuth does not require users to have solid security knowledge.

3. Description of VOAuth

Considering that the transport layer security can protect the privacy of transmitted data not only in anti-phishing but also in other security areas, VOAuth relies on transport layer security, though it is unnecessary in original OAuth protocol.

3.1. Definitions

Before the description of VOAuth framework, some related items of the framework are explained firstly.

3.1.1. Validation gateway (VGateway)

VGateway is an authentic secret key agreement server, which is used to send validation information and to receive validation responses. It plays an important role in the whole system, because it verifies the identification of users via a kind of communication methods (such as SMS or Email) and can prevent the OAuth Client from phishing by attackers. It generates random and unique validation information based on user's authorization requirements and sends information to the user who actually holds the mobile device or Email address, thus avoids phishing pages to steal user name and password.

3.1.2. Information gateway (IGateway)

IGateway is a server where validation information is sent and responded information is received. For the sake of simplicity, we assume that *IGateway* is internal controlled, secure and trusted.

3.1.3. User

The *user* refers to either mobile application or browser user. In OAuth equivalent terms, *resource owner* is used instead of *user*.

3.1.4. Validation client (VClient)

VClient actually refers to the user's mobile device or Email, which can receive validation information from *VGateway* and response to it.

3.1.5. OAuth client (client)

It is a third-party application, which is authorized to get users' resource with OAuth API. In OAuth equivalent terms, *client* is also called *consumer*.

3.1.6. Authorization server

It has centralized authentication and unified authorization function. When it works, it checks the operation of the users' or clients' requests and verifies whether the user has authorized the

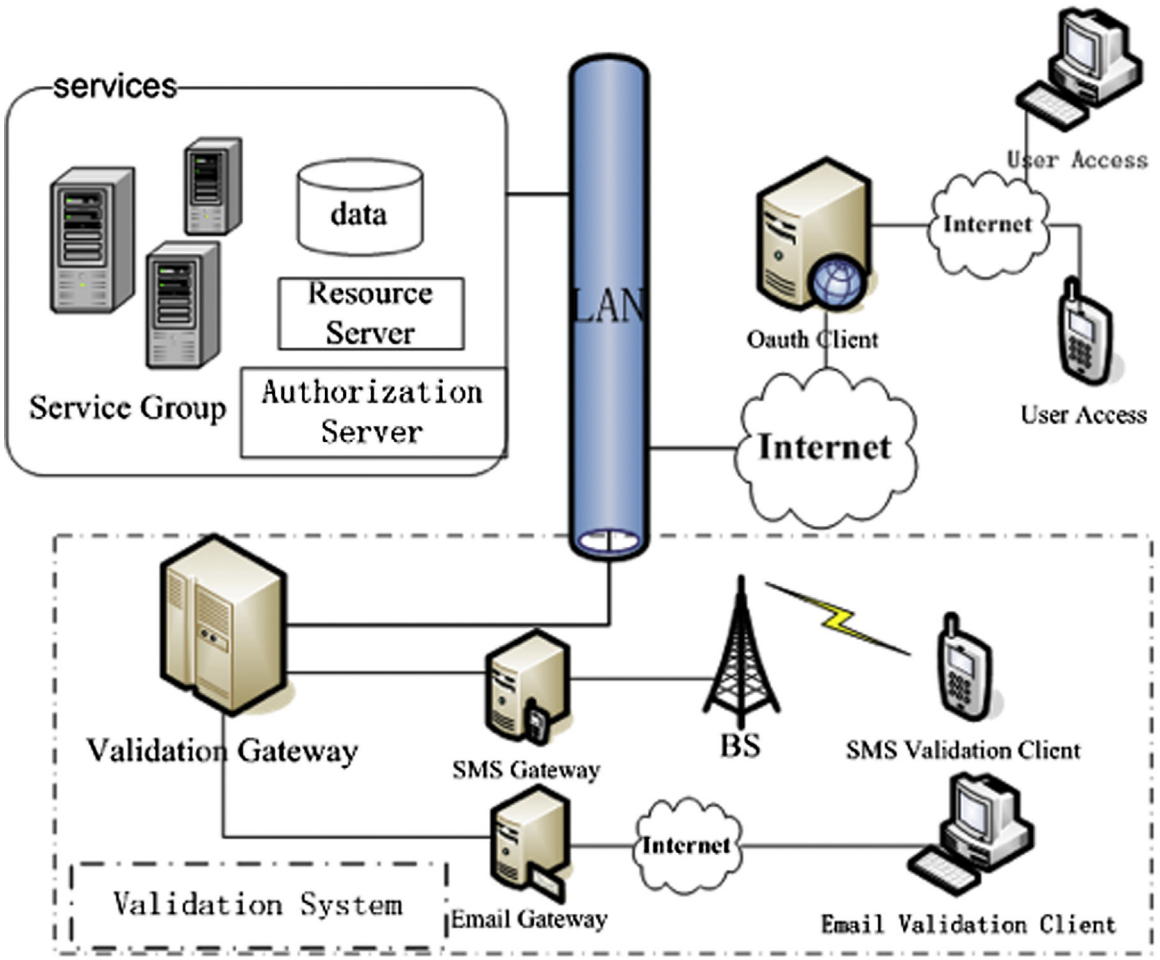

Fig. 1. System architecture.