Does the IdP Mix-Up attack really work?

Wanpeng LI and Chris J Mitchell

Royal Holloway, University of London

wanpeng.li.2013@live.rhul.ac.uk

July 14, 2016

ROYAL HOLLOWAY UNIVERSITY OF LONDON

About RHUL

Overview

ROYAL HOLLOWAY UNIVERSITY OF LONDON

1. Introduction
   - The IdP Mix-Up Attack
2. Case Study
   - Two Case Studies
3. Conclusion
   - Our Conclusion

The IdP Mix-Up Attack

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Attack. We now describe the attack on the OAuth implicit mode in detail. As mentioned, a very similar attack also applies to the OAuth authorization code mode and both attacks even work if IdP supports just one of these two modes, rather than both or all four OAuth modes. Note that these two modes are the most common modes in practice.

Attack on Implicit Mode. The IdP mix-up attack for the implicit mode is depicted in Figure 6. Just as in the implicit mode, the attack starts when the user selects that she wants to log in using HIdP (Step 1 in Figure 6). Now, the attacker intercepts the request intended for the RP and modifies the content of this request by replacing HIdP by AIdP. The response of the RP 3 (containing a redirect to AIdP) is then again intercepted and modified by the attacker such that it redirects the user to HIdP 4. The attacker also replaces the OAuth client id of the RP at AIdP with the client id of the RP at HIdP.[12] (Note that we assume that from this point on, in accordance with the OAuth security recommendations, the communication between the user's browser and HIdP and the RP is encrypted by using HTTPS, and thus, cannot be inspected or altered by the attacker.) The user then authenticates to HIdP and is redirected back to the RP 8. The RP, however, still assumes that the access token contained in this redirect is an access token issued by AIdP, rather than HIdP. The RP therefore now uses this access token to retrieve protected resources of the user (or the user id) at AIdP 12, rather than HIdP. This leaks the access token to the attacker who can now access protected resources of the user at IdP. This breaks the authorization property (see Section 5.2 below). (We note that at this point, the attacker might even provide false information about the user or her protected resources to the RP.)

The IdP Mix-Up Attack on Implicit Mode

A Simple Example of the IdP Mix-UP Attack I

ROYAL HOLLOWAY UNIVERSITY OF LONDON

1. Suppose the user wishes to use Facebook to log in to the BBC web site. The user clicks the Facebook login button. This will generate a request to the BBC which indicates that the user wants to use Facebook to login. The attacker intercepts the request and modifies it to make the BBC believe that the user wants to use EvilCo to sign in to the BBC.
2. The BBC generates the authorization request for EvilCo, and the attacker intercepts it and changes the *client_id* and *redirect_uri* to the values the BBC registered with Facebook. This will make the authorization request look as if it was intended for Facebook.
3. The user authenticates to Facebook and clicks the authorization button. An authorization response is generated by Facebook and sent to the BBC.

A Simple Example of the IdP Mix-UP Attack II

ROYAL HOLLOWAY UNIVERSITY OF LONDON

4. The authors assume that at this point the BBC will process this response as if it was generated by EvilCo; as a result it will send the received *access_token* to EvilCo to retrieve the required user information. As a result, the attacker (EvilCo) will discover the user's *access_token* for Facebook, and can then use this *access_token* to retrieve sensitive user information from Facebook.

The IdP Mix-Up Attack

ROYAL HOLLOWAY UNIVERSITY OF LONDON

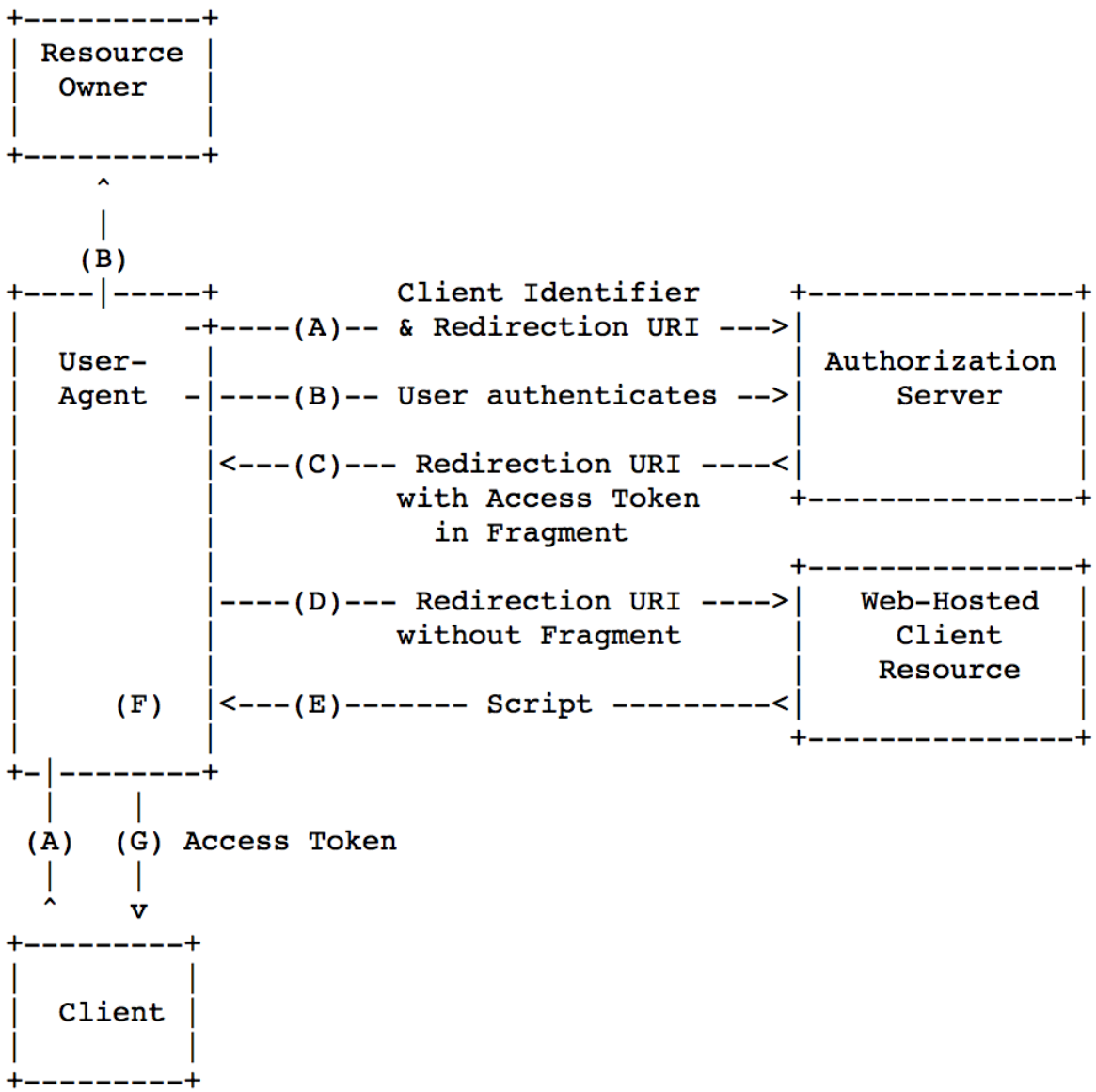
The implicit assumption under the IdP Mix-Up Attack

- user's intention is related to the first request, however, we believe user's intention should be related to the redirect_uri.

Google's Hybrid-server Side Flow

- No request was sent to RP in Step 1, the authorization request is generated by RP JavaScript Client

OAuth 2.0 Implicit Grant Flow



Two Empirical Studies

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Two Empirical Studies

- Wanpeng Li and Chris Mitchell, "Security Issues in OAuth 2.0 SSO Implementations", ISC 2014
- Wanpeng Li and Chris Mitchell, "Analysing the Security of Googles Implementation of OpenID Connect", DIMVA 2016

Two Empirical Studies

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Study the OAuth 2.0 systems deployed in China [Li and Mitchell, 2014]

- 60 RPs
- 10 IdPs
- We discovered a number of vulnerabilities which allow an attack to log in to the RP as a victim user
- We did not find any RP using the same *redirect_uri* for different IdPs

Two Empirical Studies

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Study the Google's OpenID Connect [Li and Mitchell, 2016]

- 103 RPs provide service in English
- Google as the IdP
- We found serious vulnerabilities which allow an attacker to log in to the user without knowing the user's account and password
- We did not find any RP using the same *redirect_uri* for different IdPs

Case Study

Ctrip

- a China-focused travel agency.
- has about 60 million members and 2.5 million active users.
- its services cover around 9,000 flight routes and 200,000 hotels around the world.
- Ctrip supports several SSO IdPs, including QQ, Renren, Baidu and Sina.

IdPs supported by Ctrip

Ctrip

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Ctrip *redirect_uri* registered with QQ

```
https://graph.qq.com/oauth/show?which=Login&display=pc&
client_id=100234303&response_type=code&
redirect_uri=https://accounts.ctrip.com/member/
QQLogin/QQCallBack2.aspx&state=3xuYedwnNe69E6ma
```

Ctrip

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Ctrip *redirect_uri* registered with QQ

```
https://graph.qq.com/oauth/show?which=Login&display=pc&
client_id=100234303&response_type=code&
redirect_uri=https://accounts.ctrip.com/member/
QQLogin/QQCallBack2.aspx&state=3xuYedwnNe69E6ma
```

Ctrip *redirect_uri* registered with Baidu

```
http://openapi.baidu.com/oauth/2.0/authorize?
client_id=GA3KcdrwGw5E76lojWGM3ViU&response_type=code&
redirect_uri=https://accounts.ctrip.com/member/
BaiduLogin/BaiduCallBack2.aspx
```

Ctrip

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Ctrip *redirect_uri* registered with Weibo

```
https://api.weibo.com/oauth2/authorize?
client_id=3883532126&response_type=code&
redirect_uri=https://accounts.ctrip.com/Member/
SinaLogin/SinaOAuthCallBack2.aspx&state=dBP2Fs3mfrPEdKpK&
with_offical_account=1/BaiduCallBack2.aspx
```

Ctrip

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Ctrip *redirect_uri* registered with Weibo

```
https://api.weibo.com/oauth2/authorize?
client_id=3883532126&response_type=code&
redirect_uri=https://accounts.ctrip.com/Member/
SinaLogin/SinaOAuthCallBack2.aspx&state=dBP2Fs3mfrPEdKpK&
with_offical_account=1/BaiduCallBack2.aspx
```

Ctrip *redirect_uri* registered with Wechat

```
https://open.weixin.qq.com/connect/qrconnect?
appid=wx29cad1c2709a80bc&
redirect_uri=https://accounts.ctrip.com/member
/WeChatLogin/CallBack.aspx&response_type=code&scope=snsapi_log
&state=9f051128369b4f8099467c72c19a3c30#wechat_redirect
```

Ctrip

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Ctrip *redirect_uri* registered with Wangyi

```
http://reg.163.com/open/oauth2/authorize.do?
client_id=4294805915&response_type=code&
redirect_uri=https://accounts.ctrip.com/member/
NETELogin/NeteCallBack2.aspx
```

Ctrip *redirect_uri* registered with Renren

```
https://graph.renren.com/oauth/authorize?
client_id=ecd78a2da5404e8992d6a45e89f9d1f8&
redirect_uri=https://accounts.ctrip.com/member/
RenrenLogin/CallBack.aspx&response_type=code
```

Case Study

BBC

- is the world's oldest national broadcasting organisation
- supports two SSO IdPs, including Facebook, Google

IdPs supported by BBC

BBC

BBC *redirect_uri* registered with Facebook

```
https://www.facebook.com/v2.0/dialog/oauth?
client_id=58567469885&
redirect_uri=https://ssl.bbc.co.uk/id/oauth2/consume/
facebook.com
```

BBC

ROYAL HOLLOWAY UNIVERSITY OF LONDON

BBC *redirect_uri* registered with Facebook

```
https://www.facebook.com/v2.0/dialog/oauth?
client_id=58567469885&
redirect_uri=https://ssl.bbc.co.uk/id/oauth2/consume/
facebook.com
```

BBC *redirect_uri* registered with Google

```
https://accounts.google.com/o/oauth2/auth?
response_type=code&scope=profile&
client_id=286550132048.apps.googleusercontent.com&
redirect_uri=https://ssl.bbc.co.uk/id/oauth2/consume/
google.com
```

Concerns over the IdP Mix-Up Attack

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Adversary Model

- a malicious IdP is required

Concerns over the IdP Mix-Up Attack

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Adversary Model

- a malicious IdP is required

The capability of a malicious IdP

- collecting user information
- can login to user RP account using the information he had
- can impersonate every user on a RP website (the purpose of the IdP Mix-Up Attack)

Question?

- Does a malicious IdP still need IdP Mix-Up Attack?
- We believe the security of OAuth 2.0 builds on the IdP is trustworthy, if the IdP is malicious, then the whole system of OAuth 2.0 corrupts

Concerns over the IdP Mix-Up Attack

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Fragment Component is used in the Authorization Response of the Implicit Flow:

- Facebook and Google append *access_token* with the # (hash symbol) to the authorization response

```
https://www.runtastic.com#state=STATE&
access_token=ya29.CjAeA3UkmuRHX6YocPONPz777Nr
Oikpz0p7l0CLm12g6wNWMRMbjm49uc7kuB3x4Alw
&token_type=Bearer&expires_in=3600
```

Conclusion

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Conclusion

- is the IdP Mix-up mitigation needed?
- certain assumptions underlying the formal model do not apply in practice

Thanks for listening

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Thank you for listening!
Questions?

References

Wanpeng Li and Chris J Mitchell (2014)

Security Issues in OAuth 2.0 SSO Implementations

Information Security - 17th International Conference, ISC 2014, 2014

Wanpeng Li and Chris J Mitchell (2014)

Analysing the Security of Google's Implementation of OpenID Connect

Detection of Intrusions and Malware, and Vulnerability Assessment- 13th International Conference, DIMVA 2016, 2016