Do Not Trust Me Using Malicious IdPs for Analyzing and Attacking Single Sign-On

MAR 10TH, 2016

论文下载

Abstract & Introdutcion

- 提出一种新的方法来分析SSO协议——引入一个恶意IdP。
- 使用这种方法发现了针对OpenID的四类攻击。
- 对OpenID的安全性进行系统化分析，11/16个实现都存在漏洞，包括SourceForge、Drupal、ownCloud等。
- 开发了自动化分析工具OpenID Attacker。

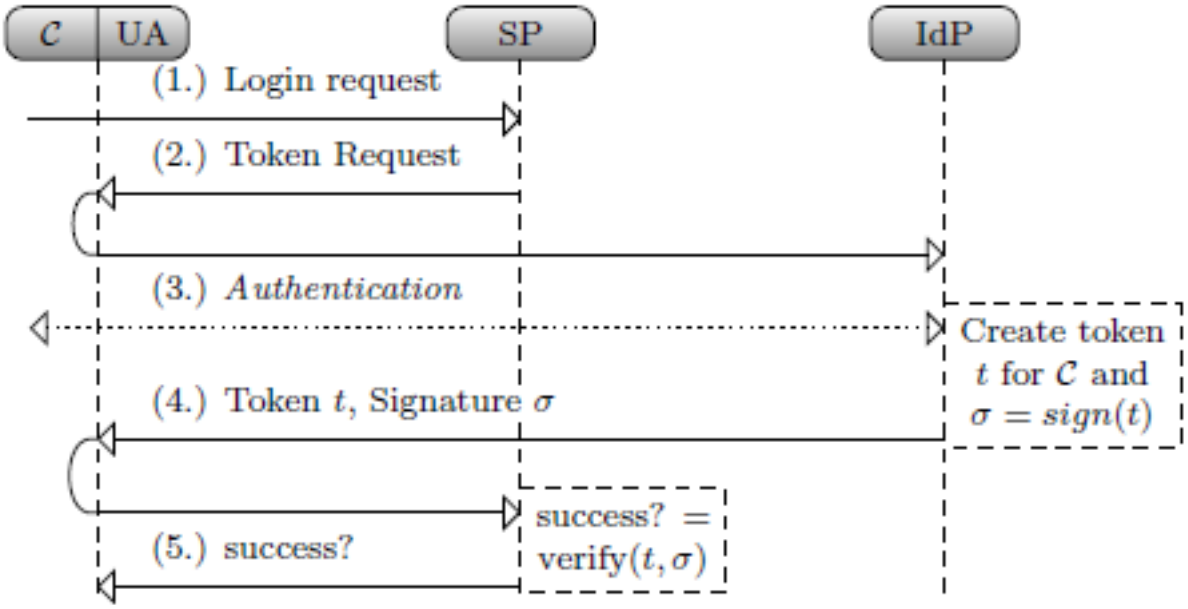

Fig. 1: Single Sign-On (SSO) overview.

Computational and Security Model

- Computational Model：OpenID中有一种开放信任关系，SP信任任意IdP创建的token，只要这个IdP在client提供的URL.IDc检索到的文档中。

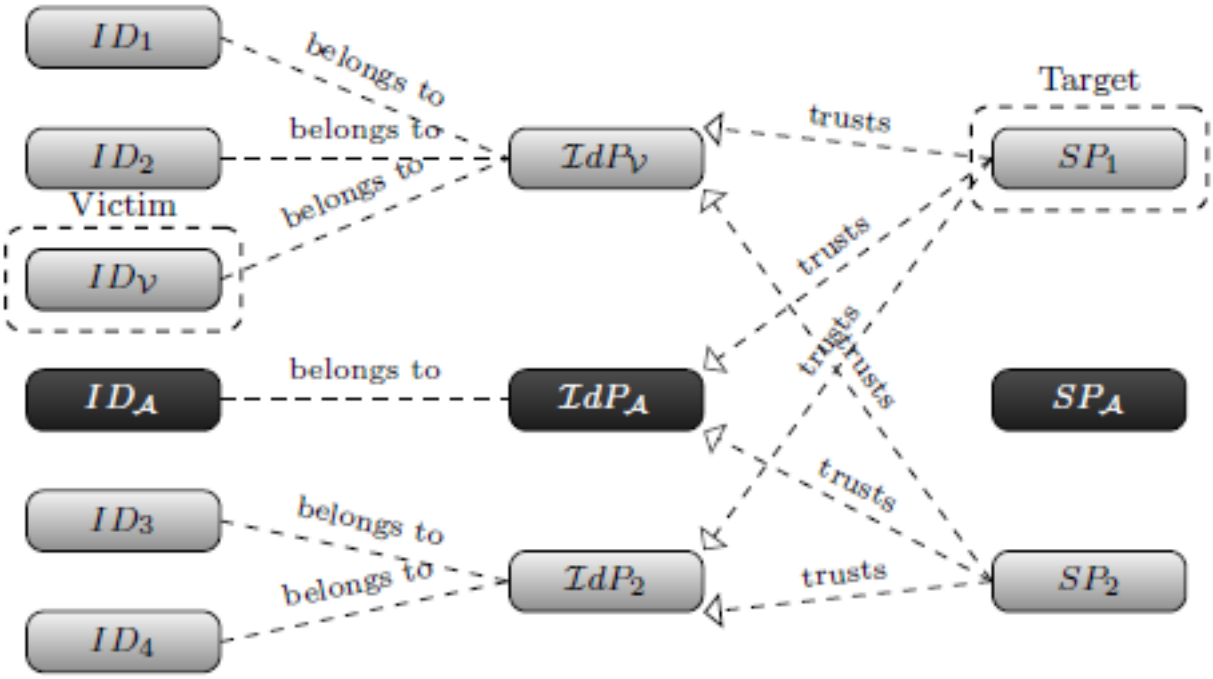

Fig. 3: SSO in the real world involves multiple clients, multiple IdPs and multiple SPs. SP_1 can even *trust* tokens of $\mathcal{I}dP_A$, but only for its corresponding clients, i.e. ID_A.

- SSO Attacker Paradigm：攻击者的目标是获取他无权访问的资源（主要是存在SP上的资源）。攻击者可以扮演恶意client/SP/IdP的角色。

OpenID： Technical Background

- OpenID中，client的一个身份是用一个URL表示的，定义为URL.IDc，相应的URL.IdPc、URL.SP。
- OpenID协议由3个阶段组成：（1）Discovery；（2）Association；（3）Token processing。

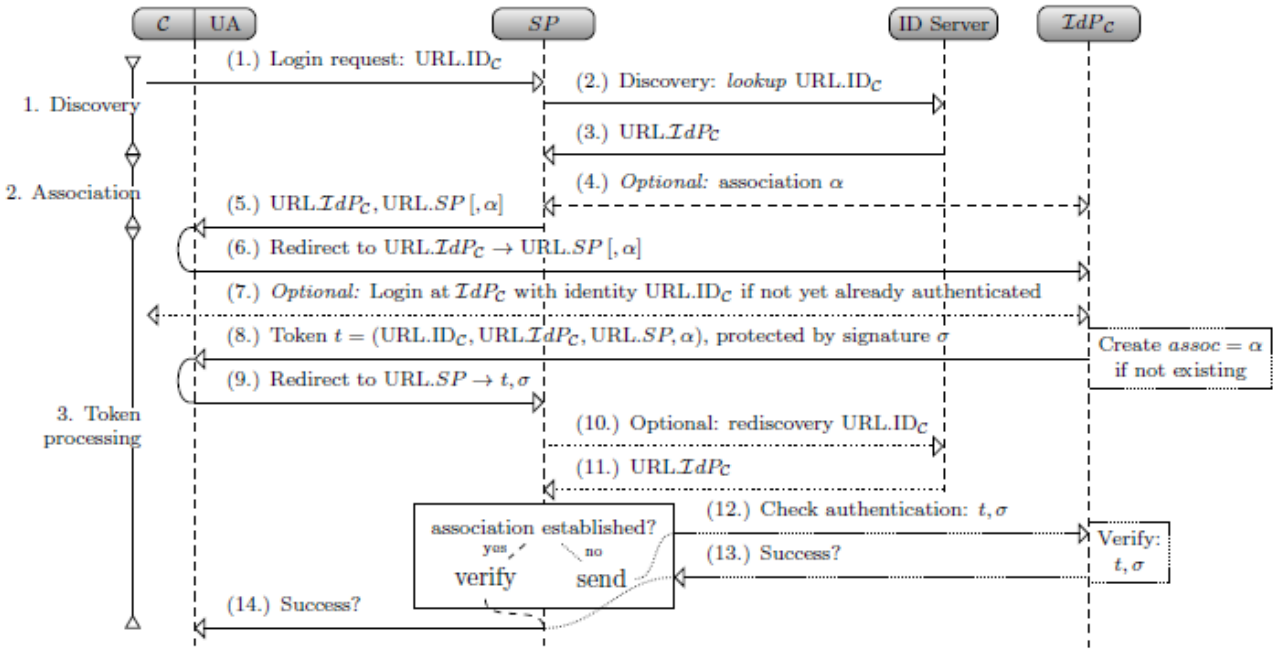

Fig. 4: The OpenID protocol flow.

```
<html><head><title/>
<link rel="openid2.provider"
      href="https://myidp.com/" />
</head><body/></html>
```

Listing 1.1: Minimal HTML discovery document.

Novel Attacks

- Token Recipient Confusion（TRC）： 缺乏对URL.SP参数的验证。（这个攻击算不上是新发现的攻击，在其它

SSO中都有存在，该攻击能够实现还有一个因素是OpenID提供两种方法校验签名）

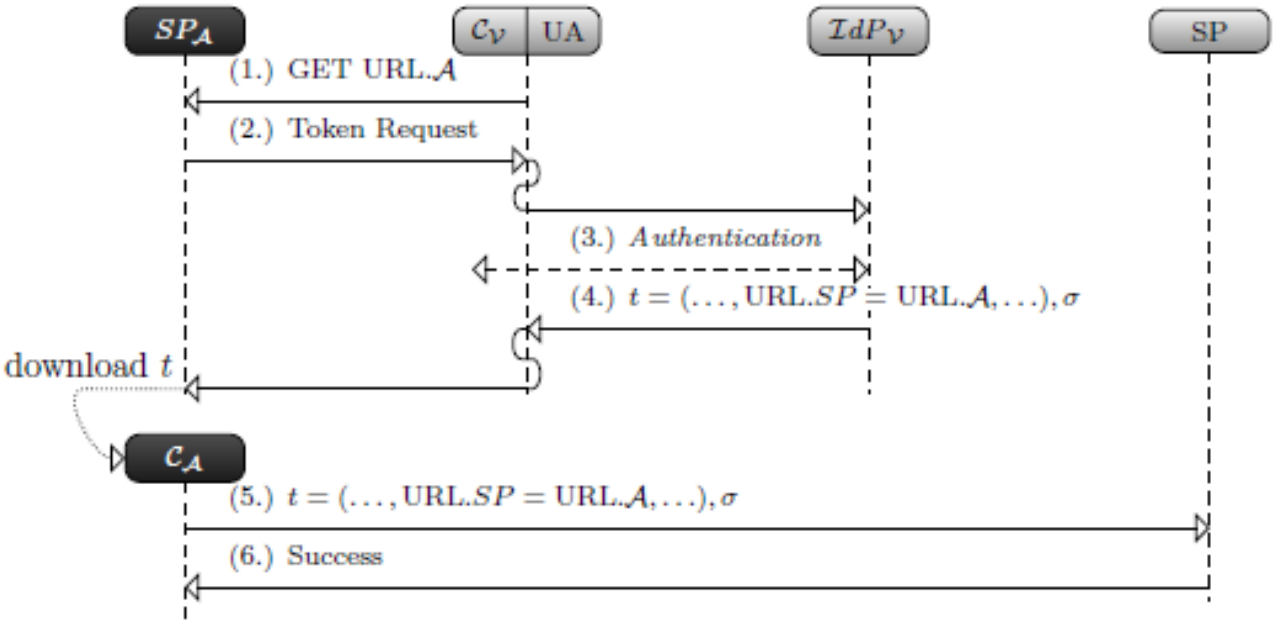

Fig. 5: Token Recipient Confusion Attack.

- Key Confusion（KC）：强制令目标SP使用攻击者选择的key去校验一个伪造token。（精巧的攻击）

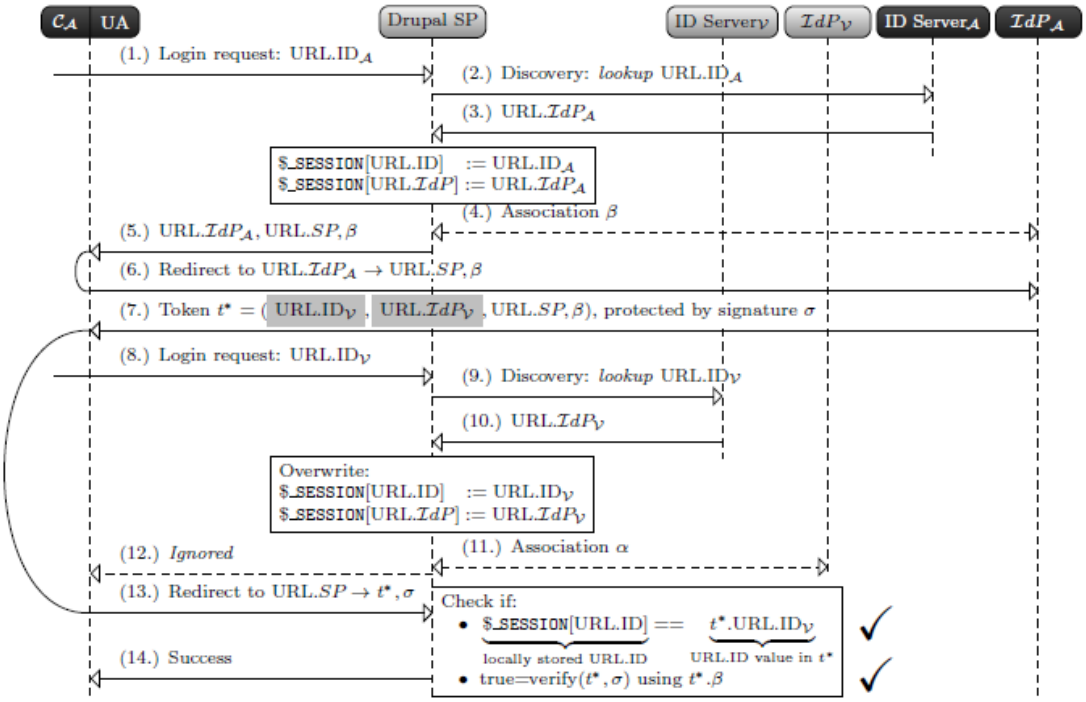

Fig. 7: Key Confusion attack on Drupal: Before the token t^* in Step (7.) is forwarded to Drupal in Step (13.), the attacker $\mathcal{C}_{\mathcal{A}}$ starts a second login request in Step (8.) using the victim's identity URL.ID$_{\mathcal{V}}$. This overwrites the URL.ID and URL.$\mathcal{I}dP$ data stored in `$_SESSION` and prevents the second discovery.

- ID Spoofing（IDS）：恶意IdP可以创建一个token包含受害者的id。
- Discovery Spoofing（DS）：OpenID特性产生，略。（攻击条件复杂）

Methodology

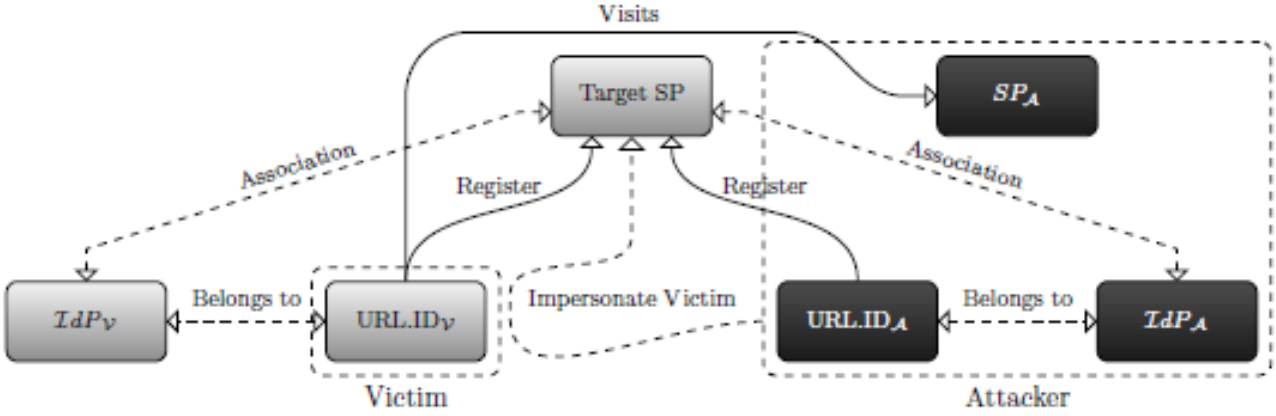

Fig. 6: Evaluation setup and goal.

OpenID Attacker

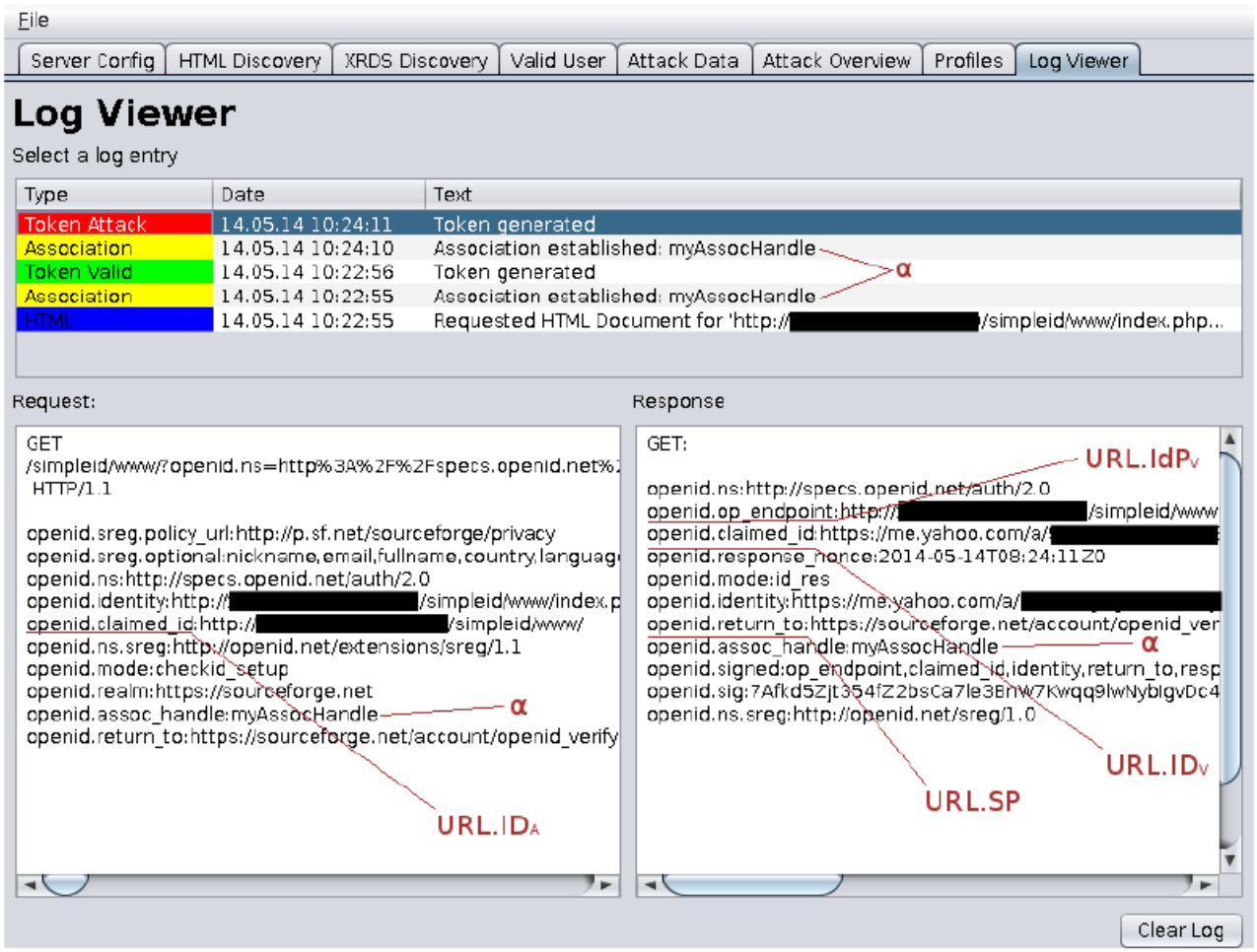

Fig. 8: IDS attack on Sourceforge. The OpenID Attacker *log viewer* window lists all exchanged OpenID messages. The Screenshot shows that the SP requests a token for URL.ID$_{\mathcal{A}}$, but the tools ignores the wish and responds with a token for URL.ID$_{\mathcal{V}}$.