**TÌM HIÊU VỀ OAUTH**

**Mở đầu**

Bài viết này dành cho những người chưa hiểu cơ bản về OAuth và Single Sign On.

OAuth là gì? Đó là câu hỏi không dễ đối với những người chưa từng làm việc với SSO (Single Sign On). Thực ra thì Single Sign On không liên quan gì mấy đến nội dung của OAuth. Tuy nhiên chúng hay đi liền với nhau. Vì vậy cũng phải có sự phân biệt cho khỏi nhầm lẫn.

Single Sign On là việc bạn có thể đăng nhập vào một website (như google.com) và sử dụng đăng nhập đó trên các website khác.

Vì vậy SSO là một tiện ích

Thường được sử dụng trên các website liên quan mật thiết đến nhau

Tiện ích SSO có nhiều phương pháp để thực hiện, SAML là một trong các phương pháp đó

OAuth là phương pháp chia sẻ tài nguyên giữa các ứng dụng mà không phải đưa ra “giấy thông hành” là username và password.

Do đó, OAuth là một phương pháp

Thường được sử dụng trên các website … chả liên quan gì nhau (thực ra là có liên quan đấy, nhưng về mặt bản chất chúng có thể hoạt động mà chẳng cần gì đến nhau, việc kết nối là để xin chút tài nguyên thôi).

Ngoài ra, bạn cũng phải phân biệt giữa hai từ Authorization và Authentication. Từ thứ 2 đơn giản là “đăng nhập” hay không, còn từ thứ nhất là “có quyền” hay không. Cần chú ý chúng khác nhau nhiều lắm, đôi khi bạn chẳng cần “đăng nhập” bạn cũng có thể “có quyền”. Ý của tôi ở đây là Authentication thường liên quan đến việc bạn phải “đăng nhập” vào hệ thống. Còn Authorization tức “có quyền” trên tài nguyên hệ thống hay không thì bạn phải yêu cầu chủ thể của tài nguyên cho phép bạn.

Nói vậy thì hơi lan man, bạn có thể bỏ qua đừng suy nghĩ gì về đoạn giải thích như đánh đố trên.

Xin được đi chi tiết hơn về OAuth, nội dung của nó thì không mới, các hãng lớn như Google, Aol, Yahoo… đều có các phương pháp Authorization của riêng mình. Nhưng nó khiến các bên thứ ba khó khăn khi tích hợp với họ. Vì vậy họ họp nhau lại để tạo ra chuẩn Open Authorization.

**1. Bắt đầu với Authorization, cụ thể là OAuth bạn phải phân biệt được những bên liên quan như sau**

Client: là ứng dụng (chú ý là một ứng dụng, có thể là ứng dụng Desktop, cũng có thể là website của bạn như http://www.youbrainy.com

), muốn có quyền sử dụng tài nguyên của Server

Server: là một ứng dụng khác, chẳng hạn như google.com.

You: chính bạn, bạn có tài nguyên trên Server và bạn muốn cho Client quyền sử dụng nó

Tóm lại: OAuth là phương pháp để Client sử dụng được tài nguyên của You bên phía Server

**2. Phân biệt hai loại OAuth**

* 2-legged OAuth: là kiểu Authorization trong đó vai trò của You và Client là như nhau. Tức là Client chính là You của Server. Đó là kịch bản Client-Server thông thường.
* 3-legged OAuth: là kiểu Authorization trong đó You và Client là phân biệt. Client muốn You chia sẻ tài nguyên đã có bên phía Server.

**3. Cách OAuth hoạt động**

***3.1. 2- legged OAuth***

1. Client đăng ký sử dụng dịch vụ với Server
2. Server cho Client
3. CONSUMER\_KEY
4. CONSUMER\_SECRET\_KEY
5. Client sử dụng các keys trên để thực hiện Authorization

***3.2. 3- legged OAuth***

1. Client đăng ký sử dụng dịch vụ với Server
2. Server cho Client
3. CONSUMER\_KEY
4. CONSUMER\_SECRET\_KEY
5. You có tài nguyên ở Server
6. You sử dụng dịch vụ ở Client, Client yêu cầu You cho phép khai thác tài nguyên của You ở Server
7. Client yêu cầu Server gửi REQUEST\_TOKEN cho You
8. Client chuyển You đến Server Authentication
9. You đăng nhập vào Server, Server hỏi You có muốn chia sẻ quyền khai thác dữ liệu cho Client hay không
10. You đồng ý, Server chuyển You về Client kèm theo ACCESS\_TOKEN
11. Client sử dụng ACCESS\_TOKEN để thực hiện thao tác trên các tài nguyên của You thuộc Server

**4. Chú ý khi cài đặt với PHP**

Các trang tích hợp OAuth phần lớn hỗ trợ thư viện để bạn có thể dễ dàng cấu hình OAuth

Nếu trong tình huống xấu, bạn chính là người cung cấp dịch vụ và muốn cung cấp mã nguồn tích hợp OAuth với dịch vụ của bạn. Thì bạn phải code rùi. Tất nhiên đây là trường hợp chủ động

Nếu bên cung cấp dịch vụ ỉm đi, không cho bạn cái gì sất. Bạn phải code phần client chẳng hạn. Bạn nên tìm hiểu các thư viện sẵn có để học hỏi. Như Zend\_OAuth chẳng hạn.

**5. Tài liệu**

http://oauth.net/core/1.0/