OAuth2.0介绍

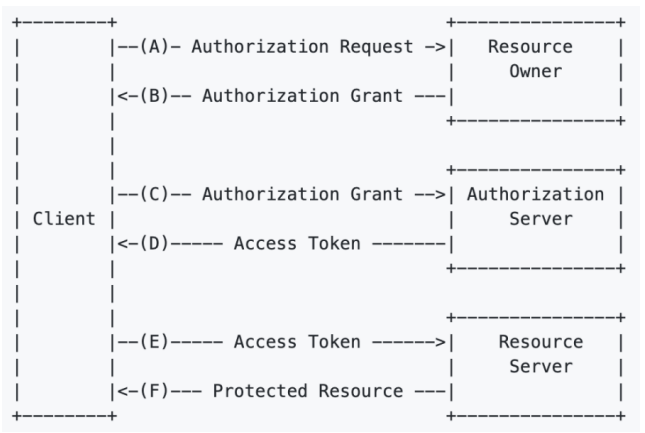
解决的问题

- 第三方应用需要存储资源所有者的凭据以供将来使用。该凭据通常是明文密码。
- 服务器需要支持密码身份认证，尽管密码认证有固有的安全缺陷。
- 第三方应用获得了对资源所有者的受保护资源的过于宽泛的访问权限，从而导致资源所有者不能限制对资源的有限子集的访问时限或权限。
- 资源所有者不能撤销某个第三方的访问权限而不影响其它第三方，并且必须更改他们的密码才能做到。
- 与任何第三方应用的妥协导致对终端用户的密码及该密码所保护的所有数据的妥协。

角色

- 资源所有者：能够许可对受保护资源的访问权限的实体。当资源所有者是个人时，它被称为最终用户。
- 资源服务器：托管受保护资源的服务器，能够接收和响应使用访问令牌对受保护资源的请求。
- 客户端：使用资源所有者的授权代表资源所有者发起对受保护资源的请求的应用程序。术语“客户端”并非特指任何特定的的实现特点（例如：应用程序是否是在服务器、台式机或其他设备上执行）。
- 授权服务器：在成功验证资源所有者且获得授权后颁发访问令牌给客户端的服务器。

协议流程



授权许可

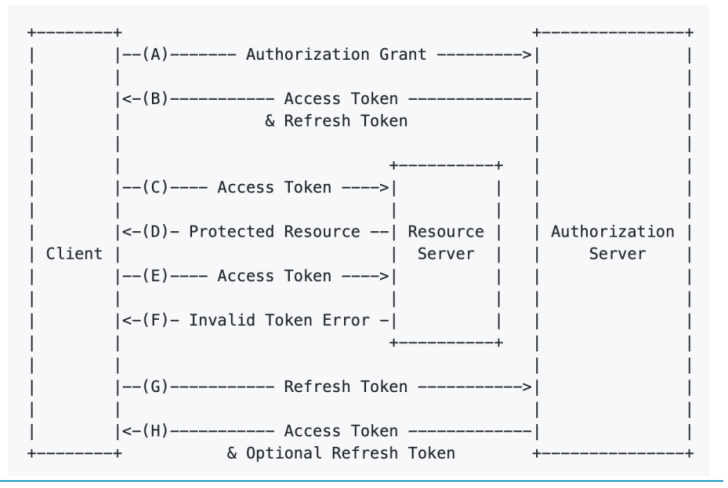
- 授权码 Authorization Code：授权码通过使用授权服务器做为客户端与资源所有者的中介而获得。客户端不是直接从资源所有者请求授权，而是引导资源所有者至授权服务器，授权服务器之后引导资源所有者带着授权码回到客户端。
- 隐式许可 Implicit：隐式许可是为用如JavaScript等脚本语言在浏览器中实现的客户端而优化的一种简化的授权码流程。
- 资源所有者密码凭据 Resource Owner Password Credentials：资源所有者密码凭据（即用户名和密码），可以直接作为获取访问令牌的授权许可。
- 客户端凭据 Client Credentials：当授权范围限于客户端控制下的受保护资源或事先与授权服务器商定的受保护资源时客户端凭据可以被用作为一种授权许可。

访问令牌

访问令牌是用于访问受保护资源的凭据。访问令牌是一个代表向客户端颁发的授权的字符串。该字符串通常对于客户端是不透明的。令牌代表了访问权限的由资源所有者许可并由资源服务器和授权服务器实施的具体范围和期限。

刷新令牌

刷新令牌是用于获取访问令牌的凭据。刷新令牌由授权服务器颁发给客户端，用于在当前访问令牌失效或过期时，获取一个新的访问令牌，或者获得相等或更窄范围的额外的访问令牌（访问令牌可能具有比资源所有者所授权的更短的生命周期和更少的权限）。



TLS版本

本规范任何时候使用传输层安全性（TLS），基于广泛的部署和已知的安全漏洞TLS的相应版本（或多个版本）将会随时间而变化。

HTTP重定向

本规范广泛采用了HTTP重定向，有此客户端或授权服务器引导资源所有者的用户代理到另一个目的地址。

互操作性

本规范中留下一些必需组件部分或完全没有定义（例如，客户端注册、授权服务器性能、端点发现等）。没有这些组件，客户端必须针对特定的授权服务器和资源服务器被手动并专门配置，以进行互操作。

符号约定

本规范中的关键词遵循ietf规范