一种网盘认证协议的分析与验证

刘璐 谭毓安 张全新 李元章

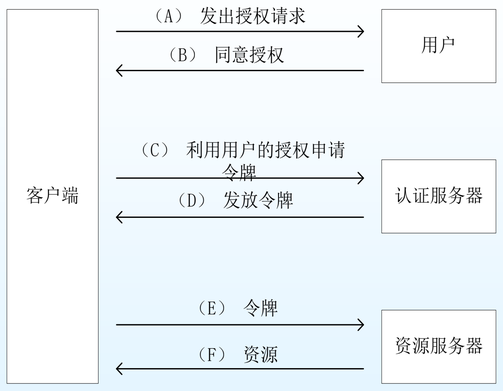
北京理工大学计算机学院

摘要

现今，各大网盘服务商都为开发者提供OAuth协议的接口。OAuth是一个用于授权的开放标准，它允许用户授权第三方访问用户存储在服务器的信息而不用泄露用户的身份信息。若用户同意授权，授权服务器会颁发给第三方应用一个令牌（token）用于访问用户的私有资源。出于安全的考虑，整个授权的流程会通过HTTPS进行数据传输。HTTPS是一种网络安全的传输协议，利用SSL/TLS对传输的数据包进行加密。本文首先在Android平台上使用新浪微盘提供的API实现了具有上传下载微盘文件功能的应用程序，并使用Burp Suite抓取HTTPS数据包的功能，获取了用户授权Android应用程序访问新浪微盘的认证过程及应用程序上传下载文件过程的流量。其次，通过抓取的数据包分析其详细的认证流程，以及上传下载文件的流程。最后，利用C语言在Linux环境下验证其认证协议，取得token并实现上传下载文件以及获取文件列表的功能。

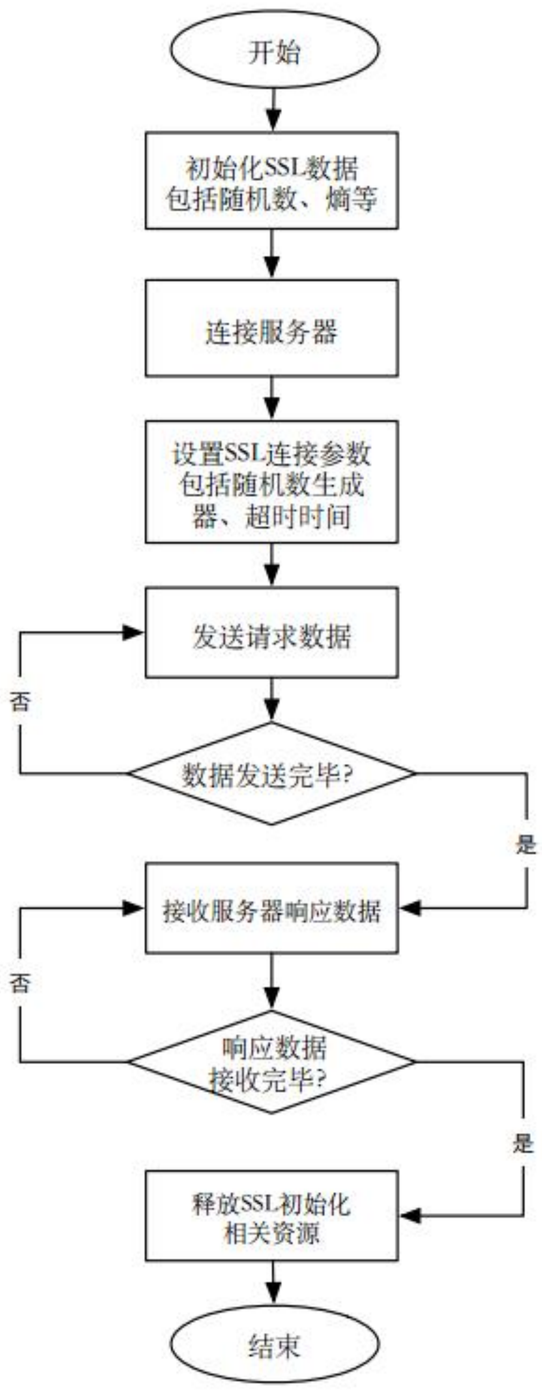
OAuth协议认证流程

（A）用户打开客户端以后，客户端要求用户给予授权。
（B）用户同意给予客户端授权。
（C）客户端使用上一步获得的授权，向认证服务器申请令牌。
（D）认证服务器对客户端进行认证以后，确认无误，同意发放令牌。
（E）客户端使用令牌，向资源服务器申请获取资源。
（F）资源服务器确认令牌无误，同意向客户端开放资源。



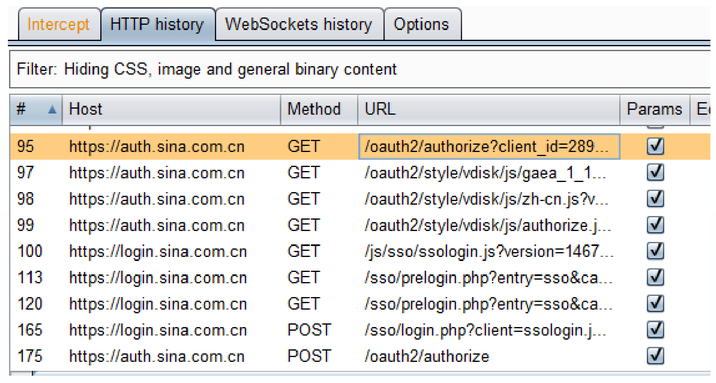
HTTPS请求流程

为了对新浪微盘OAuth协议的分析过程进行验证，我们将在不使用相关的SDK接口的情况下，对认证流程进行模拟。我们通过编写C语言程序，使用socket编程，实现将测试文件上传至该网盘以及从网盘上下载文件的功能。根据对数据包的分析，我们使用封装好的请求接口，模拟数据包交互流程。针对每一步骤，向对应的链接发送POST或者GET请求，从每一次服务器的响应数据中提取认证所需要的数据。经过模拟交互流程后，我们成功地从服务端获取到access token。在获取access token后，我们可以向网盘上传文件以及从网盘上下载文件以及获取网盘文件列表功能。



新浪微盘授权流程

为了分析和验证网盘的认证流程，首先在Android手机上实现了一个具有上传下载微盘文件功能的程序。借助对Android平台上第三方应用程序的授权流程的分析，了解详细的新浪微盘的OAuth认证流程。然后利用工具获取其认证过程中所有与服务端交互的数据包，以下是新浪微盘认证数据包拦截结果：



通过分析拦截的数据包，我们可以发现从发出请求到获得Access Token，客户端与服务器一共进行了五次关键的交互。

（1）请求登陆授权页面

https://auth.sina.com.cn/oauth2/authorize?client_id=2890504325&response_type=token&redirect_uri=http://weibo.com/

（2）请求SSO JavaScript代码

https://login.sina.com.cn/js/sso/ssologin.js?version=1448953200

（3）请求prelogin计算参数信息

https://login.sina.com.cn/sso/prelogin.php?entry=sso&callback=sinaSSOController.preloginCallBack&su=&rsakt=mod&client=ssologin.js(v1.4.15)&_=1448954523256

（4）获取ticket数据

https://login.sina.com.cn/sso/login.php?client=ssologin.js(v1.4.15)&_=1449476103800

（5）获取Access Token令牌

https://auth.sina.com.cn/oauth2/authorize

从服务器得到Access Token后，我们就可以利用Access Token进行获取文件列表，上传文件以及下载文件的操作：

- 获取文件列表：

http://api.weipan.cn/2/delta/sandbox/?access_token= Access_token

- 上传文件：

http://upload-vdisk.sina.com.cn/2/files/sandbox+filepath

+filename+?access_token=Access_token

- 下载文件：

http://api.weipan.cn/2/files/sandbox/+filename+?access_token=Access_token

结论

OAuth是一个用于授权的开放网络标准。OAuth协议为用户资源的授权提供了一个简单的、开放而又安全的标准。OAuth协议被广泛应用于各大网络供应商的开放平台，是一个值得深入研究的协议。国内外主流网盘都为开发者提供了OAuth协议的开放API，方便第三方应用安全地读、写、修改用户存储在网盘上的文件。本文首先通过对新浪微盘的登陆授权流程的详细分析，详细阐述了新浪微盘的OAuth的认证流程，同时分析阐述了HTTPS协议的交互流程。最后在Linux平台利用C语言实现了新浪微盘的登陆认证流程，并成功实现向网盘上上传文件以及从网盘下载文件和获取文件列表的功能。