web api 安全认证的方案（很严肃）

作者：mainlove
原文链接：https://ld246.com/article/1507707852093
来源网站：链滴

当你开发了你的网站的api，就必须对api的调用者进行安全认证

现在普遍的方案是（https是必须的）： 给你一个app_id 和 secret_id

1. 用app_id 和 secret_id 换取临牌token，token有时效性，一定时间再去换一个新的

2. 每个请求头都附带 app_id ,token 和 timestamps（时间戳）,nonce(随机数)，以及根据某个预设则把这些东西加上请求内容（请求的内容可以加密）用签名算法(MD5,SHA1或者HMCA-MD5)搞成个签名字符signature，一起发送给服务端

3. 服务端根据token判断是否合法的请求身份，根据signature判断请求的有效性（包含时间有效性，否被篡改），然后如果内容是加密的再进行一次解密

以上方案基本是现在微信，支付宝等的概要（如果那块说的很不对，求大家马上说明）

但我仔细想想还是有如下问题

● 第1步 直接传app_id 和 secret_id不安全，被截获了不就完了？ 我觉得secret_id永远不能直接传送不过好像支付宝有安全的第一步认证，加密摘要什么的，反正微信是没有，就直接传，这个不是很不吗?

● token 虽然有时效性，但是签名算法都是公开的，MD5，SHA1大家都会，被截获了还是有机会短间被盗用啊？ MHAC是不错的，但是HMAC利用了secret_id，那我就很好奇了为啥要去搞个token?

带着第二疑问我看到了七牛的API，七牛的API没有什么远程获取token的机制，每次的token都是自生成的，七牛每次的请求需要有一个凭证：这个凭证的生成办法是，对请求的url或者内容用secret_i做HMAC算法，然后转生base64，加上app_id 形成最后的凭证

也就是说根本不需要服务器提供token，因为HMAC算法需要一个密钥，用HMCA做摘要等于起到了个目的，1 防止篡改 2 app_id 和 secret_id的认证，因为错误的secret_id无法生成出这个app_id的证，这不就等同于用户名密码的校验了?

那个为什么还需要远程获取token这个动作？？ 个人认为这个东西有所多余了

请大家指正！！！