黑客派

AES对Restful接口进行简单的数据校验之移动篇(iOS&Android)

作者：melon

原文链接：https://hacpai.com/article/1456742681258

来源网站：黑客派

随着Restful的普及，越来越多的项目开始使用这种形式来进行接口的编写。Restful本身是无状的，所以我们要对接口进行一些安全的校验，这可以从两个维度来考虑这个问题，1.防止接口数据被意重刷造成资源和数据的浪费 2.对用户进行权限校验来防止数据被恶心篡改

1.首先来说第一种情况: （主要是防止重放攻击）
关于重放攻击
对应项目中的一些数据接口，有一些是用户不需要登录，游客情况下就可以进行查看浏览的，这候我们不需要进行用户权限信息的校验，只需要来过滤一些非法请求和无效请求即可；
实现思路 : 客户端(iOS*Android) 对请求的数据进行 paramters+timestamp+appkey=sign形的AES加密，客户端与服务器端规定好密钥，服务器接收到数据后对数据进行解密，拿到时间戳后与前时间戳进行比对，如果已经超出当前时间2分钟(可根据业务)则判定这次请求无效，不进行数据返回
<img src="https://static.hacpai.com/images/img-loading.svg" alt="" width="627" height="311" data-src="http://static.wooyun.org//drops/20151016/2015101611045213385client.png">
2.用户校验
这时调用的接口需要知道用户的状态才能进行调用，我们可以采用token的形式，就是过用户身份认证之后服务端给客户端分配一个token,这时候调用接口时的sign就变成了 paramers+timestamp+appkey+token，而且服务器端可以对token进行灵活变动，比如每个token的使次数是500次，超出后会重新下发新的token；或者对这个token的使用频次以及ip进行判定，这里可根据业务需求来进行发挥。

今天所给出的方案都是最基础最简单的方案，可以满足比较简单，对安全性能要求不高项目，后面我会慢慢增强校验的安全级别 :p