防盗链方案设计

1. **UML序列图**



1. **方案设计的三个关键点**
   1. 对客户端的检查

检查客户端是否是合法的客户端。

* 1. token的生成/检查

通过检查token中的时戳，判断是否是报文重放攻击。

* 1. url的加密/解密

通过url加密，隐藏真正的媒体资源播放地址。

1. **对客户端的检查**
   1. 检查过程上述检查过程是通用的比较完整的检查过程，如果跟网站交互，可能略嫌复杂，可采用下面的简化过程。
   2. 简化过程



* 1. 更简的过程



客户端如果可以解密，那么继续后面的流程，如果不能解密，那么服务终止。

1. **token的生成/检查**
   1. token的生成

token= (u\_int32\_t)client\_ip+(u\_int16\_t)client\_port+(u\_int64\_t)timestamp

说明：

* client\_ip为大端序
* client\_port为大端序
* timestamp为大端序
* +，意思是字符串连接
  1. token的检查

按照生成规则，解析得到client\_ip, client\_port, timestamp, 如果timestamp在6小时内，那么继续服务，否则，拒绝服务。

* 1. token加密/传输

token容易被猜解出含义，token也同样加密一次，加密算法与url加密算法相同，也采用Hill加密。

为了传输，加密之后，采用Base64编码。

接收，跟解密，是逆过程，不再详述。

1. **url的加密/解密**
   1. url加密

加密算法采用Hill密码算法，矩阵选择2阶矩阵，模选择256，可加密包含256个字符组成的字符集。关于Hill算法的介绍，请参考下面两篇文章：

<http://hi.baidu.com/199836199836z/item/6f6261a996f67e9115107331>

<http://baike.baidu.com/link?url=umH7KIZKa2wrF1r5lv6Zmff8onnawqQ2OIx6BeSmDGG5pi1snjmW_gYpSZDAOWqJ>

加密字符串，例如：funshion1，那么首先将字符串补齐为2的倍数，不够请补'\0',

每两个字符的数字值，例如fu，组成行列式（102， 117），与二阶矩阵，例如

{ 129, 77 },

{ 6, 99 }

做乘法运算，得到（13860,19437），做模256运算，得到（36,237）。

这样得到的结果，做Base64编码，方便url传输。

* 1. url解密

Hill解密算法，与Hill加密算法，计算过程完全一致，唯一不同的是，解密的二阶矩阵是加密矩阵的逆阵，对应上面就是：

{ 151, 167 },

{ 146, 189 }

* 1. decrypt\_key=Base64(逆阵)

对应上面的逆阵，传输的数据应该是"97A792BD"，固定长度为8BYTE。

如果token也采用密文，那么decrypt\_key = Base64(逆阵url) +Base64（逆阵token），固定长度为16BYTE。

1. **系统升级步骤**

为避免全系统升级，牵涉面太大，可以考虑分期实施。

* 1. 项目一期

仅牵涉client和server\_1，仅实现客户端的检查，和url加密/解密，跟交互图不同的是，由客户端解密url，后面的访问server\_2，server\_3，仍然沿用老的协议。

项目一期的客户端为flash客户端，和网站服务器。

如果证实可行和必要，移动客户端，和zeus服务器，跟进。

* 1. 项目二期

server\_2，server\_3，加入对token的检查。

1. **token与url分离还是包含**
   1. 如果是分离，那么token与url数据平行，可独立分离，分别处理
   2. 如果是包含，那么url数据内包含token参数，好处是url解密之后，可直接使用，无需拼装url和token参数。