防盗链方案设计

1. **UML序列图**



上述流程中的4个成员，可能分别对应于：

* 1. 移动客户端，zeus，jobsfe，和MediaServer；
  2. flv客户端，网站服务器，jobsfe，和MediaServer；

对应移动客户端和zeus之间：

* 客户端发送http://jsonfe.funshion.com/v3/media/get\_serial\_play报文，参考文档<http://redmine.funshion.com/redmine/projects/zeus/wiki/%E5%AA%92%E4%BD%93%E6%92%AD%E6%94%BE%E4%B8%8B%E8%BD%BD%E4%BB%BB%E5%8A%A1>
* zeus回应的json报文如下：

{

"retCode": "200",

"retMsg": "ok",

" encrypt ":"1",

" list ":"data...",

}

其中，data... = key1\_token + key2\_data + encrypt\_token + encrypt\_data

zeus内置16组加密/解密秘钥，随机选择其中一组为token或者data加密；加密完成后，将对应的解密秘钥组装到data数据包内。(组装示例，请见本文附件。)

对应flash客户端和网站服务器之间：

* 客户端发送<http://api.funshion.com/ajax/get_webplayinfo/106943/1/mp4>报文，
* 网站服务器回应的json报文如下：

{

"category": "movie",

"mediaid": "106943",

"playinfos": "data..."

}

其中，data... = key1\_token + key2\_data + encrypt\_token + encrypt\_data

网站服务器内置16组加密/解密秘钥，随机选择其中一组为token或者data加密；加密完成后，将对应的解密秘钥组装到data数据包内。(组装示例，请见本文附件。)

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**

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= client\_ip+client\_port+timestamp

说明：

* client\_ip为大端序十六进制打印形式，4BYTE
* client\_port为大端序十六进制打印形式，2BYTE
* timestamp为大端序十六进制打印形式，8BYTE
* +，意思是字符串连接

例如：

客户端的ip为10.20.30.40，那么client\_ip=0A141E28

客户端的port为55613，那么client\_port=D93D

当前的时戳为1383024435，那么timestamp=00000000526F4733

综上，那么token=0A141E28D93D00000000526F4733

* 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**

采用Hill2加密/解密算法

1. **Hill2加密/解密算法**

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>

* 1. Hill2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。

加密字符串，例如：funshion1，

每两个字符的ASCII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）。

* 1. Hill2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=Base16(逆阵)

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

1. **示例**
   1. **token**

客户端的ip为10.20.30.40，那么client\_ip=0A141E28

客户端的port为55613，那么client\_port=D93D

当前的时戳为1383024435，那么timestamp=00000000526F4733

综上，那么token=0A141E28D93D00000000526F4733

* 1. **key1 for token**

加密token的矩阵，假设为：

{ 129, 77 },

{ 6, 99 }

解密token的矩阵，应该为：

{ 151, 167 },

{ 146, 189 }

十六进制打印，得到：

97A792BD

* 1. **token，加密后，得到：**

82BE0E7EC7DC00000000EC97F914

* 1. **加密后的token，做base64编码，得到：**

gr4OfsfcAAAAAOyX+RQ=

* 1. **data**

假设为："hello, funshion"

* 1. **key2 for data**

加密data的矩阵，假设为：

{ 231, 247 },

{ 66, 21 }

解密data的矩阵，应该为：

{ 145, 245 },

{ 166, 59 }

十六进制打印，得到：

91F5A63B

* 1. **data，加密后，得到：**

E2A14C1081B52C3EEFE9957D5D6A6E

* 1. **加密后的data，做base64编码，得到：**

4qFMEIG1LD7v6ZV9XWpu

* 1. **综上，data... = key1\_token + key2\_data + encrypt\_token + encrypt\_data，**

应为如下形式：

97A792BD91F5A63Bgr4OfsfcAAAAAOyX+RQ=4qFMEIG1LD7v6ZV9XWpu