**MediaServer防盗链方案设计**

参与防盗链的角色，有三个，客户端，tuner服务器，MediaServer服务器。

交互过程有两个：

过程1：客户端到tuner服务器的登录认证过程；

过程2：客户端到MediaServer服务器请求播放视频的过程。

过程1. 客户端到tuner服务器的登录认证过程

1. 客户端连接到tuner服务器，发送自己的用户名(user)和内网IP（inner\_ip），请求一个随机秘钥；
2. tuner服务器，收到客户端的请求，计算随机秘钥random\_key，返回给客户端；计算过程如下：
   1. 得到客户端的公网ip(public\_ip)和port；
   2. 收到客户端的用户名(user)和内网IP(inner\_ip)，这时候可以做如下判断：
      1. 如果该用户名(user)不存在，或者过期用户，断开连接，拒绝服务；
      2. 如果该客户端的公网IP(public\_ip)，属于我们要屏蔽的网段，拒绝服务；
      3. 如果该客户端的公网IP(public\_ip)，我们允许，内网IP(inner\_ip)属于我们要屏蔽的网段，拒绝服务；
   3. 获取当前时间的秒数timestamp；
   4. 计算一个随机整数rand；
   5. 拼接成一个字符串，形如public\_ip:port:timestamp:rand，该字符串命名为client\_infomation;
   6. 对client\_infomation签名，生成一个MD5值，作为随机秘钥random\_key，返回给客户端；
3. 客户端接收到random\_key，执行如下步骤：
   1. 使用自己的密码password，和收到的随机秘钥random\_key，拼接一个字符串，形如password:random\_key，该字符串命名为passport，
   2. 对passport签名，生成一个MD5值，该字符串命名为client\_authentication，
   3. 客户端发送client\_authentication，和影片名称info\_hash.dat；
4. tuner服务器，执行如下步骤：
   1. 从数据库中取出该用户的密码password，
   2. 同样地执行步骤3），生成client\_authentication\_2，比较client\_authentication和client\_authentication\_2；如果不同，认证证失败，断开连接；
   3. 认证成功后，拼接一个字符串，形如user=xxxx&inner\_ip=xxx.xxx.xxx.xxx&public\_ip=xxx.xxx.xxx.xxx&timestamp=xxxxxxx，该字符串命名为token；
   4. 对token做DES加密，生成一个DES\_key;
   5. 查询拥有该影片的MediaServer，返回url地址给客户端，http://ms\_ip/info\_hash.dat?key=DES\_KEY；

过程2. 客户端到MediaServer服务器请求播放视频的过程。

1. 客户端向ms\_ip发起连接，MediaServer得到客户端的ip，命名为client\_ip;
2. 客户端发送url请求，MediaServer收到该http请求后，分离url参数，取得DES\_KEY，进行DES解密，还原得到token，得到形如user=xxxx&inner\_ip=xxx.xxx.xxx.xxx&public\_ip=xxx.xxx.xxx.xxx&timestamp=xxxxxxx，执行如下步骤：
   1. 进行字符串形式检查，如果形如上面，则继续，如果乱码，则拒绝服务；
   2. 进行ip检查，如果client\_ip等于客户端的public\_ip，或者等于客户端的inner\_ip，则继续服务，否则断开连接，拒绝服务；
   3. 检查本地时钟，如果本地时钟距离current\_seconds，已经过去4个小时，那么是过期的请求，拒绝服务；否则，提供服务。
   4. 如果提供服务，可以针对用户分类统计。

在上述两个过程中，客户端不需要了解key的生成算法，key的生成对客户端来说是透明的，它当然也不知道key里面的内容是什么。

需要的约束是：tuner服务器和MediaServer拥有一个同样的DES算法的秘钥，tuner端加密，MediaServer端解密。

用户名密码分配可以暂定如下几个：

funshion:password

360:password

anonymous:password

评审的标准：

* 能否抵御报文侦听，然后报文重放；
* 如果该方案公开，能否抵御攻击；
* 如果用户名密码泄露，能否及时补救；
* ... ...

执行方案可能结合现实条件，有所折中，或者分阶段，分步骤执行；不过方案首先要是一个完整的方案。