对于防刷票机制方案的思考

来源：八方[刷票](http://www.8fvote.com/) <http://www.8fvote.com>

随着网络的发展，越来越多的评选活动采取了网络投票的制度，也因此刷票这个概念便出现在了大众面前。作为一个程序员如何维持网络投票的公正和严谨，如何尽可能的避免刷票出现的几率成为了开发此类程序不得不考虑的问题。就目前而言着实是没有一个完美的解决方案。现行的所有机制其实都只是做到了“防君子不防小人”。  
刷票分为两个大类：一类是人为主体，通过人力去刷票。另一种更为可怕，通过特定的刷票机去代替人力完成令人恐怖的批量刷票。  
现行的防刷票机制  
1、验证码：确切的说验证码的出现不是针对于人，而是针对于机器。通过复杂度和识别难易度的控制来阻拦掉一部分刷票机，从而减少刷票的发生。但随着软件技术、识别技术的发展越来越多的验证码面对着先进的刷票软件也失去了其防范的作用。  
在看了评论者“Javascript” 的评论后，我突然发现我忽略了一种方案：就是改变验证码，让他成为可变的，这里的可变是指含义可变，然后将其封在flash等第三方载体中。这样避免机器直接通过img标签找到他解析他。同时我改变其含义，比如在flash呈现中（需要使用flashremoting,如果单独的走LoadVars从后台页面返回值则必须加密），第一次我要他输入出现的数字，第二次要他输入出现的字母中的第三个字母，更或者是一个加法题或是问答题（当然要很简单的那种），甚至我还可以通过FMS传输音频流等（当然这就太复杂了），这样一来机器识别的难度就又加大了。当然验证码的采取主要是对机器，因此高难度的验证码会降低用户友好度。  
  
2、Cookie：这个应该是很老很原始的一种方式来防止刷票了。对用户的每次投票进行Cookie的记录，当下次投票时进行检测发现Cookie中已经存在了此投票记录则禁止此次投票。很遗憾的是此方式对于大多数网民已经失去作用（当然除了特别嫩的菜鸟外）。只需要通过IE清掉Cookie限制就将解除。  
3、IP限制（+时段）：这种方式也是目前最多的防刷机制。能屏蔽掉部分的刷票。但是其存在很多局限，因此程序员也不得不放弃小群体（采用统一出口的群体，例如网吧等）来顾全大群体。人们上网大都是活动IP地址，因此是不存在真正意义上的IP防刷的。笔者认为其实IP的方案并不是真正的防刷，更应该说他是采用了一种策略：加大投票操作难度和时间成本从而使部分投票者放弃刷票。只不过这种投票操作的难度增加不会影响到当前用户的流程，他是在后台由程序员完成的。也就是说在前台用户操作上没有任何变动因此具有一定的友好性。  
4、Mac地址：这种方式比较少见，但是网上有人提出。因为IE的安全级别是不可能获得用户的Mac地址的，只能通过安装ActiveX或是对IE进行特定设置才能实现。个人觉得此效果并不好。一是加大了用户投票的难度，二是Mac地址其实也是可以修改的。  
现行方案中都没有一个很好的防止方案。防止刷票之所以很难有完美的解决主要原因在于人。人是一种很聪明、很勤奋、很有耐心的天才动物，有这么一句话“天才就是重复次数最多的人”。因此不论你如何设定防范规则都很难凑效。即便你的规则可以难倒恐怖的刷票机，你却没有办法难倒勤奋有耐心的人。你防止IP我就重复着拨号，你Cookie限制我就重复着清Cookie，你做Mac限制我跟着换，只要我肯花时间没有办不到的。这也再一次应征了那句话“防君子不防小人”  
探索新的方法或解决办法  
在上面提到了人的恐怖性，所以这里也不是说我能探讨出一个突破障碍的方法，只是想想研究研究罢了。  
1、首先，我们不从程序实现上考虑。置身事外，逆向思维，想想我们是如何突破限制而刷票的？最严重的问题莫过于我们喜欢“此地无银三百两”。从事过反汇编和软件破解的人应该都知道，软件最好的保护方式就是对于那些触碰了敏感区域的行为记录拦截而不给出明确提示（在软件领域甚至不提示）。往往一些软件在用户输错注册码后弹出一个什么“您输入的注册码有误的信息”，这不就是自报家门么？高手们便可以在浩瀚的汇编代码中根据这个提示精确定位，从而修改代码跳过注册。你辛苦多时的代码就因此举废了。因此投票程序也一样，其实我很不明白有些程序干嘛提示“此IP今日已投票，请不要再次投票”。有人说是为了客户友好，我则不然，对于菜鸟你弹出此信息他绝对是一头雾水（我刚开机，刚上网怎么就提示不能投票？），即便此时你弹出“投票受限，请明日再试”他也会是一头雾水。然则不同的是既然两者都是一头雾水，干嘛不走后者，干嘛把话说的那么明显，莫非你是想提醒他“你去找找人给你换IP吧”或是“你该重新拨号了”。同样是弹出提示这两种提示在非菜鸟的眼里结果可能就不同了，至少能让一部分人摸索一下。  
2、从程序上考虑。这里我将提出一个新的方式，通过实际测试又防止了一批小人，但是明白人还是可以突破的。这里要先从一场经历说起。  
以前读书时在学校学工处任网站部长，学工通常喜欢在每年举办一些投票的评选活动，什么“风采女生”啊“感动人物”啊的网络投票。当初就是采取了Cookie+IP的限制，然后静观其变。不久就发现了刷票情况，换着IP的情况越来越严重再加上学校机房公用一个出口因此必须解除IP限制。为此不得不采取别的方式。因为身处学工我们能够拿到在校生的学号和身份证号，于是企图通过这两者匹配登陆的方式进行刷票防治。前几日情况稳定，后来情况恶化，出现有人通过花名册来刷票，由于撤销了IP限制，这种刷票一下子暴增。我们又不得不去总结和寻找新的办法。  
不论是IP，Cookie，即便是身份证和学号的匹配，其实我们都是在“此地无银三百两”。我们明确的告诉了投票者我们的限制规则，所以必须找到一种隐秘不易察觉的方式。最后我找到一种方式。这种方式的来源还得感谢 Blueidea（很不错的网站）中的一篇关于Flash广告用户友好度的文章。我们都知道页面中的Flash广告从一个页面切换到另一个页面后又是从头播放的。那片文章提到的就是利用Flash中的一个对象（这里我就不直接指出了，有兴趣知道的朋友看看Flash就知道是什么了）来存储当前播放信息。受此启发再加上以前做“Flash接口版大头贴程序”时积累的Flash和JS交互经验，便成功的完成了此插件。原理流程如下：  
用户尝试登陆-检测登陆信息是否正确-正确则置过度变量（Session）值-进入有此flash检测的页面（当然此页面你要尽可能伪装，切不可以自自报家门，我伪装成类似于淘宝登录时证书检测的效果）-如果flash检测正常则将此账号通过flash追加到本机-调用js跳转到转正页面（即清掉过度变量Session，将过渡值转给正式的Session储存）-这样用户就可以投票了  
关于Flash的检测，其实Flash只是Load后台的设置（包括 单机允许登录的账号个数+时间戳）然后再和本机存储了的登录个数+时间戳匹配并返回结果即可  
通过此方式后，发现情况大有好转，多次活动结果表示此方案能一直稳定到活动结束。从数据库中的记录看出，同一IP同一天几乎都是5个账户的投票信息（当初限制的是单机限制5账户），而且此方式即便用户清除Cookie，重新拨号，重启电脑都是没有用的，至于为什么，那得研究Flash了，其实他是将变量存储在了一个特定的位置哦。所以这种方式由于不太常规因此知道突破的人就少。当然这里说到的是需要登录的方式，如果匿名方式可以用此方法么？其实也是可行的，只不过需要后台自动根据当前时间戳分配一个唯一标示给客户并自动模拟登录供Flash记录，流程上就又得麻烦了。  
总之：防止刷票不可能有一个完美的方式，也不可能有一个长久的方式。如何防止刷票关键在于如何“蒙蔽用户”，让他不知道你的限制规则，再加上合理增加投票的难度和成本开销，这样可以减少刷票的产生。多限制方案下手多管其下也许能达到比较好的效果。本文[**swqqcs**](http://my.csdn.net/swqqcs)编写。