你所有的脸都属于我们

——打破Facebook的社交认证

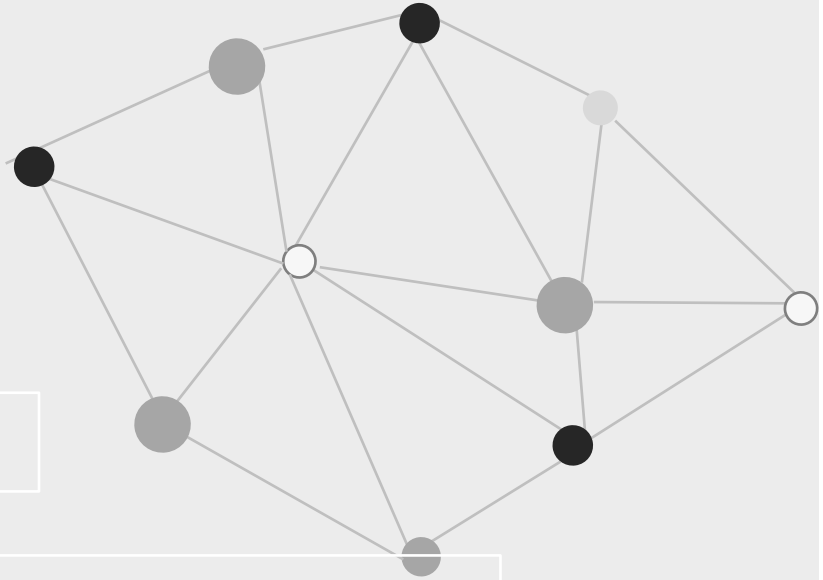
李敏
1601210947

一、简介

- 在线社交网络（OSNs）面临授权证书泄露，个人信息被窃等危机
- 目前网上银行，谷歌云服务已经采取了双因子认证策略，所谓双因子，就是用户持有双重认证的口令，一般情况下，一个因子是用户熟知的密码信息，另一因子就是具体可见的令牌环物理设备。但是物理设备对于用户携带极其不方便。
- 2011年，Facebook引进了一种所谓的社交认证（SA）的策略，作为双因子认证的第二因子，该认证方式基于用户的社交信息
- 本篇论文的核心是设计一个自动的，组合式的系统来攻破Facebook的社交认证系统

二、社交认证

2.1、认证过程



- 用户首先需要使用密码进行登录
- 当Facebook认为用户的此次登录有必要进行双重因子认证的时候，就会触发社交认证
- 在社交认证过程中，Facebook会列出7张该用户熟知的照片，然后提供6个名字，让用户从中挑选正确的名字。从而进行认证

2.2 社交认证的条件

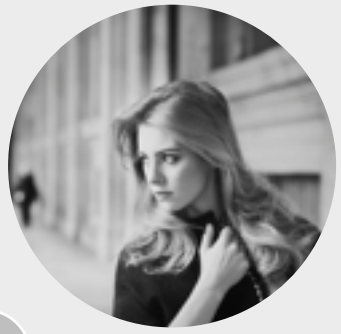
- 列出朋友清单。Facebook要求每个用户需列出50个朋友的照片作为验证
- 对照片打标签。每张照片需要打上标签，以便在进行社交认证的时候，Facebook能够给出相应被标记过的照片
- 人脸认证。一般情况下，Facebook会给出7张照片，用户需要选对其中的5张才算通过，而且时间限制在5分钟内。
- 社交认证的触发。当Facebook探测到可疑用户尝试登录的时候，就会要求用户进行社交认证。一般情况下，当用户在不同的地理位置登录，或者使用新设备第一次登录系统时，该社交认证就会被触发。

2.3、优缺点分析

- 传统的双因子认证（比如短信验证，或者物理的令牌设备）太笨重，而社交认证不需携带额外的设备，灵活而且轻便

- 设计一个社交认证系统太过困难，在较小的校园范围不适用
- 需要标记朋友的数量不易确定
- 对不经常联系的朋友识别有困难
- 认证时给出多少张照片不易确定

2.4、威胁模型



也是另外一个人的朋友

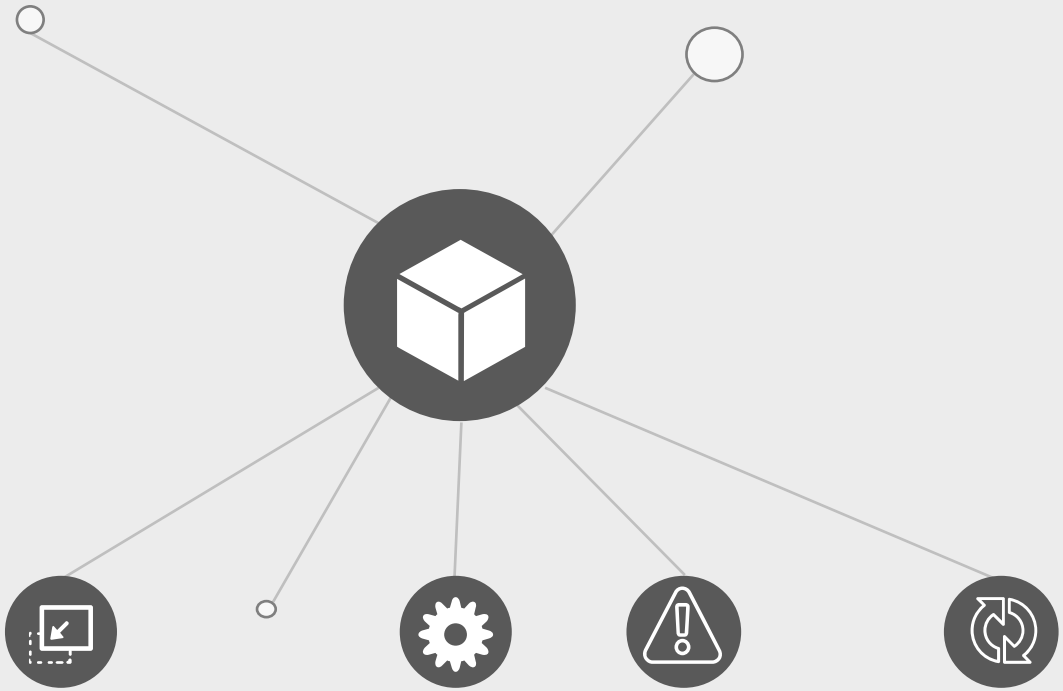
一个人的朋友很可能

2.5、攻击假设

假设双因子认证的第一因子是容易获取的，即用户密码容易获取

- 通过钓鱼网站
- 通过木马攻击
- 通过密钥登录截取
- 通过社会工程学

三、攻击社交认证



- 该攻击策略适用于所有的基于照片认证的系统，因为Facebook被广泛使用，我们以Facebook为例进行攻击说明

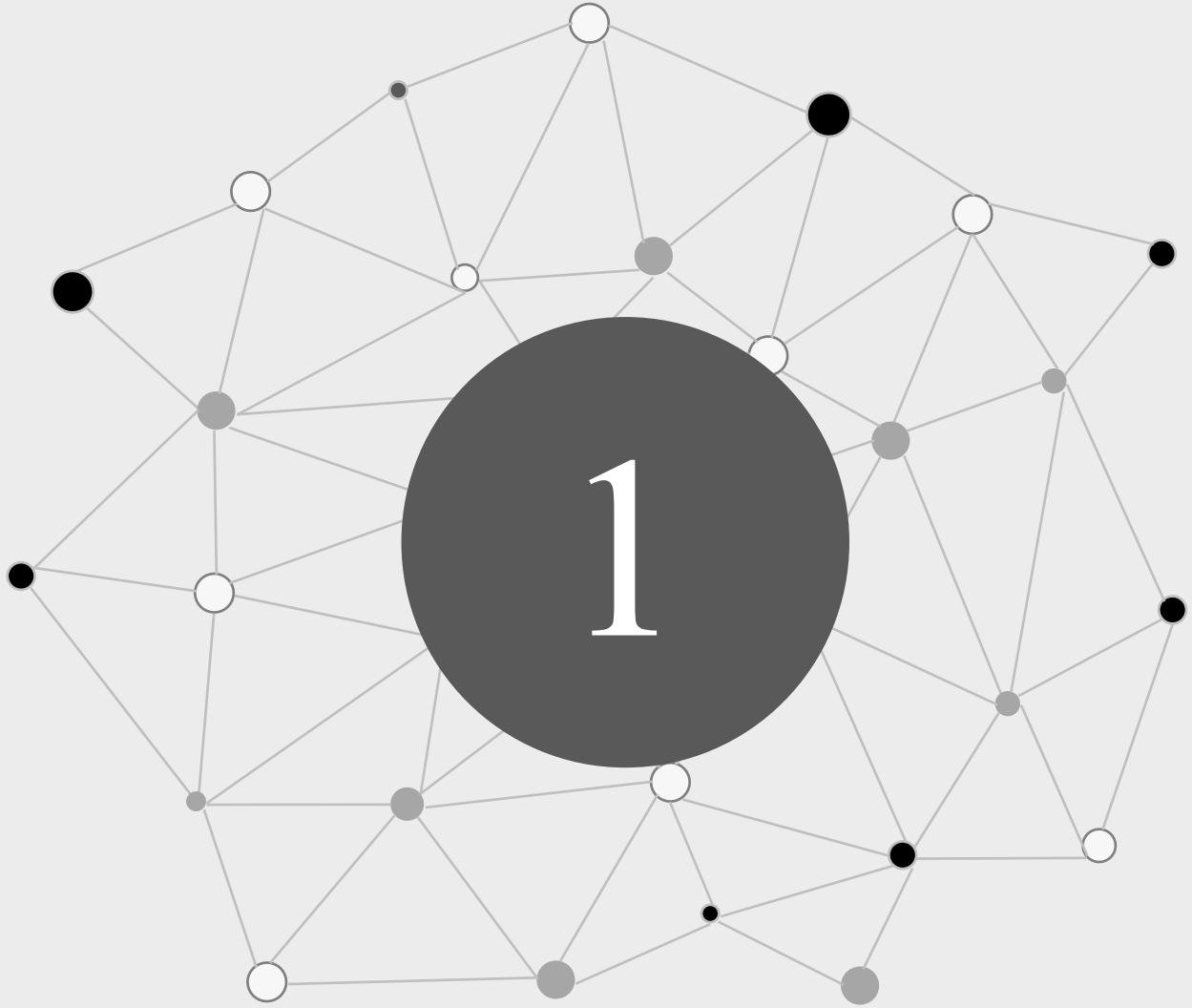
3.1、实现细节

NO.1爬取用户列表

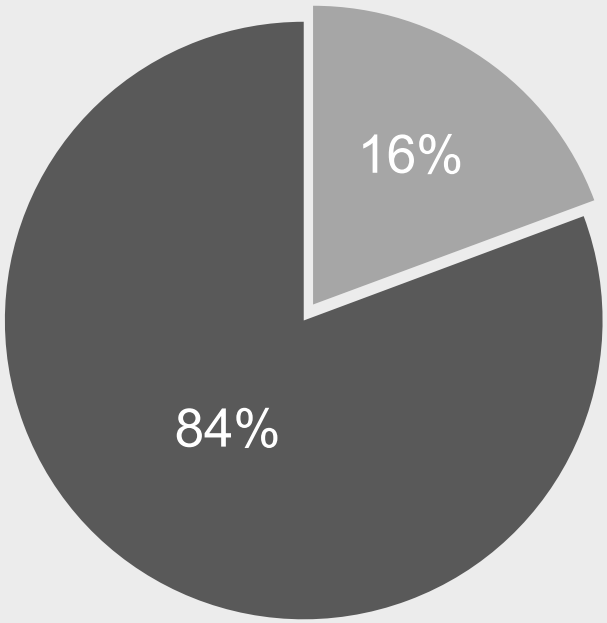
NO.2发起加友请求

NO.3照片收集

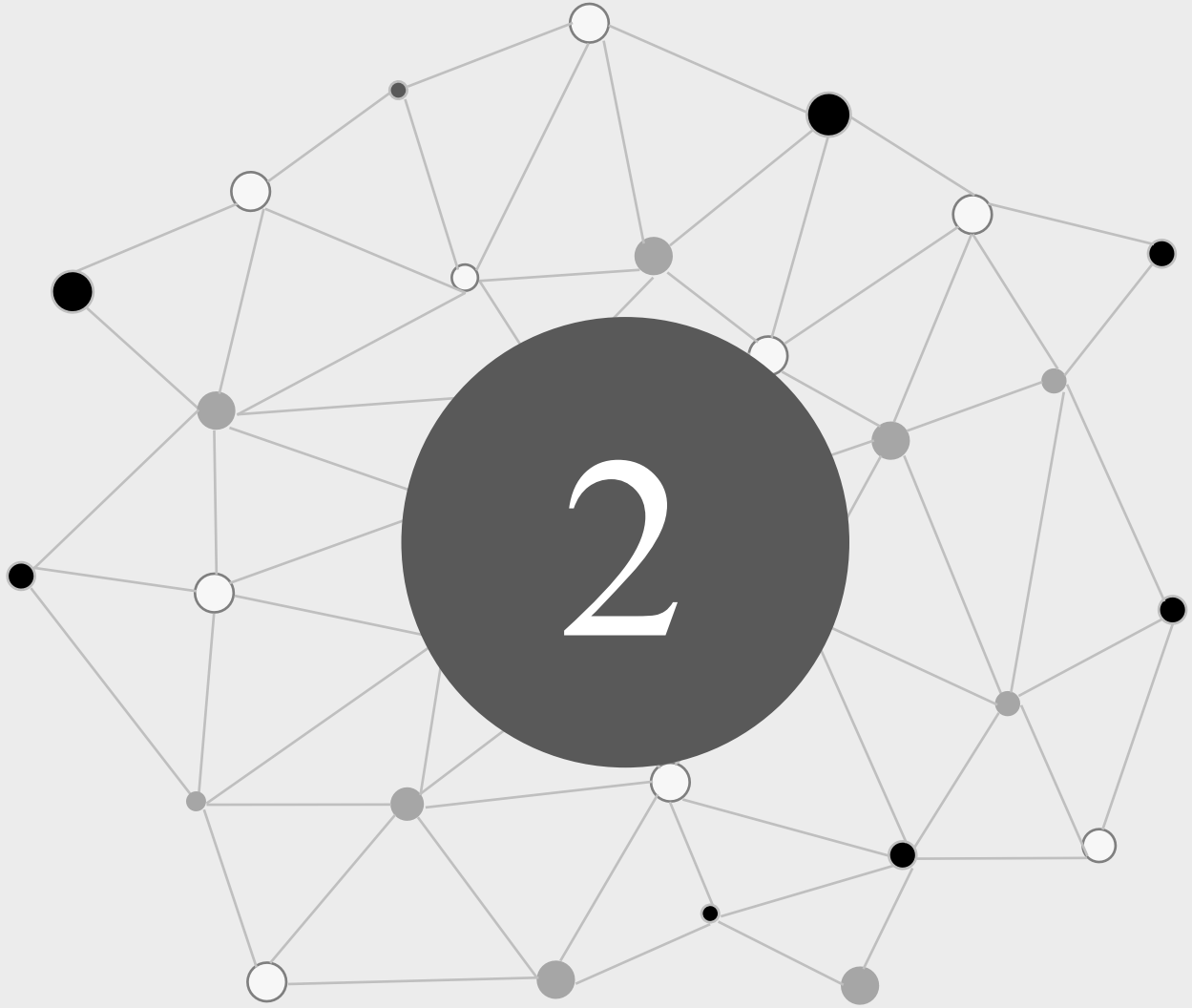
NO.4 姓名标记



爬取用户列表



- 给出被攻击者的UID，爬虫软件可以根据这个UID爬取该用户的朋友列表并将其存入到数据库中
- 弱攻击者可以获得约47%的好友列表
- 强攻击者可以通过加好友的方式，获取84%的好友列表



发起加友请求

提供吸引人的照片

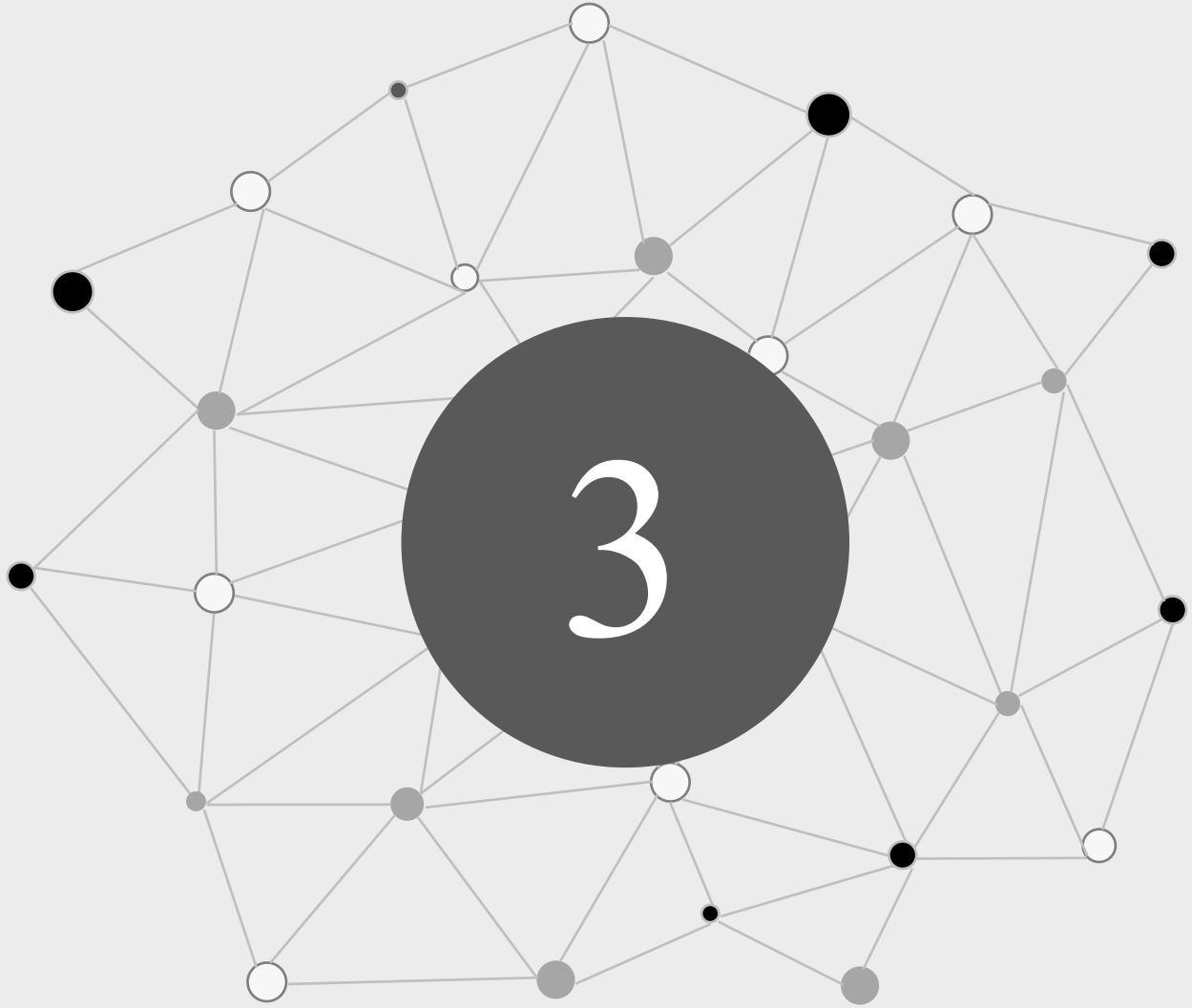
可以选择大家喜好的照片，这样更容易成功地加好友

伪造详细的个人信息

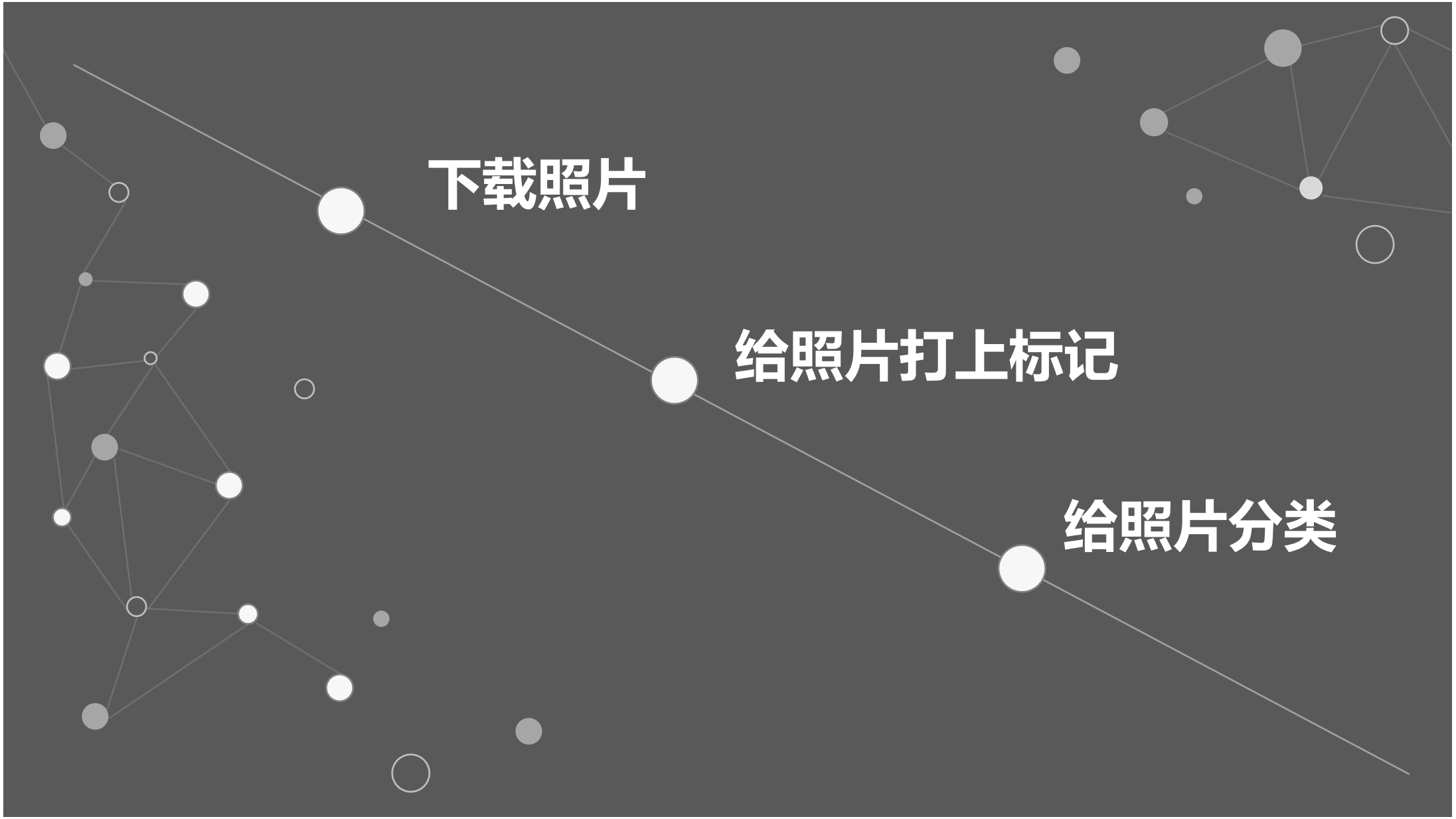
自己的个人信息越详细，就越容易成功地加好友

每天100次的好友请求

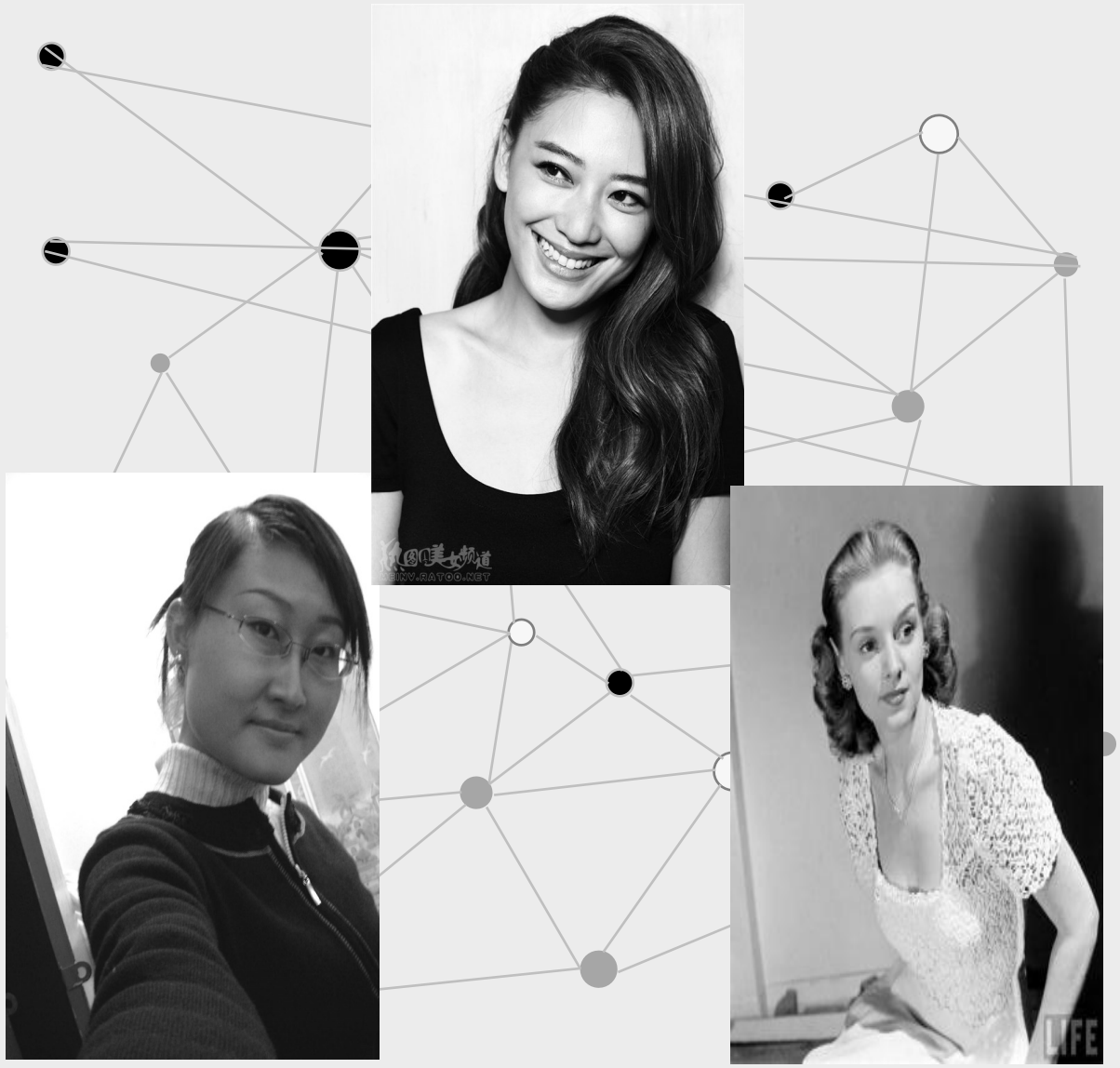
Facebook限制每天最多能有100次的好友请求，这已经足够了



照片收集


下载照片
给照片打上标记
给照片分类

姓名标记



- 该步骤需要社交认证系统辅助完成

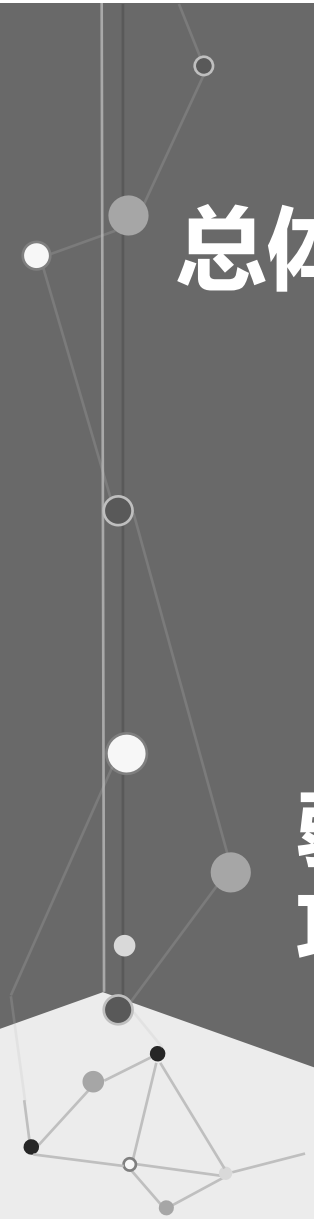
- 当尝试社交认证时，我们根据Facebook提供的6个姓名选项和7张照片，然后与我们数据库中已经分好类的照片相比较，从而可以查出对应人的UID号码，然后尝试关联姓名，并反复重复实验，最终能够得到姓名、UID、图片集的对应关系

四、实验评估

总体数据

强攻击者攻击评估

弱攻击者攻击评估



4.1、总体数据

从我们数据库中的照片来看，可以得到如下信息

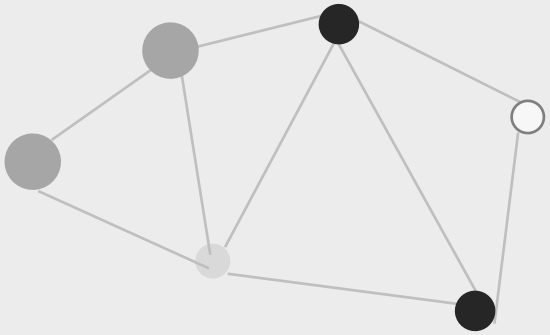
71%的用户公开他们的照片集

剩下的29%人将照片集保密

但在这29%人中，有38%的人被朋友标记过

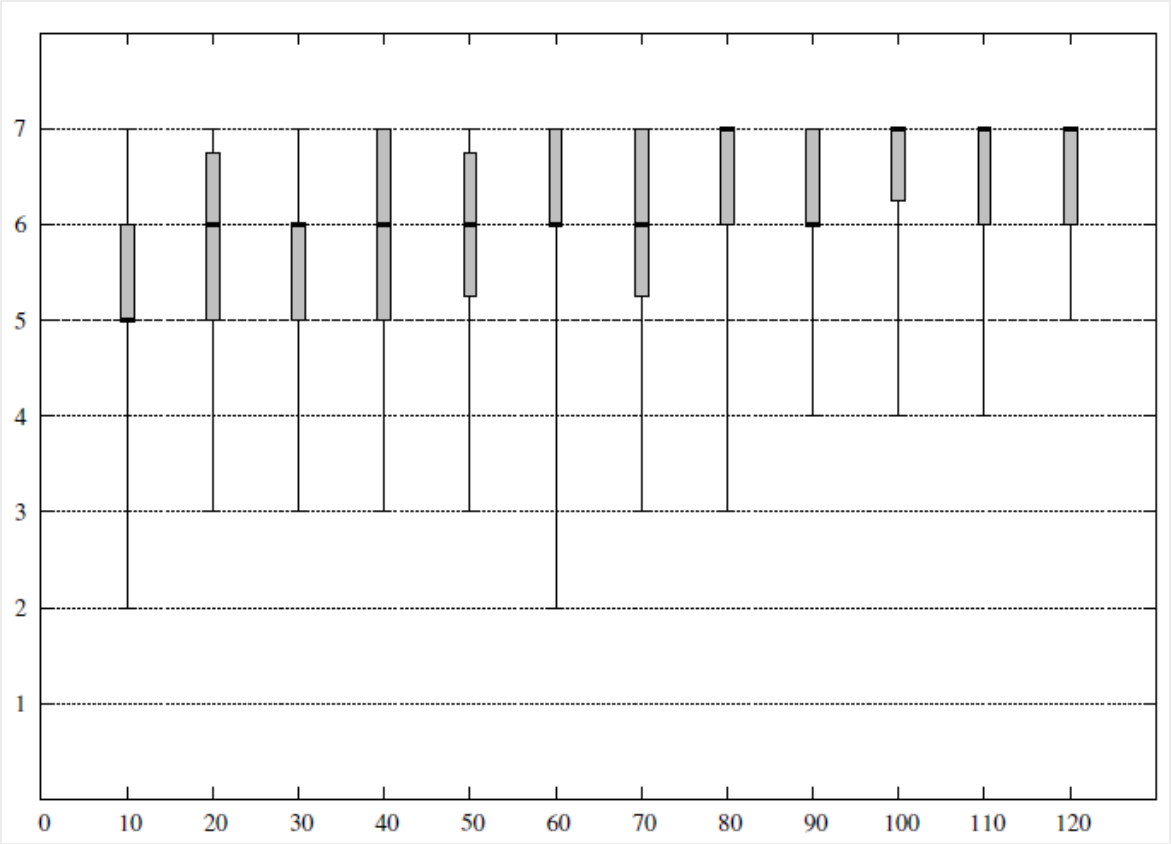
剩下的62%的照片任然不可获得

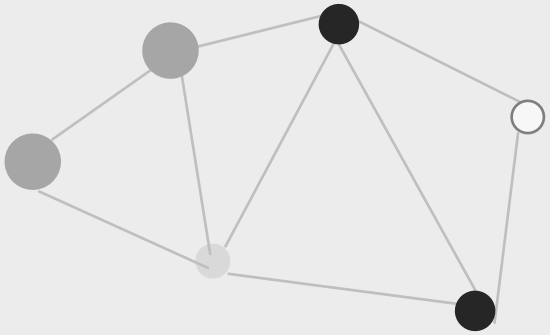
人们对照片做标记的同时，不仅泄露了自己的信息，也泄露的朋友的信息。尽管这些信息很少，但是已经足以做攻击的实验了。



可以看出，当每一个UID收集的照片超过70张时，对于社交认证中7张照片，有5张照片可以识别的概率可以达到100%

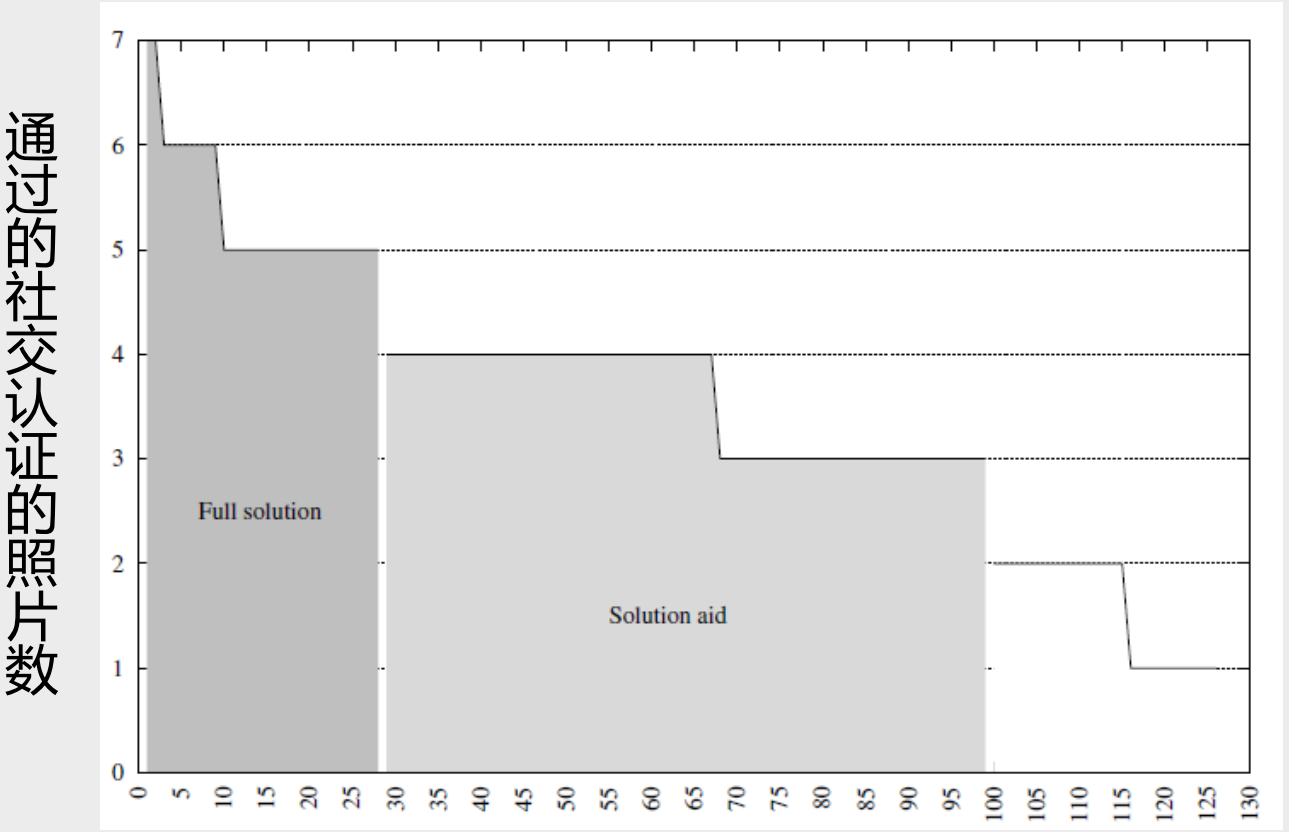
强攻击者攻击评估





可以看出，大约有22%次可以识别5张以上的照片，约71%次可以识别4张以上的照片

弱攻击者攻击评估



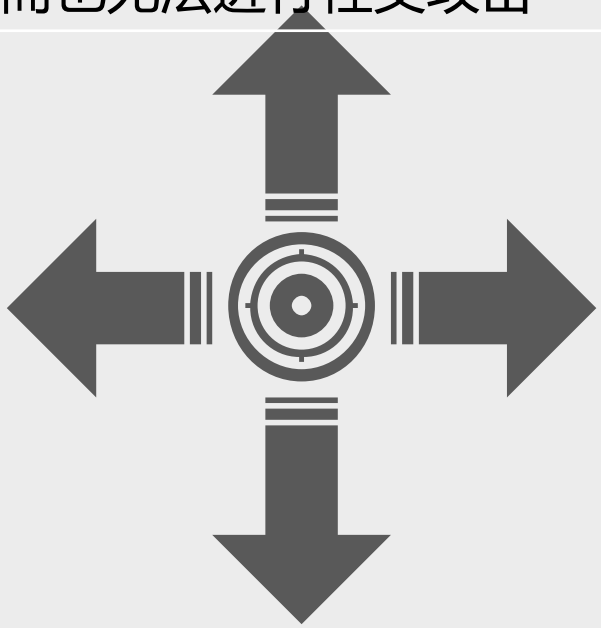
五、安全建议

列出可信设备

对于不可信的设备，不让登录，从而也无法进行社交攻击

失败登陆提示

当有黑客尝试登录，失败时给原用户发送警告通知



取消姓名提示

在社交认证过程中，会有7张照片和6个可选的姓名提示，建议不给姓名提示。

将照片换为图片

照片可以识别人脸，从而可以用机器提取特征从而识别，如果换为人们熟知的图片，机器没法识别特征，而人可以。

总结

- 在本文中，我们分析了Facebook的社交认证存在的问题
- 进行了相应的攻击实验，从攻击的效果来看，Facebook需要重新考虑社交认证的策略
- 针对Facebook社交认证的问题，提出了一些改进建议


谢谢大家！