2018年10月30日星期二

下午11时31分

在进行了三个基本的实验后，发现自己的假设与CERT数据集并不符合，因此需要重新考虑问题与假设。

自己重新仔细阅读了数据构造的相关论文，发现了其逻辑关系中用户的人格特征与组织结构共同结合影响了用户的人际关系（Relationship），而与被解雇用户的人际关系进一步影响了用户的工作满意度（Job Satisfactory），从而导致用户高倾向的不守时以及跳槽。

我们的目的就是尽量全面、准确地刻画出用户的JS变量，从而事先选定可疑的内部用户。

我们的研究方法是从现实场景假设出发，提出假设模型，然后在数据实验中进行修补。

从本实验开始，关于同一个主题的多个实验以数字进行标识版本，如之前的不同方法与模型分别被标识为【0.1~0.3】，本版本0.4中的多个变体则使用0.4X的形式进一步区分。

实验研究除了验证模型假设，解决问题之外，还要训练自己分析问题、提出假设、验证假设、修改假设的研究能力，这才是“金钥匙”。

1. 我们的假设

依据自己的工作经验分析，既然JS假设受影响于解雇用户的人际关系，那么刻画一个内部用户的人际关系便是首要的问题，摆在我们面前的是三个具体的问题：

1. 给定用户的LDAP、Psychometric以及Email通信统计信息，如何初步建模用户的人际关系？
2. 初步建模出用户的人际关系（即认识、接触的用户范围后），如何进一步明确不同人际联系的重要性？
3. 依据上述人际关系范围与联结重要性的研究分析，如何进一步刻画解雇用户对个体的JS影响？

为了回答上述问题，我们试着进行做出假设，并通过实验验证。

* 假设一
* 与解雇用户的人际关系影响着个体的JS；
* 人际关系（Relationship, RS）可以从两个方面刻画：

1. 反映在组织结构（Organizational Structure, OS），决定了用户日常工作所自然接触的人际范围；我们自然地分析上下结构（领导上下级关系）以及横向关系（同一个最小组织单位内以及第一个父单位下的兄弟组织人员范围），其中横向关系对于CERT5.2而言就是Team以及同一个Department下的不同Teams；
2. 反映在通讯关系（Email Relationship, ER），决定了用户日常交流的人际范围与频度，其中可以使用0.2实验中的邮件分析方法，从信息量的7元特征来进行刻画频度，并将邮件联系人补充到人际关系图中；

* 最终得到了用户的人际关系图（Relationship Graph, RG），该图中节点标识用户ID以及对应的Big5人格特质；边上存在使用四位编码标识OS位置距离的无向边，以及一条标识邮件通讯信息量的有向边；
* 一般而言，计算RG中单独一条联结的重要性，可以依据下述建议的公式：



* 计算用户的JS\_Risk则可以将解雇用户所在边的重要性相加，作为该用户的JS\_Risk

——————————————————————————————————————————————————————————————————————————————

2018年10月31日星期三

上午9时48分

实验4.1

为了进一步认识分析攻击者邮件通讯联系人与离职用户以及OS的关联，进行本实验

本实验选取分别选取三个用户进行分析：

1. BYO1846，一般意义的场景二攻击用户；
2. AAG1136，一个未跳槽的CERT5.2用户；
3. CKP0630，一个通讯Leave特征不明显的场景二攻击用户；

重点分析上述三个用户的邮件联系人的OS分布以及与Leave用户的交叉匹配结果

1. 首先我们考虑了邮件发送与接收时存在多个联系人的情况，比如以用户A的邮件分析为例，如果send邮件，则重新多次统计其发送给的多个邮件联系人；如果receive邮件，则重新多次统计其邮件来自的多个邮件联系人；

根据实验显示，就简单分析BYO1846而言，如果不考虑群发，有联系人426，而如果考虑群发邮件，则有联系人951~

接下来，进行两个统计分析，一个是两种情况下邮件联系人与离职人员匹配的个数；一个则是邮件联系人的OS集合以及相关的通信联系人个数；

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3 | 1 | 0 | 3 | 4 |
| 3 | 4 | 1 | 7 | 23 |

BYO1846 Leave Contacts 匹配结果。。。 V2

**0 3**

TRC1838

FDS1841

RMB1821

**1 1**

KBC1390

**2 0**

**3 3**

BRM0126

OJC0930

HXP0976

**4 4**

ZVW1475

TCP0380

RPJ1159

DTB0722

BYO1846 Leave Contacts 匹配结果。。。 V4

**0 3**

TRC1838

FDS1841

RMB1821

**1 4**

VCF1602

KBC1390

CTT0639

HIS1394

**2 1**

ZHB1104

**3 7**

LLW0179

BRM0126

OJC0930

XMG1579

HBH0111

HXP0976

EAL1813

**4 23**

WHG1669

ZVW1475

TCP0380

EPG1196

SMS0432

KVF1143

LMW0837

ICB1890

SAF1942

RPJ1159

FKS1696

DTB0722

ILG0879

STH0353

KJG1121

UKM0845

ESP1198

JSB0860

BRG0728

ZJN1492

CHP1711

ACA1126

SCI0778