基于大数据的社工信息收集与分类攻击

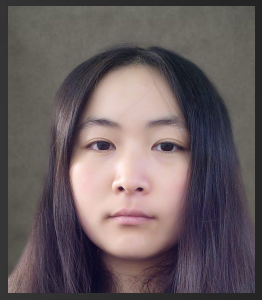
Heng

QCon, Shanghai
Oct, 2015

目录

个人简介及声明

软件工程专业，高级研究员，某知名攻防对抗平台建设者之一，曾任项目开发及专业文献翻译等工作。
DEFCON 23 议题《Classify Targets to Make Social Engineering Easier to Achieve》作者
*此次分享的内容与工作无关



这次演讲将会提到一些国内安全公司普遍忽略、尚未能够做出完善防御对策的问题，目的是提前警示并让人们提高防范意识免于被攻击而不是用于攻击，在此项研究中并未有人被用于过测试，描述倾向于攻击者立场，不应被用于非法目的。

定义

1. 社会工程学

以前：输入姓名查询身份证号码和开房记录，对已泄露数据库的内容检索，衍生出的有大数据口令猜解，撞库，钓鱼邮件，诈骗电话骚扰短信。
现在：基于大数据开发功能各异的软件实施钓鱼、网站伪造、数据收集、人物画像并分不同人群、年龄、性别在指定时间点实施更高成功率的犯罪。

2. 社会工程学方向的大数据

收集人们平时忽略掉的、不知道能被恶意利用的信息，按照一些规则筛选、分类、建模，借鉴前人对于某些问题都做了哪些尝试，做到什么程度，提供对未来的借鉴意义，预测发展趋势，先攻击者一步甚至几步地制定防御对策。

概况

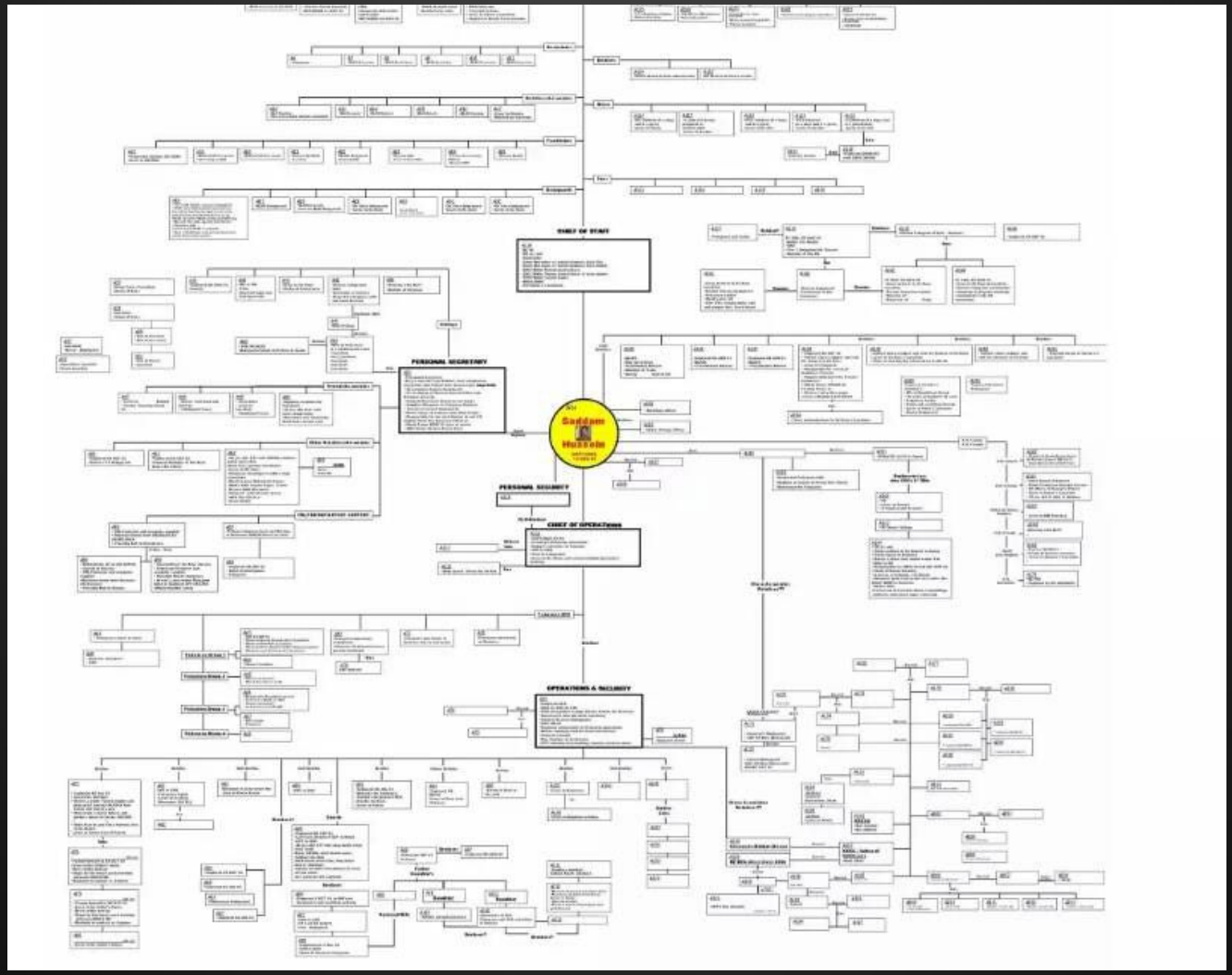
1. 国外现状分析

各种社会工程学会议、软件、整合进其他工具中的模块、比赛
做成产品出售、部分国家倾向于在编程实现上的深入研究
涉及面广、结合各种技术手段、向按照不同方法分类提高成功率的
更为精确的大规模攻击发展
建立在整个社会大部分人是不说谎不欺骗的基础上

2. 国内现状分析

局限性较大
建立在陌生人默认不可信的基础上

模型



信息泄露

1. 未被意识到的信息泄露
2. 对收集到数据的利用

分类举例

1. 基于时间
2. 基于性别
3. 基于年龄

小兔项链的故事

关闭状态

打开状态

定义

1. 社会工程学

以前：输入姓名查询身份证号码和开房记录，对已泄露数据库的内容检索，衍生出的有大数据口令猜解，撞库，钓鱼邮件，诈骗电话骚扰短信。
现在：基于大数据开发功能各异的软件实施钓鱼、网站伪造、数据收集、人物画像并分不同人群、年龄、性别在指定时间点实施更高成功率的犯罪。

2. 社会工程学方向的大数据

收集人们平时忽略掉的、不知道能被恶意利用的信息，按照一些规则筛选、分类、建模，借鉴前人对于某些问题都做了哪些尝试，做到什么程度，提供对未来的借鉴意义，预测发展趋势，先攻击者一步甚至几步地制定防御对策。

总结和问答