北京理工大學
BEIJING INSTITUTE OF TECHNOLOGY

社工库与人肉搜索

28组 宋文强 张景轩 高炳元 李安丰 商郭月

北京理工大學
BEIJING INSTITUTE OF TECHNOLOGY

社工 / Social Engineering

01 相关定义

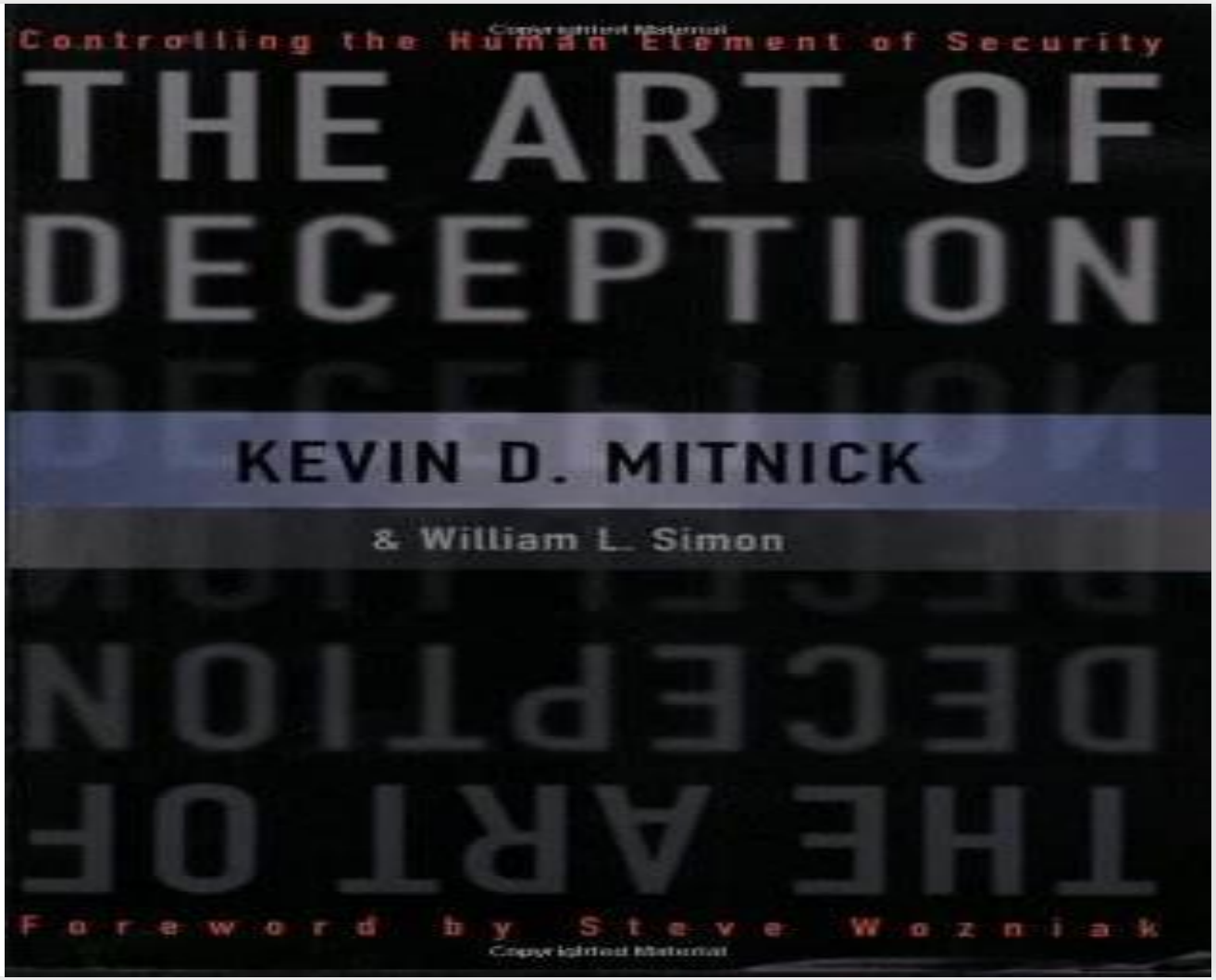
02 攻击模型

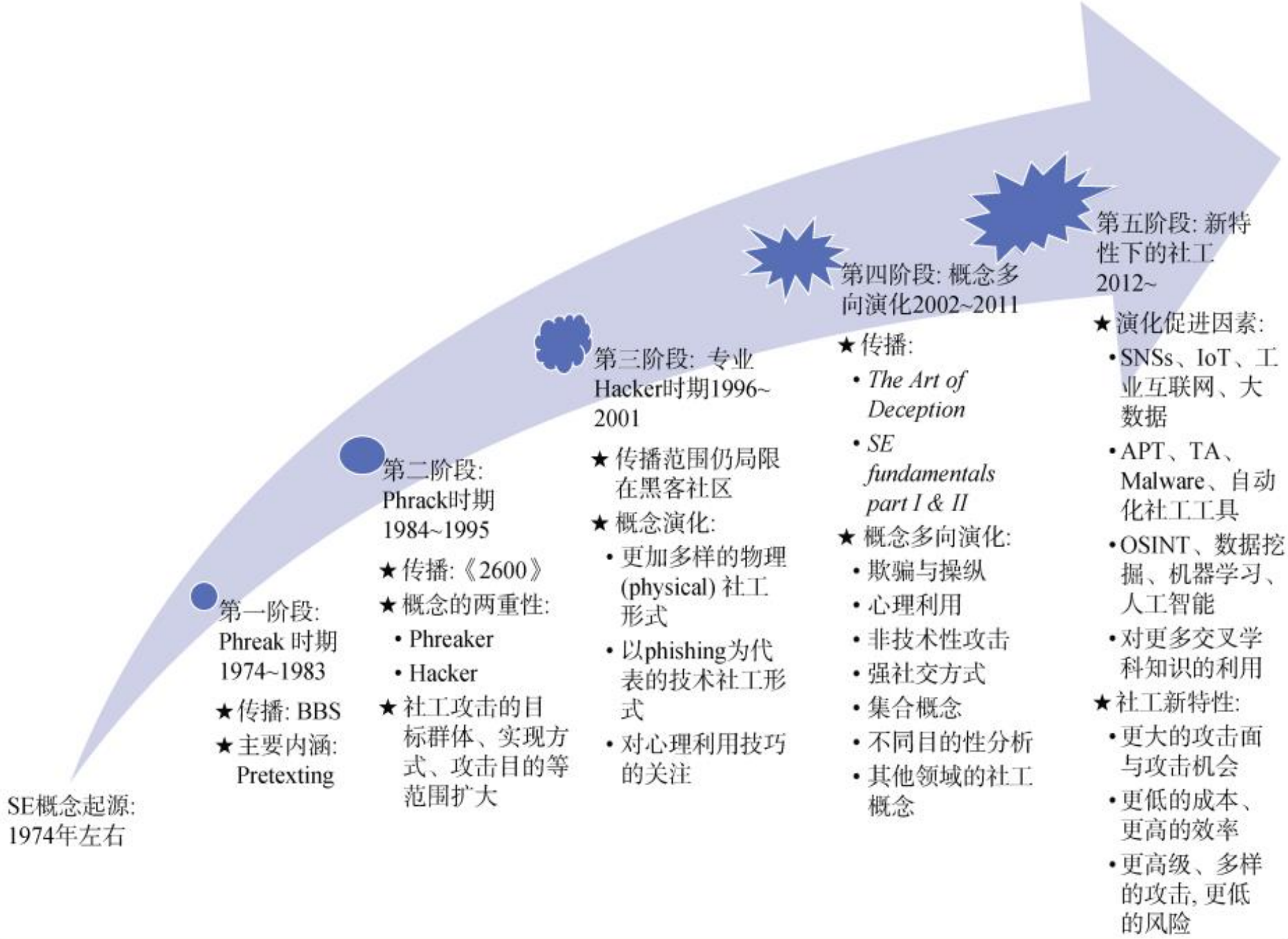
03 攻击形式

04 防御措施

了解途径

著名黑客凯文·米特尼克于2002年推出的一本关于社会工程学的公益性质的畅销书，英文名为《The Art of Deception》。




SE概念起源:
1974年左右
第一阶段:
Phreak 时期
1974~1983
★传播: BBS
★主要内涵:
Pretexting
第二阶段:
Phrack时期
1984~1995
★传播:《2600》
★概念的两重性:
• Phreaker
• Hacker
★社工攻击的目标群体、实现方式、攻击目的等范围扩大
第三阶段: 专业Hacker时期1996~2001
★传播范围仍局限在黑客社区
★概念演化:
• 更加多样的物理(physical) 社工形式
• 以phishing为代表的技术社工形式
• 对心理利用技巧的关注
第四阶段: 概念多向演化2002~2011
★传播:
• The Art of Deception
• SE fundamentals part I & II
★概念多向演化:
• 欺骗与操纵
• 心理利用
• 非技术性攻击
• 强社交方式
• 集合概念
• 不同目的性分析
• 其他领域的社工概念
第五阶段: 新特性下的社工
2012~
★演化促进因素:
• SNSs、IoT、工业互联网、大数据
• APT、TA、Malware、自动化社工工具
• OSINT、数据挖掘、机器学习、人工智能
• 对更多交叉学科知识的利用
★社工新特性:
• 更大的攻击面与攻击机会
• 更低的成本、更高的效率
• 更高级、多样的攻击, 更低的风险

北京理工大學
BEIJING INSTITUTE OF TECHNOLOGY

PART ONE

社会工程学相关定义

社科领域

解决社会问题的工程技术,是改造社会、建设社会和管理社会的科学体系,如降低社会运行成本、规范社会活动、提高工作效率、控制社会发展风险,并对社会的发展进行预测、规划、设计和评估。

网安领域

通过自然的、社会的和制度上的途径，利用人的心理弱点（本能反应、好奇心、信任、贪婪）以及规则上的漏洞，在攻击者和被攻击者间建立起信任关系，获得有价值的信息，最后可以通过未经用户授权的路径访问某些**敏感数据**和**隐私数据**。

维基：操纵他人采取特定行动或泄露机密信息的行为

社科领域

社会工作者(Social Worker),有时也简称“社工”,是指在社会福利、社会救助、社会慈善、残障康复、优抚安置、医疗卫生、青少年服务、司法矫治等**社会服务机构**中从事社会服务工作的专业技术人员。

网安领域

社工师（Social Engineer），实施**社工攻击**的攻击者。

“社工库”

拖库：本来是数据库领域的术语，指从数据库中导出数据。后被用来指不法黑客入侵有价值的网络站点，把注册用户的资料数据库全部盗走的行为。**盗走注册用户资料数据**

洗库：在取得大量的用户数据之后，黑客会通过一系列的技术手段和黑色产业链将有价值的**用户数据变现**，这通常也被称作“洗库”。

撞库：黑客将得到的数据在其它网站上进行**尝试登陆**，叫做”撞库“，因为很多用户喜欢使用统一的用户名密码，”撞库“也可以是黑客收获颇丰。

“社工库”

社工库就是一个黑客们将泄漏的用户数据整合分析，然后集中归档的一个地方。这些用户数据大部分来自以前黑客们拖库撞库获得的数据包，包含的数据类型除了账号密码外，还包含被攻击网站所属不同行业所带来的附加数据。

北京理工大學
BEIJING INSTITUTE OF TECHNOLOGY

PART TWO

攻击模型演变

社会工程学攻击模型演变

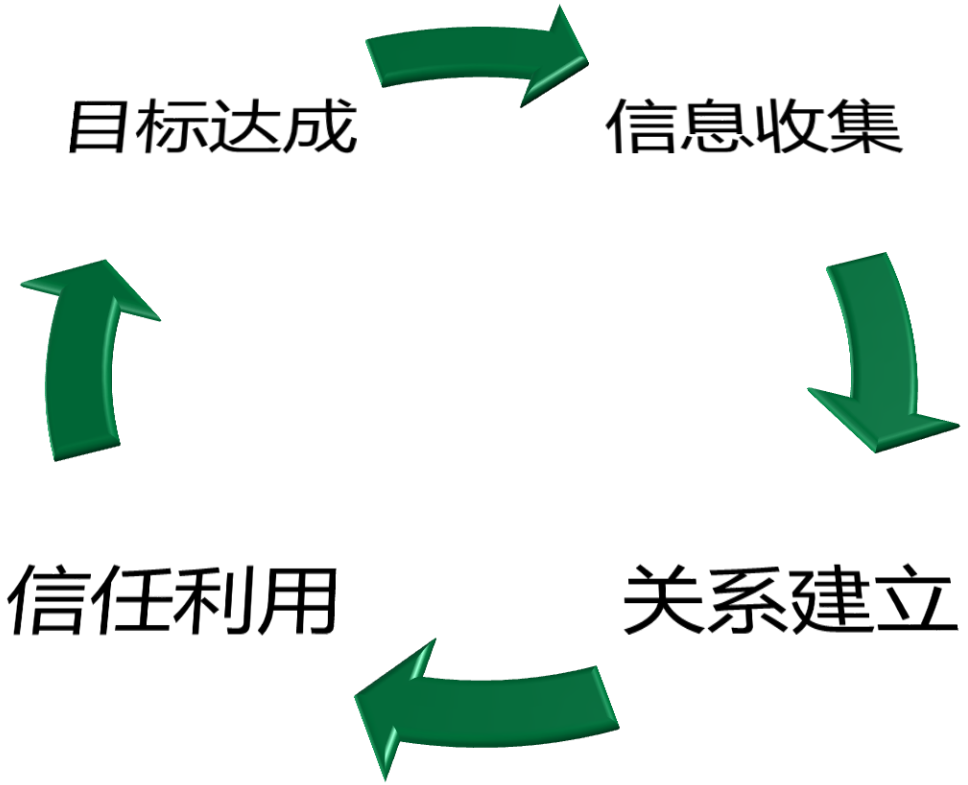
Kevin Mitnick

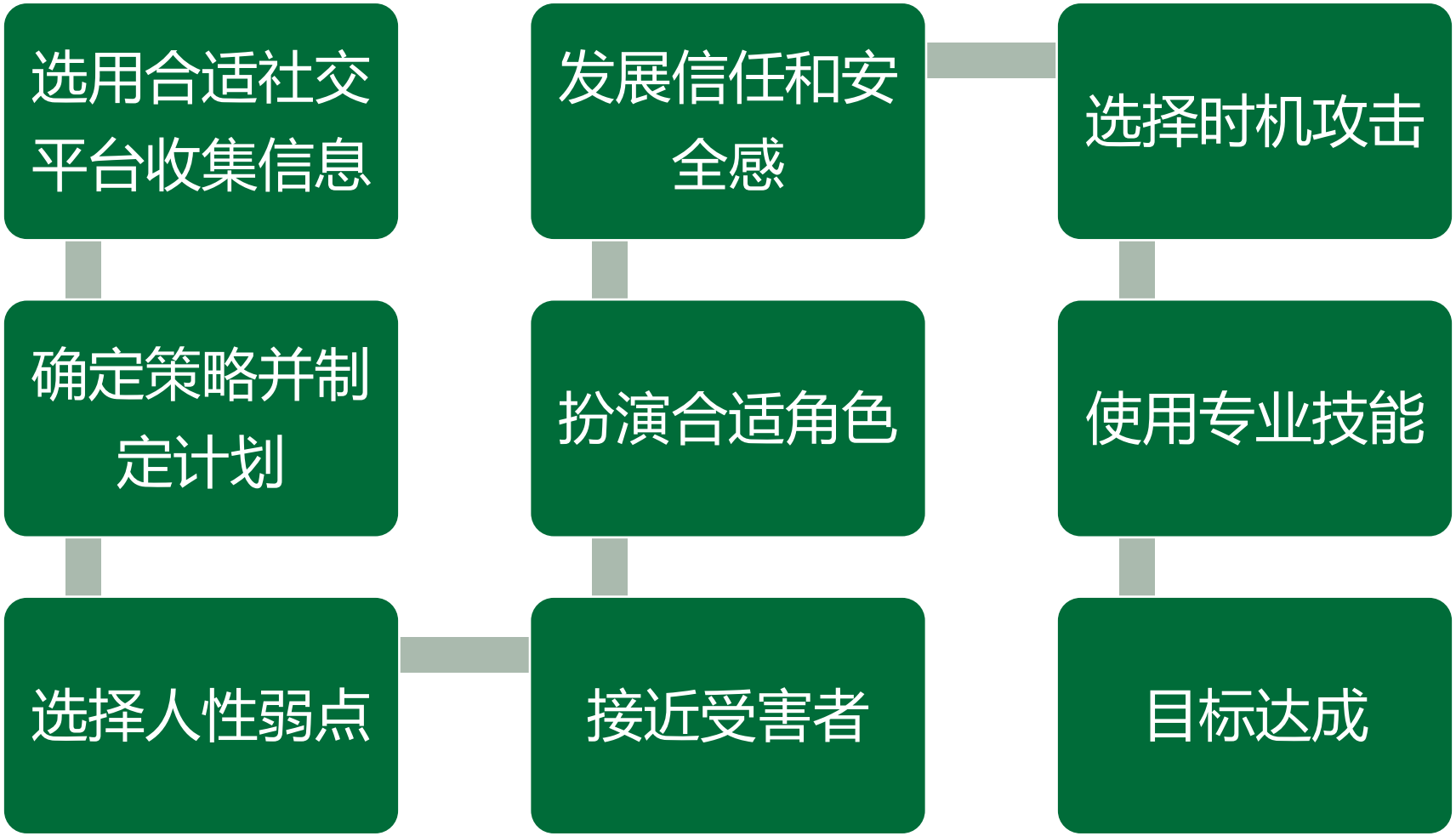
Algarni

Mouton

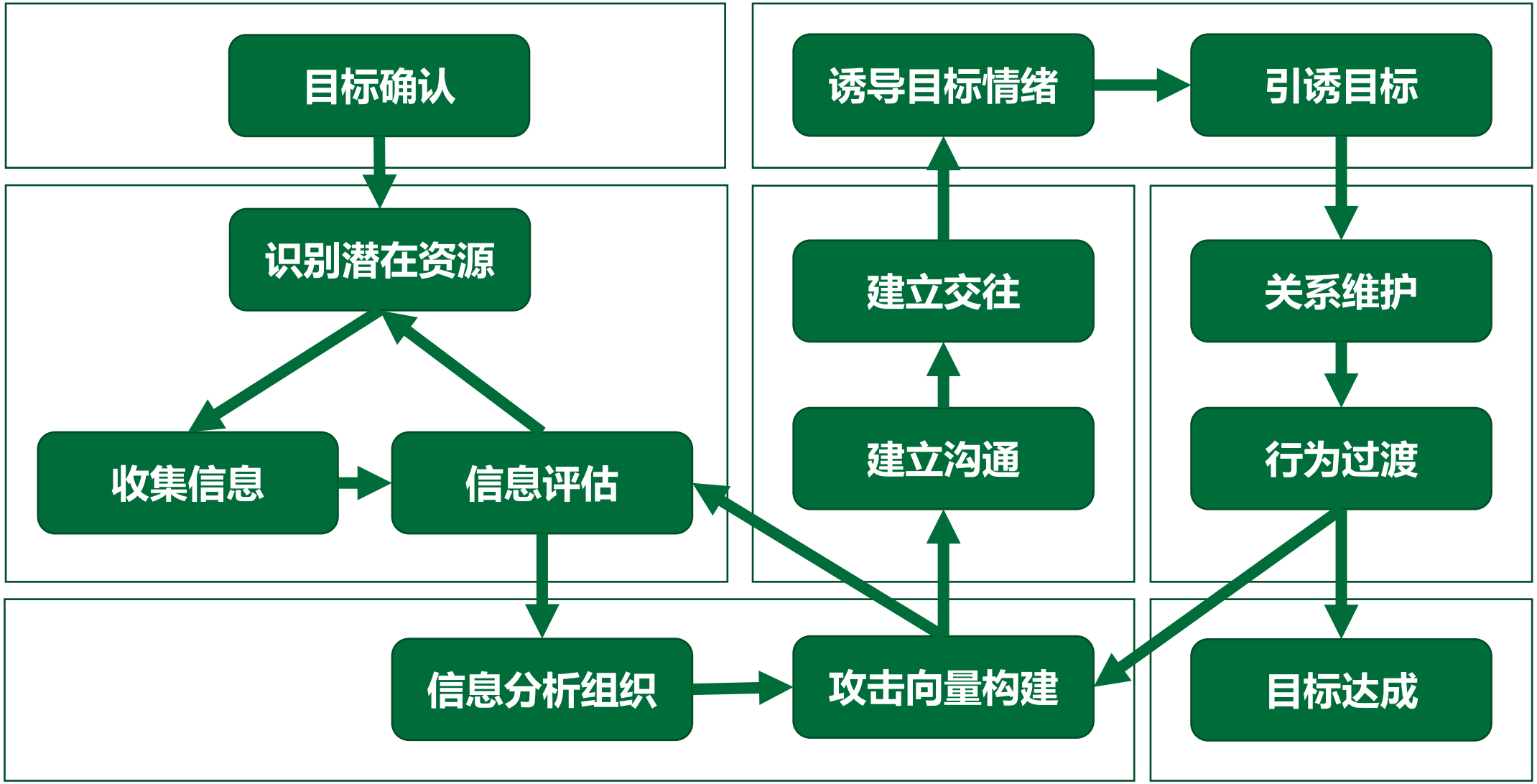
Cullen

Kevin Mitnick

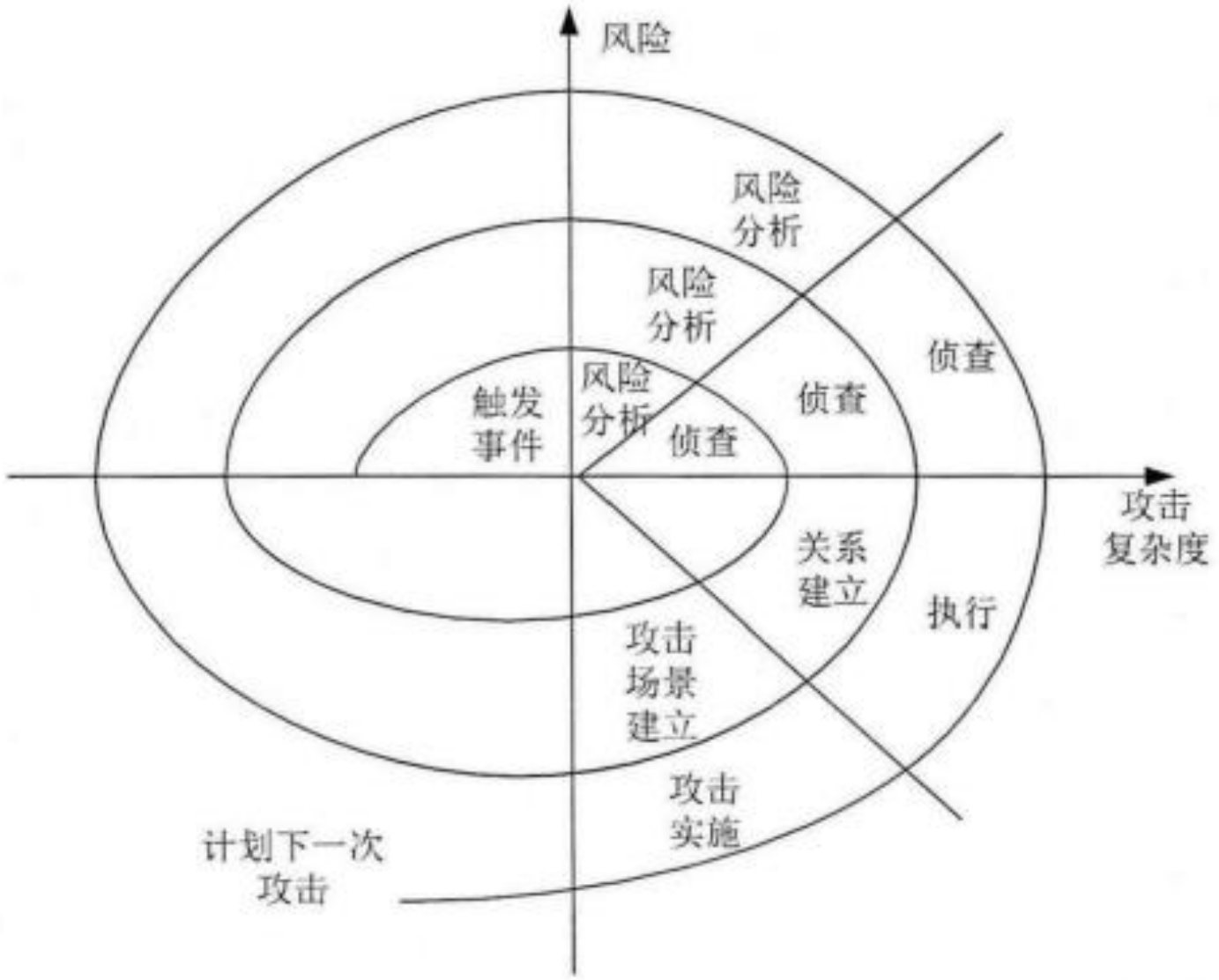



选用合适社交平台收集信息
发展信任和安全感
选择时机攻击
确定策略并制定计划
扮演合适角色
使用专业技能
选择人性弱点
接近受害者
目标达成

Mouton


目标确认
识别潜在资源
收集信息
信息评估
信息分析组织
攻击向量构建
建立沟通
建立交往
诱导目标情绪
引诱目标
关系维护
行为过渡
目标达成

Cullen

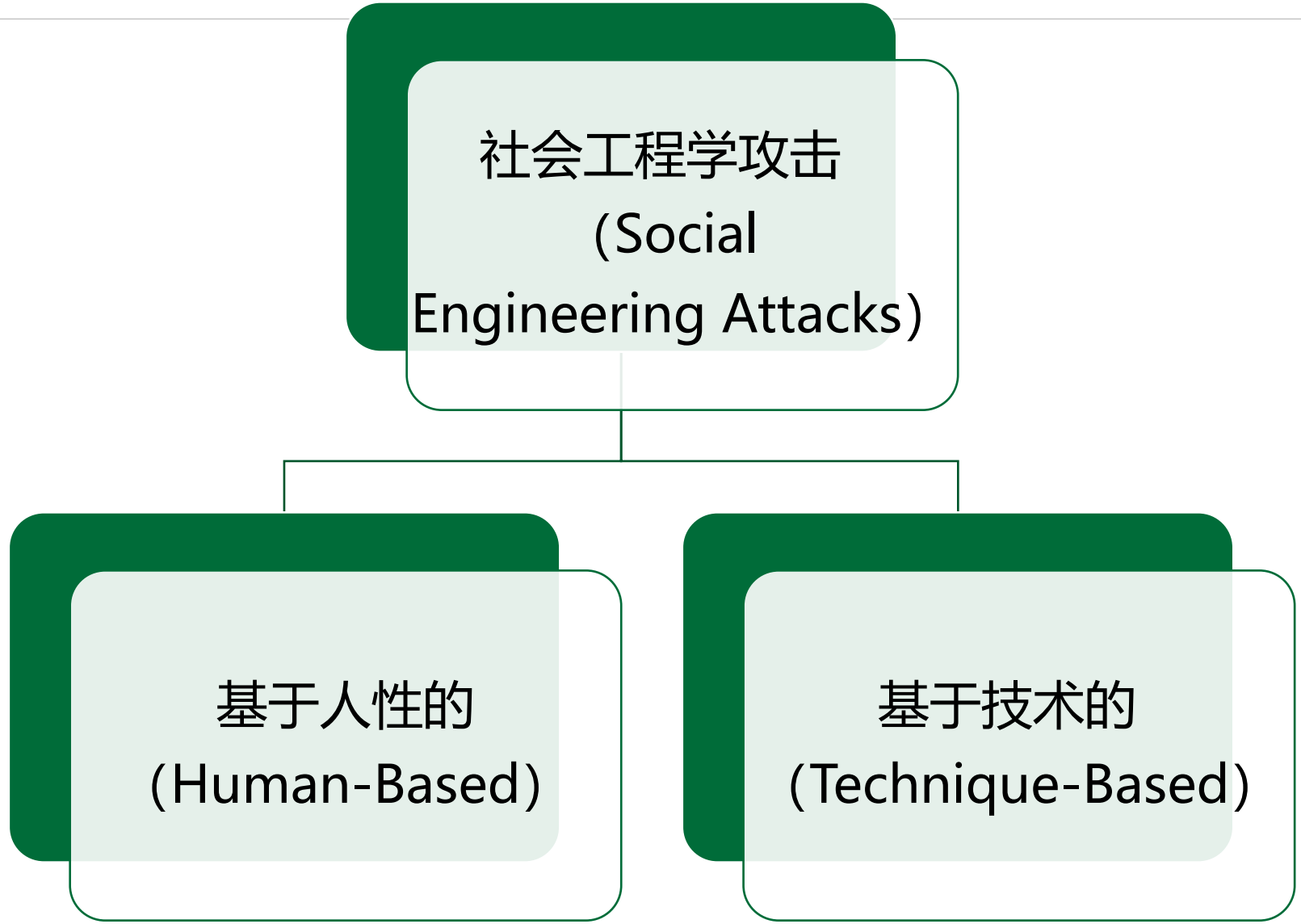

风险
风险分析
风险分析
触发事件
风险分析
侦查
侦查
侦查
攻击复杂度
关系建立
执行
攻击场景建立
攻击实施
计划下一次攻击

北京理工大學
BEIJING INSTITUTE OF TECHNOLOGY

PART THREE

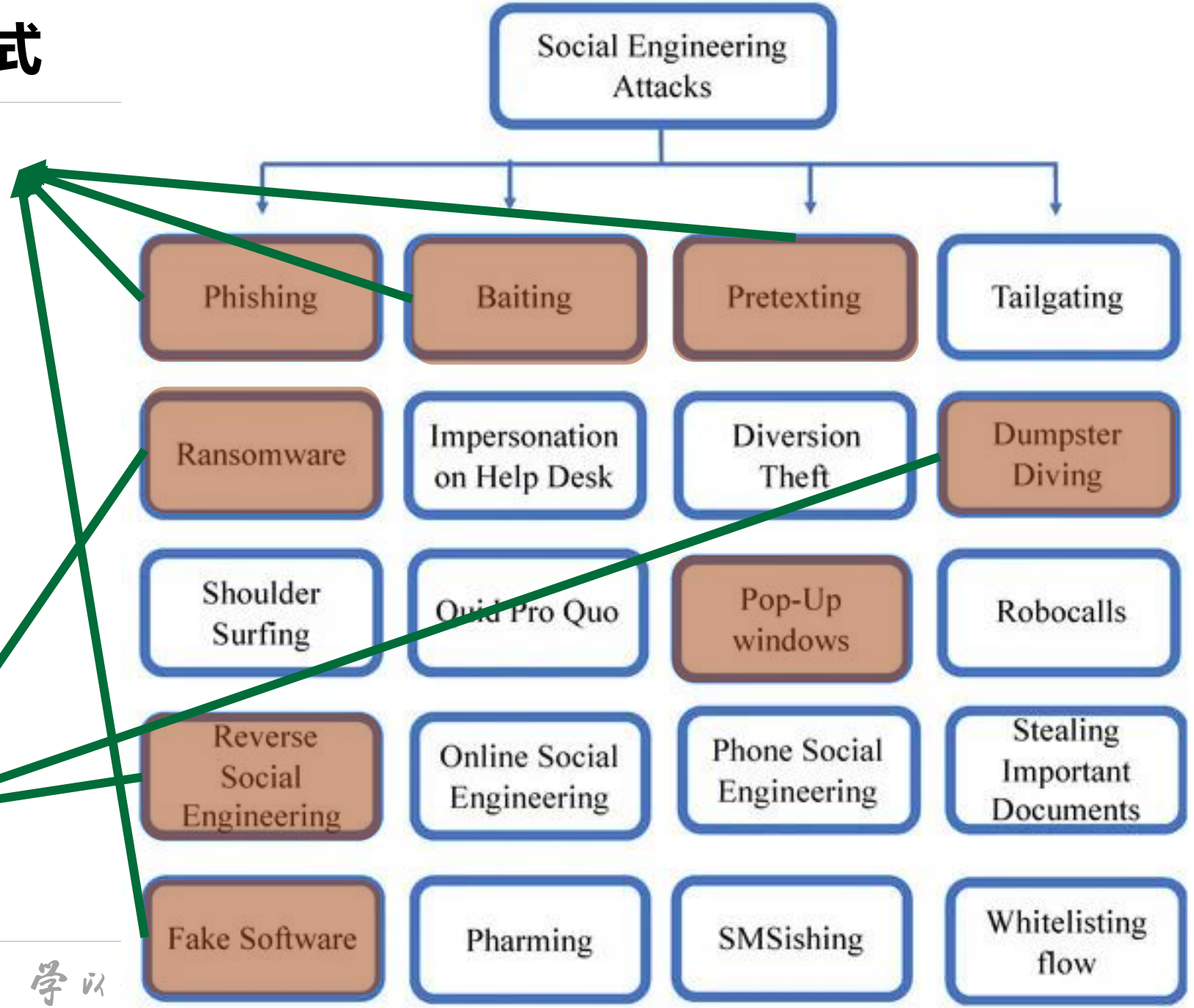
常见攻击形式

拖库三步走


社会工程学攻击
(Social
Engineering Attacks)
基于人性的
(Human-Based)
基于技术的
(Technique-Based)

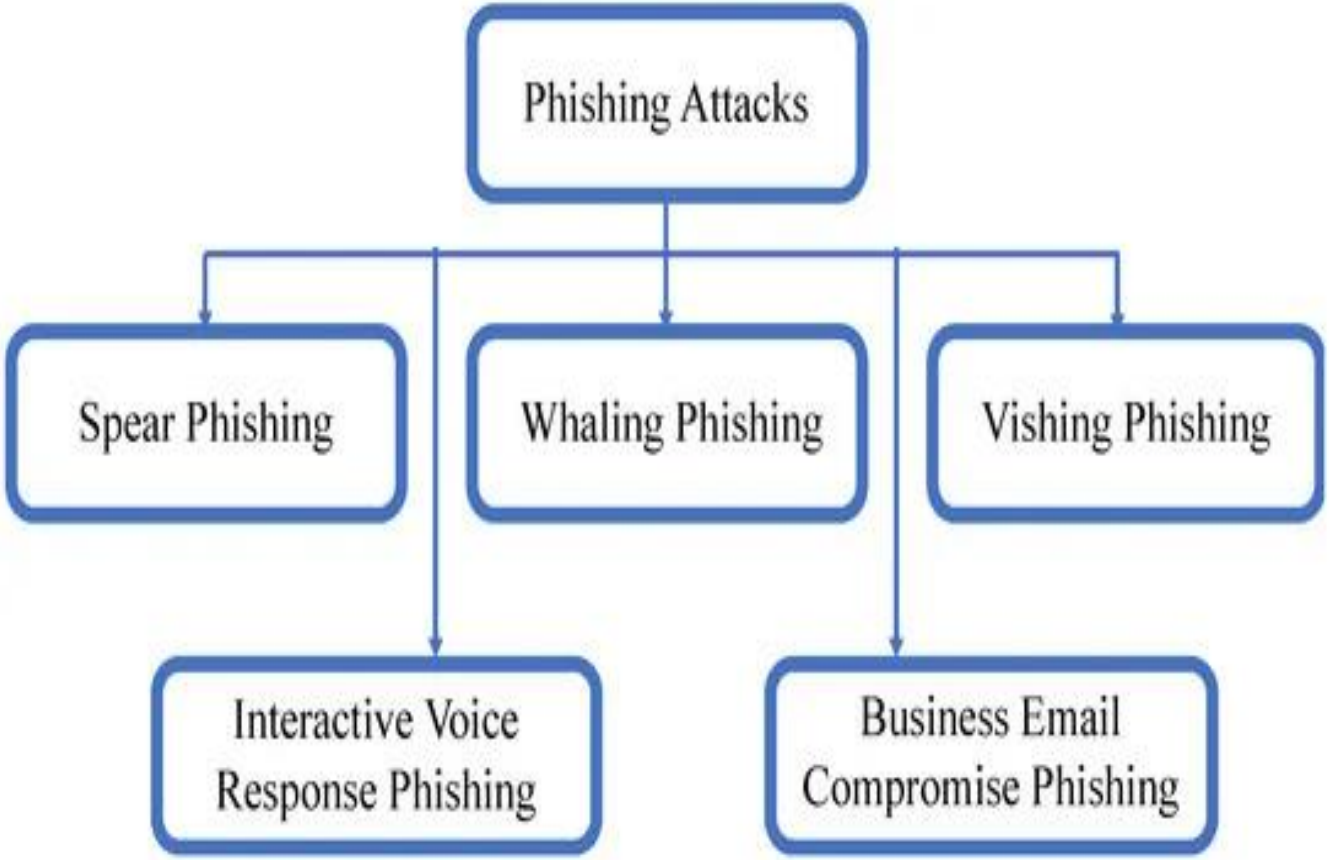
常见形式

Human Based



Technique-Based

Phishing（网络钓鱼）



网络钓鱼是攻击者通过伪造电子邮件和网站，意图引诱被攻击者泄露敏感信息（如口令、账号ID等）的一种攻击方式。

类Phishing

诱饵攻击（Baiting），一种网络钓鱼攻击，邀请用户单击链接以获取免费内容。

https://formcrafts.com/a/23293?preview=true

弹窗（Pop-Up Windows），主要有弹窗广告、虚假警报消息。

Fake Software Attack（假冒软件攻击）

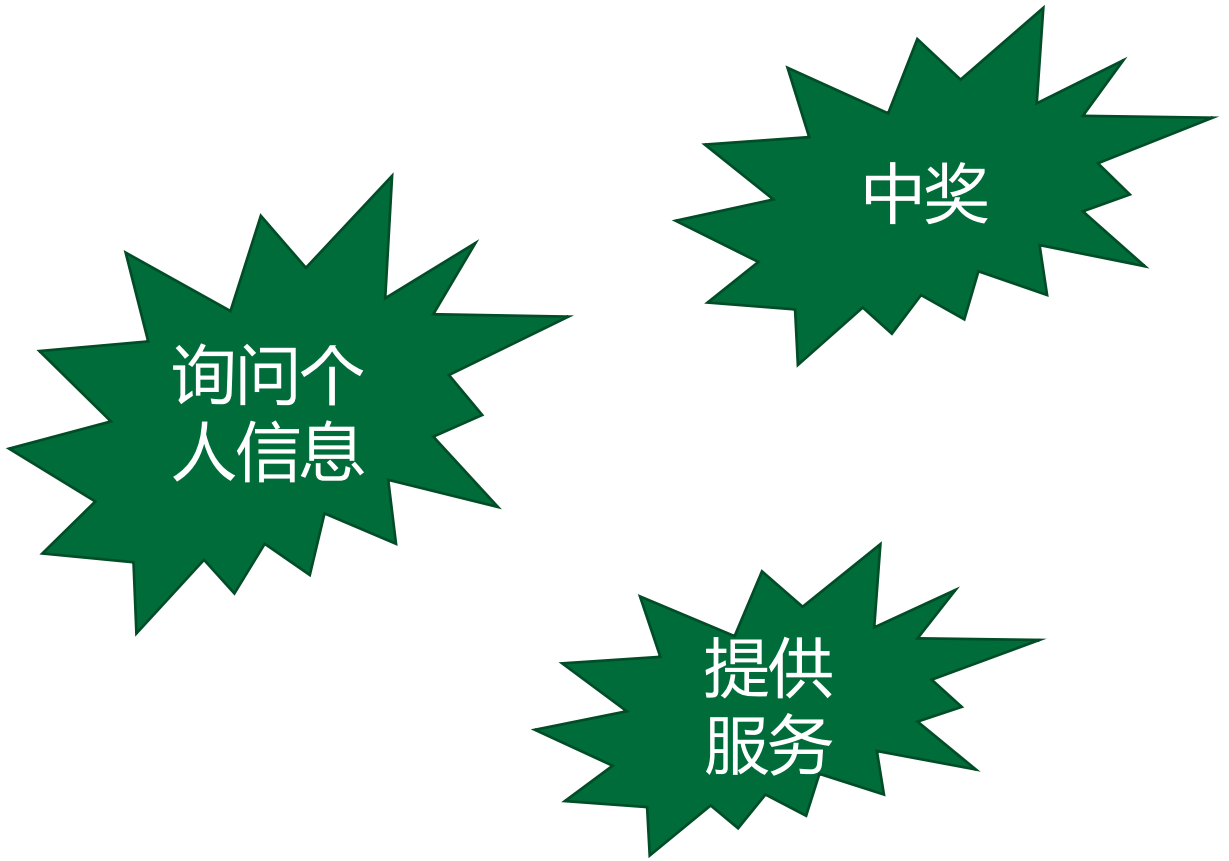
基于假冒网站，让受害者相信他们是已知且受信任的软件或网站。

受害者将真实的登录信息输入到虚假网站中，这使攻击者可以在合法网站上使用受害者的凭据，例如访问在线银行账户。

Pretexting（借口攻击）

利用虚假但令人信服的场景

以窃取受害者的个人信息。



反向社会工程学攻击(Reverse Social Engineering)

攻击者和攻击目标已经建立了联系的基础上，攻击者创造一个攻击目标需要获取帮助的情景，并且通过帮助 攻击目标获取所需的敏感信息 。

Ransomware attack（勒索软件）

勒索软件攻击通过加密来限制和阻止对受害者数据和文件的访问 。

为了恢复这些文件，受害者被威胁要发布它们，除非支付赎金 。

此付款必须使用比特币完成。

Wannacry

北京理工大學
BEIJING INSTITUTE OF TECHNOLOGY

PART FOUR

防御措施

反钓鱼工具

机器学习检测

异常检测（DAS）

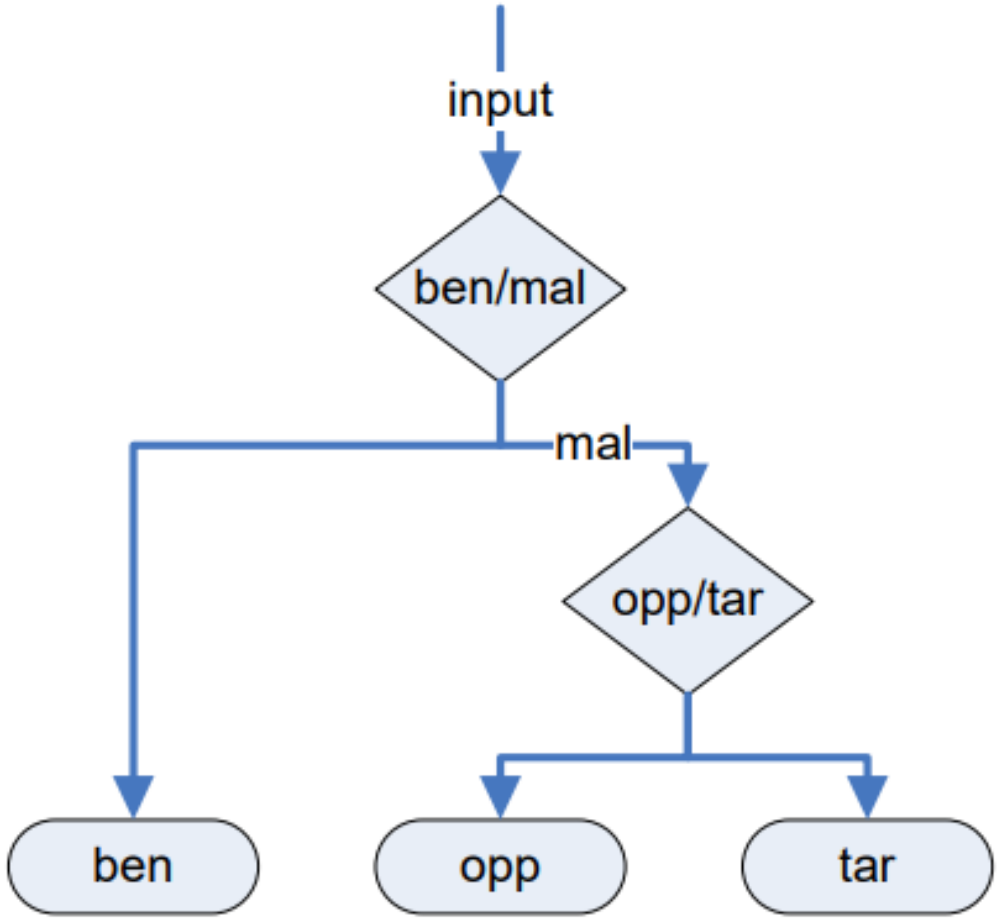
机器学习检测方法

恶意PDF钓鱼

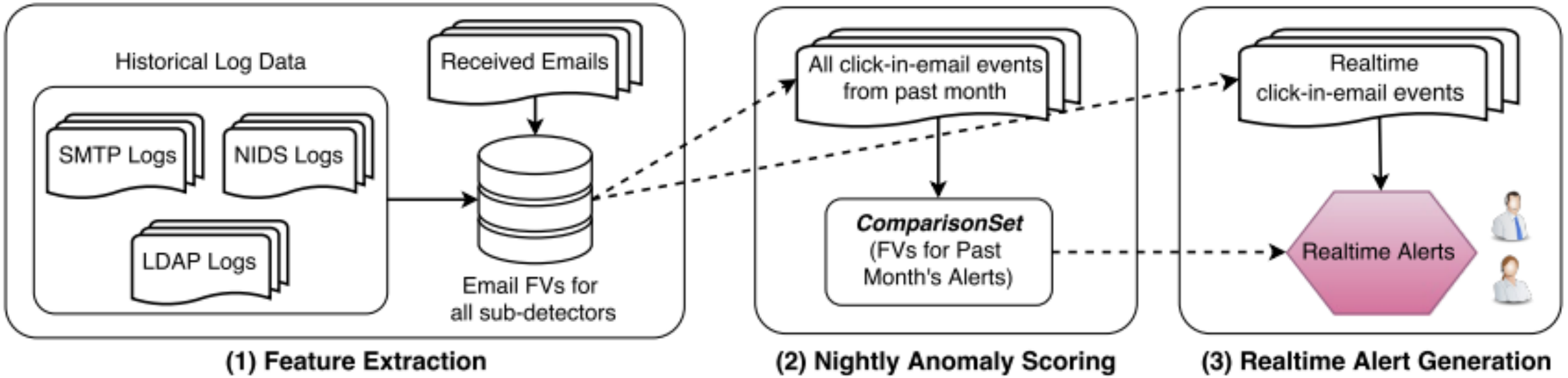
Table 15: Example Structure: Targeted

Location	Content	Description
000000 000020 000040	%PDF-1.5..%.....1 0 obj..<</Pag es 2 0 R /Type/Catalog/OpenActio n 8 0 R >>..endobj..2 0 obj..<</	PDF header and OpenAction object which executes javascript when document is opened
000140 000160	j..4 0 obj..<</Type/Font/BaseFon t/Times-Roman/Subtype/Type1>>..e	Font object: Times Roman.
000180 0001A0 ... 000390	ndobj..5 0 obj.. <</Length 471/Fi lter/FlateDecode >>stream..x.U..n ... .endstream..endobj..6 0 obj<< (Decoded, extracted raw text): Financial Reform Puts Republicans on the Spot (April 26) -- Even as they lost today's Senate vote	Object containing formatted text. The victim never sees this content. This content is not consistent with rest of social engineering used in attack.
0003E0 000400 000420	.endobj..7 0 obj..<</Type/Font/S ubtype/Type1/BaseFont/Helvetica/ Encoding/WinAnsiEncoding>>..endo	Font object: Helvetica.

Name	Description	Name	Description
size	Size of document (bytes)	version	PDF version as extracted from header
count_obj	Count of object markers	count_endobj	Count of end of object markers
count_stream	Count of stream markers	count_endstream	Count of end of stream markers
count_xref	Count of cross reference table markers	count_trailer	Count of trailer markers
count_startxref	Count of cross reference table markers	count_eof	Count of end of file markers
count_page	Count of page markers	count_objstm	Count of object stream markers
count_js	Count of JS object markers	count_javascript	Count of JavaScript object markers
count_action	Count of action (AA and OpenAction) object markers	count_acroform	Count of Acroform object markers
count_font	Count of Font object markers	count_stream_diff	Difference of count_stream and count_endstream
moddate_ts	Modification timestamp (seconds–Unix epoch)	moddate_tz	Modification timezone (seconds–UTC offset)
createdate_ts	Creation timestamp (seconds–Unix epoch)	createdate_tz	Creation timezone (seconds–UTC offset)
createdate_version_ratio	Ratio of creation date to version (days since Jan 1 1993 / version)	moddate_version_ratio	Ratio of modification date to version (days since Jan 1 1993 / version)
createdate_dot	Count of dot characters in creation date	moddate_dot	Count of dot characters in modification date
pdfid0_len	PDFid0: Count of characters	pdfid0_lc	PDFid0: Count of lower case characters
pdfid0_uc	PDFid0: Count of upper case characters	pdfid0_num	PDFid0: Count of numeric characters
pdfid0_oth	PDFid0: Count of other characters	pdfid0_dot	PDFid0: Count of dot characters
pdfid1_len	PDFid1: Count of characters	pdfid1_lc	PDFid1: Count of lower case characters
pdfid1_uc	PDFid1: Count of upper case characters	pdfid1_num	PDFid1: Count of numeric characters
pdfid1_oth	PDFid1: Count of other characters	pdfid1_dot	PDFid1: Count of dot characters
pdfid_mismatch	pdfid0 different from pdfid1 (binary)	title_len	Title: Count of characters
title_lc	Title: Count of lower case characters	title_uc	Title: Count of upper case characters
title_num	Title: Count of numeric characters	title_oth	Title: Count of other characters
title_dot	Title: Count of dot characters	author_len	Author: Count of characters


input
ben/mal
mal
opp/tar
ben
opp
tar

DAS


Historical Log Data
SMTP Logs
NIDS Logs
LDAP Logs
Received Emails
Email FVs for
all sub-detectors
(1) Feature Extraction
All click-in-email events
from past month
ComparisonSet
(FVs for Past
Month's Alerts)
(2) Nightly Anomaly Scoring
Realtime
click-in-email events
Realtime Alerts
(3) Realtime Alert Generation

4 其他预防方法

1. 流式白名单
2. 避免接触有隐患的文件、程序、链接、网络设备
3. 培养预防意识
4. 生物识别
5. 反社会工程学框架

北京理工大學
BEIJING INSTITUTE OF TECHNOLOGY

社工库

01 信息如何泄露

02 信息收集思路

03 几个检测工具

04 防范措施

北京理工大學
BEIJING INSTITUTE OF TECHNOLOGY

PART ONE

信息如何泄露

原因

- 1. 人为倒卖信息，掌握了信息的公司、机构员工主动倒卖信息。
  2. 电脑，手机等设备感染了病毒木马等恶意软件。
  3. 网站漏洞，攻击者利用网站漏洞，入侵了保存信息的数据库。
  4. 手机漏洞。使用了钓鱼Wi-Fi等。

信息泄露

8亿Q绑数据

4亿京东数据

5亿微博数据

北京理工大學
BEIJING INSTITUTE OF TECHNOLOGY

PART TWO

信息收集思路

信息收集思路

被动信息收集：

社交信息：微信、QQ、微博、游戏

职场/院校信息：领英、天眼查；校内新闻、社团；商家信息

敏感信息：姓名

住址

身份证号

(例如京东/淘宝等网站的信息泄露)

信息收集思路

主动信息收集：

手机号查姓名：如支付宝转账，使用银行卡支付能看到对方全名
企业微信实名+单位

Ip地址收集：钓鱼连接、钓鱼文件
产生社交关系套取情报

信息收集思路

北京理工大学 BEIJING INSTITUTE OF TECHNOLOGY

密码获取

QQ邮箱注册网站，网站信息泄露
钓鱼链接

排序	QQ账号	QQ密码
2	10001919	sjejemmnen3

排序	QQ账号	QQ密码
1	1001	146461

重复密码

北京理工大学
BEIJING INSTITUTE OF TECHNOLOGY

PART THREE

几个检测工具

几个检测工具

Q绑搜索


输入QQ号码即可查询密保手机和微博ID
查找
通过手机号反查
加入TG群
密保手机号码
没有找到
号码归属地
没有找到
LOL信息
(恕瑞玛)
微博UID
没有找到

几个检测工具

kallydev的简易社工库

几个检测工具

Github源码GitHub - tap6/socialdb_vue_flask

- Python语言
- 使用数据库MongoDB
- 函数库：pymongo，flask，flask-restful

后端(服务端)

- Python flask编写
- config.py 参数设置
- 泄露的数据
- main_api.py 后端接口
- bigfile_multi_insert.py 读取并写入数据文件
- mongo_client.py 用于管理mongodb数据库

前端(客户端)

- 使用nodejs、vue编写
- 包含网页所需的各种包，package
- 各类config参数
- 预设
- 网页index以共用户使用

数据库查询系统

几个检测工具

后端起了Flask服务器，默认监听5000端口，主要使用Flask Restful API编写，负责处理接口逻辑+数据库操作，其他还有写入数据库操作。在 Person类Get方法中编写get请求业务逻辑

前端只有两个component，search.vue（搜索）和 Analysis.vue（分析）其中search.vue加了级联前端和请求级联数据方法

北京理工大学
BEIJING INSTITUTE OF TECHNOLOGY

PART FOUR

防范措施

防范措施

Firefox monitor

防范措施

使用开源浏览器
关闭手机号搜索等功能
…

当一个人足够无知且无畏时，往往会认为隐私是弱者才需要去保护的累赘。无论是人还是机器，当掌握足够多关于你的数据时，这就不是一件好事。
特别是机器，它能记住的数据远比人们所想象的更多、更久。当收集到的数据达到一定量级时，它可能会比你还了解你自己。

目前想要完全保护自己的隐私，这是很难甚至不可能完成的。

北京理工大學
BEIJING INSTITUTE OF TECHNOLOGY

人肉搜索

01 什么是人肉搜索

02 由来和成因

03 积极与消极

04 常见形式

北京理工大學
BEIJING INSTITUTE OF TECHNOLOGY

PART ONE

什么是人肉搜索

人肉搜索的由来

人肉搜索就是应用人工参与方式，利用网络这个拟空间聚集不同阶层，不同知识背景的人替代“机器搜索引擎”。

什么是人肉搜索

北京理工大学 BEIJING INSTITUTE OF TECHNOLOGY

广义

特点：利用现代信息技术

狭义

特点：是将谷歌、百度等网络搜索引擎与人工搜索相结合。

北京理工大学
BEIJING INSTITUTE OF TECHNOLOGY

PART TWO

由来和成因

人肉搜索的成因

群体的感染

促进了“人肉搜索”的产生

感染理论认为集合行为是人们情绪感染的结果

匿名性

在线交流的匿名性为“人肉搜索”的产生提供了土壤

北京理工大学
BEIJING INSTITUTE OF TECHNOLOGY

PART THREE

积极与消极

人肉搜索的积极与消极

积极作用

维护社会的公平正义许多人肉搜索事件证明，人肉搜索在客观上维护了社会的公平正义

消极影响

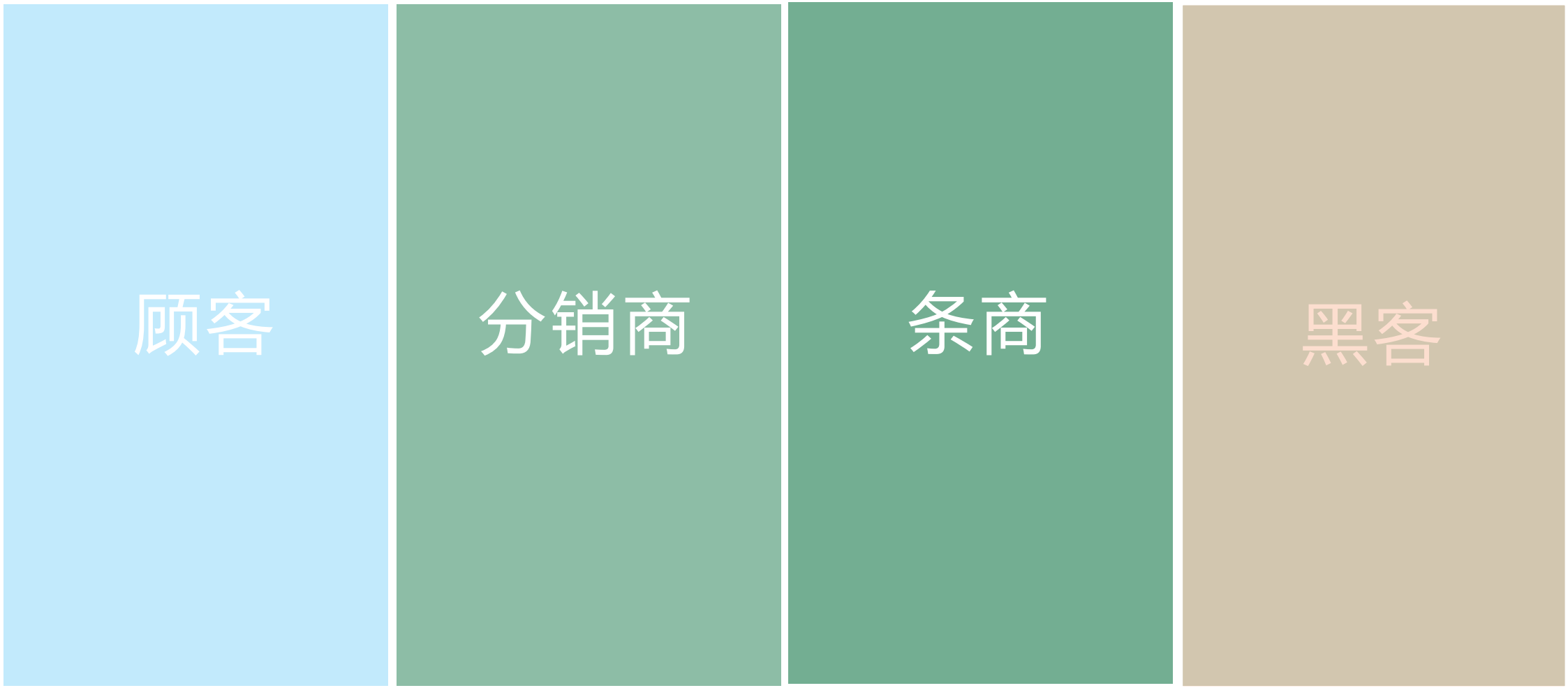
侵犯他人的隐私权

北京理工大學
BEIJING INSTITUTE OF TECHNOLOGY

PART FOUR

常见形式

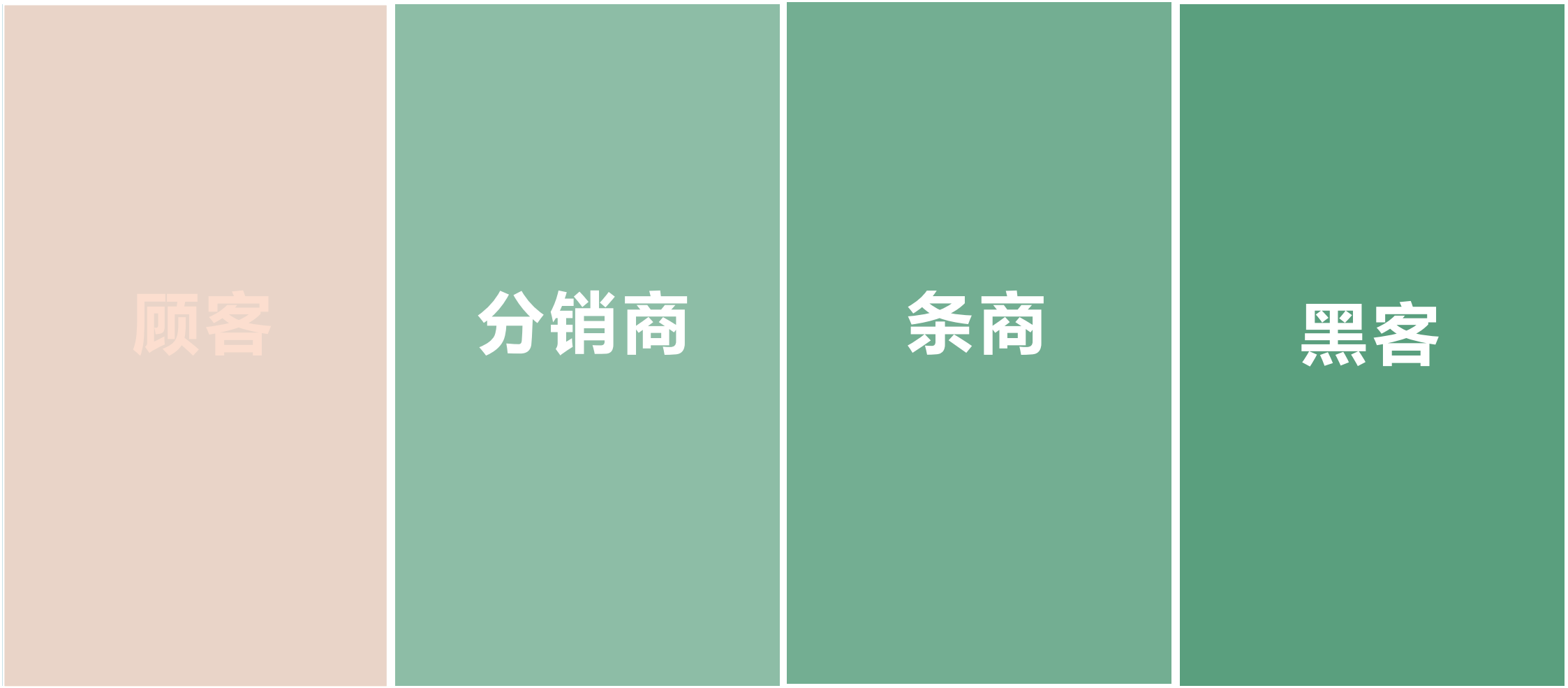
人肉搜索常见形式



人肉搜索常见形式

人肉搜索常见形式

人肉搜索常见形式



北京理工大學
BEIJING INSTITUTE OF TECHNOLOGY

人肉搜索 / Cyber Manhunt

01 基本概念

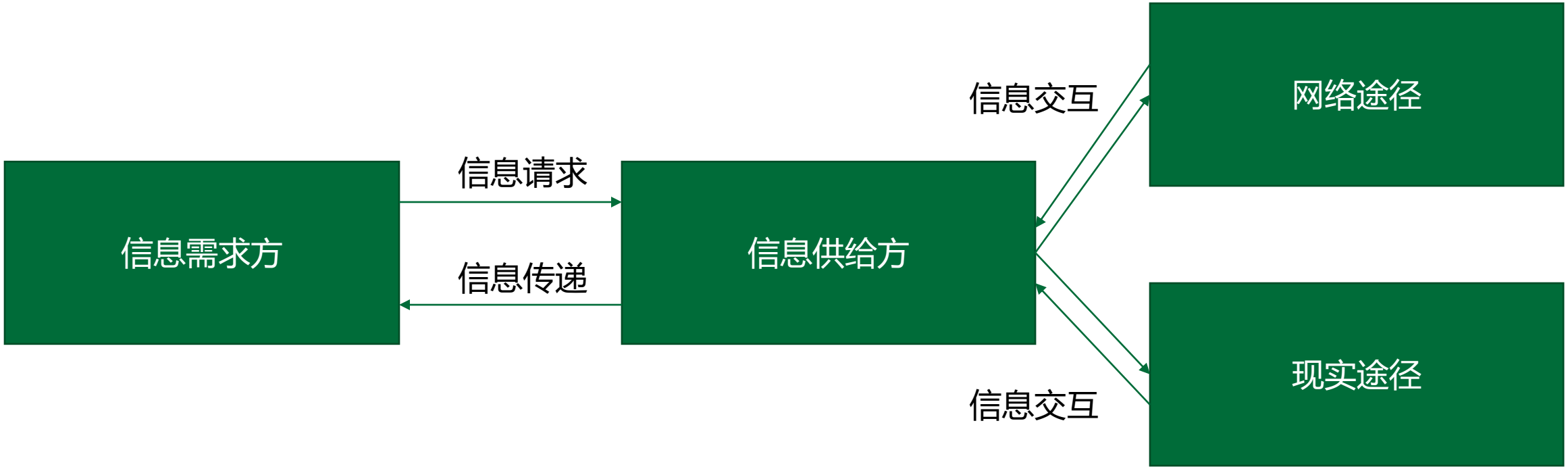
02 方式与原理

03 防御措施

人肉搜索是近年来兴起的一种信息和知识搜索工具，是利用现代信息科技，变传统的计算机网络信息搜索为人际关系型网络社区信息求助和信息帮助活动。

其本质是利用网 络让更多人参与信息共享，并对共享信息加以辨析 和提纯信息的一种方式和机制。

基本概念



基于搜索对象的分类：
1.针对知识的搜索——主要应用
2.针对某种事件及其特定主体信息的搜索——前景广阔

针对知识的搜索作为人肉搜索传统应用也是规模最大的应用已经有多年实践，事实上，包括百度知道，知乎，谷歌等搜索工具都提供了相关功能。

方式与原理

虚拟世界

现实世界

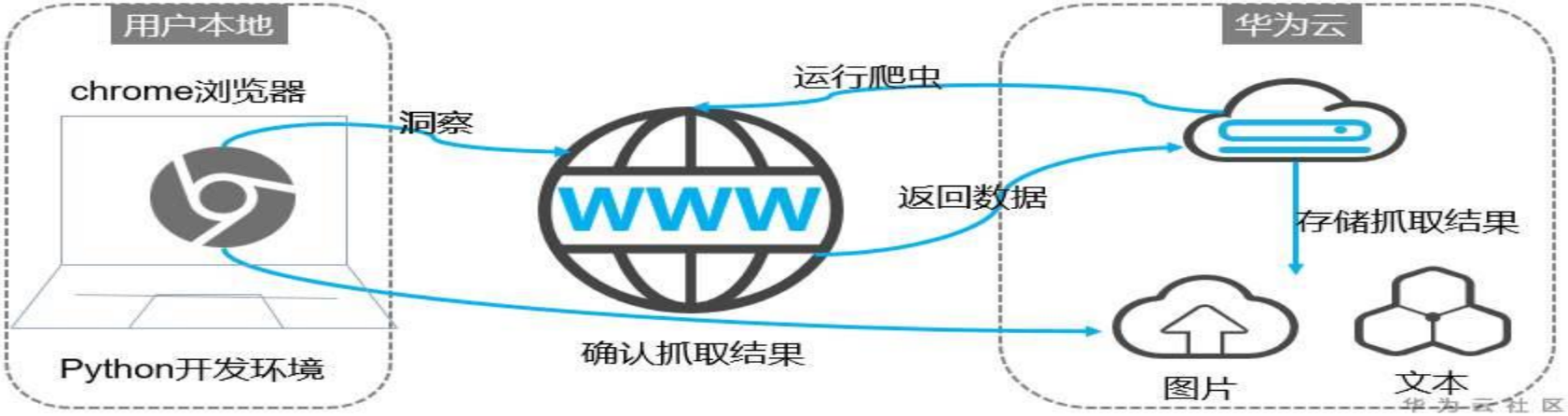
总体来说，综合虚拟世界和现实世界信息共享发力是人肉搜索发挥作用的基本原理。

方式与原理

1.搜索引擎（1）百度知道 (http://zhidao.baidu.com)
(2) Google问答 (http://wenda.tianya.cn)
(3) 新浪爱问 (http://iask.sina.com.cn)
(4) 腾讯搜搜问问 (http://wenwen.soso.com)
(5) 雅虎知识堂 (http://ks.cn.yahoo.com)
(6) 奇虎经验搜索 (http://jingyan.qihoo.com)
利用搜索引擎强大的搜索能力，通过调整关键词等方式多次访问，查找信息。

方式与原理

搜索引擎核心技术框架：
1.爬虫技术：搜索引擎通过互联网一些公开知名的网站，抓取内容，并分析其中的链接，然后有选择的抓取链接里的内容，然后再分析其中的链接，以此类推，通过有限的入口，基于彼此链接，形成强大的信息抓取能力。搜索引擎算法试图抓取并存储互联网网页信息时，可能需要访问网页的允许。
2.索引技术：要想让用户快速的通过关键词搜索到这个网页，就必须对网页做关键词的索引，从而提升查询效率，简单说就是，把网页的每个关键词提取出来，并针对这些关键词在网页中的出现频率，位置，特殊标记等诸多因素，给予不同的权值标定，然后，存储到索引库中。具体要点有分词，实时索引，权值排名等



方式与原理

搜索引擎核心技术框架：
3.查询显示技术：第一步，会检查最近时间有没有人搜索过同样的关键词，如果存在这样的缓存，最快的处理是将这块缓存提供给你，这样查询效率最高，对后端负载压力最低。
第二步，发现这个输入查询最近没有搜索，或者有其他条件的原因必须更新结果，那么会将这个用户输入的词，进行分词，没错，如果不止一个关键词，或者是一句话的情况下，应答程序会又一次分词，将搜索的查询拆成几个不同的关键词。
第三步，将切分后的关键词分发到查询系统中，查询系统会去索引库查询，索引库是个庞大的分布式系统，先分析这个关键词属于哪一块哪一台服务器，索引是一种有序的数据组合，我们用可以用近似二分法的方式思考，不管数据规模多大，你用二分法去查找一个结果，查询频次是log2(N)，这个就保证了海量数据下，查询一个关键词是非常快非常快的第四步，不同关键词的查询结果（只是按权值排序的部分顶部结果，绝对不是全部结果），基于权值倒序，会再汇总在一起，然后把共同命中的部分反馈回来，并做最后的权值排序。

网站基本信息 SEO数据风向标

【重庆seo】| 阳志刚seo优化交流博客

ALEXA排名	世界排名:-- 流量排名:-- 日均IP≈-- 日均PV≈--
SEO信息	百度权重 2 Google 反链数:1 出站链接:1 站内链接:73
域名IP	118.244.232.58[北京市 电信通酒仙桥数据中心] [同IP网站0个] [响应时间: 3334毫秒]
域名年龄	1月4天（创建于2014年12月04日,过期时间为2016年12月04日）
更多查询	ALEXA排名 友情链接检测 网站历史数据 Whois查询 备案查询 网站排名
域名备案	备案号: 渝ICP备14004370号-3 性质: 个人 名称: 阳志刚 审核时间: 2014-12-30

百度相关

百度流量预计	关键词库	百度快照	首页位置	今日收录	最近一周	最近一月
193	5	2014-12-23	1	5	5	6

网站 www.319seo.com 的收录/反链结果

搜索引擎	百度	谷歌	360	搜狗
收录	6	55	12	0
反链	4万3900↑	0	33万3↓	查询

2.目标常用对象：
博客，论坛，QQ空间，朋友圈，淘宝，贴吧.....
通过检索目标名下常用社交账户来查找信息。
分别介绍如下：

方式与原理

1.暴力破解
密码破解技术中最基本的就是暴力破解，也叫密码穷举。如果黑客事先知道了账户号码，如邮件帐号、QQ用户帐号、网上银行账号等，而用户的密码又设置的十分简单，比如用简单的数字组合，黑客使用暴力破解工具很快就可以破解出密码来。因此用户要尽量将密码设置的复杂一些。

2.键盘记录
当用户密码较为复杂，这时候的暴力破解就要到猴年马月了，这时黑客就会给用户安装木马病毒，设计“键盘记录”程序，记录和监听用户的击键操作，然后通过各种方式将记录下来的用户击键内容传送给黑客，这样，黑客通过分析用户击键信息即可破解出用户的密码。

3.屏幕录入

为了防止击键记录工具，产生了使用鼠标和图片录入密码的方式，这时黑客可以通过木马程序将用户屏幕截屏下来然后记录鼠标点击的位置，通过记录鼠标位置对比截屏的图片，从而破解这类方法的用户密码。

4.钓鱼网站

“网络钓鱼”就是利用假的电子邮件和伪造的网站登陆站点来进行诈骗活动，受骗者往往自己就把信息给你填上去了（比如银行卡，卡号密码等等），黑客是绝对暗爽。当然，网络钓鱼主要通过发送电子邮件引诱用户登录假冒的网上银行、证券网站等等，这样就轻易地骗取用户帐号密码实施盗窃。

5.不良习惯

有一些公司的员工虽然设置了很长的密码，但是却将密码写在纸上，更有甚者把账户密码写在记事本里，还有人使用自己的名字或者自己生日做密码，还有些人使用常用的单词做密码，这些不良的习惯将导致密码极易被破解。

6. Sniffer（嗅探器）
在局域网上嗅探，黑客要想迅速获得大量的账号（包括用户名和密码），最为有效的手段是使用Sniffer程序。Sniffer，中文翻译为嗅探器，对以太网设备上传送的数据包进行侦听，从而发现感兴趣的包如果发现符合条件的包，就把它存到一个Log文件中去。使用这种工具，可以监视网络数据流了。当信息以明文的形式在网络上传输时，便可以使用网络监听的方式窃取网上的传送的数据包。将网络接口设置在监听模式，便可以将网上传输的源源不断的信息截获。任何直接通过HTTP、FTP、POP、SMTP、TELNET协议传输的数据包都会被Sniffer程序监听。

7. Password Reminder
对于本地一些保存的以星号方式密码，可以使用类似Password Reminder这样的工具破解，把Password Reminder中的放大镜拖放到星号上，便可以破解这个密码了。

预防措施

由于人肉搜索的强大力量，使当事人无所遁形，甚而备受困扰，引发一系列严重后果，因此我们有必要掌握一些简单实用的预防措施。

1、不要轻易在论坛上留下你的联系方式、QQ，以免别人通过你的QQ号查询到你的论坛账号（或许就是你常用的用户名），再通过账号一步步追查出更多信息。

2、不要在一些“需要留下邮箱”这样的帖子下面留邮箱。有朝一日，你的敏感用户名被关注了，你的邮箱也暴露了。

3、邮箱、博客、个人空间不要留下自己的联系方式。

4、写日志尽量不涉及真名，用昵称或符号代替。

5、尽量避免在论坛上触犯众怒。

6、注册的各大网站用户名应该多样化，密码多样化。

7、尽量不要放亲密的人的合照，避免殃及朋友。

8、远离实名制网络，实名制是一个定时炸弹，你的信息会被永久保存。

9、各大社交网站，隐私权限要设计好，仅好友可见。

最后，关键时刻，可以利用法律手段维权。

北京理工大學
BEIJING INSTITUTE OF TECHNOLOGY

人肉搜索案例

01 虐猫女事件

02 辽宁骂人女事件

03 铜须门事件

北京理工大學
BEIJING INSTITUTE OF TECHNOLOGY

PART ONE

虐猫女事件

虐猫女事件

虐猫女事件是人肉搜索历史上一个里程碑式的案件

- 2006年2月28 日，网民“碎玻璃渣子”在网上公布了一组残忍而变态的虐猫视频截图
- 图片公布后引起了网民的愤怒，随即对图片中虐猫的女子进行了人肉搜索
- 不久，有人将有关“虐猫”事件的网址公布出来
- 紧接着，有人将该事件中女子的照片贴出来并做成“宇宙通缉令”让大家举报，有些网民甚至悬赏捉拿事件中的女子
- 随后，有人发现上传虐猫视频的网站和另一网站是同一IP，并贴出了网络注册者的信息
- 3月2日，一网民发帖公布了图片中女子的住址使事件出现关键性转变，并在3月4日得到了另一网友的确认
- 至此，距离图片公布不足6天，虐猫事件的三名嫌疑人得到确认

北京理工大學
BEIJING INSTITUTE OF TECHNOLOGY

PART TWO

辽宁骂人女事件

辽宁骂人女事件

- 2008年5月21日，国外最大视频网站YouTube出现一时长440秒的视频，视频中一女子身处网吧，用轻蔑大语气大谈对四川地震及灾区人民的看法
- 该视频在国外网站疯传，并在不到一小时后被中国网民连接到了天涯社区、猫扑等当时国内最大的论坛
- 该视频引起了网友的愤怒，一个“号召13亿人一起动手把她找出来的“搜索令”发出
- 网友通过其上网的IP地址找到其上网的具体地点
- 视频中女子的QQ号和QQ空间被找到
- 该女子QQ号和QQ空间里存储的年龄、血型、居住地等信息被公开，并随着该女的密码被网友攻破，其同事的密码也被网友攻破，更多信息公布出来
- 半小时不到，该女子的详细信息，包括出生年份、户籍所在地、身份证号码、家庭成员、具体住址、工作地点被匿名网友发出，甚至该女子的父母和哥哥的手机号也被网友拔出
- 21日下午1时，警方根据网上资料在网吧将该女子抓获

北京理工大學
BEIJING INSTITUTE OF TECHNOLOGY

PART THREE

铜须门事件

铜须门事件

- 2006年4月13日，“猫扑网”旗下《魔兽世界中国》主题论坛，一男子发帖称其妻子沉迷《魔兽世界》，并在一次玩家聚会后与一名网名为“铜须”的男子发生一夜情
- 丈夫引来网友的同情，网友利用根据搜索“铜须”在现实中的资料
- 4月15日至17日，网友通过搜索到“铜须”在河北的获奖经历后得到了他的真实姓名
- 网友通过“铜须”的QQ空间得到了他的昵称“稀帅”
- 网友得知“铜须”曾玩过“天堂2”游戏，并结婚其QQ号找到了“铜须”之前卖游戏装备的帖子
- 网友通过帖子找到了“铜须”的手机号码，并通过相关搜索得到了“铜须”的照片
- 4月17日网友“超级捣蛋”在猫扑发帖将“铜须”的资料公布