

课程简介

教师信息

- 姓名：孙惠平
- 方向：网络和信息安全、金融科技
- 关注：身份认证、区块链、智能风控
- 邮箱：sunhp@ss.pku.edu.cn
- 主页：<https://huipingsun.github.io>
- Lab：北大信息安全实验室
- 地址：北京大学燕园大厦1018、北京大学理科1号楼1530E

课程基本信息

- 基本信息

- * 上课时间：每周二、下午14点到17点 (3203)
- * 时间区间：11月3日、12月15日、12月22日
- * 课程主页：<https://huipingsun.github.io/ics2020>

- 课程内容

- * 信息安全经济学
- * 区块链

两次课后作业
论文阅读报告

信息安全管理经济学

- Security engineering is about building system to remain dependable in the face of **malice, error, or mischance**. As a discipline, it focus on the **tools, process, and methods** needed to **design, implement, and test** complete systems, and to **adapt** existing systems as their environment evolves.

- Security engineering requires **cross-disciplinary expertise**, ranging from **cryptography** and **computer security** through hardware tamper-resistance and formal methods to knowledge of **economics, applied psychology, organisations and the law**.

- 可用：

- 存储、维护、管理



可用
视角

- 经济：

- 风险多大，收益多大

经济
视角

传统
视角

- 信任：

- 信任哪些密钥

信任
视角

- 隐私：

- 托管

- 传统：

- 速度快、准确、安全

- 防火墙
- 入侵检测
- 杀病毒
- 密码算法
- 身份认证
-

隐私

Bug

网络钓鱼

系统可靠性

- 信息不对称
- 网络外部性
- 错误激励

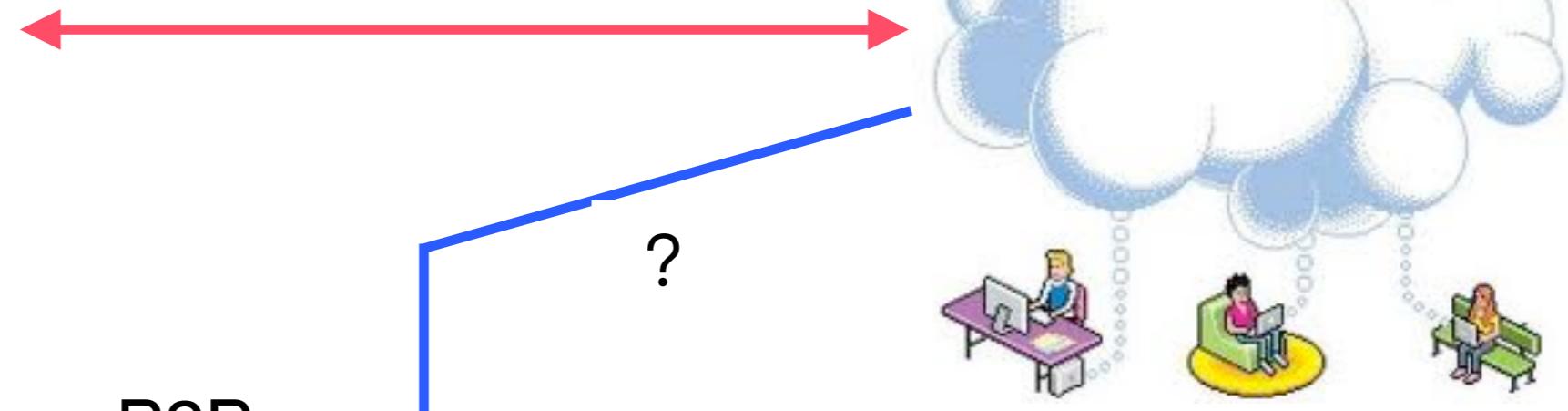
- 公共品悲剧
- 博弈/机制设计
-

2000年

2010年

- 《国富论》：自由市场+理性个体+利己动机+改进
- 19世纪：市场充分竞争、价格、均衡、边际成本
- 20世纪：完全信息、不完全信息、数学证明
- 外部性：正的外部性、负的外部性
 - 技术发明、公共教育、信息、排他性消费
 - 环境污染、
- 市场失败

计算环境变迁



P2P

区块链



Client-Server



- 2010年IT改变
 - * Phone替代PC
 - * SNS替代社交
 - * 云代替服务器
- 市场机制
 - * 行为
 - * 激励
 - * 市场
 - * 均衡
- 攻防
 - * 攻击 vs. 防护
 - * 个人 vs. 社会
 - * 隐私 vs. 安全
 - * 开发 vs. 测试
 - * 个人 vs. 商家+政府

- 价格歧视，同一件商品对不同消费者收取不同的价格
- 顾客细分，市场细分

利润最大化

- 1000个大学宿舍
- 1个学生愿意付\$4000
- 300个学生愿意付\$3000
- 1000个愿意付\$1000
- 800个， \$1400
- 帕累托改进

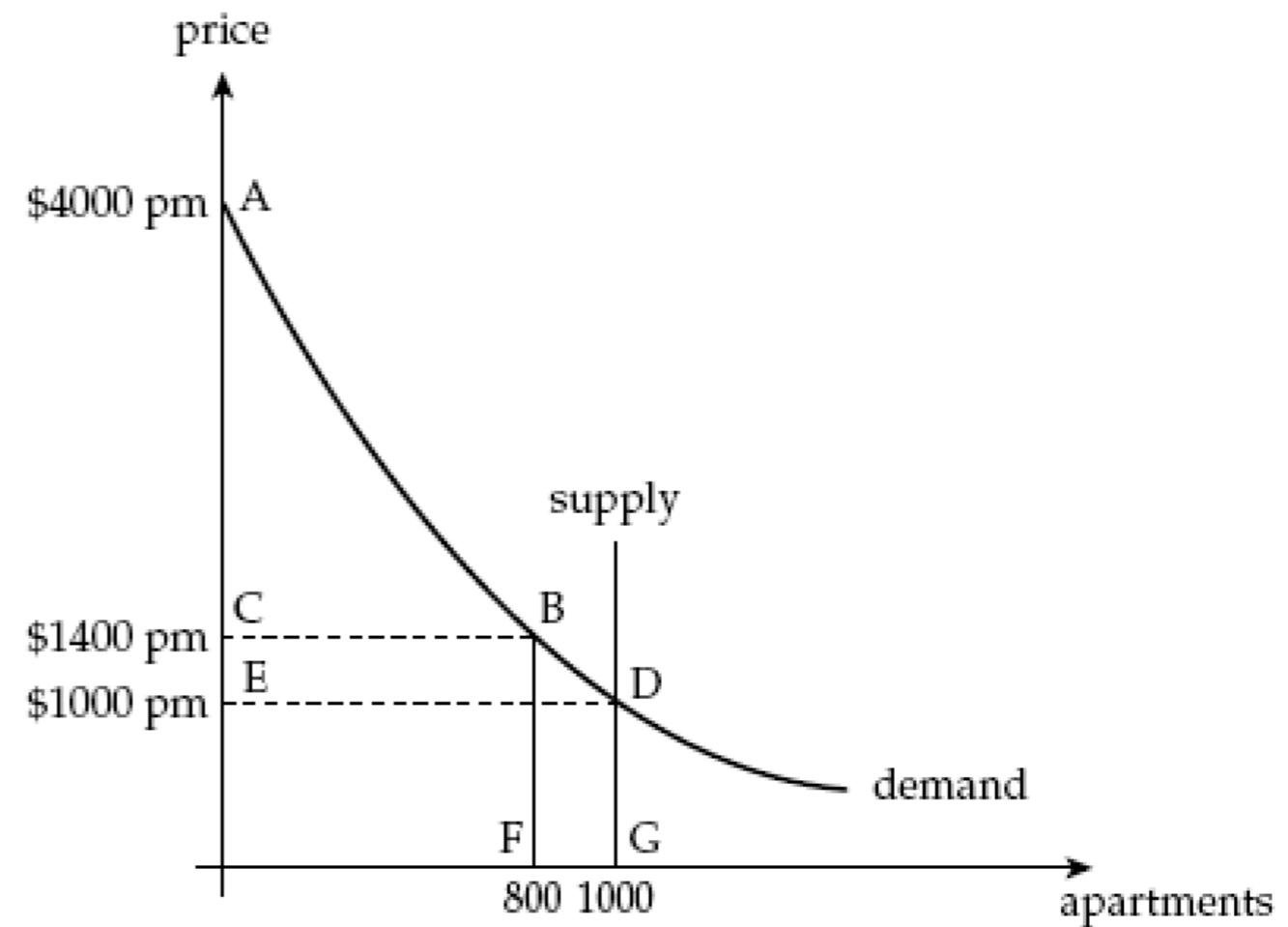


Figure 7.1: The market for apartments

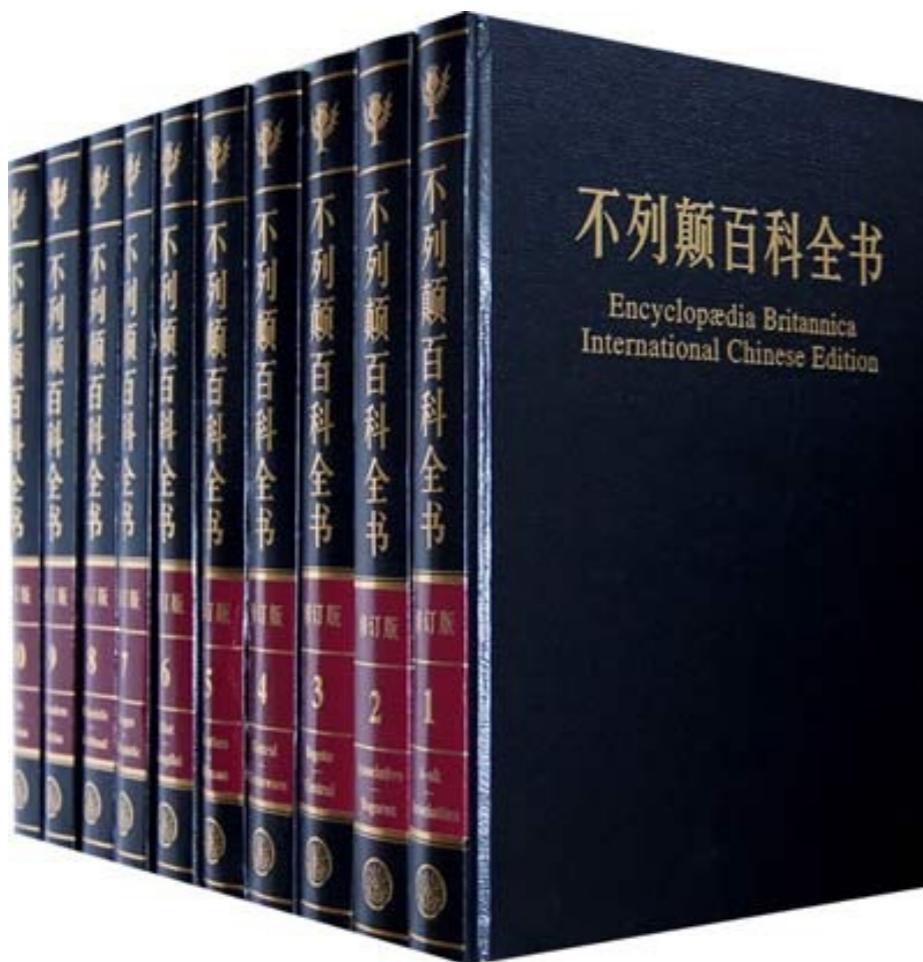
公用品悲剧

非竞争性非排他性的商品



*Internet*安全很多时候也是公用品

- 商品的价格在完全竞争市场均衡状态下等于边际成本
- 信息的边际成本等于0，复制基本无成本



维基百科

大英百科全书

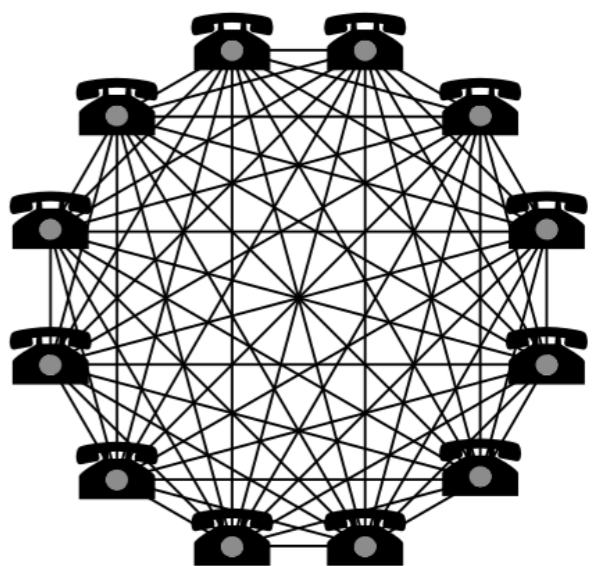
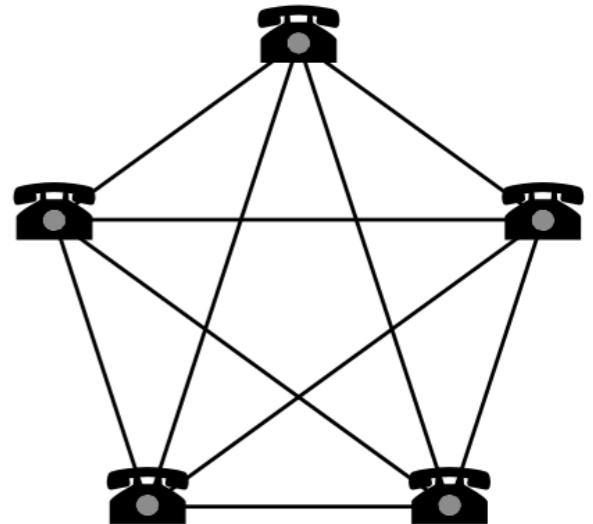
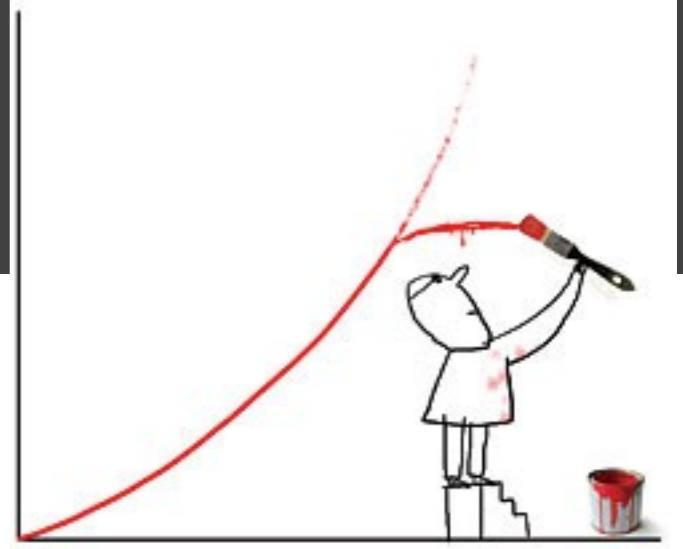
- 梅特卡夫法则：网络价值以用户的数量的平方的数量增长



乔治 吉尔德



3Com创始人



- 连接一个网络的价值取决于已经连接到该网络用户数量
- 正反馈使得强者越强，弱者越弱
- 网络一开始增长很慢，一旦正反馈建立，网络将迅速增长



- 一个产品对于一个用户的价值取决于有多少用户使用
- IT产品有高的固定成本和低的边际成本
- 交换成本（转移成本）高，（渐进vs革命）

QWERTY键盘

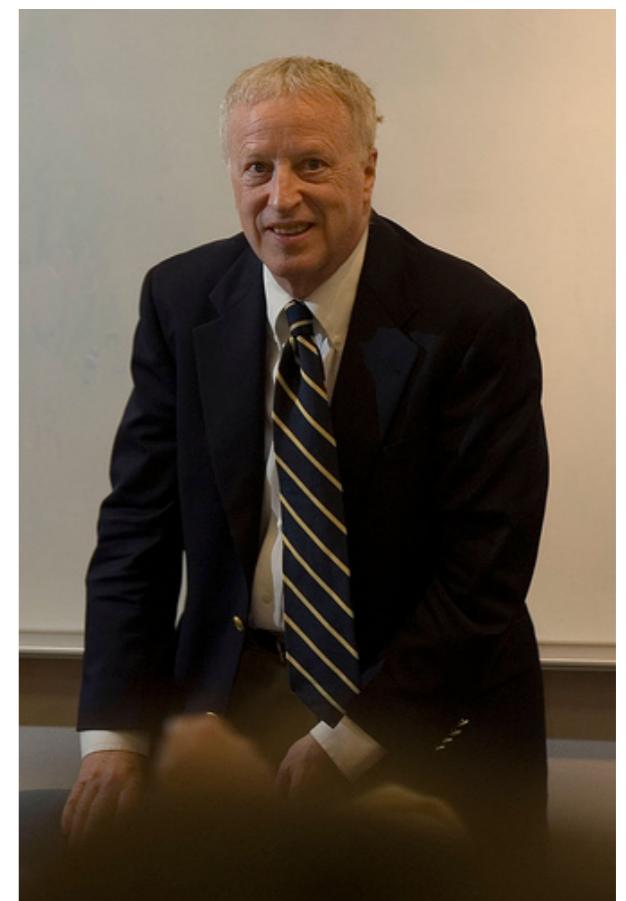


- 指参与交易各方拥有的、可影响交易的信息不同
- 信息不对称可能导致逆向选择(adverse selection), 道德风险(moral hazard), 劣币驱逐良币(bad money drives out good), 或是形成寻租行为

-
- 阿克洛夫, 2001年诺贝尔经济学奖
 - 1970年的著作《柠檬市场》

THE MARKET FOR “LEMONS”:
QUALITY UNCERTAINTY AND THE
MARKET MECHANISM *

GEORGE A. AKERLOF



柠檬市场

- 二手车市场有两种车：高质量(peach)和低质量(lemon)
- peach的价格应该高于lemon的价格，市场上平均价格应该在这两个价格之间

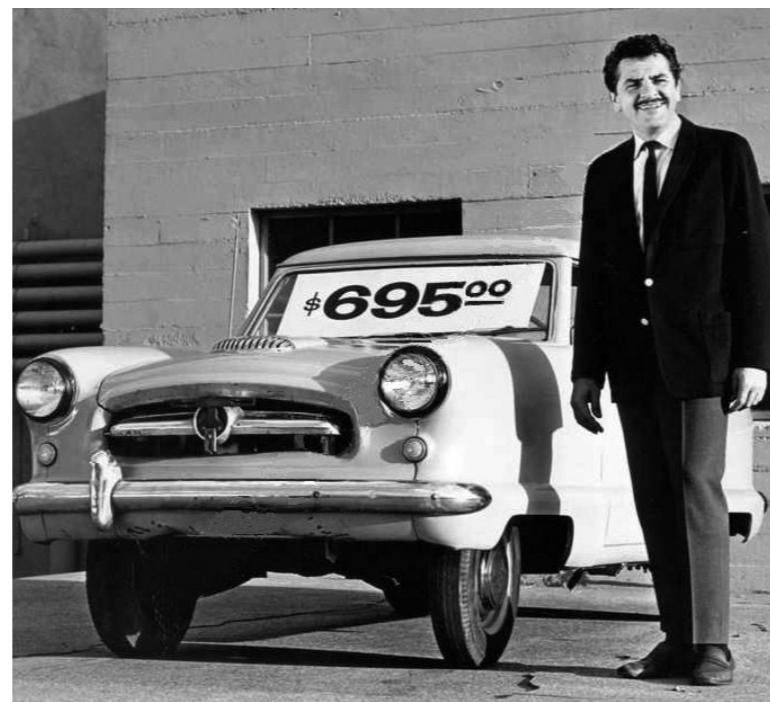
>>买方<<



不知道是peach
还是lemon



花peach的价格
花平均价格
花lemon的价格



>>卖方<<



知道是peach
还是lemon



卖peach亏本
卖lemon挣钱



市场上都
是lemon



市场失灵

信誉

担保

信息公开

反垄断

- 市场有两种信息系统：安全的信息系统和不安全的信息系统
- 安全信息系统的应该高于不安全信息系统的安全

>>用户<<



是否知道信息
系统安全与否



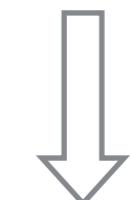
花高的价格
花低的价格



>>厂商<<



是否知道信息
系统安全与否



安全的成本高
不安全的成本低

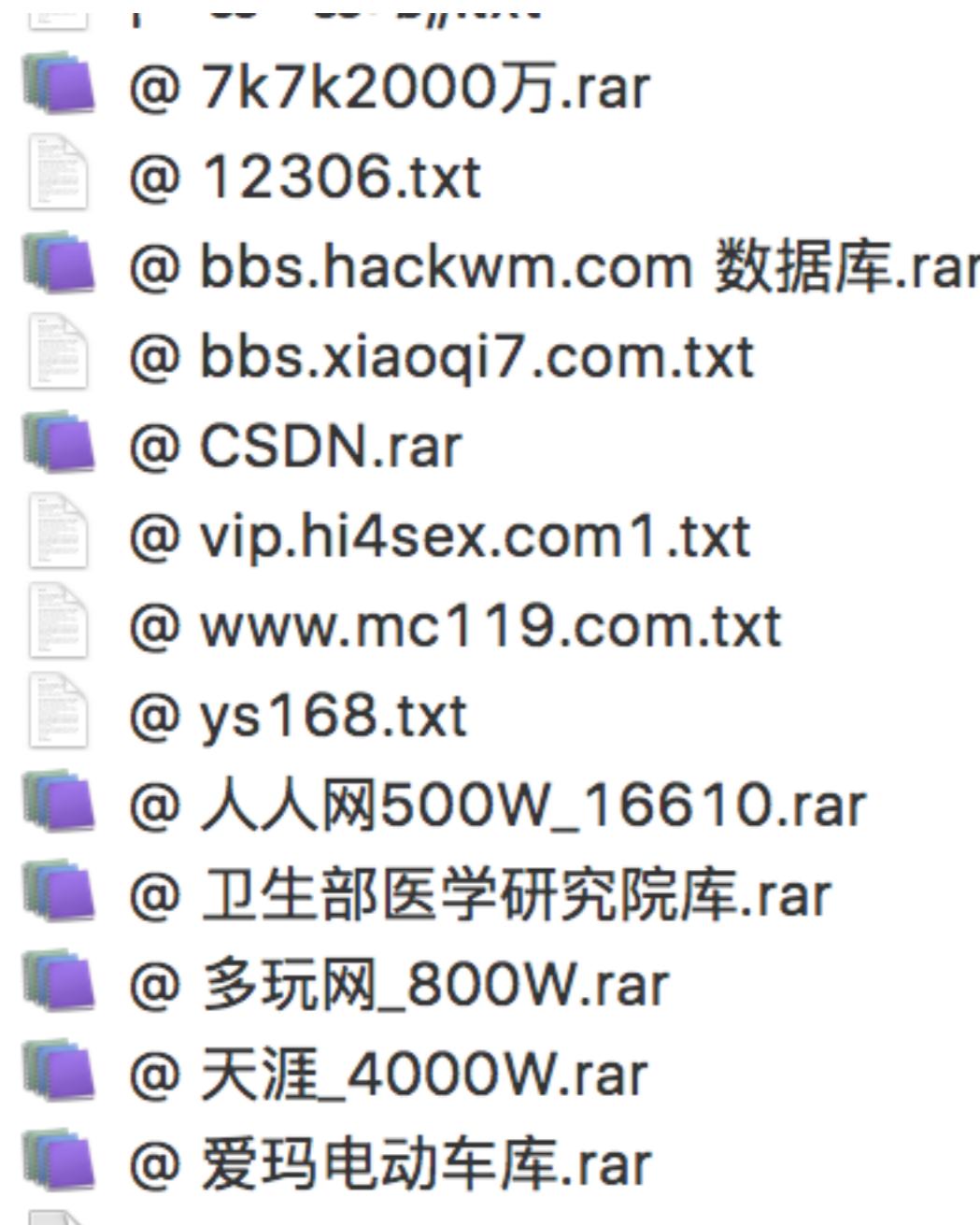
市场上信息
系统安全吗



- 信息产业倾向于产生具有支配地位的厂商， 赢者通吃
 - 如果过多的考虑安全因素， 会降低进入和占有市场的机会
 - 信息安全会给开发者和使用者带来一定的困难和障碍
 - 厂商尽可能的把安全问题留给用户
-

- 产品一开始不安全
- 安全功能很多是为厂家利益考虑的
- 厂商宁可让开发者简便容易开发， 也不会为了增强安全提高开发难度
- 厂商会将自己应该承担的安全和运维责任转嫁给用户
- 厂商使用安全算法来保障对用户的锁定和差别定价

个人信息泄漏频发，数据量越来越大



厂商为什么收集个人信息

- 厂商为了减少风险：支付欺诈；交易合法性
- 厂商为了更好的了解用户，刻画用户，为了**差别定价**
- 厂商会过量收集个人信息，但并不保护个人信息

- 厂商总是夸大信息安全的威胁
 - 受害者不愿意公开安全事件
-
- Toxic Release Inventory (TRI), 1986
 - 美国的44个州已经建立法律，要求涉及个人的信息泄漏必须披露
 - 要求掌握个人信息的公司必须保证安全
 - 目的：sunlight is the best disinfectant; right to know
 - 高的厂商花费 vs 低的社会花费

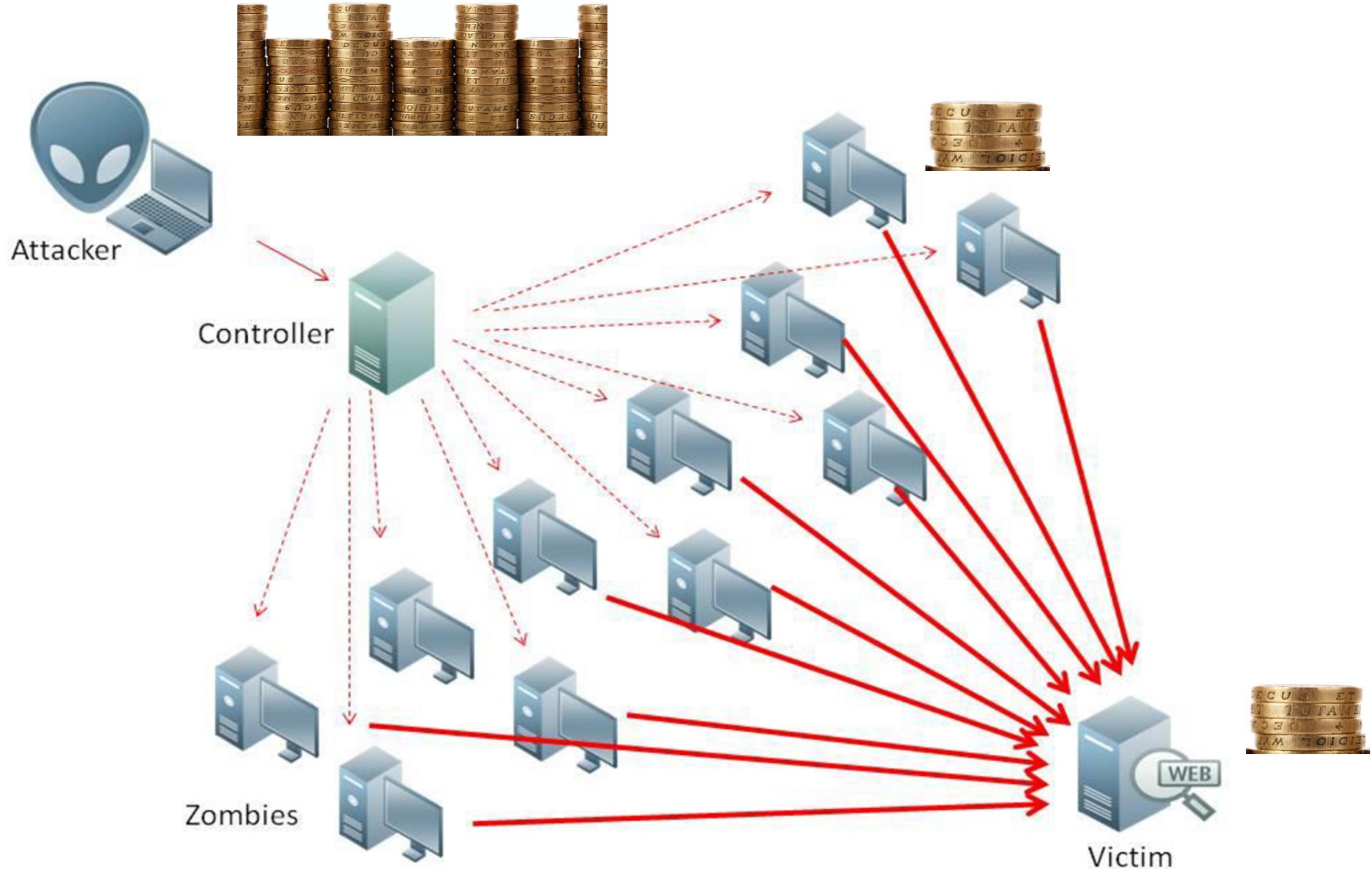
- 传统安全模型
- 仅假设攻击方能力，不考虑攻击方动机

-
- **weakest link**
 - **best shot**
 - **sum of efforts**
 - **weakest target**
 - 单个编程错误
 - 安全架构师
 - 安全测试

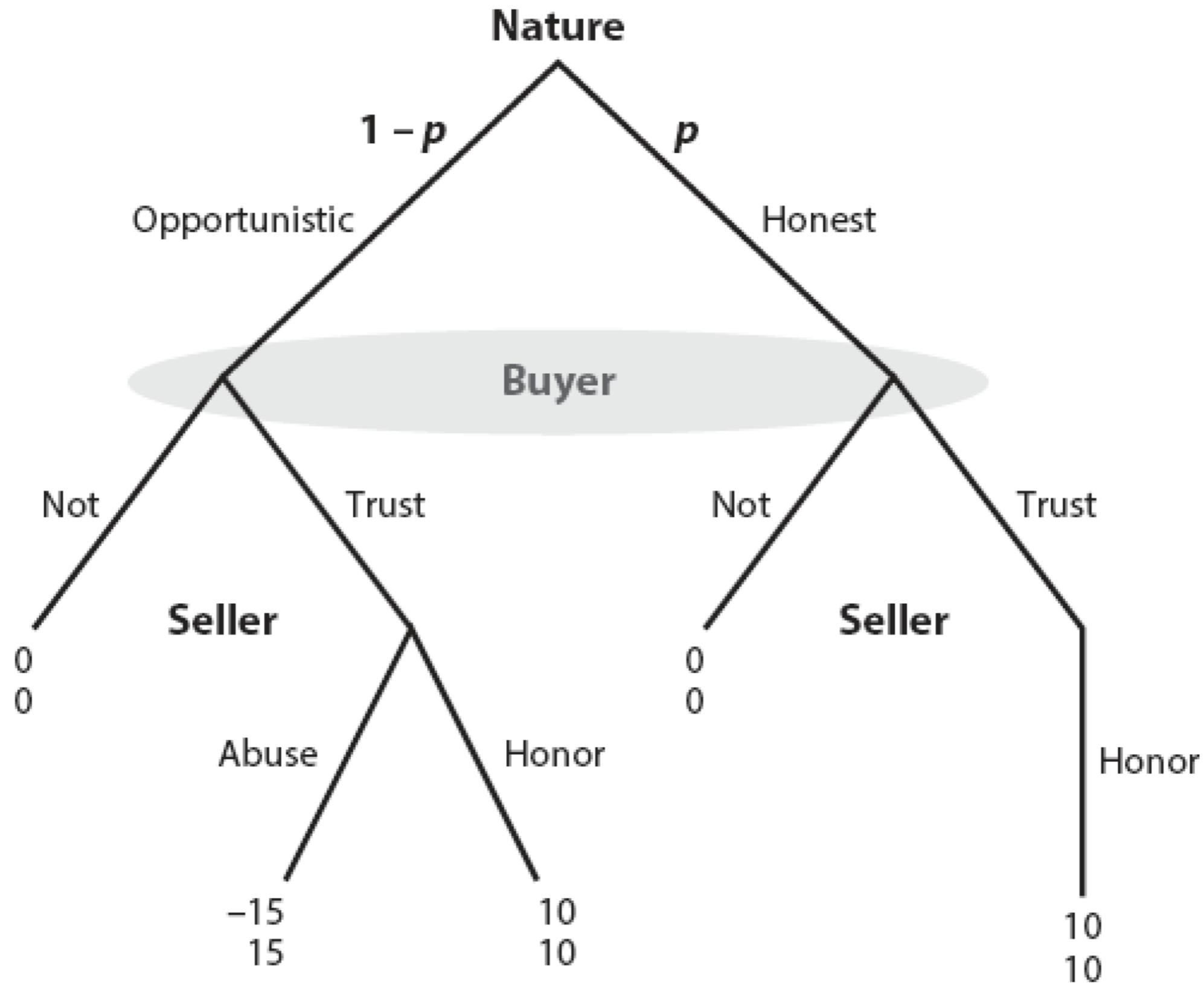
- 安全是公用品 vs 私有花费
 - 攻击者： 攻击花费、被检测可能性、成功攻击的回报
-
- 一个漏洞被发现堵上， 攻击者会发现下一个漏洞
 - 一个ISP提高了防御能力， 攻击者会转向下一个
 - P2P被分配自己感兴趣的内容， 更愿意提高自己抵御能力
 - P2P每个节点自我保护比总体保护更廉价

- 攻击者和防御者处于不平等的地位上
 - 防御者永远不知道哪个是最弱的一环
-
- 防御者需要评估每一个可能的攻击及其危害
 - 攻击者何防御者的角色是模糊的
 - 漏洞存储（保护自己 vs 打击敌人，个人收益 vs 社会成本）
 - 网络战争

分布式拒绝服务攻击 (DDOS)



博弈模型

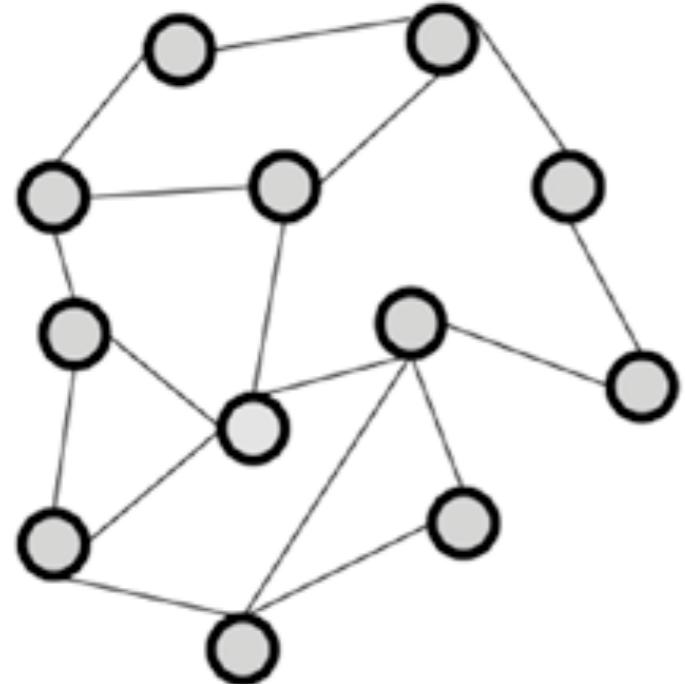


Be nice to
others who
are nice to
you

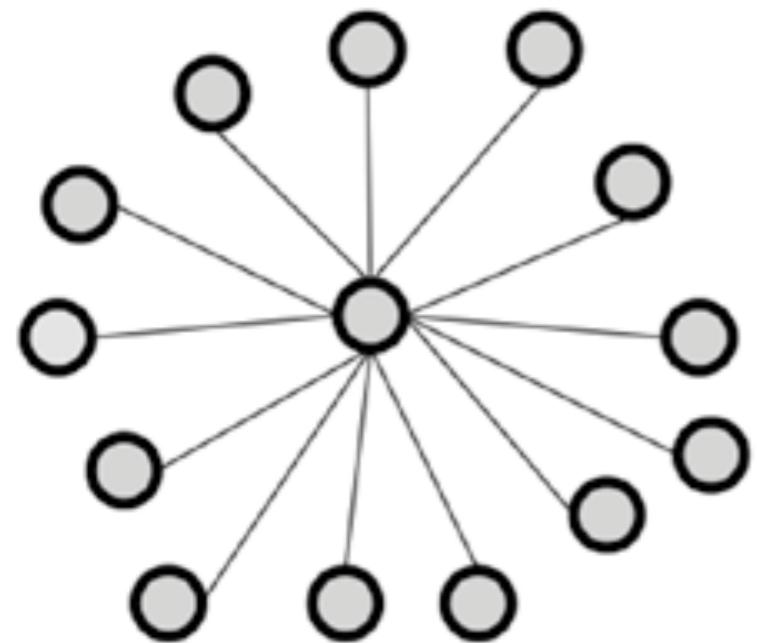
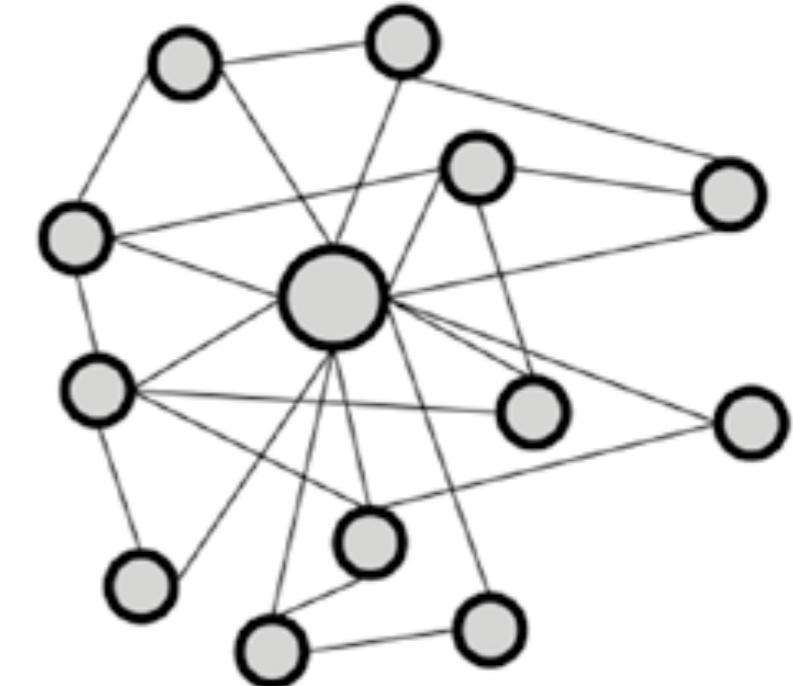


Tit-for-tat

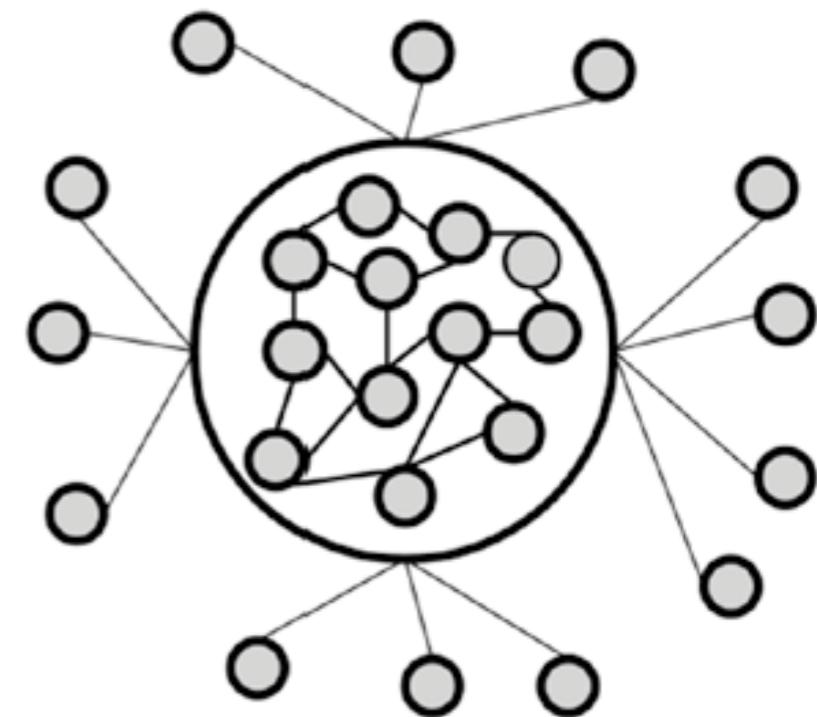
分布式系统



没有纯粹的
中心化系统
或者
分布式系统



*Internet
Email
IM
SNS*





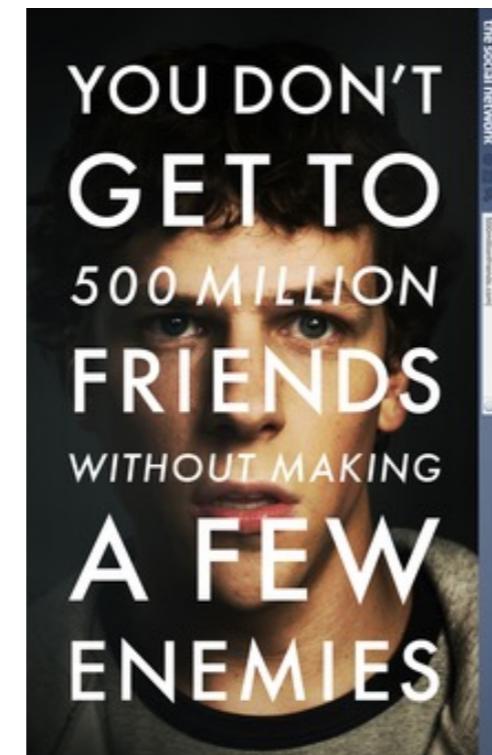
napster™

1999



Sean Parker

facebook



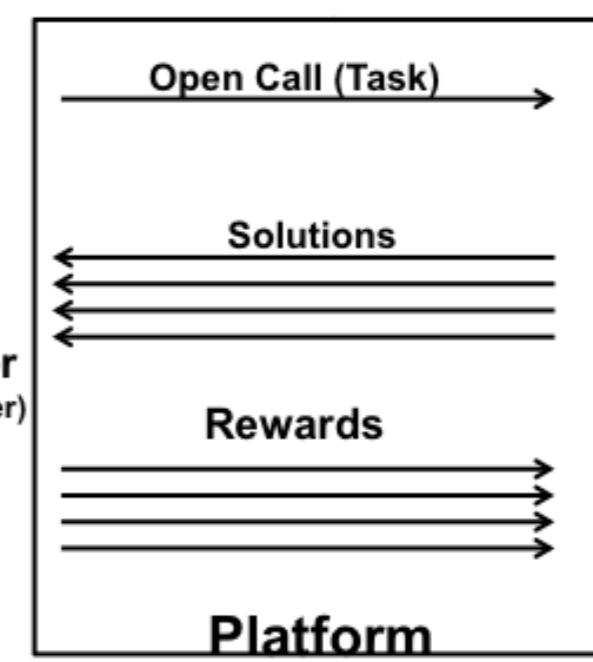
The Social Network



2003



众包



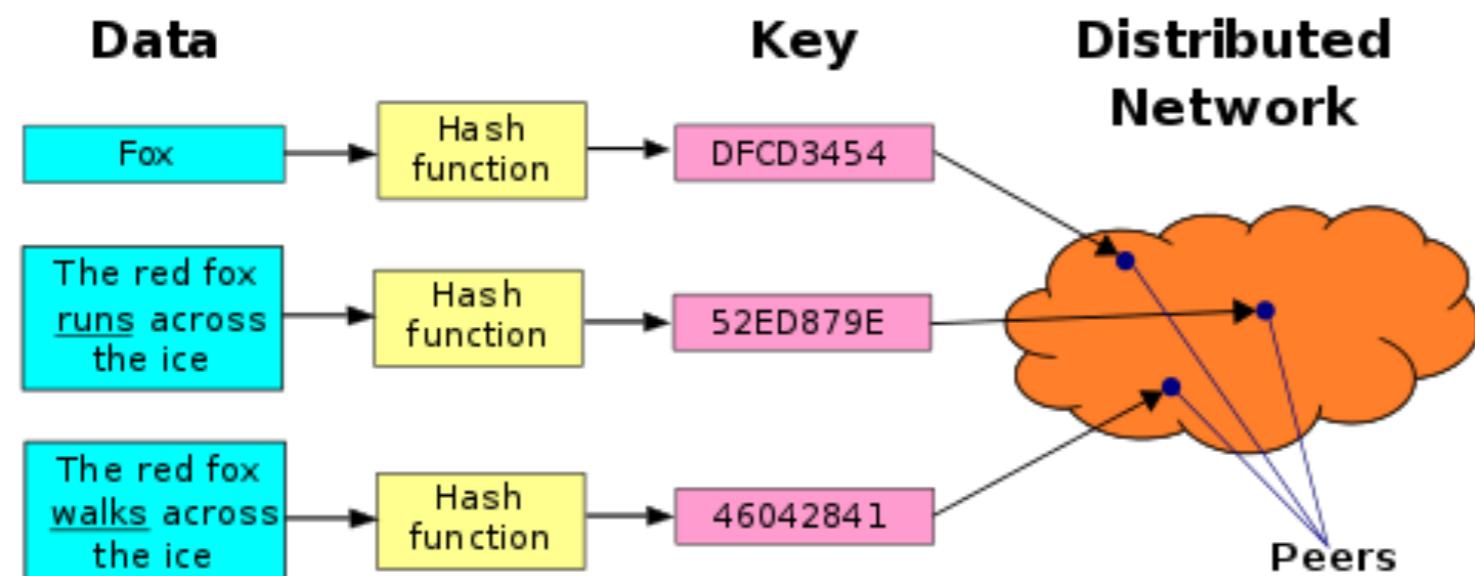


2001

Bram Cohen

BitTorrent

Distributed Hash Table

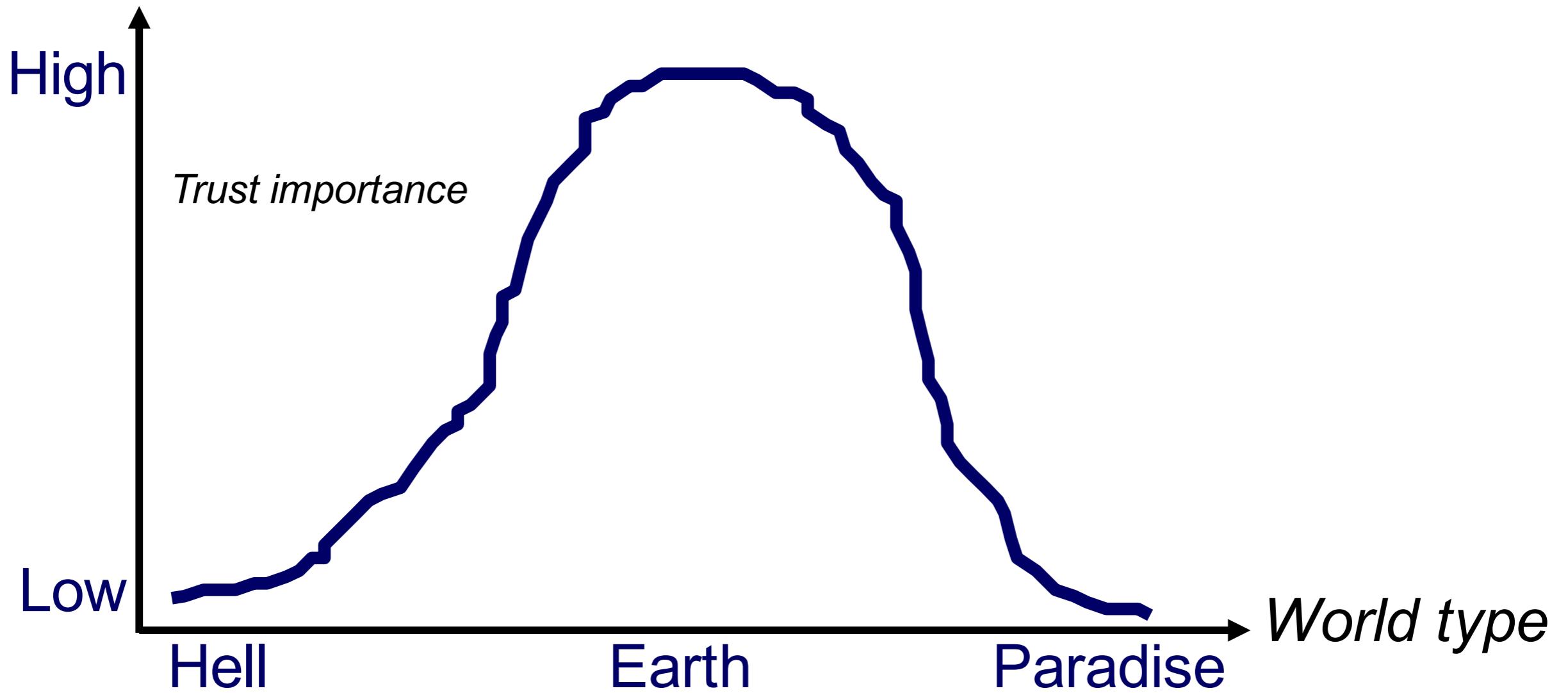


激励

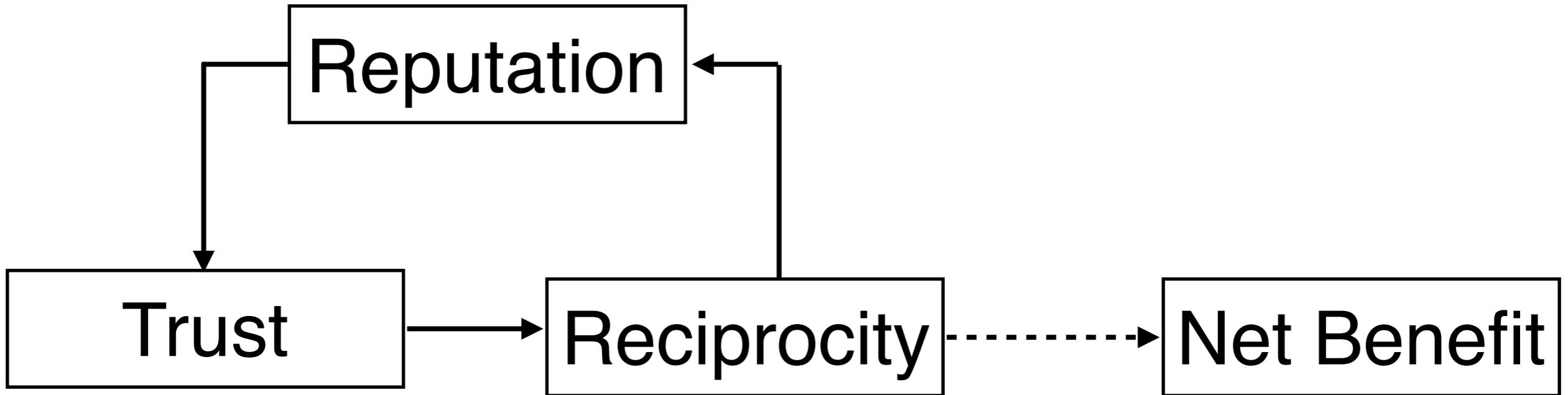
<https://en.wikipedia.org/wiki/BitTorrent>

https://en.wikipedia.org/wiki/Distributed_hash_table

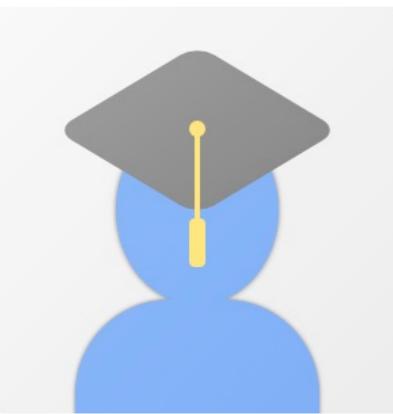
信任 >>> 信息安全



信任是社会交互的
润滑剂



- 因为你的信誉好，所以我信任你
- 虽然你的信誉不好，但是我也信任你



Paul Resnick

[Follow ▾](#)

University of Michigan

social computing, recommender systems, reputation systems, online communities

Verified email at umich.edu - [Homepage](#)

Title 1–20

Cited by Year

GroupLens: an open architecture for collaborative filtering of netnews

5446 1994

P Resnick, N Iacovou, M Suchak, P Bergstrom, J Riedl

Proceedings of the 1994 ACM conference on Computer supported cooperative ...

Recommender systems

P Resnick, HR Varian

3844 1997

Communications of the ACM 40 (3), 56-58

Reputation systems

P Resnick, K Kuwabara, R Zeckhauser, E Friedman

2623 2000

Communications of the ACM 43 (12), 45-48

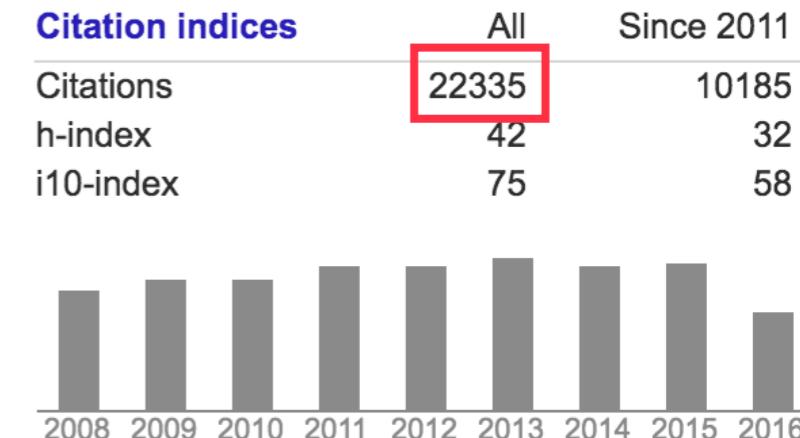
Trust among strangers in internet transactions: Empirical analysis of ebay's reputation system

1840 2002

P Resnick, R Zeckhauser

The Economics of the Internet and E-commerce 11 (2), 23-25

Google Scholar


[Get my own profile](#)
Co-authors [View all...](#)

John Riedl

Robert E. Kraut

Sean A. Munson

Caroline Richardson

eric friedman

Hal Varian



Shop by category ▾

Search...

All Categories ▾

Search

Advanced

[Back to search results](#) | Listed in category: [Computers/Tablets & Networking](#) > [Laptops & Netbooks](#) > [Apple Laptops](#) >
[See more Apple MacBook Pro A1502 13.3" Laptop - MF839LL...](#)

Apple 13.3" MacBook Pro w/Retina Display 8GB Memory - 128GB Storage MF839LL/A

1-Year Apple Warranty Included

1,119 viewed per day 103 product ratings

Item condition: **New**

Quantity:

1

More than 10 available / **236 sold**List price: ~~\$1,299.00~~

You save: \$119.90 (9% off)

Now: **US \$1,179.10****Buy It Now****Add to cart**Qualifies for: **2 yr warranty from SquareTrade - \$106.99**

323 watching

Add to watch list

Add to collection

Click to view larger image

\$ Have one to sell?

Sell now

Located in United States



| Add to watch list

**electronicsvalley** (29672) me

99.7% Positive feedback



Follow this seller

Visit store: **ElectronicsValley**[See other items](#)**Today****electronicsvalley** (29672) me

99.7% Positive feedback

主要应用

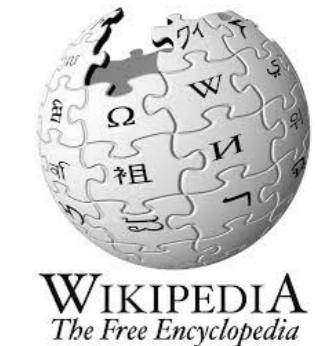
- 电子商务
- 社交网络
- 众包
- 开放协作
- 论坛
- 云计算
- 共享经济
- 金融支付
- Mooc
-



淘宝网
Taobao.com



facebook



知乎



FICO模型



<http://www.fico.com/>



短时间开立多个
信用账户的用户
风险更高

新开立的信用账户
10%

使用信用的年限
15%

使用信用账户的
历史越长分值越
高

正在使用的信用类型

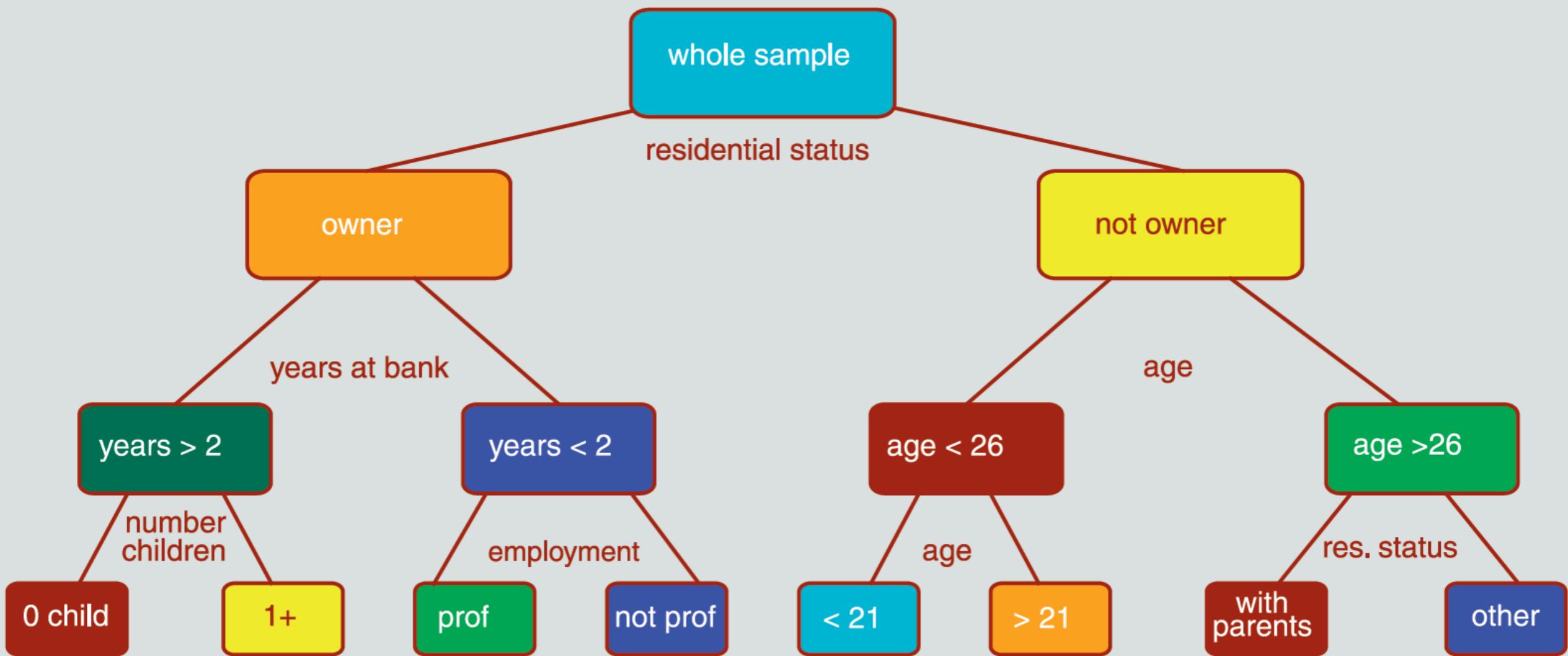


信用账户数

需还款账户的数量与用户信
还能力挂钩，FICO主要分析
该用户需要多少信用账户



- Credit scoring is a set of decision models that aid lenders in the granting of consumer credit. These techniques are used to decide who will get credit, how much credit they should get, what price they should get it at, and what operational strategies will enhance the profitability of the borrowers to the lenders.





WHERE EVERYONE WANTS TO BE AN ICON



BLACK MIRROR

大数据 >>> 信息安全

- 数字化信息

- * 被长期乃至永久保存

- * 复制简单而又准确

- * 传输容易而又廉价

- * 搜索非常便捷迅速

- 互联网

- * 目的是学术论文共享

- 地球村

- * 缺乏匿名性和秘密性

1965年、摩尔定律

一个芯片的能力

一本书→一个图书馆

终记录

25T, 450个IPod

10年20年后?

近乎免费的存储

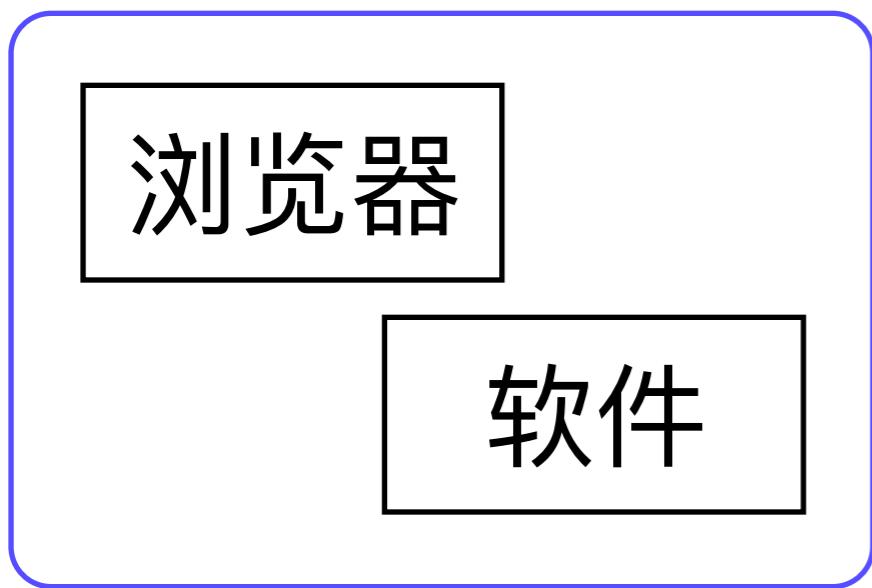
无尽的计算能力

高速链接的网络

设备指纹



硬件
行为
特征



主动
被动

软件 | 用户
行为 | 行为
特征 | 特征

特征

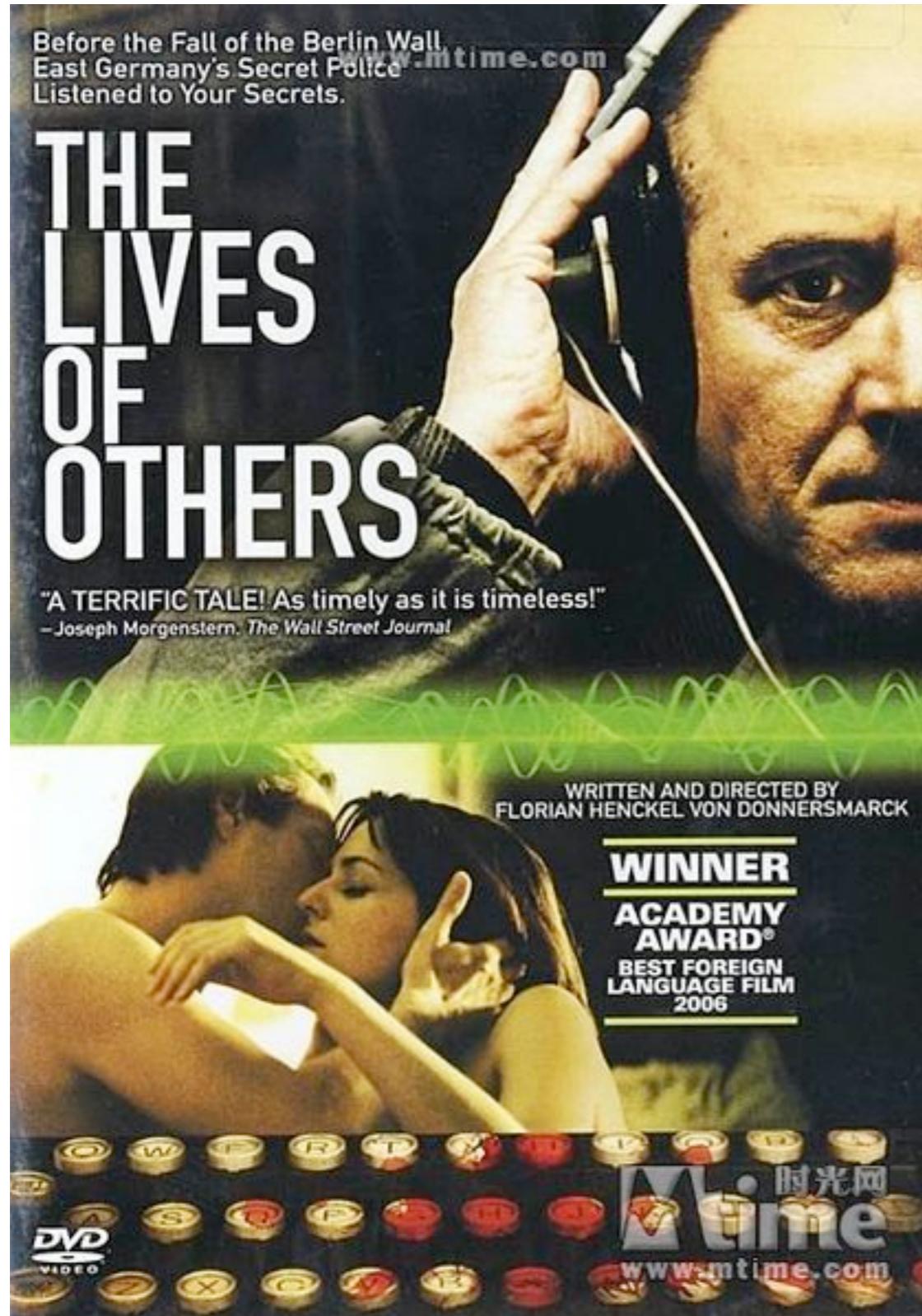
身份盗用
信用卡诈骗



Identification

<http://browserspy.dk/>
<http://noc.to/>

窃听风暴



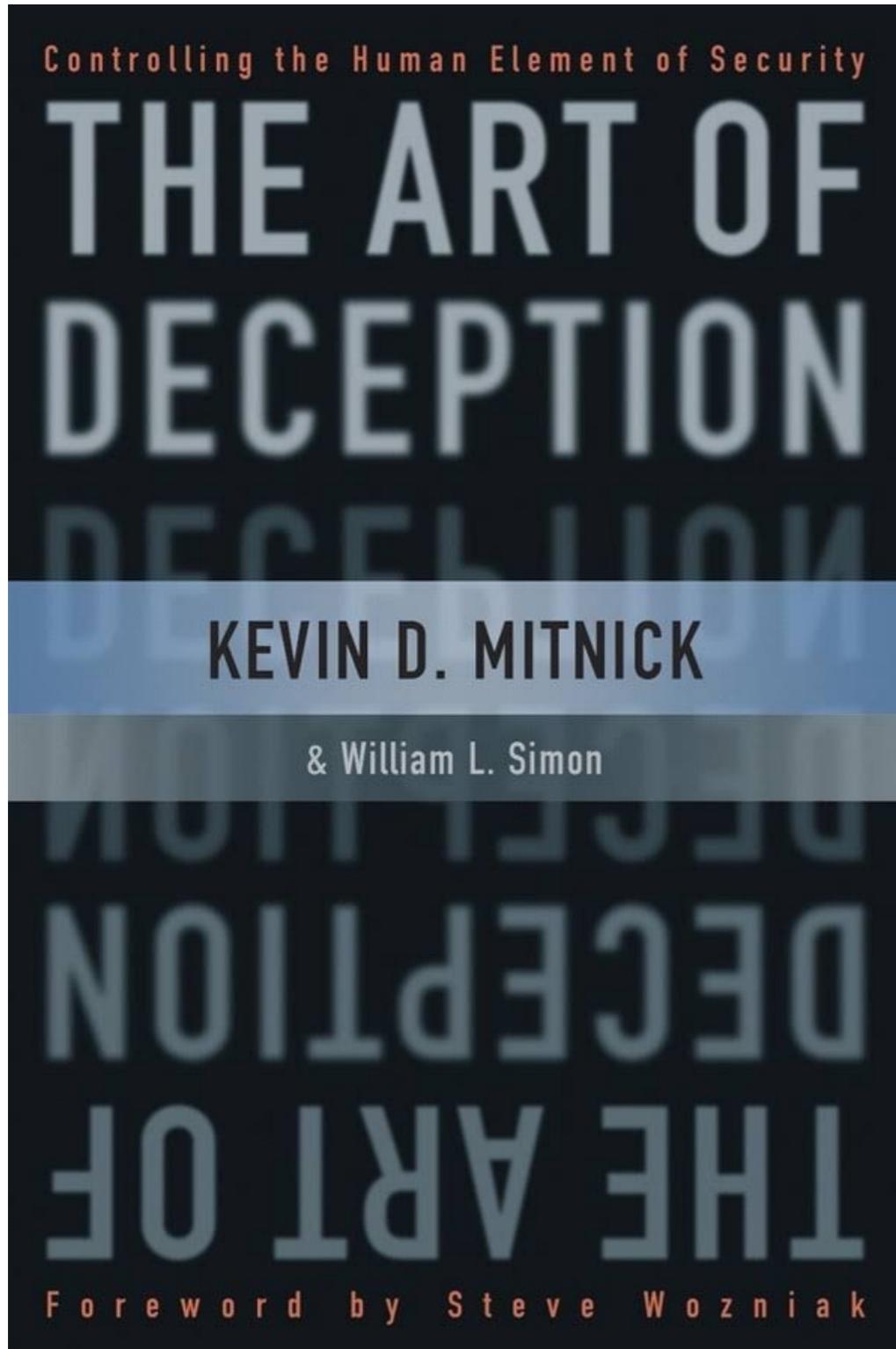
- 1984年的东德
- 2004拍摄
- 1800万人， 600万人被监视
- 28万6千雇员 = 9万1千 + 17万5千



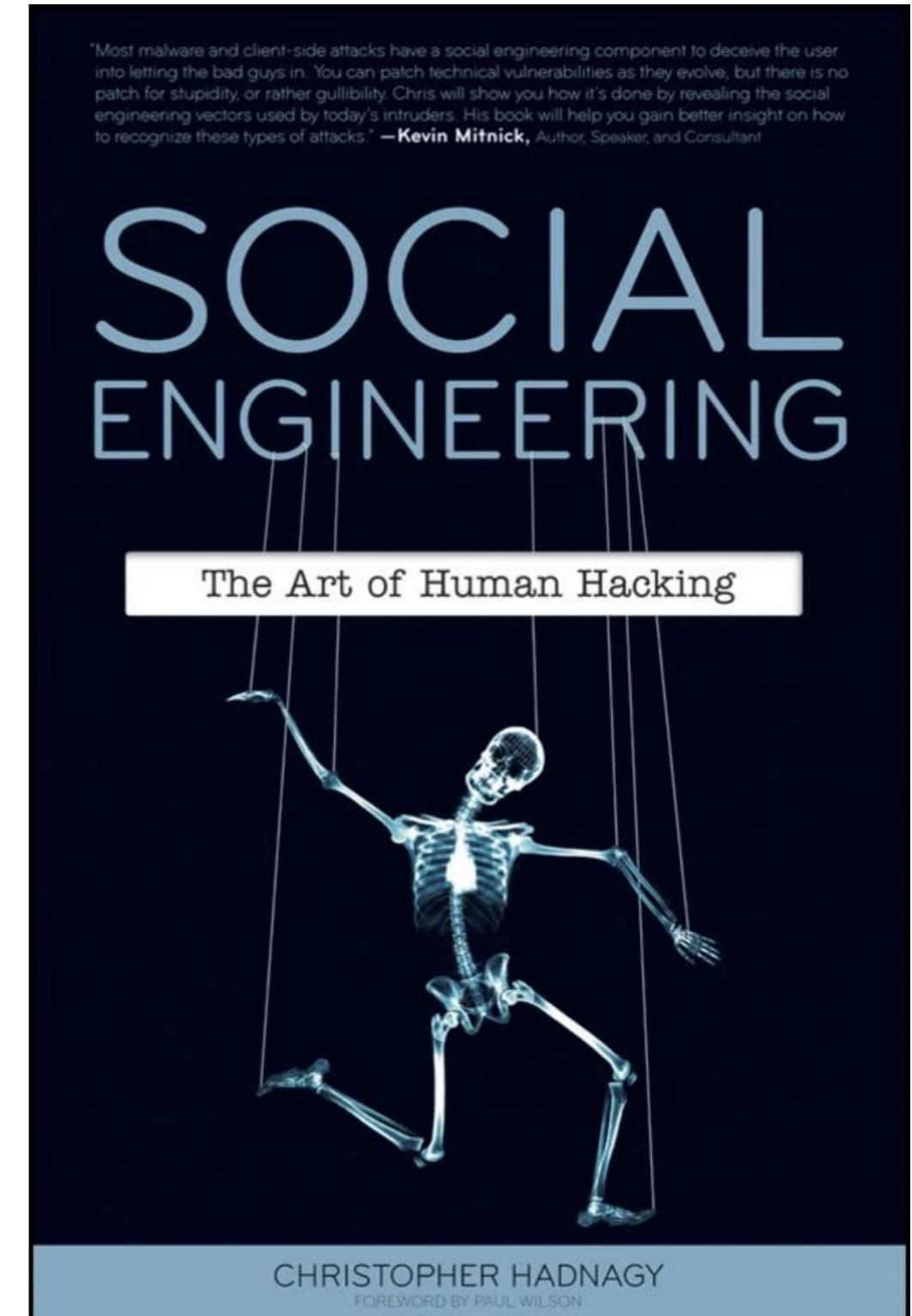
心理学 >>> 信息安全

Usable Security

社会工程学



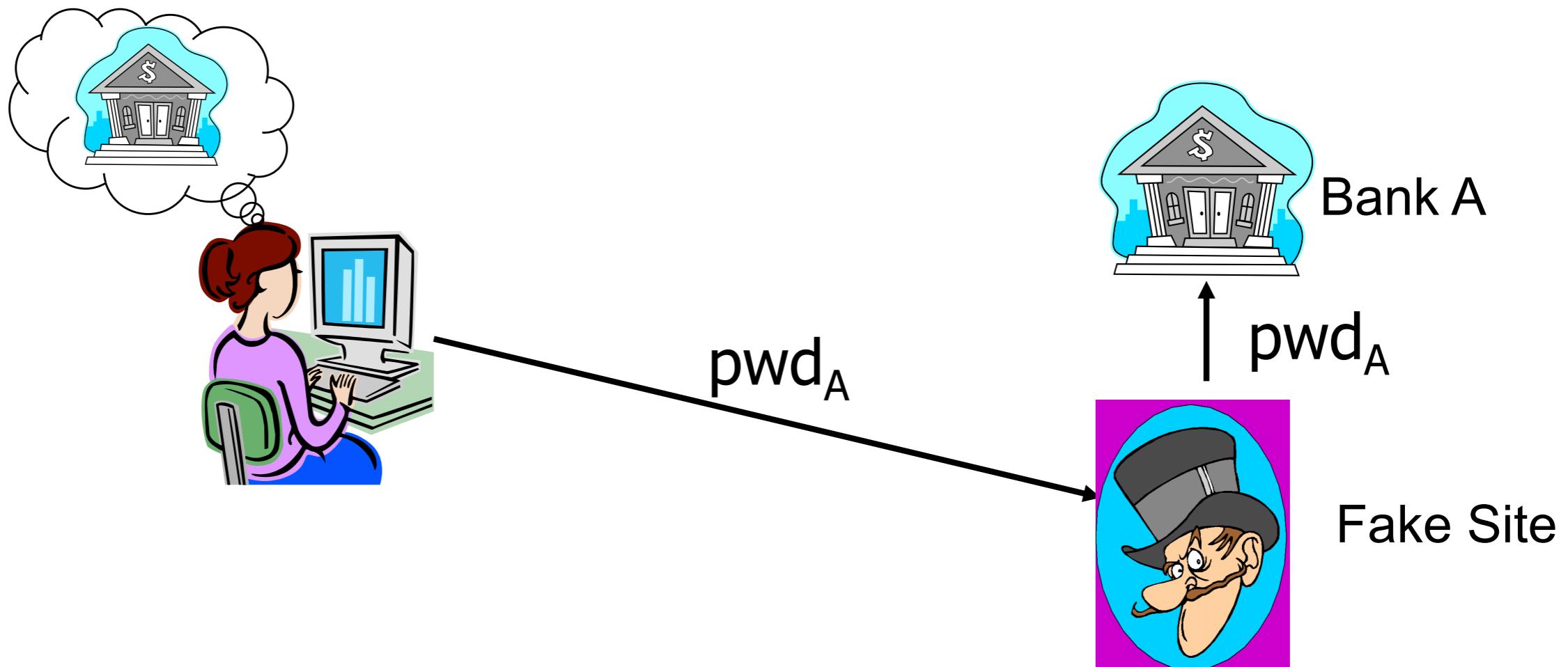
2002



2010

网络钓鱼

- 对银行的网络钓鱼开始于2003年
- 2006年，美国银行损失2亿美元



人际交流改变



非誠勿擾

- 现实社会：
 - * 面对面直接交互
- 网路环境：
 - * 面对面直接交互减少
 - * 技术替身（电话、电子邮件、短信、IM、视频等）
 - * 身体消失－隐身人

信息将证明交互



人防止欺骗的能力失效了



非誠勿擾

Usable Security

证书



The page title is "The site's security certificate is not trusted!". It includes a warning icon and a detailed explanation of the certificate issue. Buttons at the bottom are "Proceed anyway" and "Back to safety". A link "Help me understand" is also present.

The main content shows the certificate hierarchy and fields. The hierarchy tree shows:

- Builtin Object Token:VeriSign Class 3 Public Primary Certification Authority
 - OU=www.verisign.com/CPS Incorp. by Ref. LIABILITY LTD.(c)97 VeriSign,OU=Veri...
 - web.da-us.citibank.com

The certificate fields section shows:

- web.da-us.citibank.com
 - Certificate
 - Version
 - Serial Number
 - Certificate Signature Algorithm
 - Issuer
 - Validity
 - Not Before
 - Not After

At the bottom, there are "Field Value" and "Help" buttons.

Say
OK to
Any
Question
About
Security

可用性定义

- The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use. — ISO 9241-11: 1989

主观满意度 ★

是用户在使用产品过程中所感受到的主观满意和接受程度

有效性 ★

是用户完成特定任务和达成特定目标时所具有的正确和完整程度

效率 ★

是用户完成任务的正确和完成程度与所用资源（如时间）之间的比率

易学性 ★

产品是否易于学习

用户满意度 ★

用户对产品是否满意

能用

易用

易记性 ★

客户搁置一段时间后是否仍然记得如何操作

交互效率 ★

使用产品完成具体任务的效率

错误 ★

操作错误出现的频率和严重程度如何



Jakob
Nielsen

<https://www.nngroup.com/people/jakob-nielsen/>

- It is essential that the **human interface** be designed for **ease of use**, so that users **routinely** and **automatically** apply the protection mechanisms correctly. Also, to the extent that the user's **mental image** of his **protection goals** match the mechanisms he must use, **mistakes will be minimized**.

—*The Protection of Information in Computer System. In Proc. IEEE 1975*

- **User-Centered Security**, NSPW 1996
- **User Are Not the Enemy**, CACM 1999
- **Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0**, USENIX Security, 1999

计算机能力

计算、存储、网络、普及、...

用户要求

角色、需求、竞争、消失、...

- Give end-users security **controls** they can **understand** and privacy they can **control** for the **dynamic, pervasive** computing environments of the future.”

— *Computing Research Association 2003*

- 对于安全问题，技术不能提供全部的解决方案，人的因素一直被忽视，安全技术人员并不非常关心用户需要什么
- 我们需要考量用户如何同系统进行交互
- 结合HCI（人机交互）与信息安全
- 超越UI：改变用户和开发者习惯和思路

HCISec

为什么需要可用安全

- 开发人员和用户对安全和可用的认识是不同的
- 不同的用户的认识也是不同的
- 安全增加了障碍： *If you want security, you must be prepared for inconvenience*
- 安全与可用不可调和
- 不可用的安全是容易的，可用的安全是非常困难的

- 用户不理解数据、软件和系统的重要性
 - 用户不了解什么资产处在危险中
 - 用户不理解他们的行为处在风险中
 - 用户什么都不知道自己在做什么
-
- 教育训练
 - 设计时就需要考虑可用性
 - 设计一个可用的安全系统

可用安全面临挑战

- 安全是次要任务，没有人买计算机是为了安全
 - 配置安全工具的时间对于用户来说是“白白浪费”
-
- 安全系统和方案经常是比较复杂的，用户难于理解，执行经常出现错误
-
- 用户不知道是什么时间和如何执行安全相关的任务
 - 用户没有动机执行安全相关的任务
 - 用户没有能力做安全决策

可用安全的目标

- 对于需要执行的安全任务是可靠的
- 能指出如何成功的执行安全任务
- 不会出现危险的错误
- 使用和交互中足够舒适

用户为中心的设计

-
- 安全不可见
 - 安全和隐私可理解
 - 训练用户
 - 不期望用户做一些用户无法选择的决定
 - 自动化系统更加可预期和准确

用户和安全拥有足够的通信

文本口令

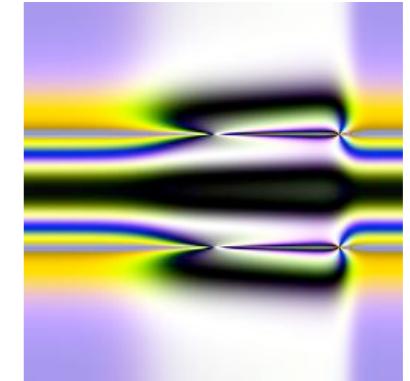
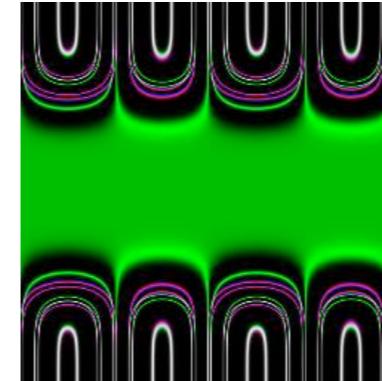
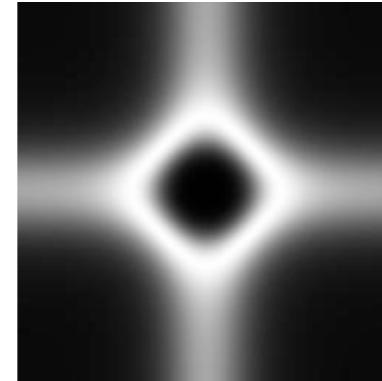
- 文本口令是研究与使用最为广泛的身份认证方法，最常用的形式：用户名 + 口令
- 选择原则：易于记忆，难于猜中或者发现，抗分析能力强

Table 1. Password characteristics.

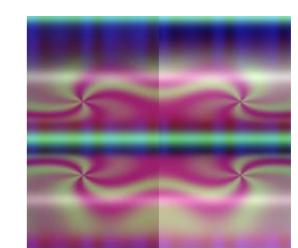
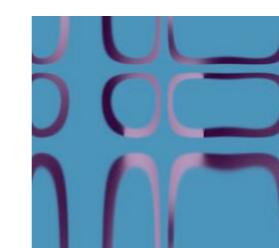
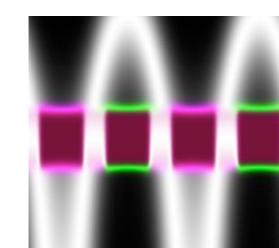
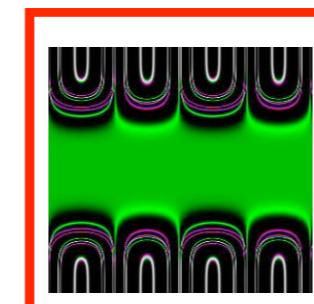
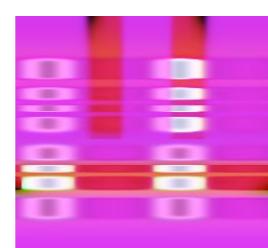
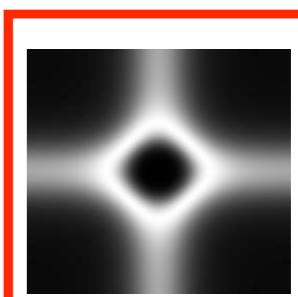
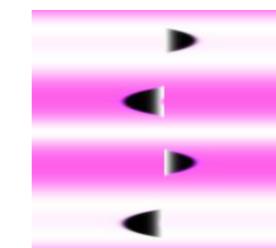
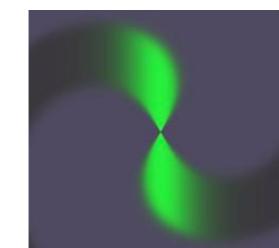
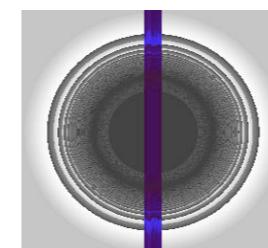
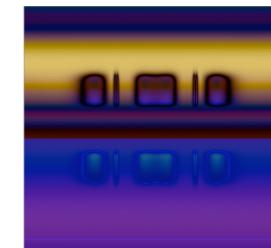
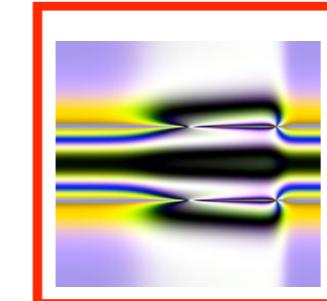
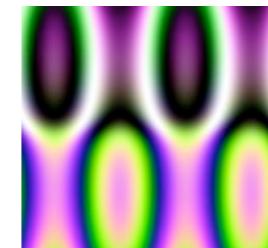
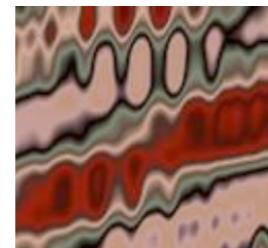
Password characteristic	Security focus	Usability focus
Length	Longer	Shorter
Composition	Heterogeneous characters	Homogeneous characters
Uniqueness	Forbid reuse	Common passwords
Change frequency	Often	Seldom

Déjà Vu

训练



挑战



PassFaces

- 系统从脸型数据库中随机选取5个人的脸型，显示给用户，并给用户一定时间让用户熟悉（注册）
- 系统每次显示9个脸型（其中仅有一个是注册时显示给用户的）让用户选择，这样的选择共进行5次
- 如果用户正确的选择了所有的5个脸型，用户身份认证成功，否则失败（登入）



PatternLock

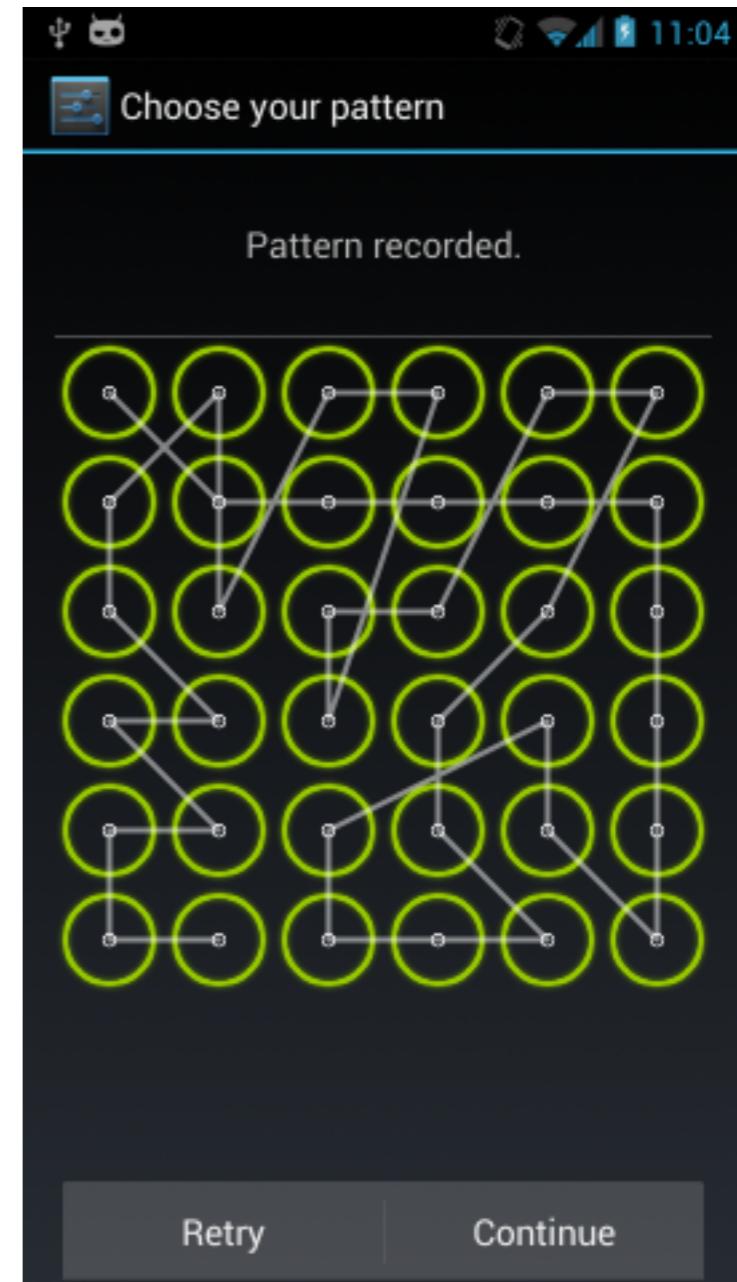
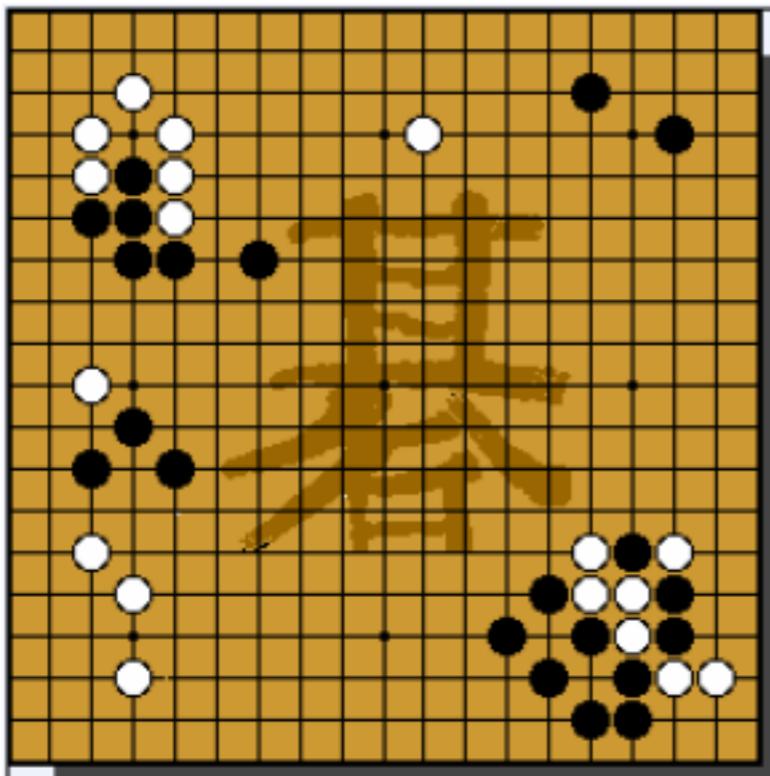
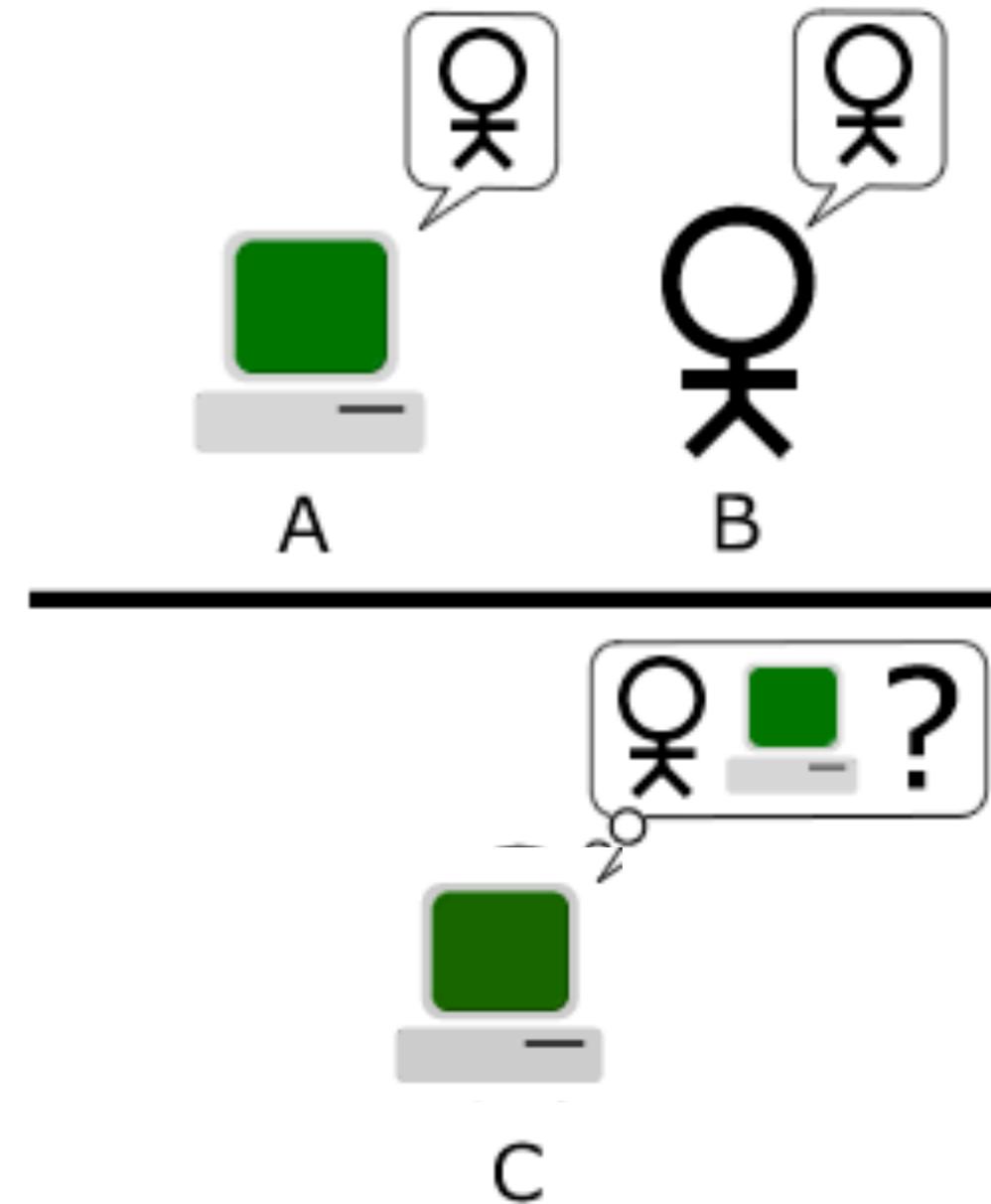
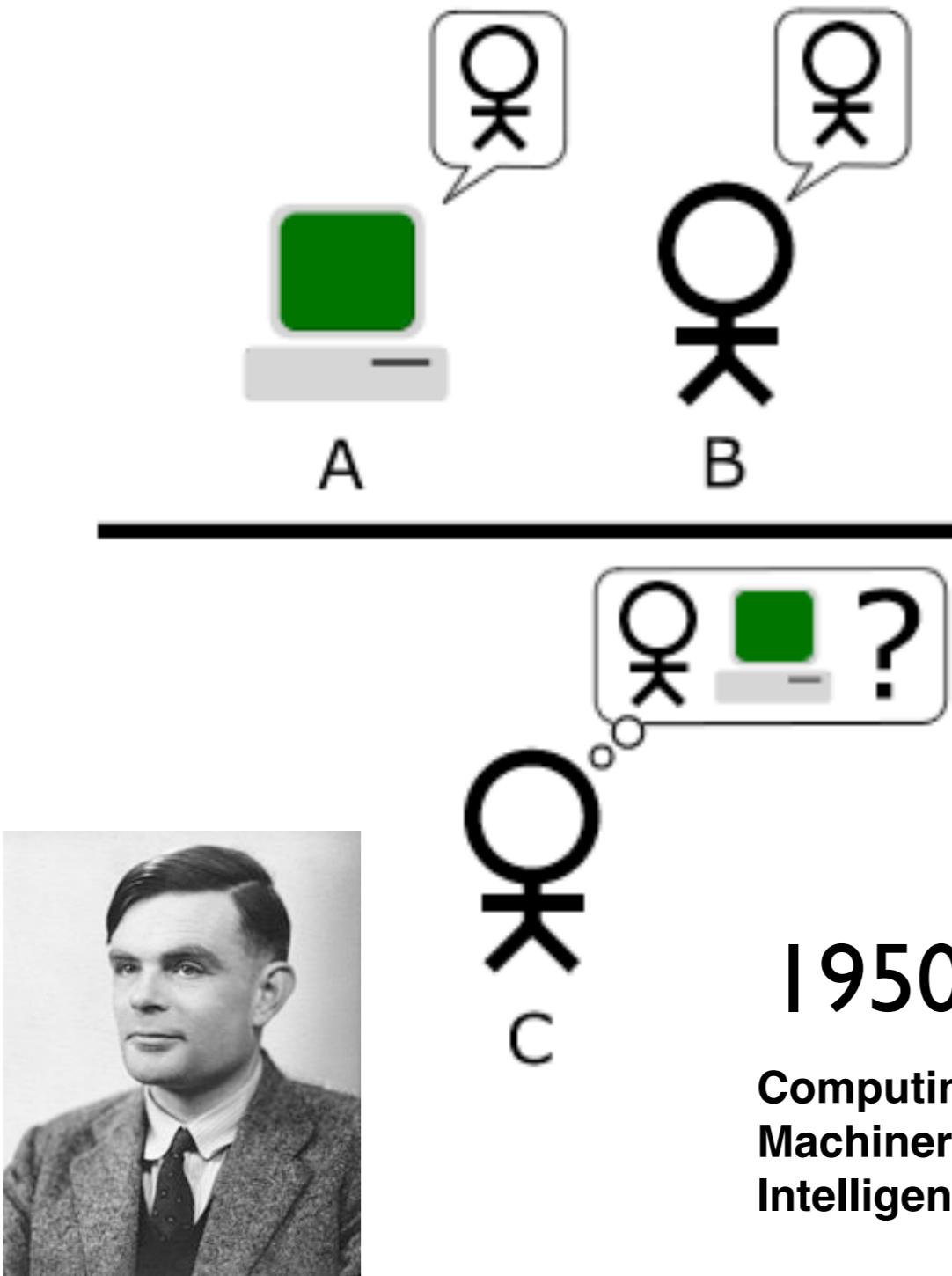


Figure 1 Go game

AI >>> 信息安全

图灵测试 vs 反向图灵测试

http://en.wikipedia.org/wiki/Turing_test



Human Computation

Luis von Ahn

- Carnegie Mellon University

* Luis von Ahn

* Manuel Blum

* Nicholas J. Hopper

* John Langford



2000年

capture

2008年

商标申请没有被批准



2005年
博士毕业
Human Computing

<http://vonahn.blogspot.com/>

2007年



2011年



duolingo.com

2006年

[http://video.google.com/videoplay?
docid=-8246463980976635143](http://video.google.com/videoplay?docid=-8246463980976635143)

Human Computation

CAPTCHA定义

● CAPTCHA

Completely
Automated
Public
Turning test to tell
Computers and
Humans
Apart

<http://www.captcha.net/>

<http://en.wikipedia.org/wiki/CAPTCHA>

Name

First Last

Choose your username @gmail.com

Create a password

Confirm your password

Birthday

Month Day Year

Gender

I am...

Mobile phone

+86

Other email address

Prove you're not a robot

reCaptcha rebuilt:

Type the two pieces of text:

CAPTCHA vs AI

- 设计CAPTCHA

- * Email

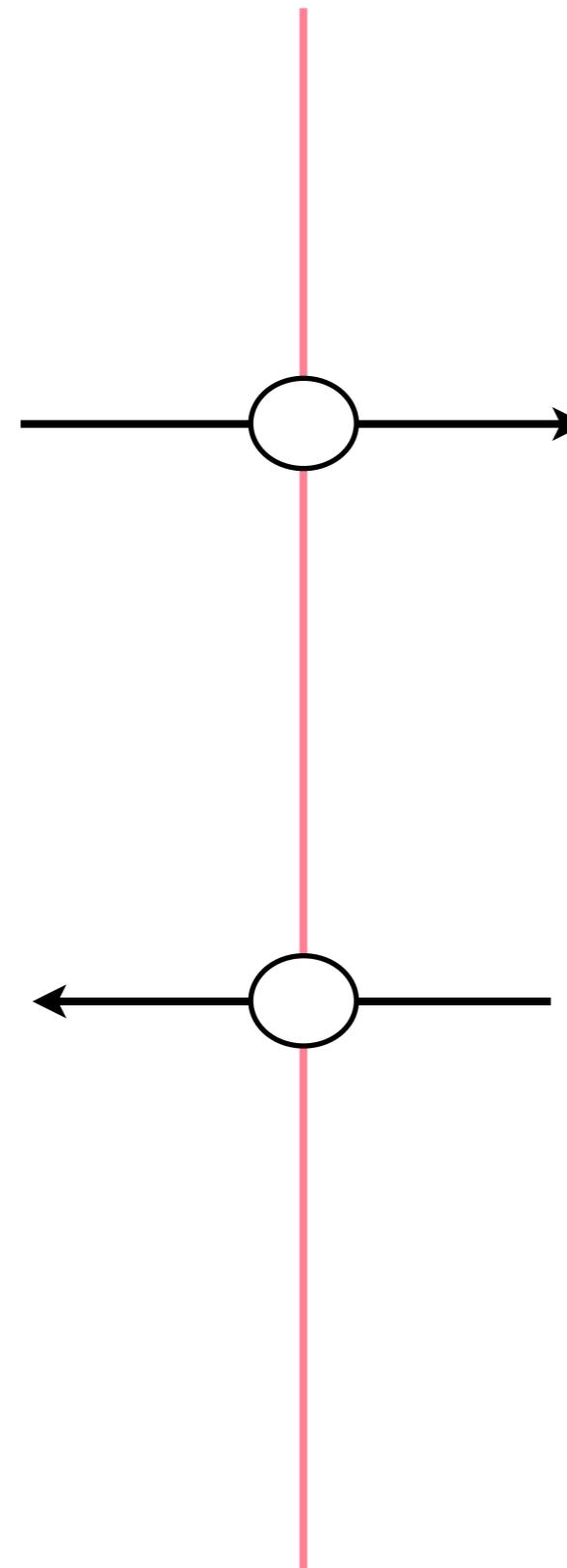
- * BBS

- * Blog

- * SNS

- * Security

- * ...



- 攻击CAPTCHA

- * 垃圾信息生产者

- * 僵尸网络掌握者

- * 打码等其余攻击者

- * 自动化测试人员

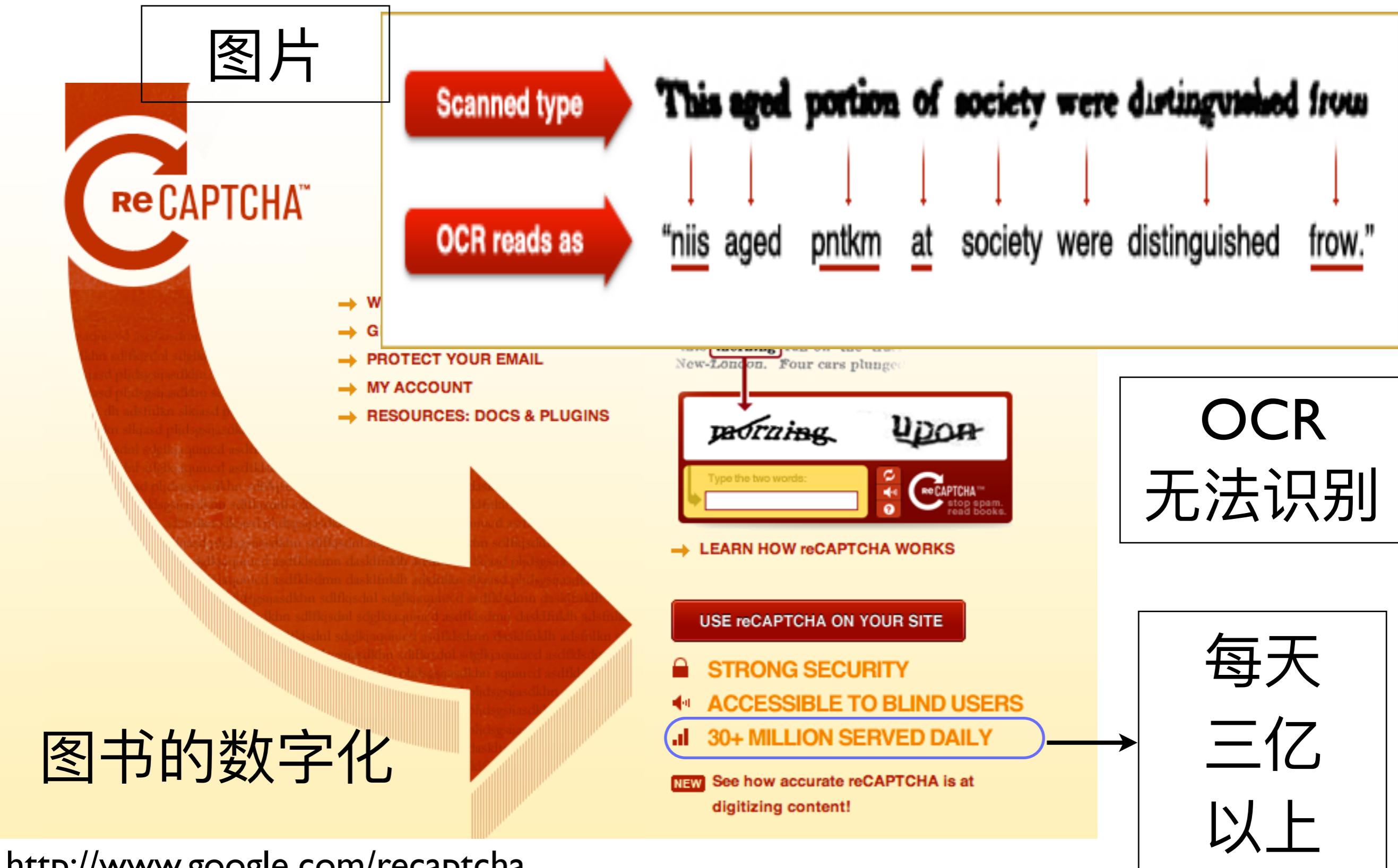
- * ...

AI难题

机器学习

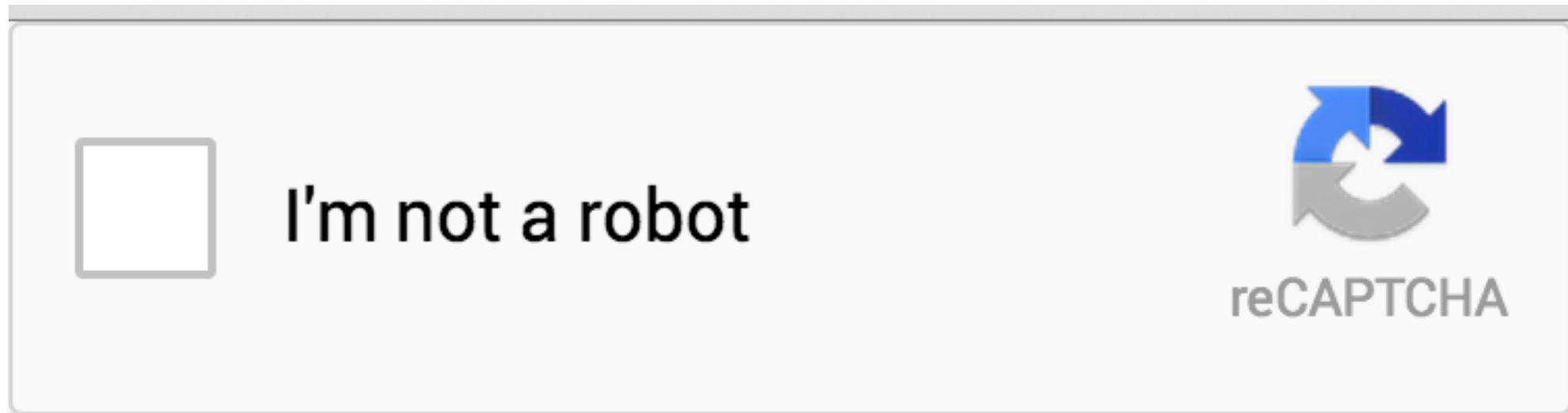
Human Computation

ReCAPTCHA



Human Computation

NoCAPTCHA



A screenshot of a standard image-based CAPTCHA. At the top, it says "I'm not a robot" next to a checkbox and the reCAPTCHA logo. Below this, the text "Select all images below that match this one:" is displayed. A large image of a turkey is shown, followed by a grid of smaller images for selection. The images include various turkeys, a bowl of cranberry sauce, bread rolls, purple flowers, a dog, a cat, a guinea pig, and some green plants. At the bottom, there are three small icons (refresh, headphones, info) and a "Verify" button.

A screenshot of another standard image-based CAPTCHA. It has the same top elements as the first one. Below, it says "Select all images below that match this one:" and shows a large image of a cat. Below it is a grid of smaller images: a cat, a dog, a dog, a dog, a cat, a cat, a guinea pig, and a plant. At the bottom, there are three small icons and a "Verify" button.

A screenshot of the NoCAPTCHA text-based CAPTCHA. It has the "I'm not a robot" checkbox and reCAPTCHA logo at the top. Below, it says "Type the text" in a large, bold, blue font. A blurred image of a house number "250" is shown for text recognition. At the bottom, there are three small icons and a prominent blue "Verify" button.

Amazon Mechanical Turk

The screenshot shows the homepage of the Amazon Mechanical Turk website. At the top, there's a navigation bar with tabs for 'Your Account' (selected), 'HITs' (highlighted in yellow), and 'Qualifications'. Below the navigation is a secondary menu with links to 'Introduction', 'Dashboard', 'Status', and 'Account Settings'. The main content area features a yellow gradient background. A central message reads: 'Mechanical Turk is a marketplace for work. We give businesses and developers access to an on-demand, scalable workforce. Workers select from thousands of tasks and work whenever it's convenient.' It also displays the statistic '433,482 HITs available. [View them now.](#)'. On the left, under the heading 'Make Money by working on HITs', it says: 'HITs - Human Intelligence Tasks - are individual tasks that you work on. [Find HITs now.](#)' Below this, a section titled 'As a Mechanical Turk Worker you:' lists three benefits: 'Can work from home', 'Choose your own work hours', and 'Get paid for doing good work'. It includes a flow diagram with three circles: 'Find an interesting task' (with a blue arrow pointing to 'Work'), 'Work' (with a blue gear icon), and 'Earn money' (with a dollar sign icon). A 'Find HITs Now' button is at the bottom. On the right, under the heading 'Get Results from Mechanical Turk Workers', it says: 'Ask workers to complete HITs - Human Intelligence Tasks - and get results using Mechanical Turk. [Register Now](#)'. Below this, a section titled 'As a Mechanical Turk Requester you:' lists three benefits: 'Have access to a global, on-demand, 24 x 7 workforce', 'Get thousands of HITs completed in minutes', and 'Pay only when you're satisfied with the results'. It includes a flow diagram with three orange circles: 'Fund your account' (with a plus sign icon), 'Load your tasks' (with a checklist icon), and 'Get results' (with a star icon). A 'Get Started' button is at the bottom.

土耳其机器人（Mechanical Turk）这个名字是从18世纪的一个国际象棋游戏机器人得来的，这个机器人在欧洲与名人比赛下象棋，其实在机器人中有一个真人躲在一个秘密隔间中，是他在操纵机器人和玩象棋。

亚马逊（Amazon）选择土耳其机器人（Mechanical Turk）这个名字来命名他们的网络服务，是因为人类的智慧隐藏在最终用户，这样服务看起来就像是自动进行的。



Human Computation

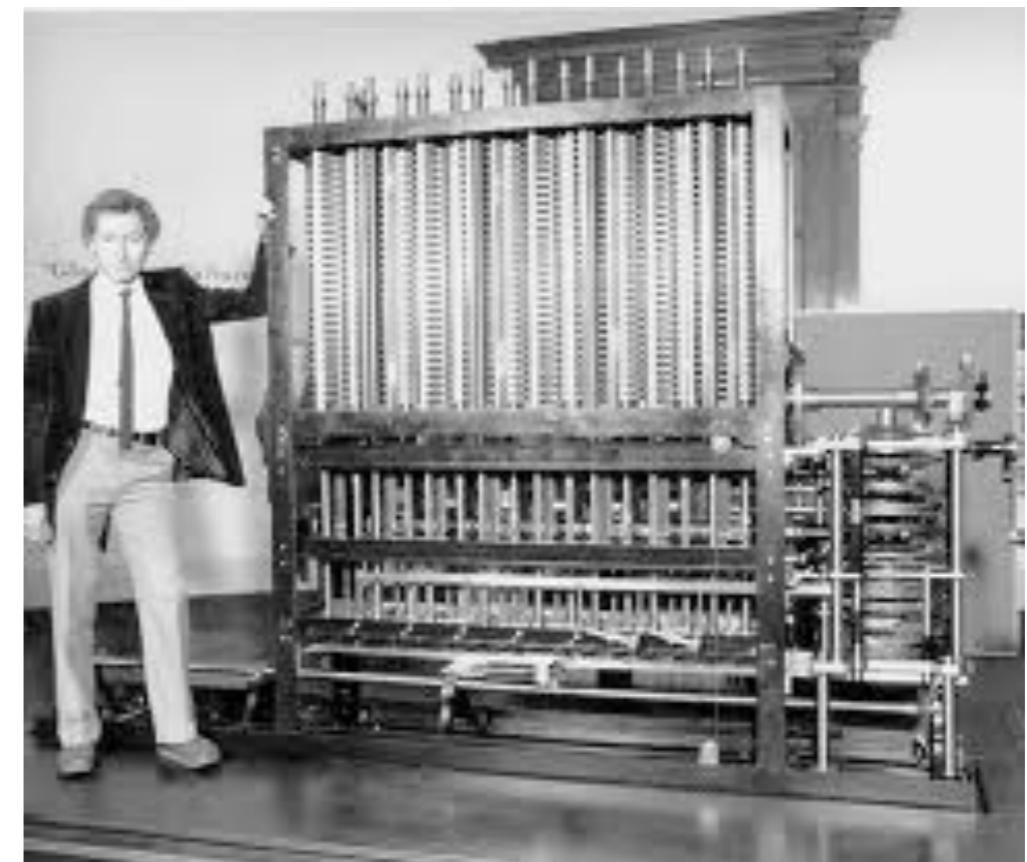
Computation 历史



计算公式 → 任务分解



操作指南 → 结果合并



- 计算
 - * 使用算法映射输入到输出的过程
- Human Computation 2005
 - * 人来执行的计算 → 人工智能难题

思考

现在有哪些Human Computation应用？

Human Computation产生需要什么基础？

- 现在依然存在许多人工智能难题
 - * 人很容易解决
 - * 但是复杂的计算机算法很难解决
- 常见的人工智能难题
 - * 感知（目标识别、分类）
 - * 自然语言分析（观点分析、翻译）
 - * 认知（计划、推理）

Human Computation

图像识别难题



Tag系统 Q&A系统

Human Computation

Human Computation

```
function quicksort(A)
    initialize empty lists L and G
    if (length(A) ≤ 1)
        return A
    pivot = A.remove(find_pivot(A));
    for x in A
        if compare(x, pivot)
            L.add(x)
        else
            G.add(x)
    return concatenate(quicksort(L), pivot, quicksort(G))

function pivot(A)
    return randomIndex(A);

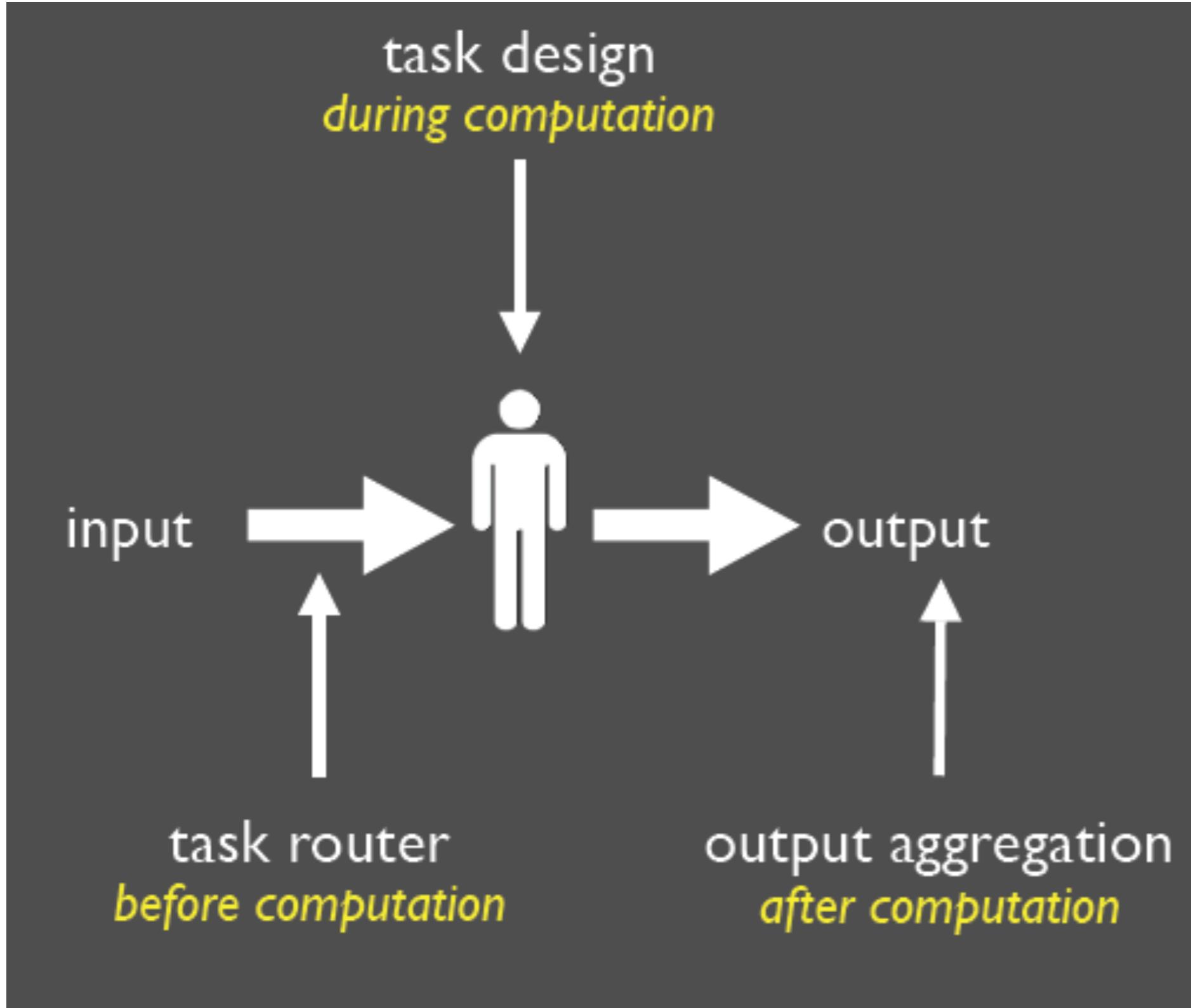
function compare(x, pivot)
    return human_compare(x, pivot)
```

Games with a Purpose



Human Computation

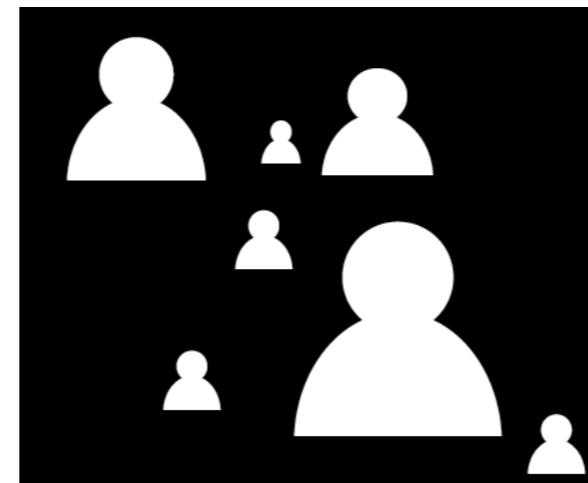
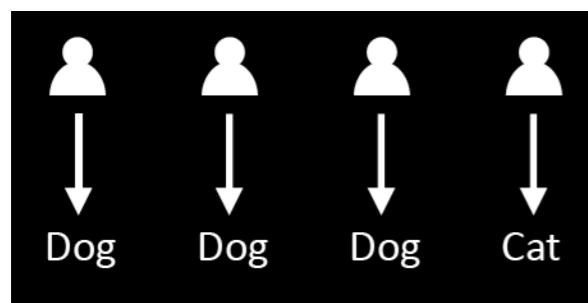
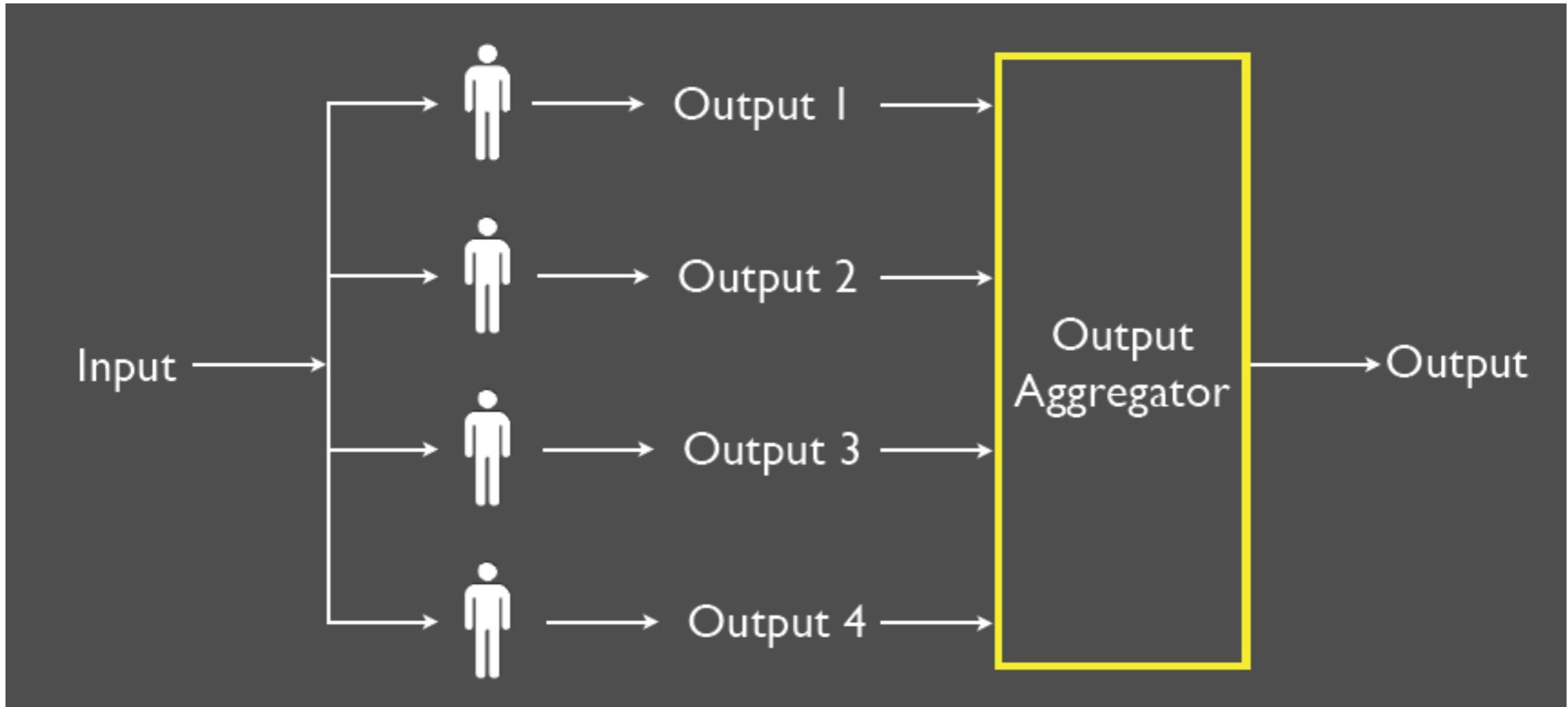
算法正确性



- Money
- Access
- Game
- Volunteer
- Learning

Human Computation

结果汇集



- Web上的图像识别是一个主要的技术挑战
- 大量图片存在，但是文本描述很少，自动识别很不准确
- 人来做标记是一个无奈的选择

Human Computati on

游戏

- 每周现在有20亿用户玩在线游戏
- 21岁美国人万游戏时间，平均一生5年



Human Computati on

ESP游戏

- 两个用户同时独立的标记一个图片
- 如果标记一致会得到奖励

score 0  **ESP Game**
Concentrate... time 2:46

What do you see?

taboo words dog



guesses

Player 1 guesses: purse
Player 1 guesses: bag
Player 1 guesses: brown

Player 2 guesses: handbag

Player 2 guesses: purse
Player 2 guesses: brown

Success! Agreement on “purse”

Play Anonymously

+ submit → pass



Human Computati on

Amazon Mechanical Turk

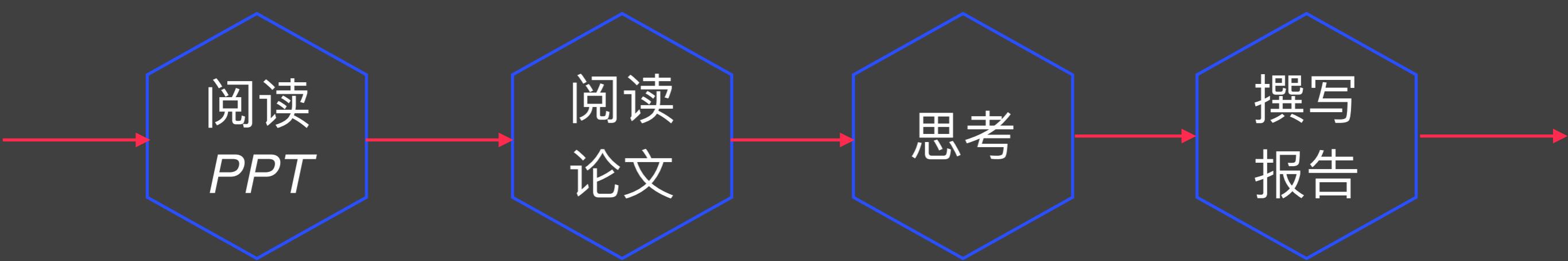
The screenshot shows the homepage of the Amazon Mechanical Turk website. At the top, there's a navigation bar with tabs for 'Your Account' (selected), 'HITs' (highlighted in yellow), and 'Qualifications'. Below the navigation is a secondary menu with links to 'Introduction', 'Dashboard', 'Status', and 'Account Settings'. The main content area features a yellow gradient background. A central message reads: 'Mechanical Turk is a marketplace for work. We give businesses and developers access to an on-demand, scalable workforce. Workers select from thousands of tasks and work whenever it's convenient.' It also displays the statistic '433,482 HITs available. [View them now.](#)'. On the left, under the heading 'Make Money by working on HITs', it says: 'HITs - Human Intelligence Tasks - are individual tasks that you work on. [Find HITs now.](#)' It lists benefits for workers: 'As a Mechanical Turk Worker you:' with bullet points: 'Can work from home', 'Choose your own work hours', and 'Get paid for doing good work'. Below this is a flow diagram: 'Find an interesting task' (blue circle with gears) leads to 'Work' (blue circle with a gear icon) which leads to 'Earn money' (blue circle with a dollar sign). A 'Find HITs Now' button is at the bottom. On the right, under the heading 'Get Results from Mechanical Turk Workers', it says: 'Ask workers to complete HITs - Human Intelligence Tasks - and get results using Mechanical Turk. [Register Now](#)'. It lists benefits for requesters: 'As a Mechanical Turk Requester you:' with bullet points: 'Have access to a global, on-demand, 24 x 7 workforce', 'Get thousands of HITs completed in minutes', and 'Pay only when you're satisfied with the results'. Below this is another flow diagram: 'Fund your account' (orange circle with a plus sign) leads to 'Load your tasks' (orange circle with a document icon) which leads to 'Get results' (orange circle with a star icon). A 'Get Started' button is at the bottom.

土耳其机器人（Mechanical Turk）这个名字是从18世纪的一个国际象棋游戏机器人得来的，这个机器人在欧洲与名人比赛下象棋，其实在机器人中有一个真人躲在一个秘密隔间中，是他在操纵机器人和玩象棋。

亚马逊（Amazon）选择土耳其机器人（Mechanical Turk）这个名字来命名他们的网络服务，是因为人类的智慧隐藏在最终用户，这样服务看起来就像是自动进行的。



课后作业



要求阅读如下论文，写论文阅读报告

In IEEE SP 2016

2016 IEEE Symposium on Security and Privacy

Beauty and the Beast: Diverting modern web browsers to build unique browser fingerprints

Pierre Laperdrix
INSA-Rennes & INRIA
Rennes, France
pierre.laperdrix@insa-rennes.fr

Walter Rudametkin
University of Lille & INRIA
Lille, France
walter.rudametkin@univ-lille1.fr

Benoit Baudry
INRIA
Rennes, France
benoit.baudry@inria.fr

<https://ieeexplore.ieee.org/document/7546540/>

选择一篇引用该文的论文，阅读该论文
并在论文阅读报告中简单介绍

- 1、论文概述
- 2、主要收获
- 3、存在疑问
- 4、所思所感
- 5、一篇引用

11月20日晚上
12点前提交

謝謝 !

Huijing Sun

sunhp@ss.pku.edu.cn

<https://huijingsun.github.io>