课程简介

北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

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：每周三、下午*14*点到*17*点 *(3204)*
  - ✴ 时间区间：*10*月*15*日、*12*月*3*日、*12*月*10*日
  - ✴ 课程主页：*https://huipingsun.github.io/ics2019*

- 课程内容
  - ✴ 信息安全经济学＋可用安全＋人计算
  - ✴ 区块链简介、基础、应用、挑战等

两次课后作业
论文阅读报告

信息安全需要多学科的支持

- 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.

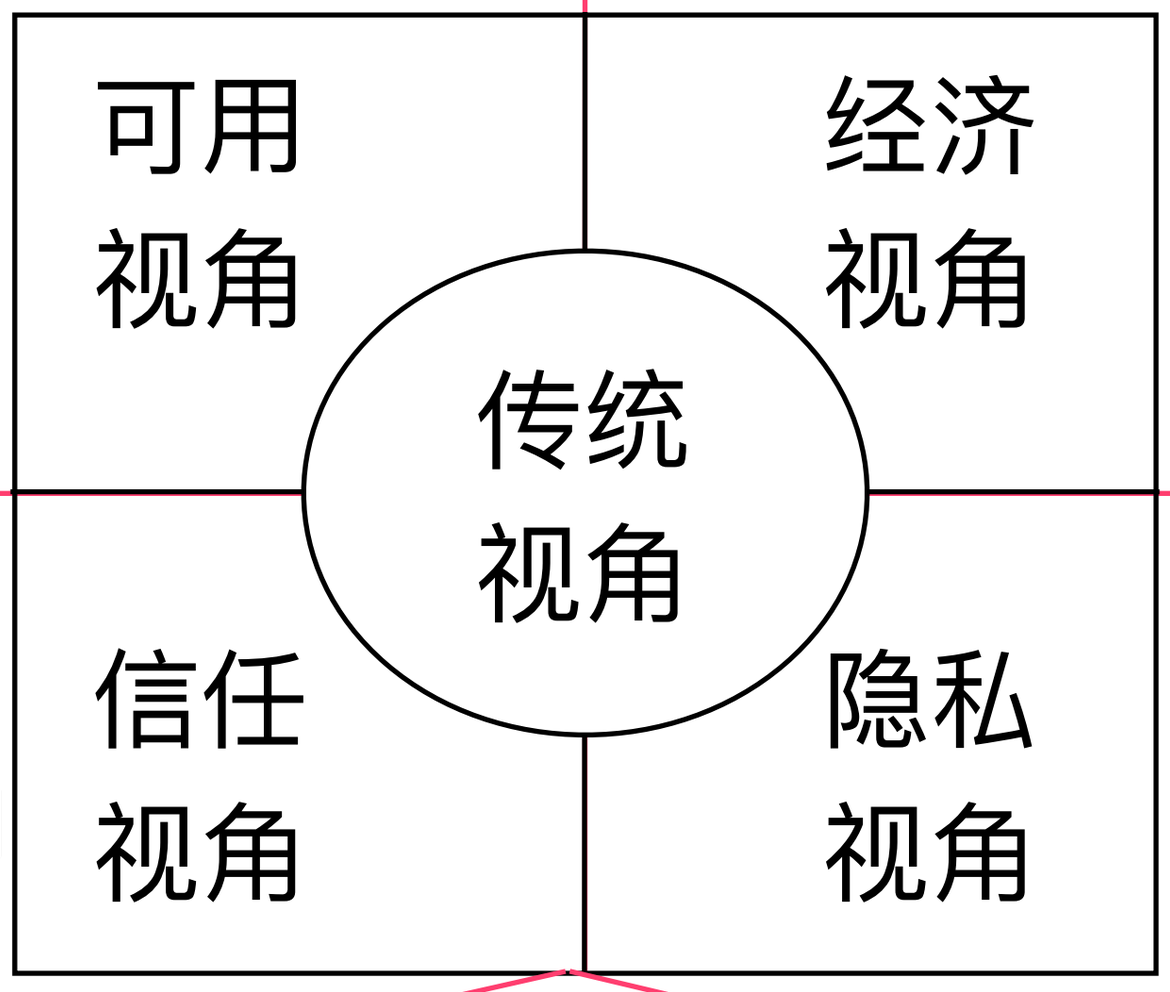
信息安全的不同视角：密码运算

- **可用：**

  ✴存储、维护、管理

- **经济：**

  ✴风险多大，收益多大



- **信任：**

  ✴信任哪些密钥

- **隐私：**

  ✴托管

- **传统：**

  ✴速度快、准确、安全

信息安全＋经济学

InfoSecEcon 信息安全: 技术视角 vs 经济学视角

- 防火墙
- 入侵检测
- 杀病毒
- 密码算法
- 身份认证
- … …

- 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
- … …

差别定价

- 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

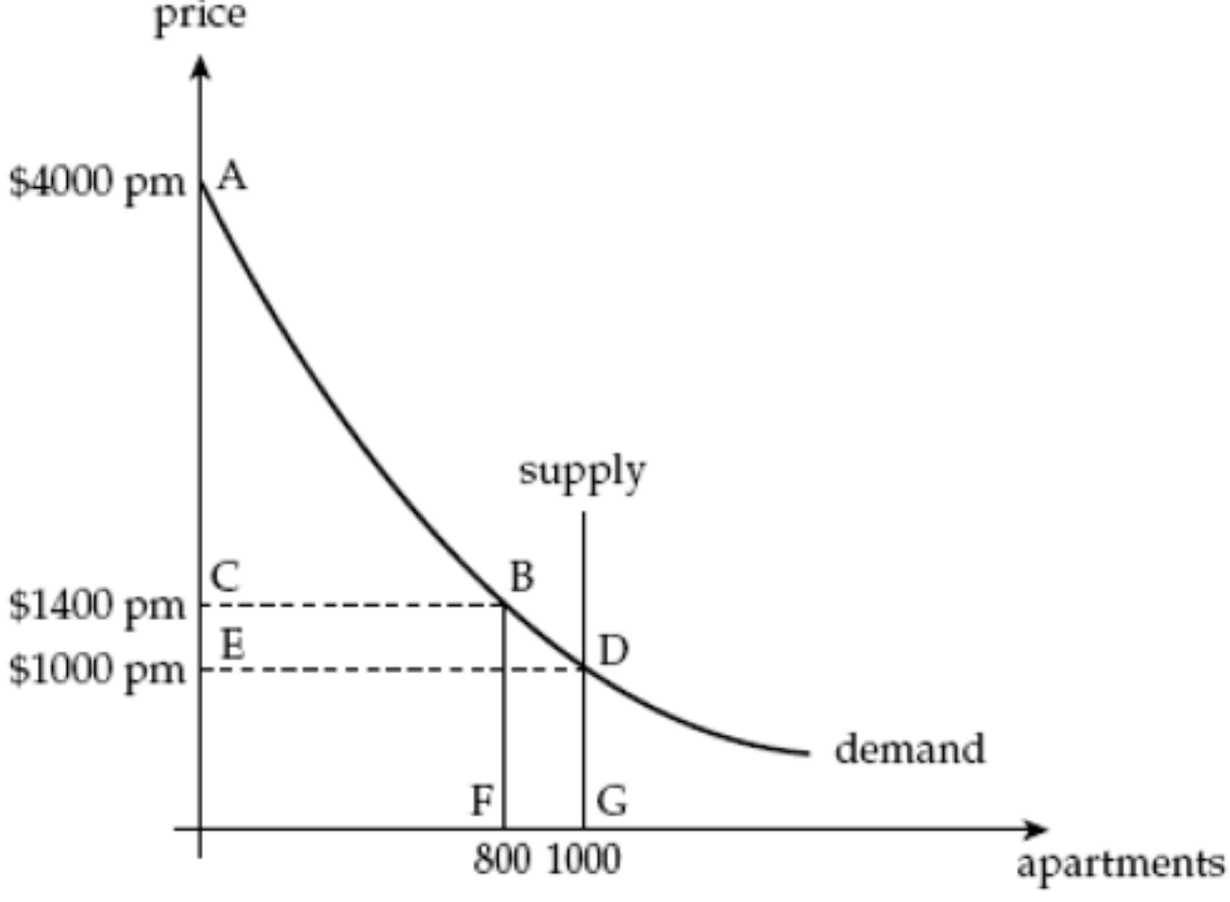


Figure 7.1: The market for apartments

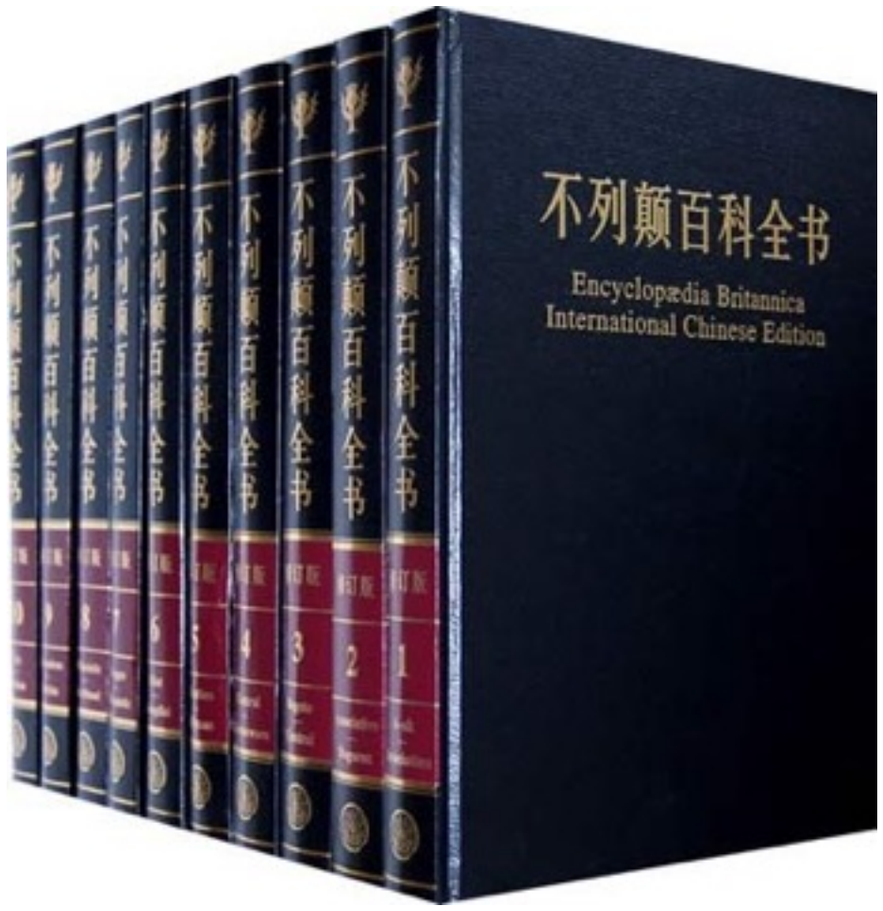
公用品悲剧

非竞争性非排他性的商品

*Internet*安全很多时候也是公用品

信息经济学：信息的价格

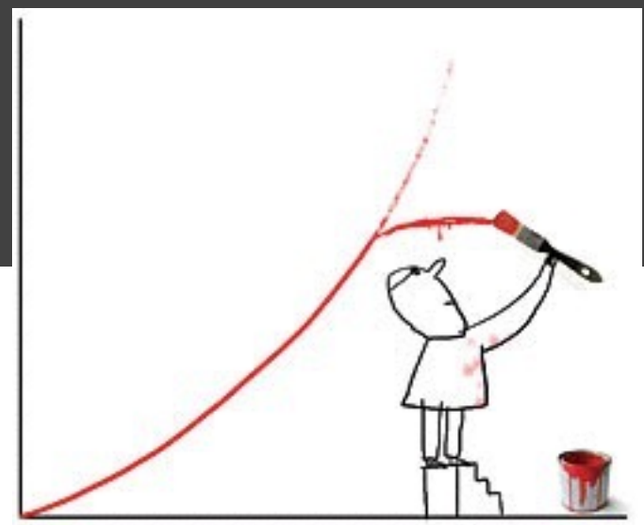
- 商品的价格在完全竞争市场均衡状态下等于边际成本
- 信息的边际成本等于0，复制基本无成本



大英百科全书

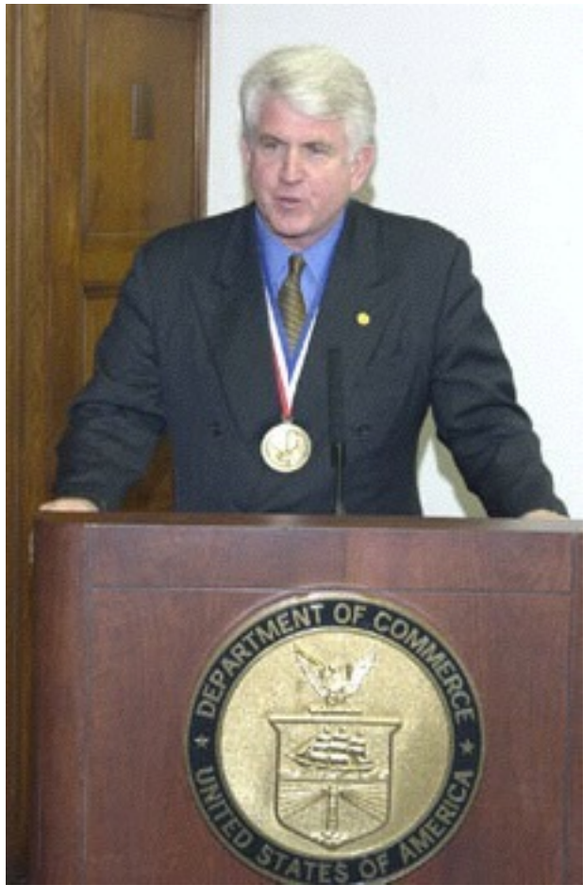
维基百科

Metcalfe法则

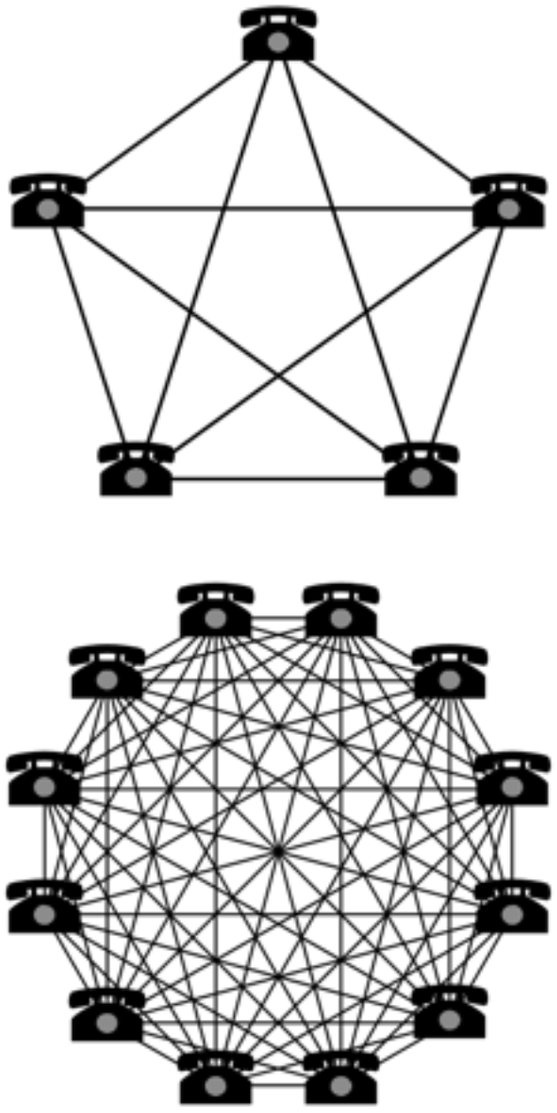


- 梅特卡夫法则：网络价值以用户的数量的平方的数量增长

乔治 吉尔德



3Com创始人



网络外部性 – 锁定

- 连接一个网络的价值取决于已经连接到该网络用户的数量
- 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

信息技术市场

- 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

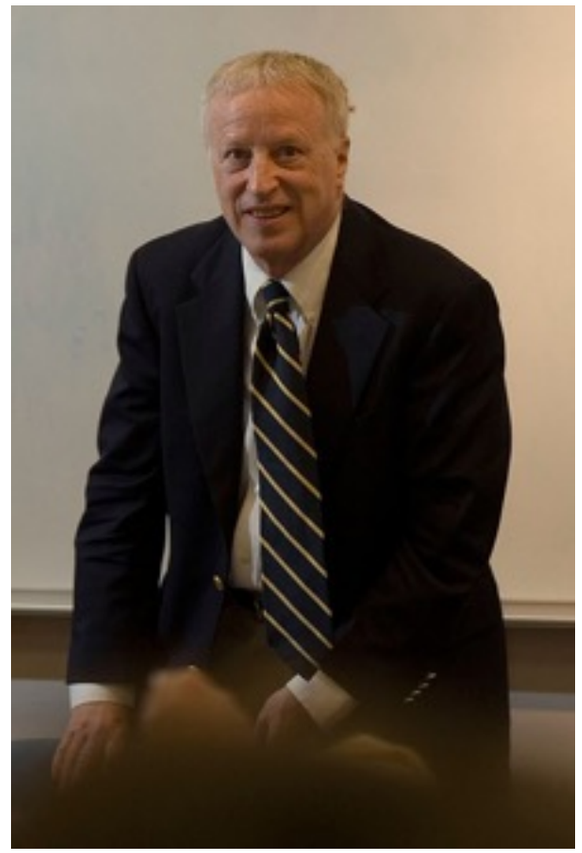
信息不对称

- 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

市场上都是lemon

>>卖方<<

知道是peach还是lemon

卖peach亏本
卖lemon挣钱

市场失灵　信誉　担保　信息公开　反垄断

信息安全柠檬市场

- 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
- 安全信息系统的价格应该高于不安全信息系统的价格

>>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

什么时间考虑信息安全

- 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

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心，但并不保护个人信息

信息安全事件披露

- 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

信息安全模型

- 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

策略性攻击

- 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

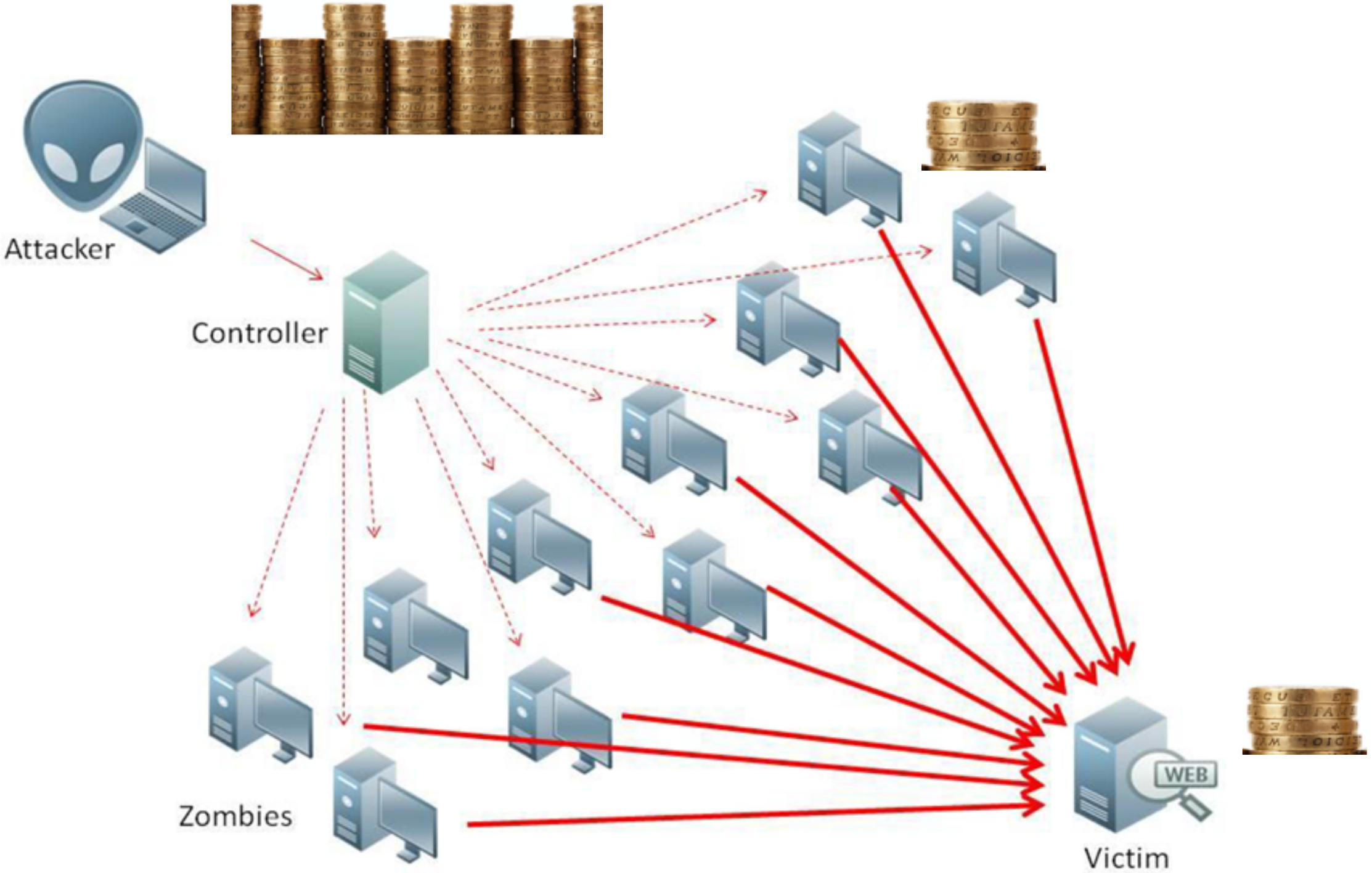
- 一个漏洞被发现堵上，攻击者会发现下一个漏洞
- 一个ISP提高了防御能力，攻击者会转向下一个
- P2P被分配自己感兴趣的内容，更愿意提高自己抵御能力
- P2P每个节点自我保护比总体保护更廉价

攻击与抵御的不对等

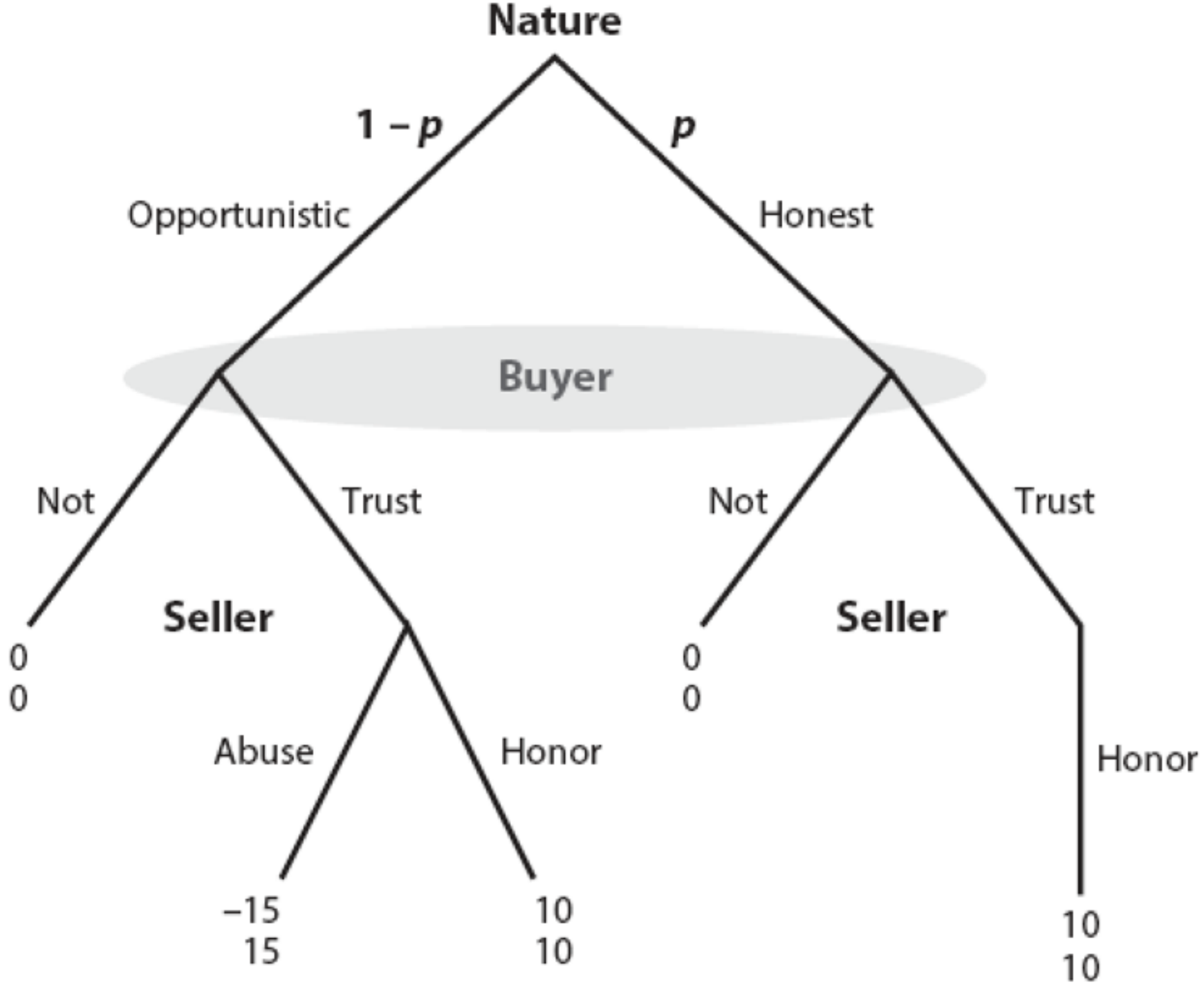
- 攻击者和防御者处于不平等的地位上
- 防御者永远不知道哪个是最弱的一环

- 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


Nature
1 – p
p
Opportunistic
Honest
Buyer
Not
Trust
Not
Trust
Seller
Seller
0
0
0
0
Abuse
Honor
Honor
–15
15
10
10
10
10

Be nice to others who are nice to you

Tit-for-tat

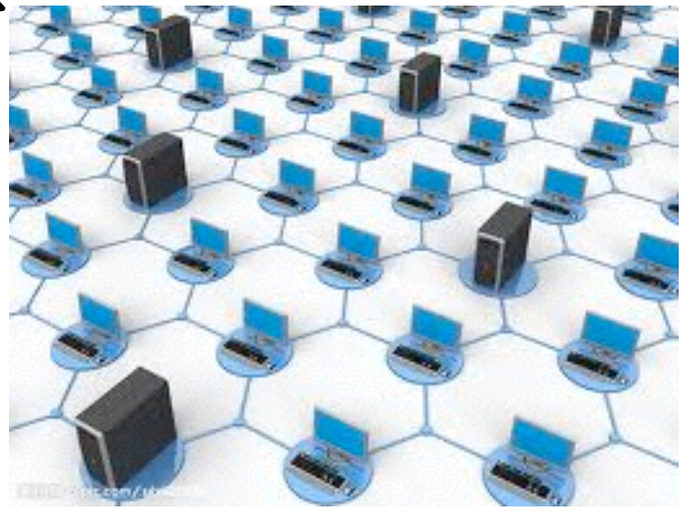
计算环境变迁

?

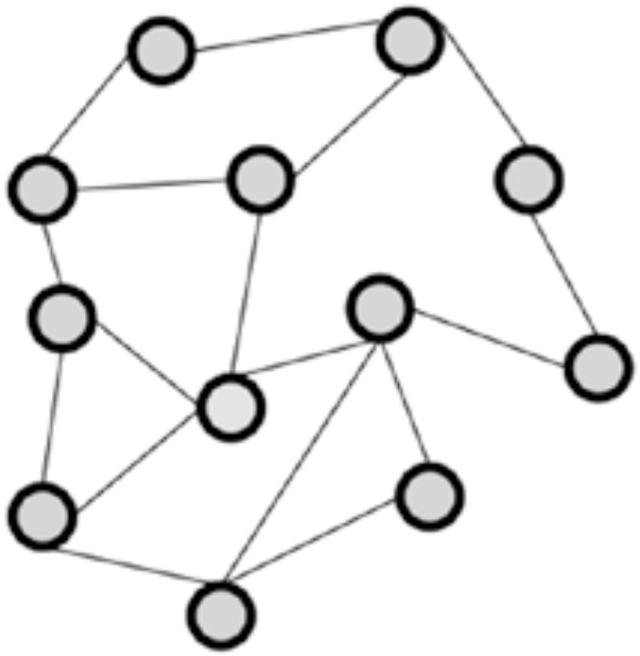
P2P

区块链

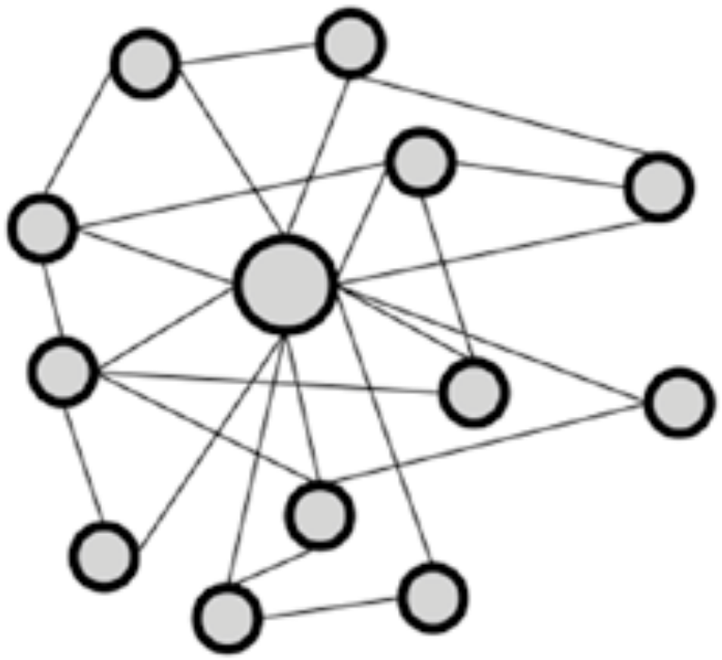
Client-Server

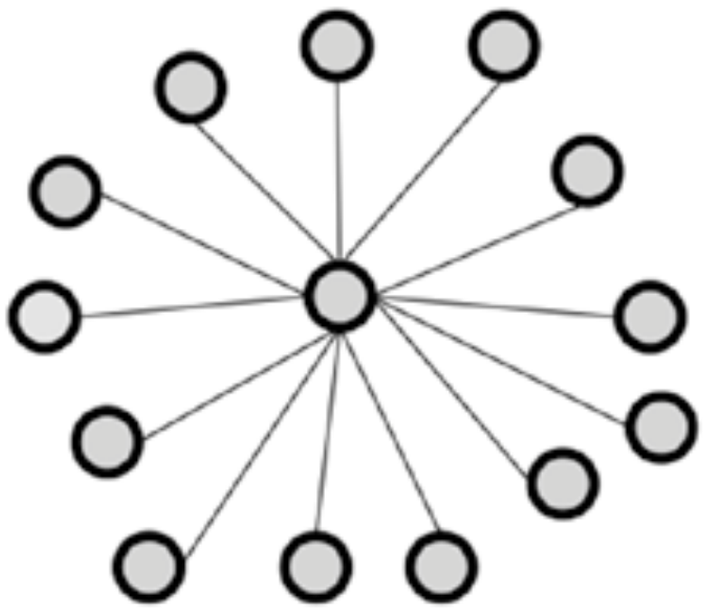


分布式系统

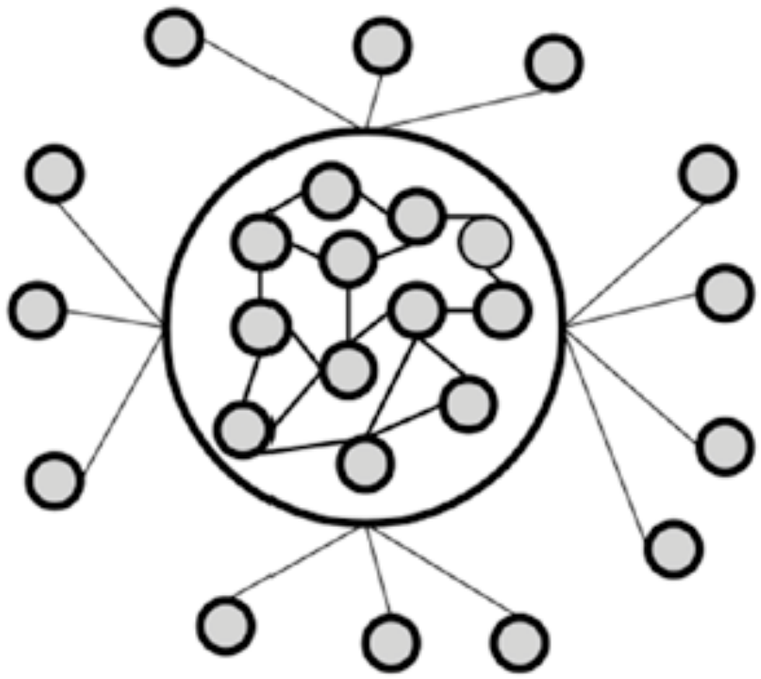


没有纯粹的
中心化系统
或者
分布式系统





Internet
Email
IM
SNS



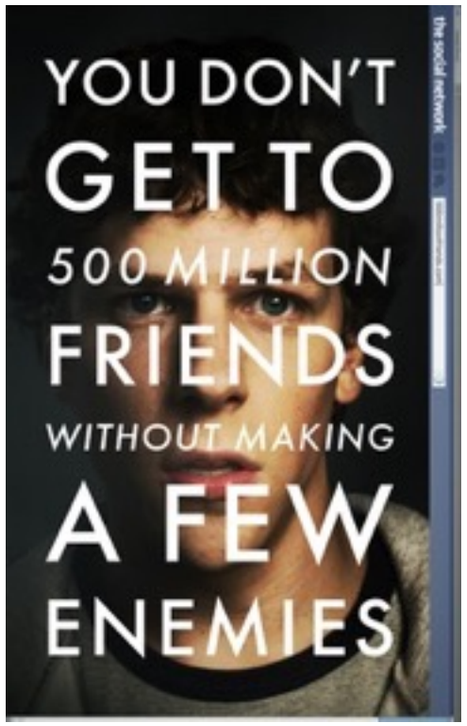
Peer to Peer

napster™

1999

Sean Parker

facebook

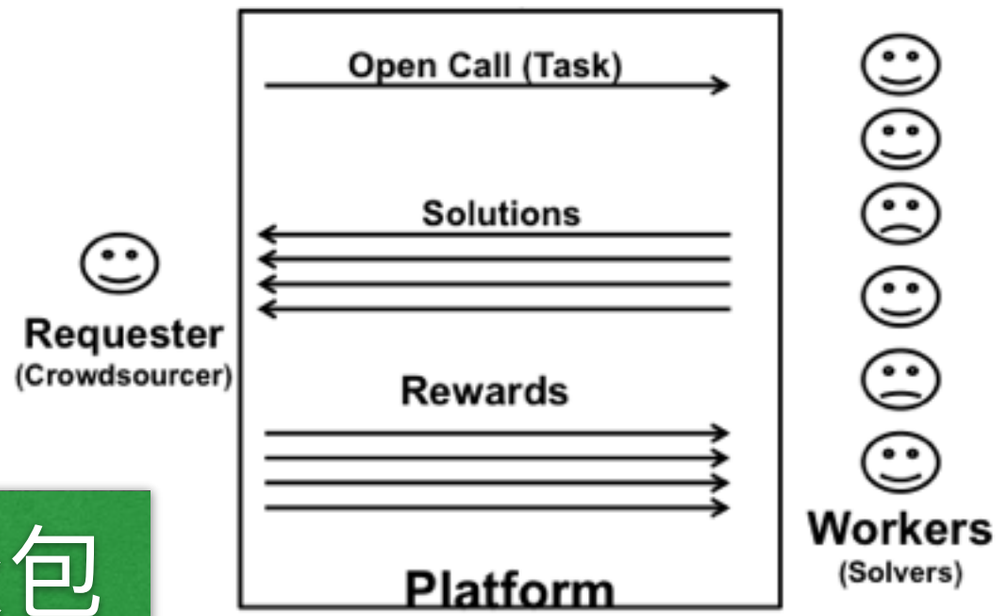


The Social Network

skype™

2003

KaZaA



众包

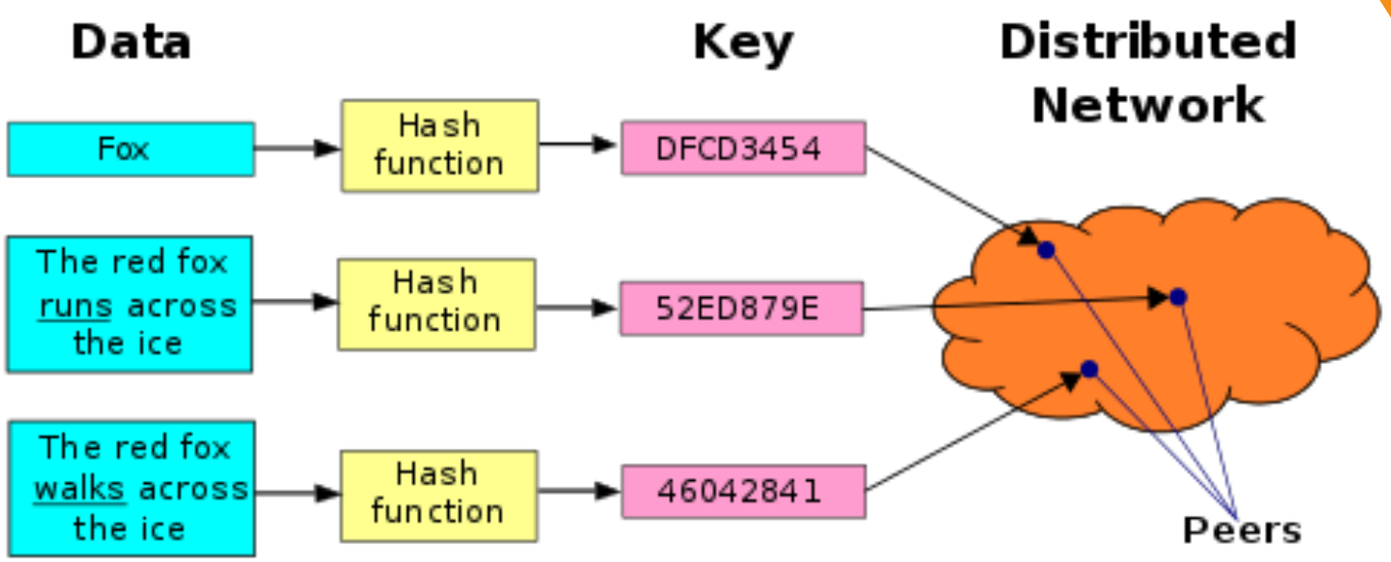
BitTorrent

2001

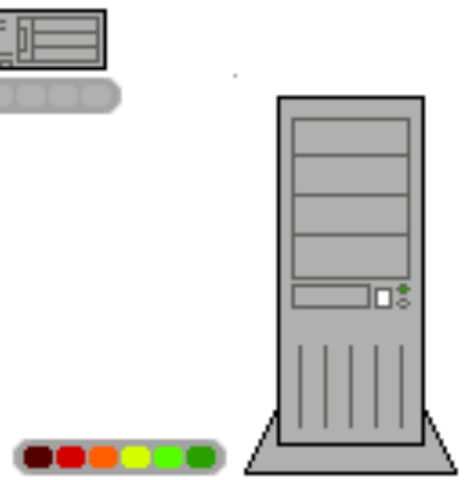
Bram Cohen

BitTorrent

Distributed Hash Table

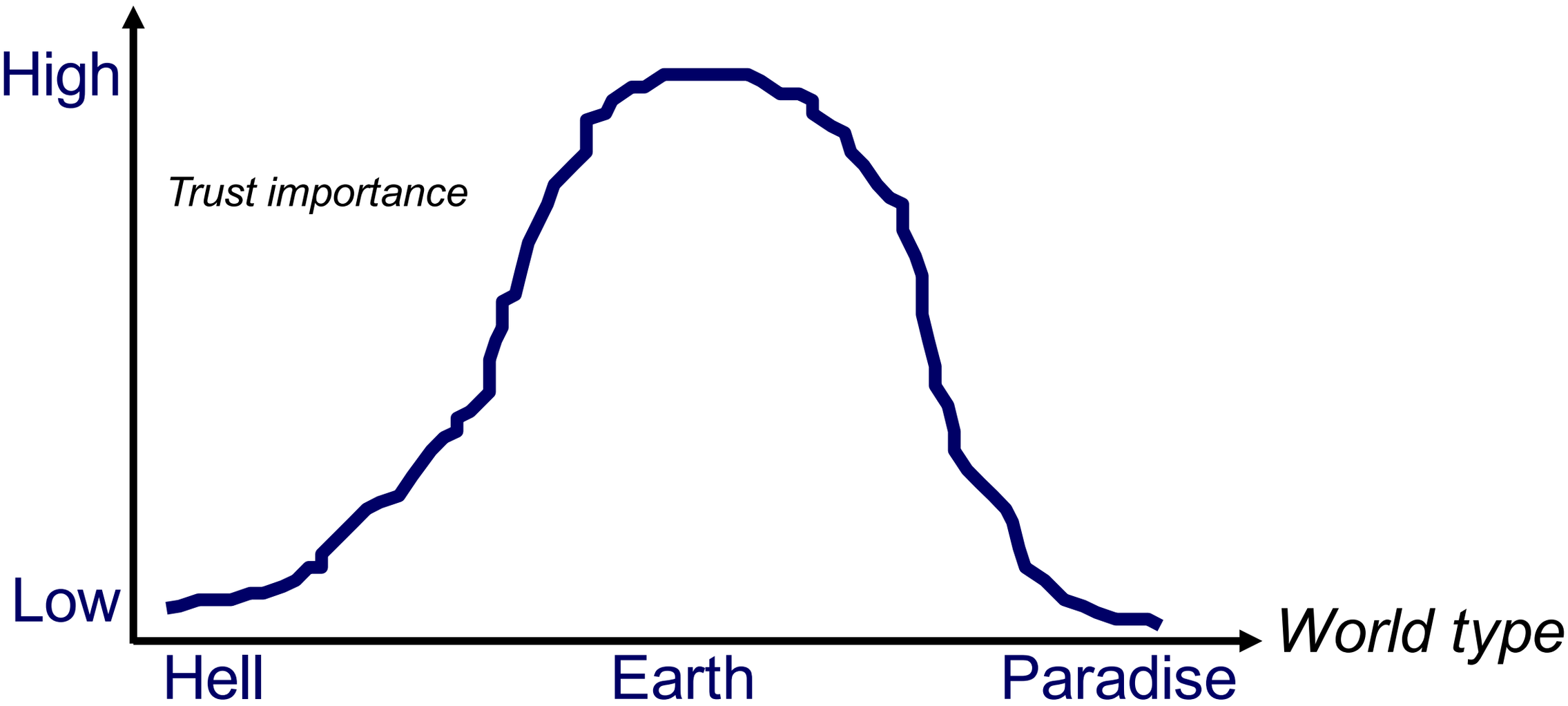


https://en.wikipedia.org/wiki/Distributed_hash_table



激励

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



信任是社会交互的润滑剂

Google Scholar

Paul Resnick

Follow

University of Michigan

social computing, recommender systems, reputation systems, online communities

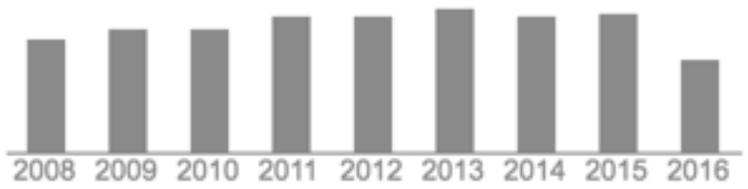
Verified email at umich.edu - Homepage

Title 1–20	Cited by	Year
GroupLens: an open architecture for collaborative filtering of netnews P Resnick, N Iacovou, M Suchak, P Bergstrom, J Riedl Proceedings of the 1994 ACM conference on Computer supported cooperative ...	5446	1994
Recommender systems P Resnick, HR Varian Communications of the ACM 40 (3), 56-58	3844	1997
Reputation systems P Resnick, K Kuwabara, R Zeckhauser, E Friedman Communications of the ACM 43 (12), 45-48	2623	2000
Trust among strangers in internet transactions: Empirical analysis of ebay's reputation system P Resnick, R Zeckhauser The Economics of the Internet and E-commerce 11 (2), 23-25	1840	2002

Google Scholar

Get my own profile

Citation indices	All	Since 2011
Citations	22335	10185
h-index	42	32
i10-index	75	58



Co-authors View all…

John Riedl

Robert E. Kraut

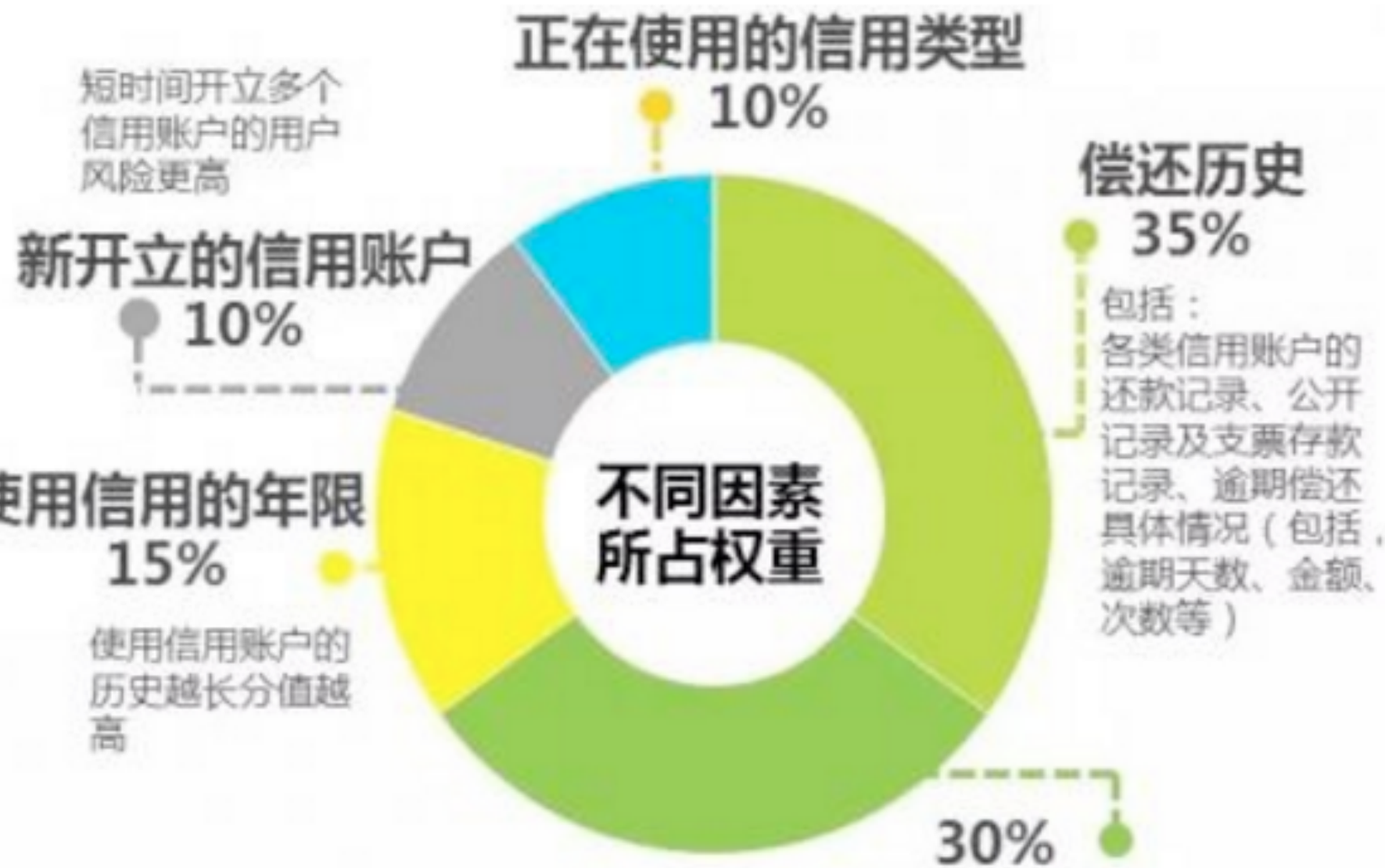
Sean A. Munson

Caroline Richardson

eric friedman

Hal Varian

FICO模型



http://www.fico.com/

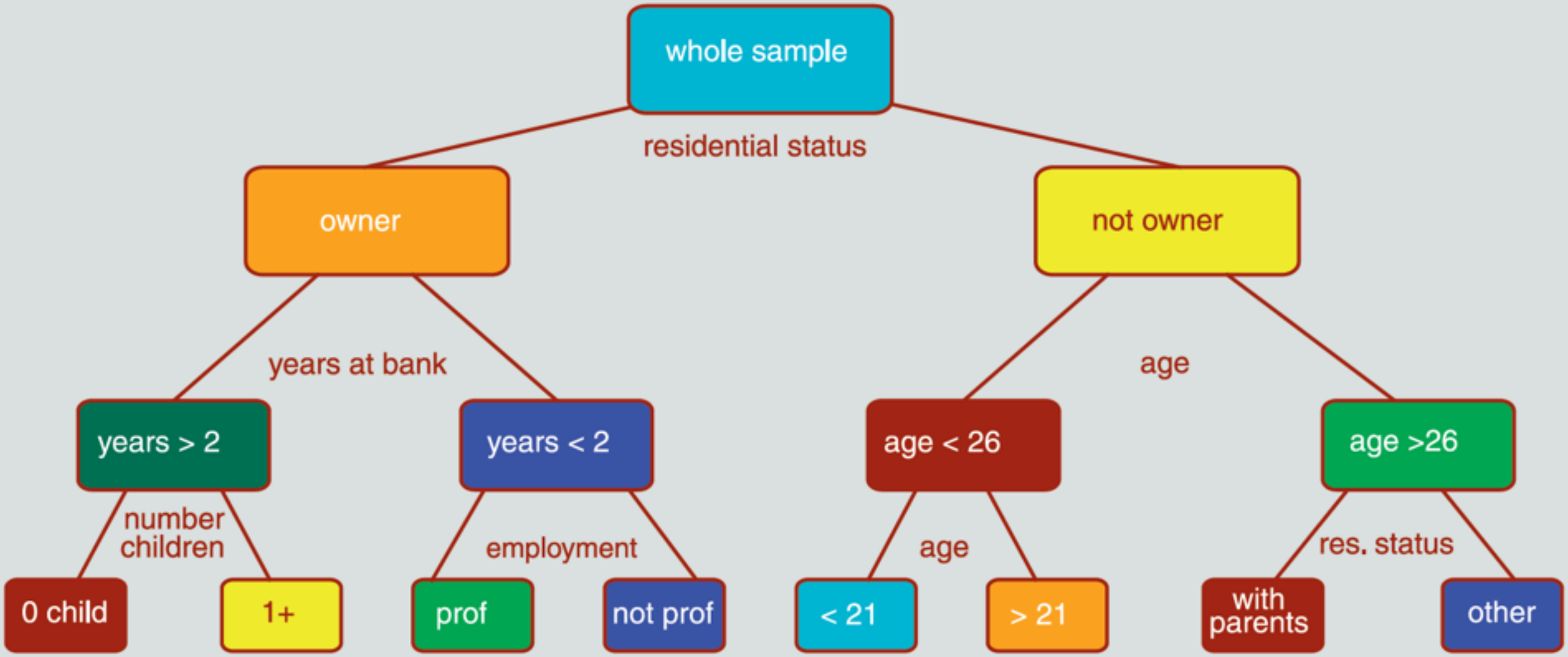
FICO®

芝麻信用 ZHIMA CREDIT 因为信用 所以简单

腾讯信用

信用评分

- 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.

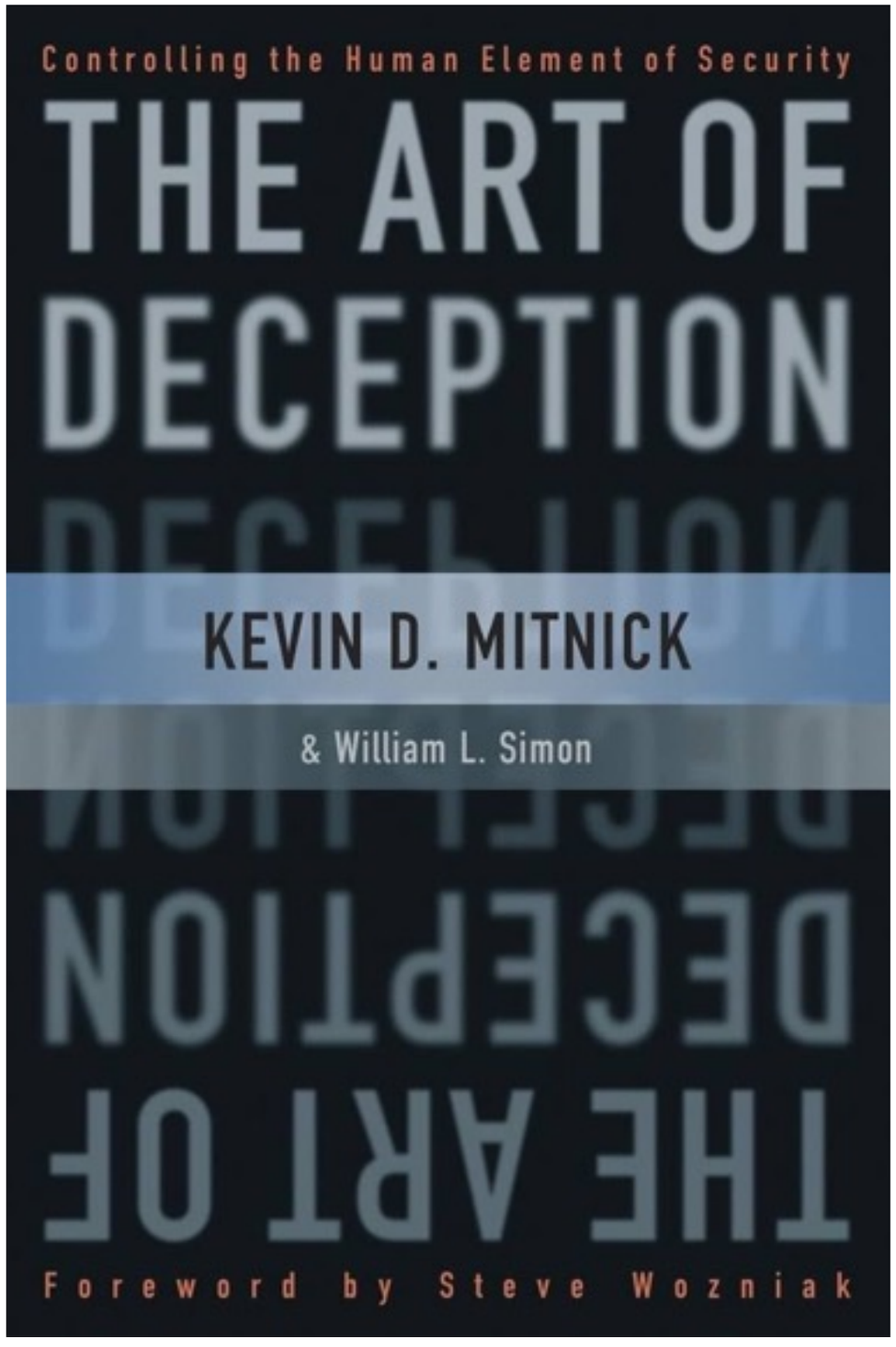


未来

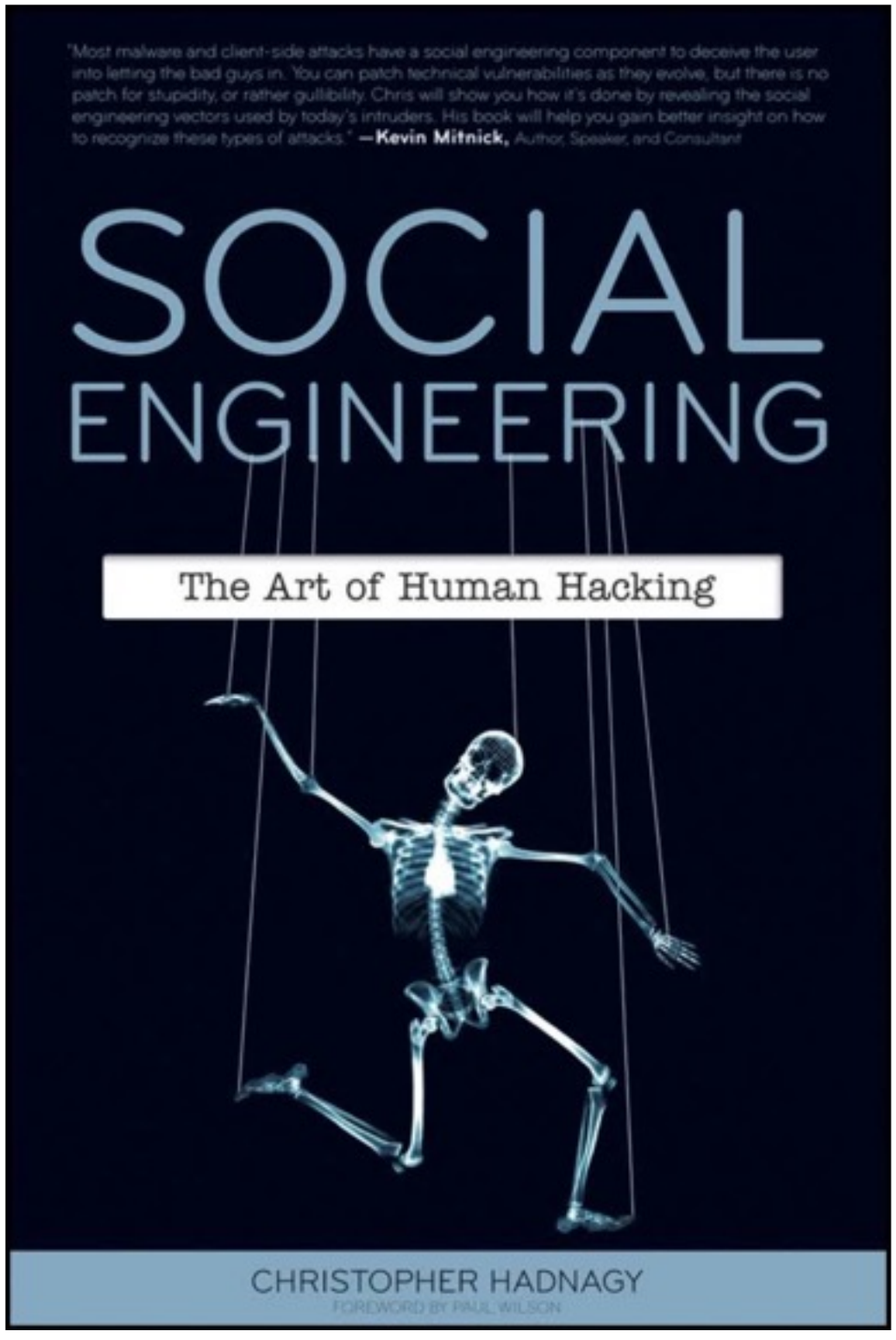
BLACK MIRROR

信息安全＋心理学

社会工程学



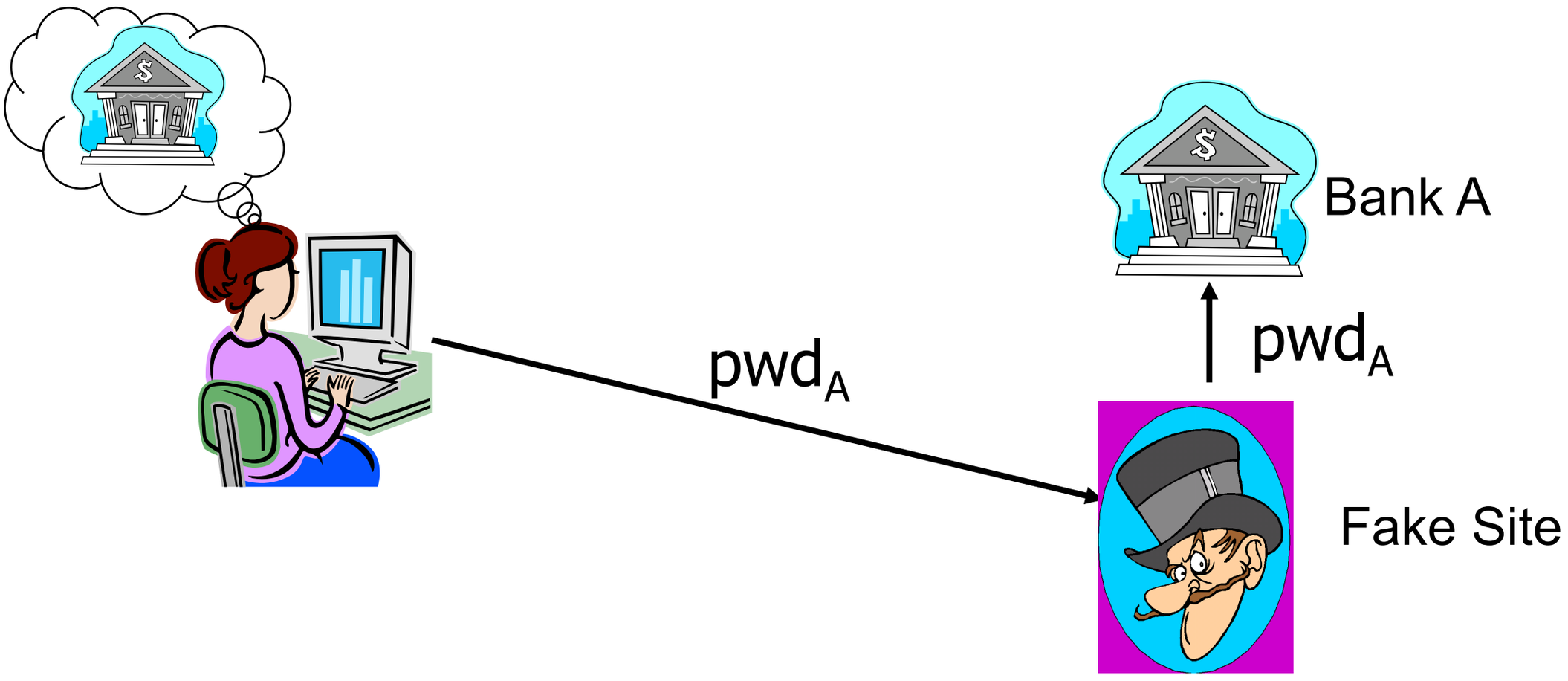
2002



2010

网络钓鱼

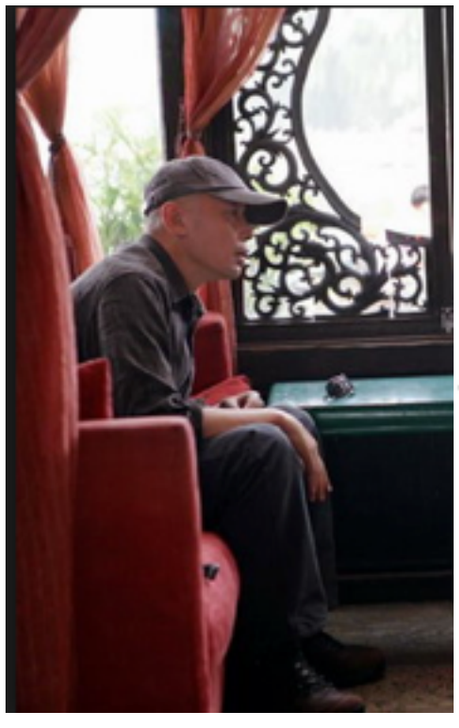
- 对银行的网络钓鱼开始于2003年
- 2006年，美国银行损失2亿美元



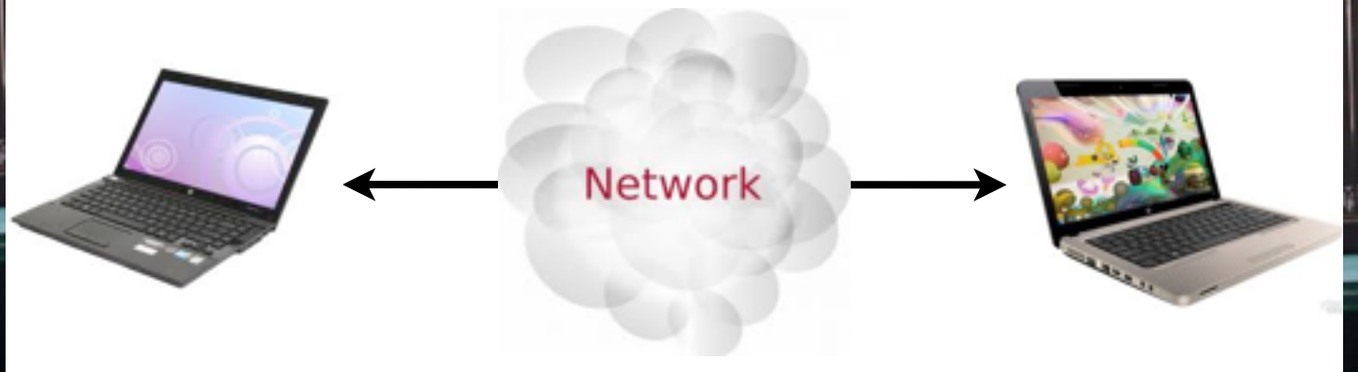
人际交流改变

- 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

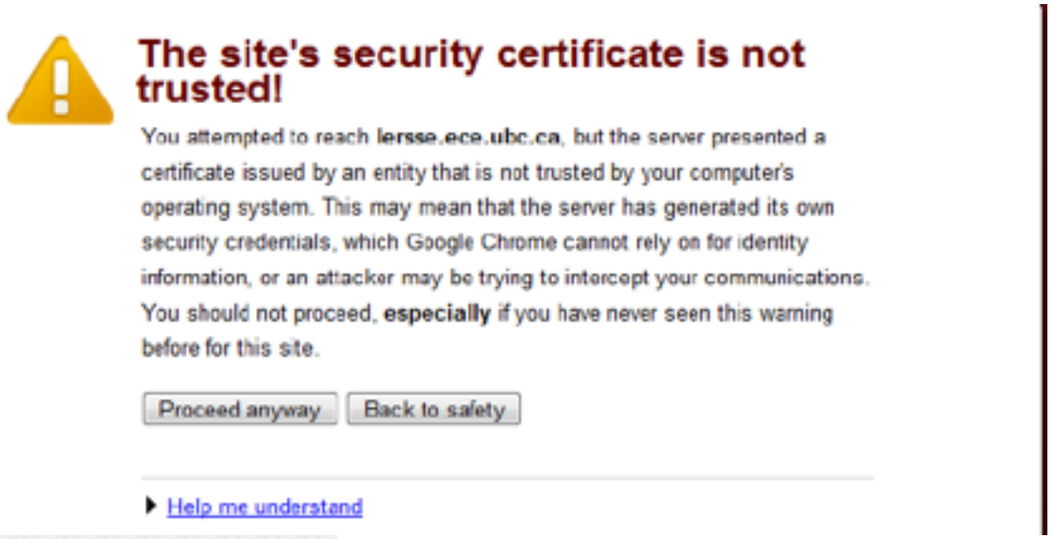


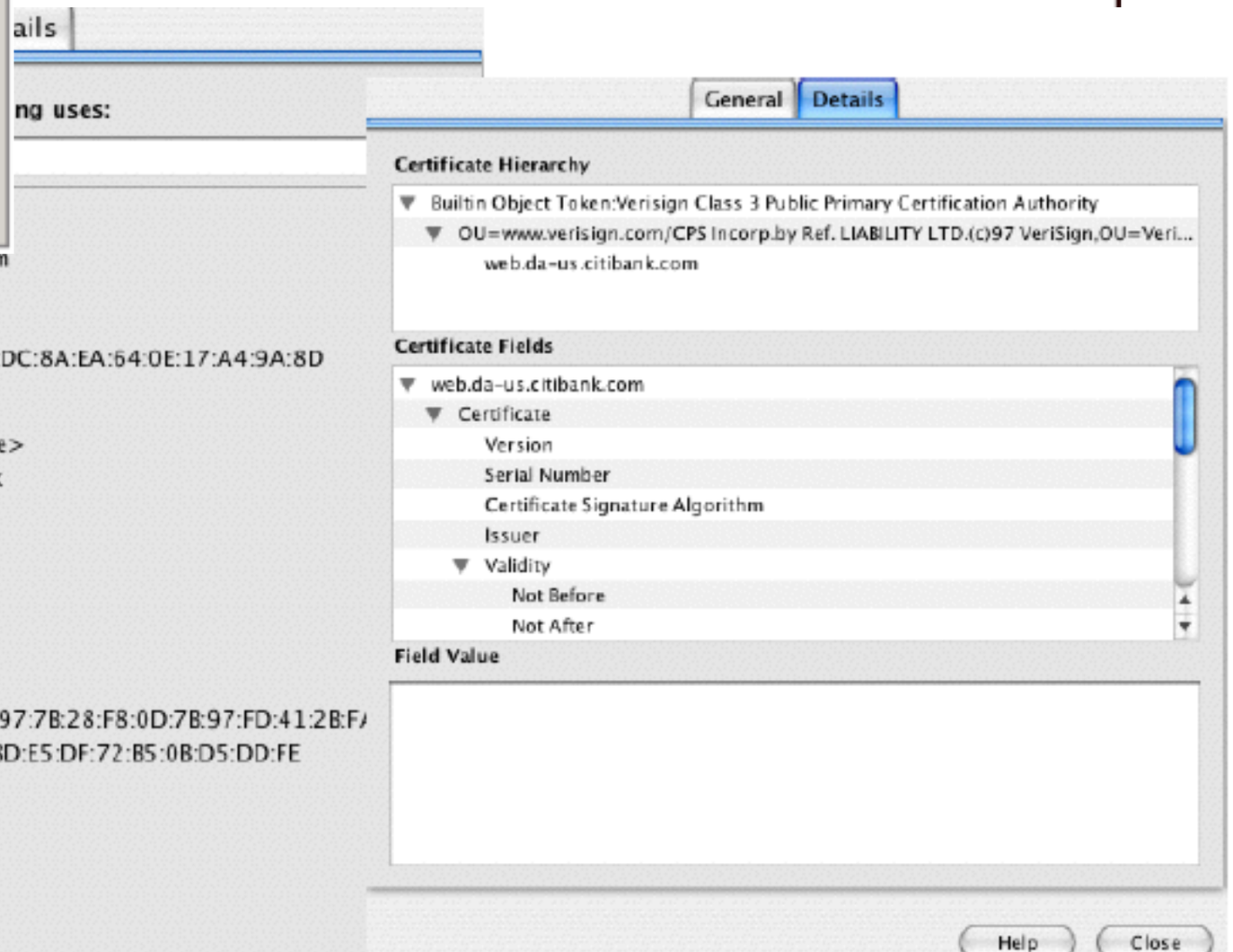
信息将证明交互



人防止欺骗的能力失效了

证书





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/

可用安全起源

- 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、…

Usable Security

可用安全

可用＋安全

- 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….

- 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

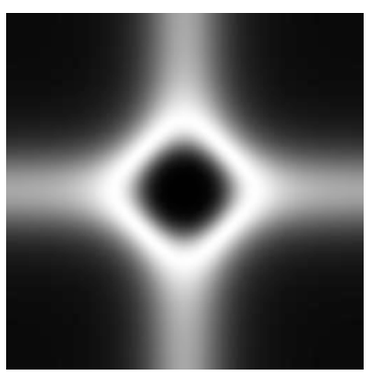
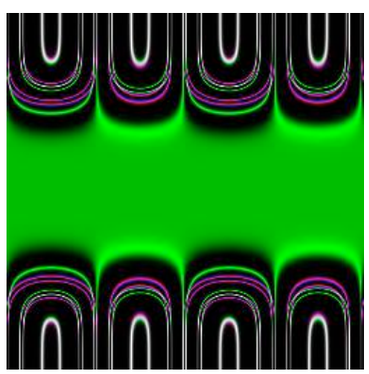
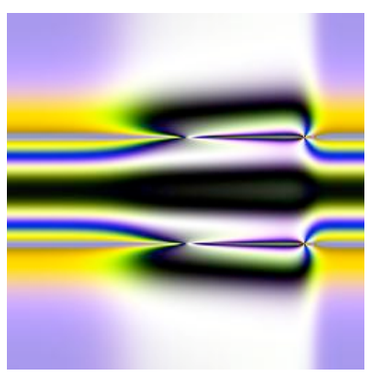
- 文本口令是研究与使用最为广泛的身份认证方法，最常用的形式：用户名＋口令
- 选择原则：易于记忆，难于猜中或者发现，抗分析能力强

Table 1. Password characteristics.

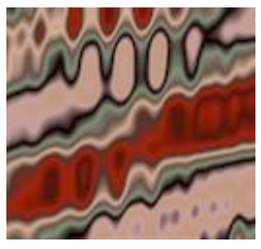
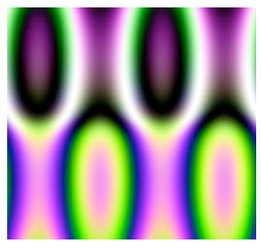
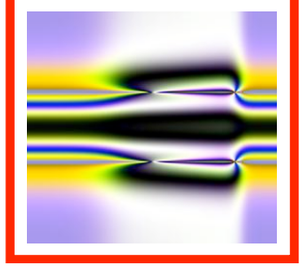
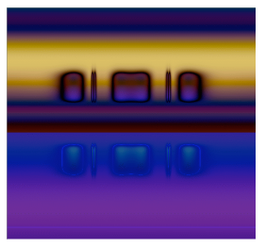
Password characteristic	Security focus	Usability focus
Length	Longer	Shorter
Composition	Heterogeneous characters	Homogeneous characters
Uniqueness	Forbid reuse	Common passwords
Change frequency	Often	Seldom

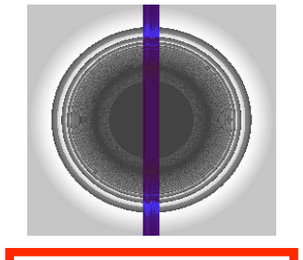
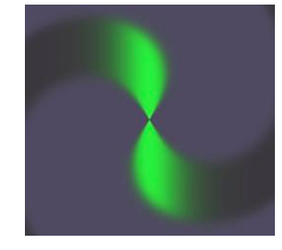
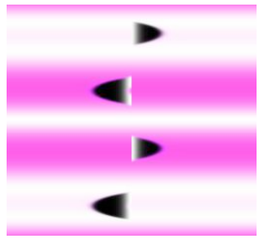
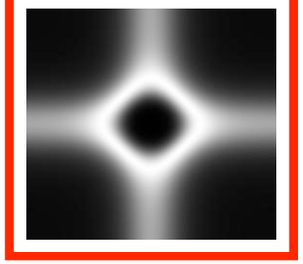
Déjà Vu

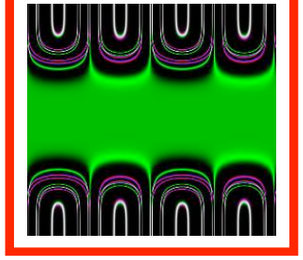
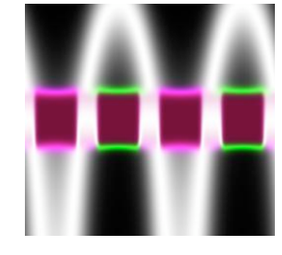
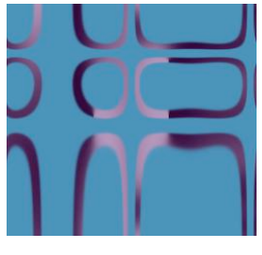
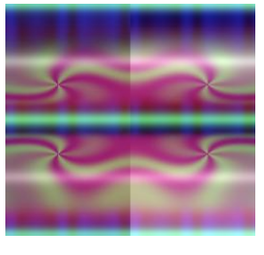
训练

挑战

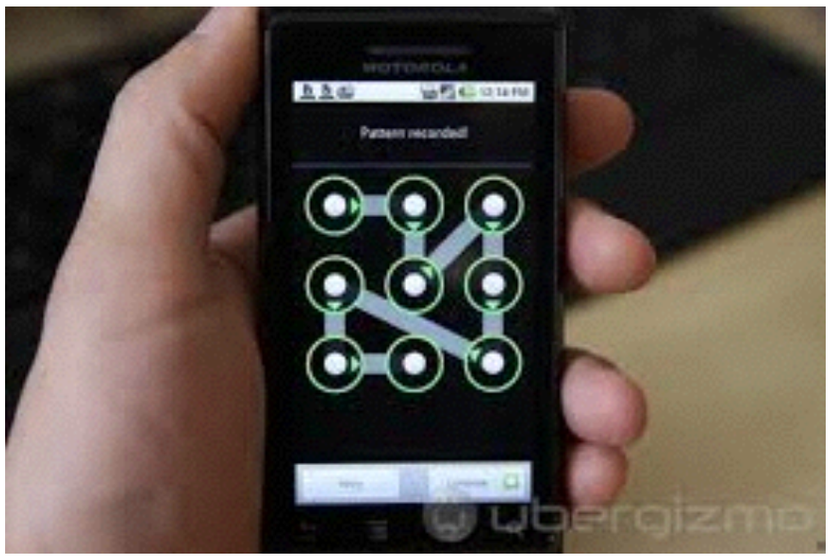
PassFaces

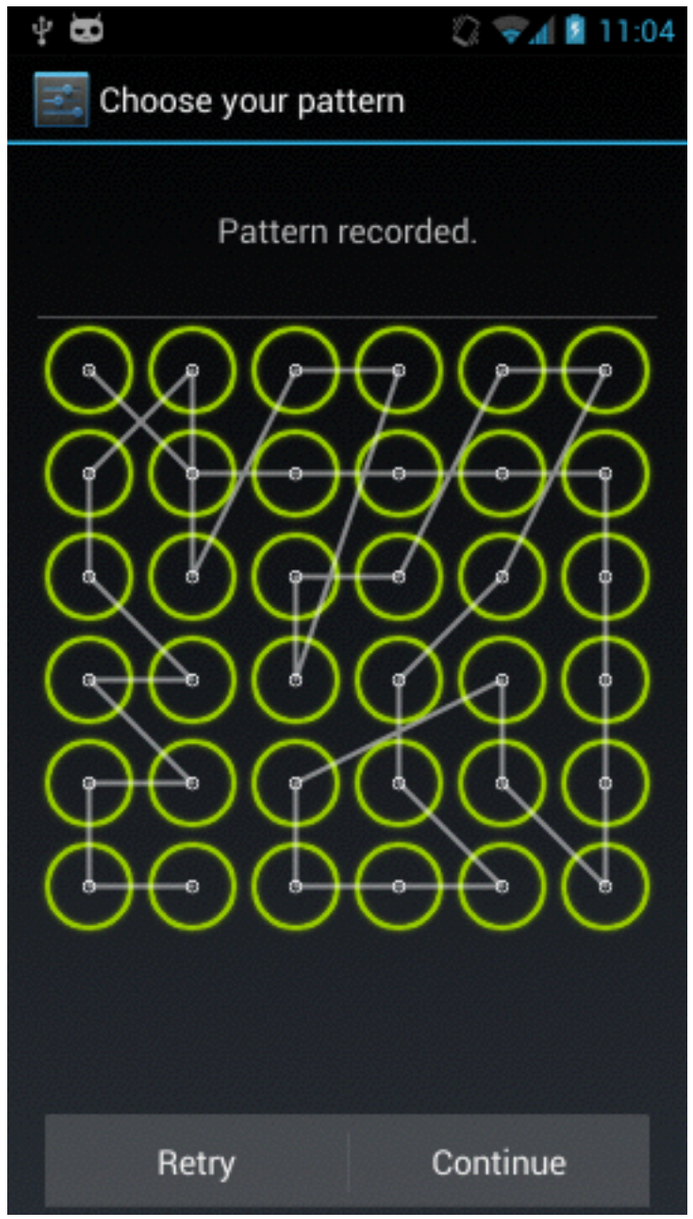
- 系统从脸型数据库中随机选取5个人的脸型，显示给用户，并给用户一定时间让用户熟悉（注册）

- 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





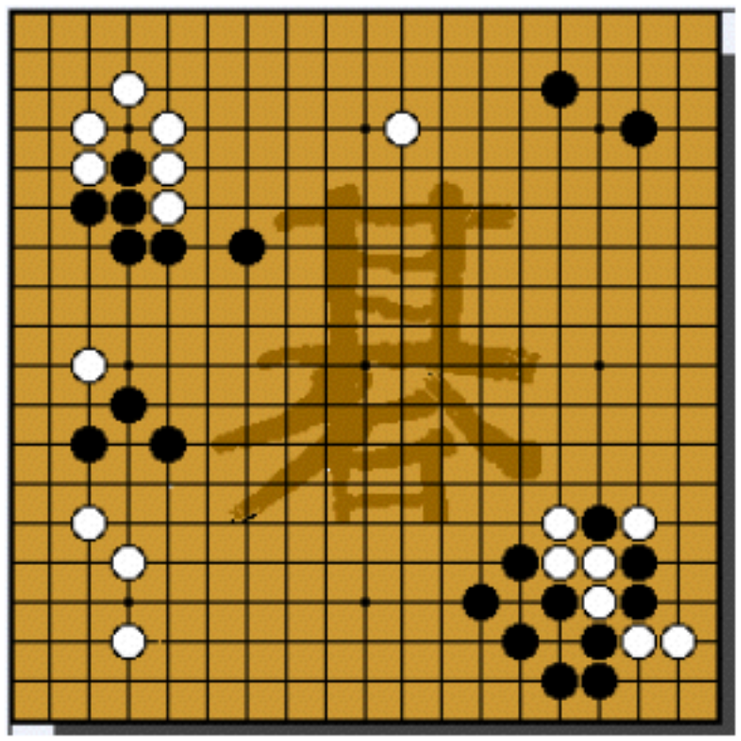
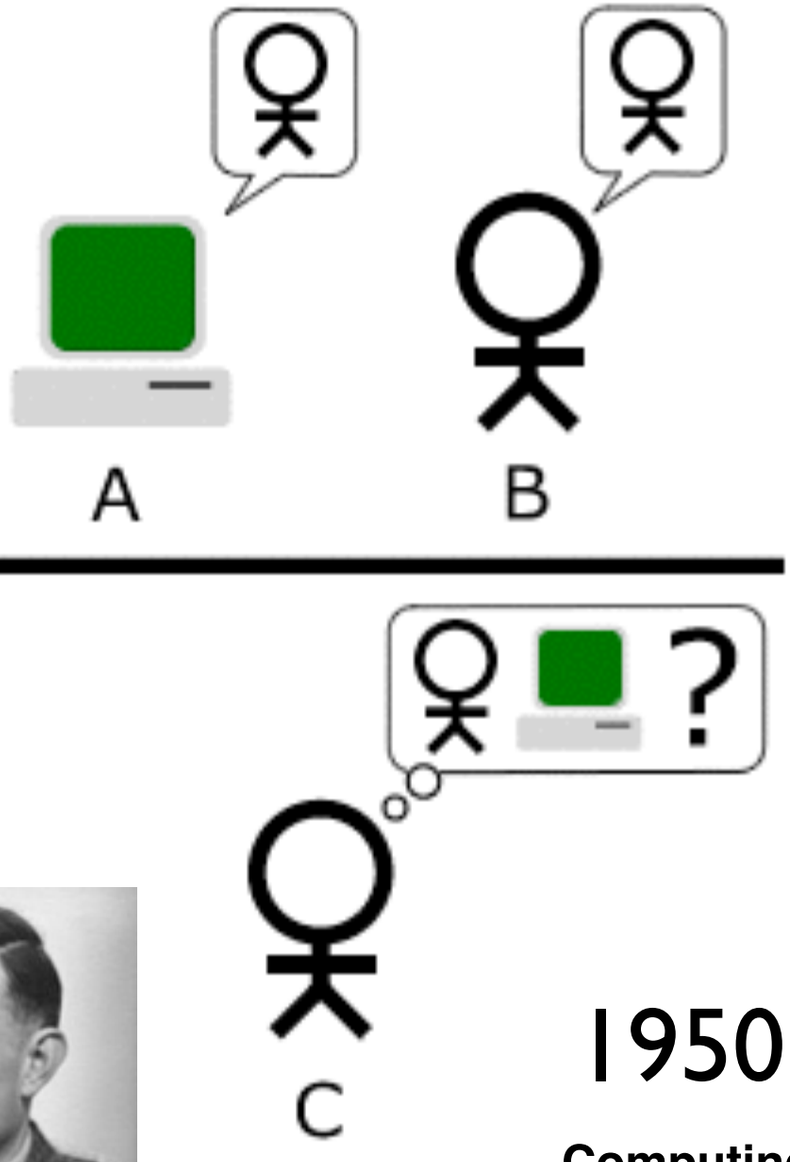


Figure 1 Go game

信息安全+AI

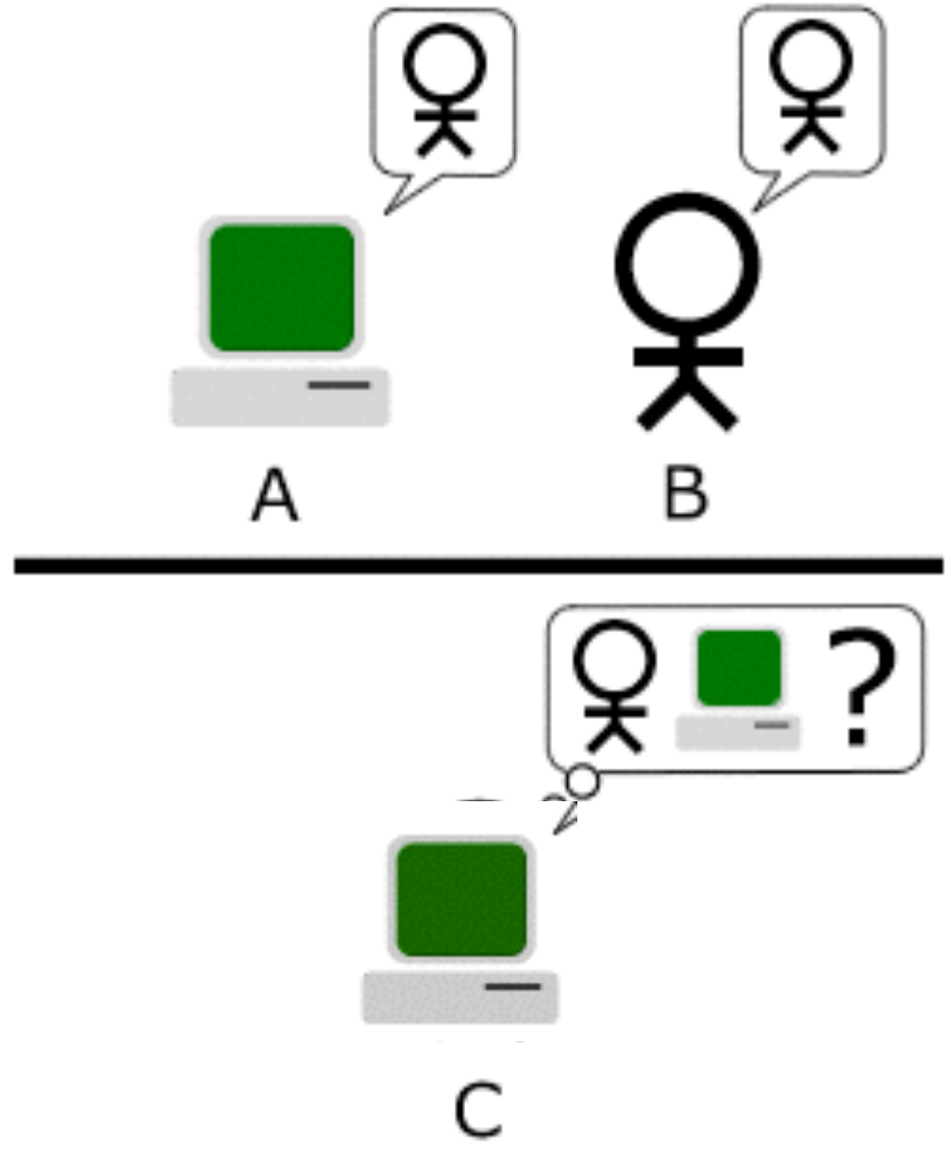
图灵测试 vs 反向图灵测试

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



1950

Computing Machinery and Intelligence



Luis von Ahn

- Carnegie Mellon University
  - ✶ Luis von Ahn
  - ✶ Manuel Blum
  - ✶ Nicholas J.Hoper
  - ✶ John Langford 2000年

2005年
博士毕业

Human Computing

http://vonahn.blogspot.com/

2007年

reCAPTCHA

2011年

duolingo.com

capture

2008年

商标申请没有被批准

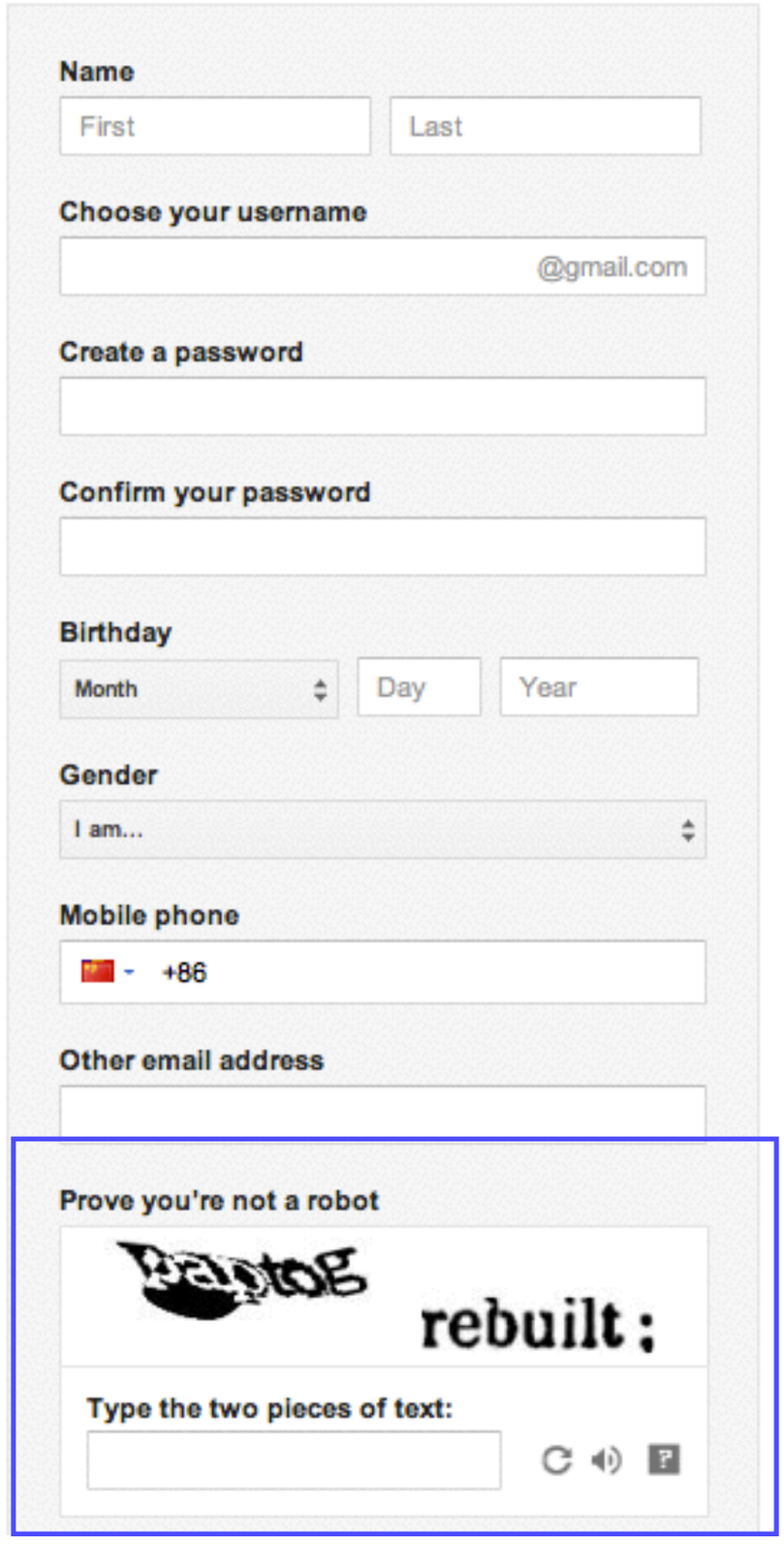
2006年 http://video.google.com/videoplay?docid=-8246463980976635143

CAPTCHA定义

- CAPTCHA
  - Completely
  - Automated
  - Public
  - Turning test to tell
  - Computers and
  - Humans
  - Apart

http://www.captcha.net/

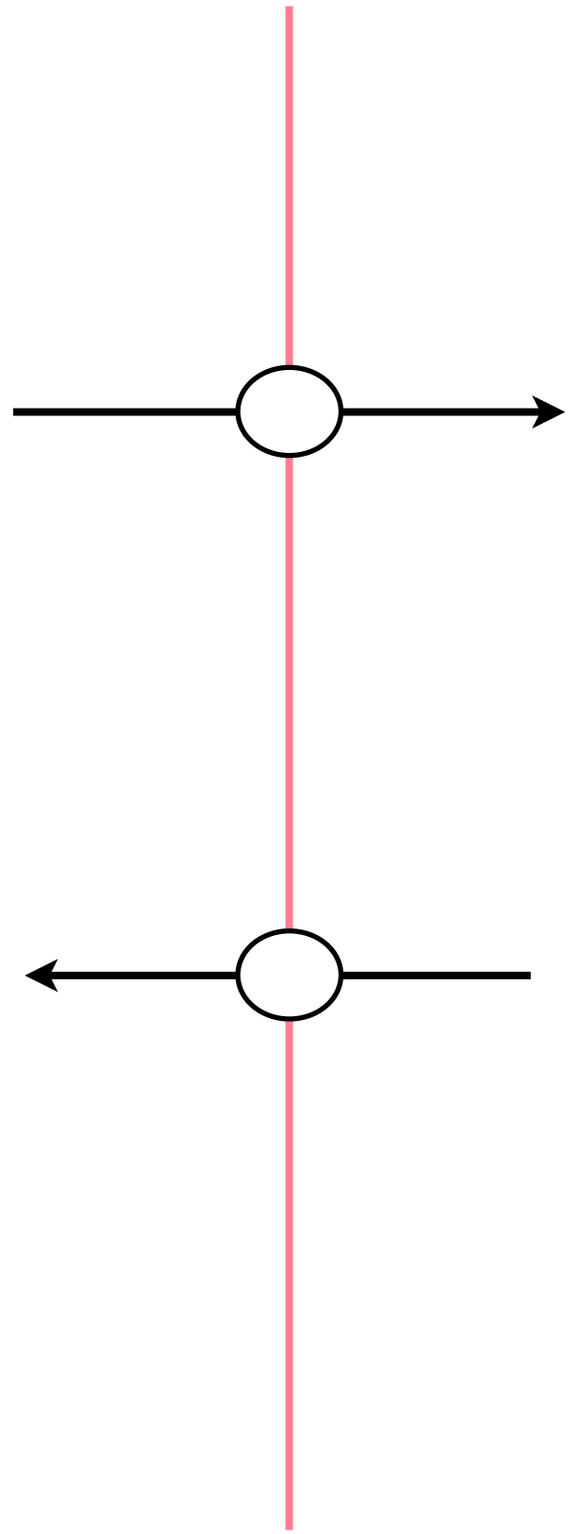
http://en.wikipedia.org/wiki/CAPTCHA



CAPTCHA vs AI

- 设计CAPTCHA
  - Email
  - BBS
  - Blog
  - SNS
  - Security
  - ... ...

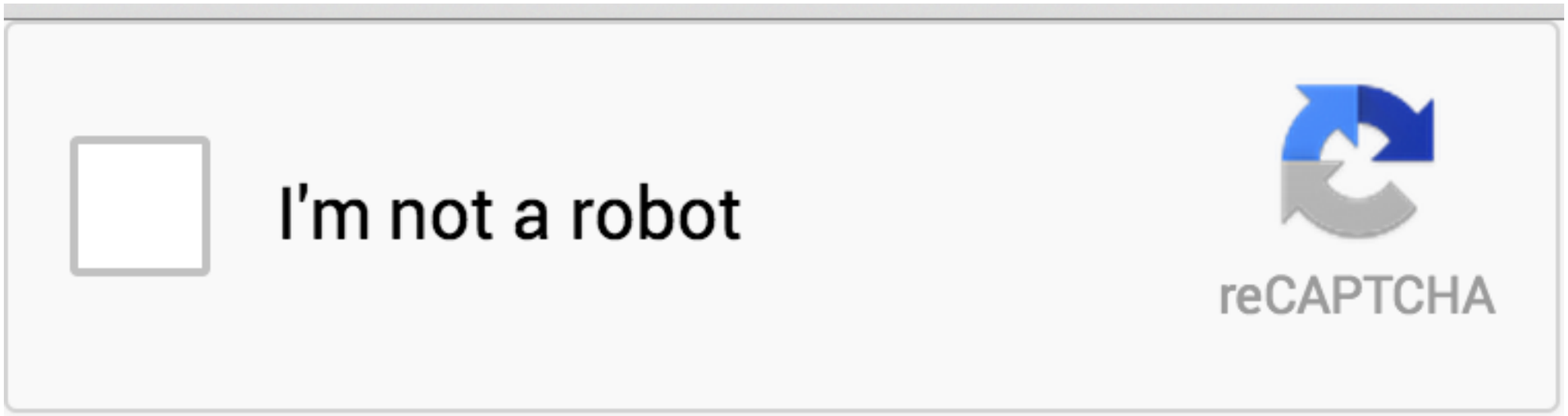
AI难题



- 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
  - ... ...

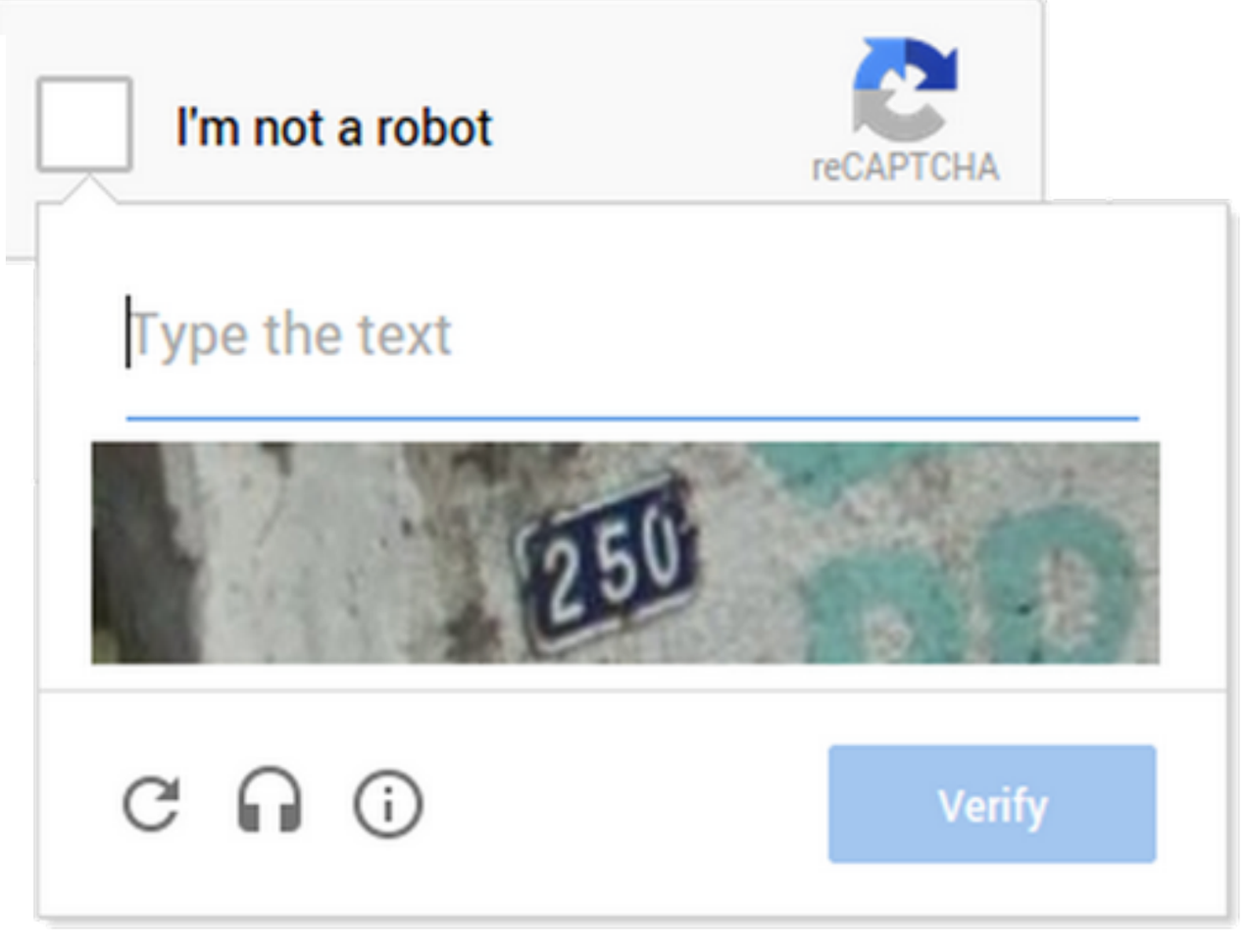
机器学习

NoCAPTCHA


I'm not a robot
reCAPTCHA


I'm not a robot
reCAPTCHA
Select all images below that match this one:
Verify


I'm not a robot
reCAPTCHA
Select all images below that match this one:
Verify

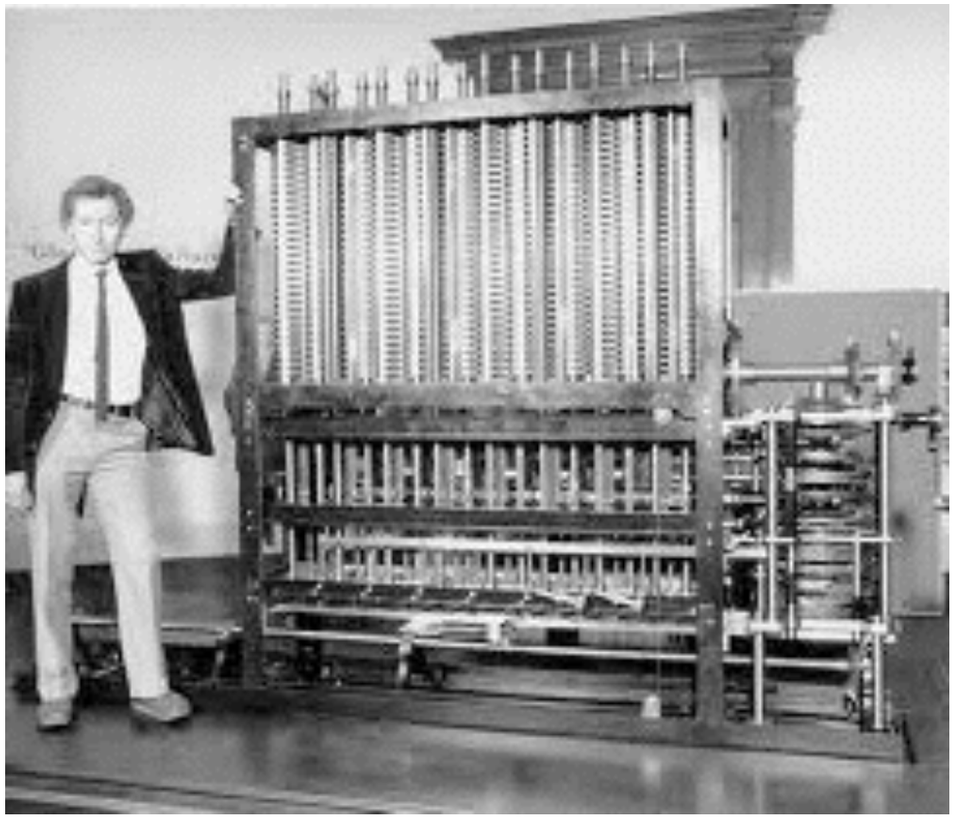

I'm not a robot
reCAPTCHA
Type the text
250
Verify

Computation历史

计算公式 → 任务分解

↓

操作指南 → 结果合并



Human Computation

- 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?

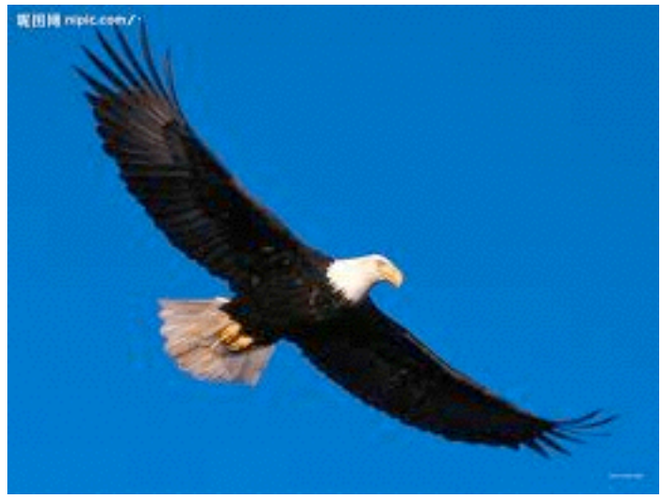
人工智能难题

- 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

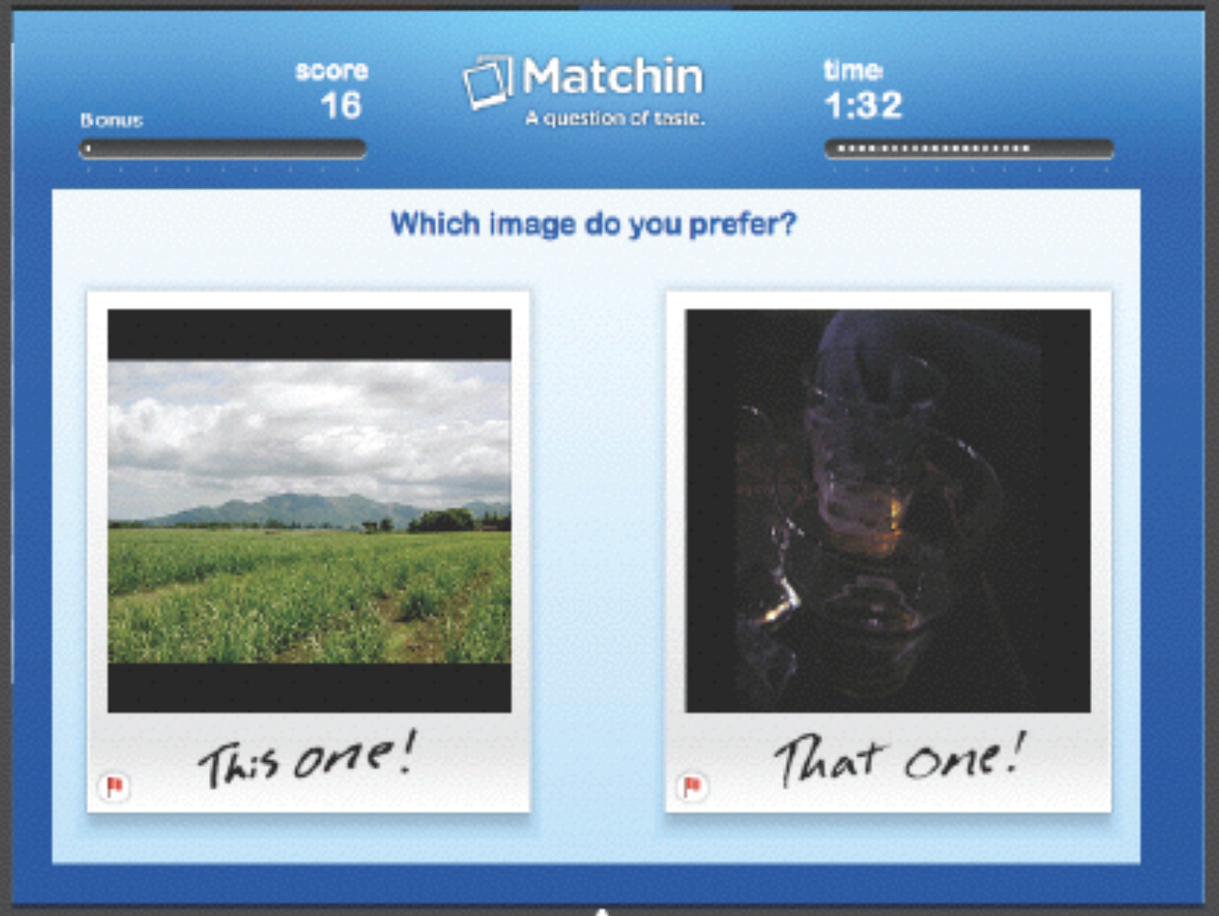


Tag系统　Q&A系统

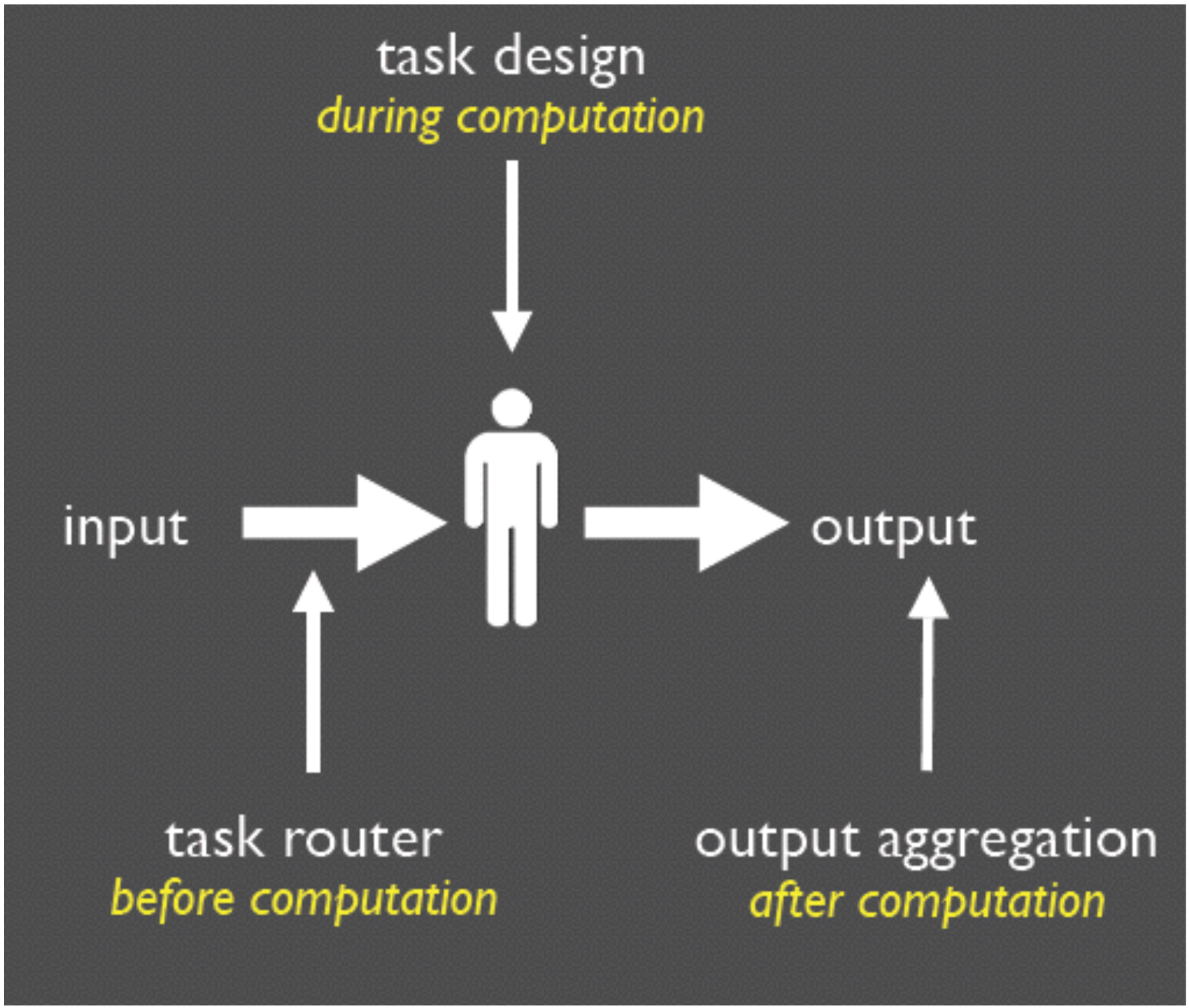
Human Computation

```
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

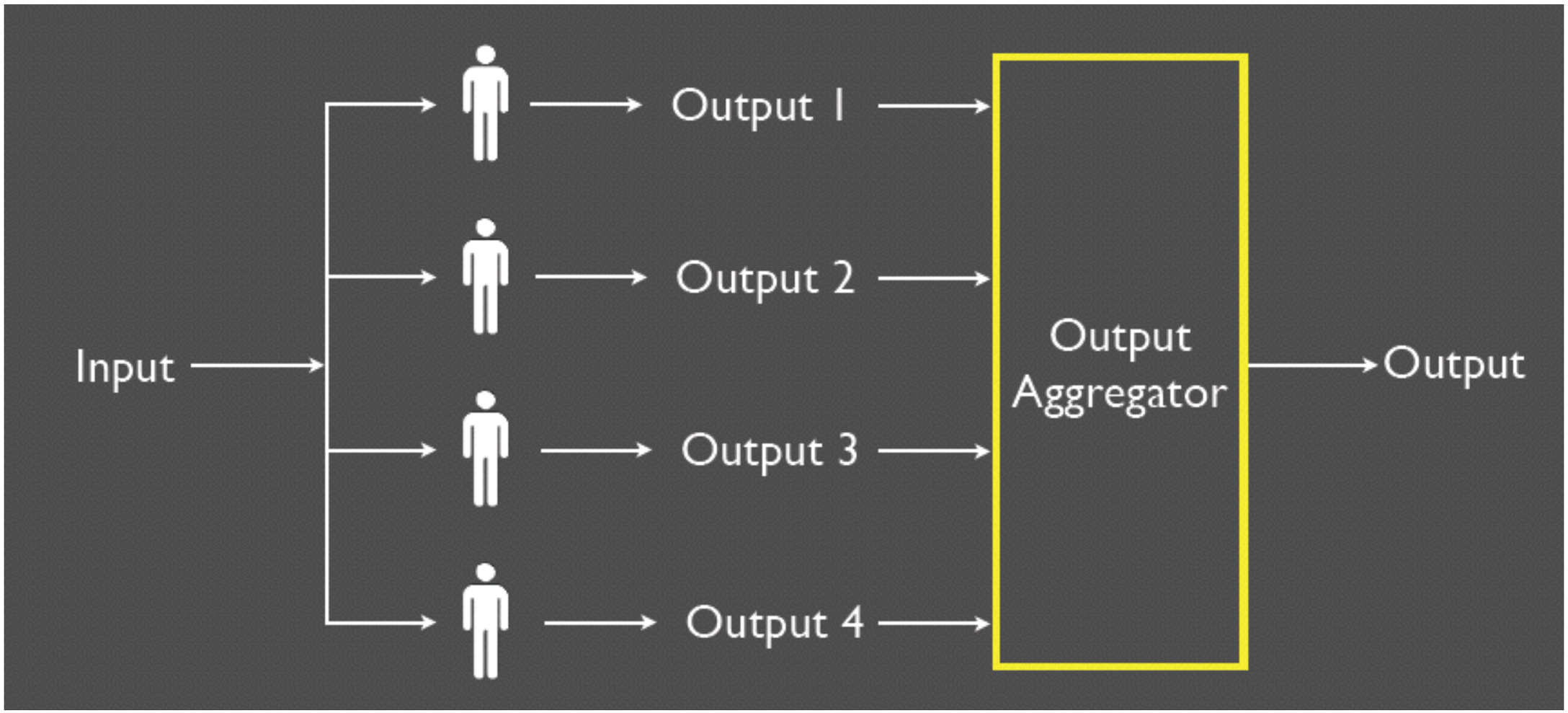


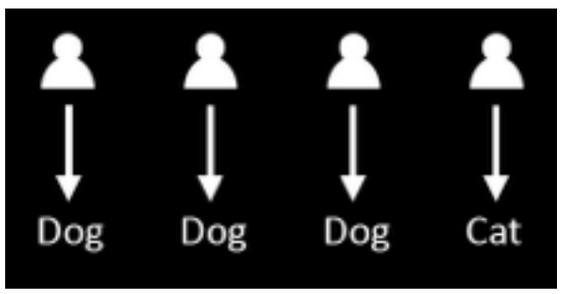
算法正确性



- Money
- Access
- Game
- Volunteer
- Learning

结果汇集


Input
Output 1
Output 2
Output 3
Output 4
Output Aggregator
Output


Dog
Dog
Dog
Cat


Type the two words:
reCAPTCHA
stop spam.
read books.

ESP: Web图形识别

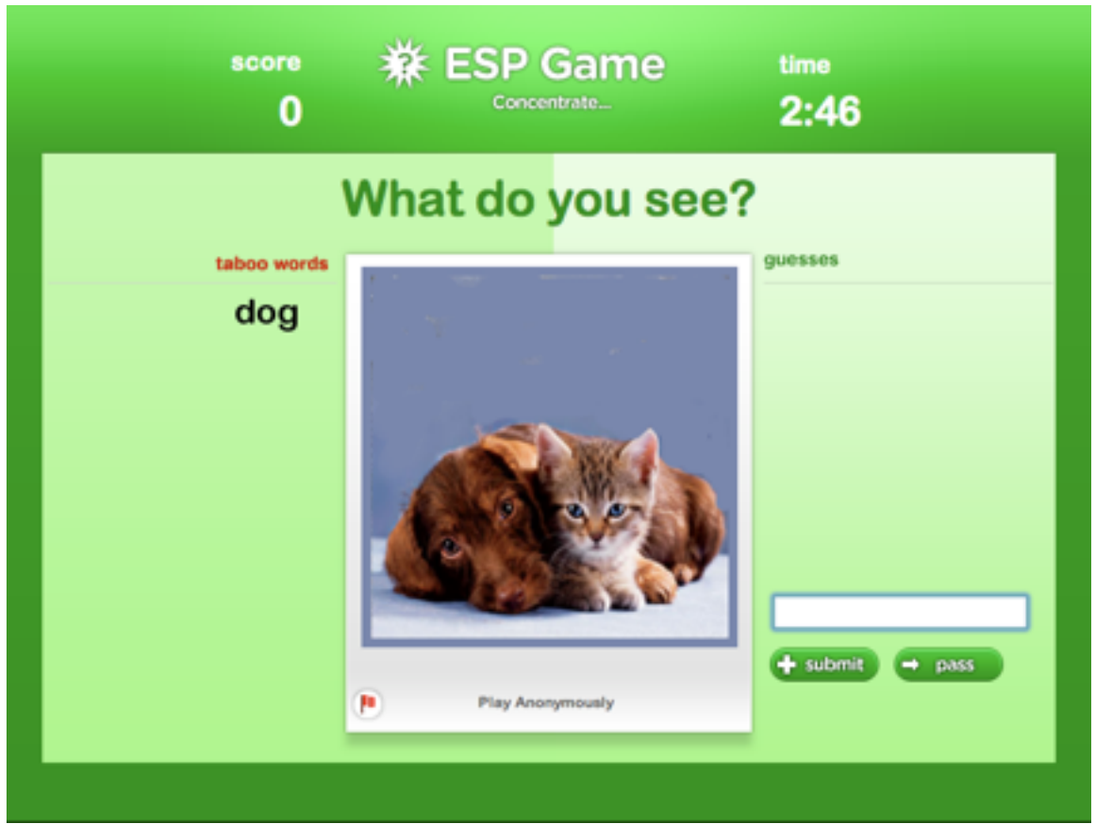
- Web上的图像识别是一个主要的技术挑战
- 大量图片存在，但是文本描述很少，自动识别很不准确
- 人来做标记是一个无奈的选择

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

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



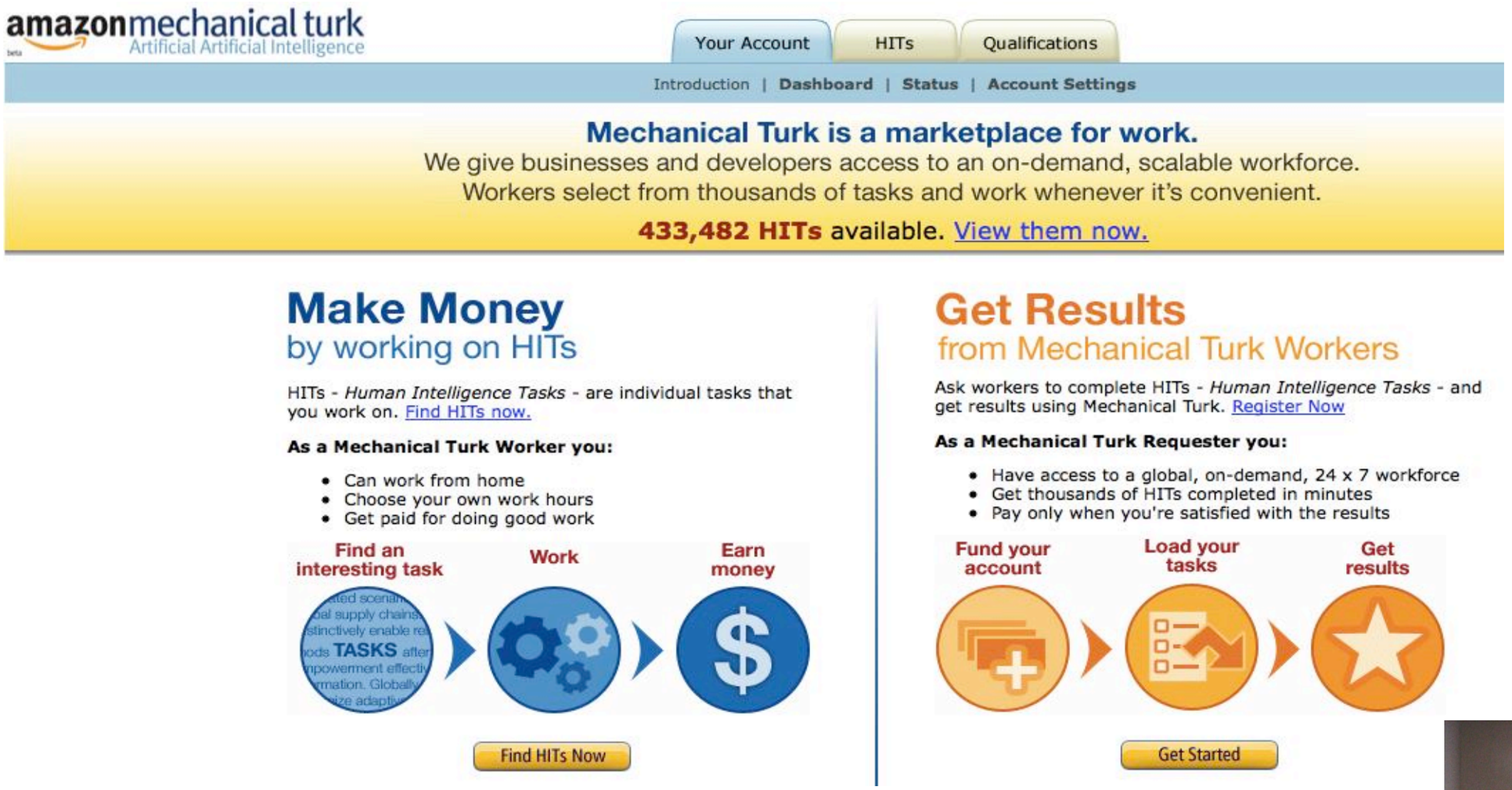
Player 1 guesses: purse
Player 1 guesses: bag
Player 1 guesses: brown

Success! Agreement on “purse”

Player 2 guesses: handbag

Player 2 guesses: purse
Success! Agreement on “purse”

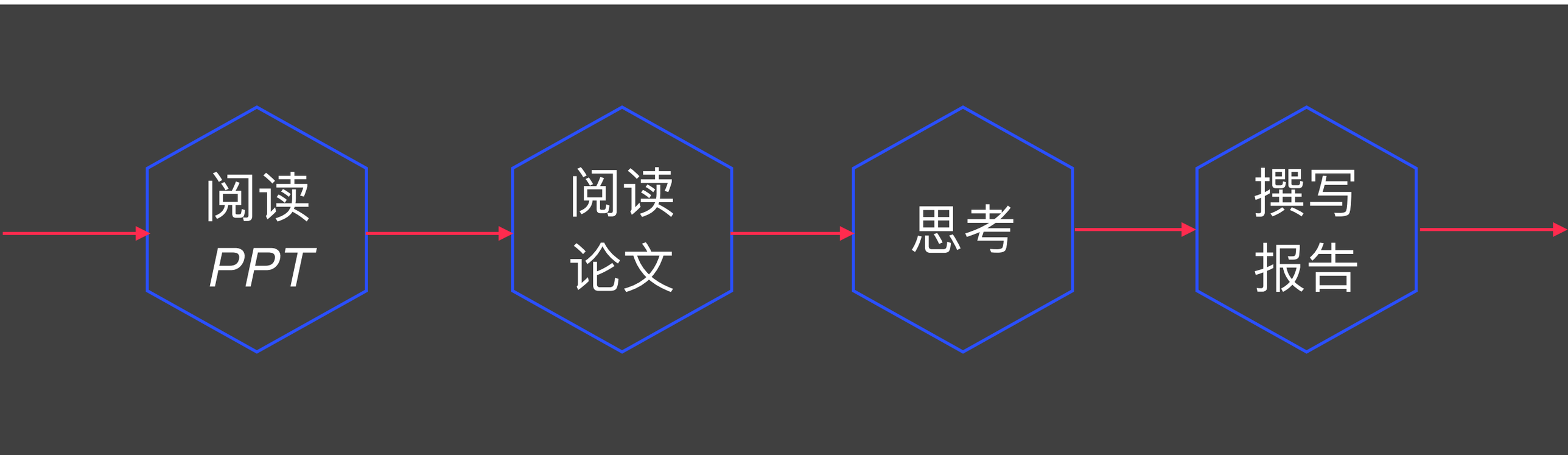
Amazon Mechanical Turk



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。

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。

课后作业



Homework

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1日晚上
12点前提交

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

https://huipingsun.github.io