

Information Security Engineering

2017.09.13

课程简介



Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

课程内容

- 课程基本情况介绍
- 经济学和信息安全
- 心理学和信息安全
- 社会学和信息安全
- 人工智能和信息安全
- 大数据和信息安全

教师信息

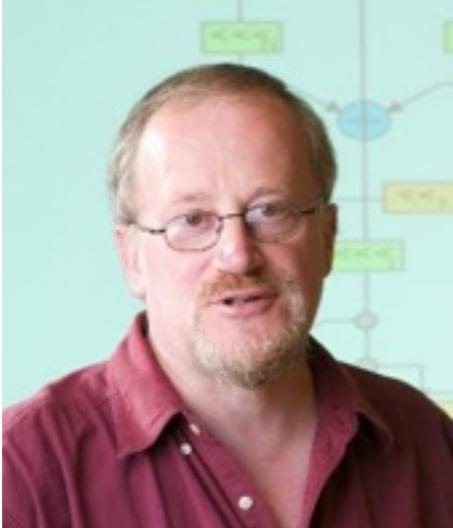
- 姓名：孙惠平
- 方向：网络和信息安全
- 兴趣：身份管理、信任管理
- 关注：智能手机认证、可用安全口令、CAPTCHA
- 邮箱：sunhp@ss.pku.edu.cn
- 主页：sunhp.org
- 地址：理科I号楼I530E（北大信息安全实验室）

- 基本信息
 - * 上课时间：每周四、上午8点半到11点半
 - * 上课地点：3305
 - * 助教 : 郝昊天
 - * 北大系统：01712720
 - * 课程主页：sunhp.org/ise2017

- 考察方式
 - * 平时成绩：60%（课堂报告、随堂测试、课后作业）
 - * 项目成绩：40%（后续课程将介绍）

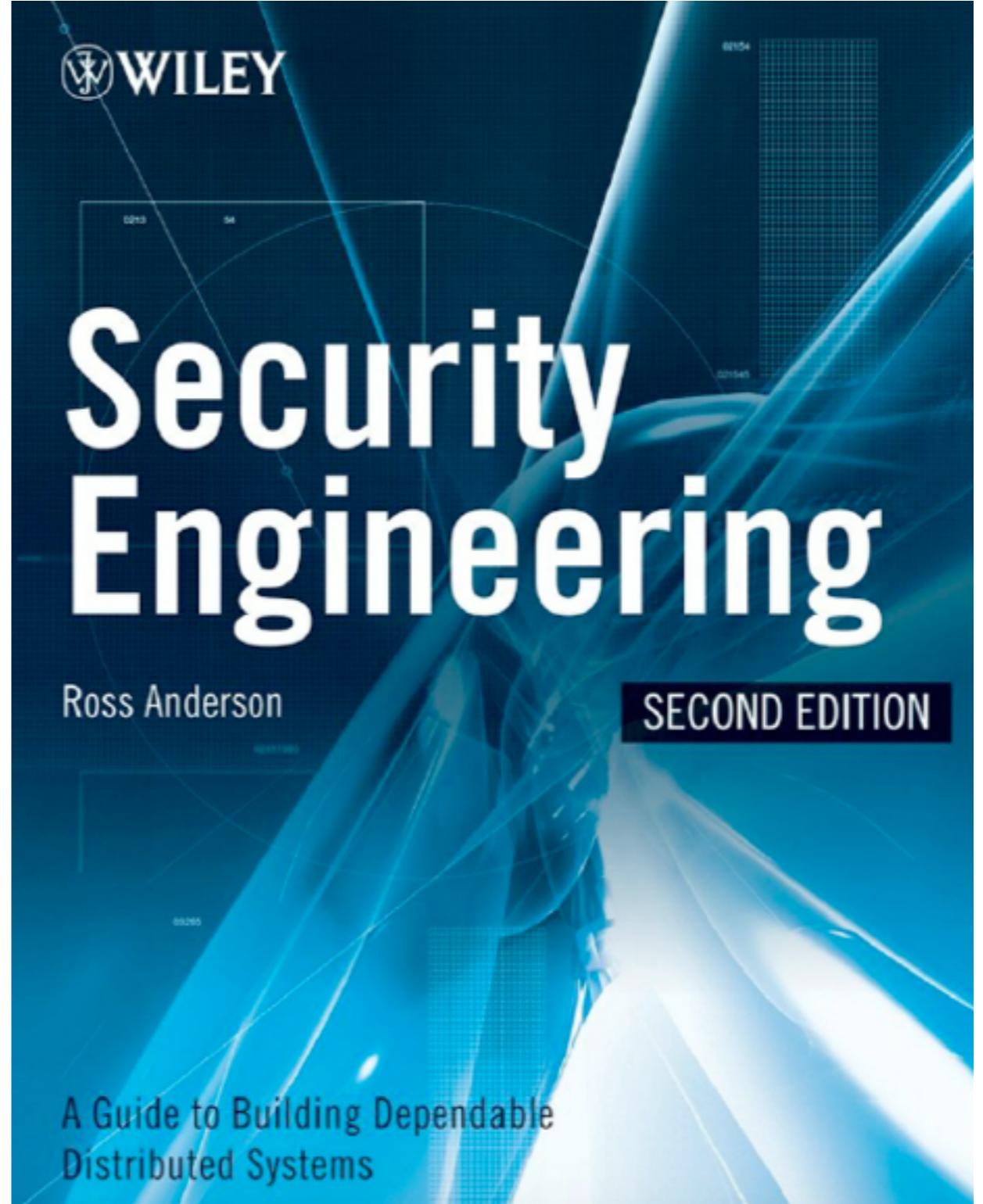
Course Overview

课程教材



Ross Anderson.
Security Engineering
Second Edition
Wiley. 2008

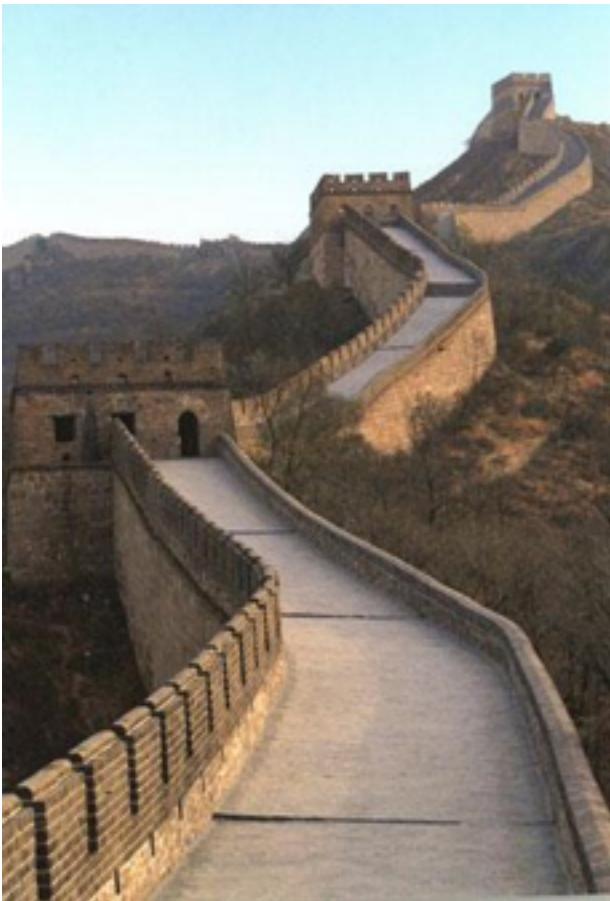
<http://www.cl.cam.ac.uk/~rja14/book.html>



安全是什么？

- “安全”一词的基本含义为，“远离危险的状态或特性”或“主观上不存在威胁，主观上不存在恐惧”
- 安全提供资产和威胁之间的**隔离**，这种隔离一般称为“**控制**”
- 感觉安全 vs. 实际安全

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



- 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**.

经济学 >>> 信息安全

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
-

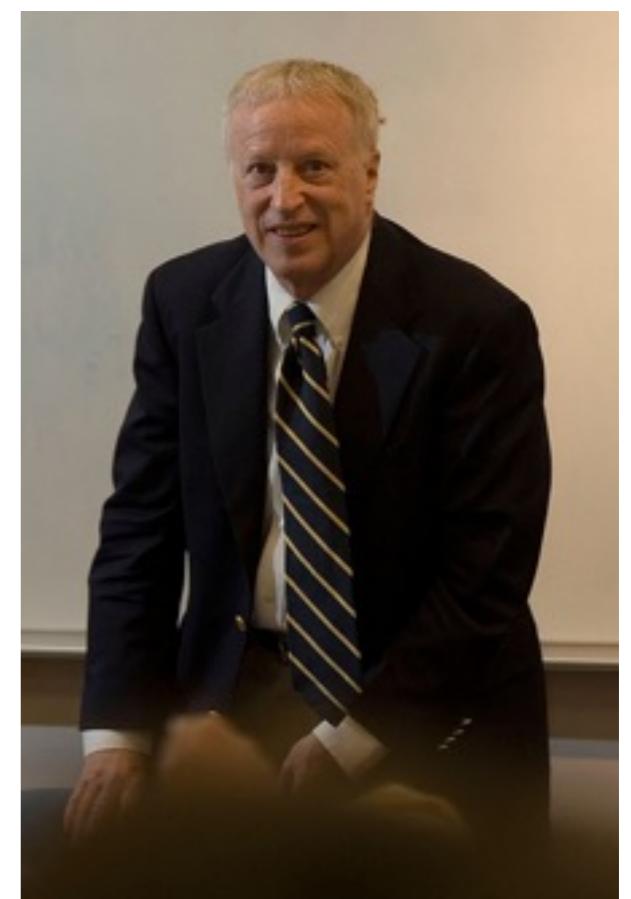
- 信息不对称
- 网络外部性
- 错误激励
- 公共品悲剧
- 博弈/机制设计
-

- 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

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
- 安全信息系统的应该高于不安全信息系统的

>>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

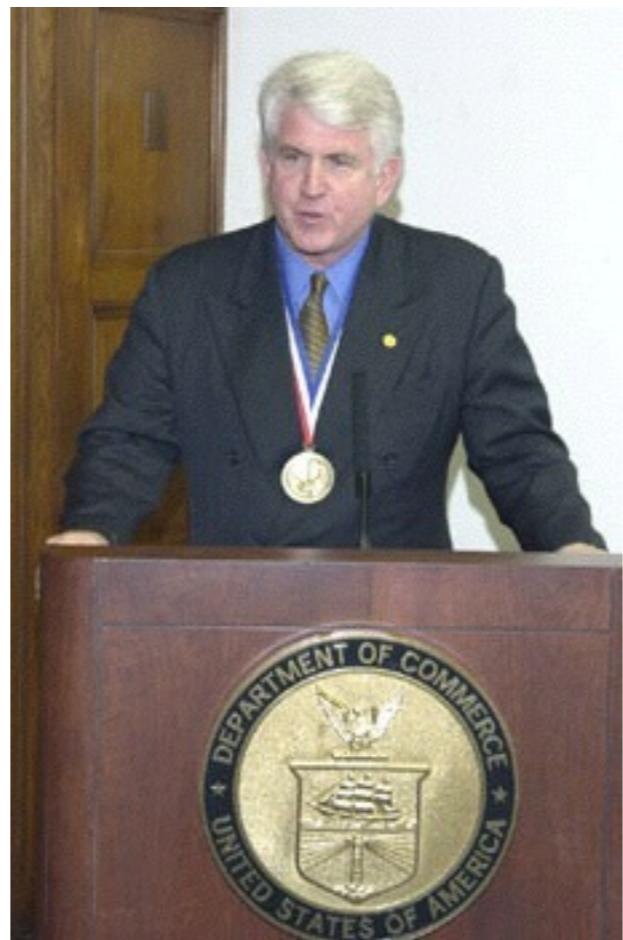


Metcalf法则

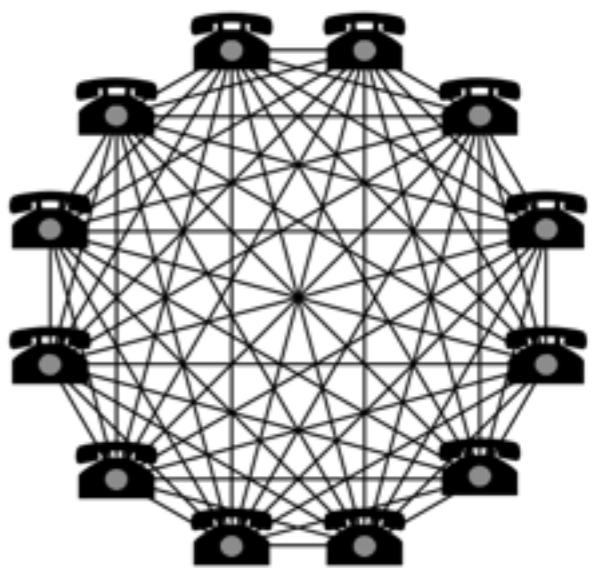
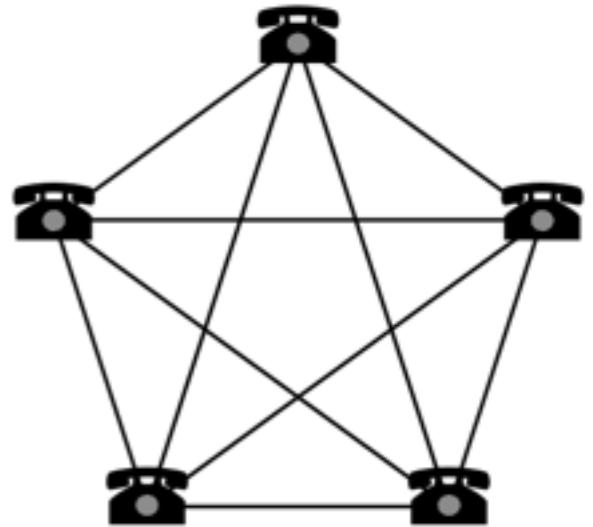
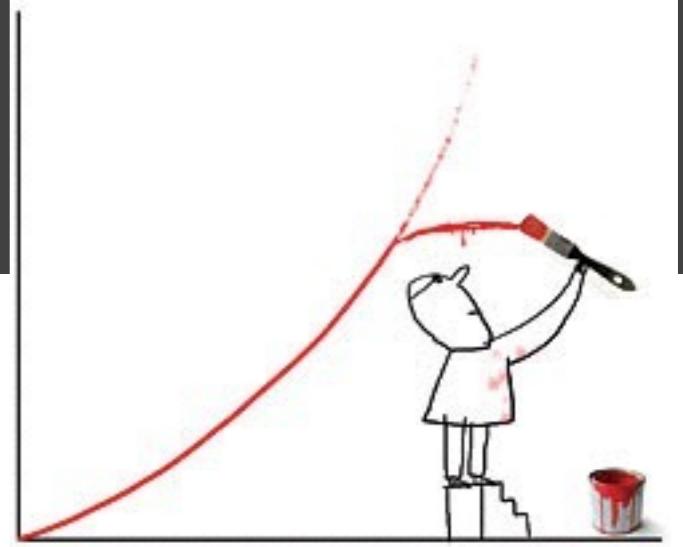
- 梅特卡夫法则：网络价值以用户的数量的平方的数量增长



乔治 吉尔德



3Com创始人



两个例子

- 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



- 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
-

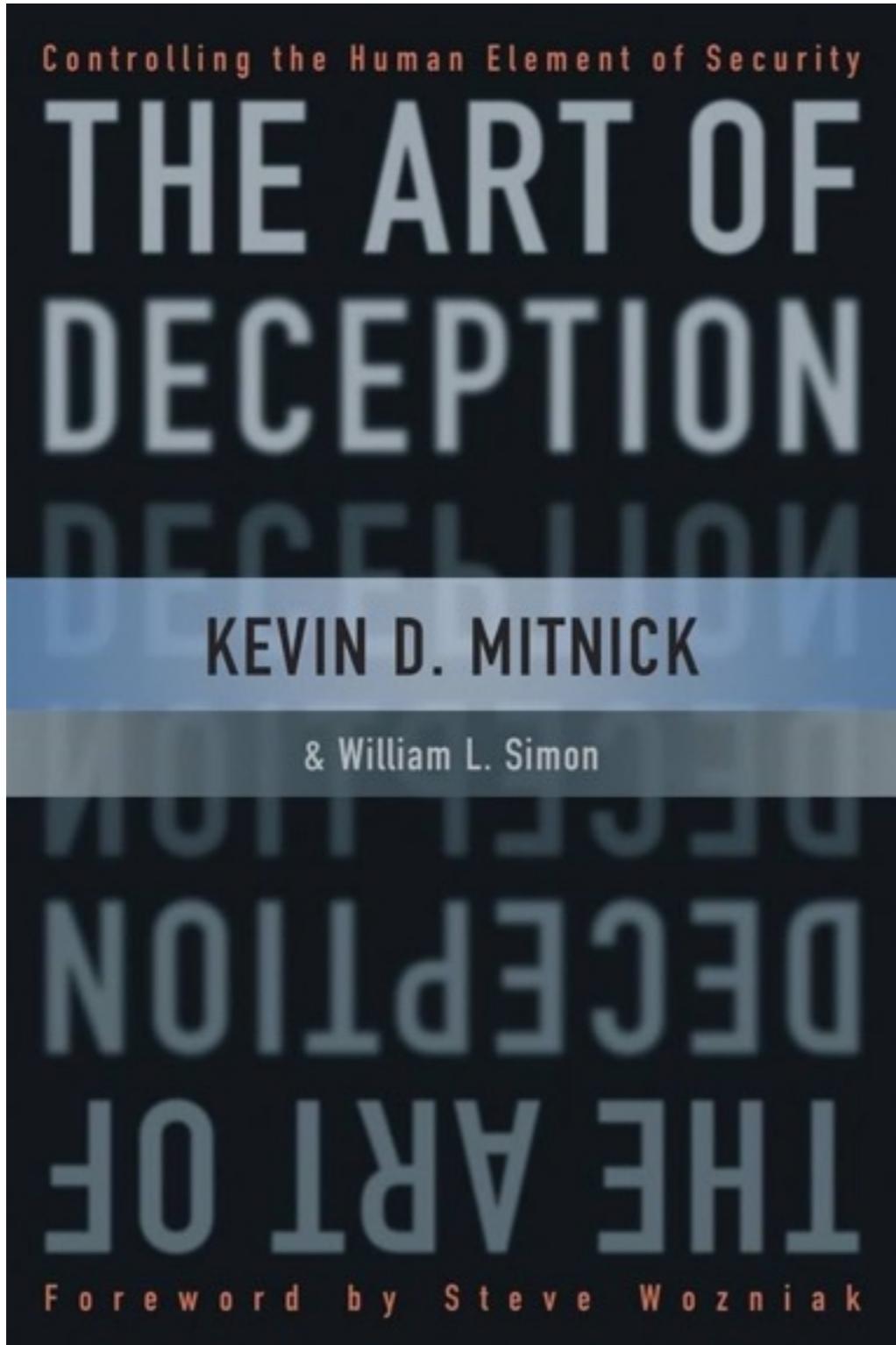
- 产品一开始不安全
- 安全功能很多是为厂家利益考虑的
- 厂商宁可让开发者简便容易开发， 也不会为了增强安全提高开发难度
- 厂商会将自己应该承担的安全和运维责任转嫁给用户
- 厂商使用安全算法来保障对用户的锁定和差别定价

心理学 >>> 信息安全

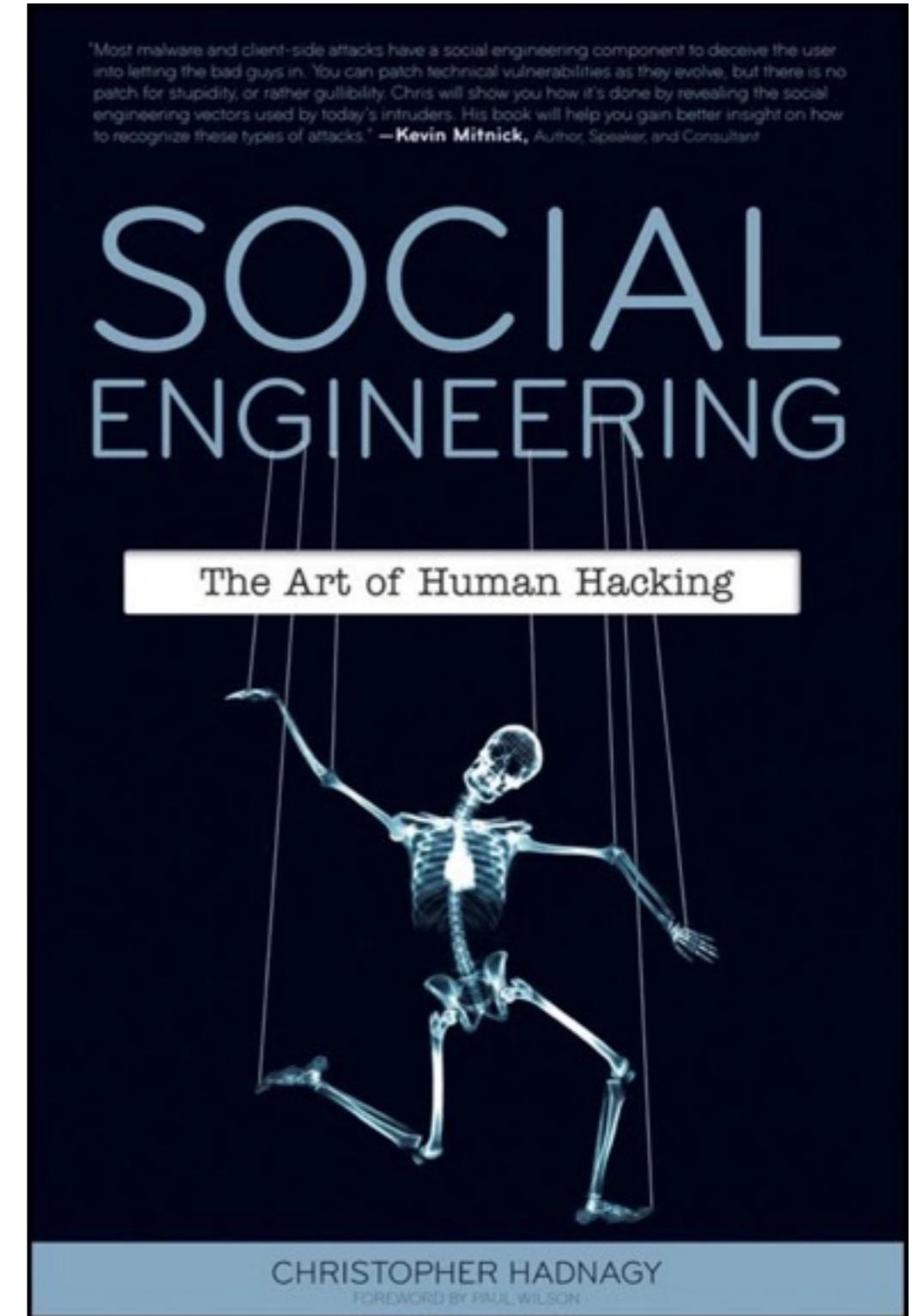
信息安全部
人
是最弱的一环！

Weakest Link

社会工程学



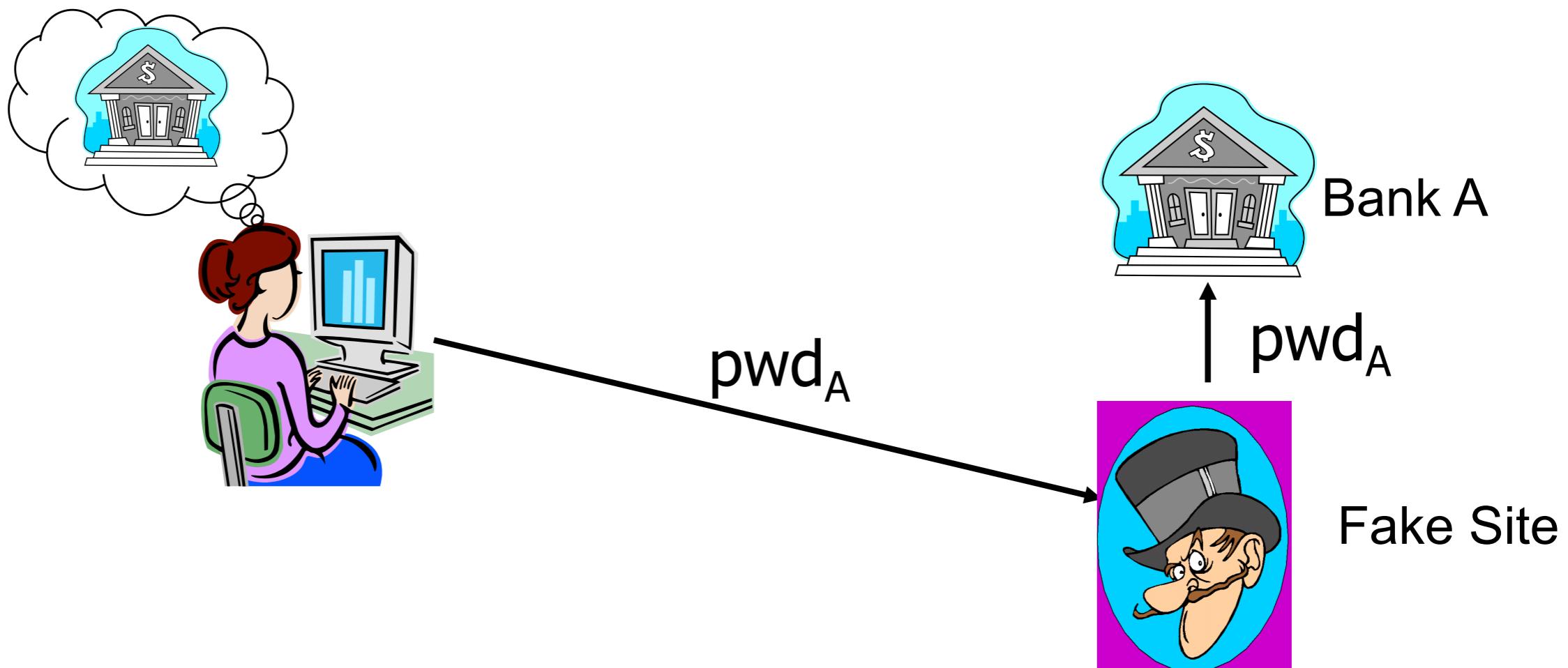
2002



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



非誠勿擾

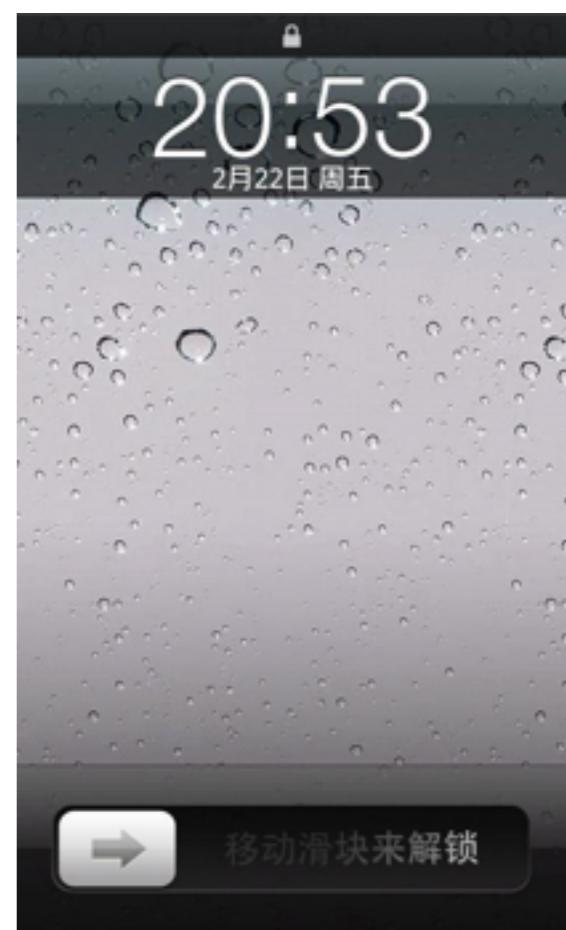
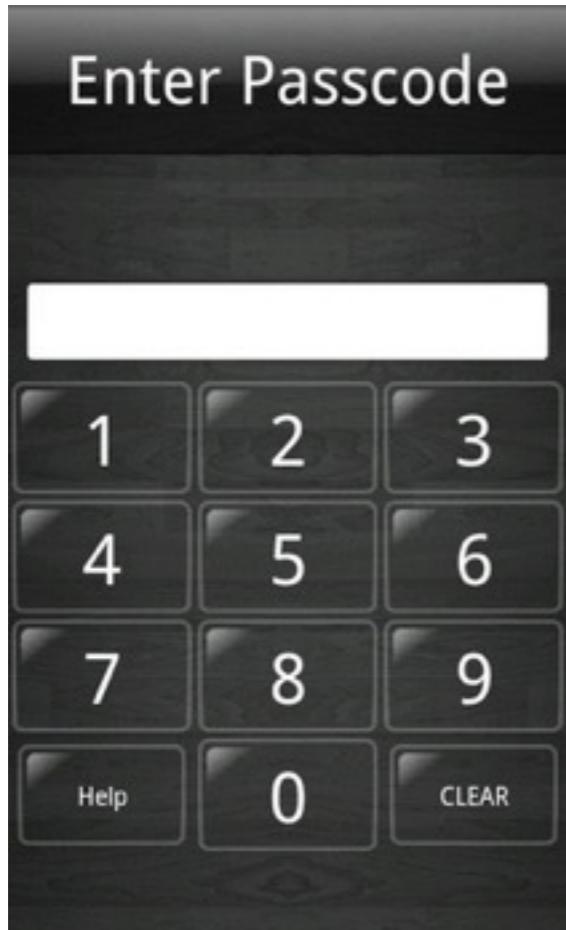
人的能力是有限的！

人是会犯错误的！

人与人是不同的！

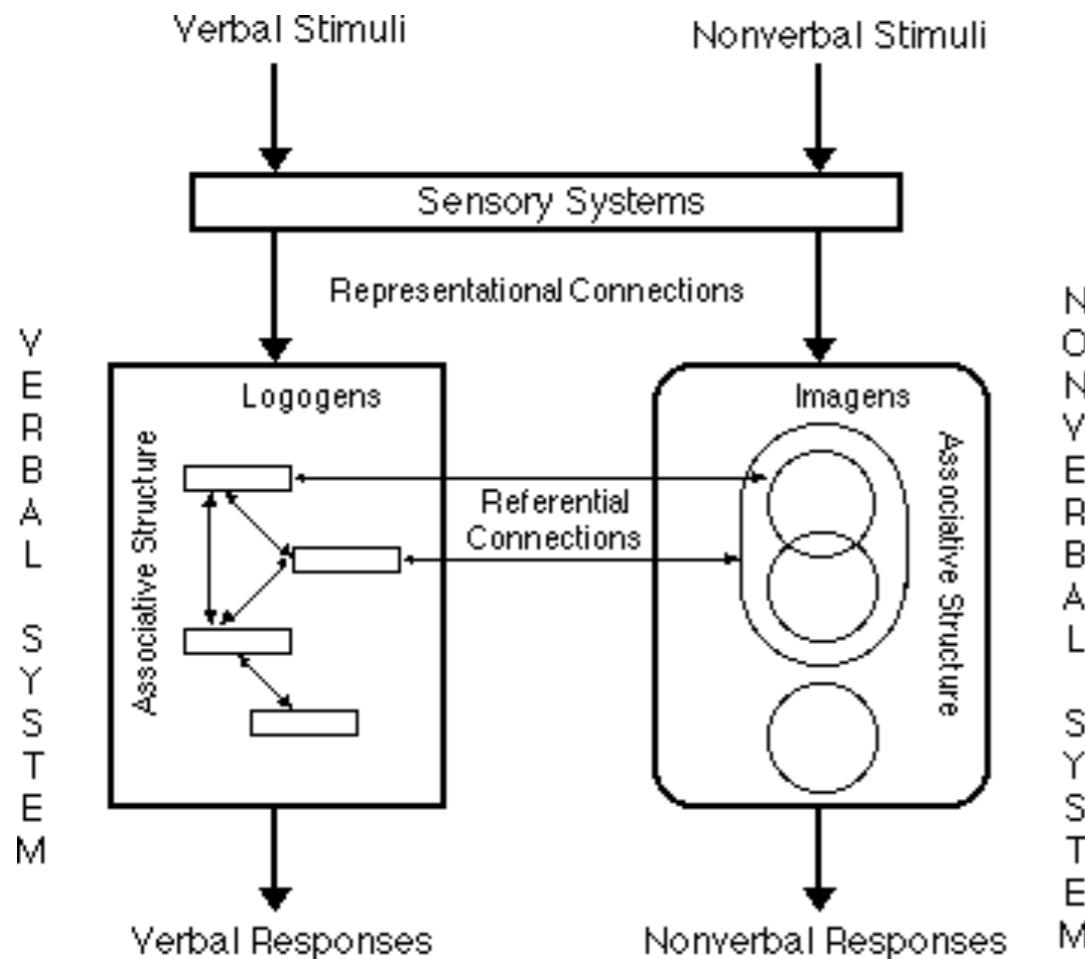
Weakest Link

手机解锁



Weakest Link

心理学基础



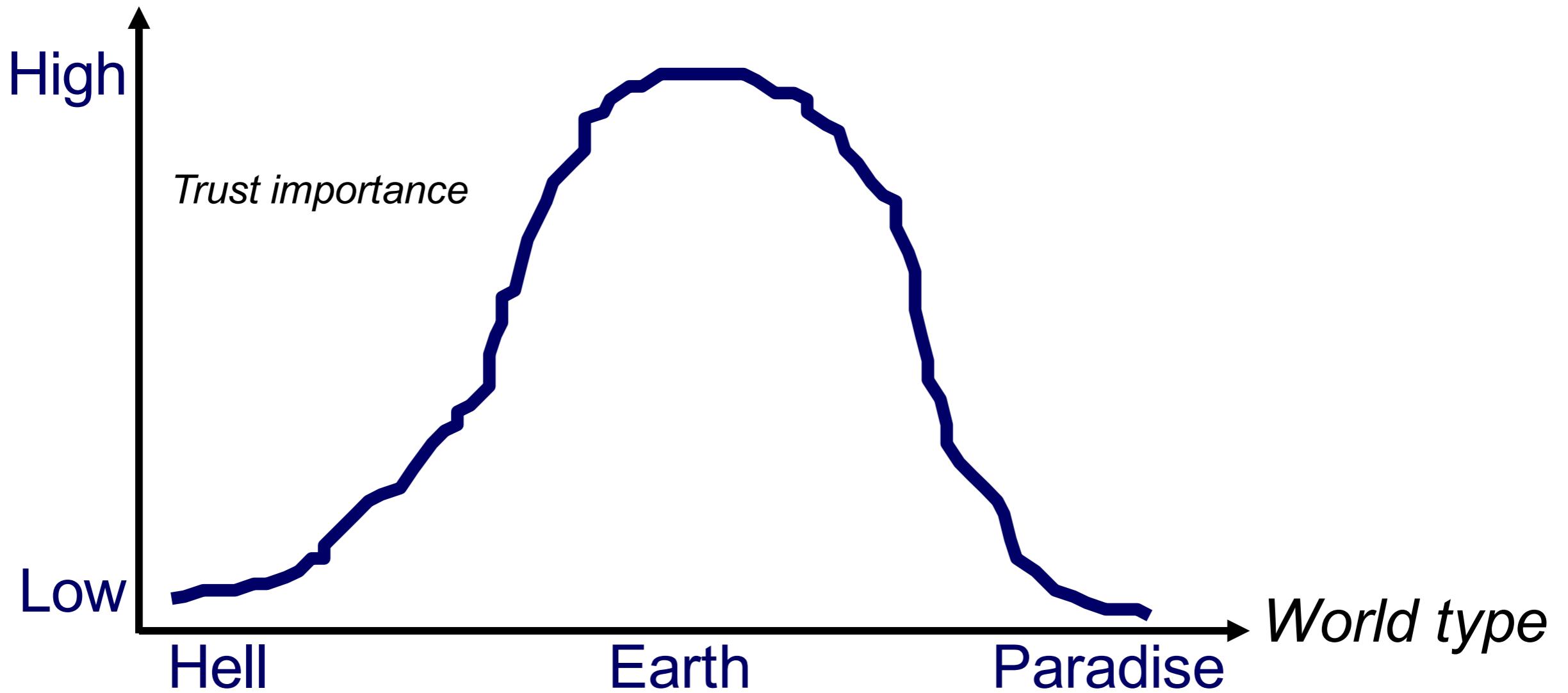
Dual Coding Theory

- Recall
- Recognition
- Cued Recall

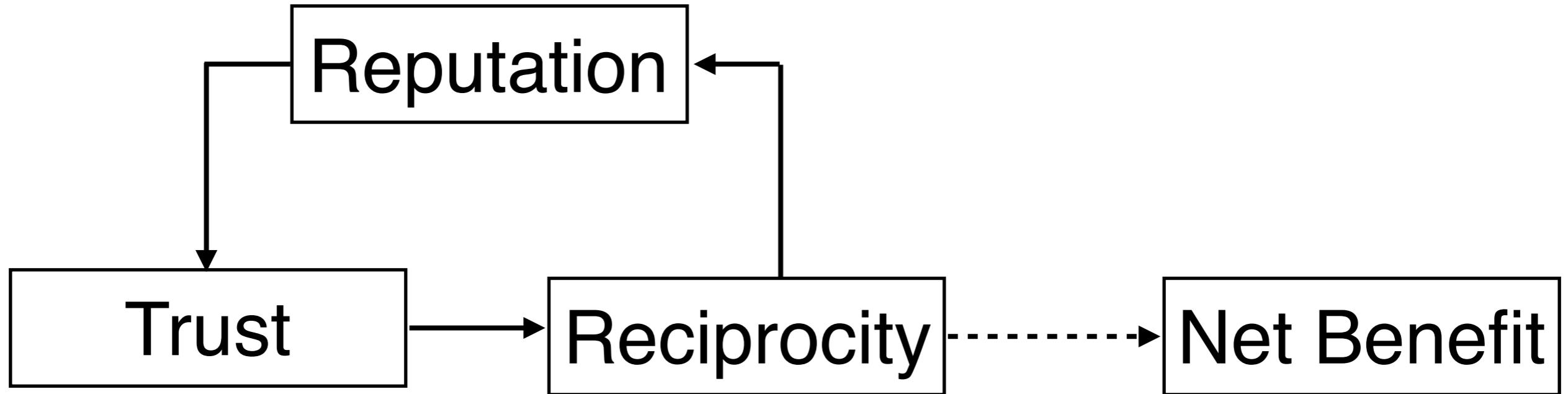
Recognition is an easier memory task than recall

With the aid of a retrieval cue, more information can be retrieved

社会学 >>> 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

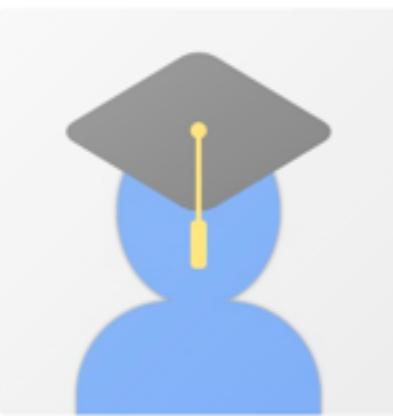
Be nice to
others who
are nice to
you



Tit-for-tat

Reputation

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](#)

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

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

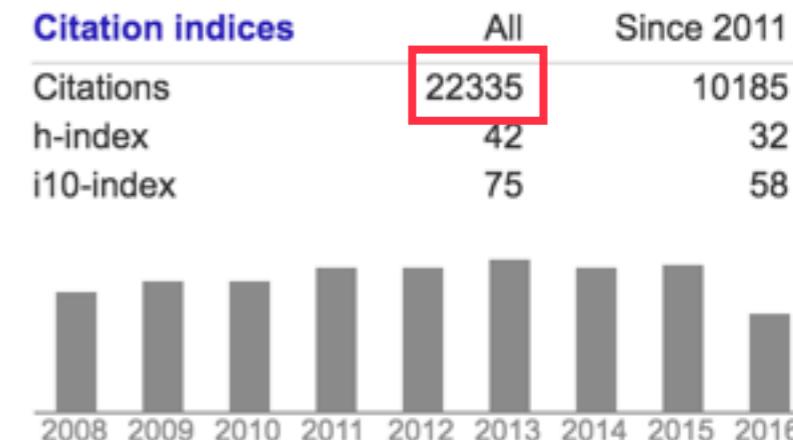
The Economics of the Internet and E-commerce 11 (2), 23-25

1840 2002

Google Scholar



[Get my own profile](#)



Co-authors [View all...](#)

John Riedl

Robert E. Kraut

Sean A. Munson

Caroline Richardson

eric friedman

Hal Varian

Online Reputation

eBay

ebay [Shop by category](#) 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: 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](#)

Located in United States

[Click to view larger image](#)

[\\$ Have one to sell? Sell now](#)

Electronics VALLEY

electronicsvalley (29672) 
99.7% Positive feedback

[Follow this seller](#)

Visit store:  [ElectronicsValley](#)

[See other items](#)



Today



Electronics VALLEY

electronicsvalley (29672) 
99.7% Positive feedback



Online Reputation

主要应用

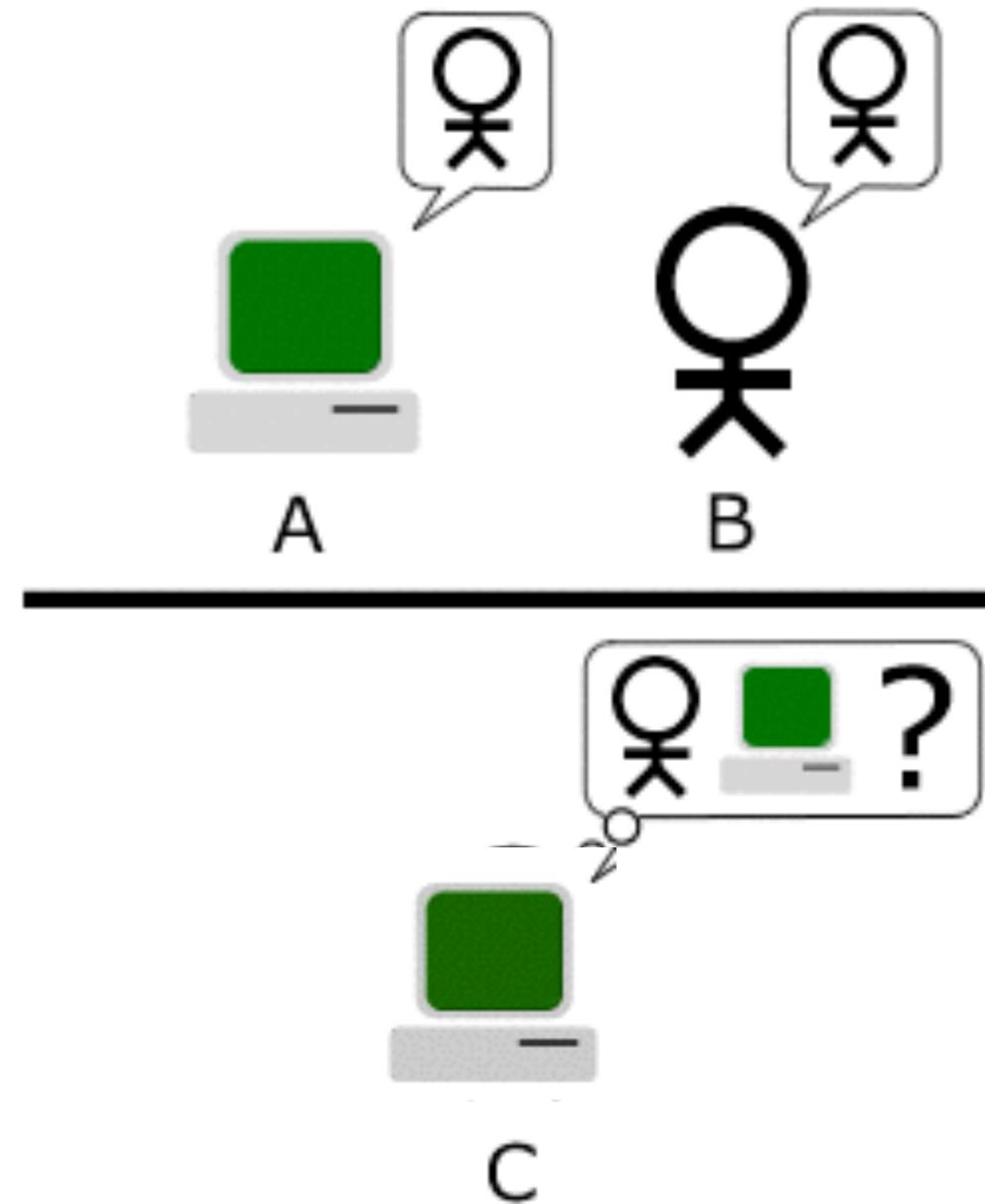
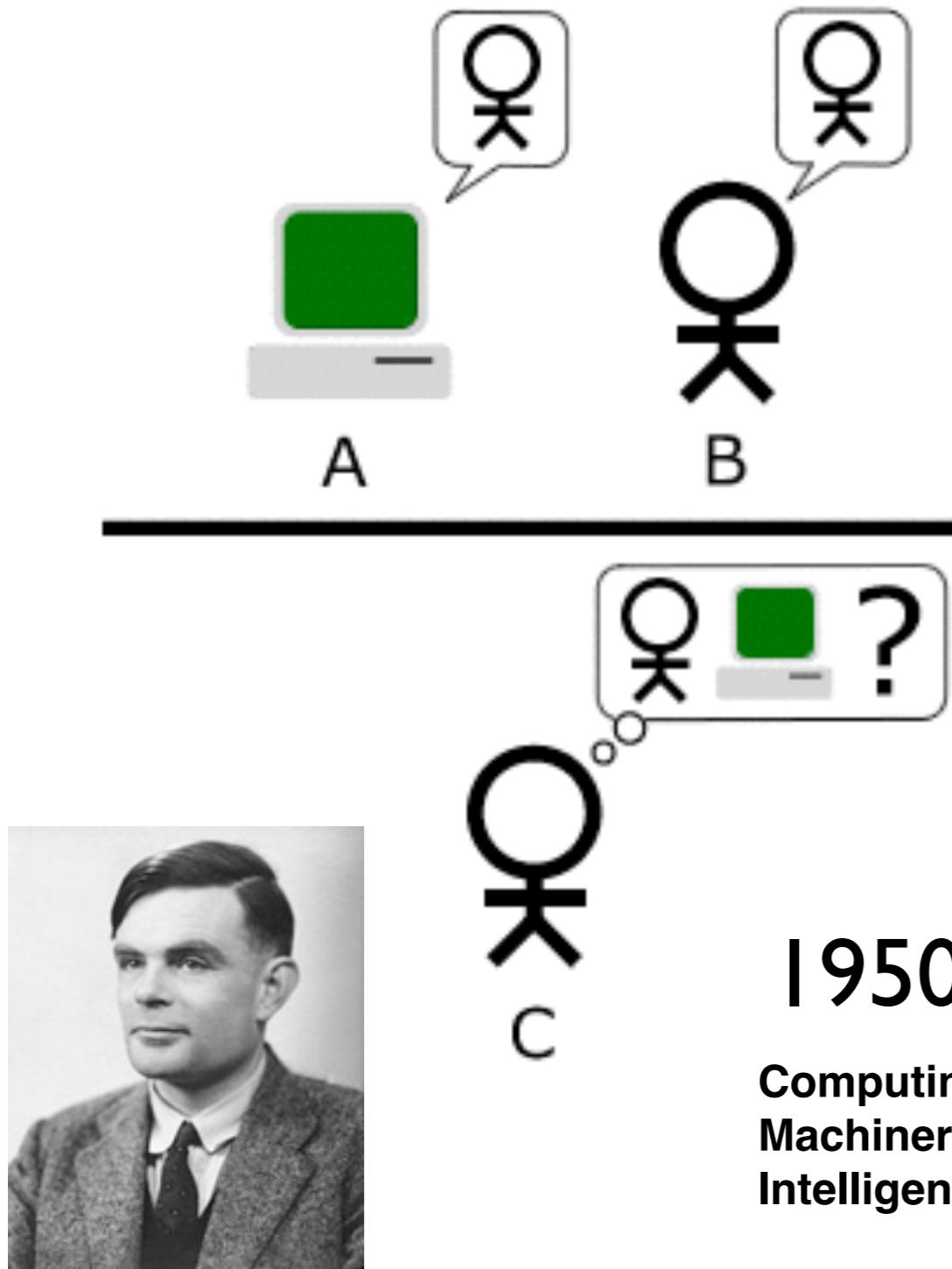
- 电子商务
- 社交网络
- 众包
- 开放协作
- 论坛
- 云计算
- 共享经济
- 金融支付
- Mooc
-



人工智能 >>> 信息安全

图灵测试 vs 反向图灵测试

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



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)

ReCAPTCHA

图片



Scanned type

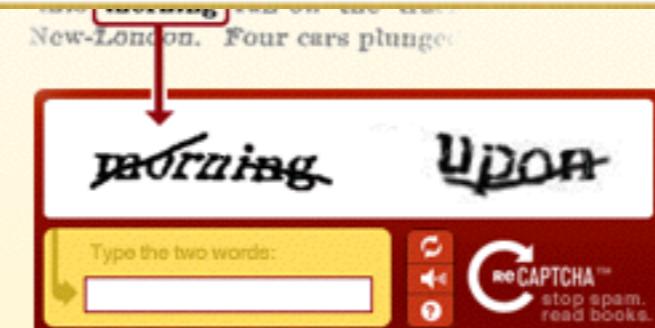
This aged portion of society were distinguished from

OCR reads as

"niis aged pntkm at society were distinguished frow."

→ W
→ G

- PROTECT YOUR EMAIL
- MY ACCOUNT
- RESOURCES: DOCS & PLUGINS



→ LEARN HOW reCAPTCHA WORKS

USE reCAPTCHA ON YOUR SITE

- 🔒 STRONG SECURITY
- 🔊 ACCESSIBLE TO BLIND USERS
- 📊 30+ MILLION SERVED DAILY

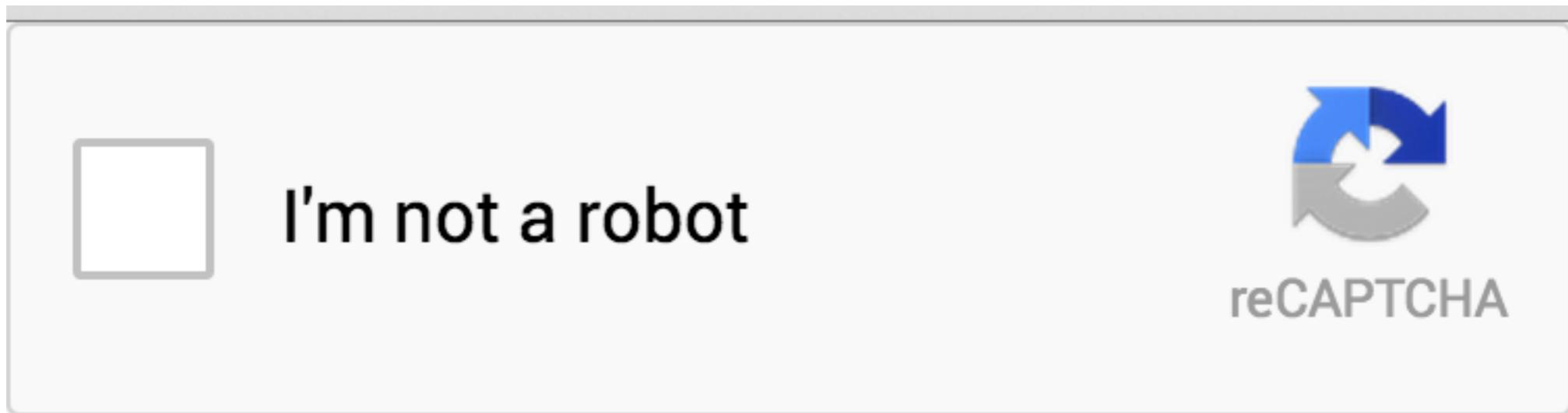
NEW See how accurate reCAPTCHA is at
digitizing content!

图书的数字化

OCR
无法识别

每天
三亿
以上

NoCAPTCHA



I'm not a robot

Select all images below that match this one:





















Verify

I'm not a robot

Select all images below that match this one:



Verify

I'm not a robot

Type the text



↻ 🔍 ⓘ

Verify

Amazon Mechanical Turk

The screenshot shows the Amazon Mechanical Turk homepage. 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 navigation bar 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: 'Find an interesting task' (blue circle with gears) → 'Work' (blue circle with a gear icon) → '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](#)'. 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: 'Fund your account' (orange circle with a plus sign) → 'Load your tasks' (orange circle with a document icon) → '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。



大数据 >>> 信息安全

数字技术威胁

- 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

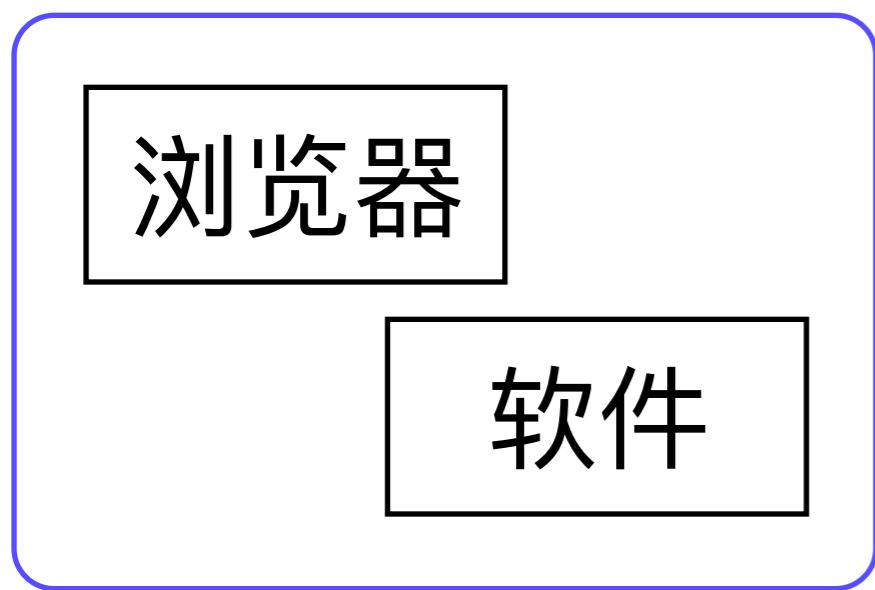
无尽的计算能力

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

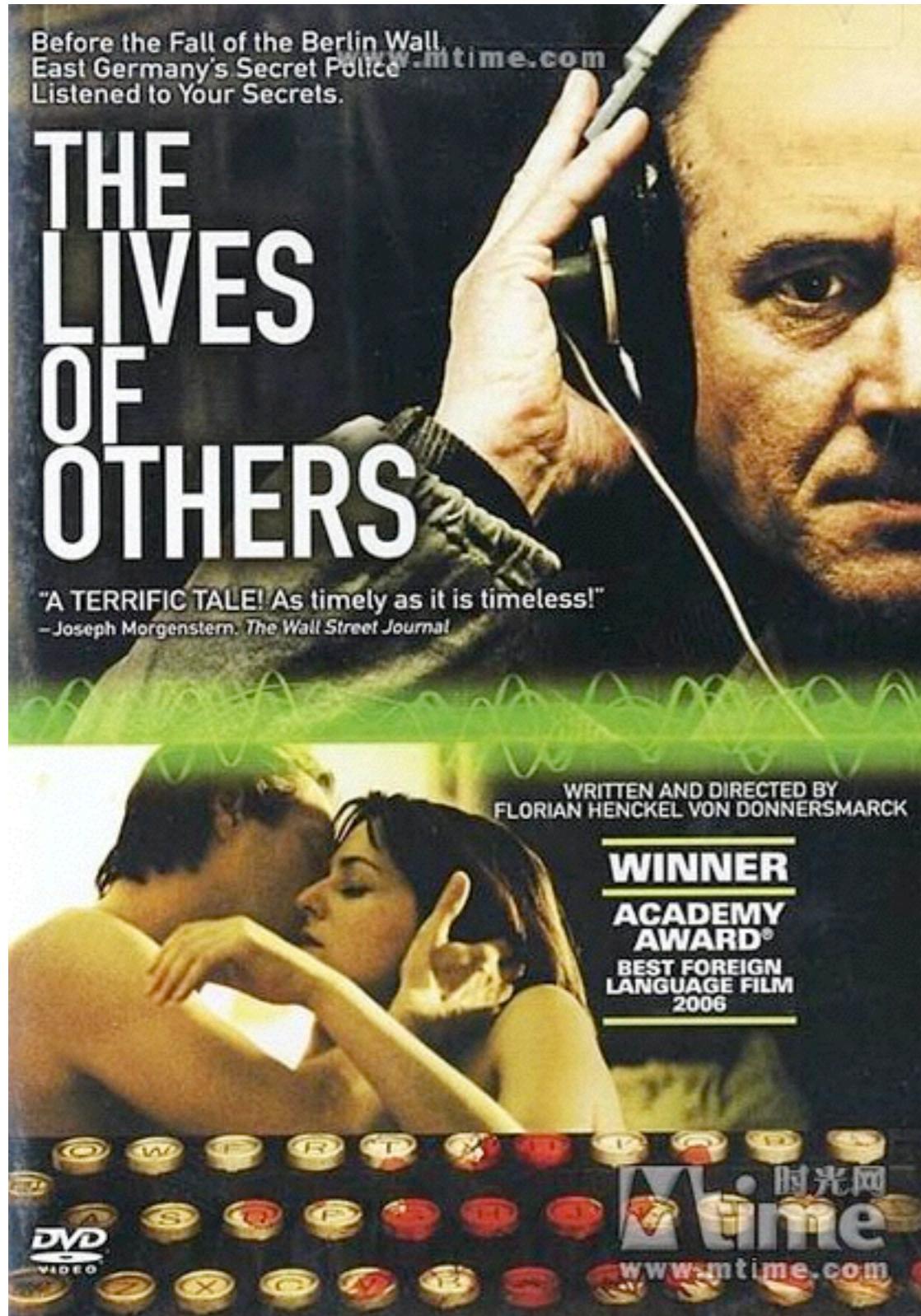
身份盗用
信用卡诈骗



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



课程内容

信息安全
经济学

可用安全

口令

生物学认证

智能手机安全

隐私

物理保护

设备指纹

验证码

网络犯罪

AI安全

众包安全

以人为本
的计算

支付安全

区块链

信誉

谢谢！

孙惠平

sunhp@ss.pku.edu.cn