

可用安全



课堂测试时间

- 1、简述信息安全工程和软件工程的区别。
- 2、简述信息安全工程分析框架中的Policy、Incentive、Mechanism和Assurance的含义。
- 3、从信息安全工程的角度分析银行卡使用会面临哪些危险。
- 4、简述Tragedy of Commons，及其在信息安全中的例子。
- 5、简述Differentiated Pricing，及其在信息安全中的例子。
- 6、阅读Why Information Security is Hard及其引用论文，你有什么感想？

上次课程内容回顾

课程简介

- 基本信息
- 课程内容
- 课程教材
- 课程组织
- 考核方式

信息安全 经济学

- 安全
- 信息安全工程
- 柠檬市场
- 网络外部性
- 考虑安全

反欺诈 信任信用

- 社会工程学
- 可用安全
- 活体检测
- 信任信誉
- 信用评分

其余

- 图灵测试
- MTurk
- 设备指纹
- 分布式系统
- 区块链

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

- 专家评估 / 用户实验 / 实际使用
- lab study / field study
- 问卷 / 访谈
- 实验人数、多个session、盲试
- IRB: 伦理审查
- 专家 / 频繁使用 / 不频繁使用 / 特殊用户
- 设备和环境的不同
- 基于Web: Amazon Mechanical Turk

- 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***

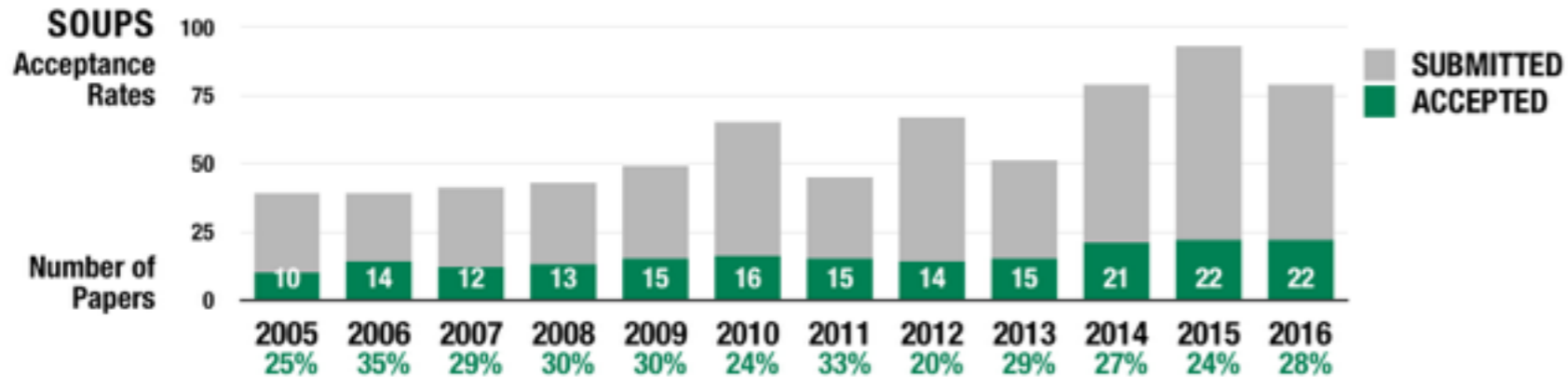
计算机能力

计算、存储、网络、普及、...

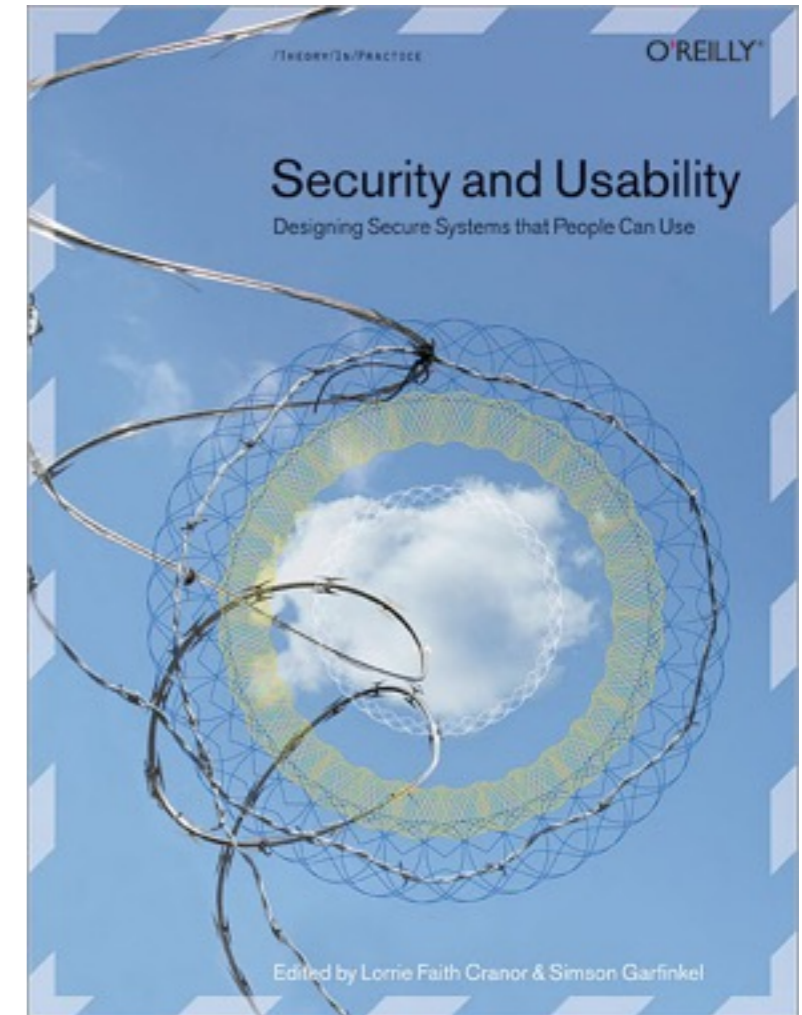
用户要求

角色、需求、竞争、消失、...

Security and Usability: Designing Secure Systems that People Can Use (2005)



<http://shop.oreilly.com/product/9780596008277.do>



- Innovative security or privacy functionality and design
- Field studies of security or privacy technology
- Usability evaluations of new or existing security or privacy features
- Security testing of new or existing usability features
- Longitudinal studies of deployed security or privacy features
- Studies of administrators or developers and support for security and privacy
- The impact of organizational policy or procurement decisions
- Lessons learned from the deployment and use of usable privacy and security features
- Foundational principles of usable security or privacy
- Ethical, psychological, sociological aspects of usable security and privacy
- Usable security and privacy implications/solutions for specific domains (e.g., IoT, medical, vulnerable populations)
- Replicating or extending important previously published studies and experiments

<http://cups.cs.cmu.edu/soups/>



Symposium on Usable Privacy and Security (2005-Present)



- 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

- 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....
- 教育培训
- 设计时就需要考虑可用性
- 设计一个**可用的安全系统**

- 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

- 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
-
- 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

用户为中心的设计

用户和安全拥有足够的通信

- 让安全机制不可见
 - 成功案例：SSH、SSL、VPN、自动更新、IBE
-
- 但是方便容易带来威胁

自动化处理

减少人机交互

- 安全与隐私可见
 - 安全与隐私更直观
 - 帮助用户做安全决策
-
- 用户是否理解，是否注意
 - 用户是否了解安全机制
 - 用户是否实际去做，是否会持续去做

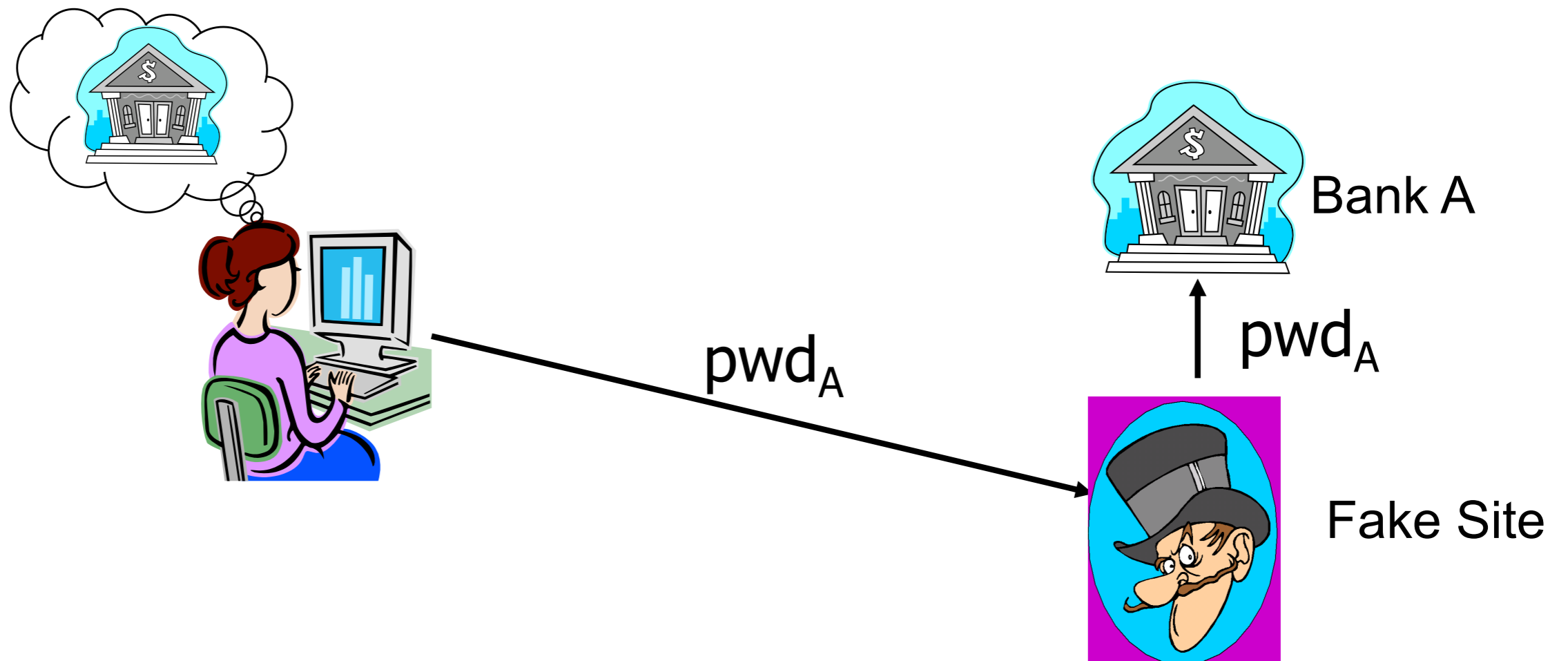
提问时间！

人的能力是有限的！

人是会犯错误的！

人与人是不同的！

- 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



Usable Security Example

证书



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

- The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
- The security certificate has expired or is not yet valid.
- The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?



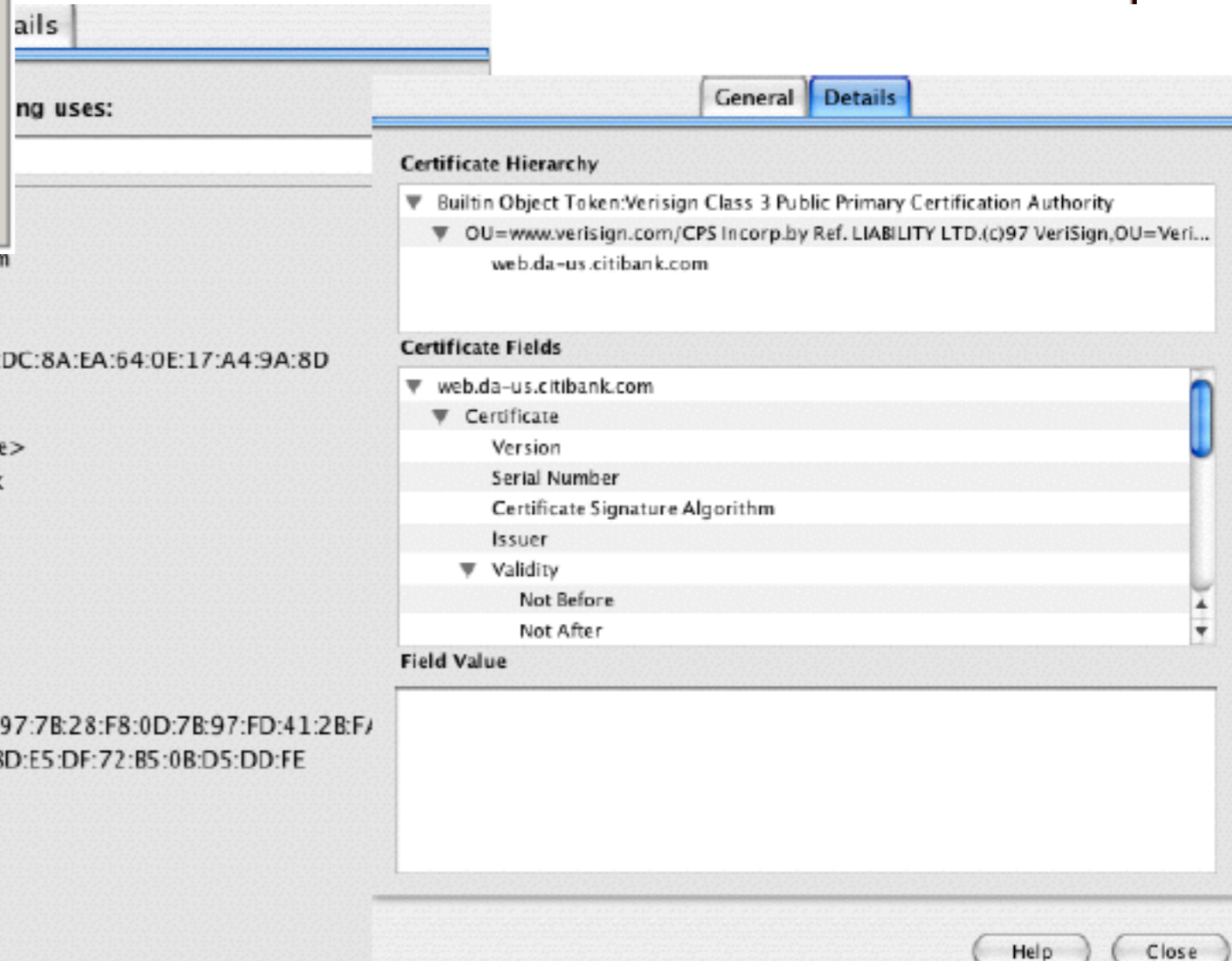
The site's security certificate is not trusted!

You attempted to reach lerisse.ece.ubc.ca, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, **especially** if you have never seen this warning before for this site.

[Help me understand](#)

**Say
OK to
Any
Question
About
Security**

Common Name (LN)	web.da-us.citibank.com
Organization (O)	Citigroup
Organizational Unit (OU)	GSO
Serial Number	58:A4:AB:20:81:75:DD:DC:8A:EA:64:0E:17:A4:9A:8D
Issued By	
Common Name (CN)	<Not Part Of Certificate>
Organization (O)	VeriSign Trust Network
Organizational Unit (OU)	VeriSign, Inc.
Validity	
Issued On	7/21/04
Expires On	7/22/06
Fingerprints	
SHA1 Fingerprint	D5:5E:D1:03:EA:70:3A:97:7B:28:F8:0D:7B:97:FD:41:2B:F7
MD5 Fingerprint	AB:DB:89:FA:9E:B6:FA:8D:E5:DF:72:B5:0B:D5:DD:FE



ails

ng uses:

General Details

Certificate Hierarchy

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

Certificate Fields

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

Field Value

Help Close

- 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

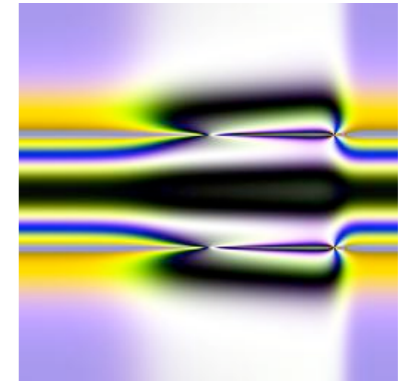
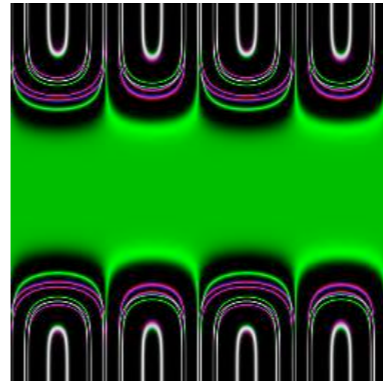
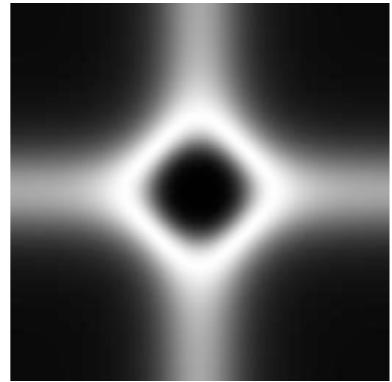
Table 1. Password characteristics.

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

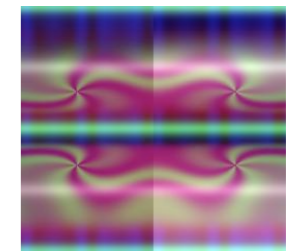
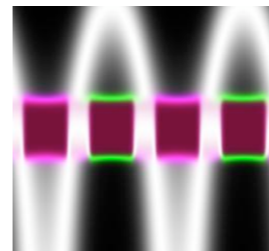
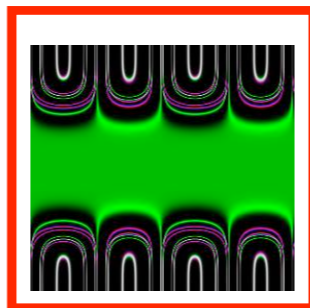
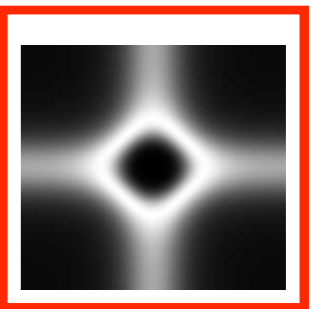
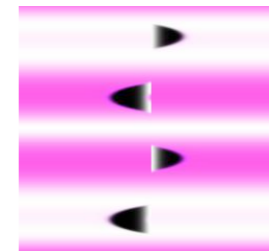
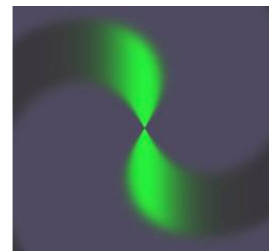
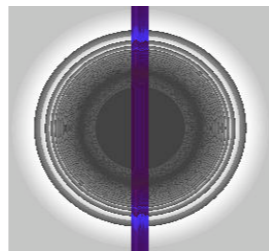
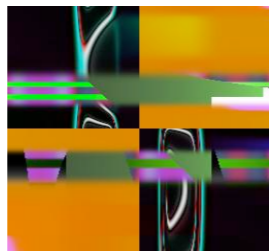
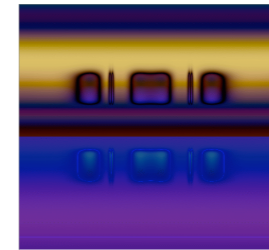
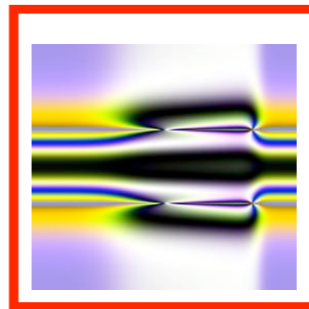
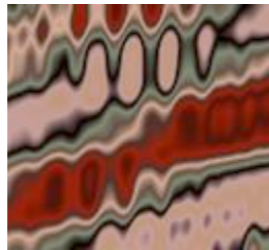
- 密码要足够长（至少7个字符）
- 包括大小写字母、数字和符号
- 六位必须至少有一个符号字符
- 至少使用四个不同的字符（不要重复同一字符）
- 使用随机数和字母
- 不要使用全部或部分登录名
- 不要使用任何语言中的实际词
- 不要使用数字代替类似的字母来构成单词
- 不要使用连续字母或数字（如“abcdefg”或“234567”）
- 不要使用键盘中的邻近键（如“qwerty”）

Déjà Vu

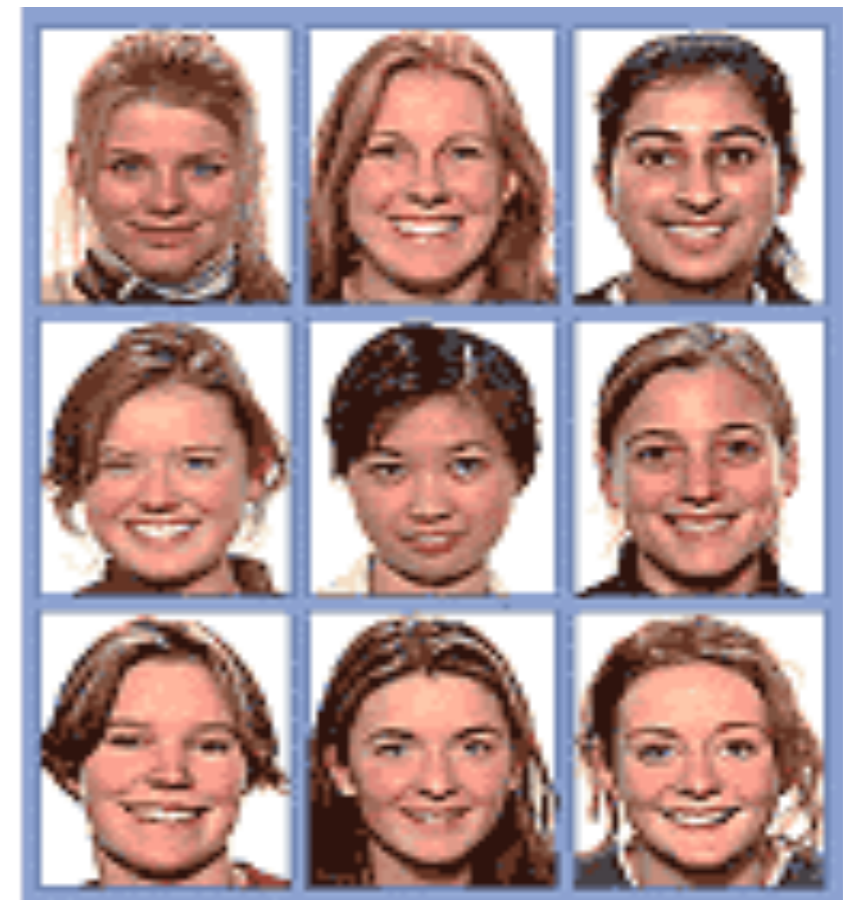
训练



挑战



- 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）



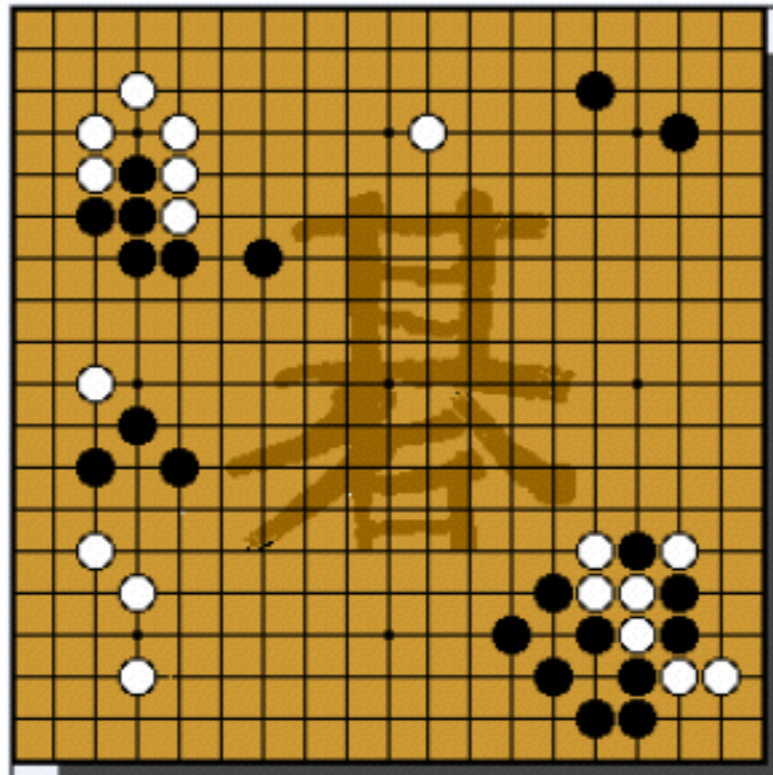


Figure 1 Go game

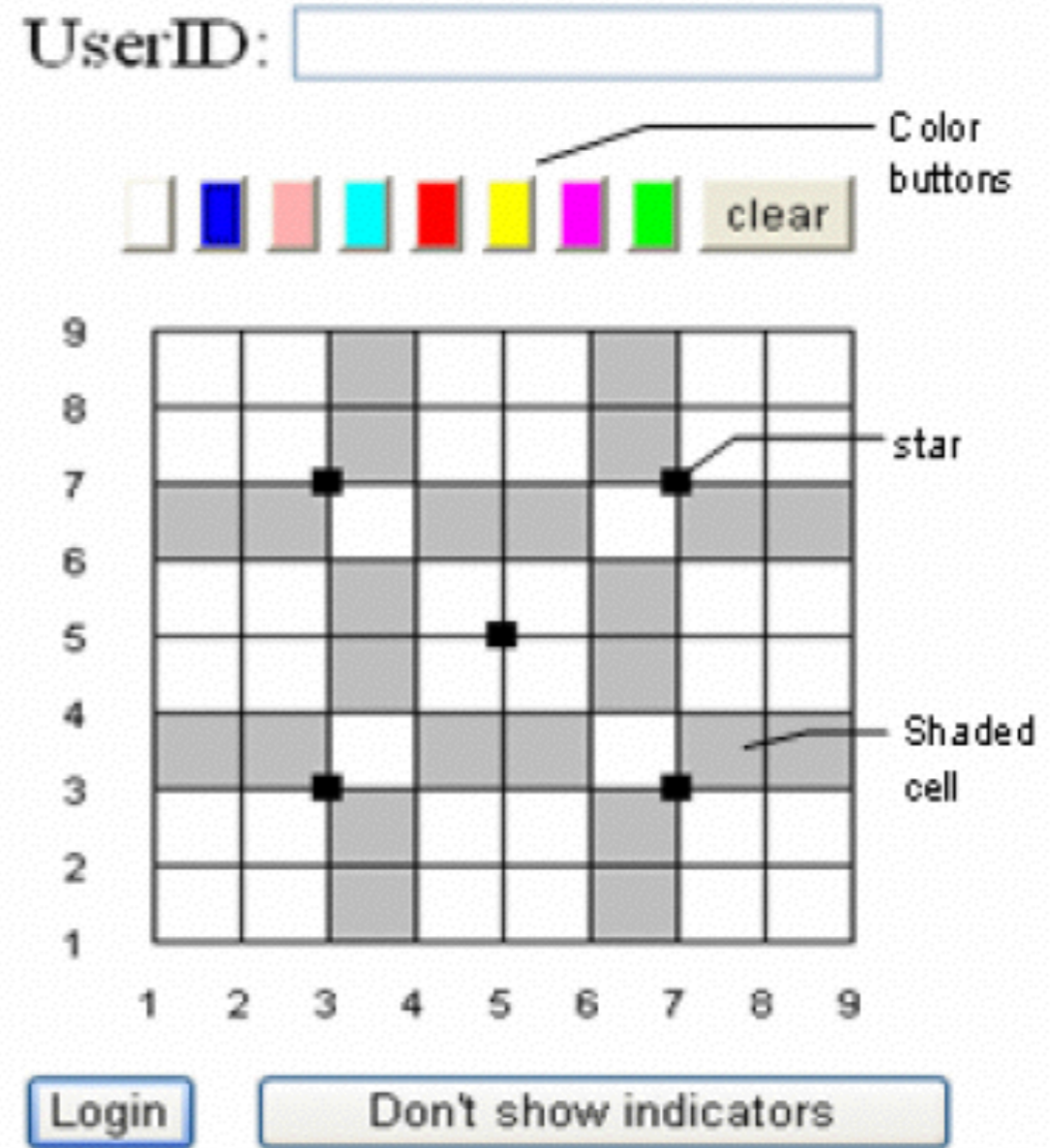
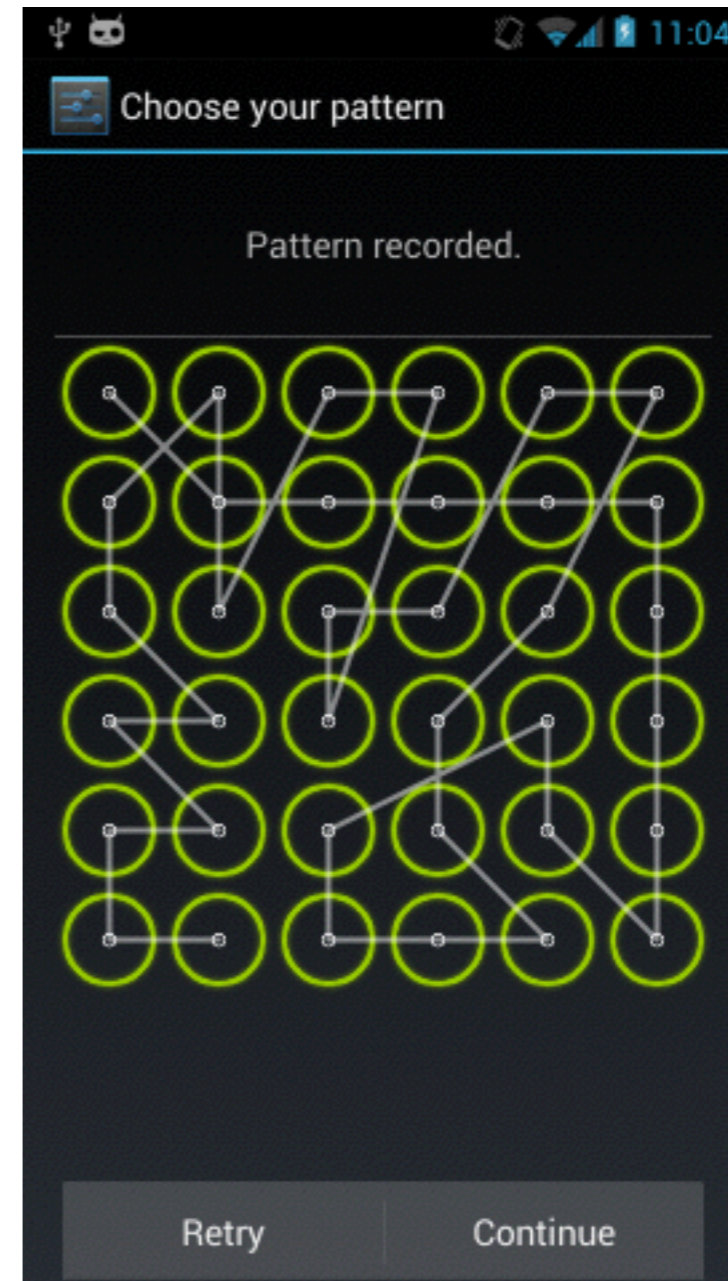


Figure 22 Main login interface

Pattern Lock



- 网站点隐私策略

- ✳ 很多，但用户很少读

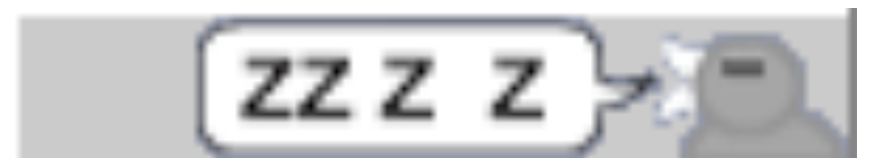
- Privacy Bird

- ✳ 决定是否站点策略和用户隐私策略项匹配

- ✳ 通知用户



<http://www.privacybird.org/>



提问时间！

课后作业

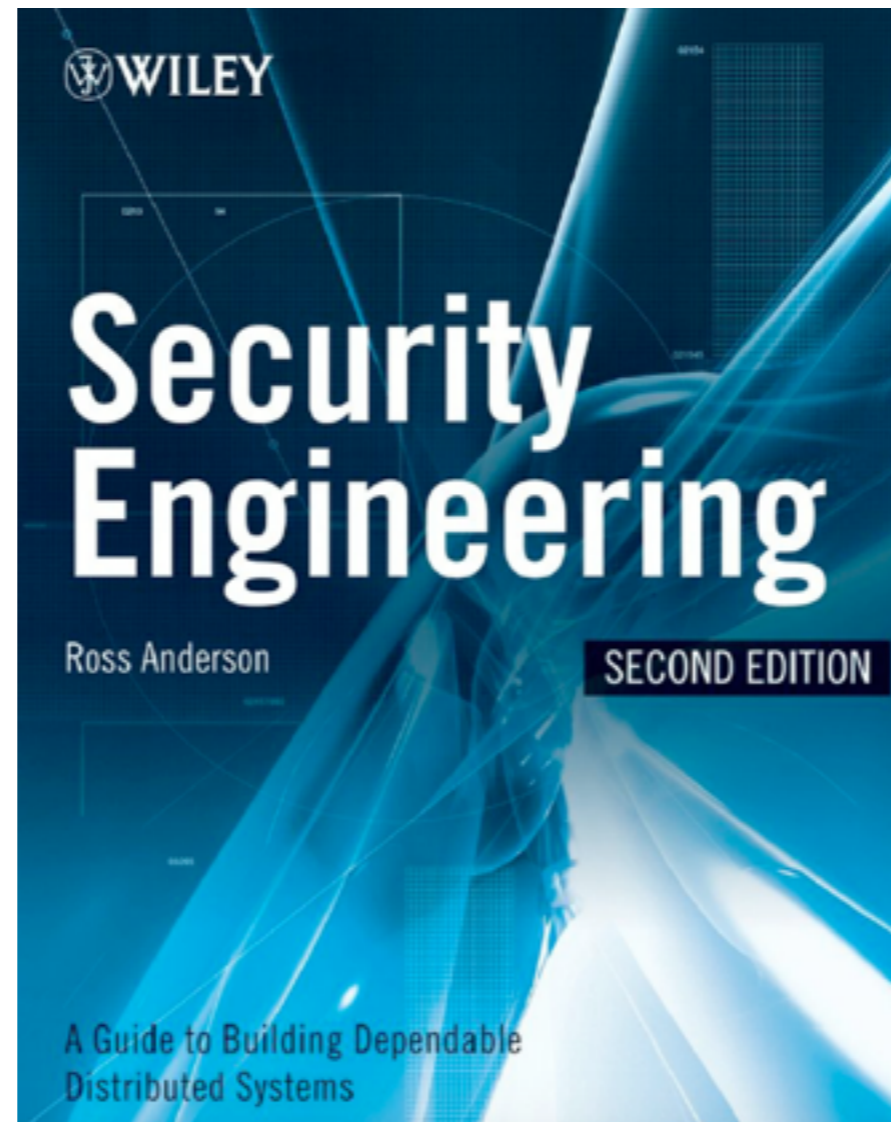
```
graph LR; A[阅读教材] --> B[阅读论文]; B --> C[思考]; C --> D[撰写报告];
```

阅读教材

阅读论文

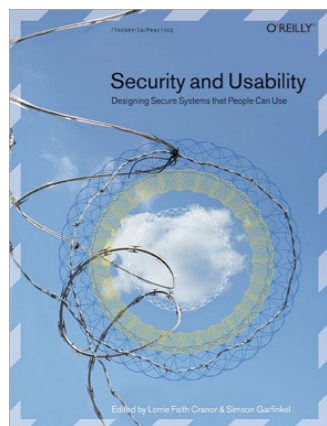
思考

撰写报告



阅读第二章

要求阅读如下文章，写阅读报告



Book Chapter 2005

Usable Security **Why Do We Need It? How Do We Get It?**

M. ANGELA SASSE AND IVAN FLECHAIS

- 1、文章概述
- 2、主要收获
- 3、存在疑问
- 4、所思所感
- 5、一篇论文

周六晚上12点
前提交

检索一篇Usable Security相关的2017-2018的
论文，简单阅读，杂志的文章最好

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

<https://huipingsun.github.io>