CHI'15-Al-Ameen-Towards Making Random Passwords Memorable: Leveraging Users' Cognitive Ability Through Multiple Cues.

概述：(S) 如何构造易记忆的，系统分配的随机口令一直是一个难题。(T) 本文旨在提供一种帮助用户记忆系统生成的随机口令的方法。(A) 通过构造图形口令，并为用户提供visual, verbal和spatial的多种cue帮助用户记忆口令，并且采用variant response抵抗shoulder surfing和keystroke loggers攻击，并通过implicit response保证攻击无法从响应中获取有效信息；生成口令熵约为28bit (R) 通过用户调研表明用户对方案满意度较高，虽然登录时间较长，但可记性较高（与文本口令对比）

优点：① 从心理学的角度给出了提升用户记忆图形口令的能力，例如多cue，较有说服力

② 本文给出的用户调研的论述较好，且讨论部分的分析比较清晰

问题：① 本文引言中论述系统应为用户分配口令的优势，但考虑到本文研究人和交互具很多不同的研究表明用户不愿意放弃自己生成和管理的权利

② 在对Biddle提出的7点图形口令的要求的论述中，与文本口令的对比不够客观公平，因为这是两个用户群体在不同时间测试，结果不可用于直接比较。

③ 根据Usenix'14的研究，老年人可能产生self-efficiacy自我怀疑，进而使登录和注册时间增加使CuedR较难应用。

1、如何使系统为用户生成的口令更容易记忆依然是一个挑战。

▲本文提出新的认证方式应更好地利用人的认知能力，并且可以适应不同学习风格的用户。

2、CuedR系统设计

1> 从不同的组合中为用户随机分配6个keywords.

提供了三种cue，即graphical, verbal, spatial.

▲每一个页面包含26个图案，对应a-z，26个字母分别对应26个keywords.

每次页面加载后，用户可以找到keywords对应的字母，并依次输入字母

▲在此过程中每一次keywords对应的字母会发生改变，提供variant response属性.

→可以更好地抵抗 shoulder surfing 和 simple keystroke loggers 攻击.

2> 用户注册时，系统为用户生成6个图案页面并分发给用户关键字

登录时需在6个页面中依次输入字母值.

当用户的输入出现错误时，CuedR会显示一个不同于注册时的图案页面，这一点作为输入错误的implicit feedback，而攻击者无法分辨.

▲ Implicit feedback is thus a desirable feature to enhance usability when passwords have multiple parts.

3> 6个keywords可以加盐并使用慢哈希函数哈希后进行存储.

3、CuedR在认知心理学角度的设计要点（如何做到容易记忆）

1> Long-Term Memory：想要短期记忆变成长期记忆，必须对信息做进一步的处理和编码，且最好该信息与有意义的信息可以相关联，例如cue.

2> 在恢复口令时，采用的是更容易的recognition.

3> 心理学表明，没有cue，将很难主动地记住信息，而cue最好在刚记忆时出现.

CuedR提供多种cue，用户只需记忆部分cue即可回忆起keywords

▲另外，用户记忆图形能力比记忆文本强。→ picture superiority effect.

在CuedR中，keyword和cue在图案中的位置是不变的（无论什么时候加载图案页面）

4、2011年 Biddle 提出了7个图形口令方案应具备的功能.

1> 理论口令空间应符合 intended domain 的安全策略

口令空间为：$\log_2(26)^6 \approx 28$ bit，符合安全策略要求

2> 避免由于用户选择口令而导致安全性降低

CuedR提供了两个安全特性，① 有效口令空间和理论口令空间相等，而非由于用户选择而导致的非均匀分布。② 为用户选择提供了弹性，但可以避免用户重用口令或使用PIN带来的问题

3> 通过variant response，对shoulder surfing和key logging有抵抗能力

若攻击可以用摄像机同时记录monitor和keystroke，则建议用户在安全的环境注册.

4> 使用cue来增强可记忆性

提供多种cue，允许用户使用自己熟悉的cue来记忆 keywords

5> 可用性可以与文本口令相比，甚至比文本口令好.

通过对比用户对文本口令（最简单的口令策略 basic12）和 CuedR 的记忆能力的对比（其中文本口令的研究是先前的），发现CuedR甚至比文本口令更高.（尽管 CuedR 的登录时间较长，但仍有84%的参与者(51)愿意在实际生活中使用.

6> 当口令由多个部分构成时，可以为合法用户提供 implicit feedback.

本文提供了该特征，由于用户可以区分图案的类别，故可快速得知先前步骤出错

7> 尽可能利用现存的用户已有的知识构造.

例如添加用户个人照片作为线索，防止字典猜测攻击。但本文未提供该功能

5、讨论（37个学生的用户调研）

1> 92%参与者报告图片always或often作为回忆口令的cue，62% spatial，43% phrase，14% number.（表明多种cue有助于用户回忆口令）

2> 当参与者使用多个口令时，3个网站，11位参与者，所有参与者可以在3次尝试中登录成功（login1 login2 一周后）

3> Impact：采用多种cue帮助用户记忆系统分配的口令，83.8%用户使用多种cue记忆

4> Acceptance：84%的参与者愿意将CuedR作为文本口令的替代品

5> Applications：认为该方案耗时比文本口令长，但可以用于对安全性需求较高的认证场景