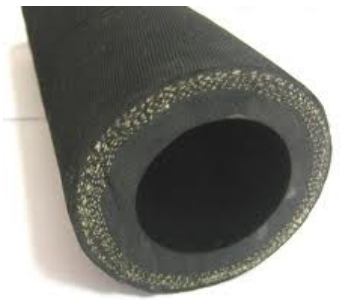


Neuroscience Meets Cryptography:

*Designing Crypto Primitives Secure
Against Rubber Hose Attacks*

Hristo Bojinov | Daniel Sanchez | Paul Reber | Dan Boneh | Patrick Lincoln

rubber-hose cryptanalysis



UN NEWS CENTRE

With breaking :
newswire

[Home](#) | [Press Room](#) | [Multimedia](#) | [Tools & Services](#) | [Resources](#) | [News Focus](#) | [What, When a](#)



Print



Email



Share

12



Like

Many countries still appear willing to use torture, warns UN human rights official

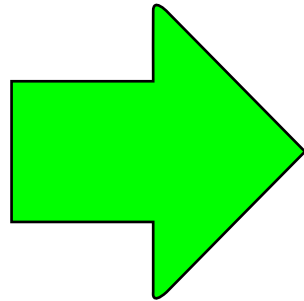


Van Boven
briefs
press

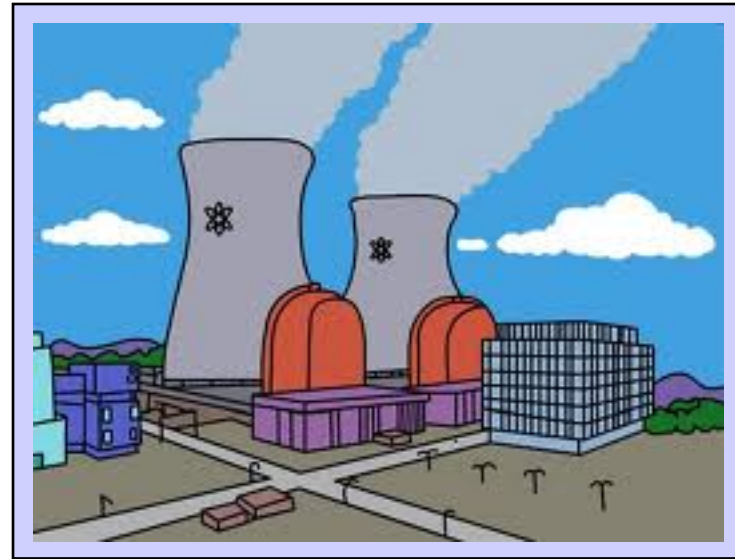
27 October 2004 – Torture and cruel, inhuman or degrading punishment continue to be meted out by many States, often in the name of fighting terrorism, a United Nations human rights expert warns as he calls for a complete prohibition on the practice.

The warning came from Theo van Boven, Special Rapporteur on torture, as he presented his annual **report** to the General Assembly's social, humanitarian and cultural committee. The committee also heard reports by the Special Rapporteurs on extrajudicial, summary or arbitrary executions; the freedom of religion or belief; the right to food; and the human rights of migrants.

access to a secure facility

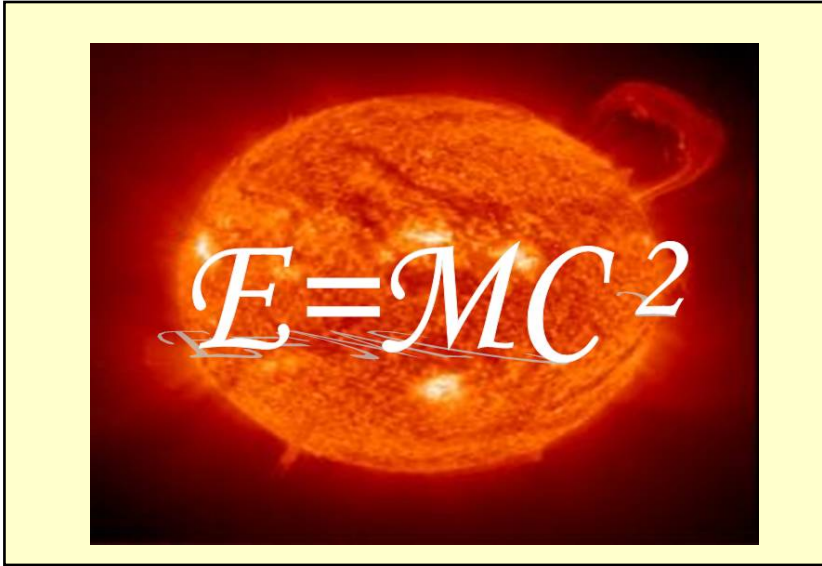


in-person authentication



Goal: Passwords that cannot be revealed consciously.

human memory systems



declarative

vs.

procedural

procedural memory is "implicit"

rubber hose-resistant passwords

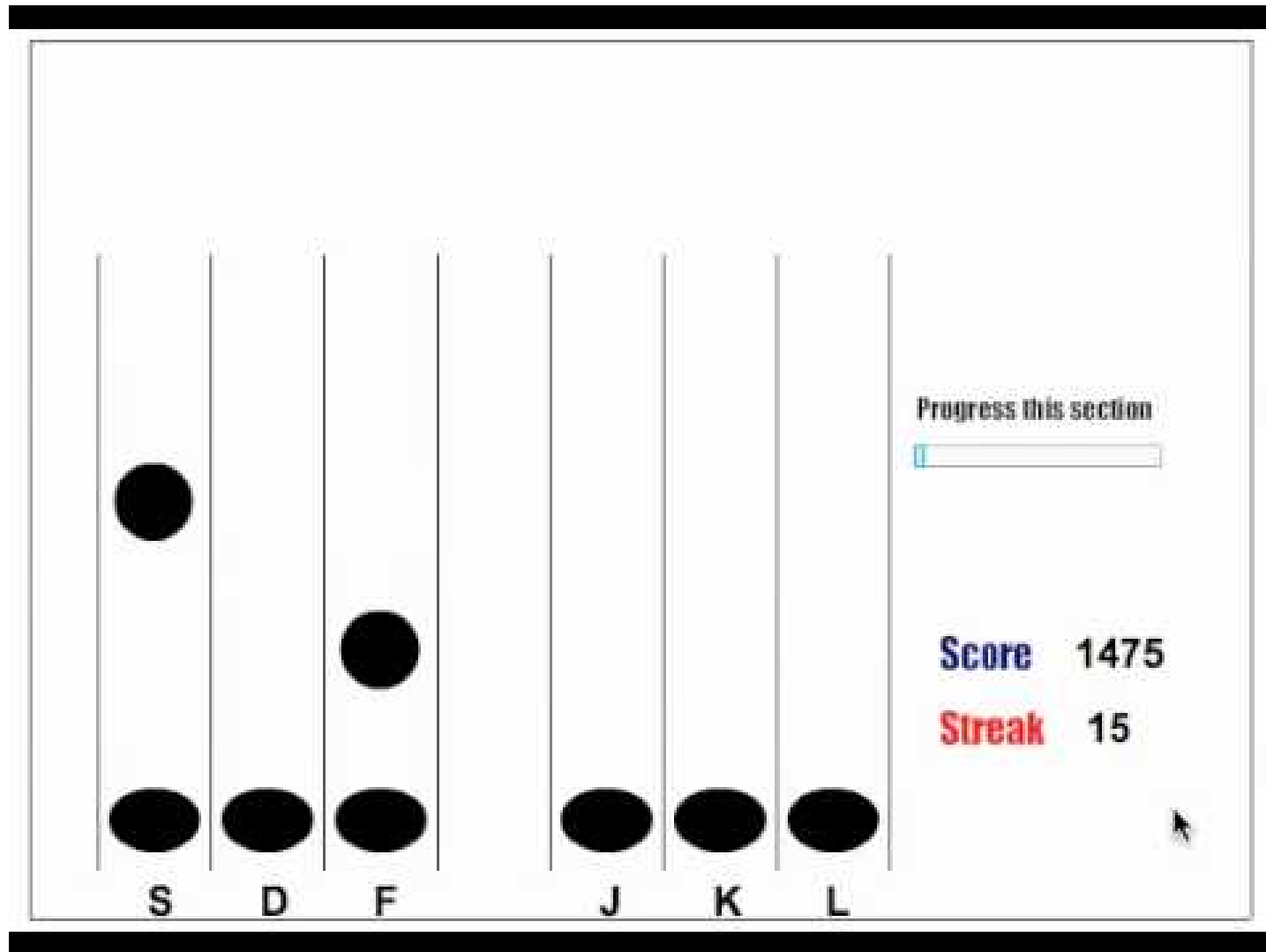
teach the user a skill (in a game)

authenticate by measuring the skill

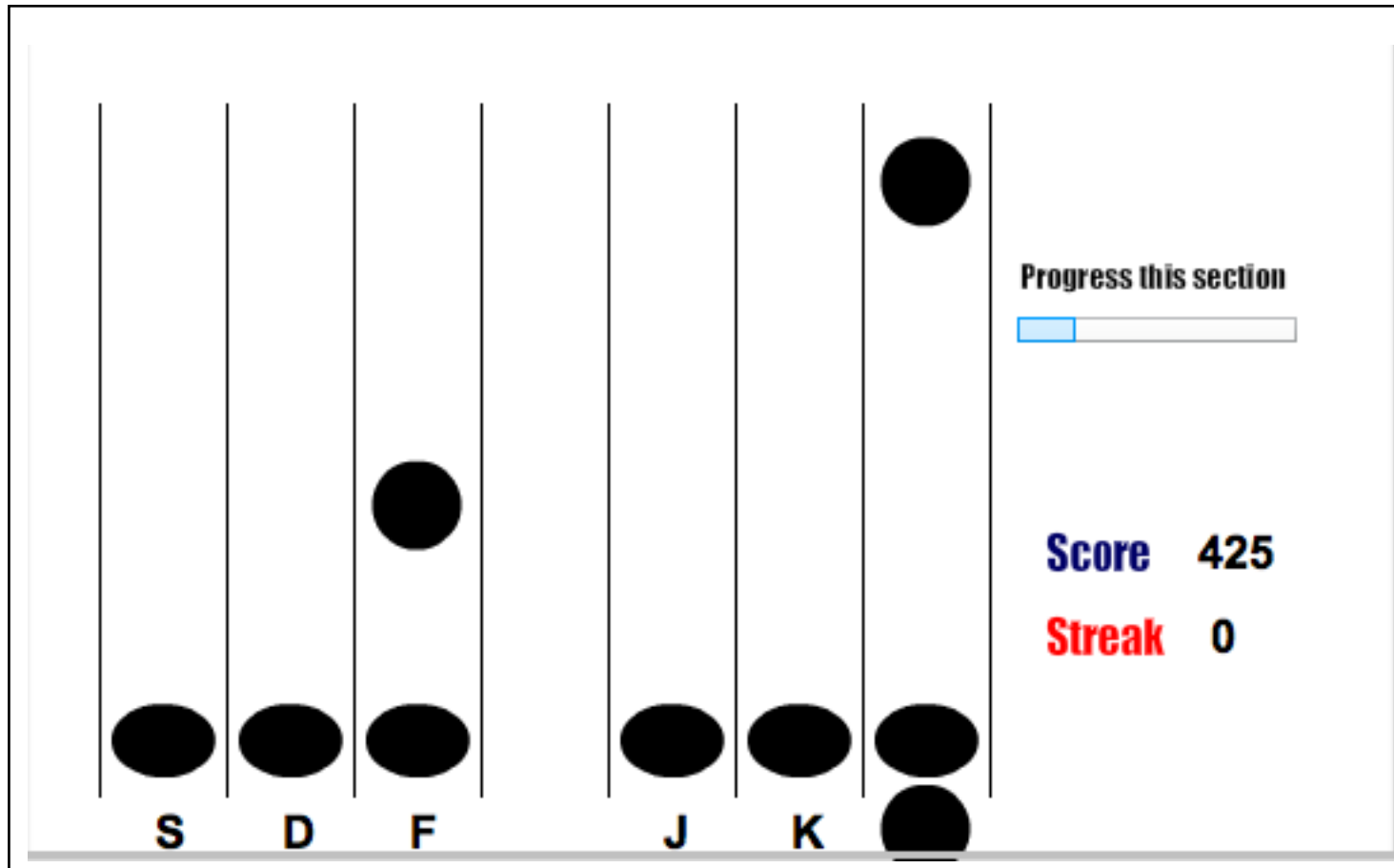
guitar hero



our authentication game



our authentication game



cost of training and authentication

training: 30-40 min

authentication: 5-10 min

designing the game

Serial Interception Sequence Learning

user trains with a sequence

test: trained vs. unknown (% correct)

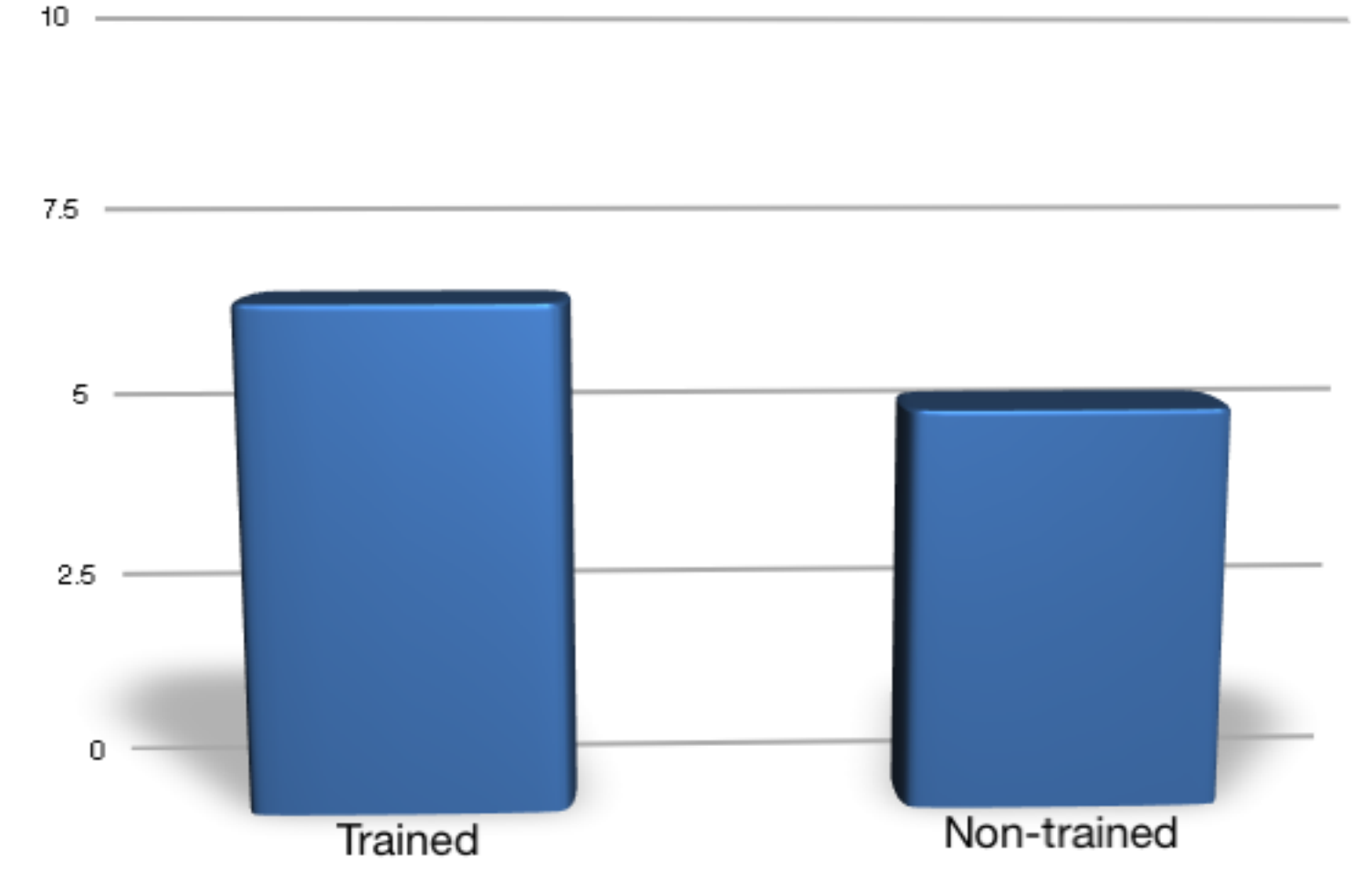
also test explicitly

the key point

Users don't recognize their sequences in explicit tests.

"... When I played the tempo was so high it was incredibly difficult to keep a track of the circles. Most of the time my fingers moved by themselves, at least it felt that way. ..."

recognition experiment



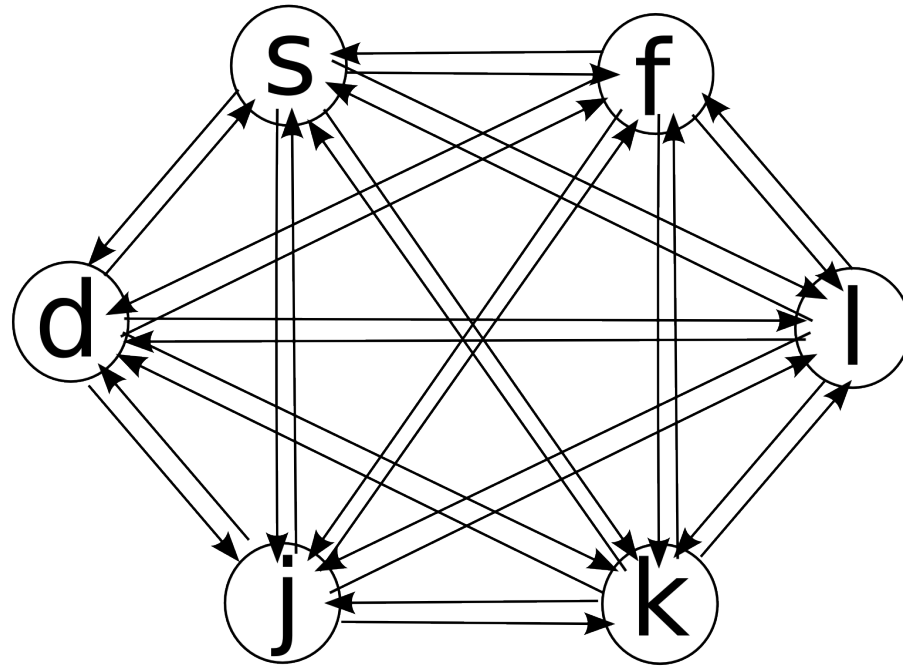
sequences for authentication

uniform single-character distribution

uniform pair (bigram) distribution

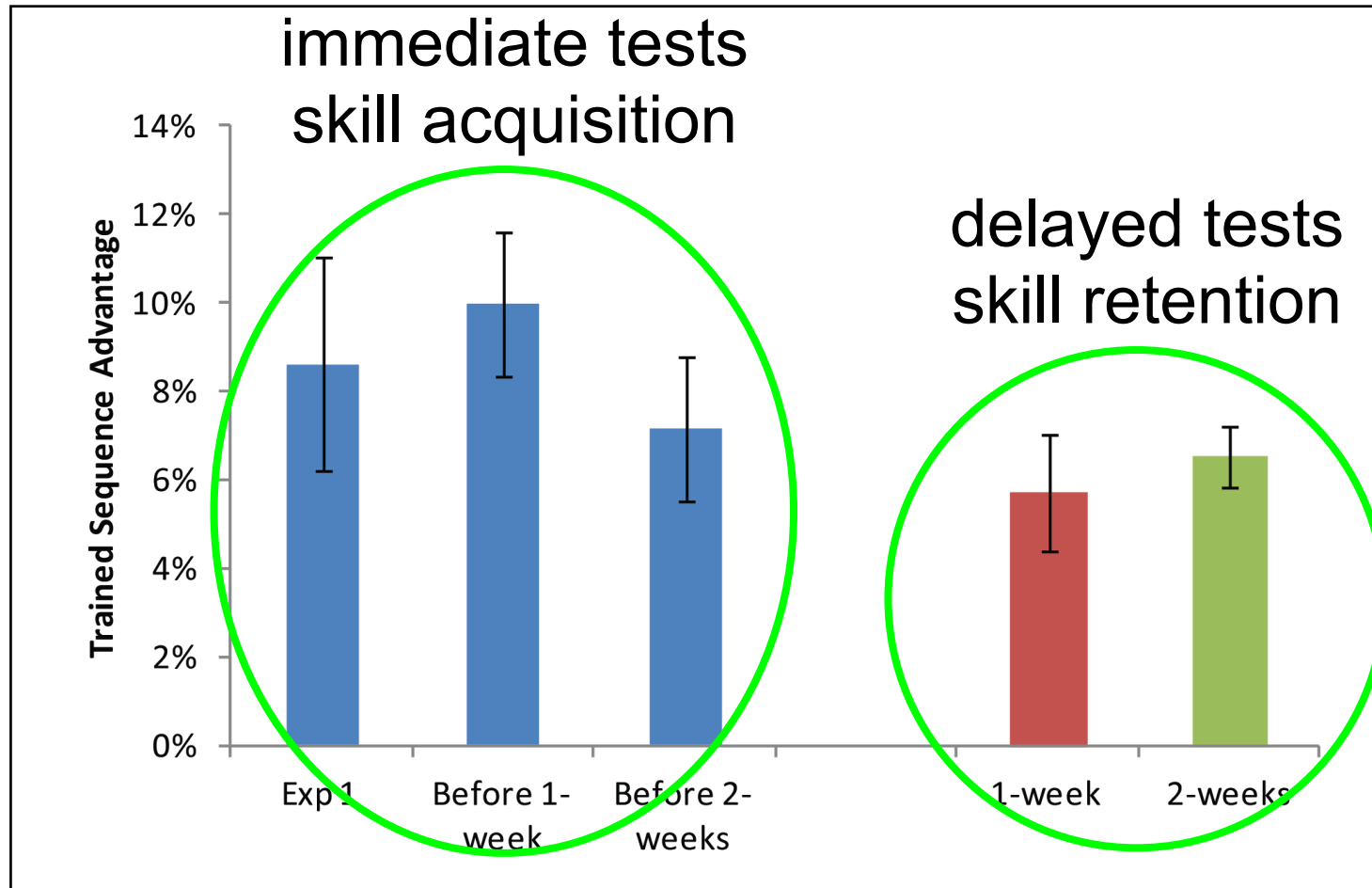
$6 \times 5 = 30$ characters in sequence

counting the number of sequences

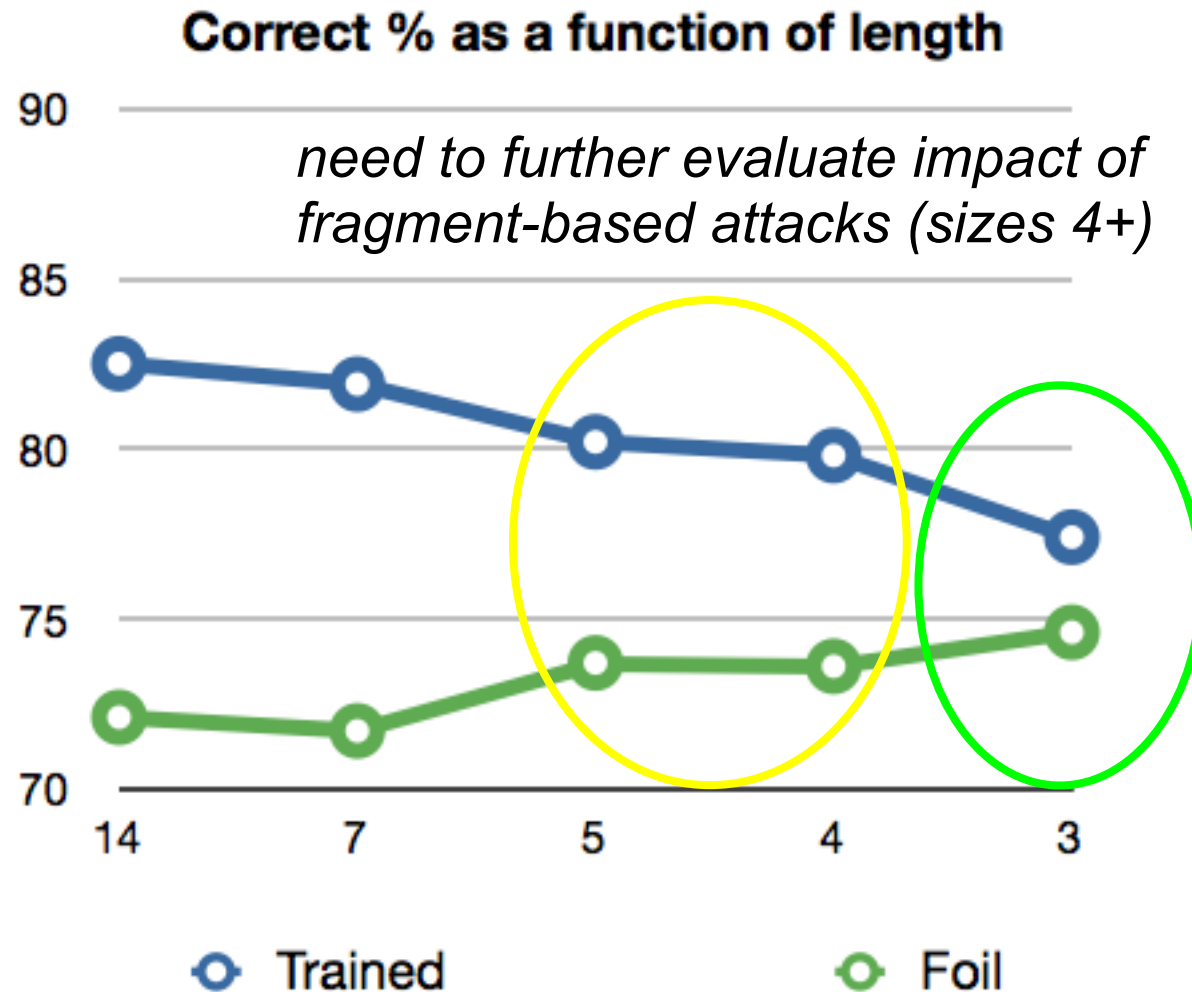


- Euler cycles
- BEST theorem: $6^4 \times 24^6$
- ~ 37.8 bits of entropy

skill acquisition and retention



feasibility of profiling subsequences



skill expression (by fragment size)

minimal expression for trigrams

reinventing psychology experiments

Amazon Mechanical Turk

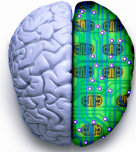
large number of available subjects

~370 users in our experiments

getting results in hours

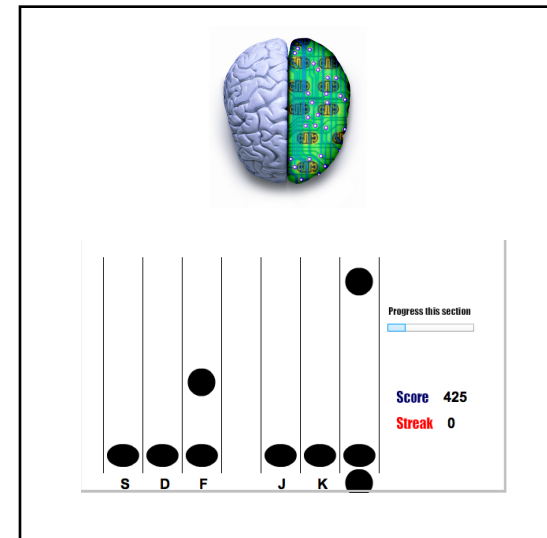
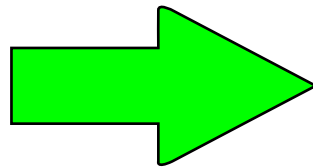
experiment workflow

amazon

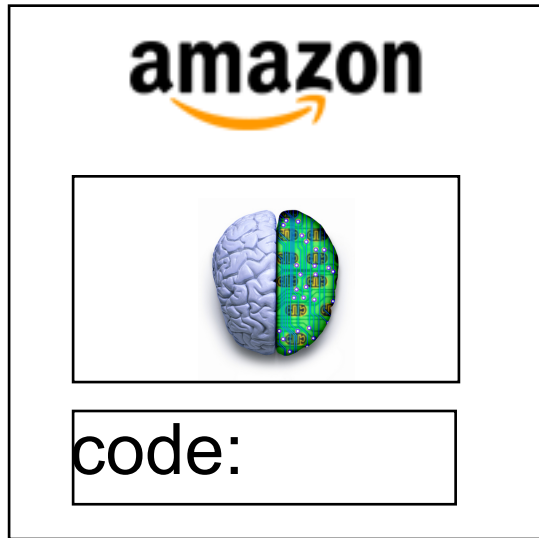


code:

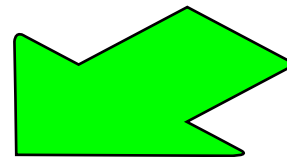
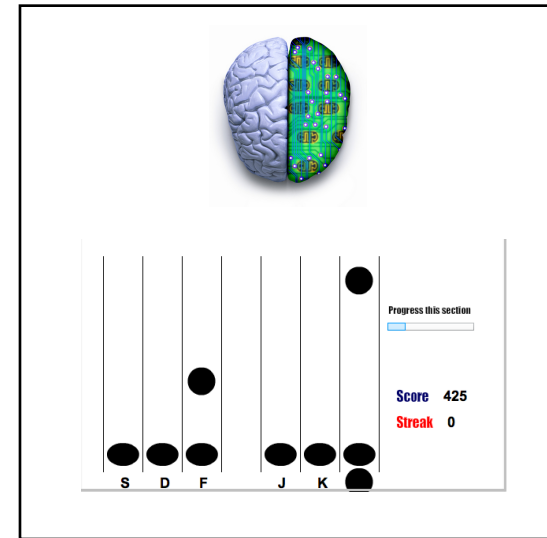
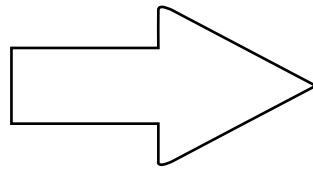
1 Accept HIT



experiment workflow



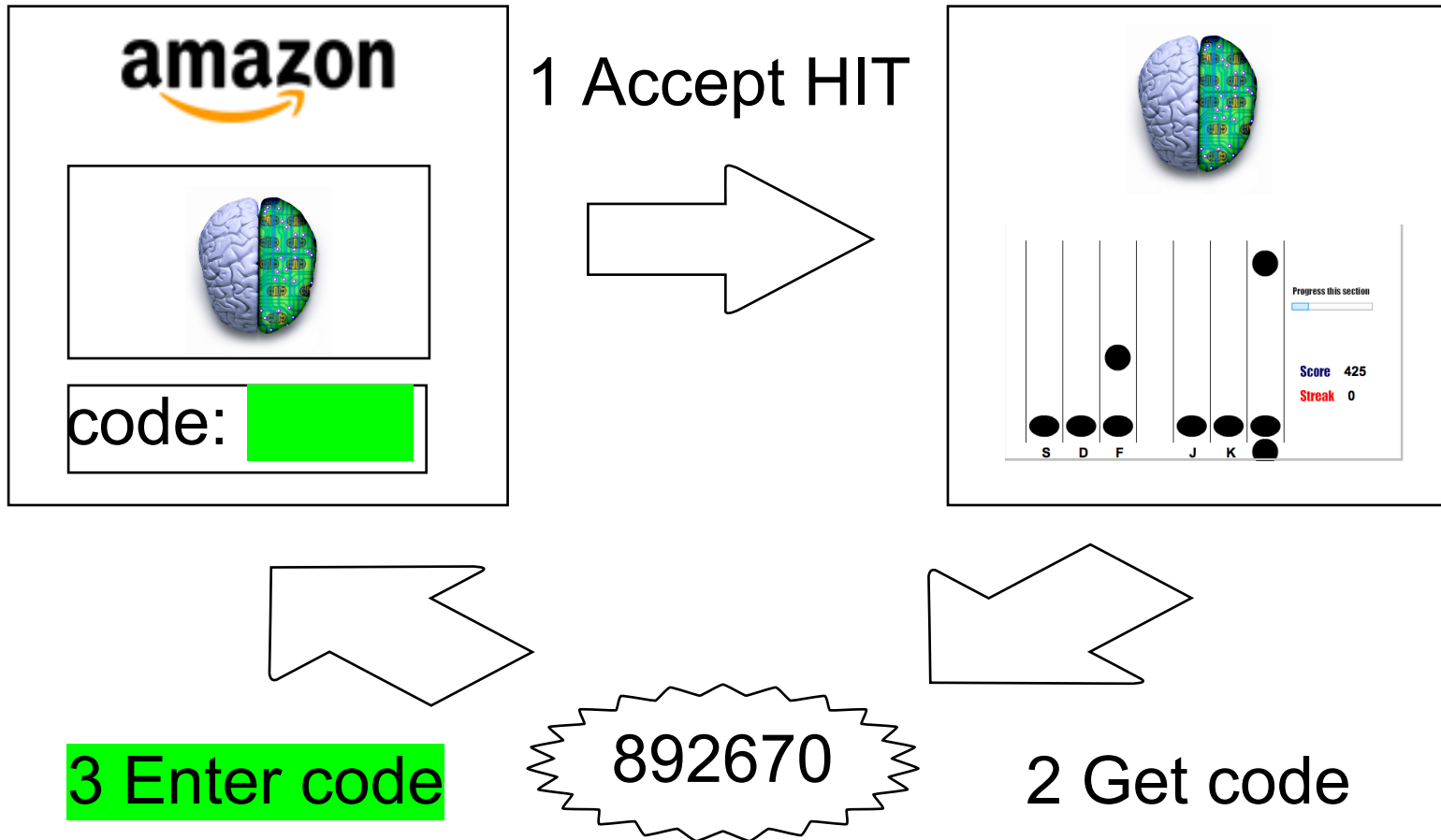
1 Accept HIT



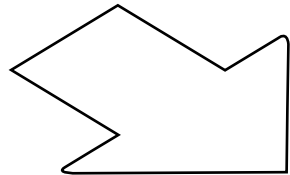
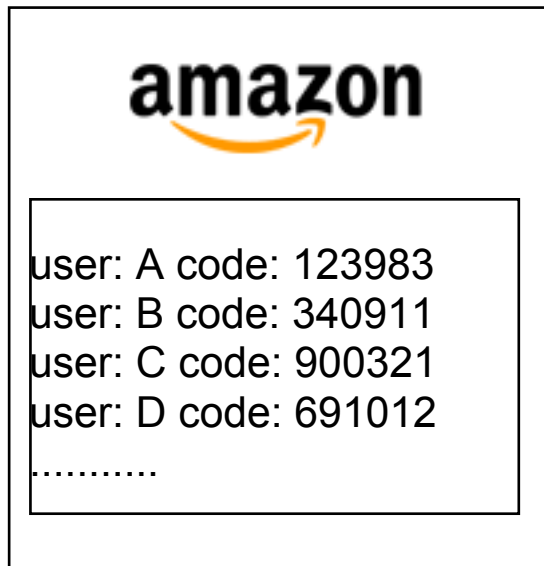
892670

2 Get code

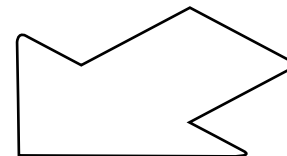
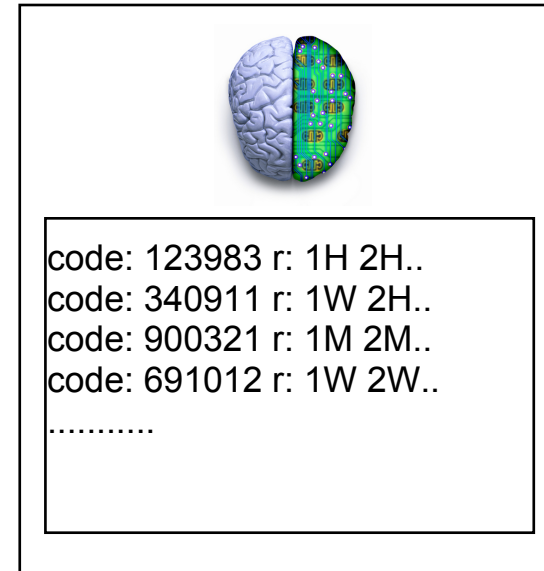
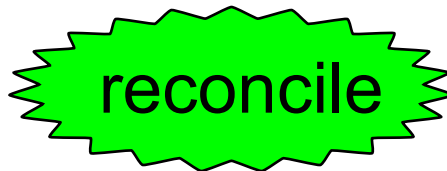
experiment workflow



approval workflow

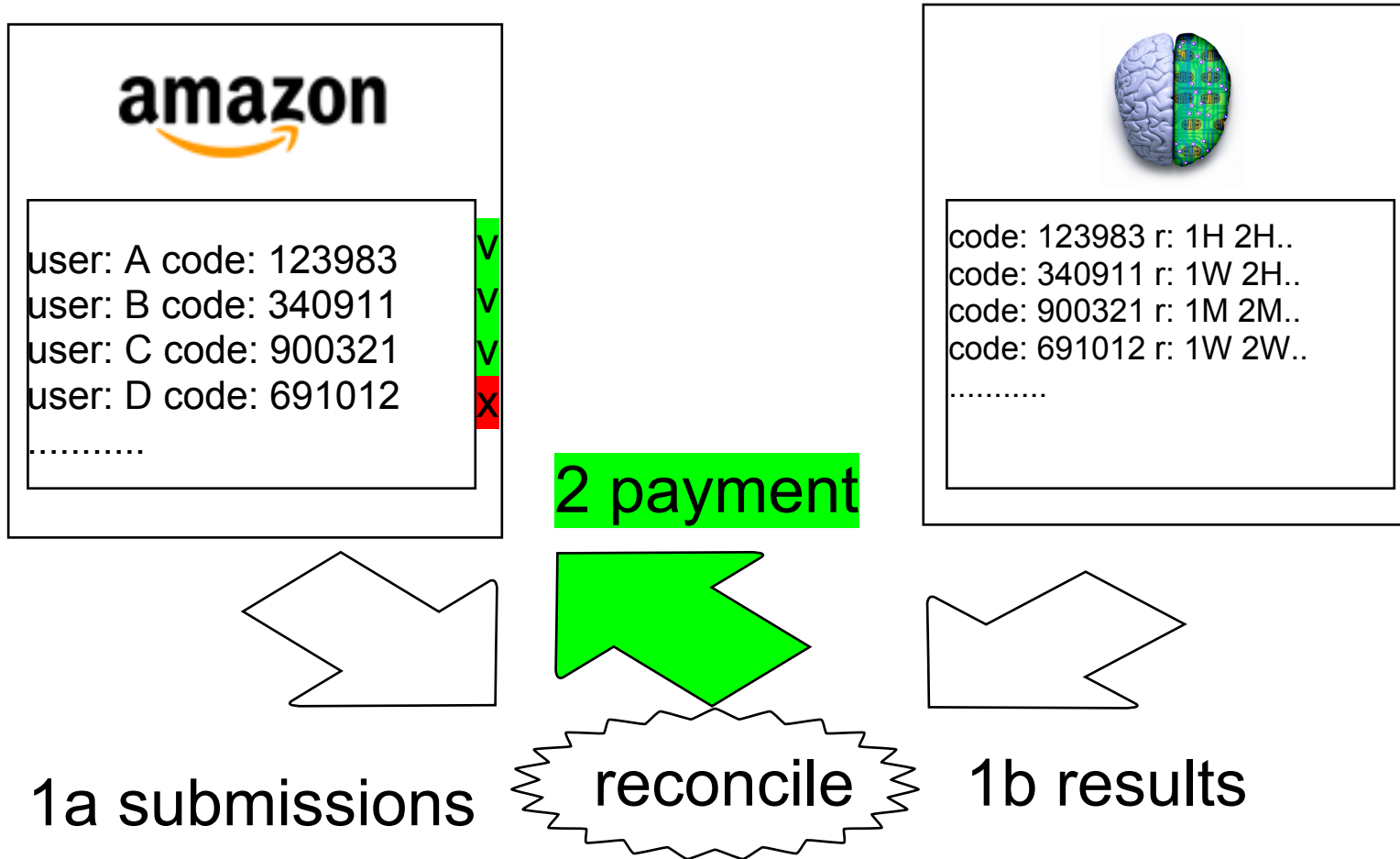


1a submissions



1b results

approval workflow



abuse facts

we rejected ~5% of submissions

random or empty receipt

repetition of keys (automation?)

large stretches without user activity

related work

Tamara Denning, Kevin D. Bowers, Marten van Dijk, Ari Juels
Exploring implicit memory for painless password recovery (CHI 2011)

Daphna Weinshall, Scott Kirkpartick
Passwords you'll never forget, but can't recall
(CHI 2004)

Keystroke timing work since the 1970s
Mouse movement analysis

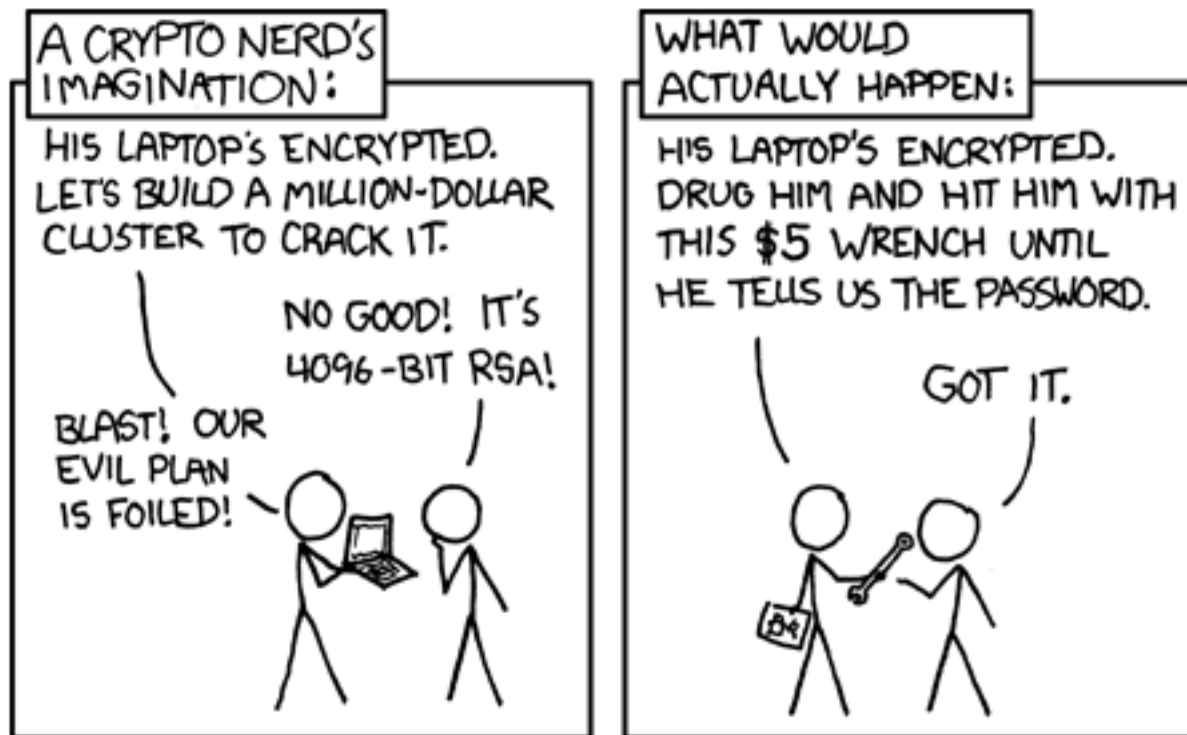
summary

passwords that cannot be extracted
(and can be changed!)

future work

implement challenge-response
(provides eavesdropping resistance)

speed up authentication (EEG data?)



<http://seclab.stanford.edu/>
hristo@cs.stanford.edu
or just google us... :-)