

# Guessing human-chosen secrets

Joseph Bonneau  
Security and Human Behavior  
New York, NY, USA  
June 4, 2012

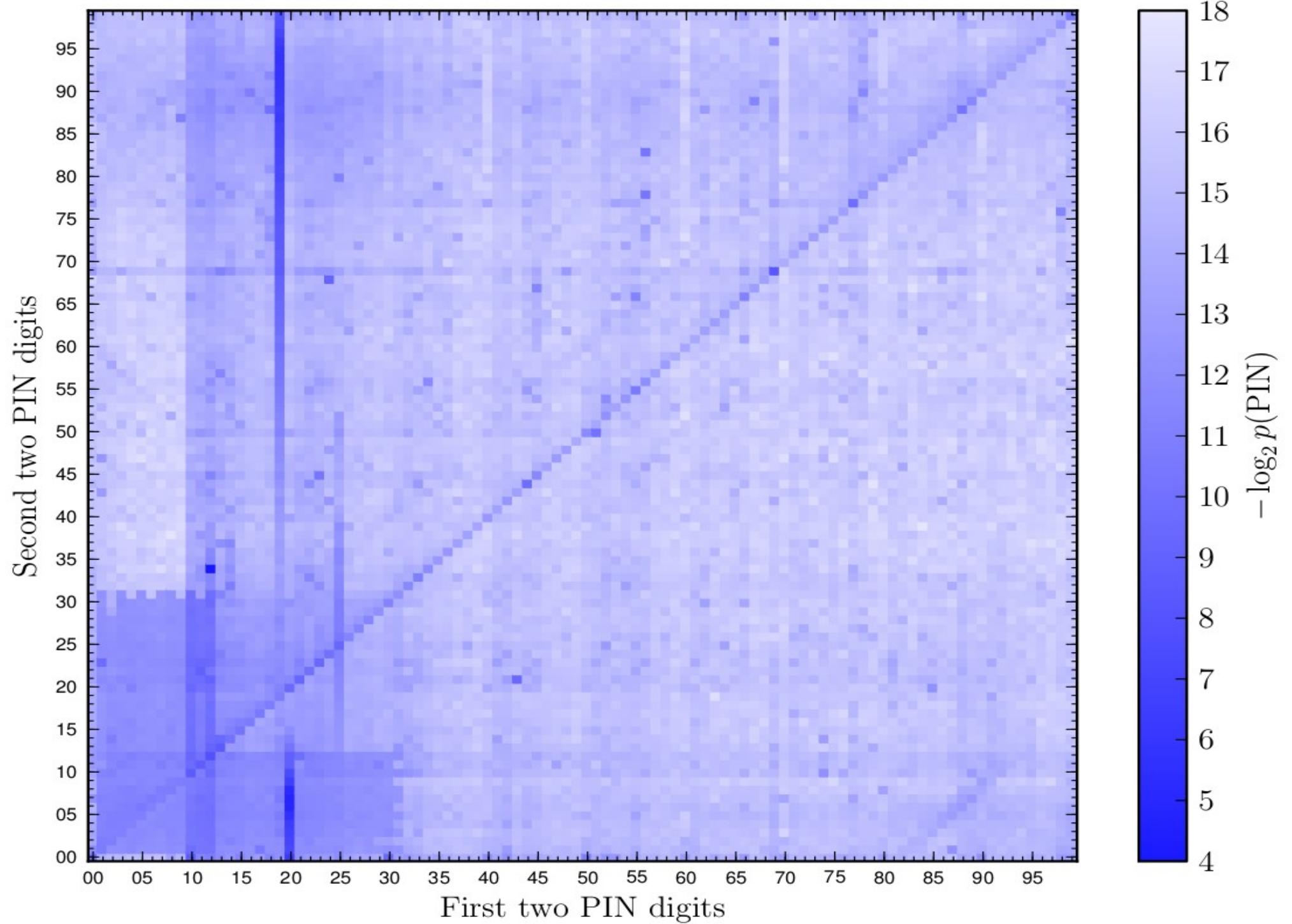
# What's easier to guess?

- Passwords chosen by older or younger users?
- Passwords or random 9-digit numbers?
- PINs or mother's maiden name?

# My PhD research

- **Measuring guessing difficulty empirically**
  - How do different user groups compare?
  - How do authentication schemes compare?

# Case study #1: 4-digit PINs



# Guessing a PIN with 6 guesses

- 2% chance of success against a random user
- 8% given the user's birthday!



JESUS KEYS IN HIS PIN NUMBER

# 'Pin number' burglar used victims' cards

## He struck as couple slept

» GARRY WILLEY

A JUDGE laid down a pin number warning after he heard how a couple fell victim to a "cunning" career crook.

Serial offender Paul Miller - whose grim record carries 167 previous convictions - crept into the victim's North Tyneside home while they slept.

His haul included cash, laptops, a handbag and driving licence.

But Miller, 31, also pocketed two Barclays cards, Newcastle Crown Court heard. And within hours he was plundering £1,000 from an ATM on nearby Wallsend High Street when he guessed right the owner had used her date of birth as a pin. Jailing Miller for four and a half years, Judge Roger Thorn said: "If anybody is still using their date of birth as a pin they should learn a lesson from this case."

"You knew that by using the driv-

ing licence you could get the date of birth and having identified that you took a chance that the holder was using it as a pin. You were right."

The dead-of-night raid last summer has left the victims feeling paranoid in their own home, the court heard.

Miller, of Wilberforce Street, Wallsend, denied burglary and fraud but was convicted by a jury.

He slipped inside the house when he realised the front door was unlocked, prowling through rooms and rounding up property while the couple slept.

Miller was later captured on CCTV using the cards to withdraw batches of cash from the same ATM. A pre-sentence report said Miller - a heroin addict who first took drugs when he was 12 - posed a risk of harm through potential confrontations with homeowners. His record includes offences of arson and robbery as well as 32 previous burglaries - nine targeting homes.

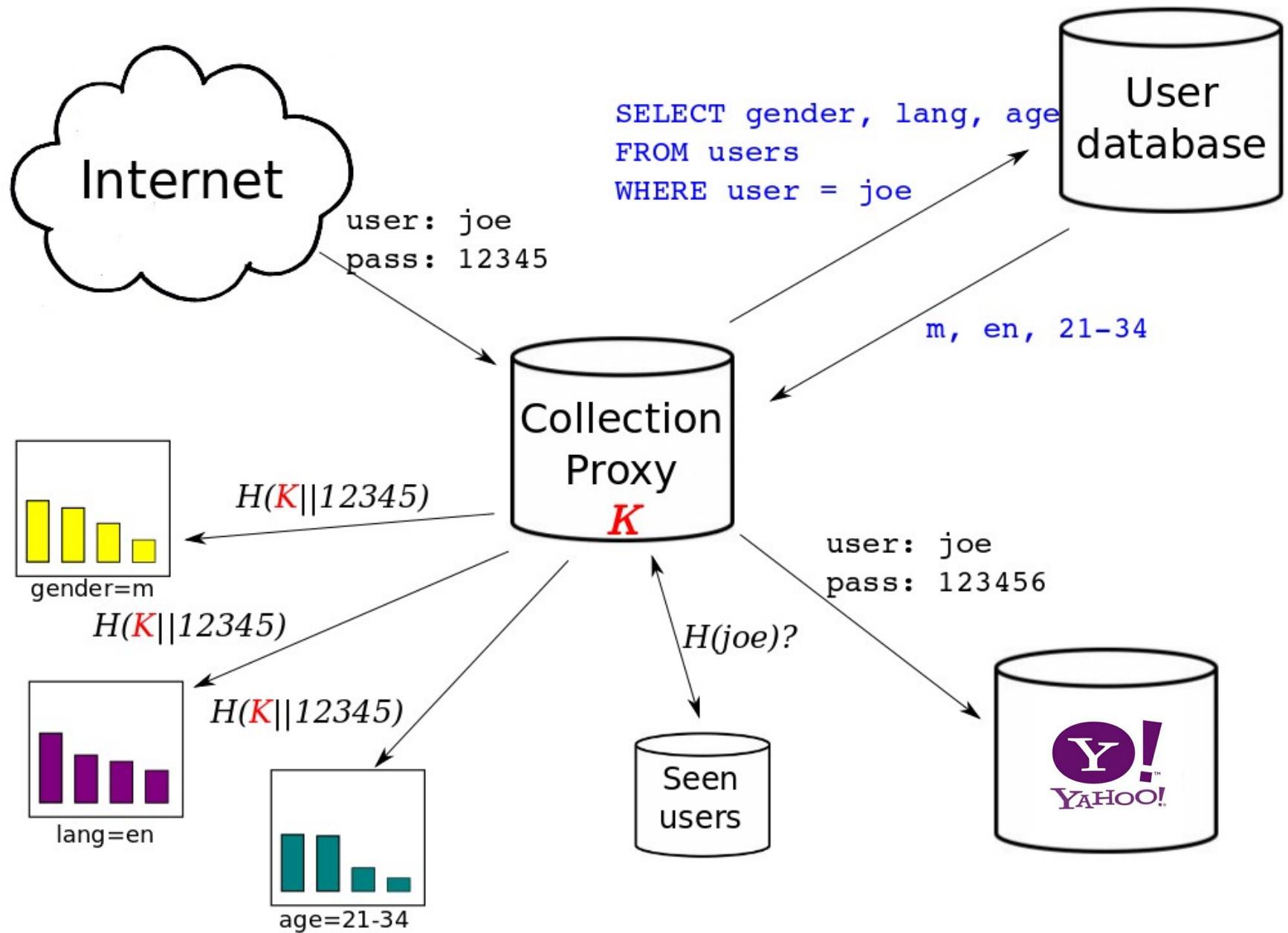


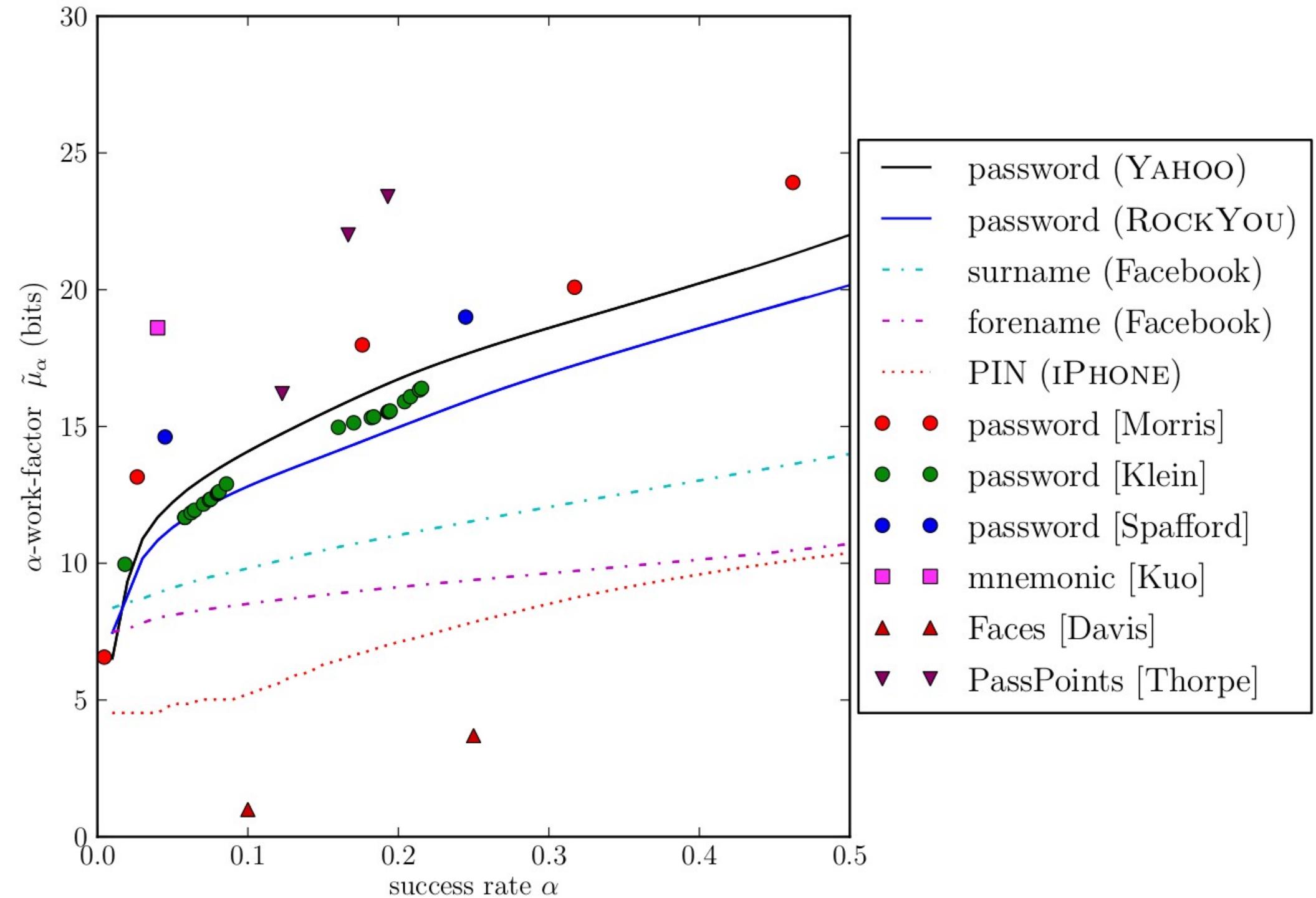
**CONVICTED** Miller

## research in action...

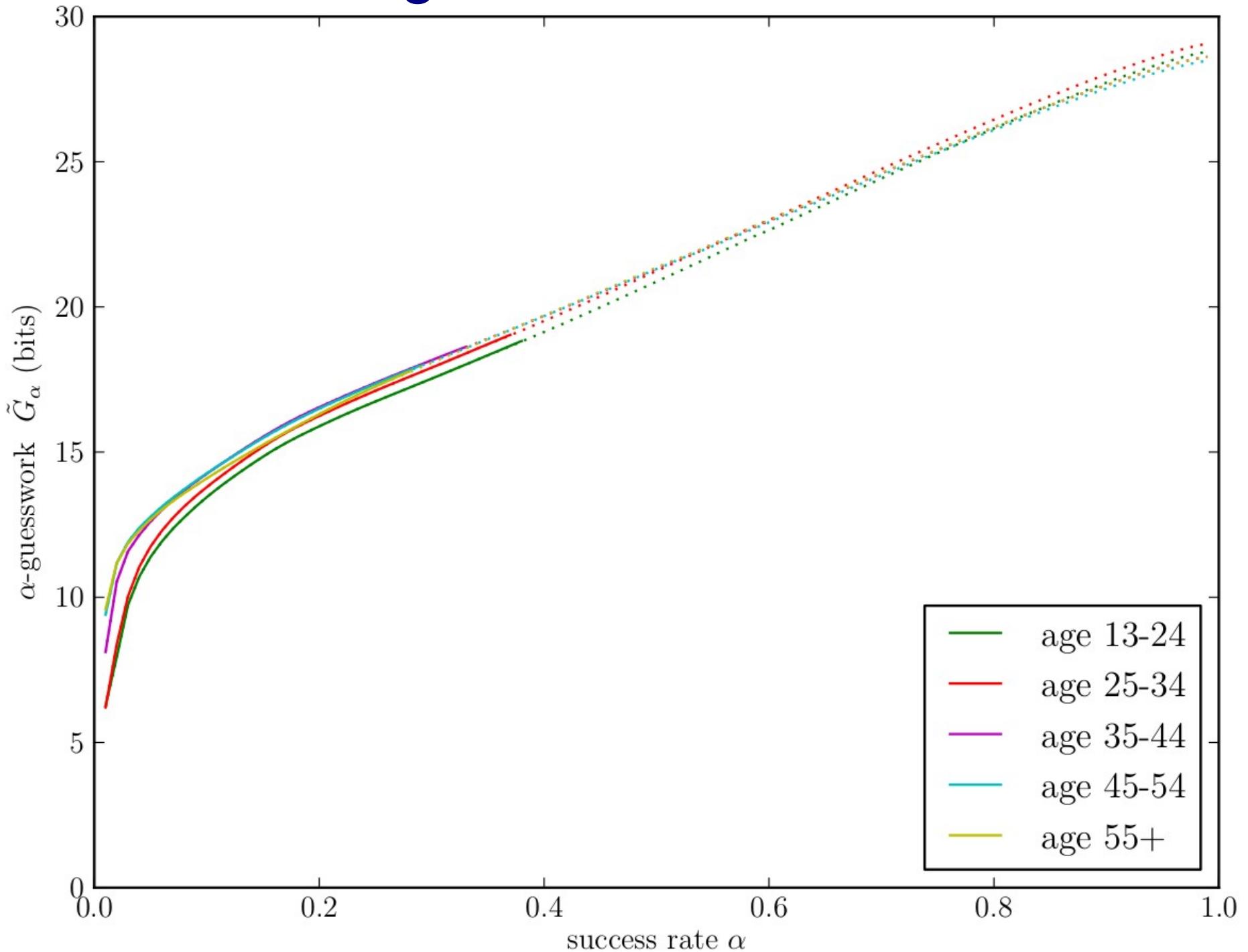
# Case study #2: basic passwords

# Password collection at Yahoo

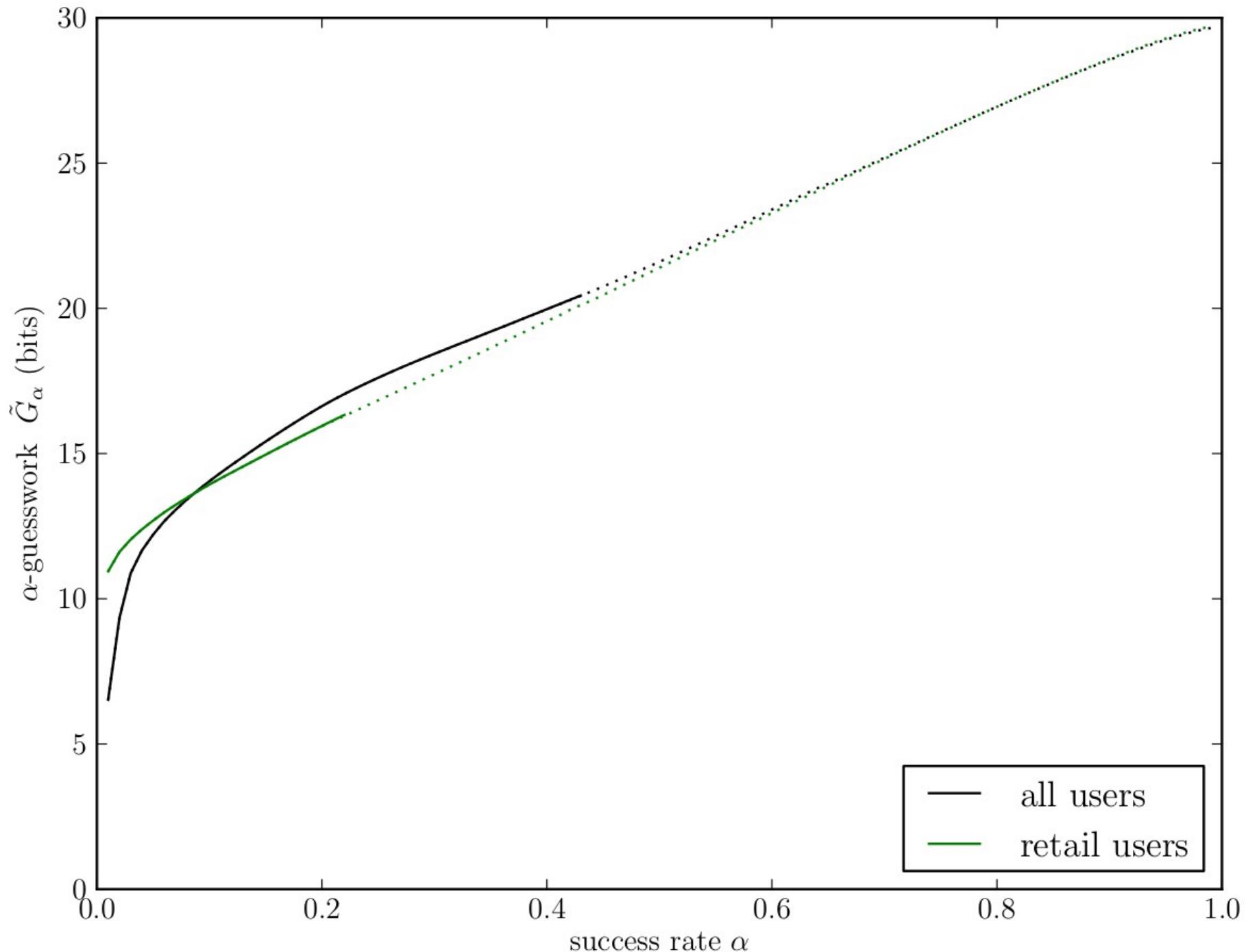




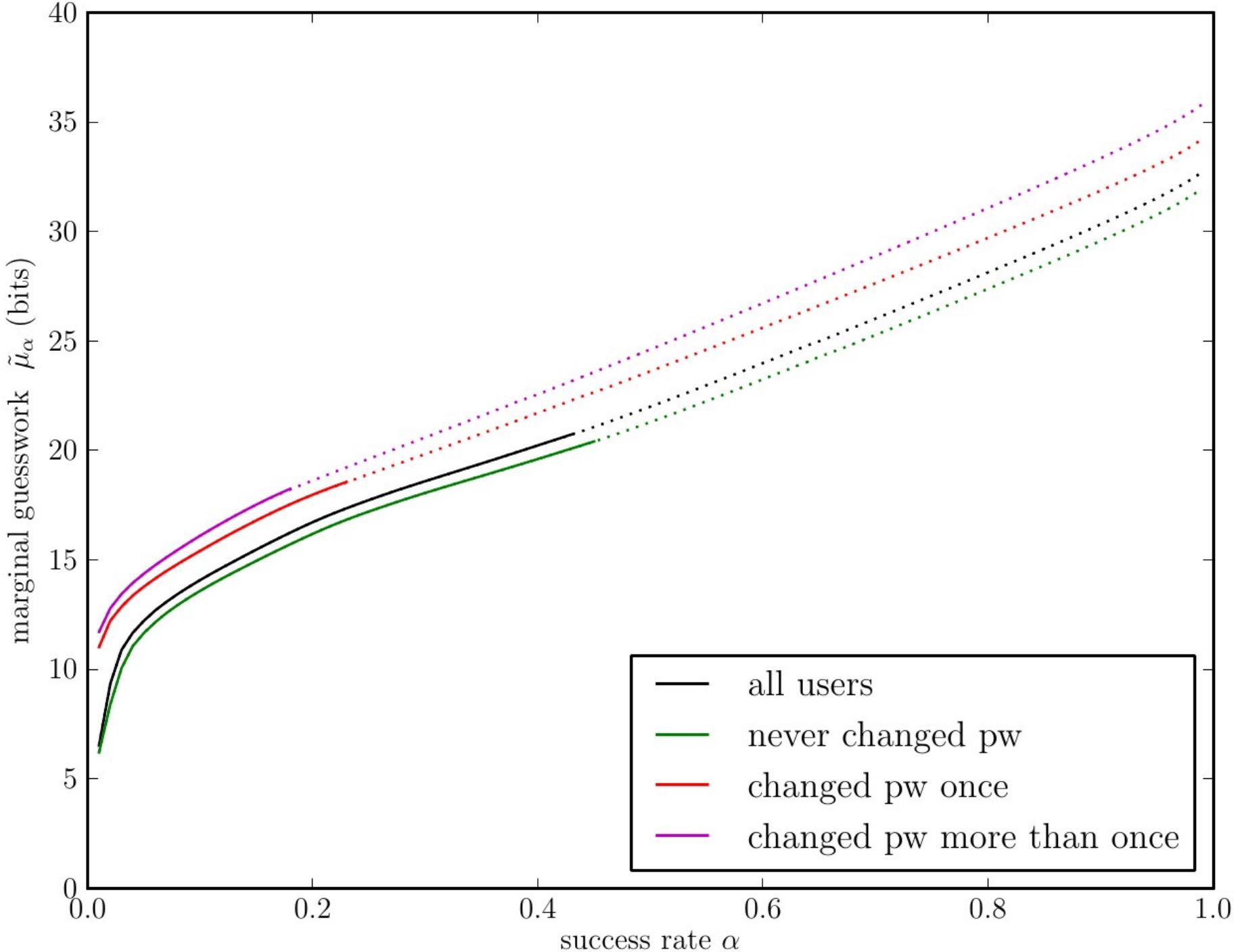
# Age matters a little bit..



# Financial motivation matters a little bit...



# Security interest matters much more



# Case study #3: password advice

# Password strength meter at Yahoo

Get free email and other leading web services with a Yahoo! account.

---

Name

Gender

Birthday

Country

Postal Code

## Select an ID and password

---

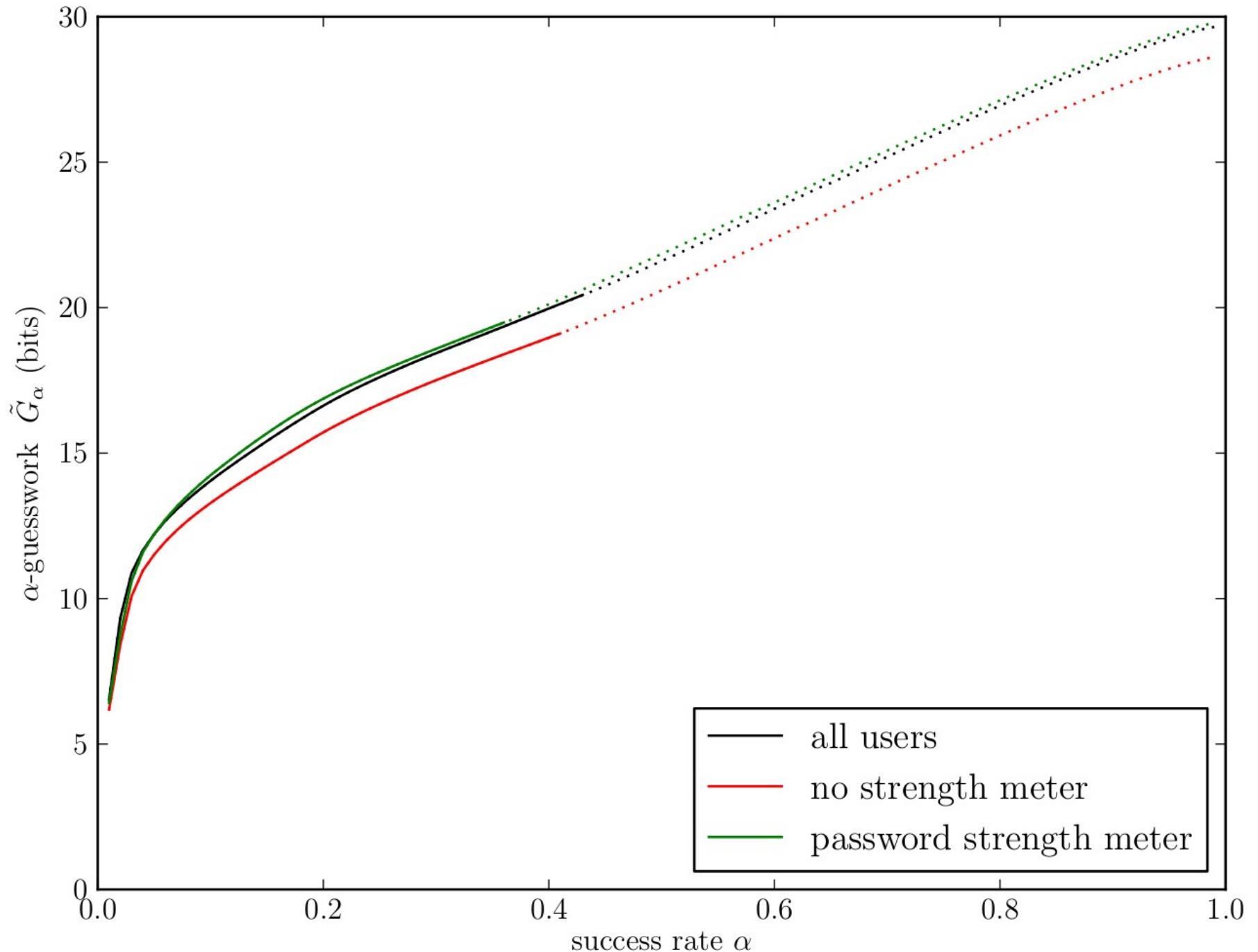
Yahoo! ID and Email  @

Password  Weak 

Capitalisation matters. Use 6 to 32 characters, and  
do not use your name or Yahoo! ID.

Re-type Password

# Strength meter makes 1 bit of difference



To be or not  
to be, that is  
the question.



Want to create a really strong password? Ask Hamlet.

Or Macbeth. Or Othello. Or even take a lyric from your favourite song. The more unusual the better. Try thinking of a memorable line like, 'To be, or not to be, that is the question' and then use numbers, symbols and mixed letters to recreate it:

2bon2btitq is a password with quadrillions of variations. Which is a lot.

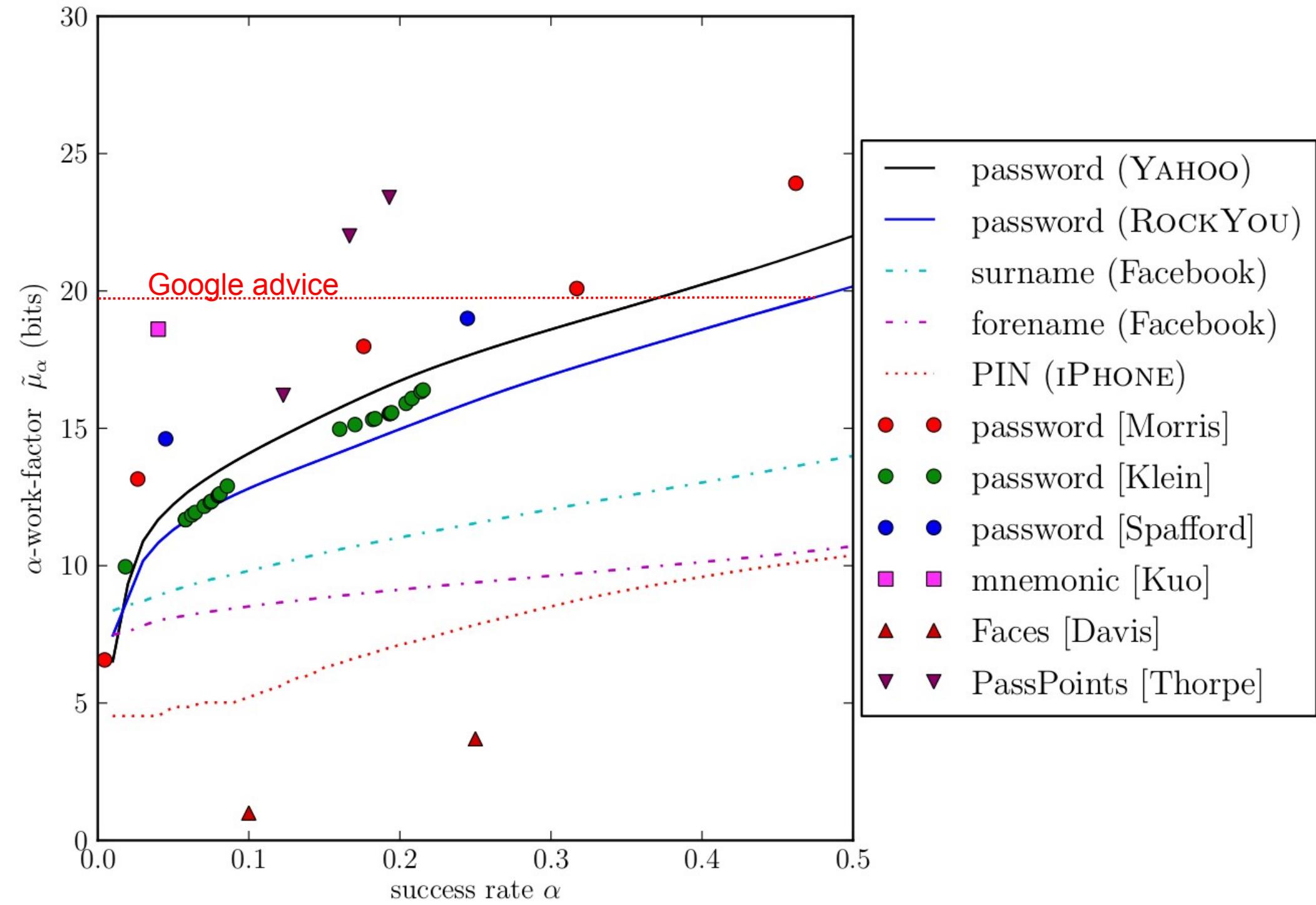
In short, strong passwords can keep you safe online, which is good to know.

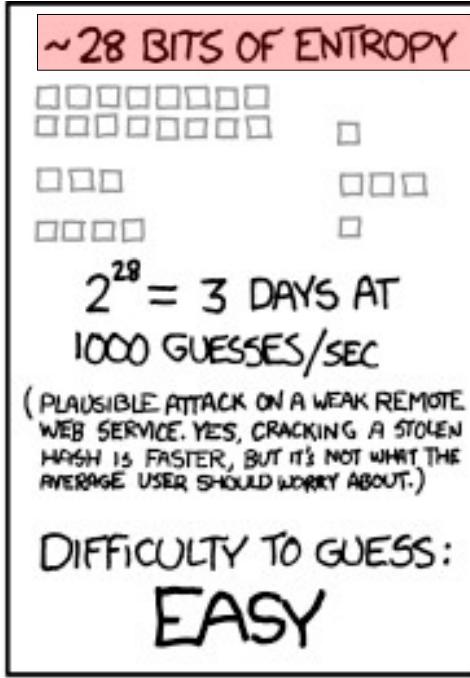
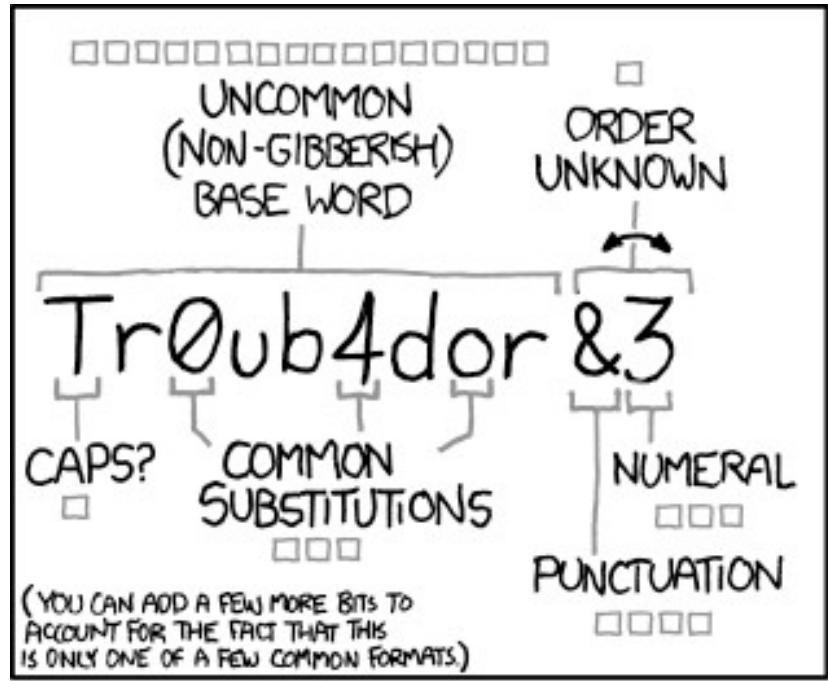
To find out more on how to be safer on the Internet go to [google.co.uk/goodtoknow](http://google.co.uk/goodtoknow)

1 quadrillion  
variations

≈

50 bits?

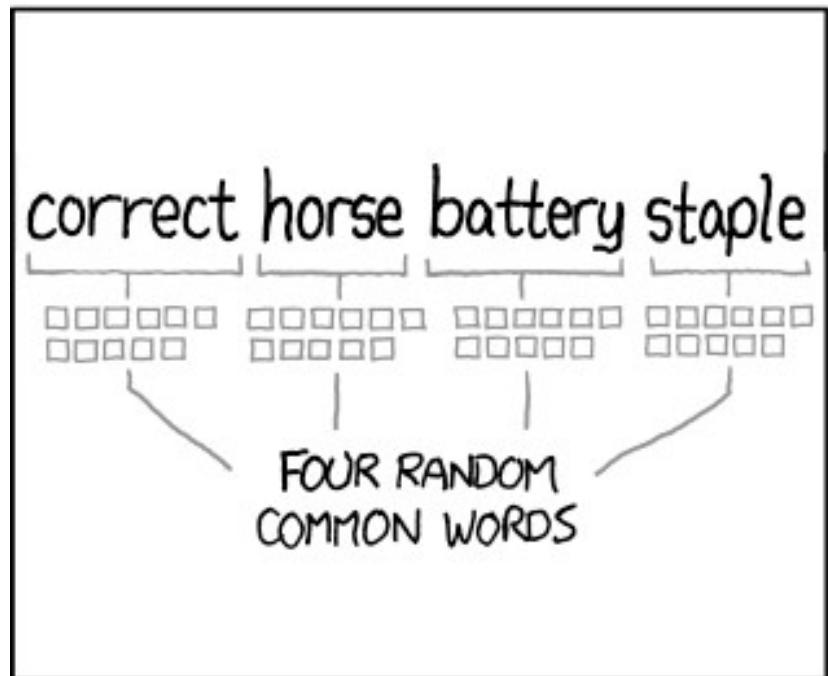




WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?  
AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER:  
**HARD**

A stick figure is shown thinking about a password. The text above the figure discusses various possibilities like "TROMBONE" and "TROUBADOR", and notes that one of the zeros was actually a zero, and there was some symbol.

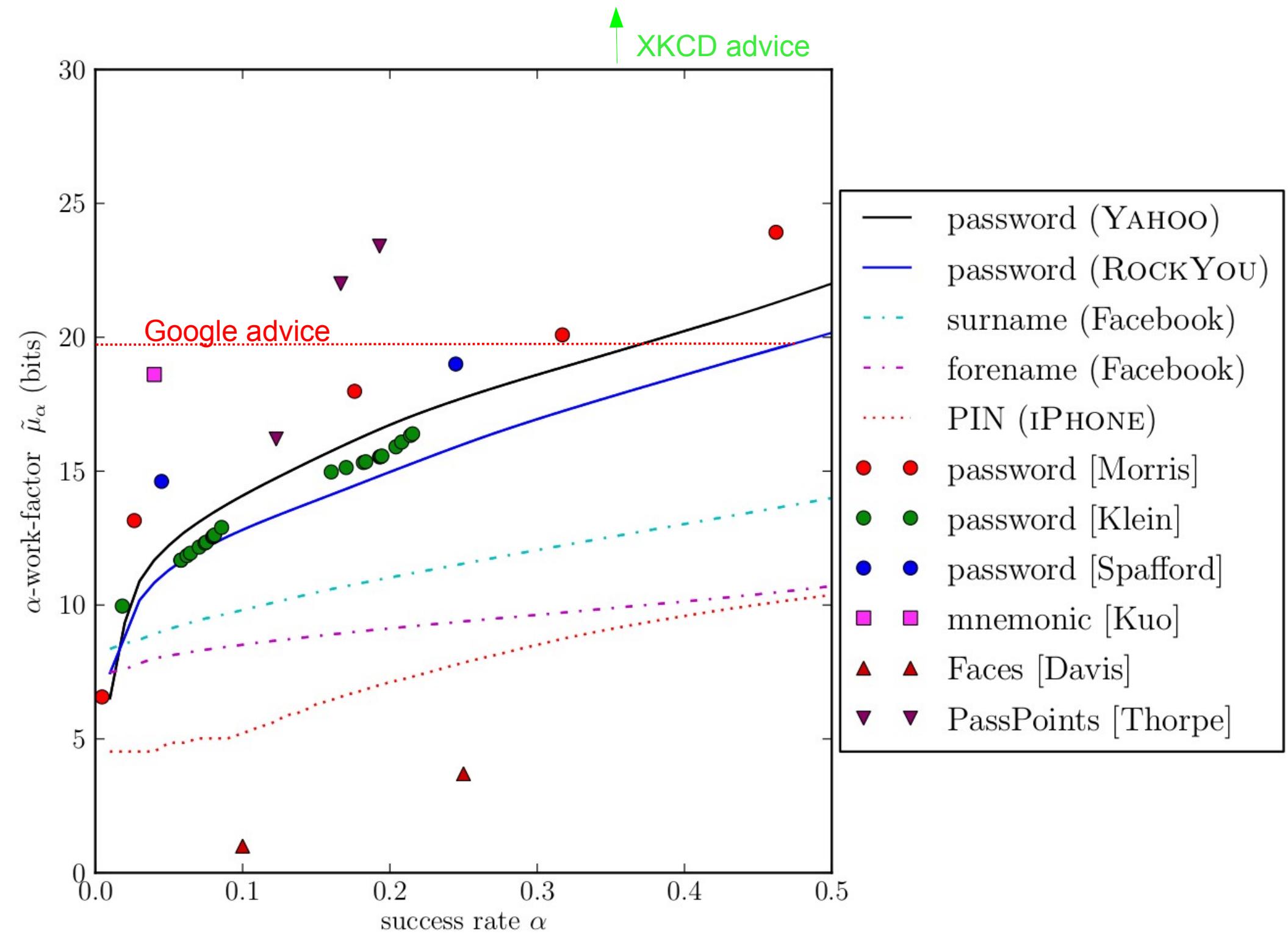


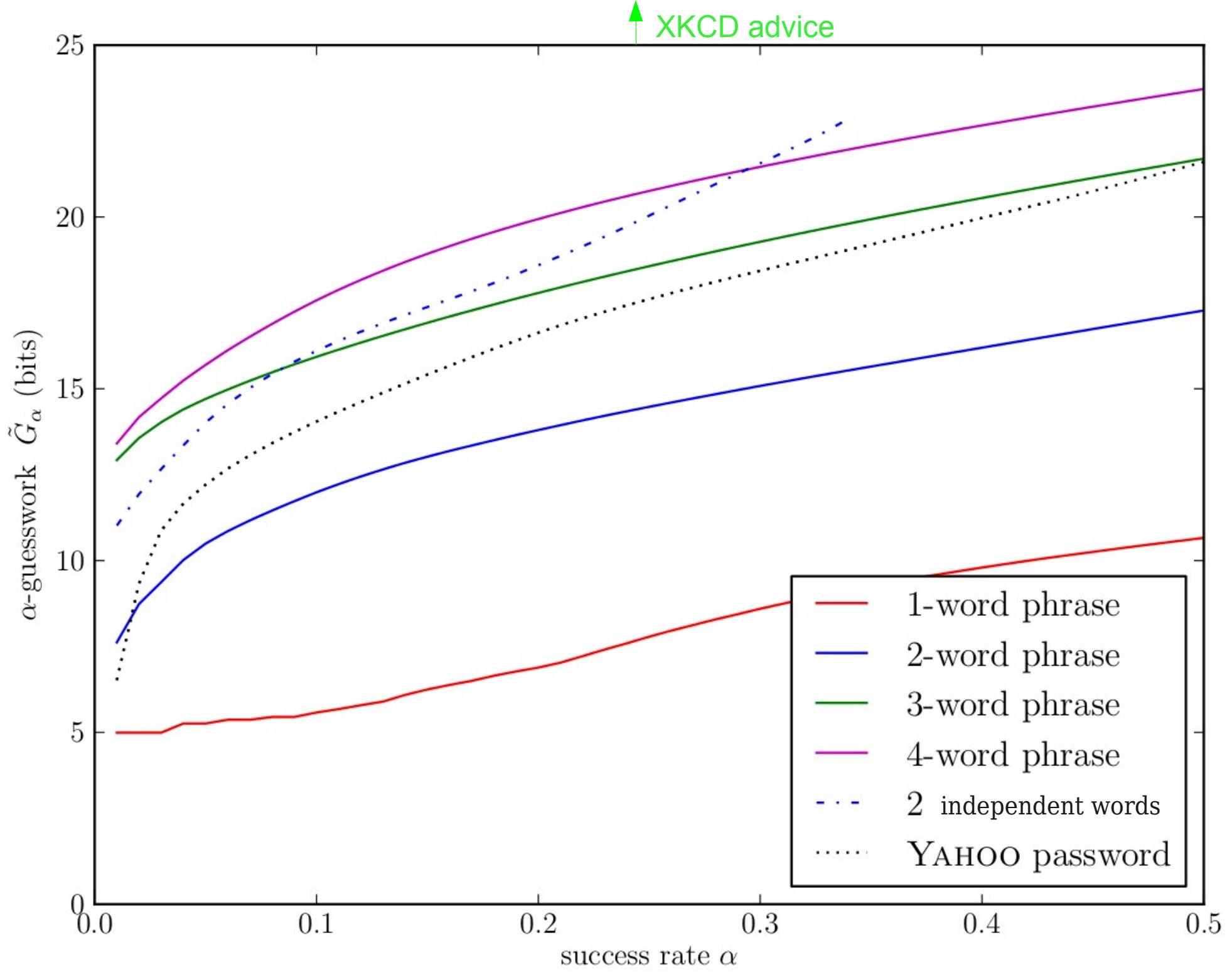
THAT'S A BATTERY STAPLE.  
CORRECT!

DIFFICULTY TO REMEMBER:  
YOU'VE ALREADY MEMORIZED IT

A stick figure is shown thinking about a password. A thought bubble contains the text "THAT'S A BATTERY STAPLE." and "CORRECT!". Below the thought bubble, the text "YOU'VE ALREADY MEMORIZED IT" is written.

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.





# Case study #4: passwords and language

123456  
12345  
123456789  
**password**  
**iloveyou**  
**princess**  
**1234567**  
**rockyou**  
**12345678**  
**abc123**  
**nicole**  
**daniel**  
**babygirl**  
**monkey**  
**lovely**  
**jessica**  
**654321**  
**michael**  
**ashley**  
**qwerty**  
**111111**  
**iloveu**  
**000000**  
**michelle**  
**tigger**

123456  
111111  
000000  
123456789  
123123  
**111222tianya**  
5201314  
123321  
12345678  
123  
666666  
7758521  
888888  
1314520  
1234567  
**wangyut2**  
**woaini**  
11111111  
a123456  
111222  
112233  
654321  
100200  
123654  
123123123

123456  
12345  
123456789  
password  
iloveyou  
princess  
1234567  
rockyou  
12345678  
abc123  
nicole  
daniel  
babygirl  
monkey  
lovely  
jessica  
654321  
michael  
ashley  
qwerty  
111111  
iloveu  
000000  
michelle  
tigger

The diagram illustrates a many-to-many relationship between two sets of password lists. It consists of two rectangular boxes, one pink on the left labeled "RockYou" and one blue on the right labeled "CSDN". The "RockYou" box contains 25 entries, and the "CSDN" box contains 25 entries. Numerous black arrows connect pairs of passwords between the two sets, indicating that each password in the "RockYou" list is connected to multiple passwords in the "CSDN" list, and vice versa. This visualizes the concept of password reuse or similarity across different datasets.

123456  
111111  
000000  
123456789  
123123  
111222tianya  
5201314  
123321  
12345678  
123  
666666  
7758521  
888888  
1314520  
1234567  
wangyut2  
woaini  
11111111  
a123456  
111222  
112233  
654321  
100200  
123654  
123123123

123456  
12345  
123456789  
password  
iloveyou  
princess  
1234567  
rockyou  
12345678  
abc123  
nicole  
daniel  
babygirl  
monkey  
lovely  
jessica  
654321  
michael  
ashley  
qwerty  
111111  
iloveu  
000000  
michelle  
tigger

The diagram illustrates a many-to-many relationship between two sets of password lists. On the left, the RockYou list contains 25 entries. On the right, the CSDN list contains 25 entries. Bidirectional arrows connect pairs of passwords from each set. The connections are as follows:

- RockYou's 123456 connects to CSDN's 123456
- RockYou's 12345 connects to CSDN's 111111
- RockYou's 123456789 connects to CSDN's 000000
- RockYou's password connects to CSDN's 123456789
- RockYou's iloveyou connects to CSDN's 123123
- RockYou's princess connects to CSDN's 111222tianya
- RockYou's 1234567 connects to CSDN's 5201314
- RockYou's rockyou connects to CSDN's 123321
- RockYou's 12345678 connects to CSDN's 12345678
- RockYou's abc123 connects to CSDN's 123
- RockYou's nicole connects to CSDN's 666666
- RockYou's daniel connects to CSDN's 7758521
- RockYou's babygirl connects to CSDN's 888888
- RockYou's monkey connects to CSDN's 1314520
- RockYou's lovely connects to CSDN's 1234567
- RockYou's jessica connects to CSDN's wangyut2
- RockYou's 654321 connects to CSDN's woaini
- RockYou's michael connects to CSDN's 11111111
- RockYou's ashley connects to CSDN's a123456
- RockYou's qwerty connects to CSDN's 111222
- RockYou's 111111 connects to CSDN's 112233
- RockYou's iloveu connects to CSDN's 654321
- RockYou's 000000 connects to CSDN's 100200
- RockYou's michelle connects to CSDN's 123654
- RockYou's tigger connects to CSDN's 123123123

123456  
12345  
123456789  
password  
iloveyou  
princess  
1234567

123456  
111111  
000000  
123456789  
123123  
111222tianya  
5201314

## Bad passwords are universal...

nicole  
daniel  
babygirl  
monkey  
lovely  
jessica  
654321  
michael  
ashley  
qwerty  
111111  
iloveu  
000000  
micelle  
tigger

666666  
7758521  
888888  
1314520  
1234567  
wangyut2  
woaini  
11111111  
a123456  
111222  
112233  
654321  
100200  
123654  
123123123

# Non-ASCII passwords poorly supported

The screenshot shows the IMDbPro website's "Forgotten Password" page. At the top, there is a navigation bar with the "IMDbPro" logo, a search bar, and a "Go" button. Below the navigation bar, there are links for "Careers", "Industry Directory", and "In Production". The main content area has a breadcrumb trail: "Home > Your Account > Forgotten Password". The title "Forgotten Password" is displayed prominently. A sub-instruction "Please choose a new password." is present. Below it, there are two input fields: "Password" and "Confirm Password", both containing five dots ("....."). A red error message "Password too long (max. 64 characters)" is displayed above the "Change" button. A cursor arrow is visible near the error message. Below the "Change" button is a link "Need [help?](#)".

Search  Go

Careers ▾ Industry Directory ▾ In Production ▾

[Home](#) > [Your Account](#) > [Forgotten Password](#)

## Forgotten Password

Please choose a new password.

**Password too long (max. 64 characters)**

Password: .....

Confirm Password: .....

**Change**

Need [help?](#)

# East Asian scripts disabled for passwords

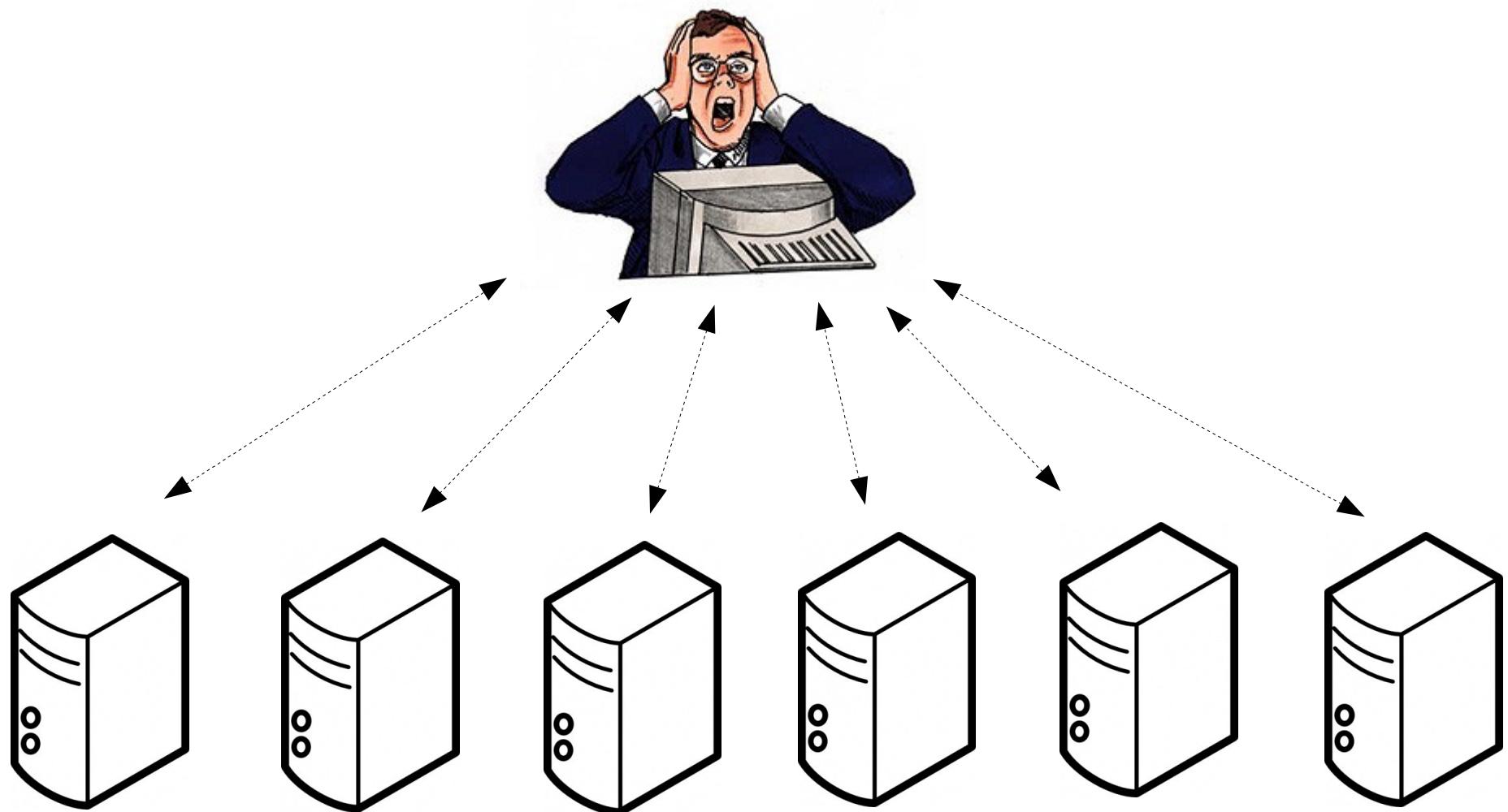
mimal



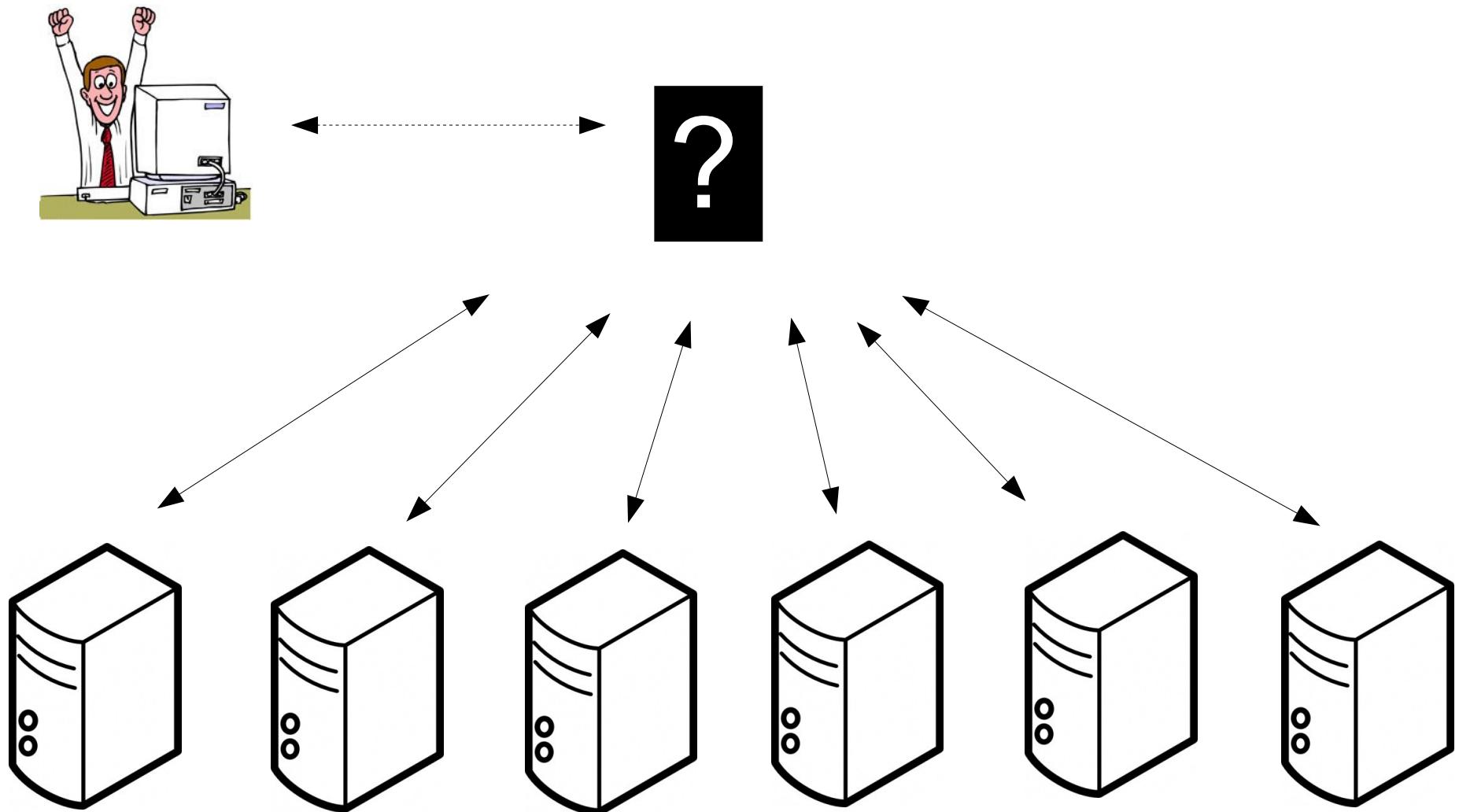
- 1.密码
- 2.米玛
- 3.米
- 4.迷
- 5.密



# Today's Internet identity layer



# Tomorrow's Internet identity layer



# Thanks to many collaborators 😊

Ross Anderson, Sören Preibusch, Frank Stajano, Ekaterina Shutova  
(Cambridge)

Elizabeth Zwicky, Henry Watts, Richard Clayton, Ram Marti, Clarence Chung, Christopher Harris (Yahoo!)

Paul van Oorschot (Carleton)

Cormac Herley (Microsoft Research)