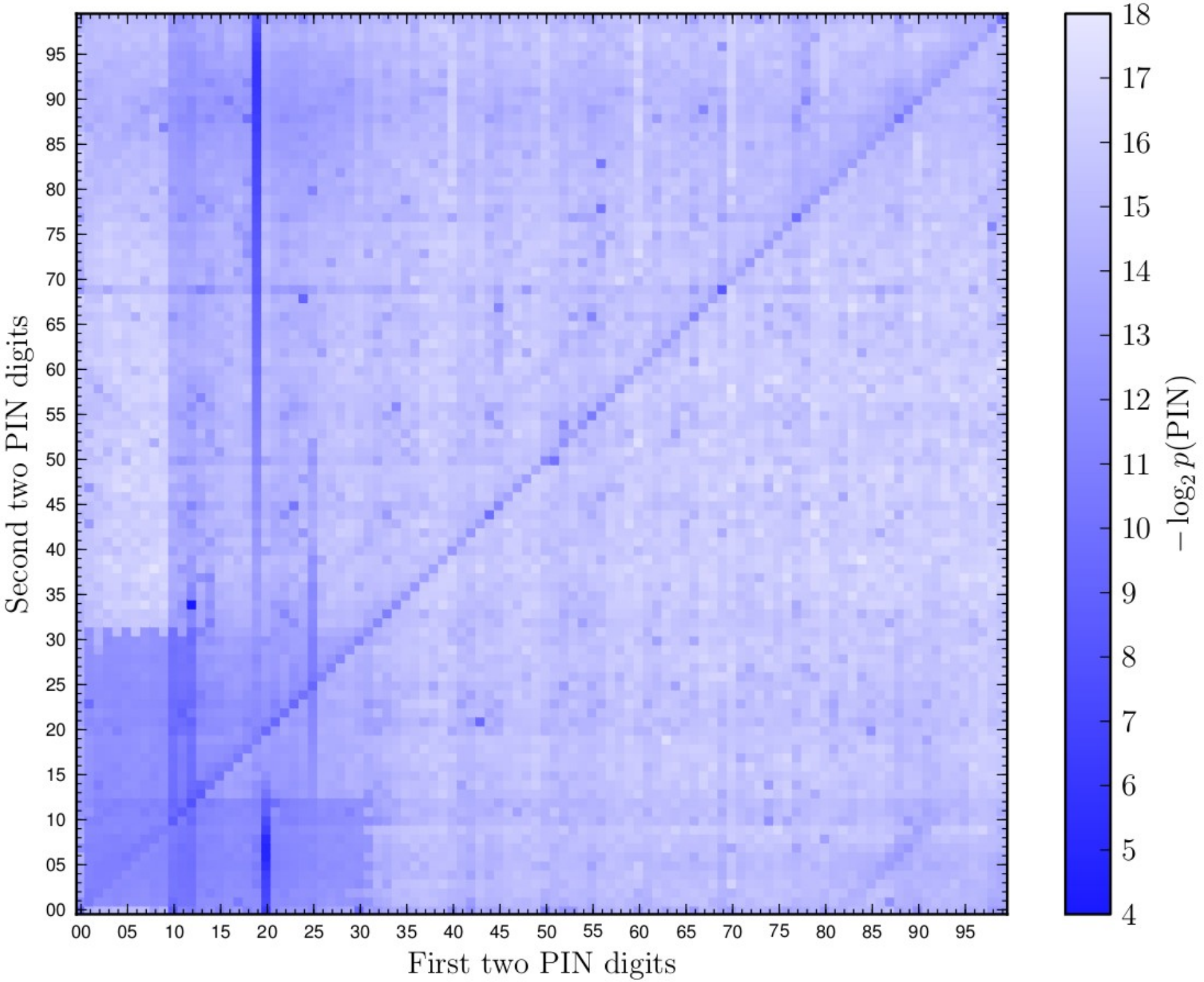
Authentication in a networked world

Joseph Bonneau
Gates Scholars Internal Symposium
May 2, 2012

Finding #1

People choose banking PINs poorly


Second two PIN digits
First two PIN digits
00 05 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80 85 90 95
$-\log_2 p(\mathrm{PIN})$
4 5 6 7 8 9 10 11 12 13 14 15 16 17 18

'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 driving 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.

CONVICTED Miller

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

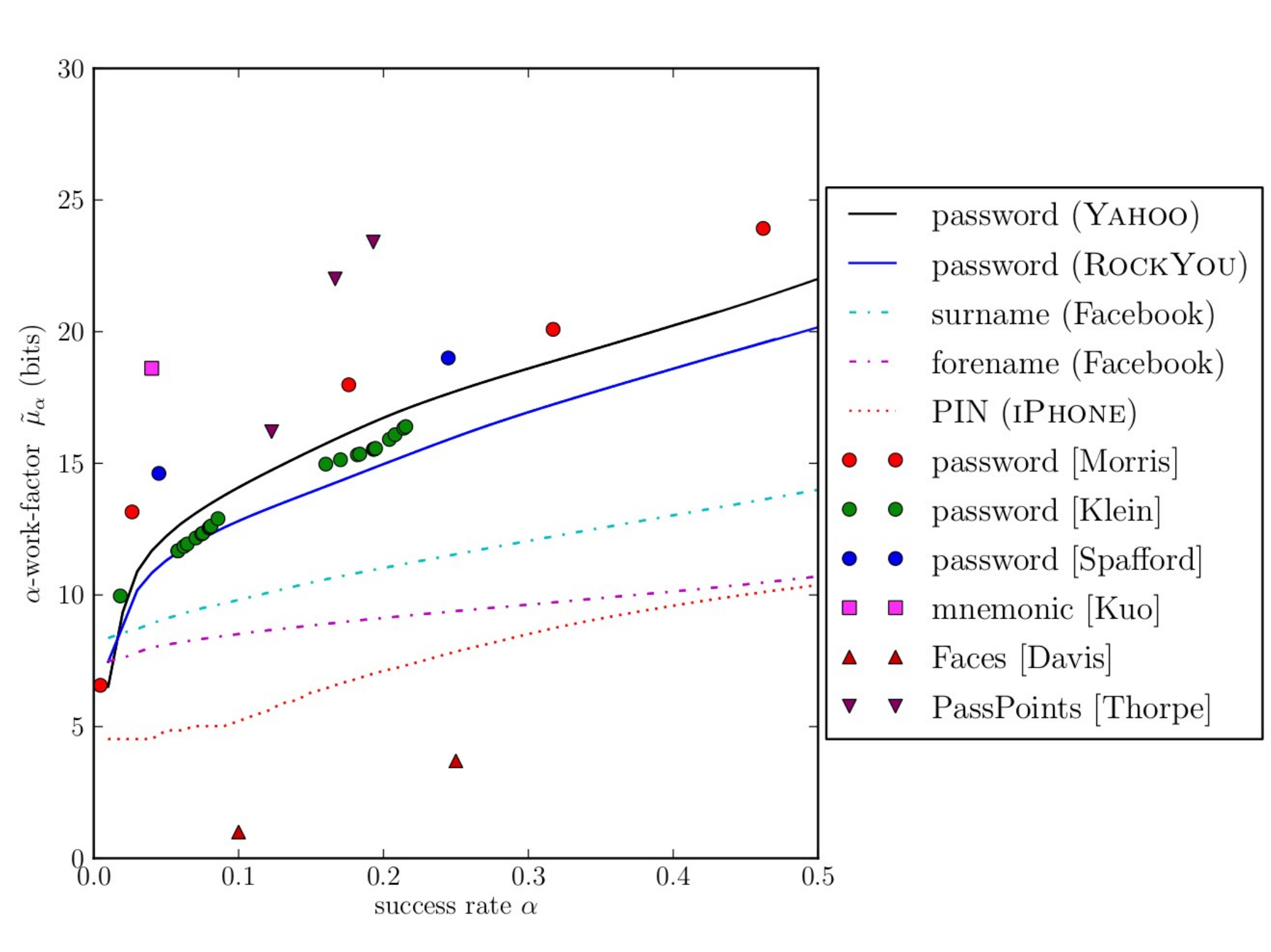
He slipped inside the house when he realised the front door was unlocked, prowling through rooms and rounding up property while the couple slept.

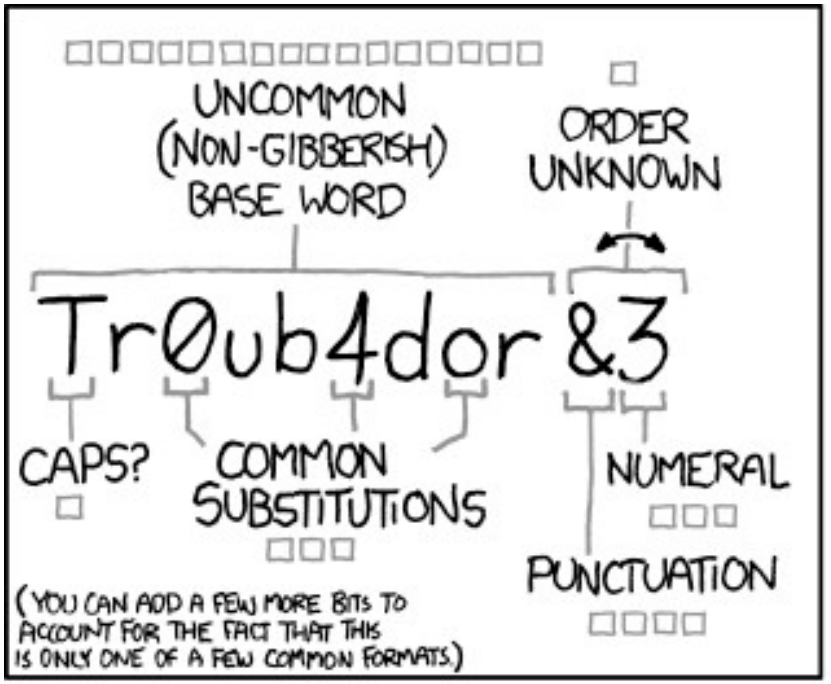
Miller was later captured on CCTV using the cards to withdraw batches of cash from the same ATM. A pre-sentence report said Miller - a heroin addict who first took drugs when he was 12- posed a risk of harm through potential confrontations with homeowners. His record includes offences of arson and robbery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

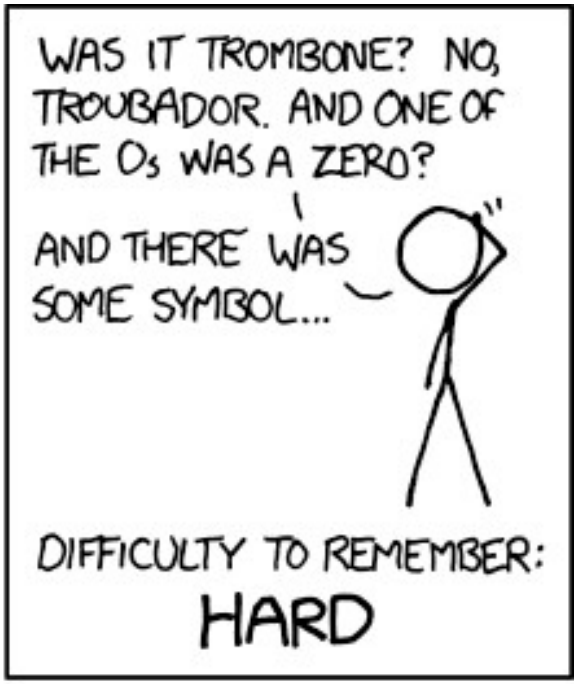
research in action...

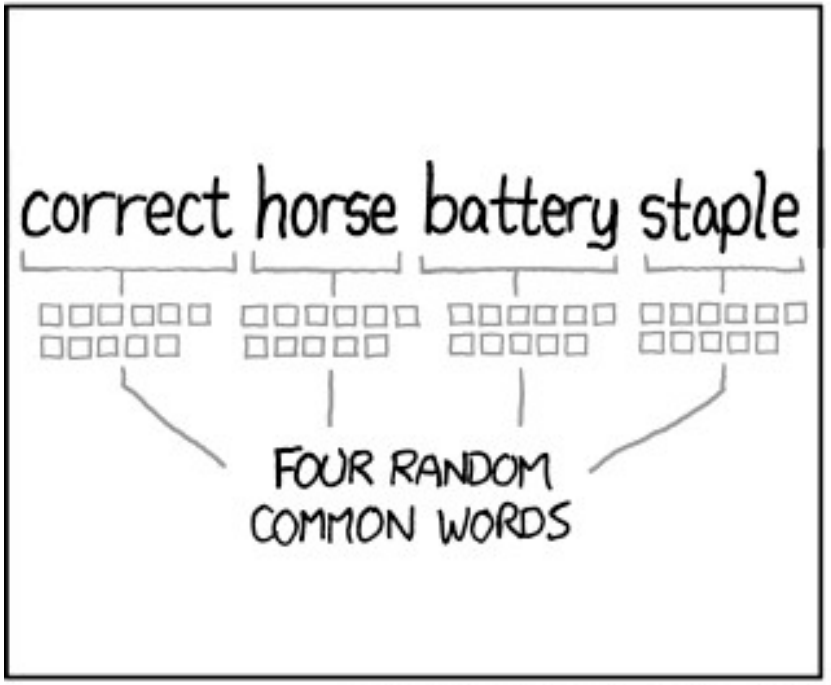
Finding #2

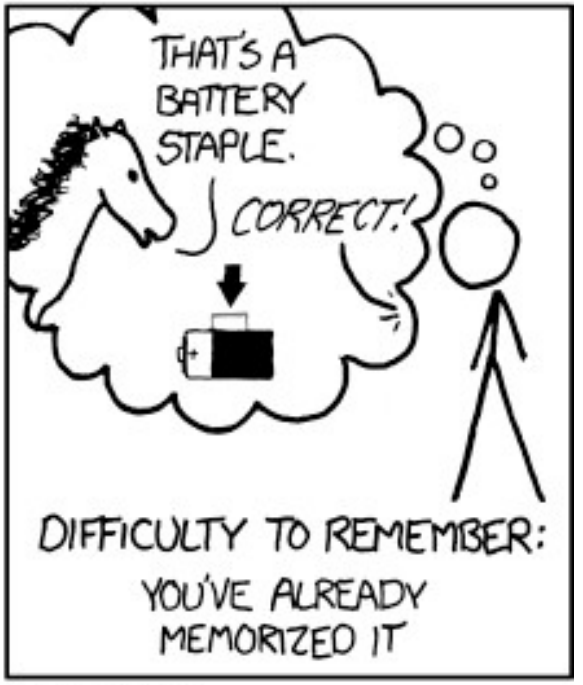
People choose passwords poorly


30
25
20
15
10
5
0
0.0
0.1
0.2
0.3
0.4
0.5
α-work-factor $\tilde{\mu}_\alpha$ (bits)
success rate α
password (YAHOO)
password (ROCKYOU)
surname (Facebook)
forename (Facebook)
PIN (IPHONE)
password [Morris]
password [Klein]
password [Spafford]
mnemonic [Kuo]
Faces [Davis]
PassPoints [Thorpe]

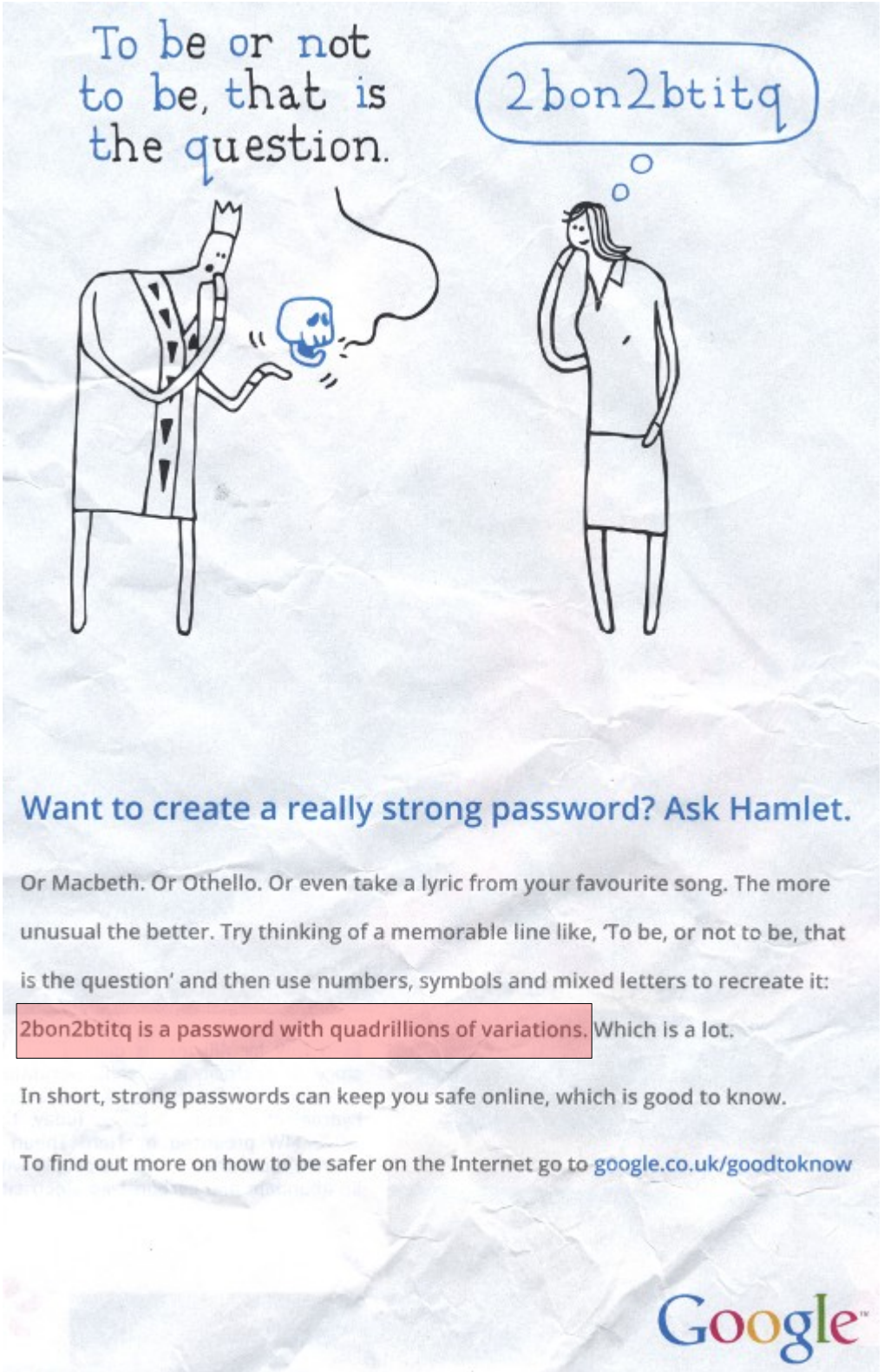








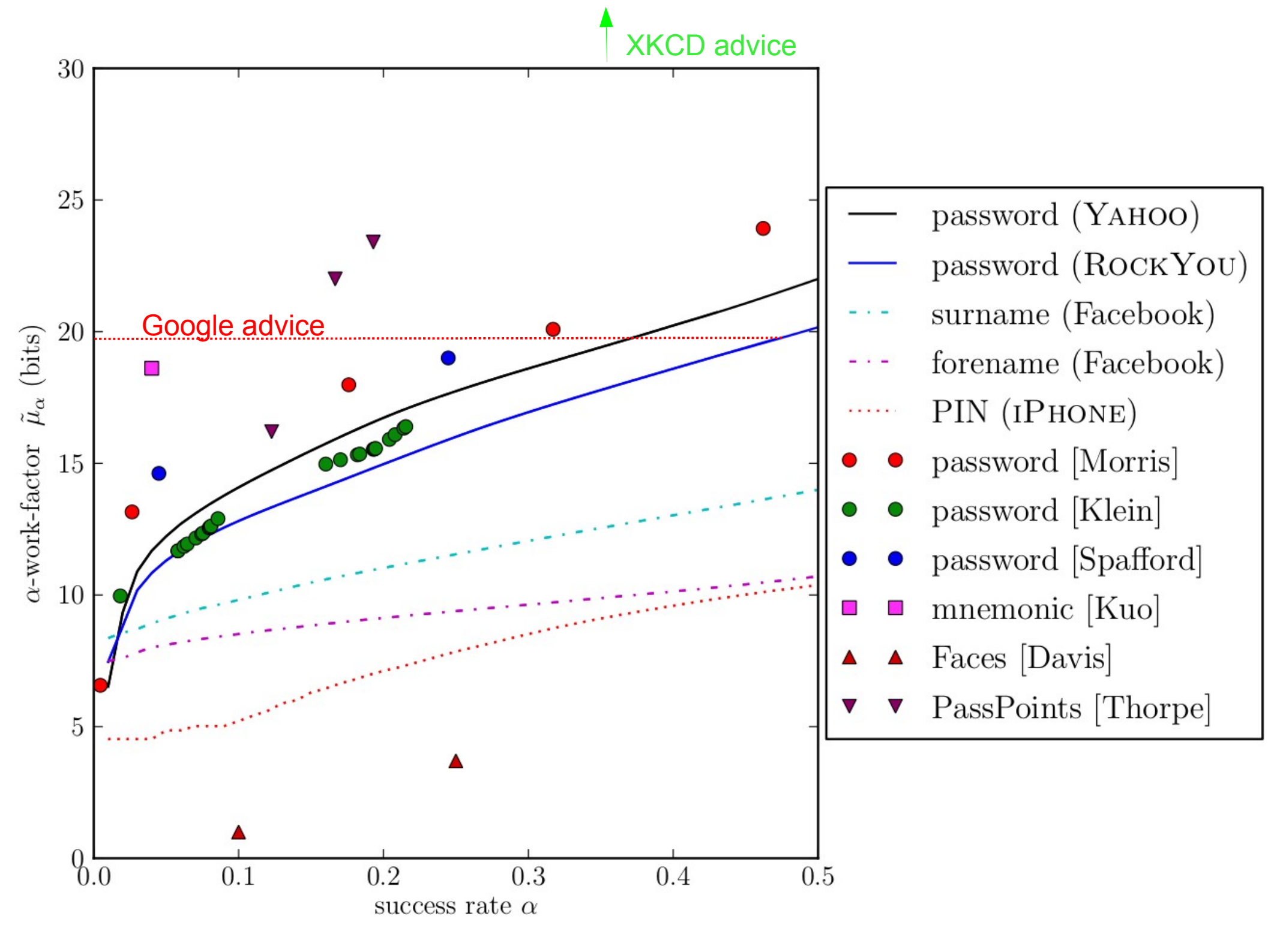
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

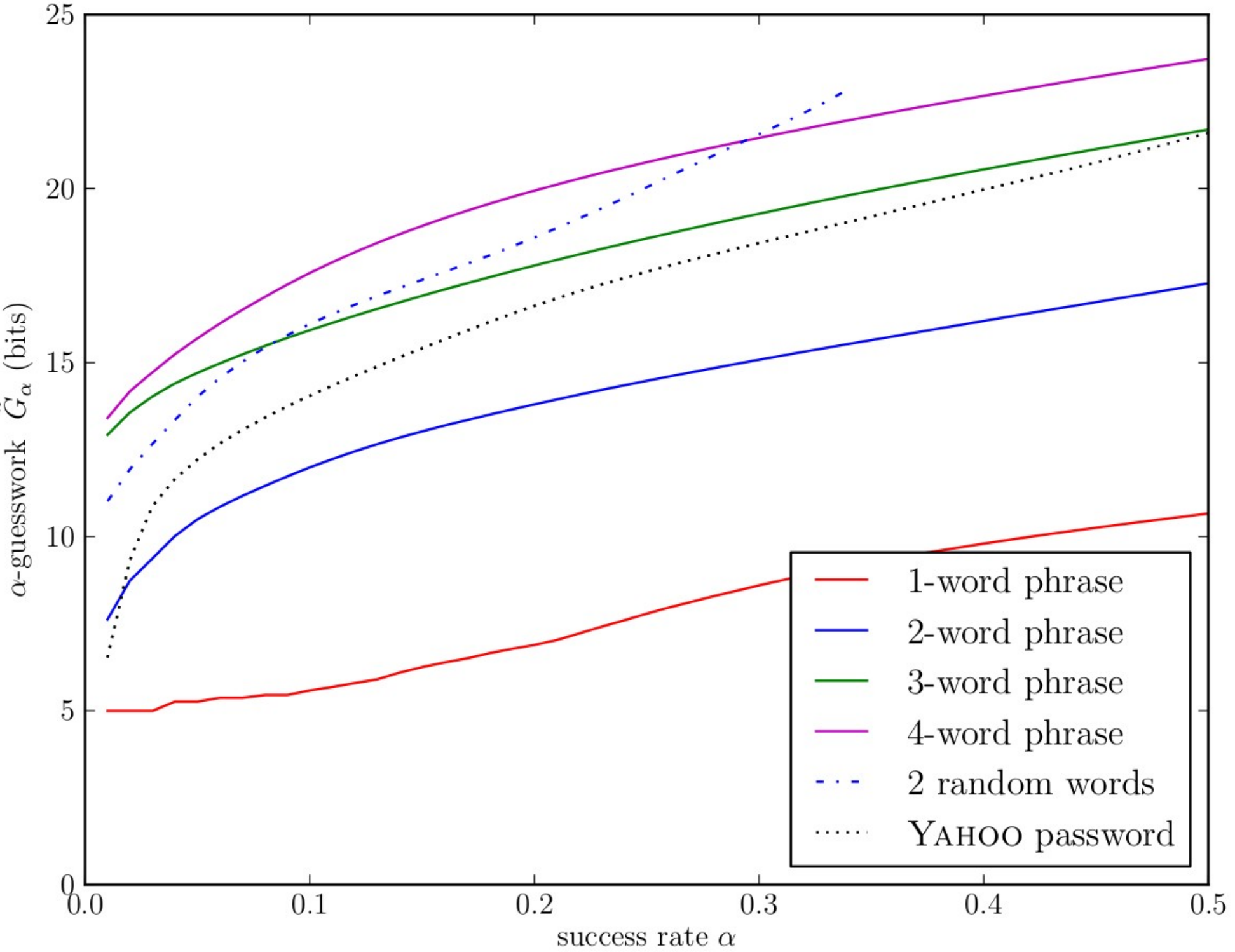


1 quadrillion variations

≈

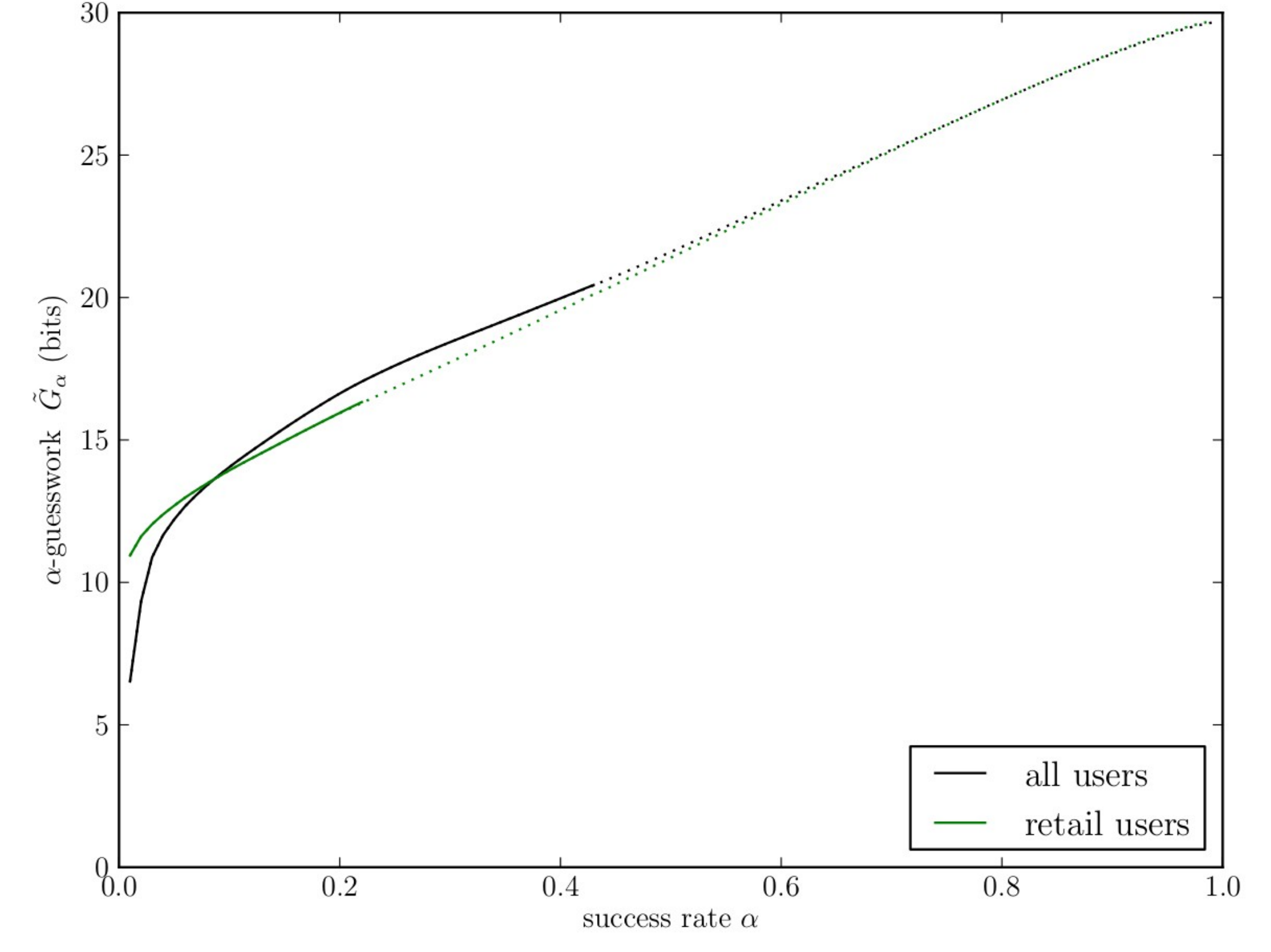
50 bits?

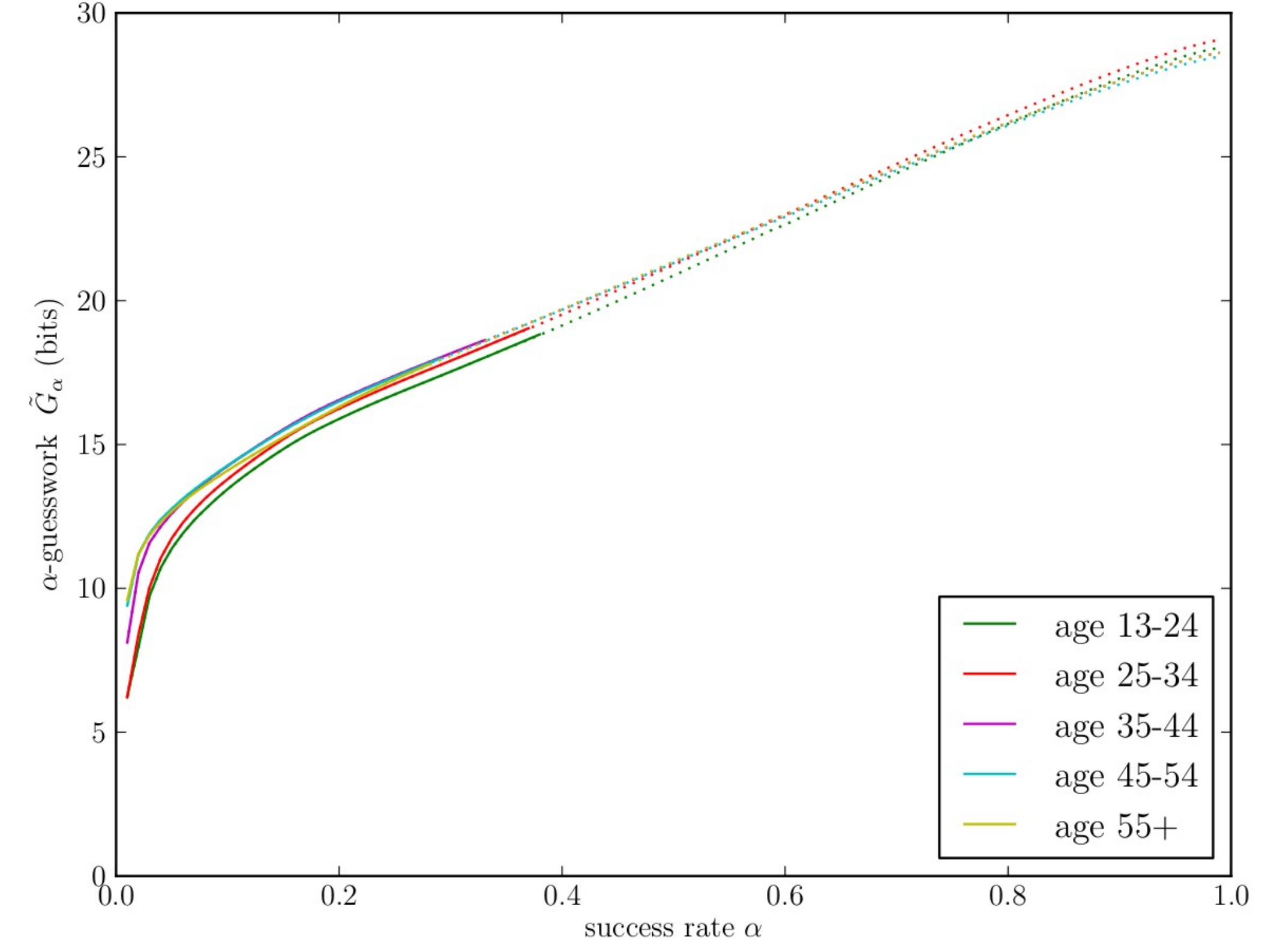

XKCD advice
Google advice
30
25
20
15
10
5
0
0.0
0.1
0.2
0.3
0.4
0.5
α-work-factor $\tilde{\mu}_\alpha$ (bits)
success rate α
password (YAHOO)
password (ROCKYOU)
surname (Facebook)
forename (Facebook)
PIN (IPHONE)
password [Morris]
password [Klein]
password [Spafford]
mnemonic [Kuo]
Faces [Davis]
PassPoints [Thorpe]


25
20
15
10
5
0
0.0
0.1
0.2
0.3
0.4
0.5
α-guesswork $\tilde{G}_\alpha$ (bits)
success rate α
1-word phrase
2-word phrase
3-word phrase
4-word phrase
2 random words
YAHOO password

Finding #3

Motivation doesn't really matter


30
25
20
15
10
5
0
0.0
0.2
0.4
0.6
0.8
1.0
α-guesswork $\tilde{G}_\alpha$ (bits)
success rate α
all users
retail users


30
25
20
15
10
5
0
0.0
0.2
0.4
0.6
0.8
1.0
α-guesswork $\tilde{G}_\alpha$ (bits)
success rate α
age 13-24
age 25-34
age 35-44
age 45-54
age 55+

Finding #4

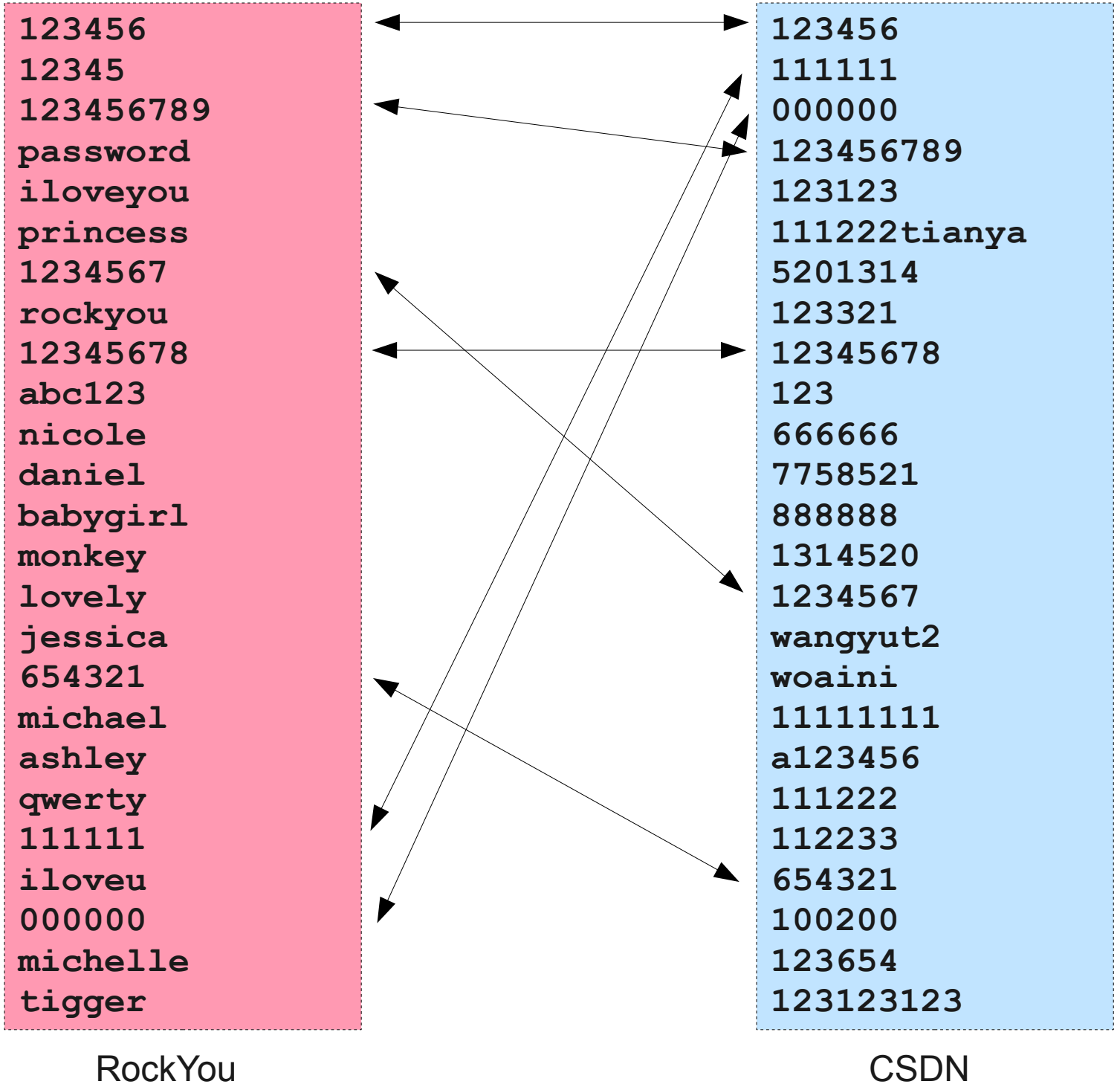
Bad passwords are universal

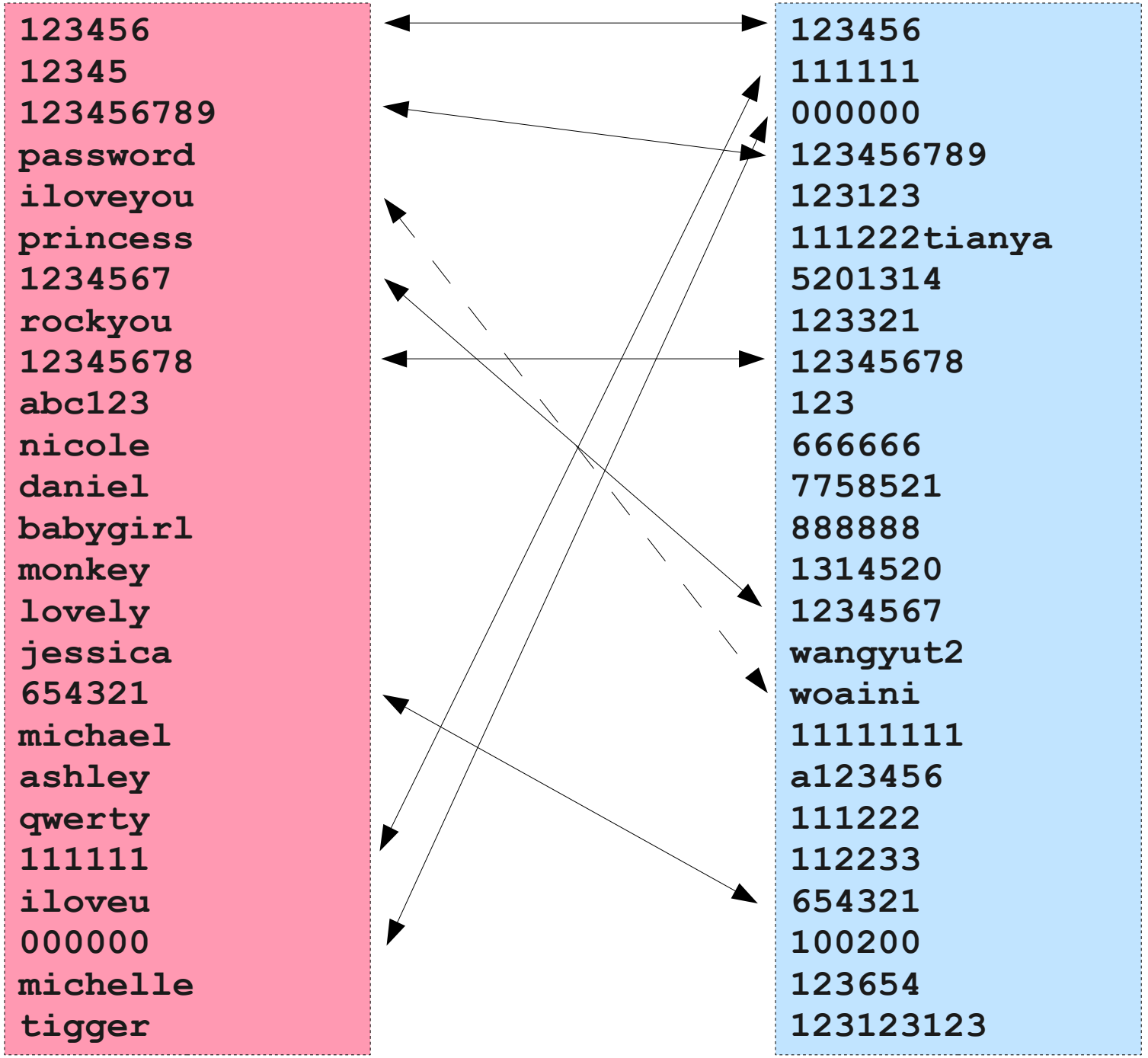
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger

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

RockYou
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

CSDN
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

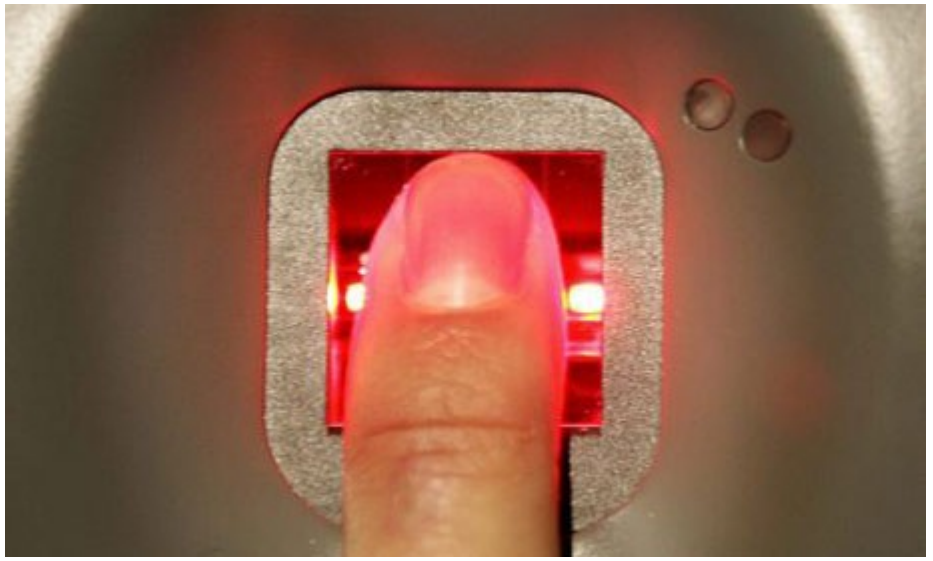

123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger
123456
111111
000000
123456789
123123
111222tianya
5201314
123321
12345678
123
666666
7758521
888888
1314520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


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
RockYou
CSDN

Challenge #1

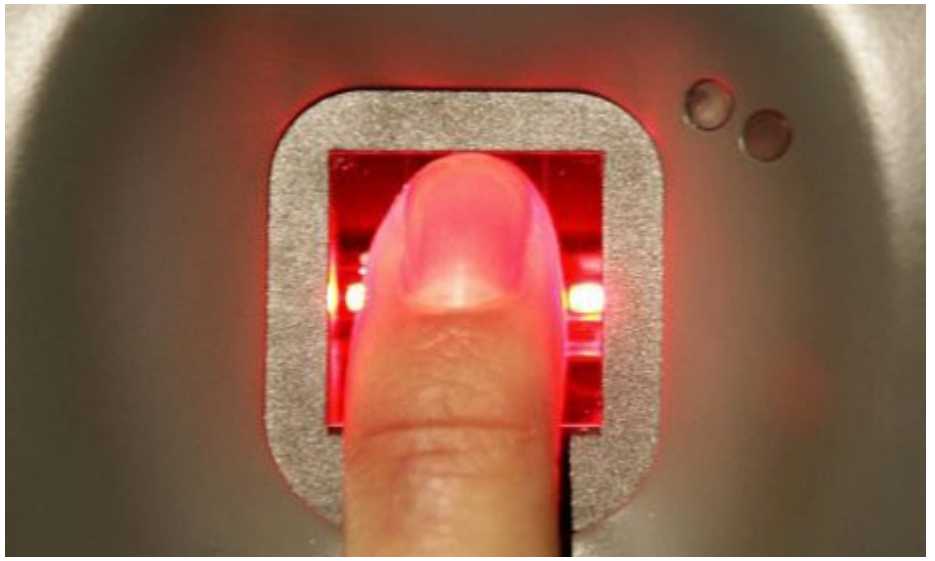
human-machine authentication

trusted hardware?

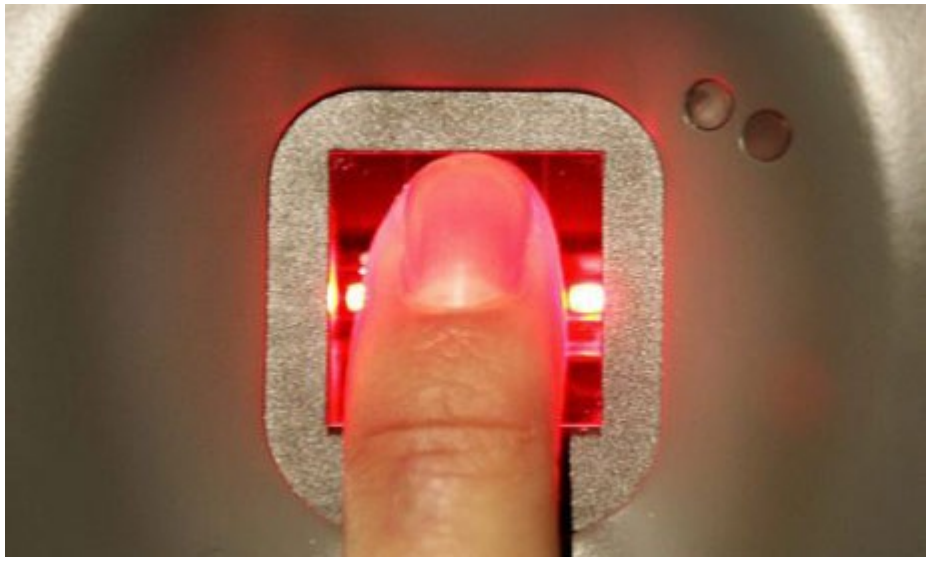


fingerprint biometrics

fingerprint biometrics

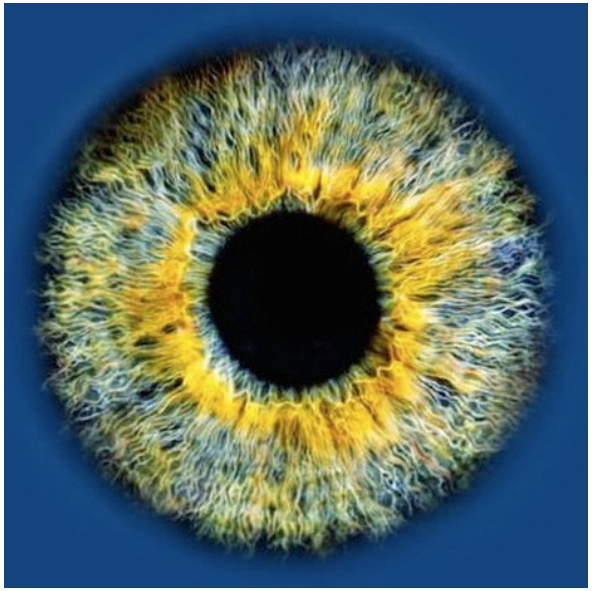


fingerprint biometrics

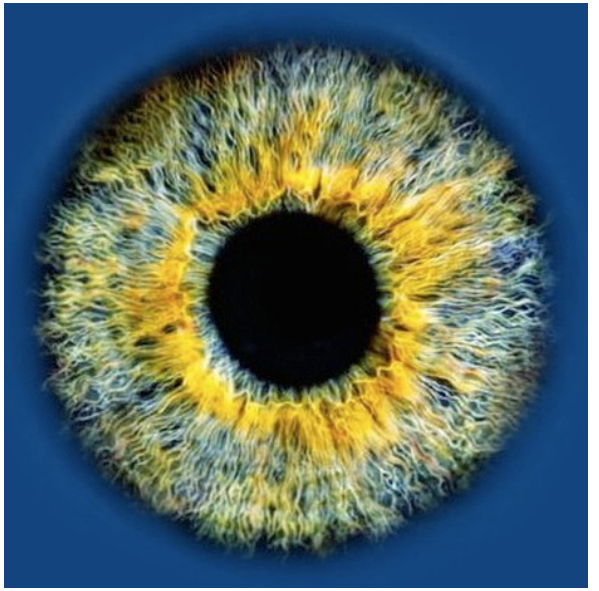


Matsumoto et al. 2002

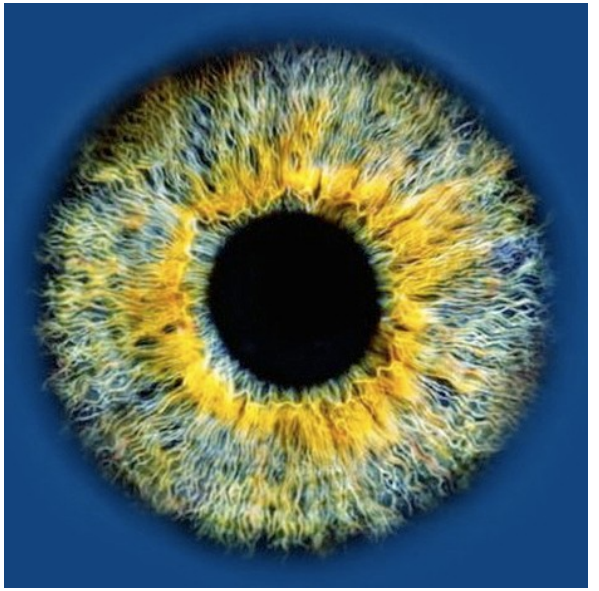
iris biometrics

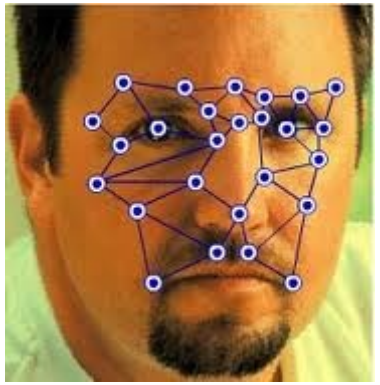


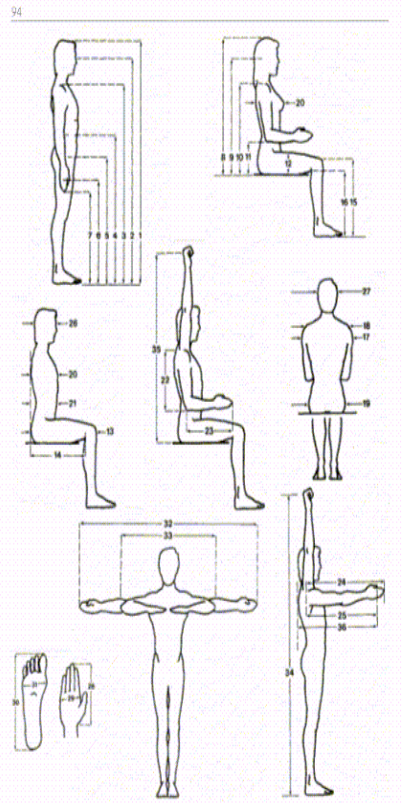
iris biometrics



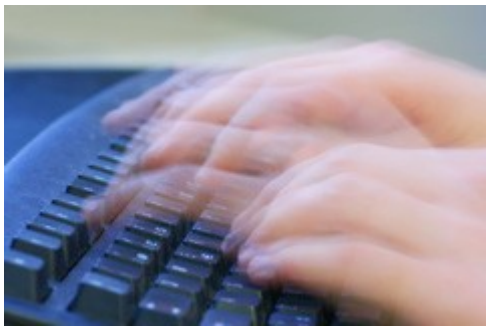
iris biometrics







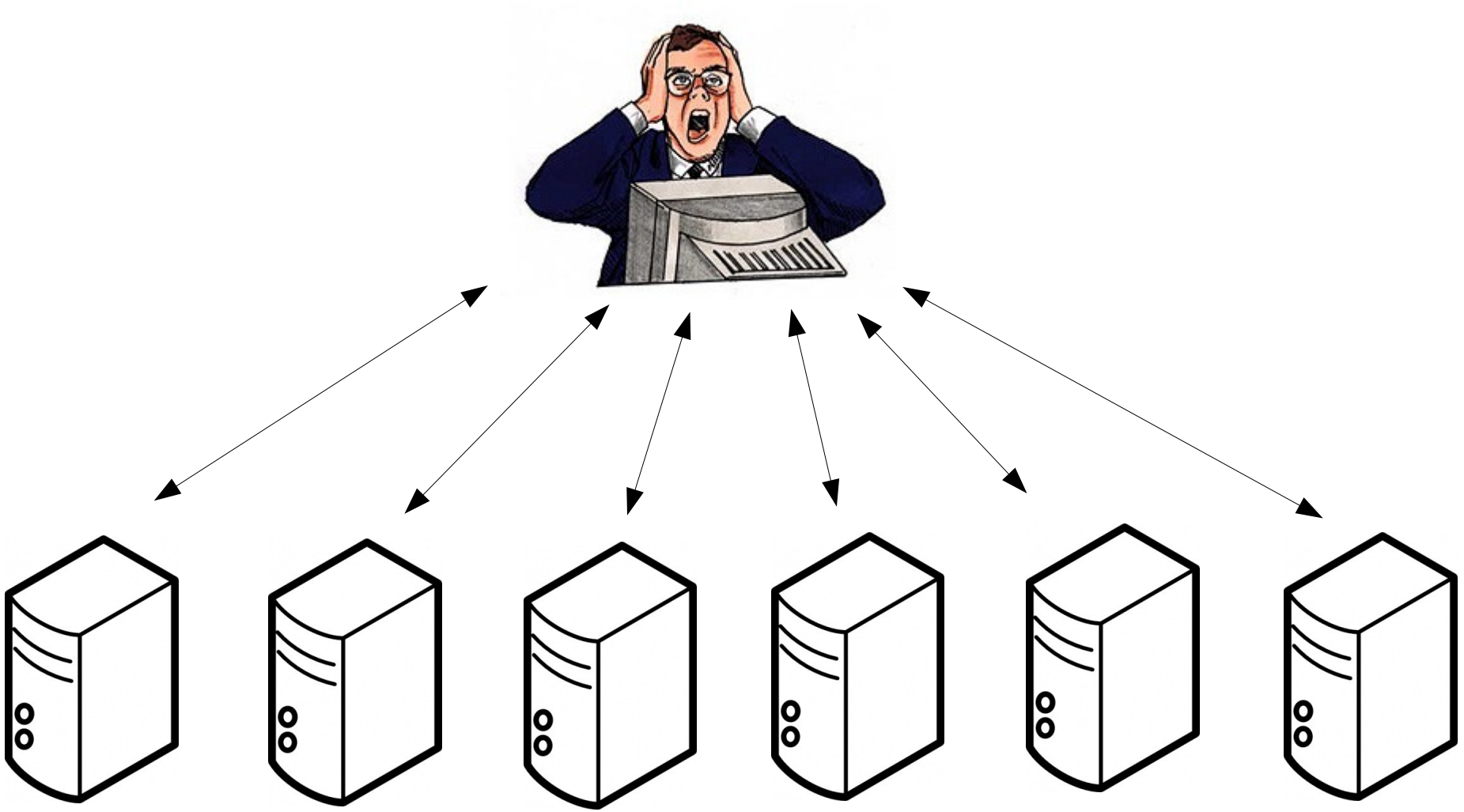
other biometrics



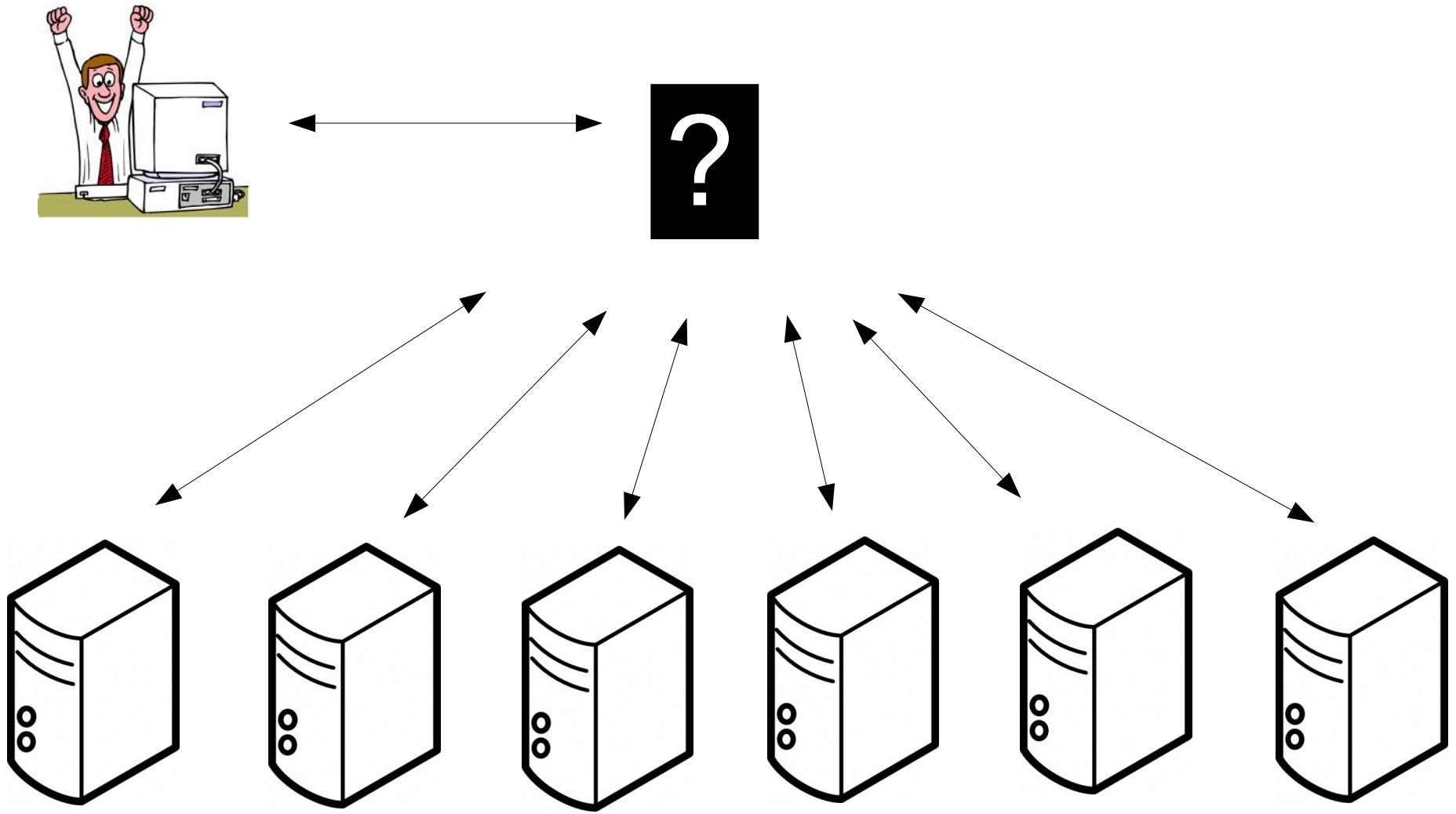
Challenge #2

the Internet identity layer
(machine-machine)

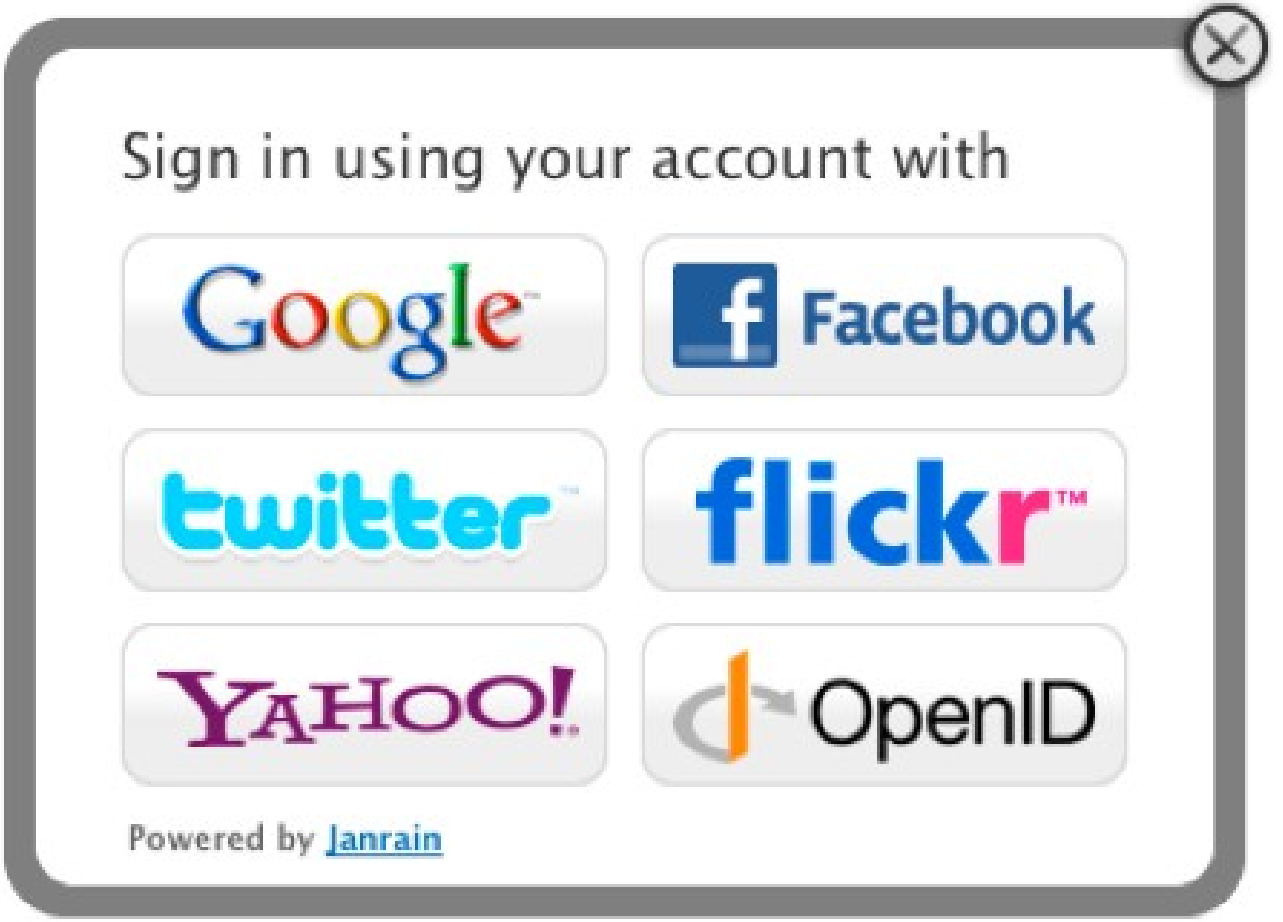
Today's Internet identity layer



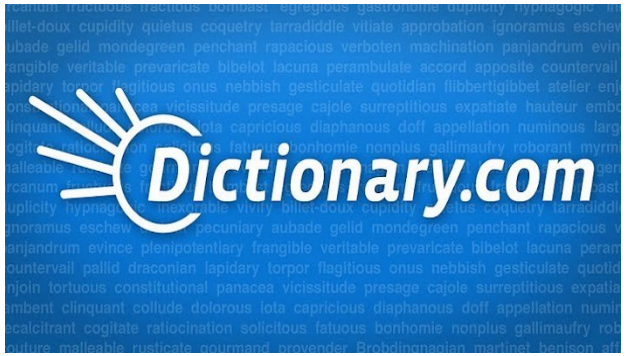
Tomorrow's Internet identity layer



Today's approximation



Who controls your identity?



the state or fact of **remaining** the same

...we may replace past names associated with your Google Account so that you are represented consistently across all our services.

Google™

Challenge #3

machine-human authentication

Secure Connection Failed

www.vedetta.com uses an invalid security certificate.

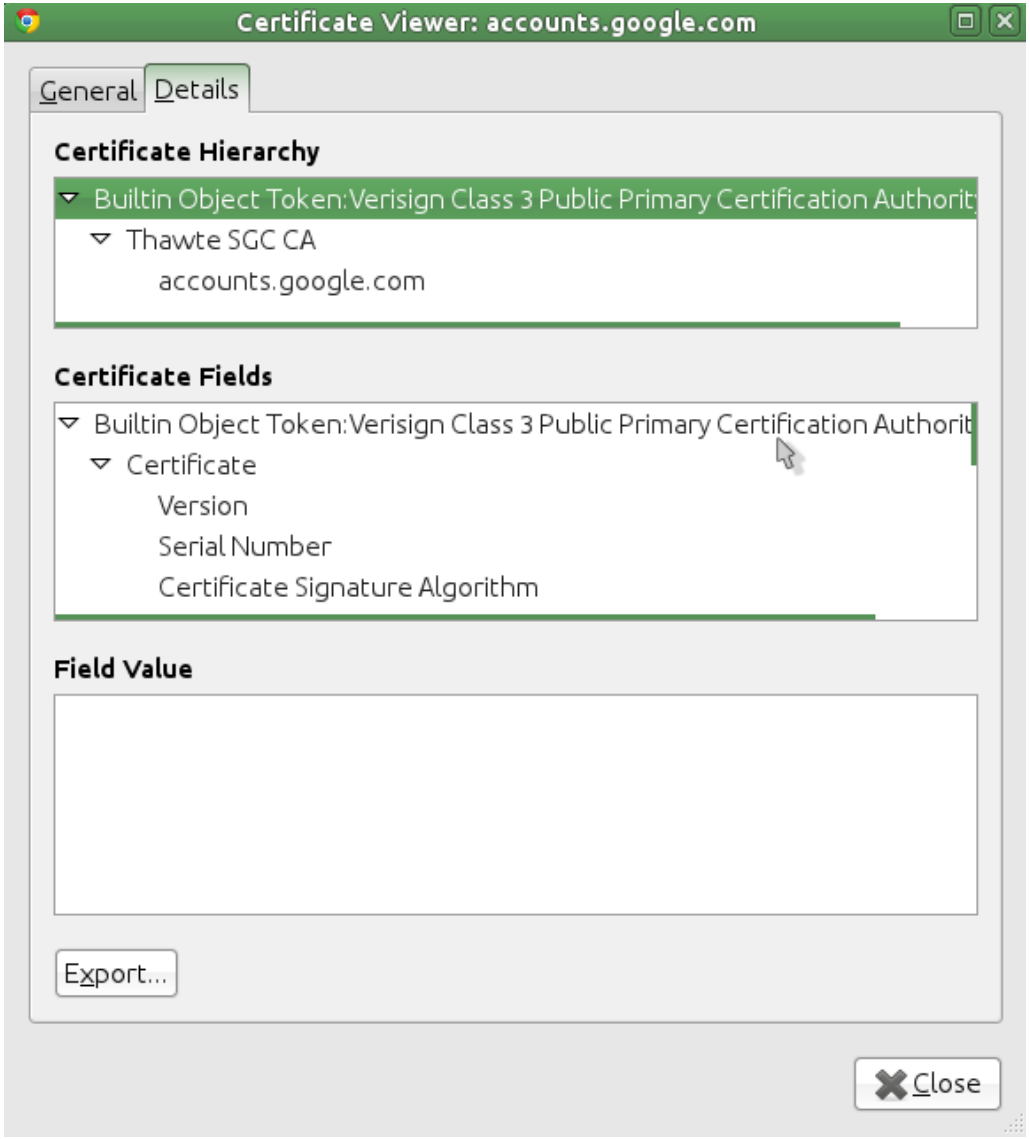
The certificate is not trusted because it is self signed.

(Error code: sec_error_ca_cert_invalid)

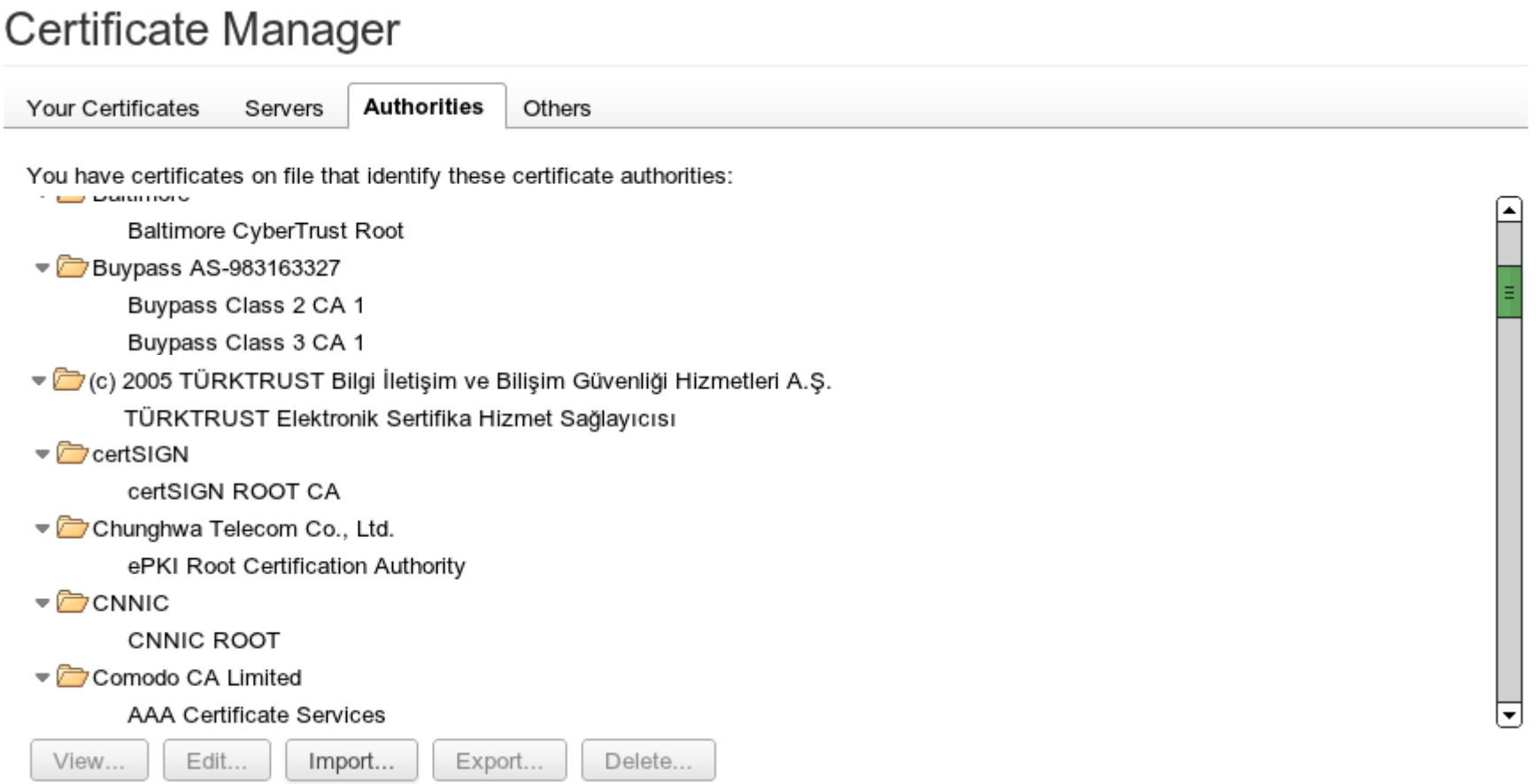
- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

Or you can add an exception...

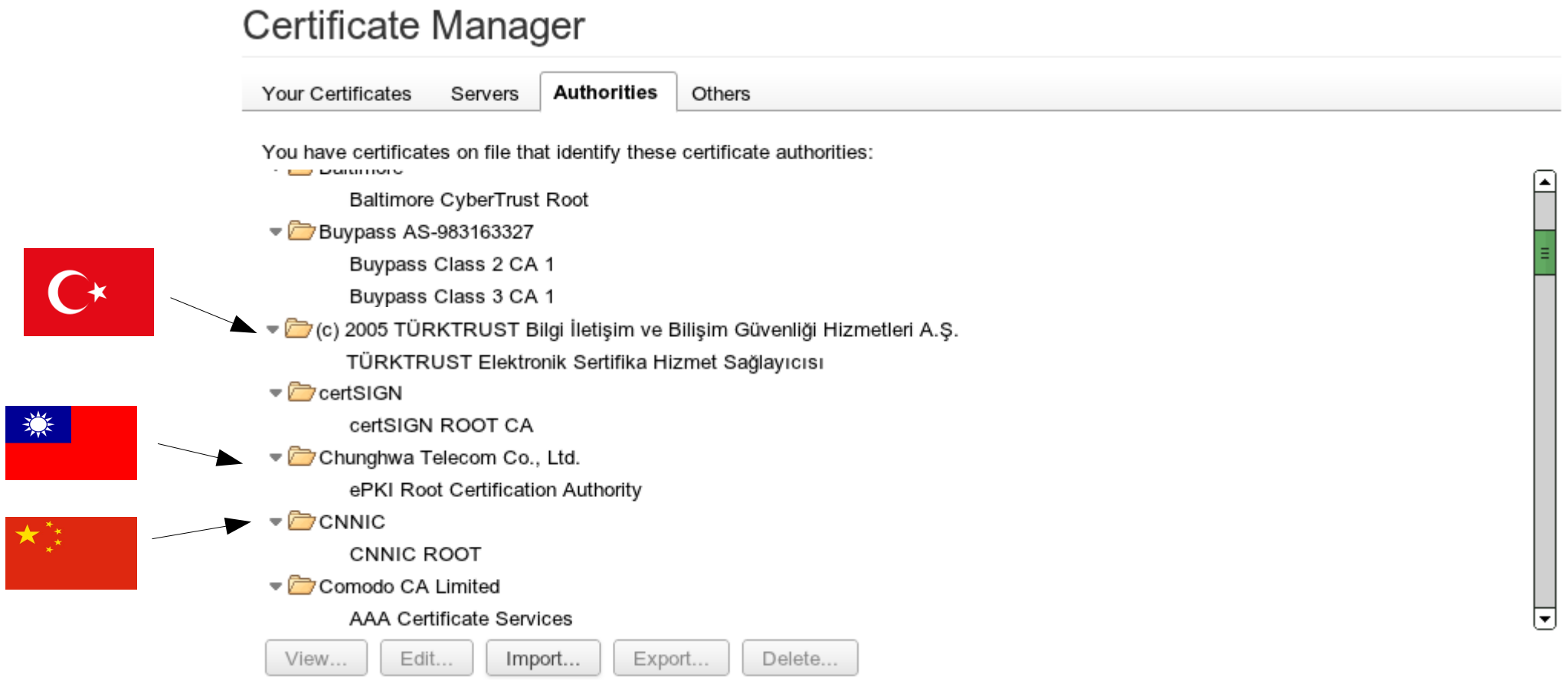
https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.com/mail/?tab%3Dwm&scc=1&ltmpl=default&ltmplcache=2



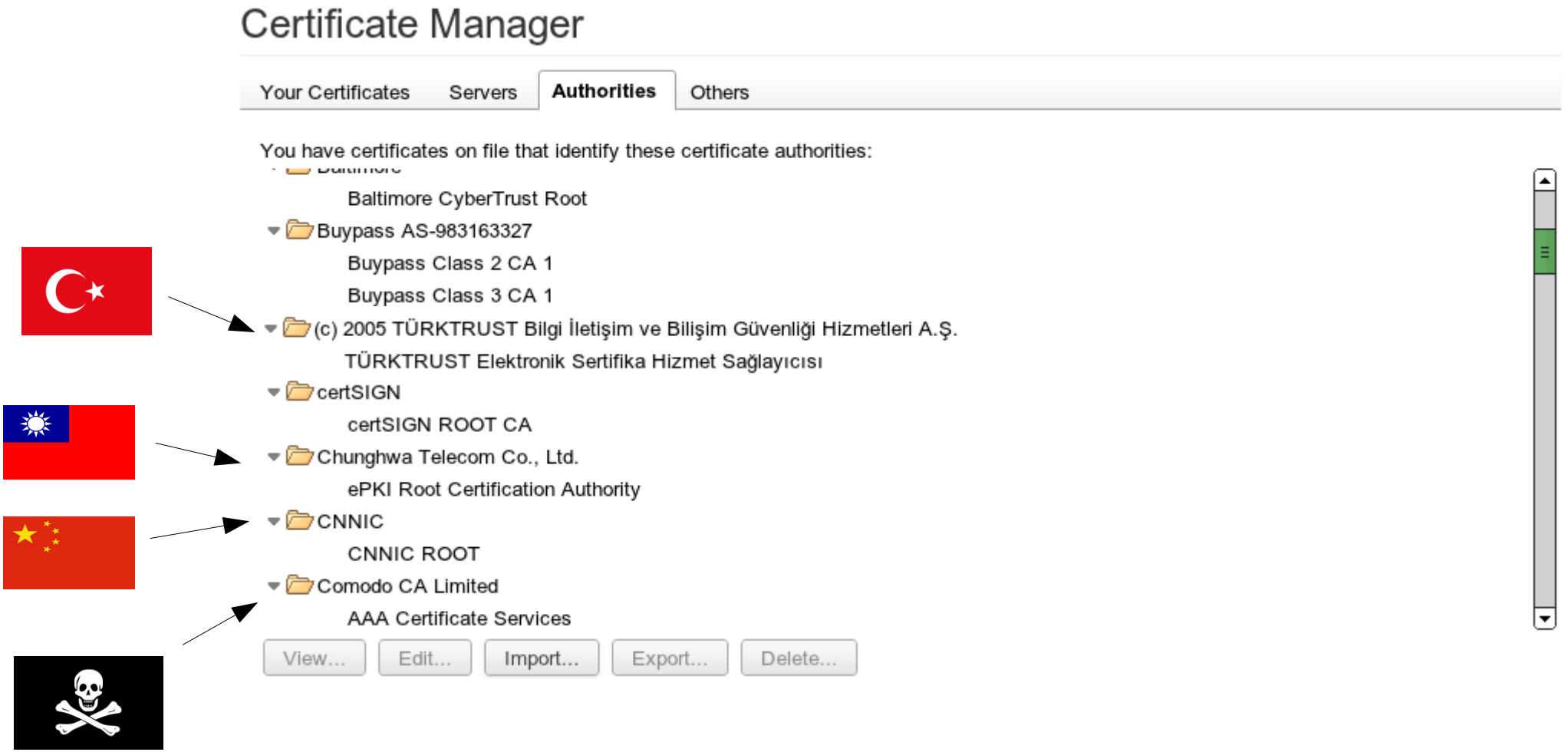
Whom do you trust by default?



Whom do you trust by default?



Whom do you trust by default?



Better models

Is this the key everybody else sees?

Is this the key you gave me at first?

Computers are useless

They can only give you answers

Pablo Picasso, 1968

Thank you all ☺

Guessing human-chosen secrets

Joseph Bonneau

University of Cambridge
Churchill College

April 2012

This dissertation is submitted for
the degree of Doctor of Philosophy