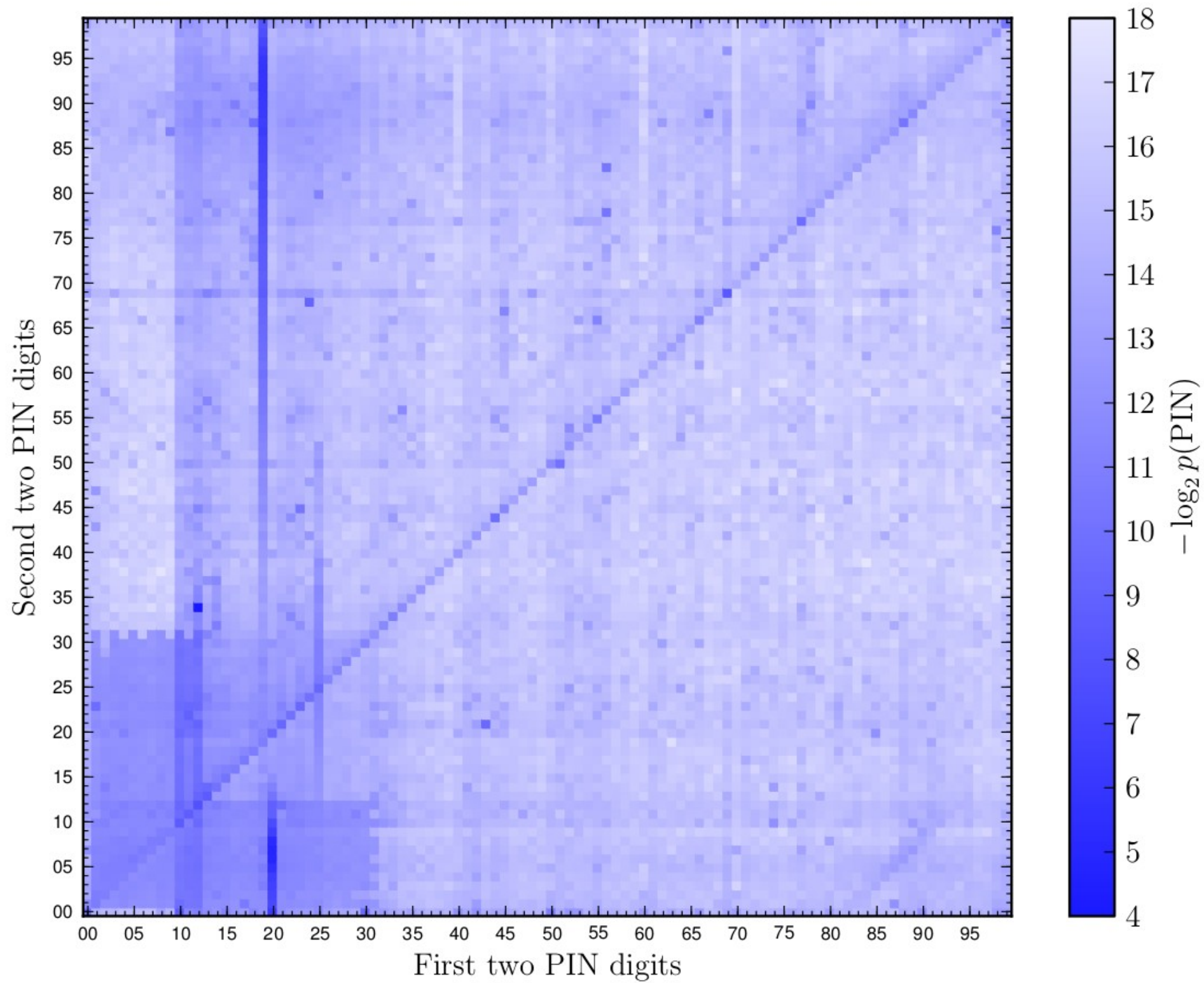


Authentication in a networked world

Joseph Bonneau
Gates Scholars Internal Symposium
May 2, 2012

Finding #1

People choose banking PINs poorly



'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 Wall-

send 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.

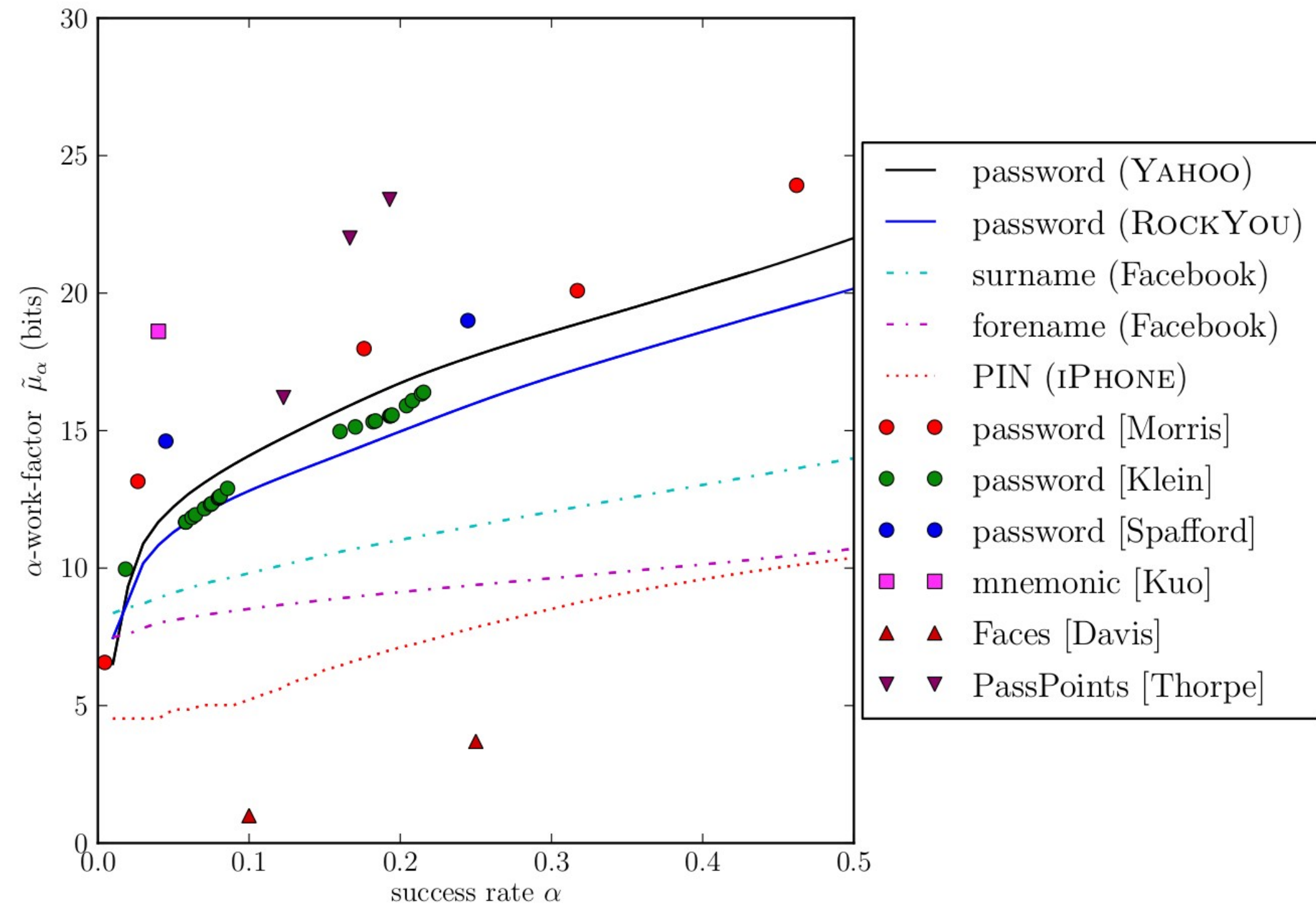


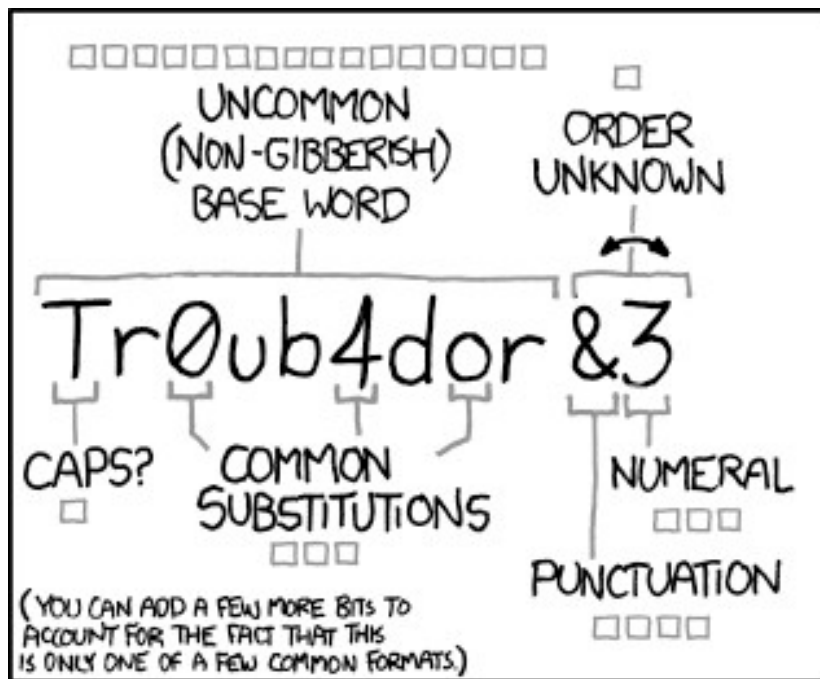
CONVICTED Miller

research in action...

Finding #2

People choose passwords poorly





~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

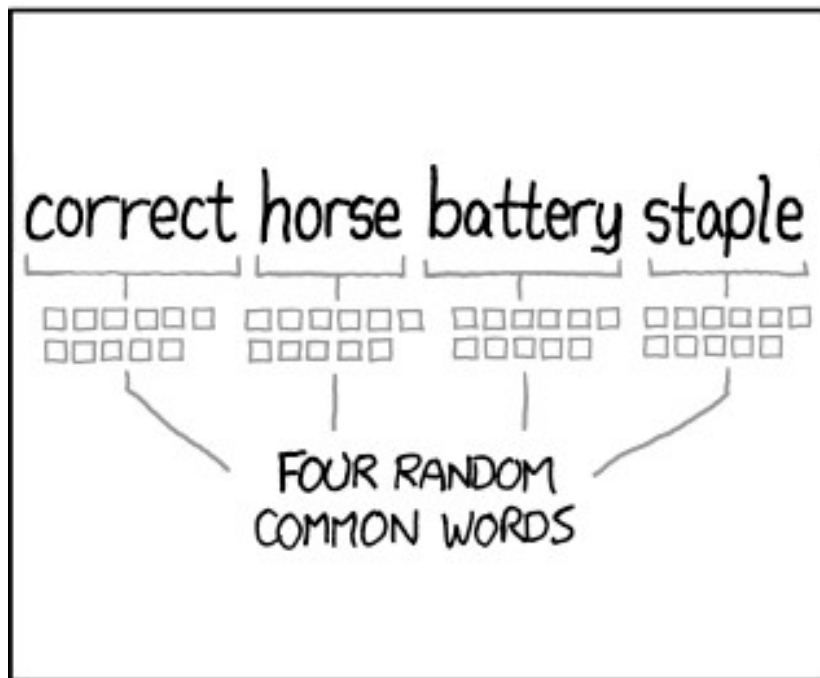
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

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

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

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.

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



2bon2btitq



1 quadrillion
variations
≈
50 bits?

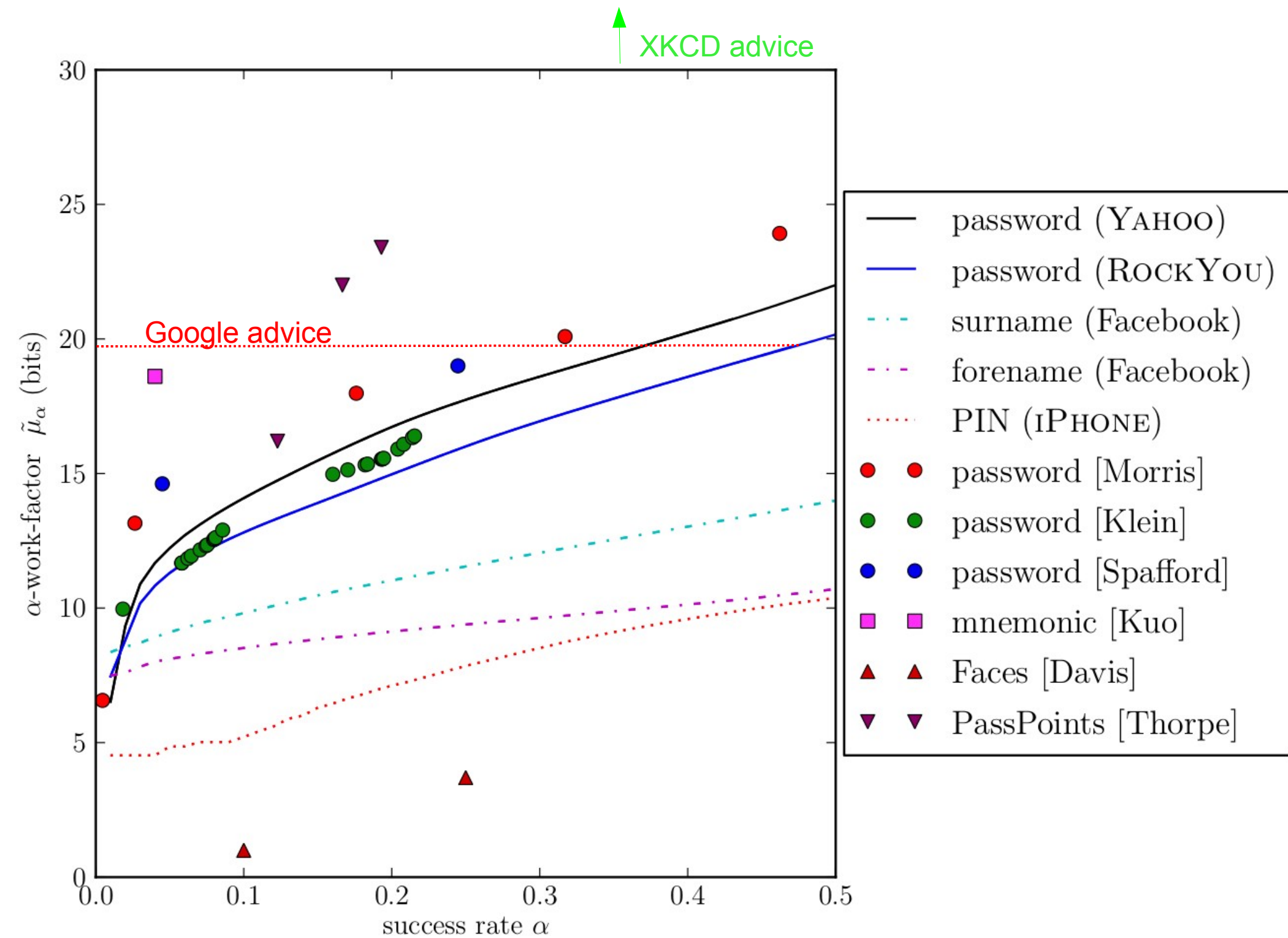
Want to create a really strong password? Ask Hamlet.

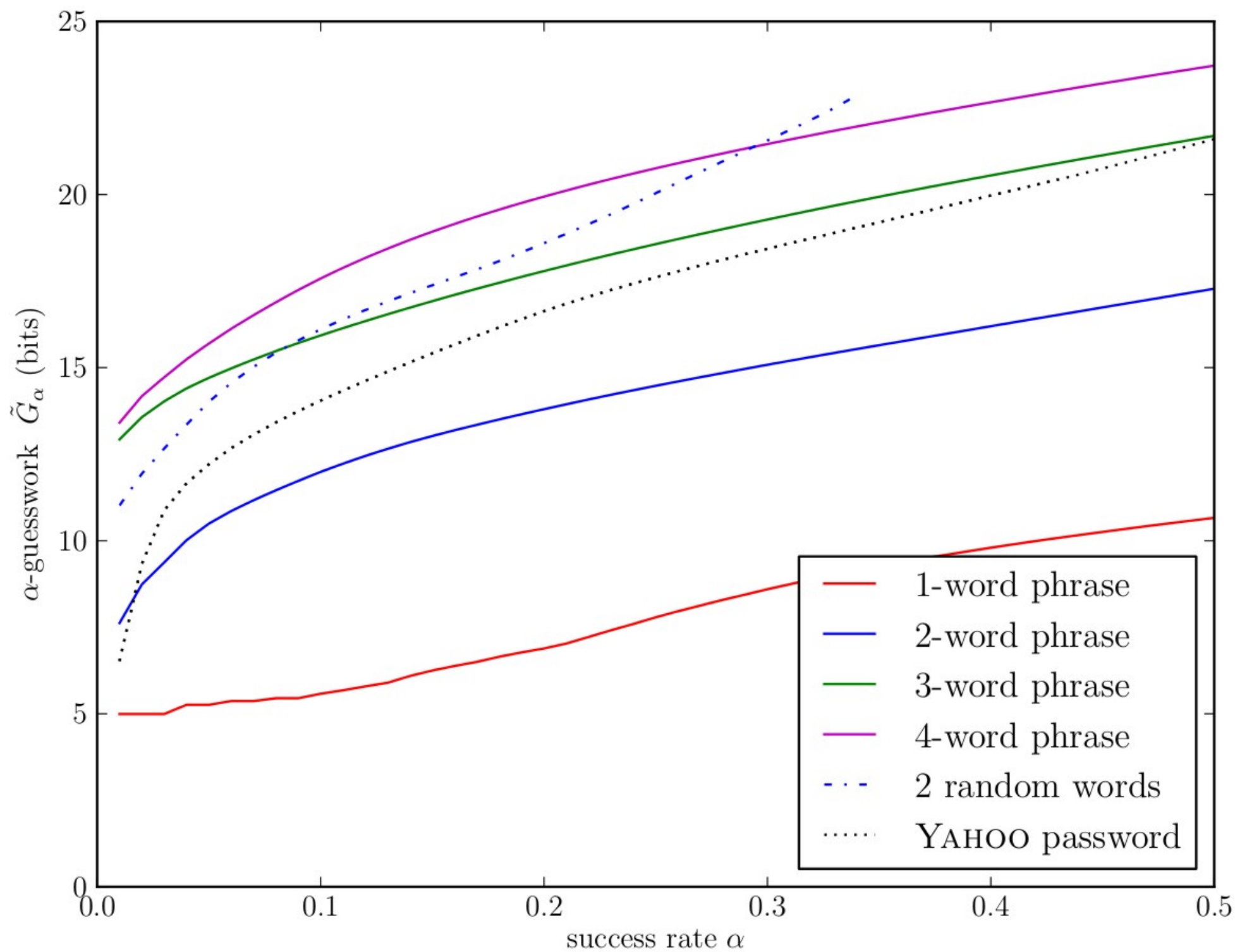
Or Macbeth. Or Othello. Or even take a lyric from your favourite song. The more unusual the better. Try thinking of a memorable line like, 'To be, or not to be, that is the question' and then use numbers, symbols and mixed letters to recreate it:

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.

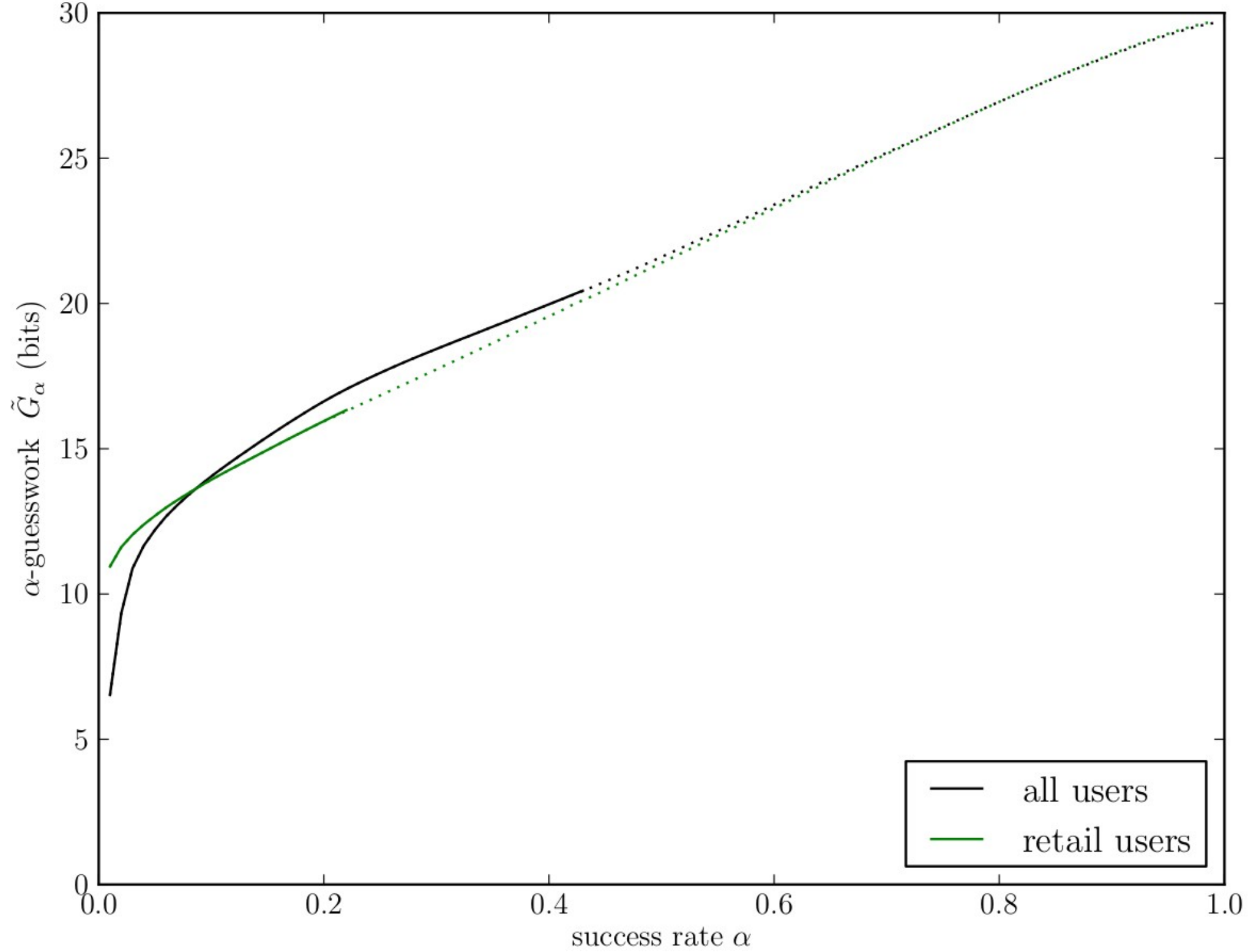
To find out more on how to be safer on the Internet go to google.co.uk/goodtoknow

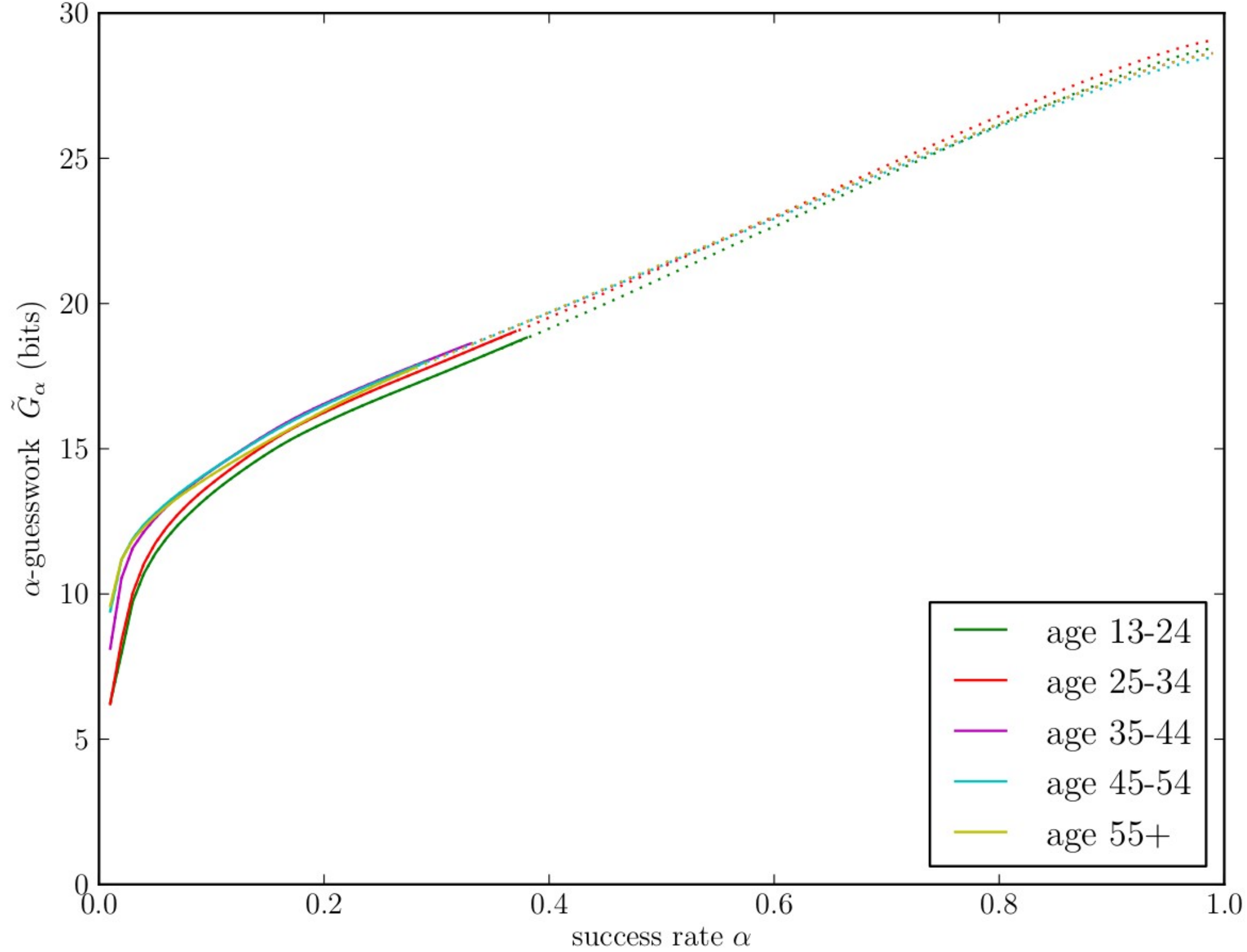




Finding #3

Motivation doesn't really matter





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

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

RockYou

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

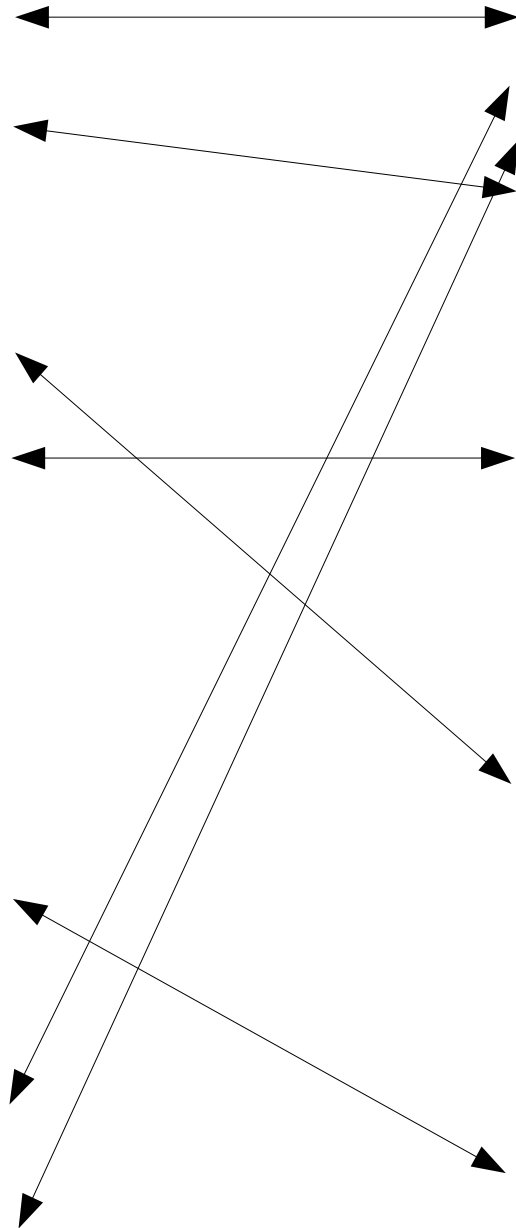
CSDN

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

RockYou

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

CSDN

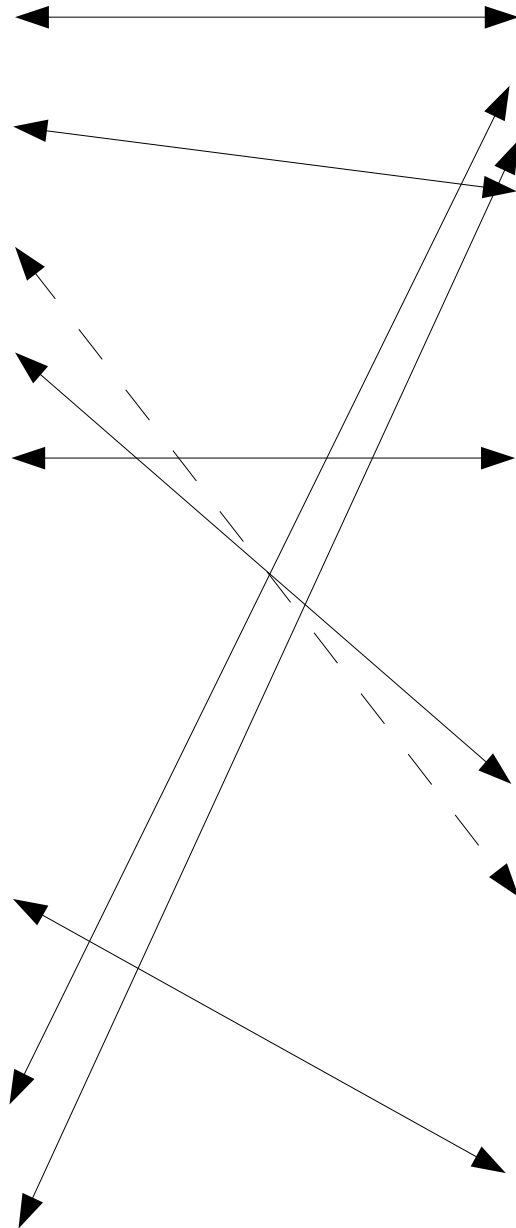


123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger

RockYou

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

CSDN



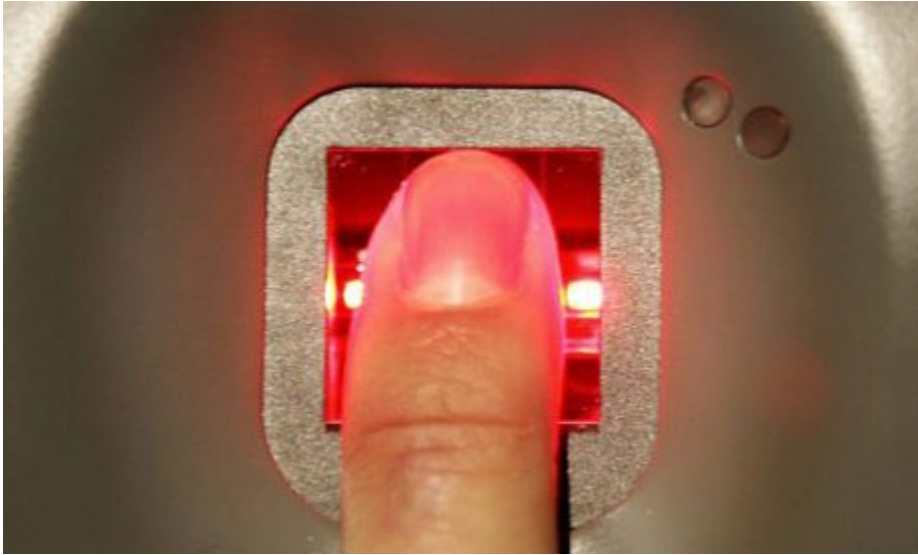
Challenge #1

human-machine authentication



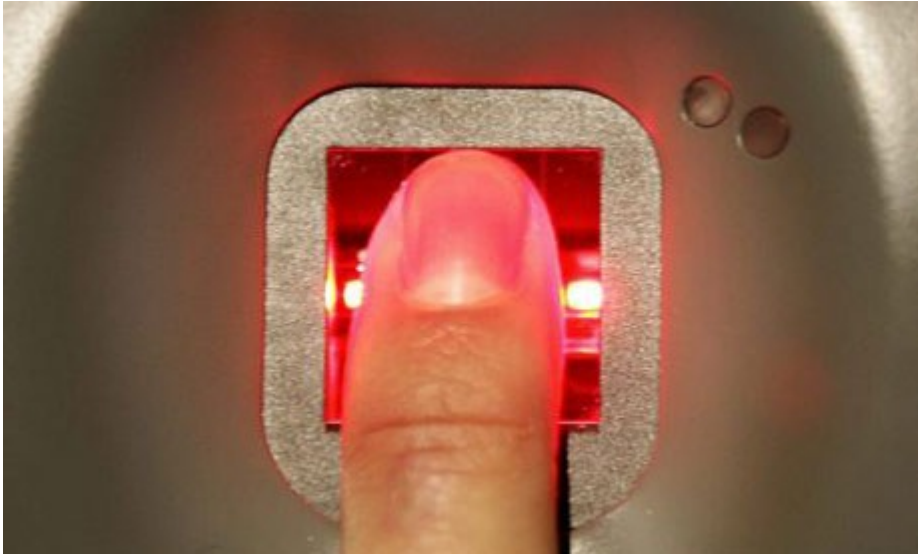
trusted hardware?



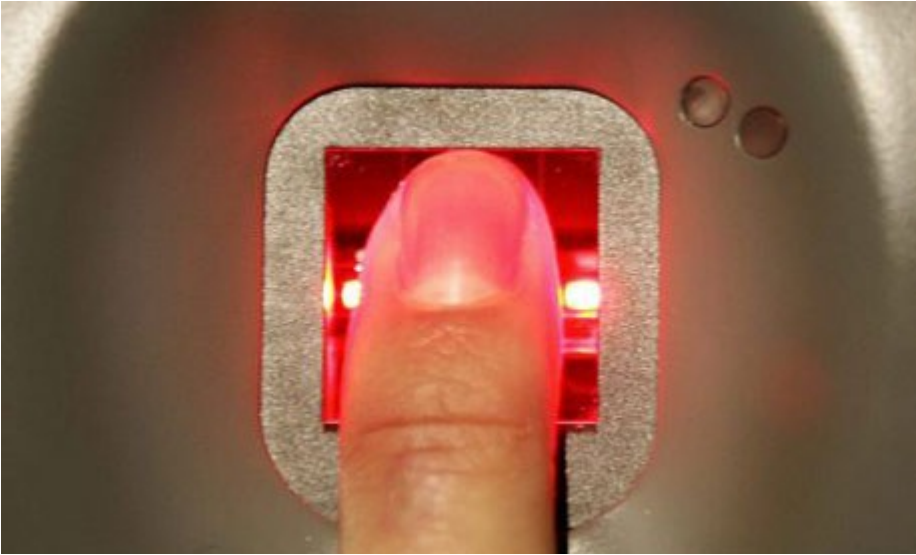


fingerprint
biometrics

fingerprint biometrics



fingerprint biometrics



Matsumoto et al. 2002

iris biometrics

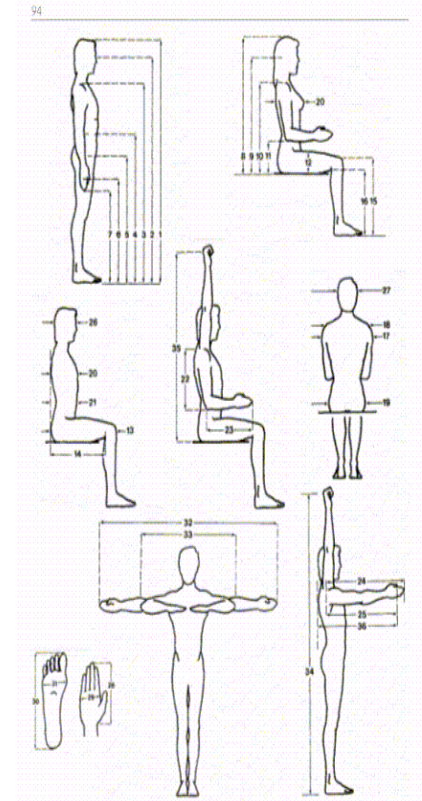
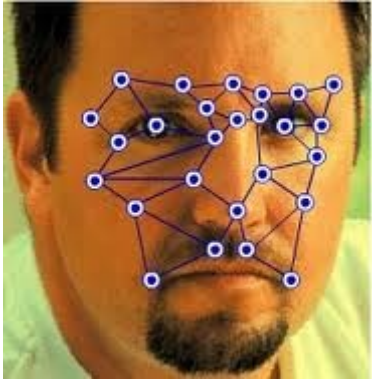


iris biometrics



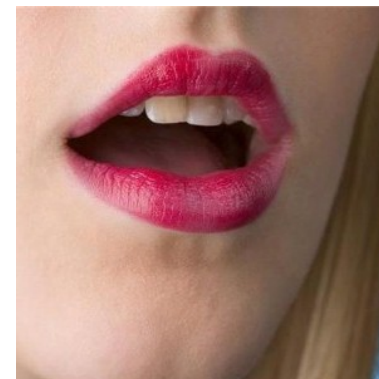
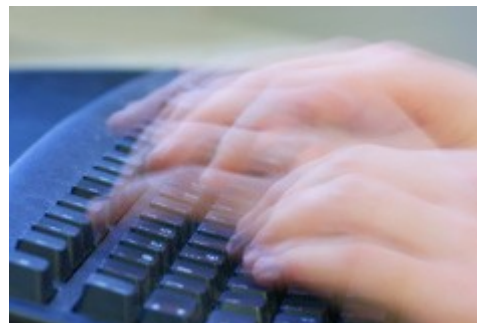
iris biometrics





Joseph
B...

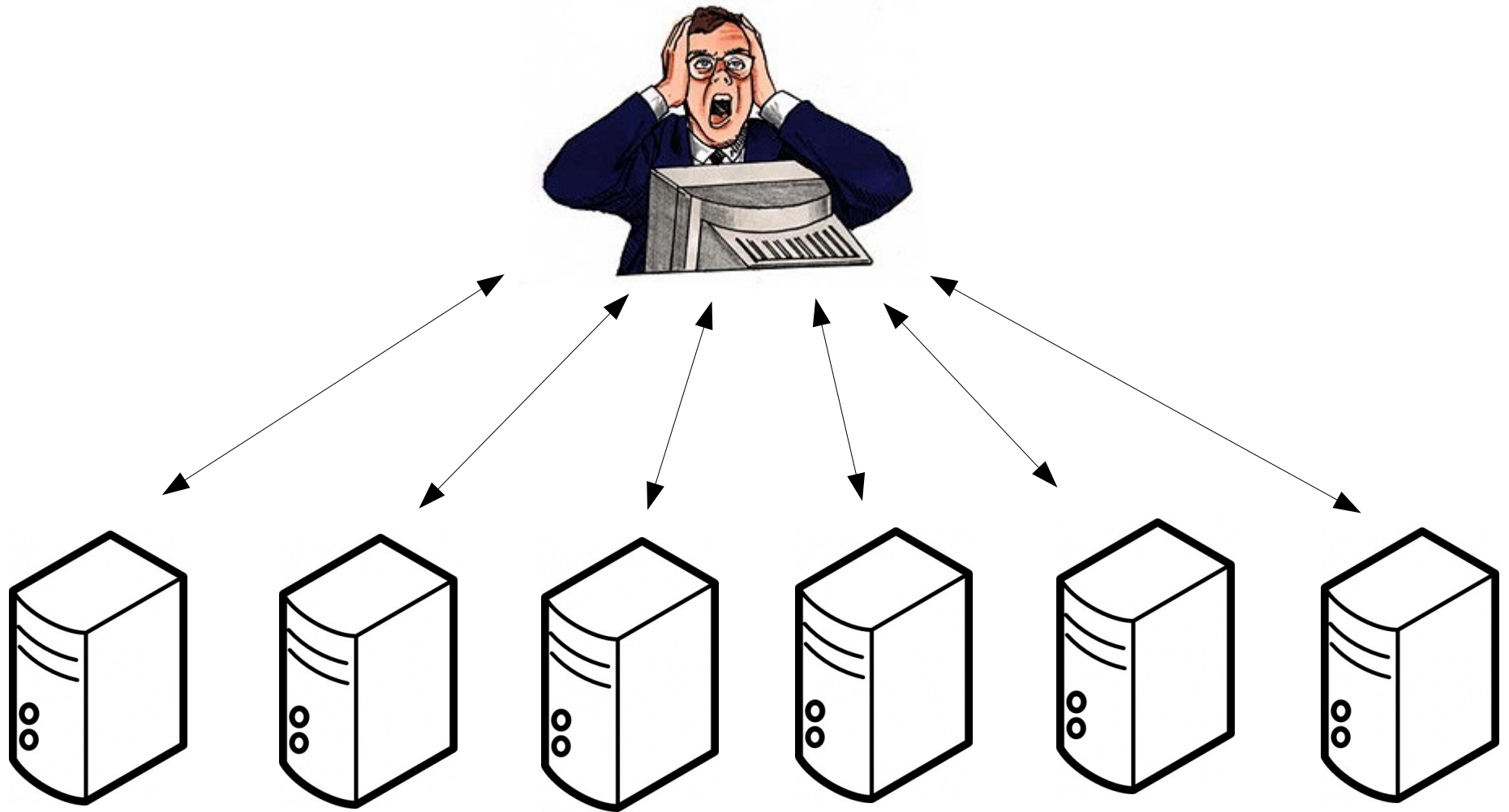
other biometrics



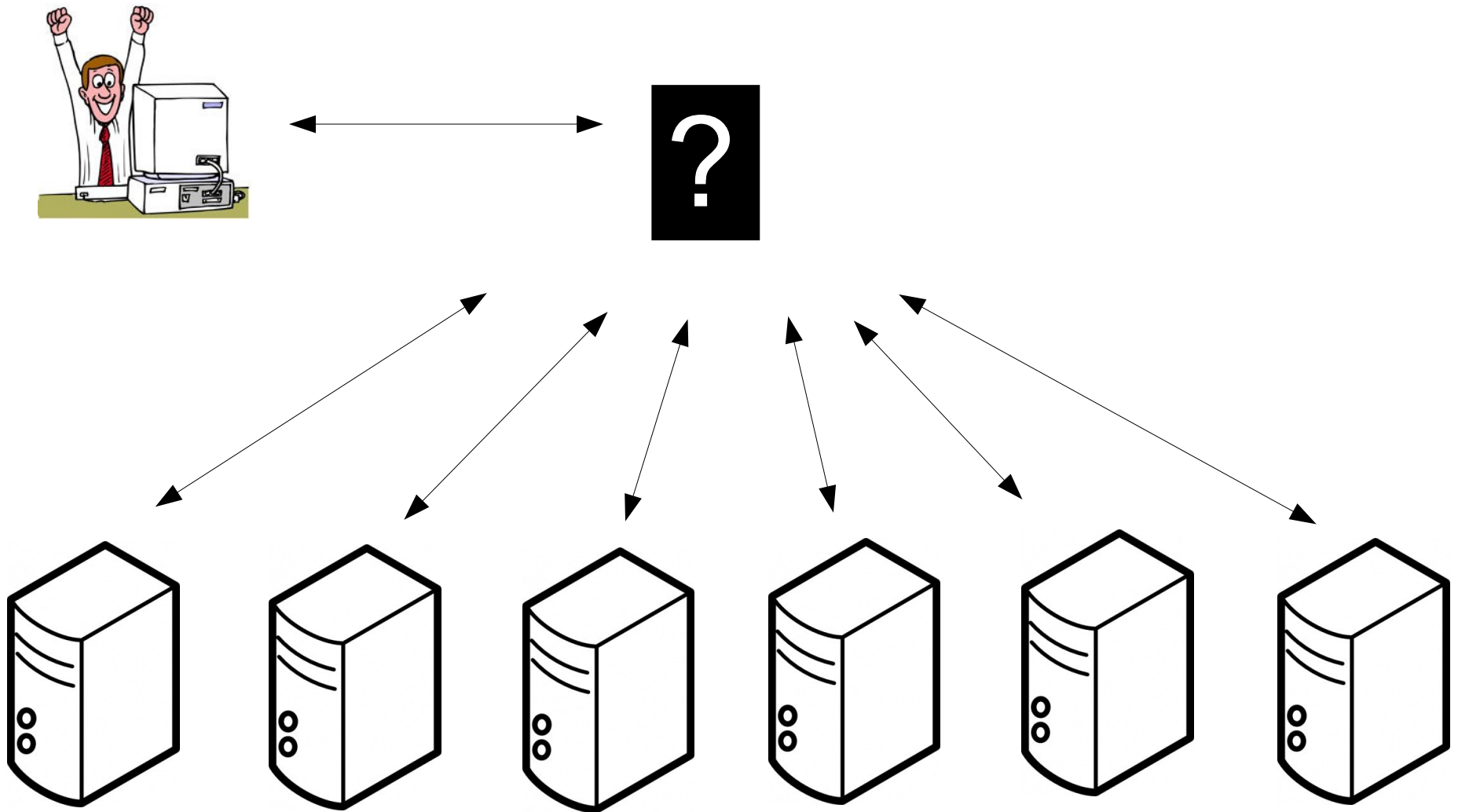
Challenge #2

the Internet identity layer
(machine-machine)

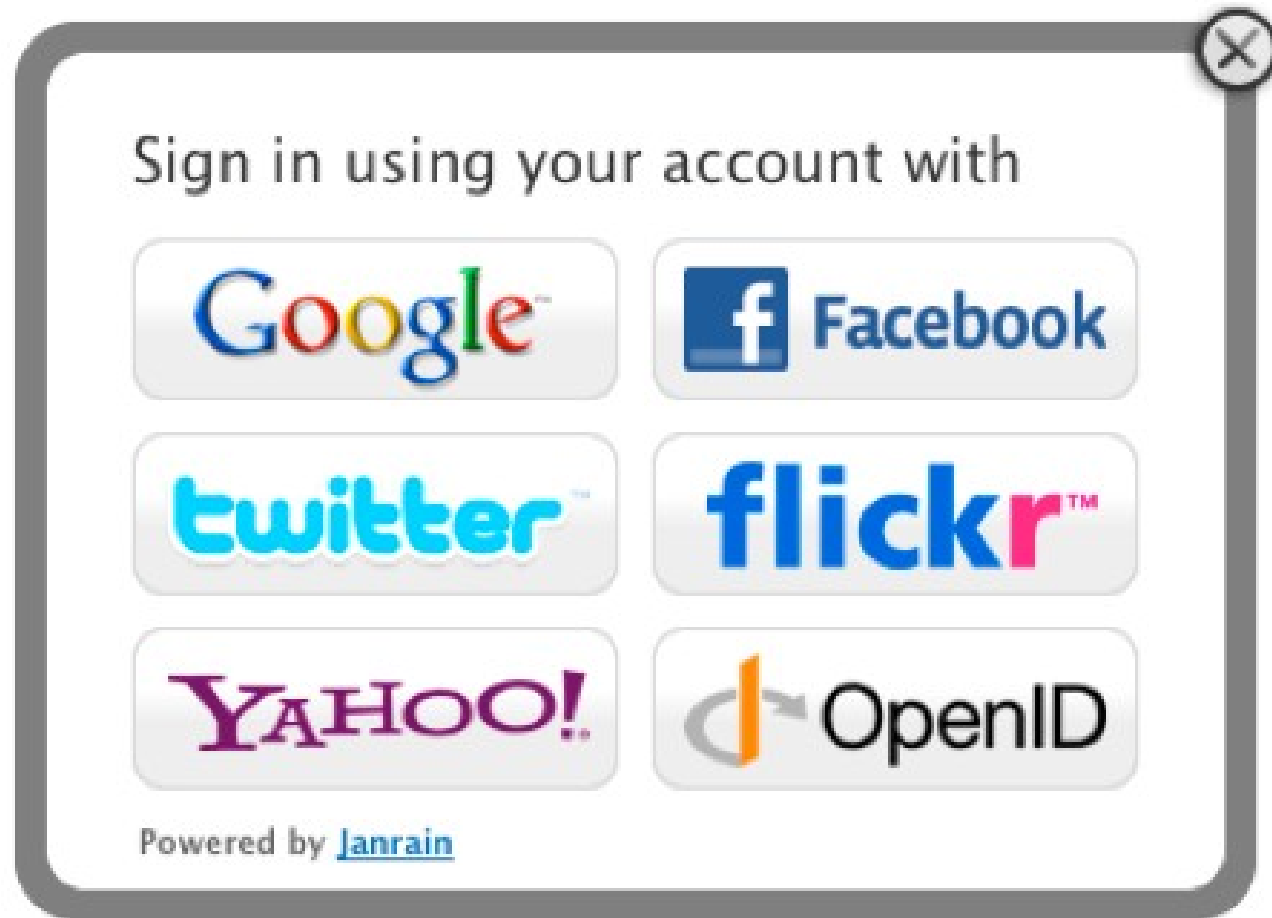
Today's Internet identity layer



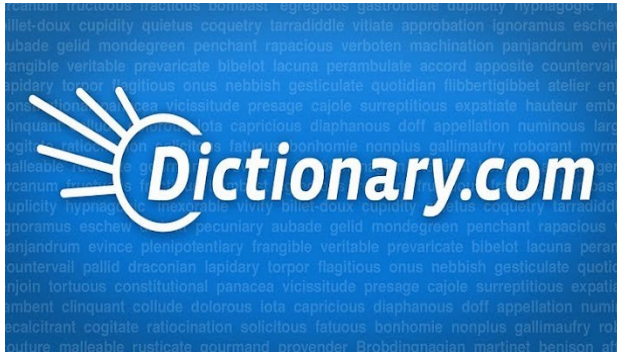
Tomorrow's Internet identity layer



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.



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...](#)

Certificate Viewer: accounts.google.com

General

Details

This certificate has been verified for the following usages:

SSL Server Certificate

Issued To

Common Name (CN)

accounts.google.com

Organization (O)

Google Inc

Organizational Unit (OU)

<Not Part Of Certificate>

Serial Number

23:85:64:29:21:93:80:1E:61:89:C4:51:A2:74:FB:F7

Issued By

Common Name (CN)

Thawte SGC CA

Organization (O)

Thawte Consulting (Pty) Ltd.

Organizational Unit (OU)

<Not Part Of Certificate>

Validity Period

Issued On

7/21/11

Expires On

7/19/13

Fingerprints

SHA-256 Fingerprint

BE 4E ED C4 E0 7D 2B 36 81 02 24 A4 CF 9A 9E F5 4D 08 4B 31 E4 8F 5D CB 6A 67 4D 79 DD A8 D5 D6

SHA-1 Fingerprint

E6 96 99 69 49 A7 17 FD D8 AF B6 B1 3A 40 39 EA 6A 73 34 44

Close

Certificate Viewer: accounts.google.com

General

Details

Certificate Hierarchy

Builtin Object Token:Verisign Class 3 Public Primary Certification Authority

Thawte SGC CA

accounts.google.com

Certificate Fields

Builtin Object Token:Verisign Class 3 Public Primary Certification Authority

Certificate

Version

Serial Number

Certificate Signature Algorithm

Field Value

Export...

Close

Whom do you trust by default?

Certificate Manager

Your Certificates Servers **Authorities** Others

You have certificates on file that identify these certificate authorities:

- ▶ Baltimore
 - Baltimore CyberTrust Root
- ▼ Buypass AS-983163327
 - Buypass Class 2 CA 1
 - Buypass Class 3 CA 1
- ▼ (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.
 - TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı
- ▼ certSIGN
 - certSIGN ROOT CA
- ▼ Chunghwa Telecom Co., Ltd.
 - ePKI Root Certification Authority
- ▼ CNNIC
 - CNNIC ROOT
- ▼ Comodo CA Limited
 - AAA Certificate Services

View... Edit... Import... Export... Delete...

Whom do you trust by default?

Certificate Manager

Your Certificates

Servers

Authorities

Others

You have certificates on file that identify these certificate authorities:

▼ Baltimore

Baltimore CyberTrust Root

▼ Buypass AS-983163327

Buypass Class 2 CA 1

Buypass Class 3 CA 1

▼ (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.

TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı

▼ certSIGN

certSIGN ROOT CA

▼ Chunghwa Telecom Co., Ltd.

ePKI Root Certification Authority

▼ CNNIC

CNNIC ROOT

▼ Comodo CA Limited

AAA Certificate Services

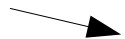
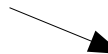
View...

Edit...

Import...

Export...

Delete...



Whom do you trust by default?

Certificate Manager

Your Certificates

Servers

Authorities

Others

You have certificates on file that identify these certificate authorities:

▼ Baltimore

Baltimore CyberTrust Root

▼ Buypass AS-983163327

Buypass Class 2 CA 1

Buypass Class 3 CA 1

▼ (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.

TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı

▼ certSIGN

certSIGN ROOT CA

▼ Chunghwa Telecom Co., Ltd.

ePKI Root Certification Authority

▼ CNNIC

CNNIC ROOT

▼ Comodo CA Limited

AAA Certificate Services

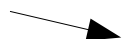
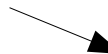
View...

Edit...

Import...

Export...

Delete...



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