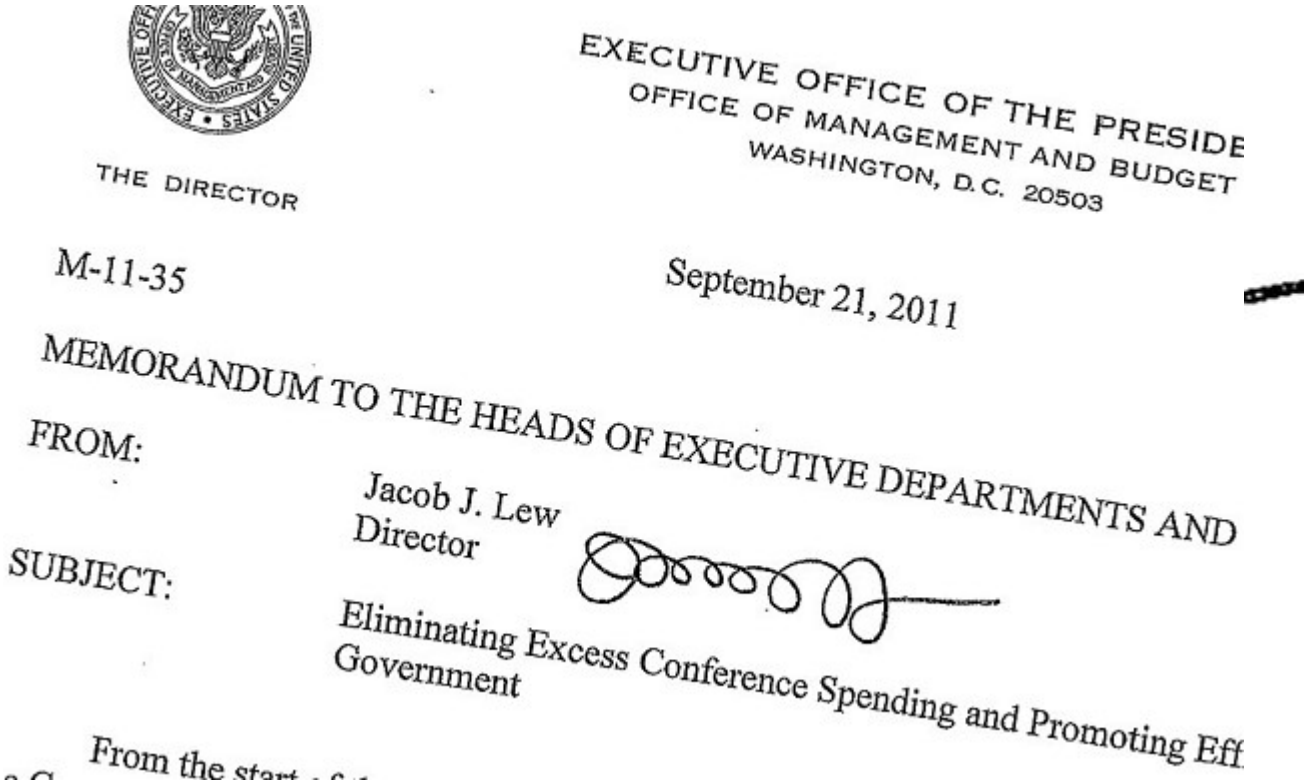
'Does anyone remember what our User ID and Password was?'

Humans – The Weakest Link?

During a recent password audit by a company, it was found that an employee was using the following password:
"MickeyMinniePlutoHueyLouieDeweyDonaldGoofySacramento"
When asked why she had such a long password, she rolled her eyes and said: "Hello! It has to be at least 8 characters and include at least one capital."

In the beginning

- **Identification by ID document/passport**
- **Authentication by signature**



EXECUTIVE OFFICE OF THE PRESIDE
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

M-11-35

September 21, 2011

MEMORANDUM TO THE HEADS OF EXECUTIVE DEPARTMENTS AND

FROM: Jacob J. Lew
Director

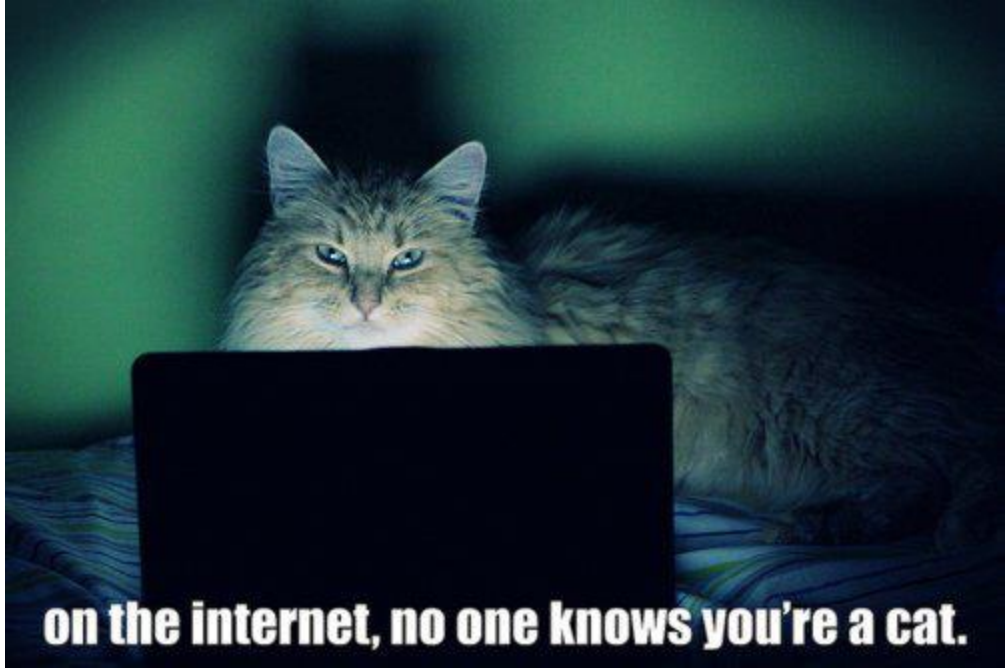
SUBJECT: Eliminating Excess Conference Spending and Promoting Eff
Government

From the start

What's the difference?

- Identification
- Authentication
- Authorisation

Identification



On the Internet, nobody knows you're a dog

Replace

Enrol

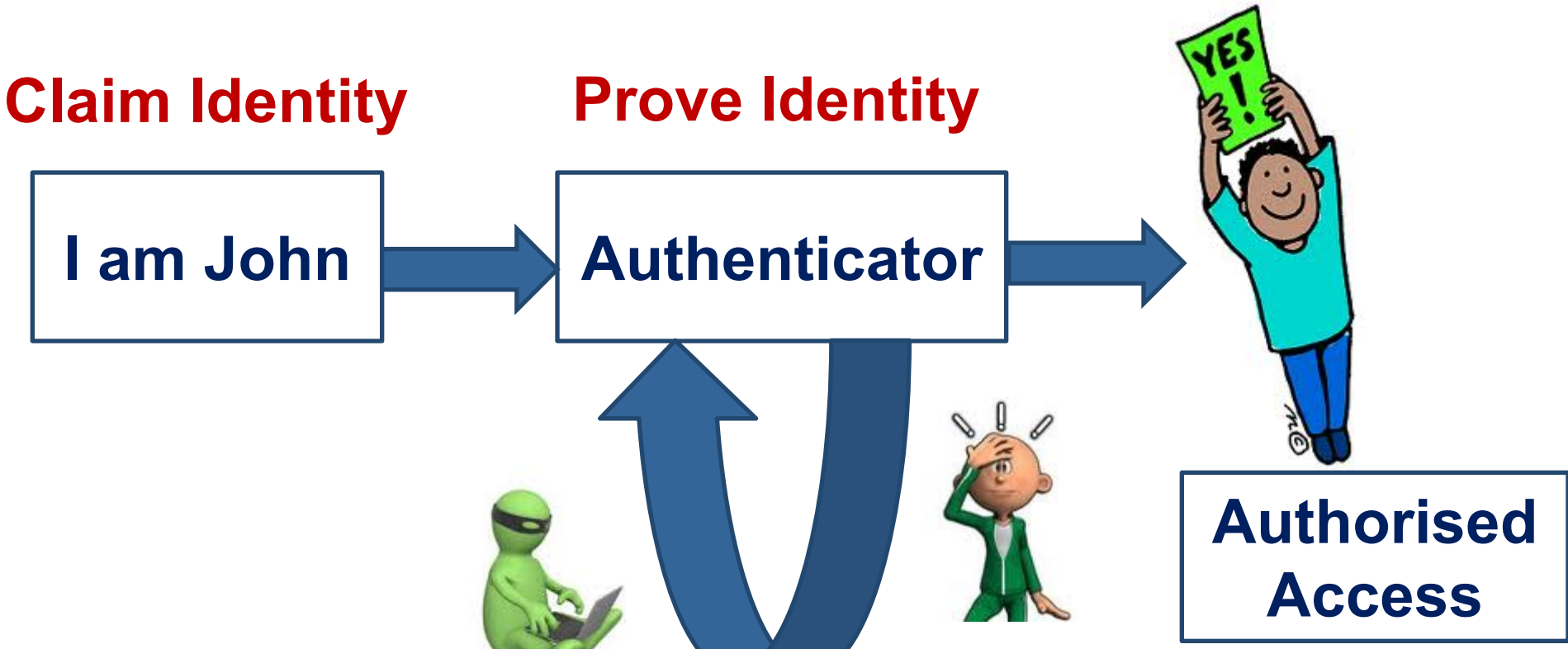
Authenticate

Close Account

Identifier

Authenticator

Stages


Claim Identity
Prove Identity
I am John
Authenticator
YES !
Authorised Access

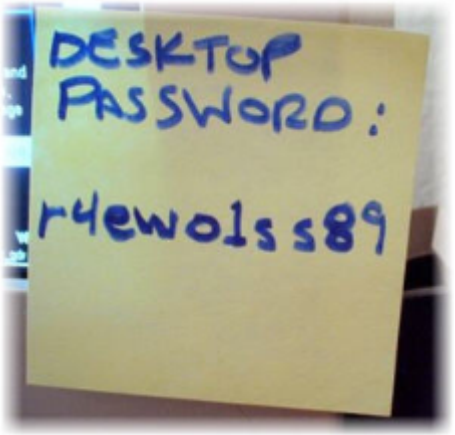
Process

Types….

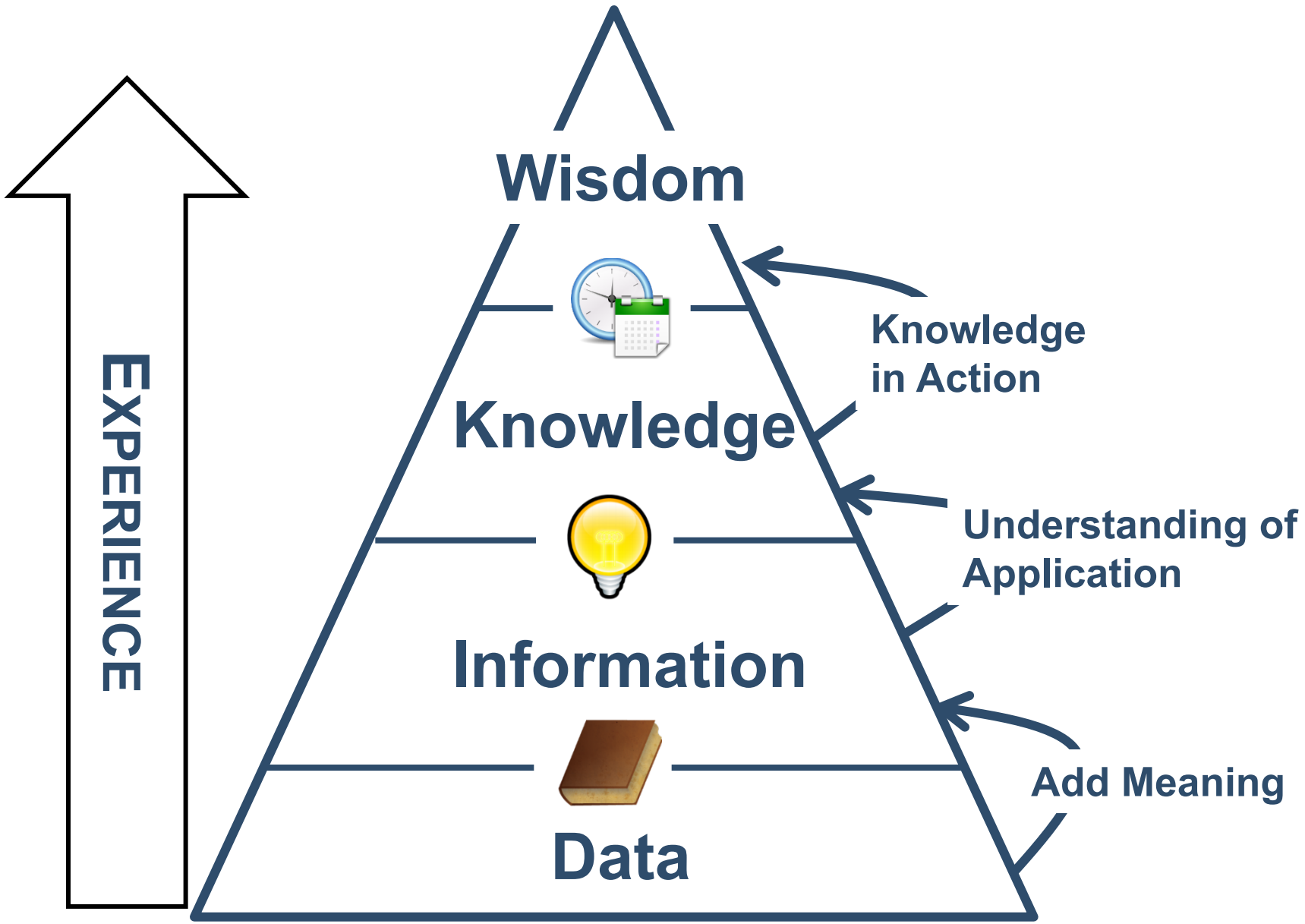
- What you know
- What you hold
- What you are

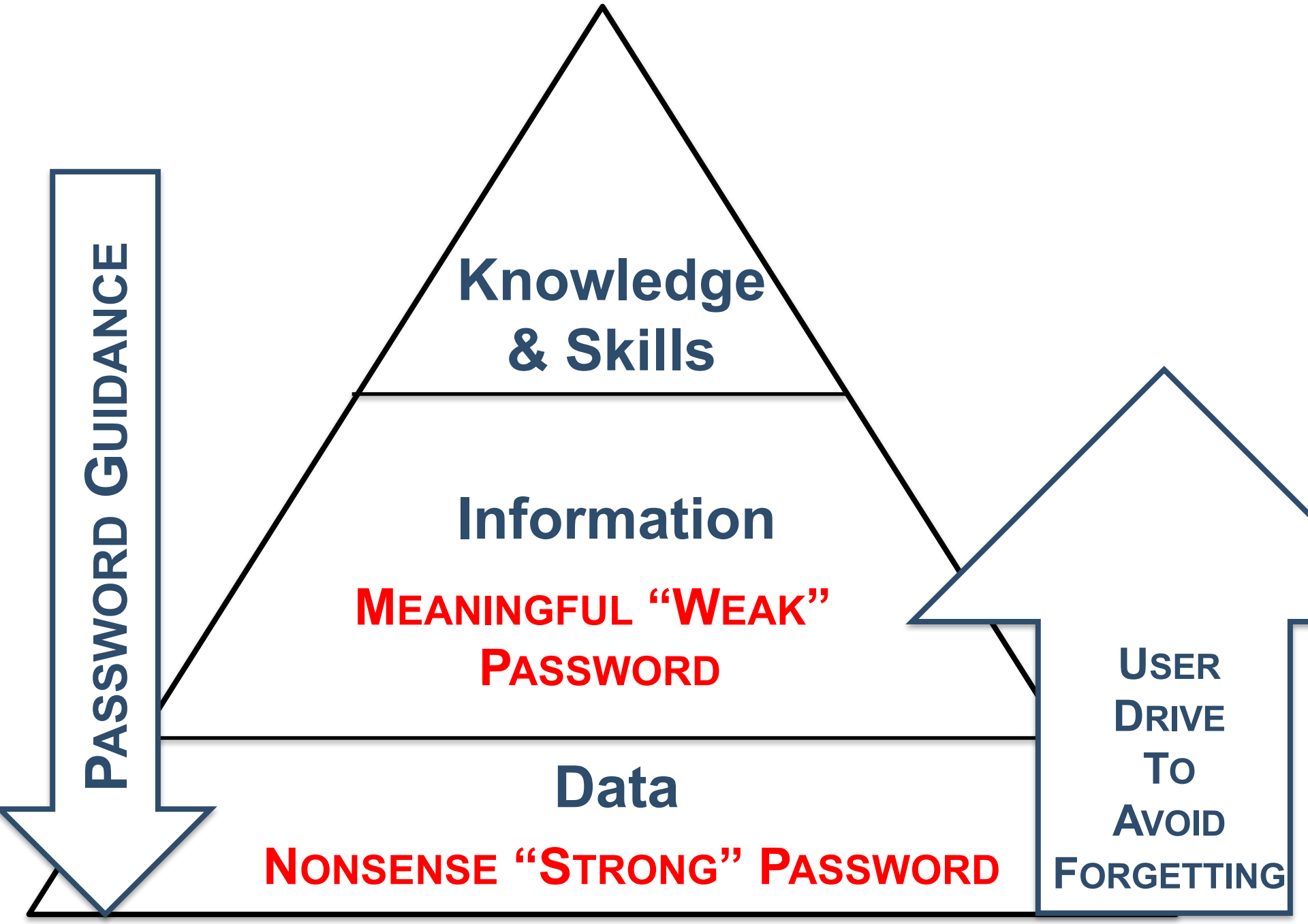
Judging an Authentication Mechanism (Security)

- Memorability
- Guessability
- Observability
- Recordability



What you Know (DIKW)



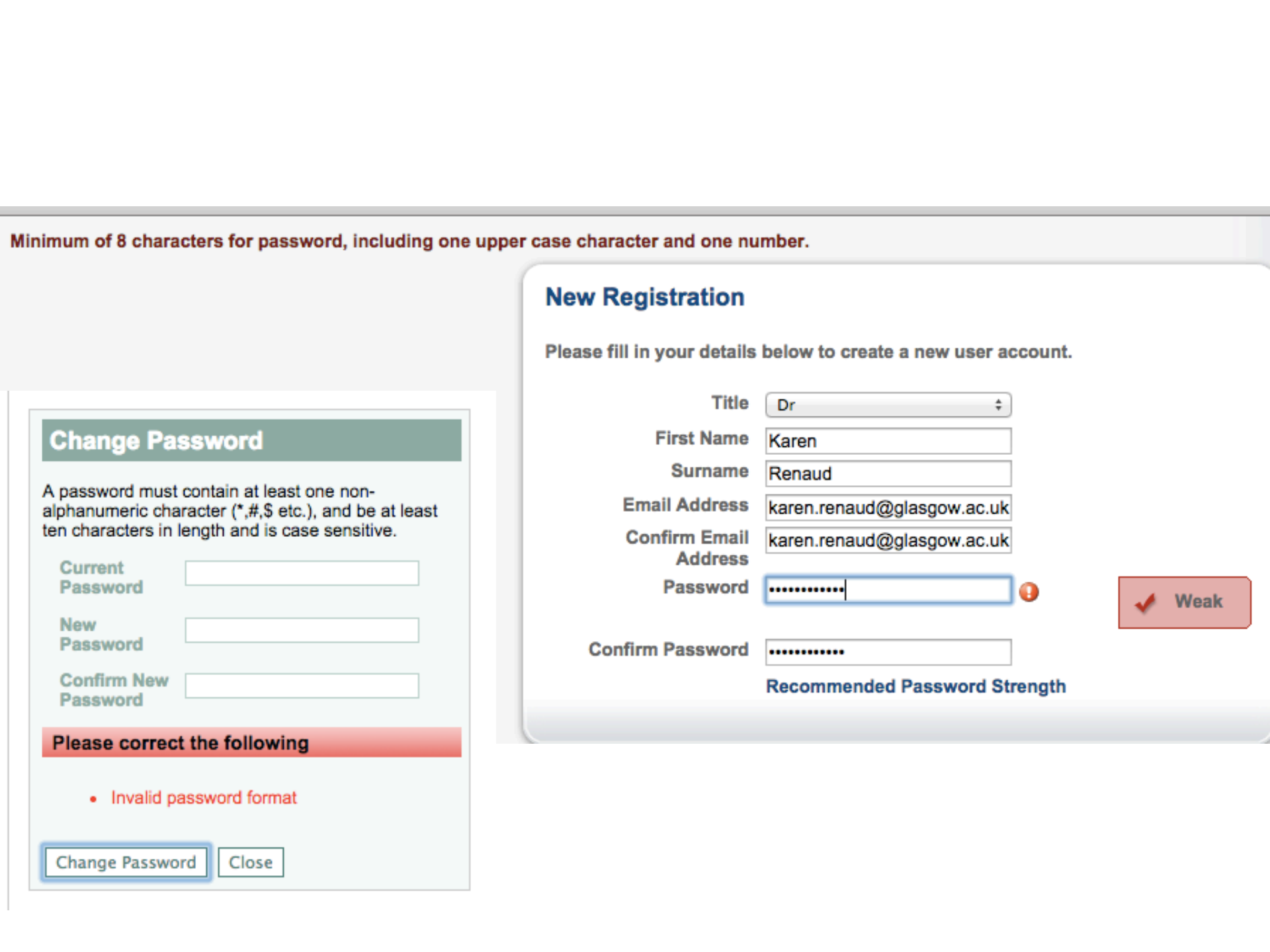

Knowledge & Skills
Information
MEANINGFUL "WEAK" PASSWORD
Data
NONSENSE "STRONG" PASSWORD
PASSWORD GUIDANCE
USER DRIVE TO AVOID FORGETTING

Problems with "What You Know"

- Human Aspects
  - Hard to remember
  - Hard to create
  - Take time to type in
- Security:
  - Guessability
  - Observability
  - Recordability

More Problems

- No agreement as to “strong password” requirements
- They don’t tell users much, and they display instructions in the wrong place


Minimum of 8 characters for password, including one upper case character and one number.
New Registration
Please fill in your details below to create a new user account.
Title
Dr
First Name
Karen
Surname
Renaud
Email Address
karen.renaud@glasgow.ac.uk
Confirm Email Address
karen.renaud@glasgow.ac.uk
Password
Weak
Confirm Password
Recommended Password Strength
Change Password
A password must contain at least one non-alphanumeric character (*,#,$ etc.), and be at least ten characters in length and is case sensitive.
Current Password
New Password
Confirm New Password
Please correct the following
Invalid password format
Change Password
Close

Memorability

FACT: People can't remember all their passwords

- How do they cope?
  - Write them down
  - Ask others to share
  - Use other passwords that have been written down
  - Use the same password for multiple systems
  - Use a variation of their own name or the system name
  - Use "common" passwords
  - Use weak passwords


https://arxiv.org/edit-user/index.php
Would you like to remember the password for "karen.renaud" on arxiv.org?
Remember Password
(step 1 of 2)
You should only register with arXiv once: arXiv now connects papers that you hav
which will cause confusion and wasted time for both you and us.
If you remember your password but would like to change your e-mail address, you c
at your old address, you can easily recover your password. If you have forgotten you
Errors were found in this form. You must correct errors marked with to proceed
correctly.
E-Mail:
You must be able to receive mail at this address to register. We take strong measure
address that belongs to someone else: if we discover that you've done so, we will su
karen.renaud@glasgow.ac.uk

You Have Exactly Three Passwords, Don't You?

An independent analysis of passwords leaked after Sony was hacked show why most of us need to stop being lazy about protecting our information.

By Jill Duffy | June 7, 2011 03:22pm EST | 31 Comments | Email | Print

You have exactly three passwords, don't you? The first is one you use for all the logins that you don't think house anything worth stealing. You use it when you are signing up for a Web site that you might not visit ever again. It's the default password you deploy when you're required to "create a free account" to read an online newspaper or RSVP to an e-invitation.

The second one is medium security. It's probably fewer than eight characters long. It might be alpha-only or alpha-numeric, but does not contain special characters. You probably use this same password for both email and Facebook. And it's possible you don't have a medium security password at all, so let's skip to the third.

The third password is what you use for your bank accounts—all of them. Or worse, you have one password that you use for everything.

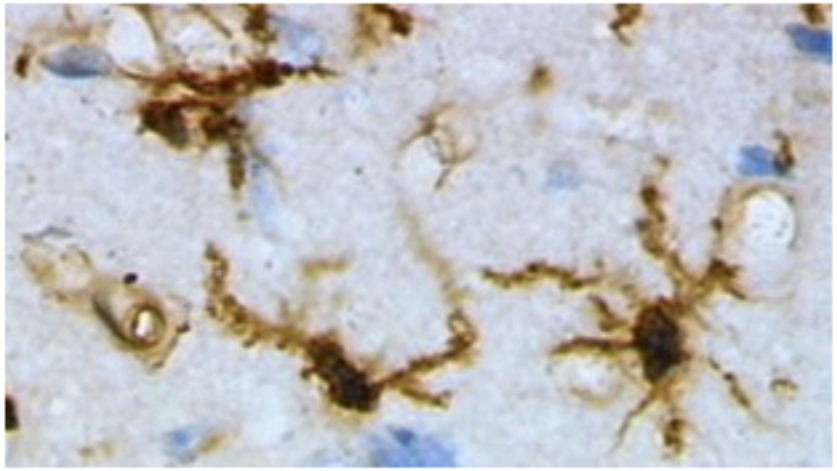
David Miranda

- Was also holding the password to an encrypted file written on a piece of paper, the government has disclosed.
- "Much of the material is encrypted. However, among the unencrypted documents ... was a piece of paper that included the password for decrypting one of the encrypted files on the external hard drive recovered from the claimant."

Pruning Synapses Improves Brain Connections

Without microglia to pluck off unwanted synapses in early life, mouse brains develop with weaker connections, leading to altered social behavior.

By Ed Yong | February 2, 2014

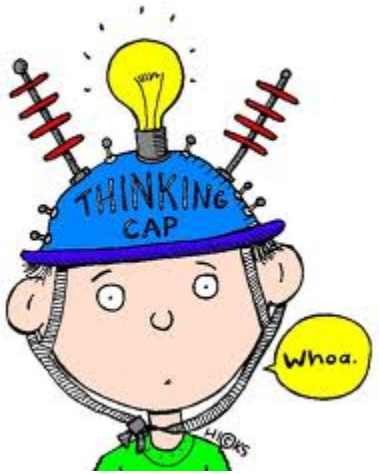


Rat microglia
WIKIMEDIA, GRZEGORZ WICHER

As the brain matures, a group of resident immune cells called microglia crawl between the growing neurons and engulf invading microbes or damaged cells. They are also thought to pluck off some of the synapses that connect different neurons.

This destructive act is important for the developing brain. The microglia prune away weak or unwanted connections, allowing more productive ones to become stronger. Without this "synaptic pruning," a team of researchers led by Cornelius Gross at the European Molecular Biology Laboratory has shown that mice grow up with weaker connections between different parts of their brains.

Guessability



Who are you protecting yourself against when you choose a password?

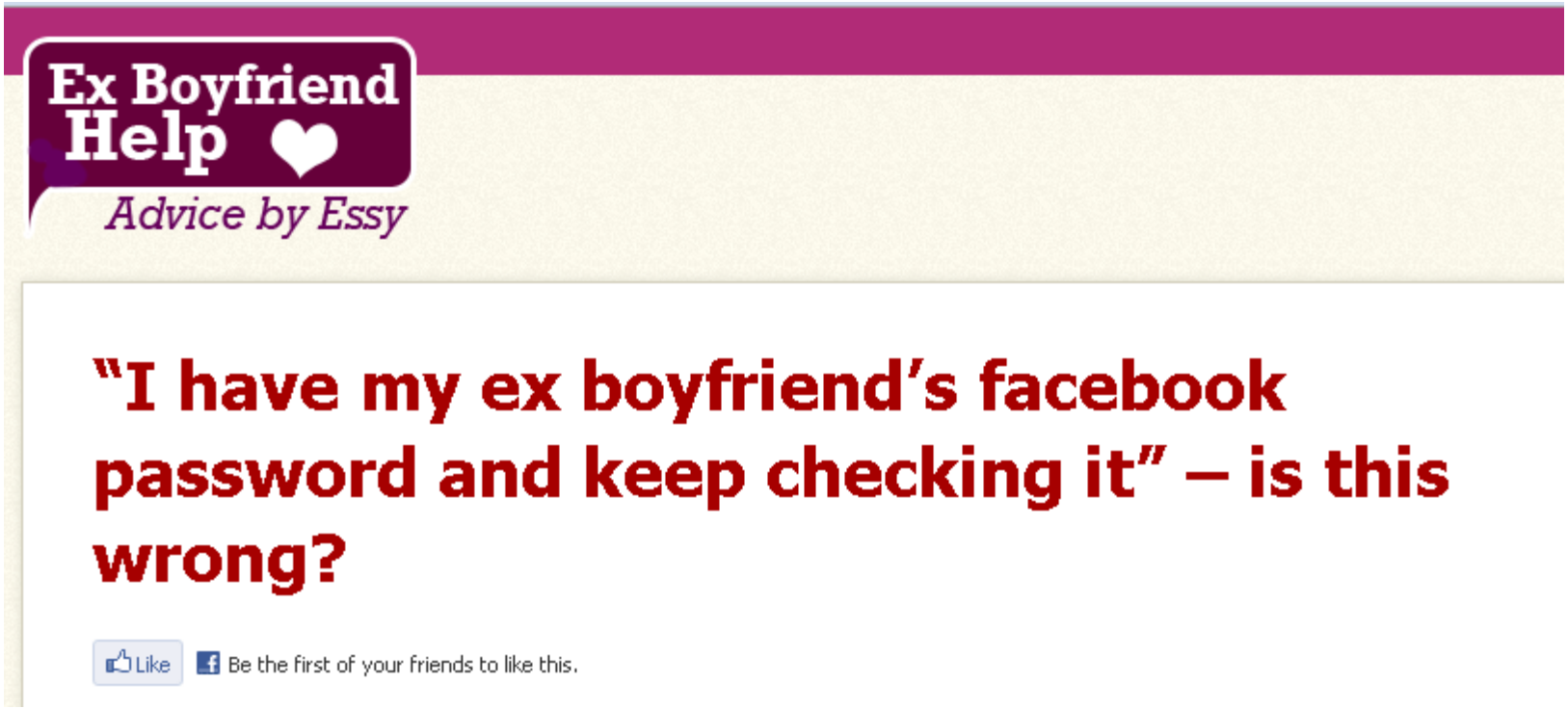
- Hacker?
- Ex-partner?
- Family member?

Ask an Expert

Ask a Question
Questions by Tag Cloud
Questions by Topic
About Website
Compulsive Lying
Dealing With Suspicion
Discovering Deception

My girlfriend is snooping on me

I found out my girlfriend is logging on to me email accounts and is reading my private emails, also checking to see who calls on cell. I'm so angry I don't event want to talk to her. What should I do?



Ex Boyfriend Help

Advice by Essy

"I have my ex boyfriend's facebook password and keep checking it" – is this wrong?

Like Be the first of your friends to like this.

answerbag
Every Question Deserves a Great Answer

HOME CATEGORIES QUESTIONS FORUMS BLOG Google™ Cu

Home / Questions / Relationship Advice / Love In Relationships

QUESTION

by Anonymous on February 19th, 2007

Help answer this question below.

I know my ex-boyfriend's e-mail password. I found it out by trying a few different words. I'm not suspicious of anything I just can't stop checking it! I want to stop! What can I do? Simply "just stopping" isn't working!I want him 2 change his password!

Answer Question

March 1, 2005, 12:00 AM

How To Break Into Your Girlfriend's E-mail (And Why You Probably Shouldn't)

To be or not to be a spy.

PORN AND SELF-GOOGLING are overrated. The most addictive thing your PC has to offer is your girlfriend's e-mail. Even better is your ex's. I know firsthand. I've got two exes blissfully blind to the fact that I start my mornings with a cup of coffee and a peek at their in-boxes. It's the ultimate voyeuristic thrill and the ultimate betrayal. And it's all too easy. Paranoid about the computer vice squad in human resources, most of us use Web-based e-mail (Yahoo, Hotmail, et cetera) for our most personal correspondence. And as luck would have it, it's Web mail that's easiest to crack.

Think you need an MIT degree to hack a password? Not so much. In most cases, you need only her cat's name. You might also try password. If she's really crafty, she'll use a zip code, phone number, or parent's name. Date someone more creative? Try Googling "Yahoo mail" + "password crack" for access to free or inexpensive hacker software that'll run through millions of variations. "The fact is, an unfortunate number of people still use their own first name as their passwords," says Toby Weir-Jones of Counterpane Internet Security. Once in, you'll want to familiarize yourself with Yahoo's "mark as unread" feature, a handy option that lets you read her latest mail and cover your tracks. You'll also want to exercise her "save sent items" option; outgoing mail is often home to the best bits, although the real gold mine might just be

Denard Gets Hacked

By Chris Dart

OH SNAP!

Michigan quarterback Denard Robinson had his Twitter accound hacked by his girlfriend — who I assume is now his ex-girlfriend — and it was nothing short of ugly. Apparently there's been some infidelity in the relationship, and the woman who wanted to be Mrs. Robinson wanted to let all 27,000 of Robinson's followers know about his cheatin' heart, and put a couple of other ladies on blast, as well.

I feel like there are two lessons to be learned here:

1) Young ladies, don't date FBS football players. They're going to cheat on you. It's almost a given.

2) Gentlemen, particularly those of you who are elite-level athletes, stop using your dog's name as your password for everything. That's way too easy to figure out. At least replace an "e" with a "3" or something.

The Telegraph

Phone Hacking

Hugh Grant: 'Half a dozen newspapers were phone hacking'

At least half a dozen newspapers will be implicated in the phone hac Hugh Grant said tonight.

The News of the World is based at News International's London headquarters in Wapping Photo: EPA

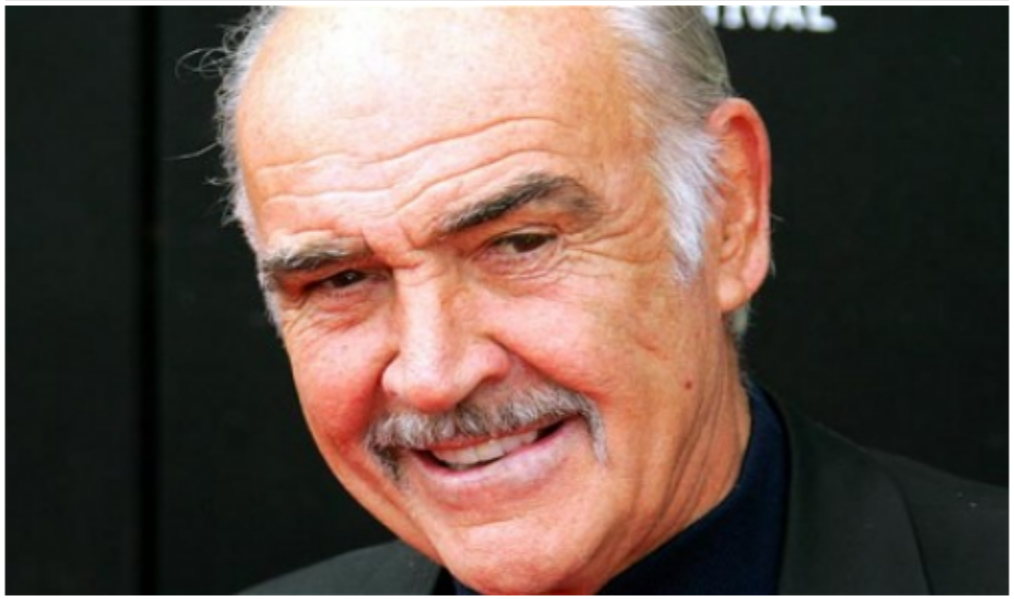
By Christopher Hope and Holly Watt
6:04PM BST 04 Oct 2011

The Hollywood actor was speaking ahead of his meeting with Prime Minister David Cameron at the Tory party conference.

The meeting is the first since the scandal broke over the summer, forcing Mr Cameron to order a judge-led inquiry into the affair by Lord Justice Leveson.

Sean Connery's phone hacked, says biographer

The pressure on Alex Salmond over his close relationship with Rupert Murdoch has increased after it emerged that police have warned Sir Sean Connery his mobile phone was repeatedly hacked.



His biographer has said Sir Sean Connery's phone was hacked around ten times Photo: Jack Photography Ltd/Rex Features

By Simon Johnson, Scottish Political Editor
6:03PM BST 30 May 2012

The Oscar-winning actor, a friend of the First Minister and the SNP's most high-profile supporter, has been informed that the Murdoch media empire illegally accessed his voicemail messages around ten times.

Murray Grigor, Sir Sean's biographer, said the James Bond actor told him about the hacking on Tuesday this week while in Switzerland.

It is understood his name appears in the records of Glenn Mulcaire, the private detective employed by the News of the World and later jailed for hacking.

Enlarge this image

Is 0$gUll45i9 unhackable? Turns out long, common-word passwords are safer

DAKSHANA BASCARAMURTY
Globe and Mail Blog
Posted on Wednesday, August 10, 2011 5:55PM EDT

If you were smart you would've tattooed your password on your arm *before* you went on that three-week vacation to Cuba. Now you're back at your desk, trying to remember it.

Was it 0$gUll45iB? Or 0$gUll45i9? Or maybe 4hhRR9 per cent02*? No, that's your web banking password. Great, now you've tried and failed enough times that the system has locked you out.

The longer the password, the longer it takes to hack using the brute force strategy. That means a memorable string of random (but common) words offers more protection than an eight-character jumble of meaningless characters, symbols and numbers.

Internet and security wizard Steve Gibson explains this as a password haystack – the bigger the haystack (or longer the password), the harder to find the needle (in this case, randomly guess the password).

"Once an exhaustive password search begins, the most important factor is password length," he writes.

Try a padded password. A string of periods or zeros surrounding a common word could make your password much stronger, he says.

Philips hacked, plaintext passwords revealed as R00tbeer gang strikes again

by Paul Ducklin on August 21, 2012 | Comments (6)
FILED UNDER: Data loss, Featured, Law & order, Vulnerability

Sadly, `r00tbeer` has done it again, this time attacking Dutch technology giant Philips and digging out data from a range of Philips-branded sites.

A few small SQL databases have been leaked in full, divulging a few thousand records.

These include, amongst other things, names, telephone numbers, addresses, passwords and password hashes.

That's right: passwords. One of the databases, fortunately containing fewer than 400 records, has passwords stored in plain text.

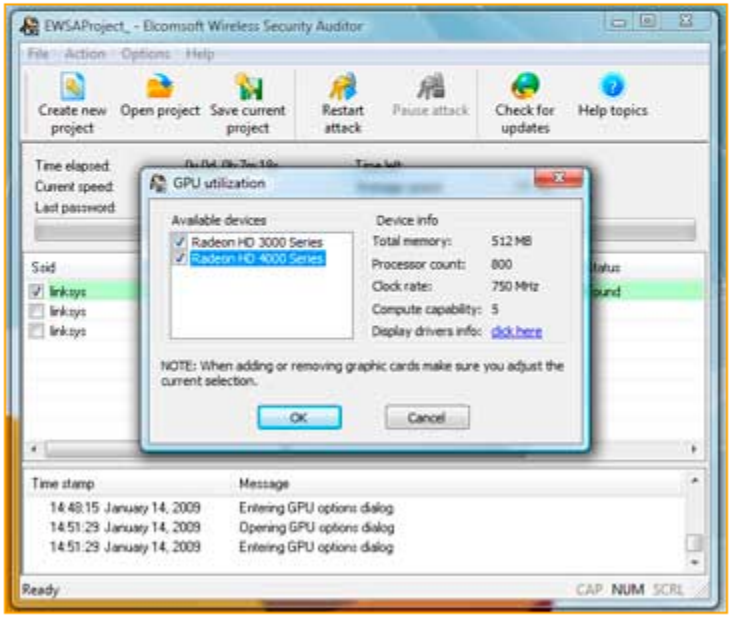
It's hard to know just how much an attacker might be able to do with these passwords, but are are three massive problems here:

1. **The passwords shouldn't have been accessible in the first place.**
2. **The passwords shouldn't have been stored in plain text.**
3. **The passwords were almost without exception poorly chosen.**

GPUs Used to Successfully Crack Wi-Fi Passwords

Thursday, January 15, 2009 - by Daniel A. Begun

Because of the computational power of today's GPUs, GPUs are starting to be harnessed more and more to help out CPUs with some hardcore number crunching. That is the concept behind Nvidia's CUDA, ATI's Stream, and Apple's OpenCL frameworks. There aren't many apps available yet that take advantage of these relatively new technologies, but the ranks are slowly growing. The latest GPU-assisted app to come available is one designed for IT managers to make sure their wireless networks are secure--and inevitably for hackers to try to break into wireless networks.



Russian-based ElcomSoft has just released ElcomSoft Wireless Security Auditor 1.0, which can take advantage of both Nvidia and ATI GPUs. ElcomSoft claims that the software uses a "*proprietary GPU acceleration technology*," which implies that neither CUDA, Stream, nor OpenCL are being utilized in this instance. At its heart, what ElcomSoft Wireless Security Auditor does is perform brute-force dictionary attacks of WPA and WPA2 passwords. If an access point is set up using a fairly insecure password that is based on dictionary words, there is a higher likelihood that a password can be guessed. Brute force attacks that send random dictionary words to an access point can eventually successfully guess the password, if given enough time--the more computational power behind it, the faster the software can send passwords attempts and possibly guess the password. *

Observability

Prince William & Passwords….

EUROPEAN ASSOCIATION FOR VISUAL DATA SECURITY

SECURE

Username Pass

Tel: (+44) 20 7839 2140

Home | About Us | Visual Data Security | News | Our Members | Contact Us

RAF's Prince William security lapse shows need for visual data security procedures

The publication of photographs of Prince William working on a computer with uncensored information on the screen fully visible, clearly demonstrates that visual data security is now the Achilles' Heel of data security.

Organisations spend millions each year ensuring the physical security of their data, yet little is done to promote awareness of the risks posed by a visual data security breach, the ease with which one can occur and the substantial threat that they pose to organisations and individuals.

The European Association for Visual Data Security's Information Security Expert Brian Honan commented: "incidents like this highlight the urgent need for organisations in both the public and private sector to take the threat posed by visual data security breach seriously – especially those that deal with national security or commercially sensitive information."

"The growing use of high resolution digital cameras", he continued, "ensures that sensitive information on display can be easily and effectively captured and misused".


TAXI
Thereifixedit.com


CAMERA LENS
ON SIDE OF
BAG

Actually....

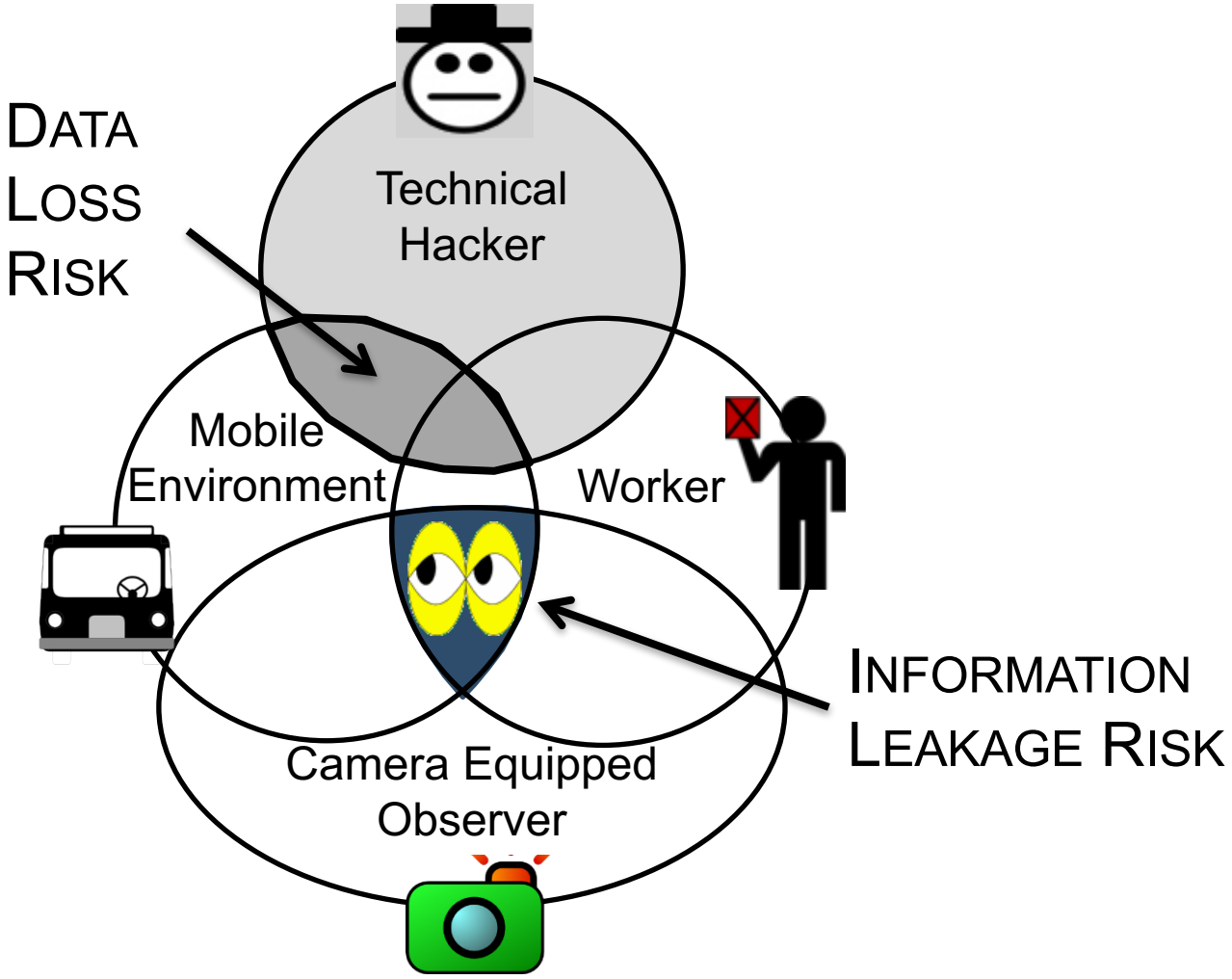
- The stronger the password, the easier it is to see what the password is if you watch someone
- Keyloggers are easy to install
- The sounds of your typing leak your password

"Three students at UC-Berkley used a 10 minute recording of a keyboard to recover 96% of the characters typed during the session. The article details that their methods did not require a 'training text' in order to calibrate the conversion algorithm as has been used previously. The research paper [PDF] notes that '90% of 5-character random passwords using only letters can be generated in fewer than 20 attempts by an adversary; 80% of 10-character passwords can be generated in fewer than 75 attempts.'"

SpiPhone: How someone could use an iPhone to find out what you are typing on your computer

- it can decipher vibrations to record what is being typed on a nearby computer keyboard
- Working with dictionaries comprising about 58,000 words, the system reached word-recovery rates as high as 80 percent.

Working on the Move



Recordability


New User? Register | Sign In | Help
YAHOO! ANSWERS
Search
HOME
BROWSE CATEGORIES
ABOUT
Ask
What would you like to ask?
Continue
Answ
Why Yahoo! Answers? Share your knowledge, help others and be an e
What are you looking for?
Search Y! Answers
shady
I gave my ex girlfriend my password for my yahoo and now i cant get the password right or my security answers?
1 year ago
OUCH!

@MarkDavidson Fires Twitter Ghostwriter But Never Changed Password, Guess What Happens Next...

By Mariel Loveland | September 22, 2011 12:36 pm EST | Comments (0)

Image credit: Flickr

Sometimes your attempts at reaching fans through social media completely fail — especially if you fired the person who handles your accounts but forgot to change the passwords.

Mark Davidson, a social marketing and communications strategist, learned that angry ex-employees can completely ruin your credibility in one of the most hilarious Twitter tirades I've seen.

TechCrunch first spotted the tweet about Mark Davidson's account. Apparently, Davidson had hired 3 ghostwriters to handle his Twitter account. With a little over 56,000 followers, it's hard to see why Davidson needed to hire anyone to handle his Twitter account when he only posts a couple of tweets a day on average. Unfortunately, Davidson didn't change his password, so the angry ex-ghostwriter decided to flame his old boss via his boss' Twitter account.

The ex-employee started by revealing the truth about Davidson — he never wrote his own tweets. Lots of people don't write their own tweets, so there isn't much of a shock there.

TODAY @ PCWORLD

Hackers, IT Pros Share Personal Information Online, Study Finds

By Christina DesMarais, PCWorld Oct 15, 2011 7:58 AM

Hackers apparently can be just as careless as their victims.

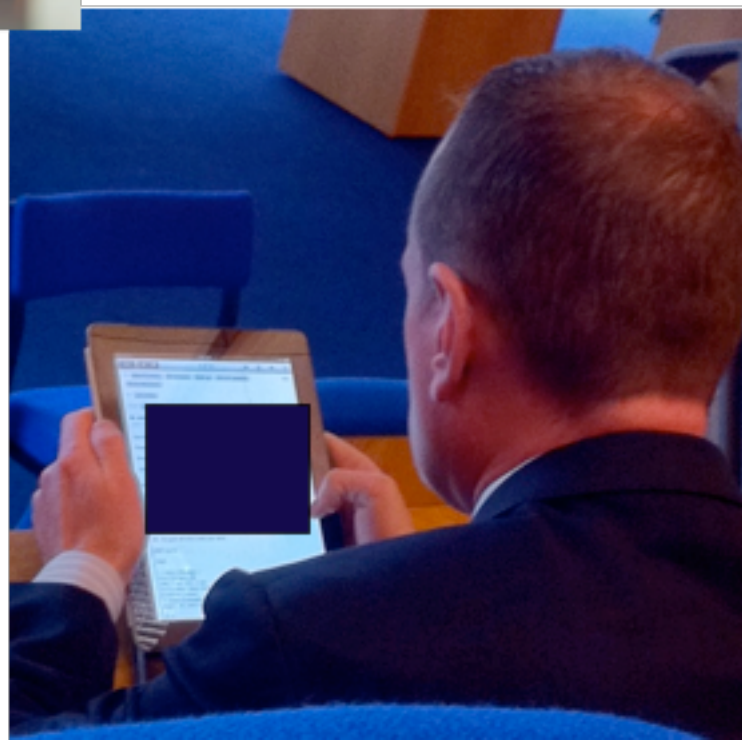
A new study finds that people with technical backgrounds are very inclined to disclose sensitive information like addresses and passwords to strangers they meet online, even though they should know better.

Antivirus software company BitDefender recently published the results from the study.

The researcher found that 75 percent of those contacted disclosed personal information such as addresses, phone numbers, information about their children and their parents' names. Nearly all of those contacted also offered up a description of their password and 13 percent of IT professionals contacted actually disclosed various passwords to online accounts.

Datcu makes the point that social networks, forums and online chat rooms "create ideal worlds, in which users have the ability to transform themselves into very attractive people or very communicative ones, and in which everybody can confide in everybody and be everybody's friend."

For more information about the study, visit Virus Bulletin.



49 BRILLIANT USES FOR YOUR SMARTPHONE'S CAMERA

Beijing 2008

So what passwords are people choosing?

Common Passwords

PINS

- How many are there?
  - 10 000
- People can define their own. Which ones do they use?

DataGenetics

Home | Blog | About Us | Work we do | Content | Contact Us

PIN analysis

A good friend of mine, Ian, recently forwarded me an internet joke. The headline was something like:

"All credit card PIN numbers in the World leaked"

The body of the message simply said 0000 0001 0002 0003 0004 ...

What is the least common PIN number?

There are 10,000 possible combinations that the digits 0-9 can be arranged to form a 4-digit pin code. Out of these ten thousand codes, which is the least commonly used?

Which of these pin codes is the least predictable?

Which of these pin codes is the most predictable?

If you were given the task of trying to crack a random credit card by repeatedly trying PIN codes, what order should you try guessing to maximize your chances of selecting the correct number in the shortest time?

If you had to make predication about what the least commonly used 4-digit PIN is, what would be your guess?

This tangentially relates to the XKCD cartoon. In Randall's cartoon, the perpetrator's plan backfired because his selected license plate was so unique that it was very memorable. What is the least memorable license plate? Ask any spy you know (snigger) what the best way to blend into a crowd is. Their answer will be not stand out, to appear "normal", and not be notable in any way.

People are notoriously bad at generating random passwords. I hope this article will scare you into being a little more careful in how you select your next PIN number.

Are you curious about what the least commonly used PIN number might be?

How about the most popular?

Read on ...

The most popular password is 1234 …

… it's *staggering* how popular this password appears to be. Utterly *staggering* at the lack of imagination …

… nearly 11% of the 3.4 million passwords are 1234 *!!!*

The next most popular 4-digit PIN in use is 1111 with over 6% of passwords being this.

In third place is 0000 with almost 2%.

A table of the top 20 found passwords in shown at the right. A staggering 26.83% of all passwords could be guessed by attempting these 20 combinations!

(Statistically, with 10,000 possible combination, if passwords were uniformly randomly distributed, we would expect the these twenty passwords to account for just 0.2% of the total, not the 26.83% encountered)

Looking more closely at the top few records, all the usual suspects are present 1111 2222 3333 … 9999 as well as 1212 and (snigger) 6969 .

It's not a surprise to see patterns like 1122 and 1313 occurring high up in the list, nor 4321 or 1010 .

2001 makes an appearance at #19. 1984 follows not far behind in position #26, and James Bond fans may be interested to know 0007 is found between the two of them in position #23 (another variant 0070 follows not much further behind at #28).

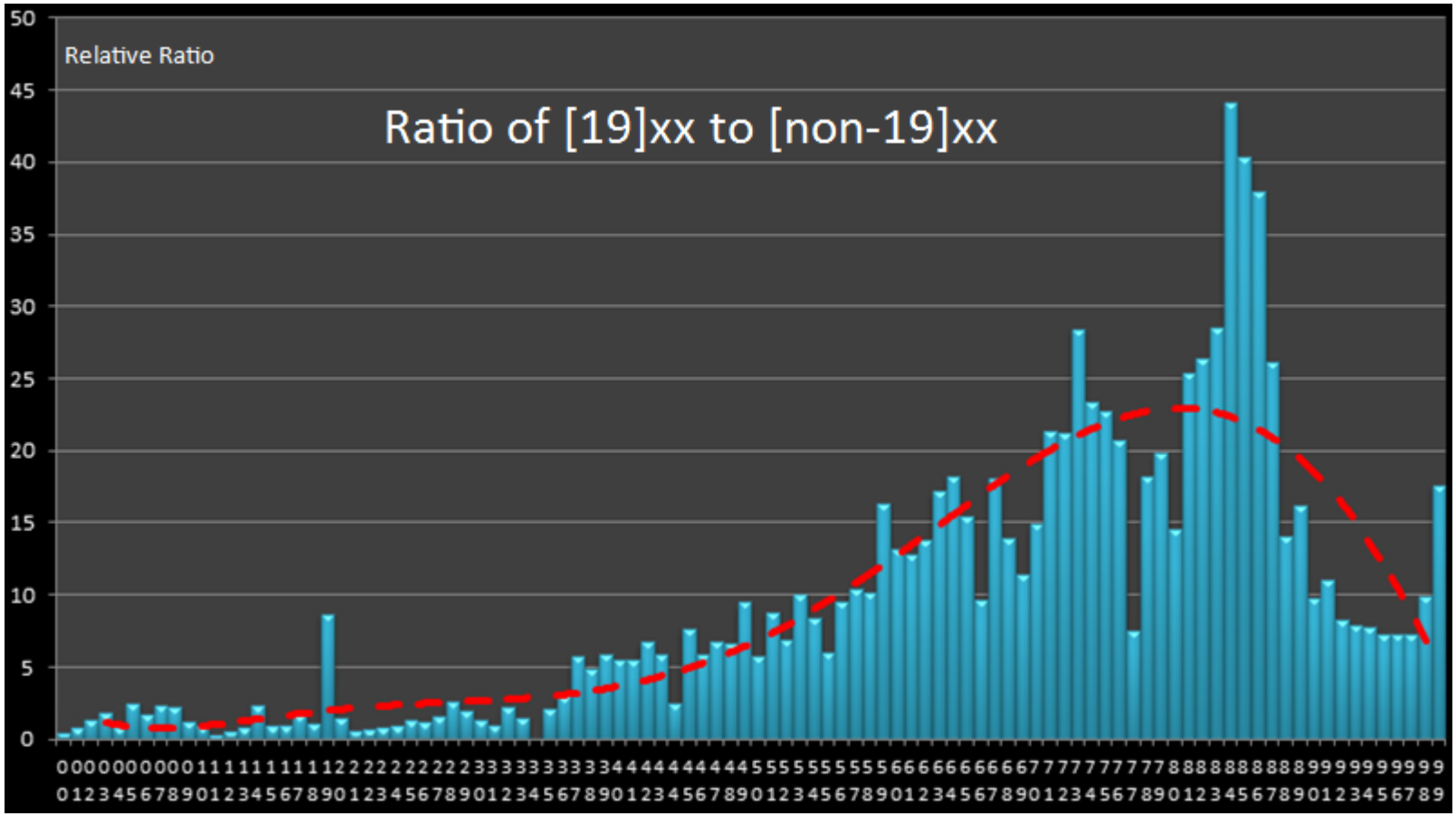
	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%
#20	1010	0.285%

The first "puzzling" password I encountered was **2580** in position #22. What is the significance of these digits? Why should so many people select this code to make it appear so high up the list?

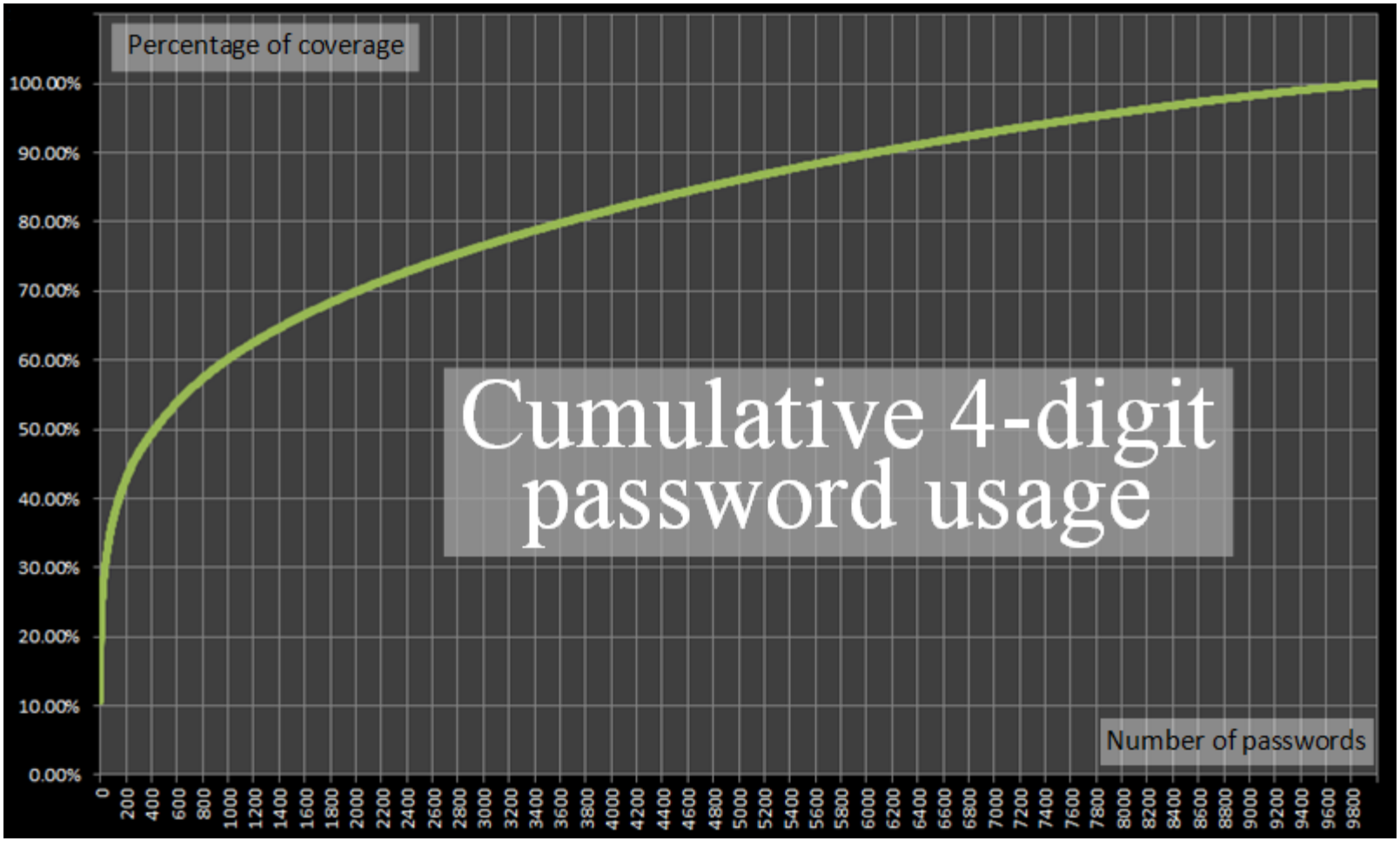
Then I realized that **2580** is a straight down the middle of a telephone keypad!

(Interestingly, this is very compelling evidence confirming the hypothesis that a 4-digit password list is a great proxy for a PIN number database. If you look at the numeric keypad on a PC-keyboard you'll see that 2580 is slightly more awkward to type on the PC than a phone because the order of keys on a keyboard is the inverted. Cash machines and other terminals that take credit cards use a phone style numeric pads. It appears that many people have an easy to type/remember PIN number for their credit card and are re-using the same four digits for their online passwords, where the *"straight down the middle"* mnemonic no longer applies).

(Another fascinating piece of trivia is that people seem to prefer even numbers over odd, and codes like **2468** occur higher than a odd number equivalent, such as **1357**).


Relative Ratio
Ratio of [19]xx to [non-19]xx
50
45
40
35
30
25
20
15
10
5
0
0000000000111111111122222222223333333333444444444455555555556666666666777777777788888888899999999990
0123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789

Statistically, *one third* of all codes can be guessed by trying just 61 distinct combinations!



Bottom of the pile

OK, we've investigated most frequently used PINS and found they tend to be predictable and easy to remember, let's turn for a second to the bottom of the pile.

What are the least "interesting" (least used) PINS?

In my dataset the answer is 8068 with just 25 occurrences in 3.4 million (this equates to 0.000744%, far, far fewer than random distribution would predict, and five orders of magnitude behind the most popular choice).

To the right are the twenty least popular 4-digit passwords encountered.

Warning Now that we've learned that, historically, 8068 is (was?) the least commonly used password 4-digit PIN, please don't go out and change yours to this! Hackers can read too! They will also be promoting 8068 up their attempt trees in order to catch people who read this (or similar) articles.

Check out about the Nash Equilibrium

	PIN	Freq
#9980	8557	0.001191%
#9981	9047	0.001161%
#9982	8438	0.001161%
#9983	0439	0.001161%
#9984	9539	0.001161%
#9985	8196	0.001131%
#9986	7063	0.001131%
#9987	6093	0.001131%
#9988	6827	0.001101%
#9989	7394	0.001101%
#9990	0859	0.001072%
#9991	8957	0.001042%
#9992	9480	0.001042%
#9993	6793	0.001012%
#9994	8398	0.000982%
#9995	0738	0.000982%
#9996	7637	0.000953%
#9997	6835	0.000953%
#9998	9629	0.000953%
#9999	8093	0.000893%
#10000	8068	0.000744%

Passwords – Epic Fail

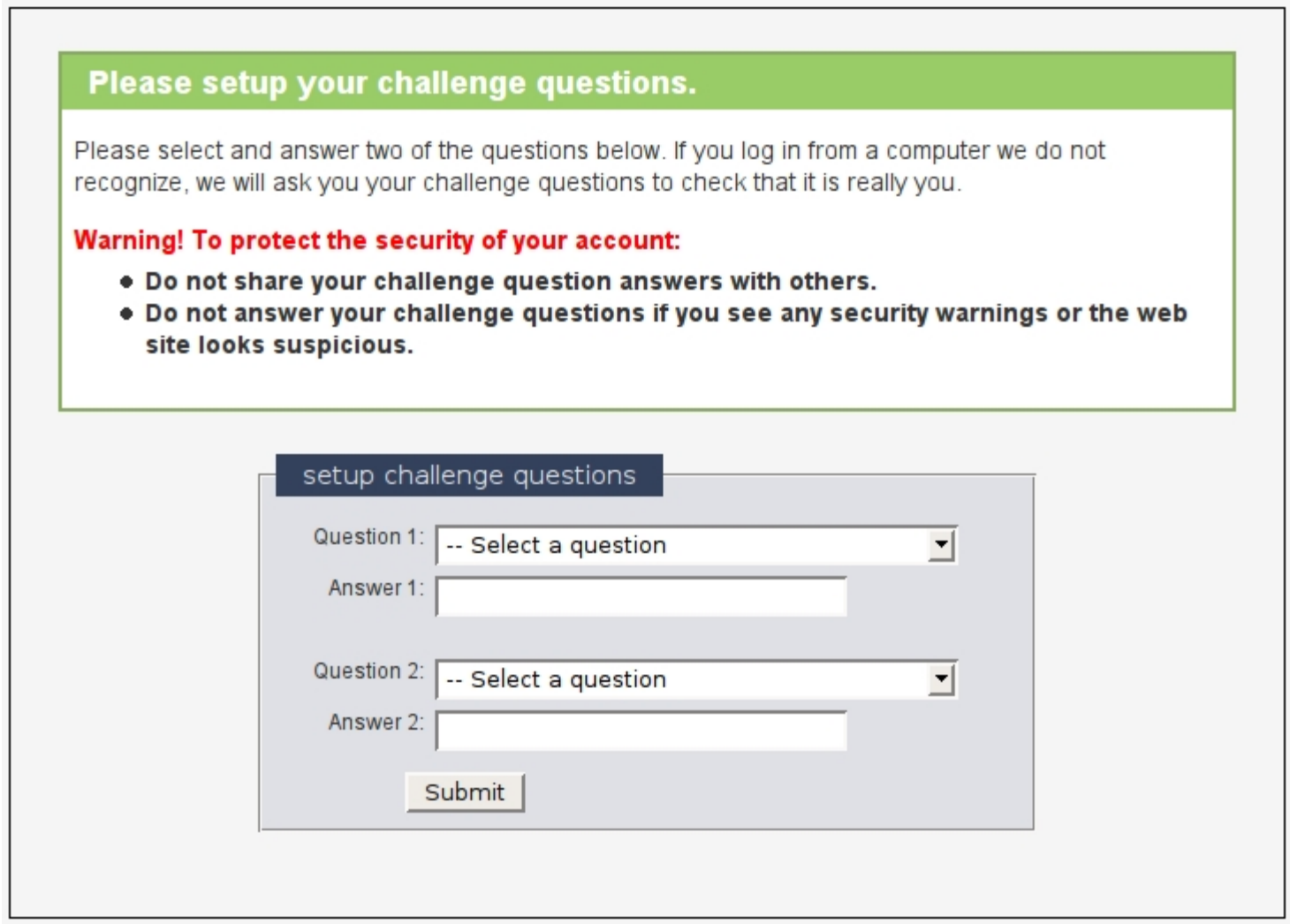
- Guessability
  - Poor!
- Observability
  - Poor!
- Recordability
  - Poor!
- Memorability
  - ????

"I forgot my password, but surely you *recognize* me!"

Even if we obey all the rules…..

- Passwords have to be stored somewhere
- Some developers don't do this properly
- Sony: Hacker breaks into Sony Playstation and steals passwords and user details. (April 2011) – 100 Million People's accounts compromised

Challenge Questions



Cueblots (McBryan & Renaud)

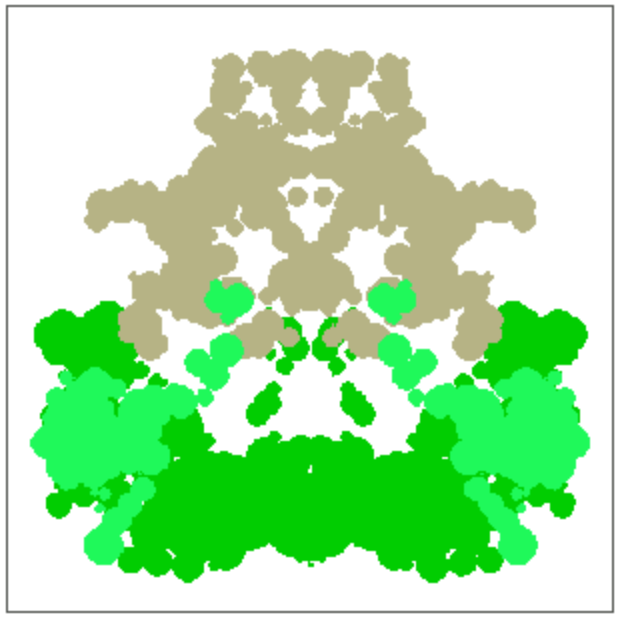
Max Diameter :

Number of blots :

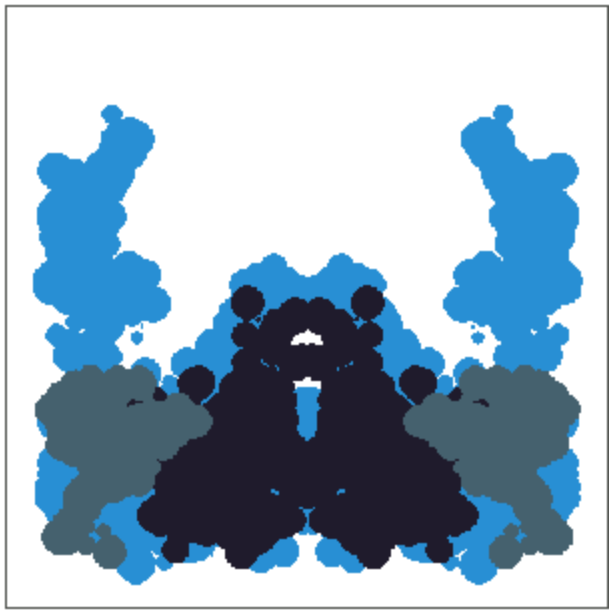
Blot seperation :

Number of colours :

New Inkblot

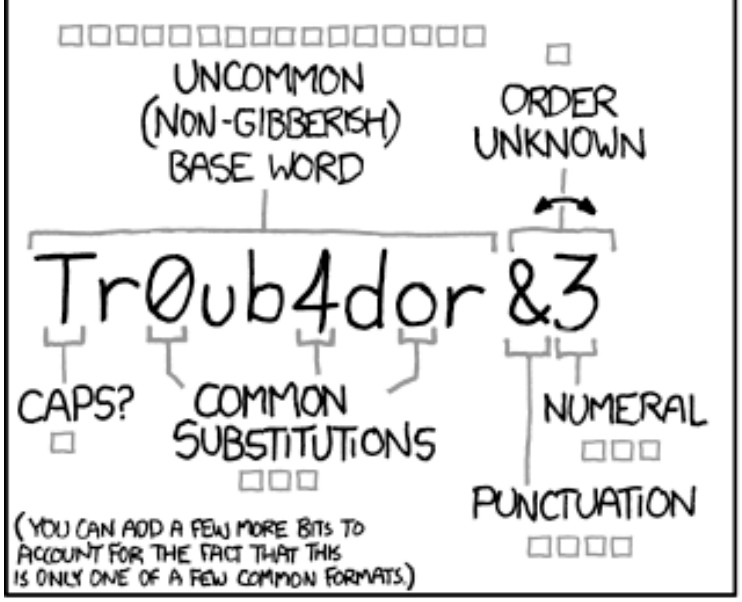


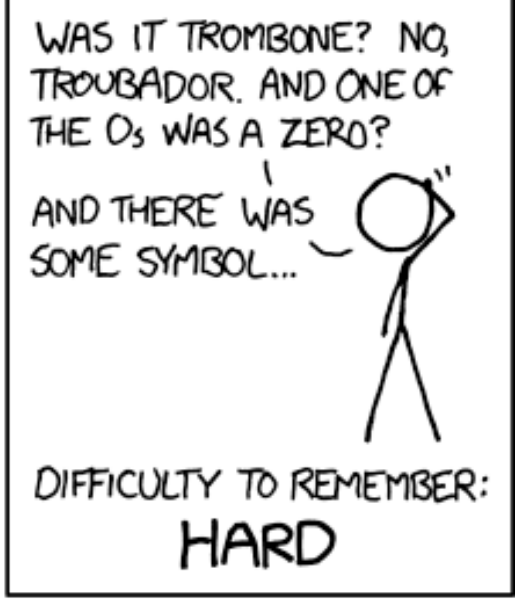
Use this inkblot

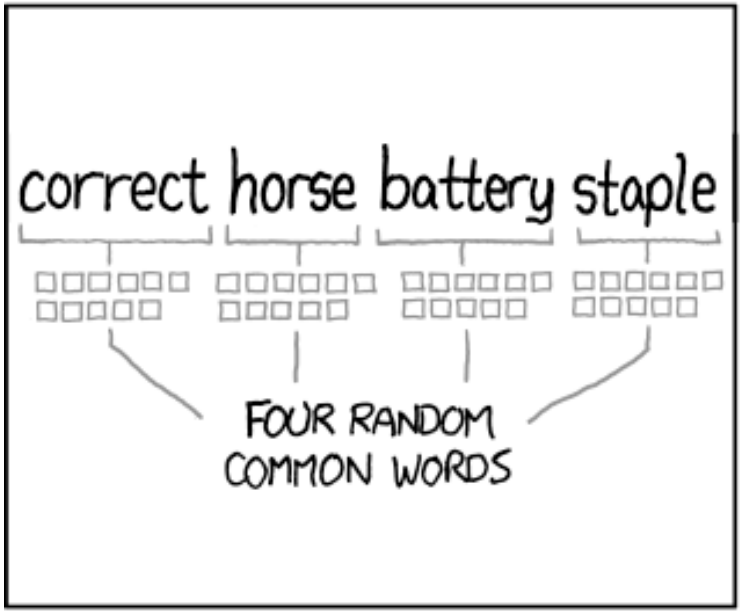


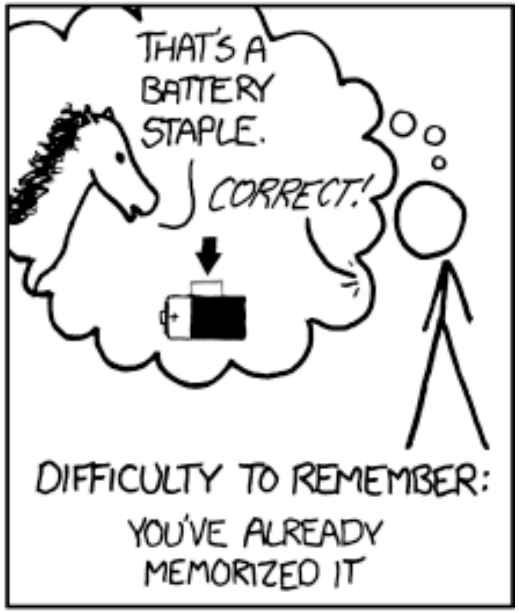
Description :

Submit Reset









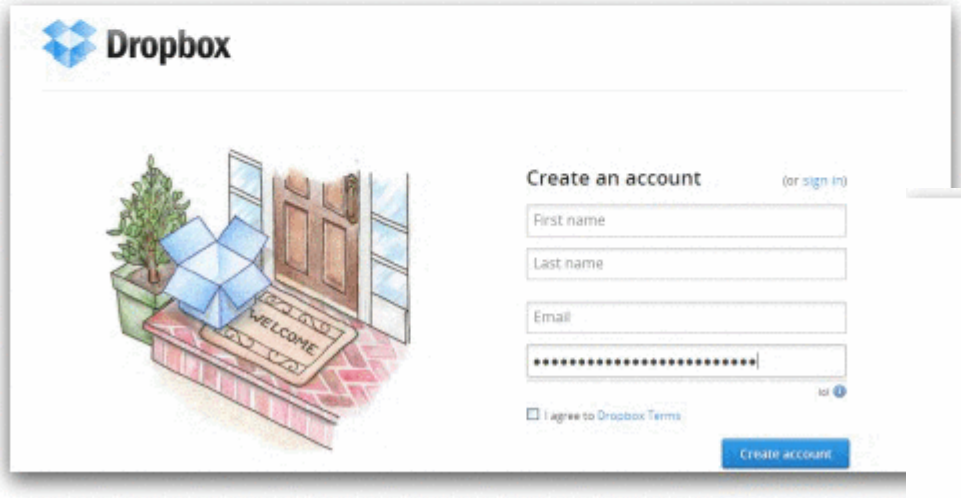
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

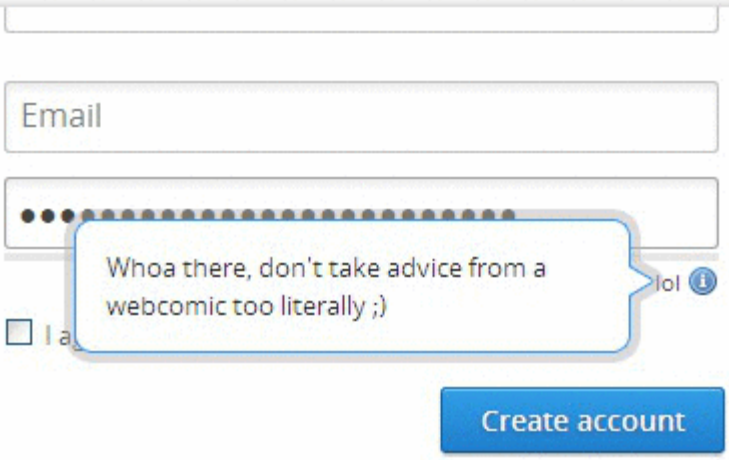
Correcthorsebatterystaple - the guys at Dropbox are funny

by Graham Cluley on August 13, 2012 | Comments (21)
FILED UNDER: Featured, Privacy

Remember that famous xkcd cartoon, suggesting passphrases like "correcthorsebatterystaple" are harder for hackers to crack than the likes of "Tr0ub4dor&3"?

Well, I'm full of admiration for whoever the web developer was at Dropbox who implemented this on their sign-up form...





What you hold

- On it's own not an authenticator!
- Biometric/PIN
- Probs:
  - Cost
  - Reader Requirement & Cost
  - Cannot be used remotely

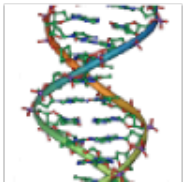

CALYPSOKEY

Biometrics

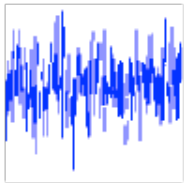
- Instead of what I know, what I am
  - Physiological
- Or the way I behave (because humans are unique)
  - Behavioural

Biometrics

Physiological

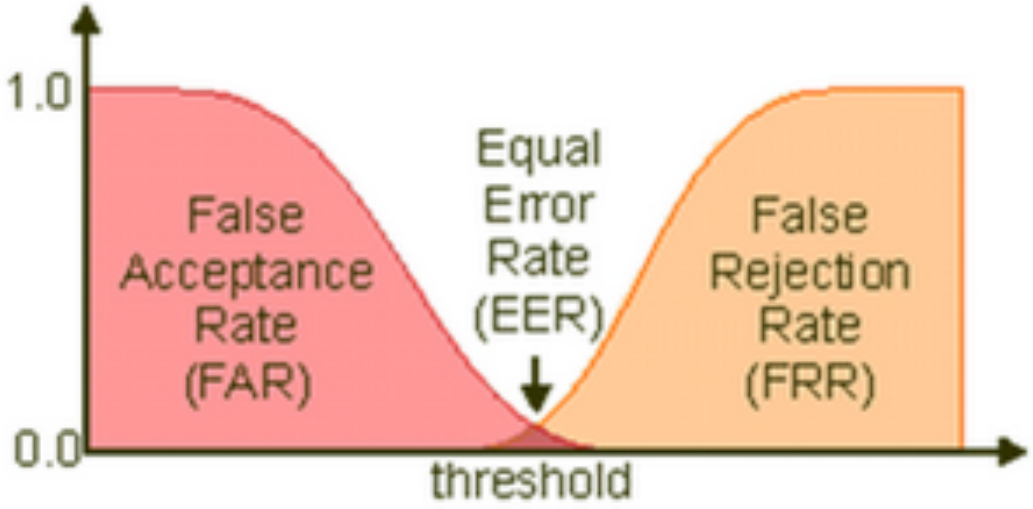
- face 
- fingerprint 
- hand 
- iris 
- DNA 

Behavioral

- keystroke 
- signature 
- voice 

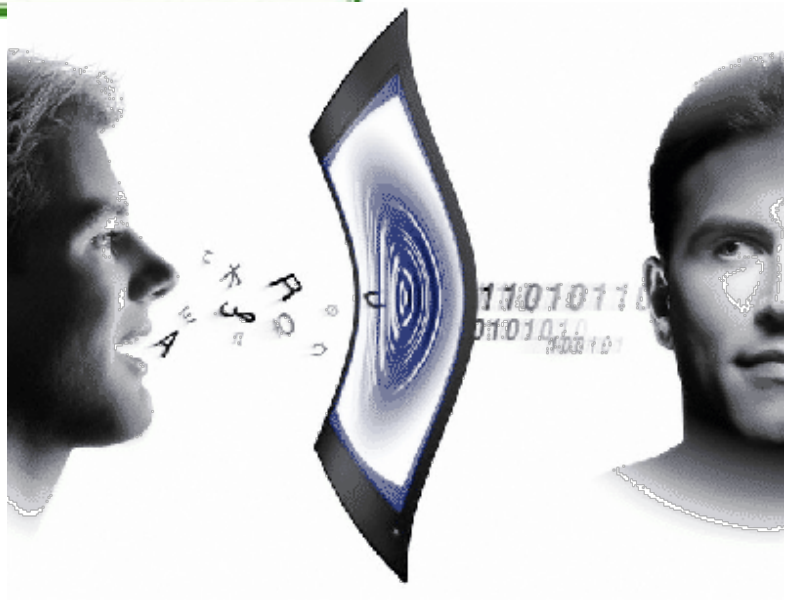
Performance

- FAR
- FRR
- EER
- FTE
- FTC
- Template Capacity



Physiological

Behavioural



As old as civilization

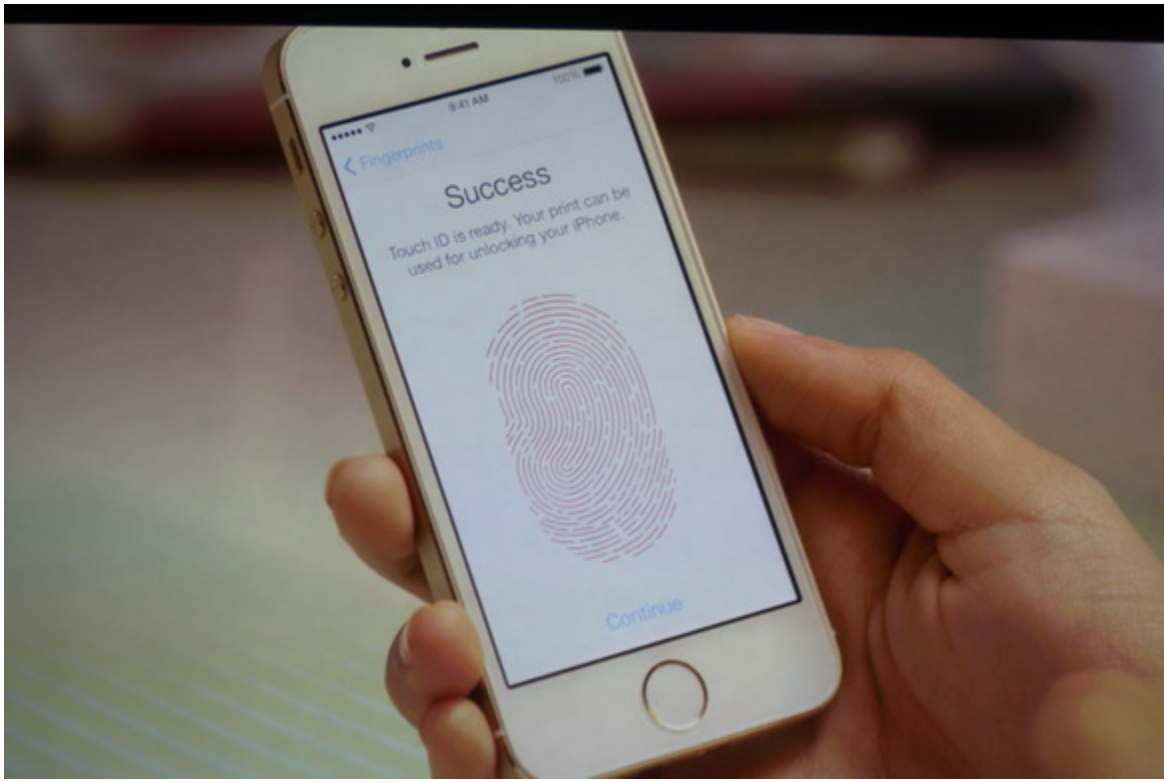
- Hand-prints that accompanied cave paintings from over 30,000 years ago are thought to have been signatures.
- The early Egyptians used body measurements to ensure people were who they said they were.
- Fingerprints date back to the late 1800s.

Bertillon (1882)

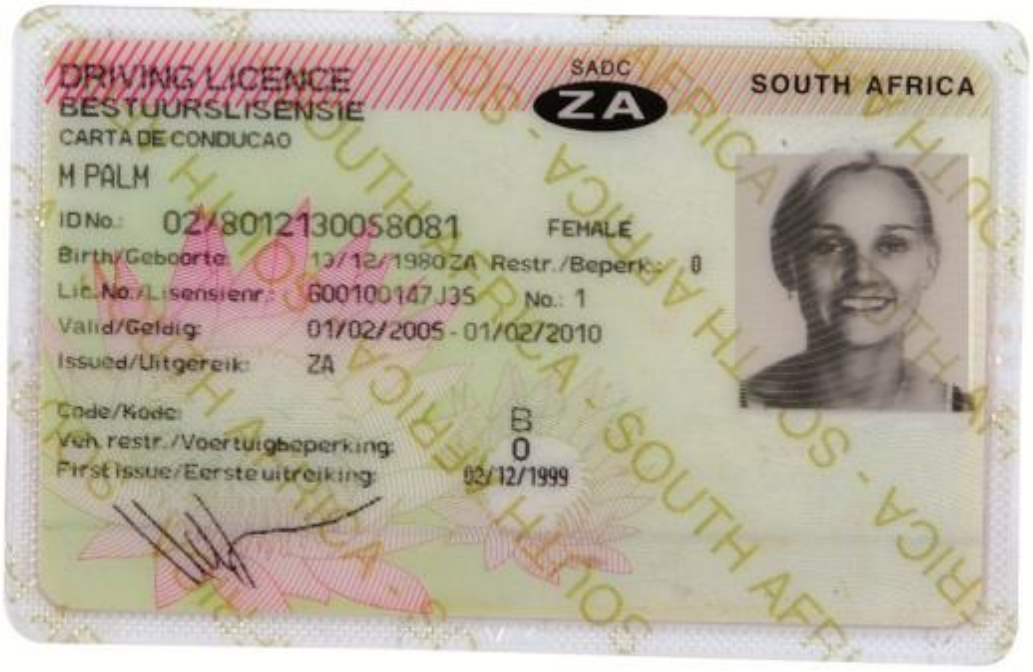
Fingerprints

- Divides print into loops, whorls and arch
- Calculates minutiae points (ridge endings)
- Finger Placement
- Dirt, grime, wounds, age, missing fingers
- Spoof!


Finger Print Scanner
Don't Allow
OK


Fingerprints
Success
Touch ID is ready. Your print can be used for unlocking your iPhone.
Continue


BANKNOTY


DRIVING LICENCE
BESTUURSLISENSIE
CARTA DE CONDUCAO
SADC
ZA
SOUTH AFRICA
M PALM
ID No.: 02/8012130058081
FEMALE
Birth/Geboorte: 13/12/1980 ZA
Restr./Beperk.: 0
Lic.No./Lisensienr.: G00100147J35
No.: 1
Valid/Geldig: 01/02/2005 - 01/02/2010
Issued/Uitgereik: ZA
Code/Kode: B
Veh. restr./Voertuigbeperking: 0
First issue/Eerste uitreiking: 02/12/1999


DRIVER RESTRICTIONS
0 None
1 Glasses / contact lenses
2 Artificial limb
PrDP CATEGORIES
P Passengers
G Goods
D Dangerous goods
VEHICLE RESTRICTIONS
0 None
1 Automatic transmission
2 Electrically powered
3 Physically disabled
4 Bus > 16000 kg (GVM) permitted
A
A1 ≤ 125 cc
B
GVM ≤ 3500 kg
≤ 750 kg
C1
GVM ≤ 16000 kg
C
GVM > 16000 kg
EB
EC1
EC
EC
No Print

PICKED FOR TV WTF | APRIL 01, 2008 | 7 COMMENTS

Hackers publish fingerprints of biometrics-touting Minister

SOURCE: http://www.boingboing.net/2008/04/01/hackers-publish-thou.html

Hackers in Germany have published thousands of copies of the fingerprints of German minister Wolfgang Schauble, a loud advocate of fingerprint biometrics. Hackers from the Chaos Computer Club lifted a fingerprint from the Interior Minister, printed it on plastic, and distributed it by the thousands with their magazine for anyone who wants to impersonate the Minister at a biometric checkpoint. Short of amputation, a biometric identifier can't be revoked or changed. Schauble is a big proponent of the use of fingerprints in passports but is not the CCC's only target. The group has called for help

Malaysia car thieves steal finger

By Jonathan Kent
BBC News, Kuala Lumpur

Police in Malaysia are hunting for members of a violent gang who chopped off a car owner's finger to get round the vehicle's hi-tech security system.

The car, a Mercedes S-class, was protected by a fingerprint recognition system.

Accountant K Kumaran's ordeal began when he was run down by four men in a small car as he was about to get into his Mercedes in a Kuala Lumpur suburb.

The gang, armed with long machetes, demanded the keys to his car.

It is worth around $75,000 second-hand on the local market, where prices are high because of import duties.

But having stripped the car, the thieves became frustrated when they wanted to restart it. They found they again could not bypass the immobiliser, which needs the owner's fingerprint to disarm it.

They stripped Mr Kumaran naked and left him by the side of the road - but not before cutting off the end of his index finger with a machete.

Flawed fingerprint evidence led to a travesty of justice

by DAVID JONES

Last updated at 22:00 25 April 2007

The solitary fingerprint was found halfway up a bathroom door frame in the bungalow where a reclusive spinster named Marion Ross had been brutally stabbed to death.

At first, detectives attached no importance to the slightly smudged print, for, over the years, dozens of people had been in the house. Indeed, the print was among 400 discovered when fingerprint officers dusted down the murder scene.

Besides, the police had already arrested David Asbury, a young builder from the same town where 51-year-old Miss Ross lived, and were convinced he had killed her - with such savagery that she was found pinned to the blood-soaked carpet by a pair of scissors which had been driven through her throat and spinal column.

It was only when the supposedly 'insignificant' print on the door frame was examined by criminal records experts that events took a different turn.

Shirley McKie: Victim of a high level cover-up?

This was in the winter of 1997 and over the next decade the result of that one routine test would drive a dedicated young Scottish policewoman to the brink of suicide and destroy her promising career.

Brazilian doctor arrested for faking biometric prints

Share

Friday, March 15, 2013

A doctor in Sao Paulo, Brazil was arrested for using fake fingers to punch into a hospital's biometric time clock.

As posted on The Province, the doctor, Thauane Nunes Ferreira, used silicone fingers imprinted with real fingerprints to clock in for other employees.

Ferreira had fingers for 11 doctors and 20 nurses, and these staffers would pay him each month for clocking into more overnight shifts than they actually worked.

Authorities charged Ferreira with falsifying a public document. The doctor faces prison time.

Ear Biometrics

- Ears are remarkably consistent
- Passive
- No cosmetics, emotions, colour changes (graying hair)
- Smaller than the face (faster processing)
- No problem with glasses
- Hair & Earrings

Tuesday, December 15, 1998 Published at 23:47 GMT

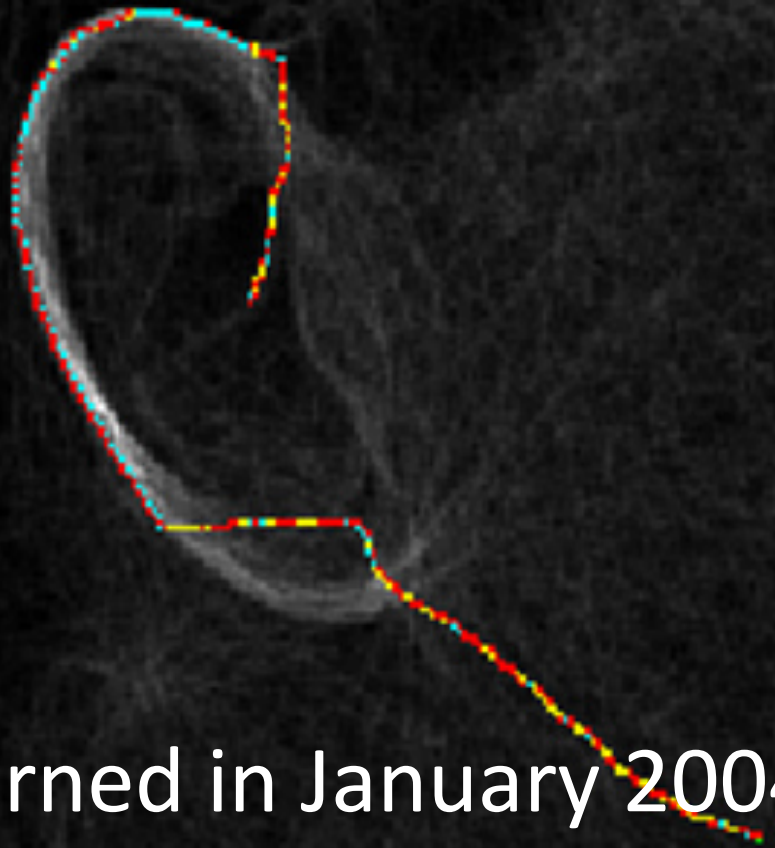
UK

Ear print catches murderer

Dorothy Wood (centre) was suffocated with a pillow during a burglary

A man has been convicted of murdering an elderly spinster on the basis of "earprint" evidence, in what is believed to be a legal first.

- In 1998 an ear print left on a window led to the conviction of Mark Dallagher for murdering a 94-year-old woman.

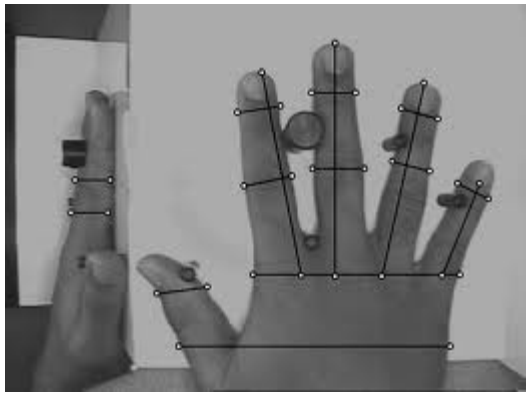


- Overturned in January 2004
  - Flawed evidence
  - subjective opinion of an ear expert.

Hand Biometric

Hand Geometry

- Geometry of users hands
- More reliable than fingerp
- Balance in performance and usability
- Very large scanners
- Arthritis
- Jewellery
- Growing children

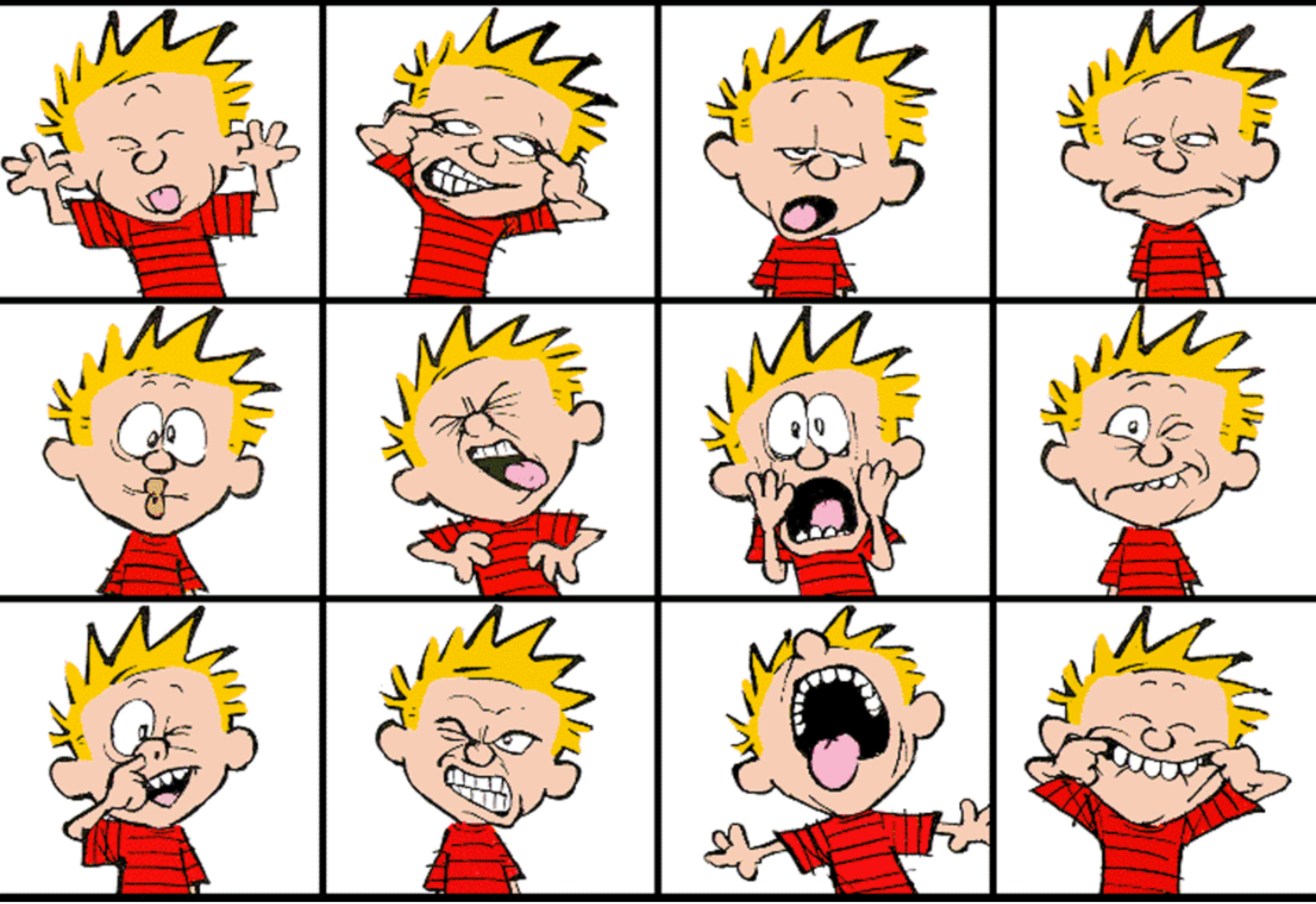


Iris Recognition

- Scans unique pattern of iris
- Iris is colored and visible from far
- No touch required
- Overcomes retinal scanner issues
- Contact lenses an issue?
- Intrusive
- Expense

Face Recognition

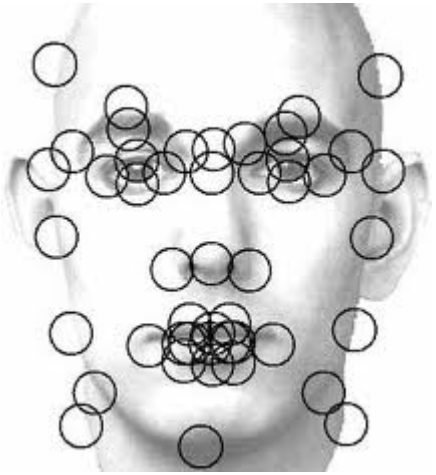
- User faces camera
- Neutral expression required
- Appropriate lighting and position
- Algorithms for processing



Boston Bombing

- Systems are only as good as the data they're given to work with
- Despite having an array of photos of the suspects, the system couldn't come up with a match
- facial recognition isn't an instantaneous, magical process
- Facial recognition and other biometric and image processing technologies (gait recognition) helped by retailers' own computerized surveillance systems.

Face Recognition



- User faces camera
- Neutral expression required
- Appropriate lighting and position
- Algorithms for processing
- Expression
- Spoof
- Tougher Usability

Alex Covert
800 Trends
3.1 MM Views
★★★★
Star

Face-Recognition Vending Machines Fail

"Are you going to buy it with your good looks or mine?" As it turns out, underage smokers in Japan can easily buy cigarettes using someone else's photo or an image from a magazine.

Most of Japan's 570,000 cigarette vending machines are being outfitted with RFID readers that check the purchaser's Taspo age-verification card. For those who don't have a card, they can buy their cigarettes over the counter or from one of 4,000 face-recognition vending machines. The system compares the buyer's face to a database of over 100,000 people, looking for signs of old age. It seems, however, that the system can be tricked by holding up a photograph of someone else.

Eyeball Reflexes: Security and Biometrics That Cannot Be Spoofed

ScienceDaily (Sep. 4, 2008) — Electronic fingerprinting, iris scans, and signature recognition software are all becoming commonplace biometrics for user authentication and security. However, they all suffer from one major drawback - they can be spoofed by a sufficiently sophisticated intruder.

See Also:

Matter & Energy
- Biometric
- Engineering
- Electronics

Computers & Math
- Information Technology
- Artificial Intelligence
- Hacking

Reference
- Identity theft
- Computer security
- Fingerprint
- Security engineering

Writing in the International Journal of Biometrics, Japanese researchers describe a new approach based on a person's reflexes that could never be copied, forged, or spoofed.

Masakatsu Nishigaki and Daisuke Arai of Shizuoka University, Japan, explain how the use of biometrics for user authentication is becoming increasingly widespread. "Biometrics makes it possible to authenticate a person accurately," they say.

A digital fingerprint pad hooked up to a computer, for instance, can provide access to online resources only to specific individuals based on their unique fingerprint. Signature recognition allows a person to receive information or goods only if their signature matches the imprint held in a database. Iris scanning technology identifies a person and allows them access to a building only if they have authorization. There are several other biometrics in development, based on the pattern of blood vessels in the retina or skin and other such phenomena.

"However, biometric information can easily be leaked or copied," the researchers point out. "It is therefore desirable to devise biometric authentication that does not require biometric information to be kept secret."

http://www.sciencedaily.com/releases/2008/09/080904102751.htm

Replacing passwords and PINs with your heartbeat

Posted on 04 September 2013.

We've been hearing for a while now that passwords will soon become a thing of the past and, as it seems now, biometric authentication is likely to take their place.

The latest innovation in this field comes from Canadian startup Bionym, whose team created Nymi, a bracelet / wristband containing an ECG (electrocardiogram) sensor that "reads" the unique heartbeat pattern of the wearer and uses it to authenticate into a variety of electronic devices (cars, computers, smartphones, TVs, etc.).

DNA

- Unique – cheaper to sequence than ever before
- Twins?

“With identical twins, even if you sequenced their whole genome you wouldn’t find difference,” forensic scientist Bob Gaensslen told ABC News at the time. More recent research shows that this isn’t the case, but teasing out the difference can be expensive — in the Marseilles case, police were told that such a test would cost £850,000.

DNA Evidence Can Be Fabricated, Scientists Show

By ANDREW POLLACK
Published: August 17, 2009

Scientists in Israel have demonstrated that it is possible to fabricate DNA evidence, undermining the credibility of what has been considered the gold standard of proof in criminal cases.

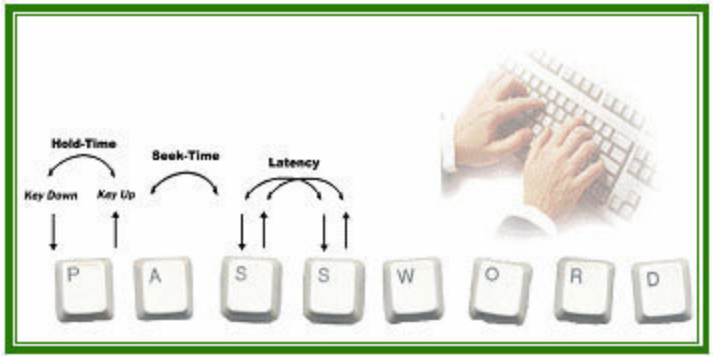
The scientists fabricated blood and saliva samples containing DNA from a person other than the donor of the blood and saliva. They also showed that if they had access to a DNA profile in a database, they could construct a sample of DNA to match that profile without obtaining any tissue from that person.

"You can just engineer a crime scene," said Dan Frumkin, lead author of the paper, which has been published online by the journal Forensic Science International: Genetics. "Any biology undergraduate could perform this."

Dr. Frumkin is a founder of Nucleix, a company based in Tel Aviv that has developed a test to distinguish real DNA samples from fake ones that it hopes to sell to forensics laboratories.

Behavioural Biometrics

- Authorship – did the person write this or draw this?
- Computer usage:
  - Interaction with mice, keyboards which are distinct and different from others
    - Mouse movements
    - Keystroke dynamics
  - Strategies, knowledge or skill used during interaction with software
    - Email behaviour

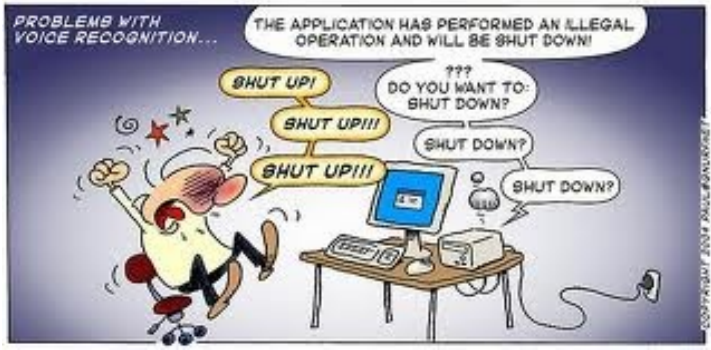


Voice Recognition

- Speech input
  - Frequency
  - Duration
  - Cadence
- Neutral tone
- User friendly

Disadvantages

- Local acoustics
- Background noise
- Device quality
- Illness , emotional behavior
- Time consuming enrollment
- Large processing template
- Spoof



What Traits make something suitable as a biometric?

- Universality
- Uniqueness
- Permanence
- Measurability
- Performance
- Acceptability
- Circumvention

Log your routine and say goodbye to passwords

- 03 January 2014 by **Paul Marks**
- Magazine issue 2950. **Subscribe and save**
- For similar stories, visit the **Computer crime** Topic Guide

---

SICK of having to remember a zillion passwords? Logging in using obscure facts about your everyday life could be the answer.

Called narrative authentication, the system was developed by Carson Brown and colleagues at Carleton University in Ottawa, Canada. It uses software running in the background on a computer or smartphone to log your activities. The system can, for example, note how long you spent playing a video game, which one it was and the time you stopped. It also logs videos you posted to Facebook and any check-ins you made on social networking sites such as Foursquare. You can also add your own events to the narrative, such as when you passed your driving test.

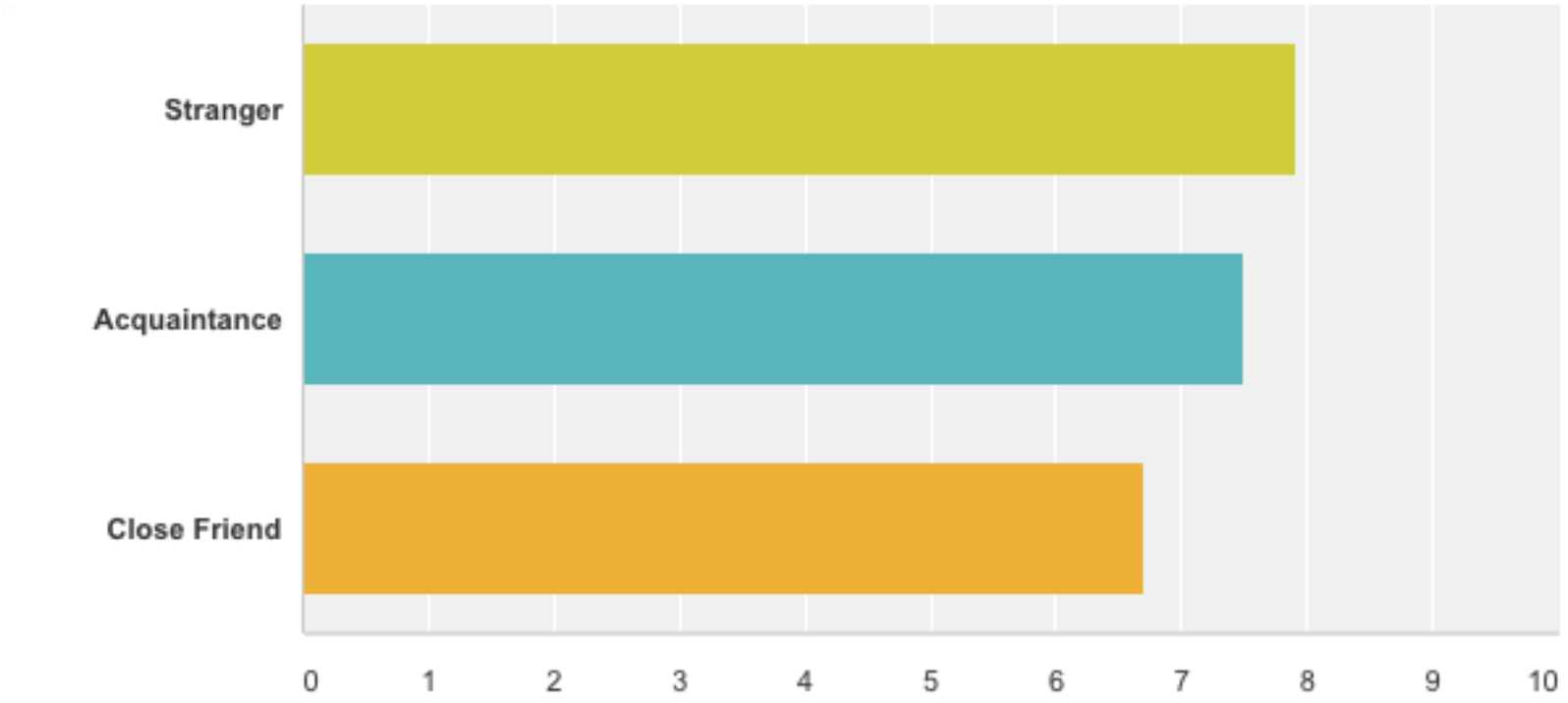
Once set up, the system will generate questions based on its records – making logging in a little like playing a text-based adventure game, according to Brown. It's fun, he says, and nowhere near as boring as entering passwords. The work was first presented at a security conference in September.

Robert Ghanea-Hercock, chief security researcher at BT's lab in Ipswich, UK, says the system could be a valuable addition to our range of login strategies. "Humans are better equipped to process stories than random pass phrases," he says

Alternative Authentication

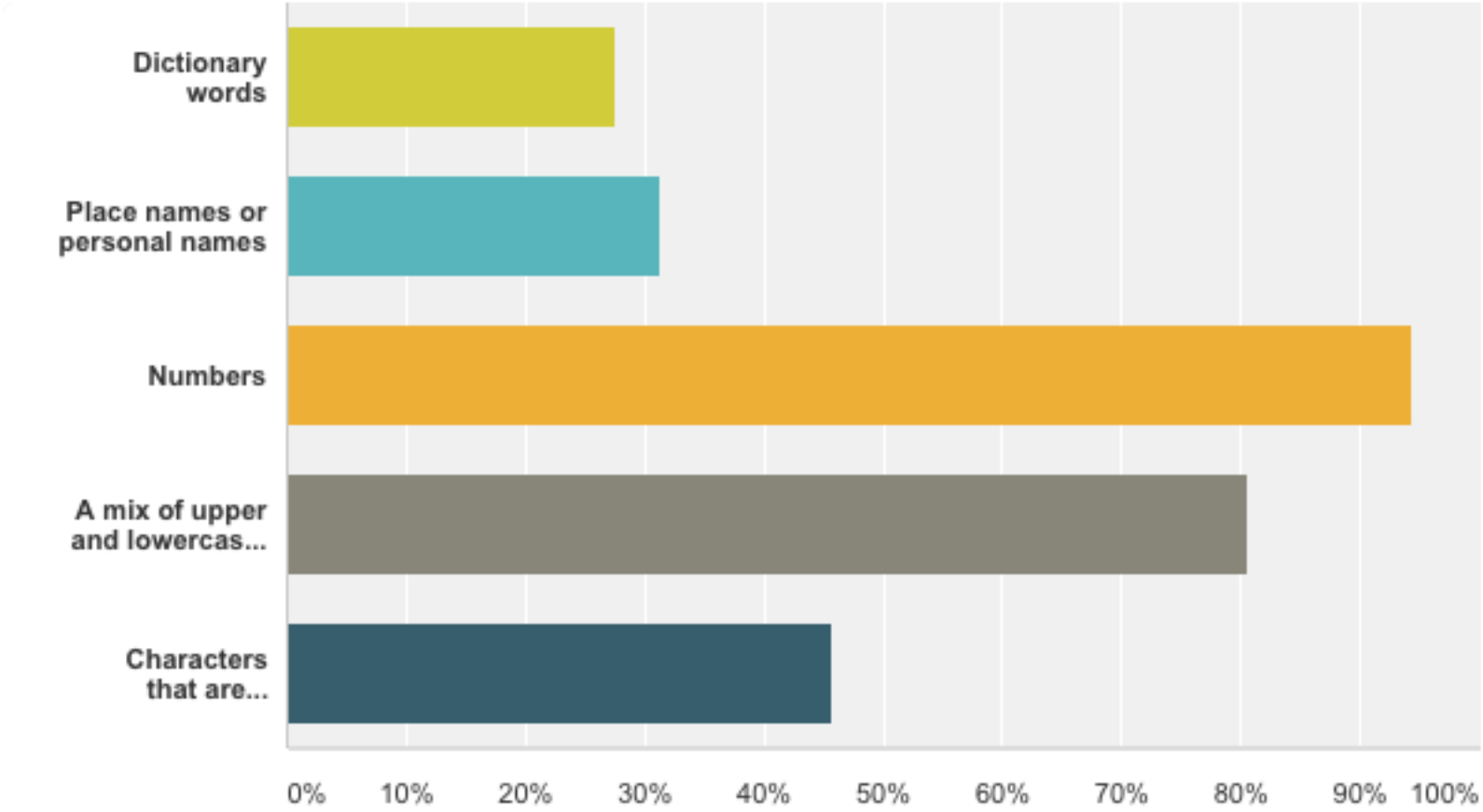
How easy do you think it would be for the following to guess or break the password for your university account ?

Answered: 160 Skipped: 0



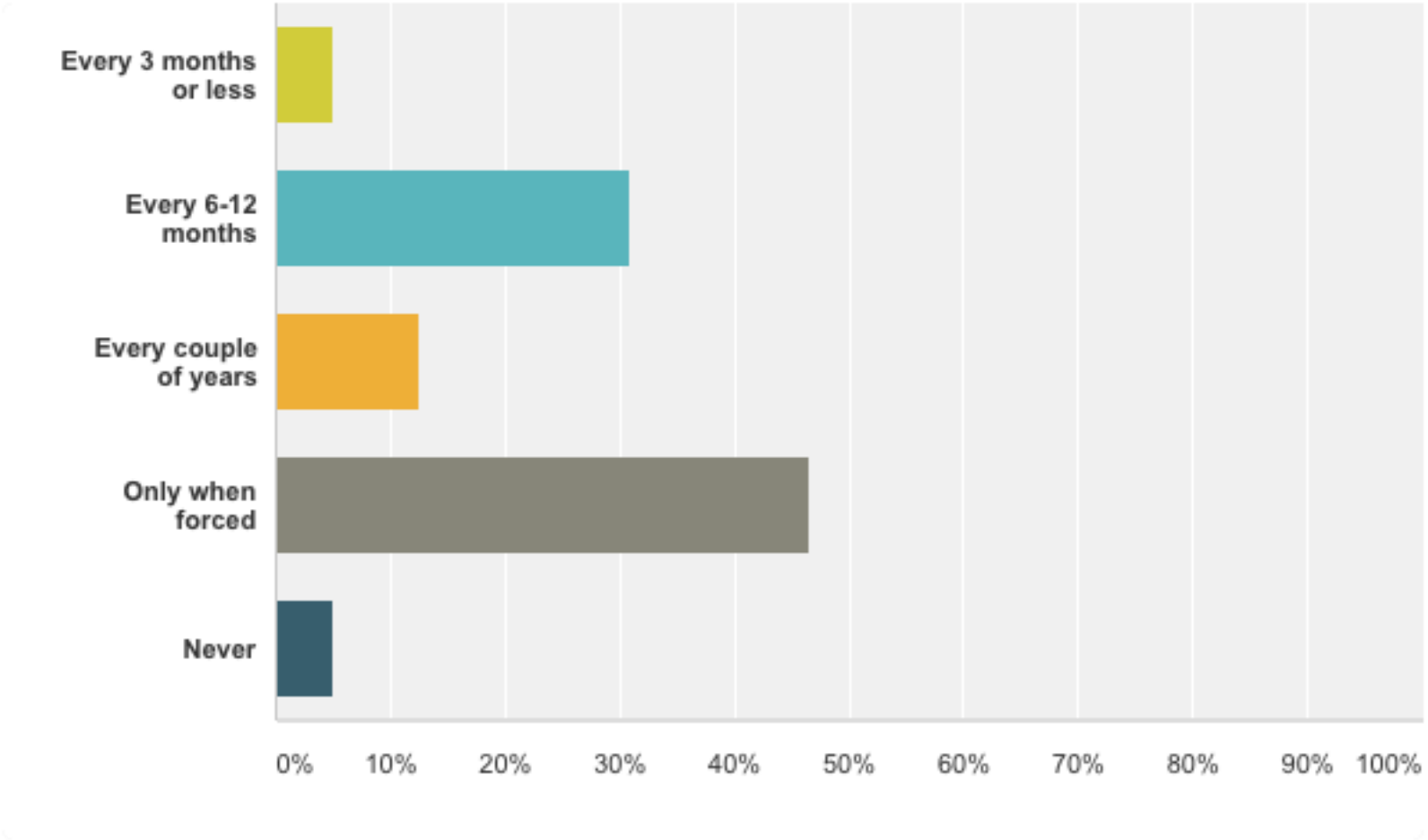
Do you include any of the following when creating an important password? (Choose as many as you like)

Answered: 160 Skipped: 0



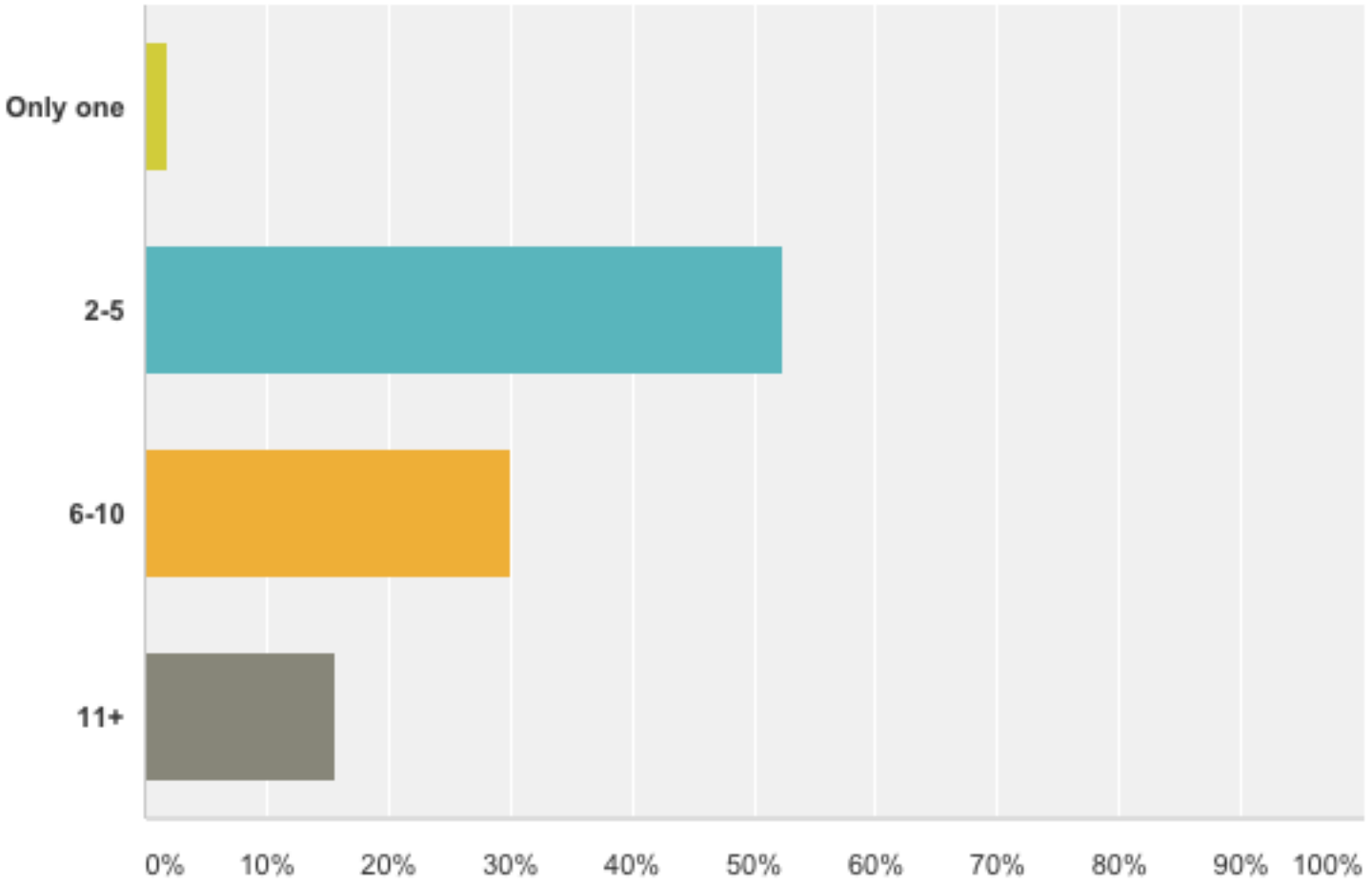
How often do you change your passwords ?

Answered: 159 Skipped: 1



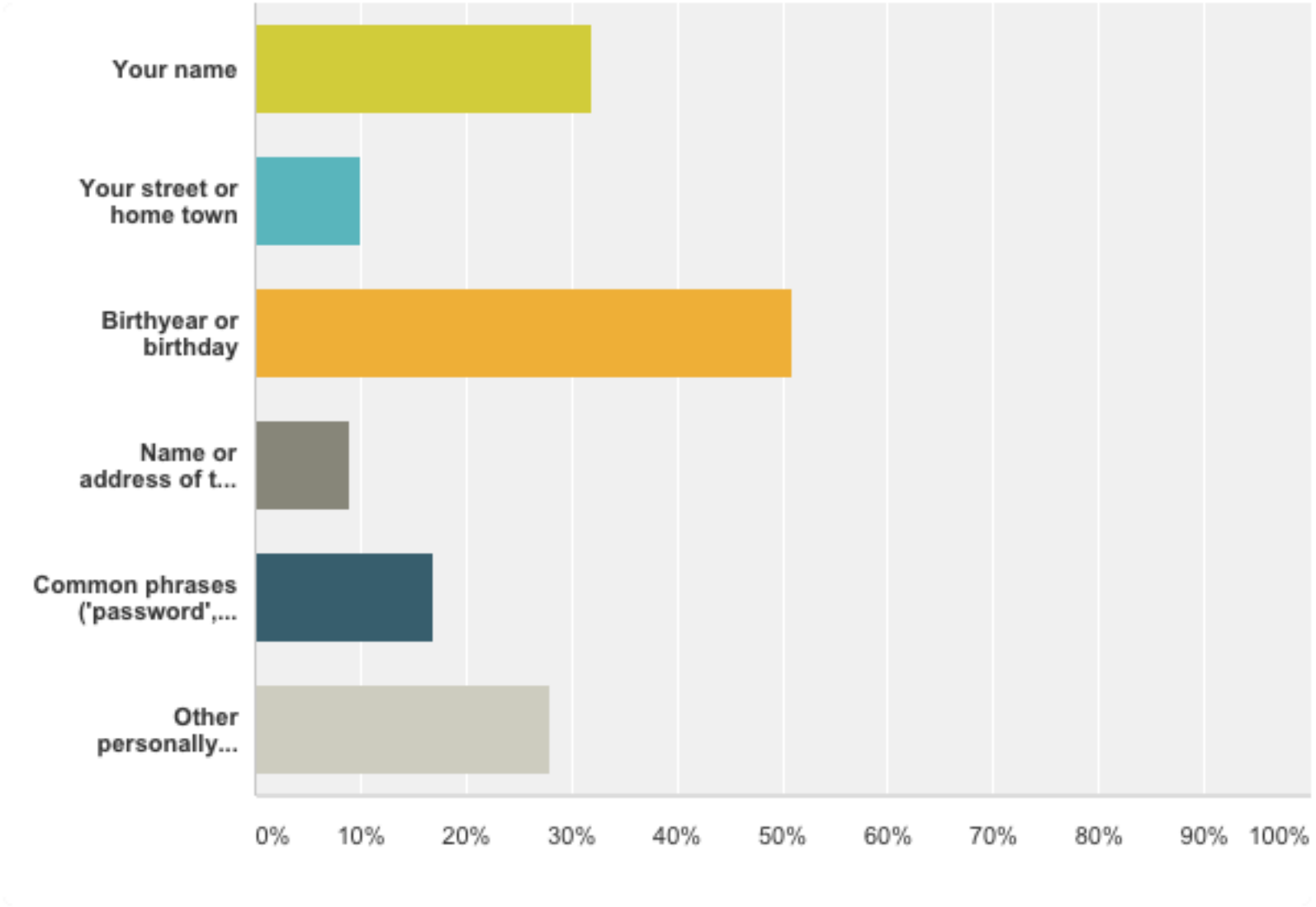
How many different passwords do you use across your accounts ?

Answered: 160 Skipped: 0



Have you ever used any of the following as part of a password ?

Answered: 100 Skipped: 60



Paranoid about passwords? Just take a pill

JOHN HARLOW The Times June 24, 2013 12:00AM

STRUGGLING to remember your long list of computer or bank passwords? Forgotten your driving licence or company ID card? Now there's a pill for that.

A US phone company is working with doctors to perfect a tiny, swallowable device that stores your codes and ID in your stomach. The pill, which has been approved for medical use by the US Food and Drug Administration, can automatically hook up with smartphones and confirm your identity to an array of devices. It is powered by stomach acid to broadcast encrypted details to code readers on phones or even office doors.

The pill is being championed by Regina Dugan, who has been called "America's smartest engineer".

She was the first female director of the US government's spy technology agency Darpa (Defence Advanced Research Projects Agency) before joining Google's Motorola Mobility division as creative boss last year.

She told a conference last month that Motorola was looking at "ingestibles" as well as "wearables" such as glasses and tattoos to turn the human body into a "wired being".

Two Factor Authentication

- **Not 2 passwords!**
- **2 different types**

Dropbox two-factor authentication available to early adopters

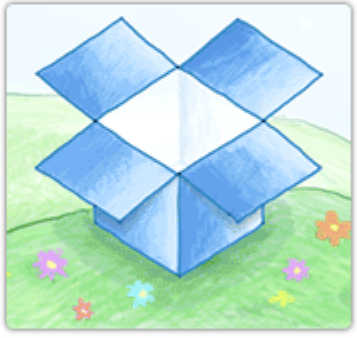
Join thousands of others, and sign up for Naked Security's newsletter

you@example.com Do it!

Don't show me this again X

by Paul Ducklin on August 27, 2012 | Comments (15)

FILED UNDER: Data loss, Featured



A few weeks ago we wrote about a spam problem reported by Dropbox users.

Email addresses which had only ever been used with Dropbox accounts (at least so far as the account holders were aware) experienced a surge in spam, leading people to conclude that something had gone wrong at Dropbox.

As we reported at the time, the truth was actually a little more complex than that.

Some users had set the same password on multiple sites, and a compromise elsewhere led to their Dropbox accounts being unlawfully accessed and assaulted by spammers.

Other spam-affected users were affected indirectly, because one of those "compromised elsewhere" accounts belonged to an employee at Dropbox itself. This staffer's was account was raided and gave up not one email address, but many, thanks to what Dropbox described as "a project document with user email addresses."

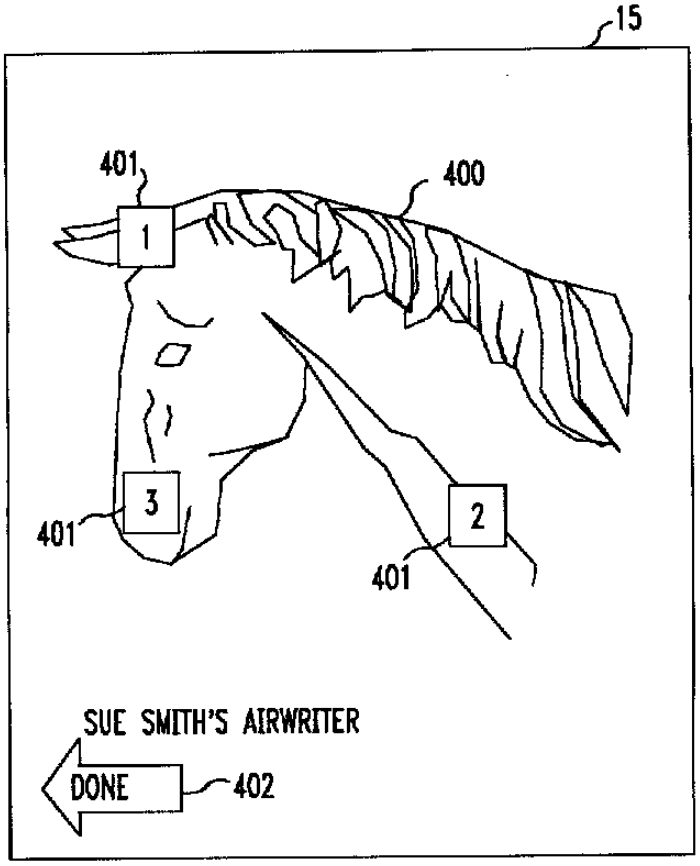
Part of Dropbox's response was to promise a two-factor authentication (2FA) system using your mobile phone as the second factor.

Alternative Authentication Mechanisms

How Memory is Assessed

- Recall Based
- Cued-Recall Based
- Recognition Based

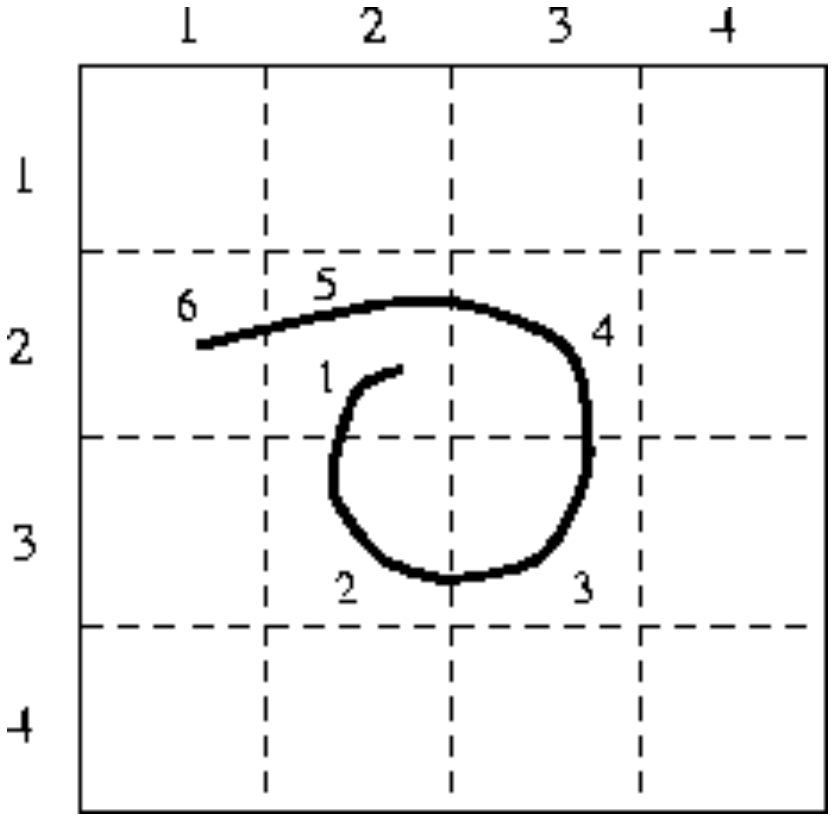
Blonder (1997)



PassClick -mininova labs

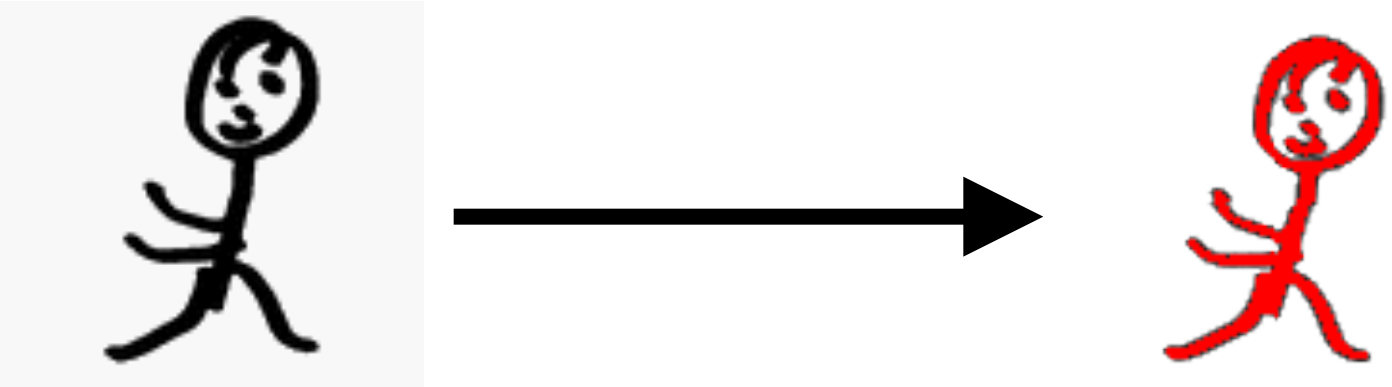
PassClick (157090 people)

Jermyn (2000): Draw a Secret

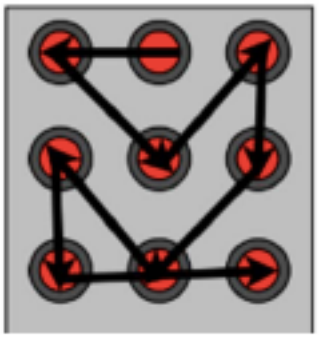


Drawmetric

User needs to redraw an image in the same stroke order



Android sketch authentication



Sketch Based Recall

- Shortcomes?
  - Dictionary attack
  - Symmetric drawings
  - Three strokes only
- Restrictions?

Paper: Android's Graphical Passcodes are Insecure

August 12, 2010

Written by: **Frederic Lardinois**

Most Android phones allow users to protect their phones from unauthorized access by drawing a pattern on their device's touchscreens. According to a team of researchers from the University of Pennsylvania, however, these graphical passwords are actually extremely easy to crack, as "oily residues, or smudges, on the touch screen surface, are one side effect of touches from which frequently used patterns such as a graphical password might be inferred."

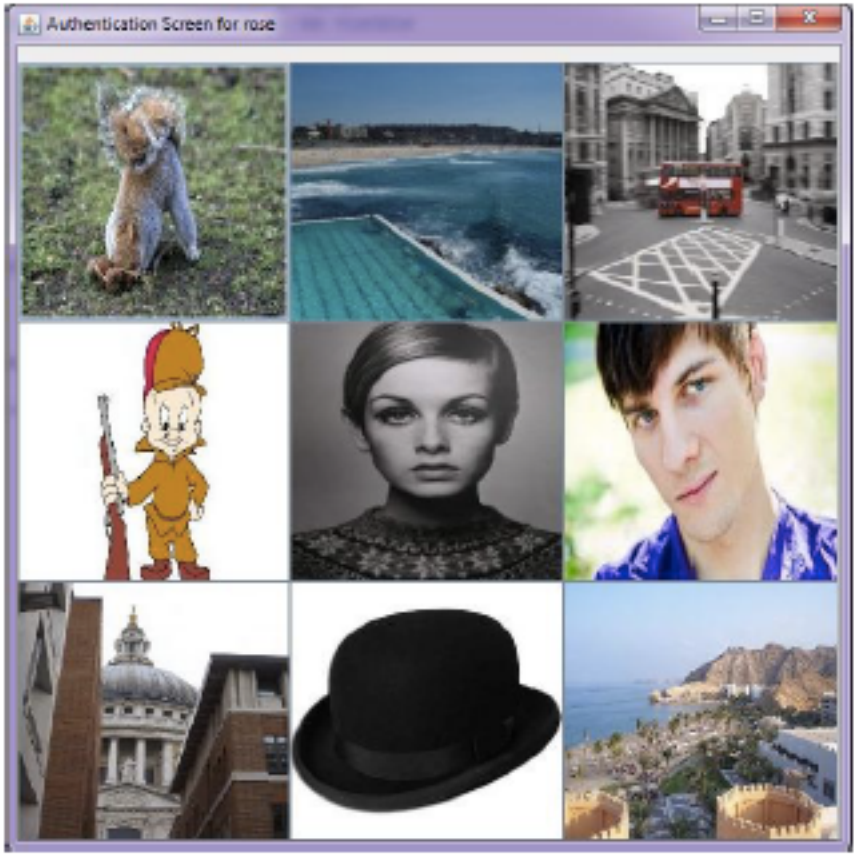
The team, which presented its findings during the Woot '10 USENIX workshop in Washington, DC, found that by simply taking photographs of the screens with the right lightning and camera positions allows unauthorized users to guess a user's security pattern.

If you think that just cleaning the screen regularly would prevent this, then think again. According to the researchers, "smudges are surprisingly persistent in time." They found that "it is surprisingly difficult to incidentally obscure or delete smudges through wiping or pocketing the device." In the team's experiments, the pattern was partially identifiable 92% of the time and in 68% of cases, it was fully identifiable.

You can find the full paper here.

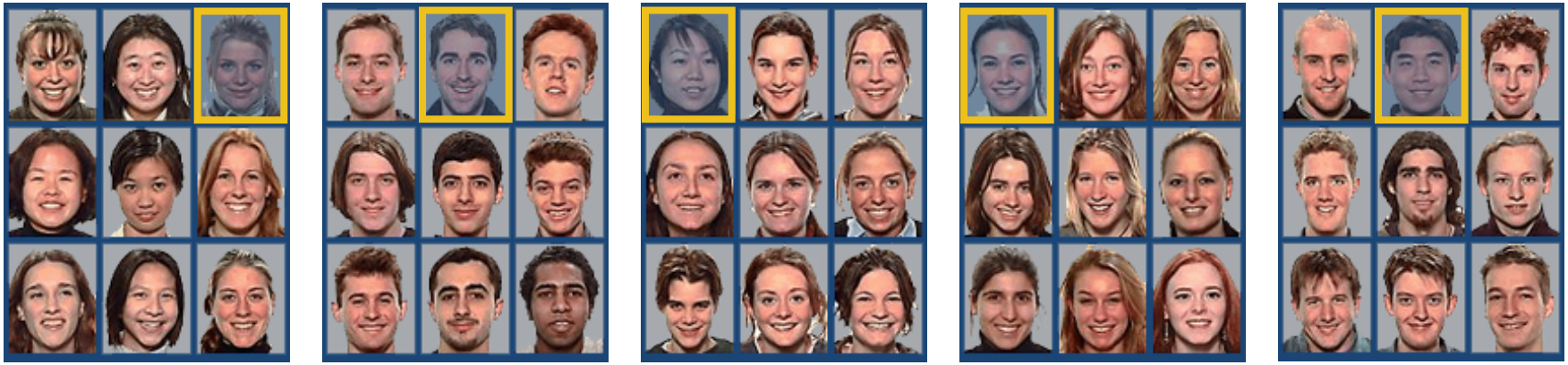
https://docs.google.com/viewer?url=http://www.usenix.org/events/woot10/tech/full_papers/Aviv.pdf

Recognition-Based Graphical Authentication



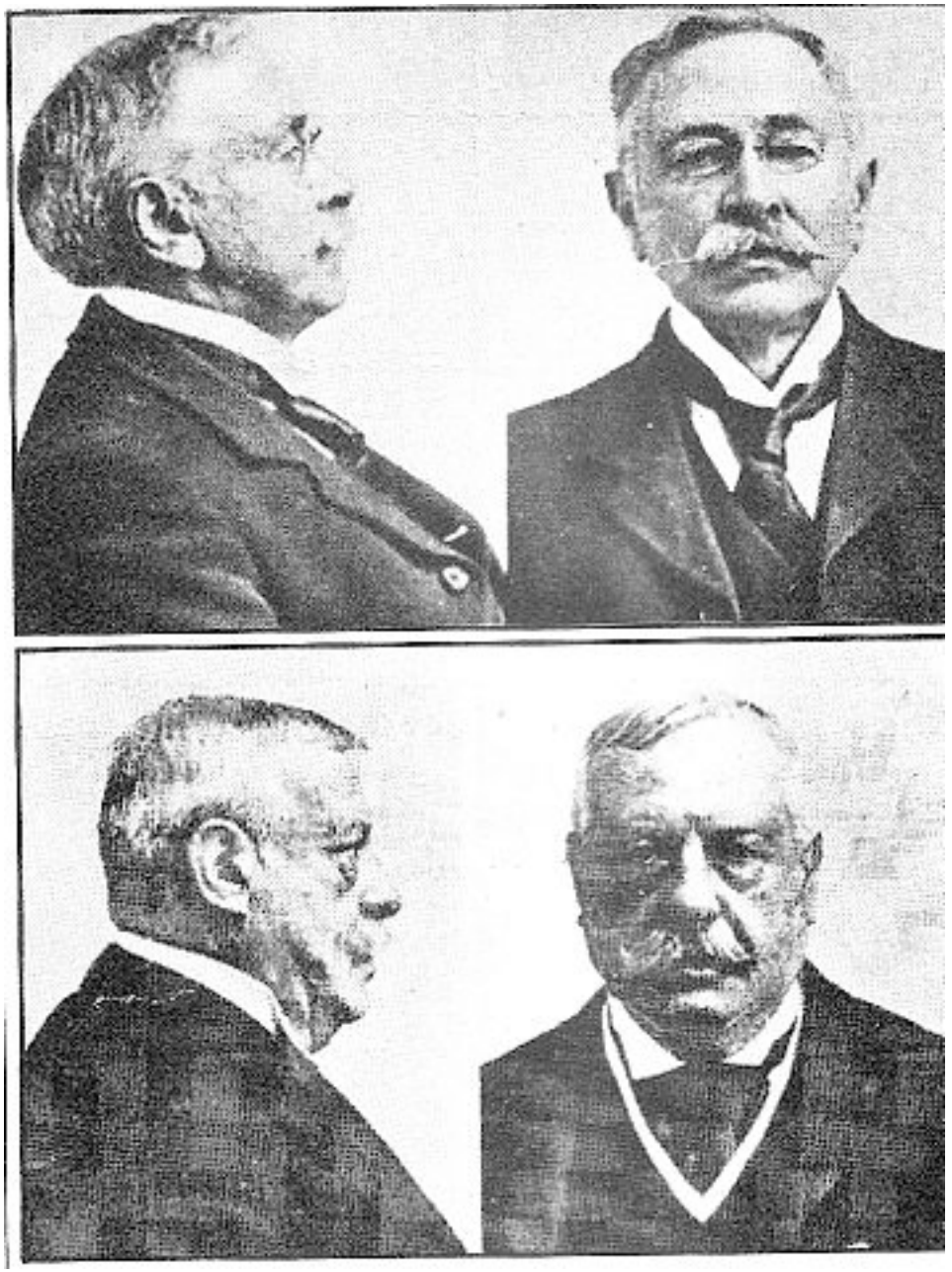
Passfaces

- 5 Passfaces are Associated with 40 associated decoys
- Passfaces are presented in five 3 by 3 matrices each having 1 Passface and 8 distractors



Snags

- People are good with FAMILIAR faces



A

B

C

D

E

F

G

H

J

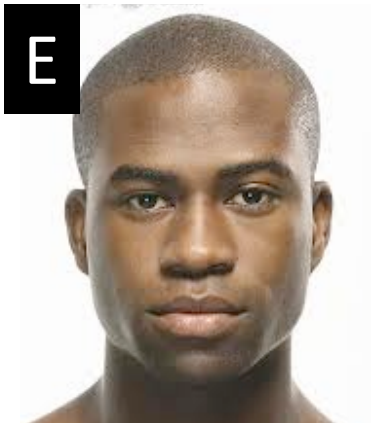
A

B

C

D

E

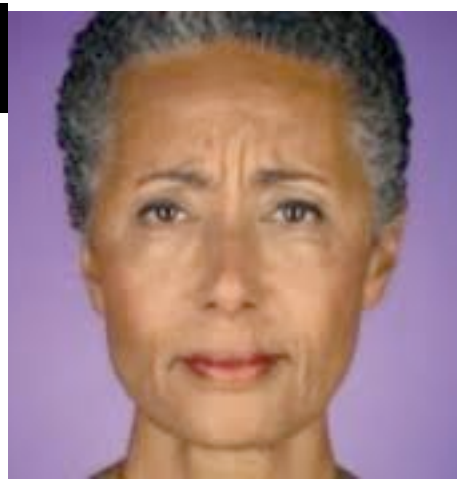


F

G

H

J



A

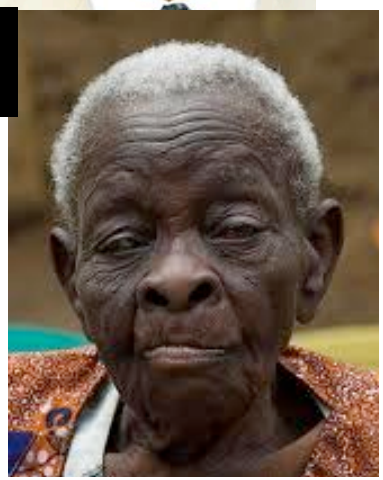
B

C

D

E

F



G

H

J

A

B

C

D

E

F

G

H

J

Facelock

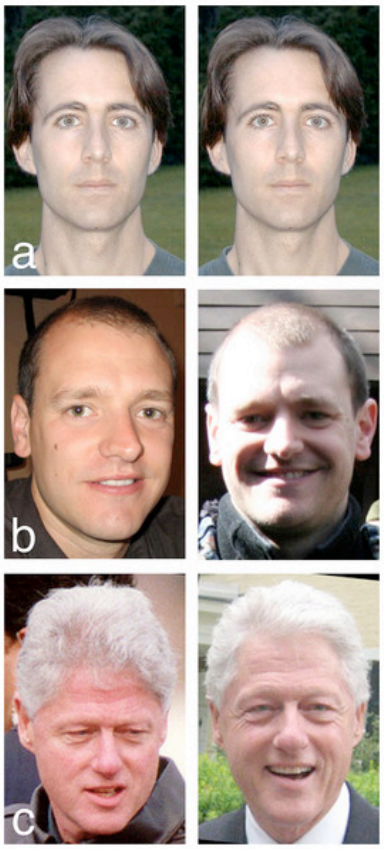
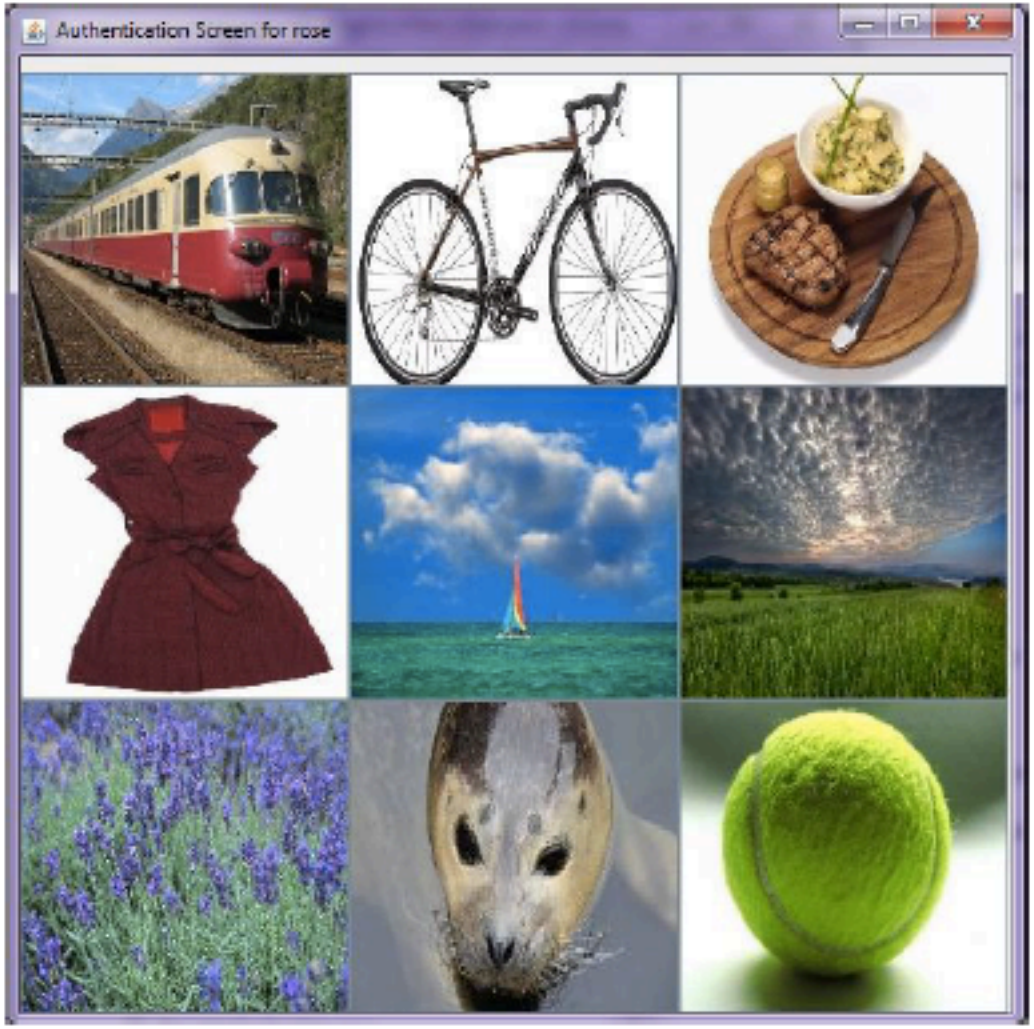


Figure 2: Familiar and unfamiliar face matching.

(A) Matching identical images is trivial. (B) Matching different images of unfamiliar faces is hard. (C) Matching different images of familiar faces is easy.

How many images per screen?



What type of images?

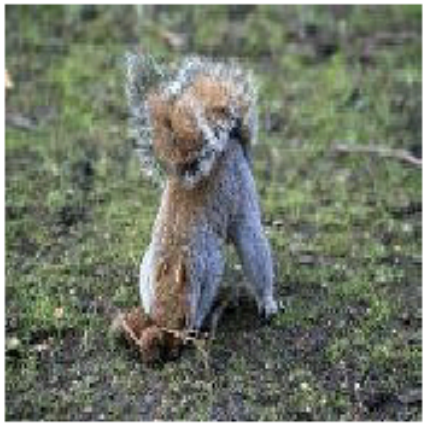
Where will you get the images?

copyright

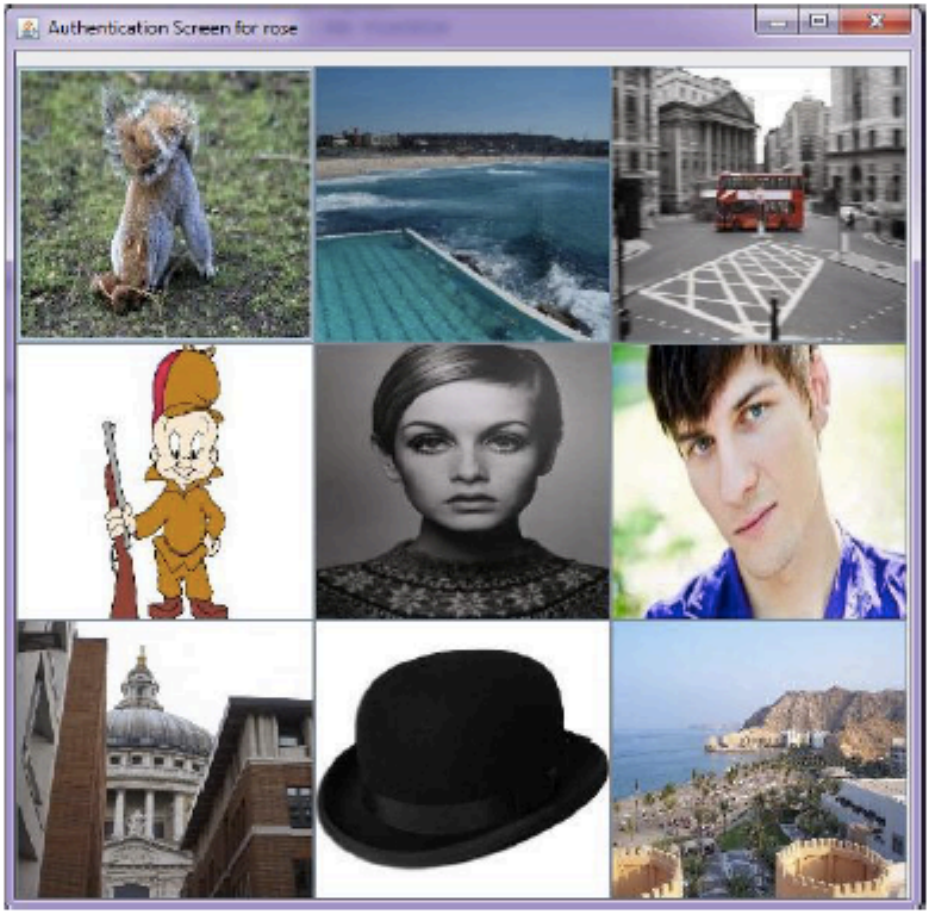
all rights reserved

Can the user pick their images?

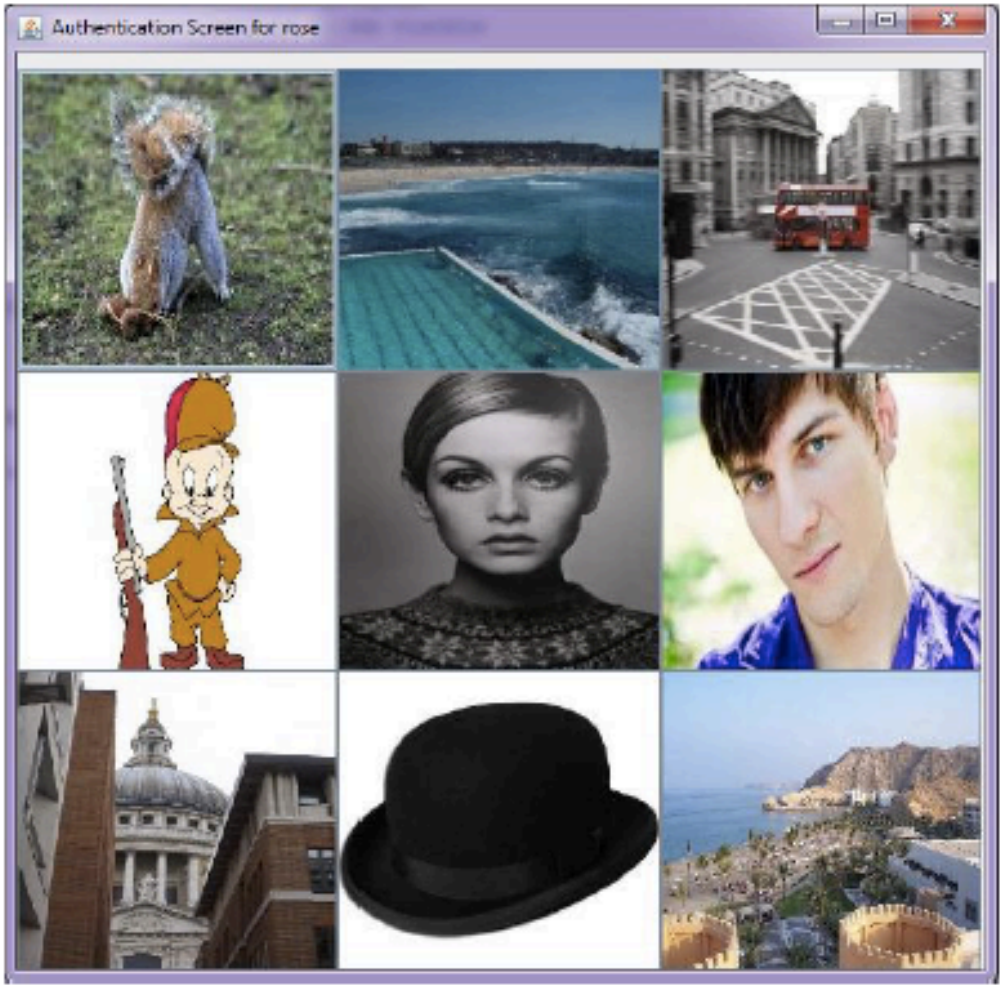
How many images should a user have?

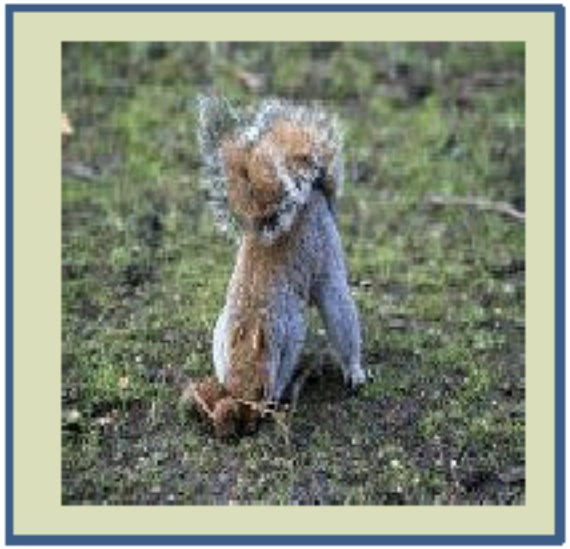
How many challenge screens to authenticate?



How will you pick the other images on the screen?

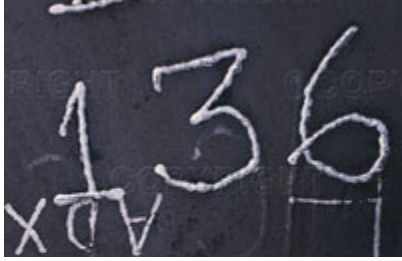


Will you highlight which image has been selected?



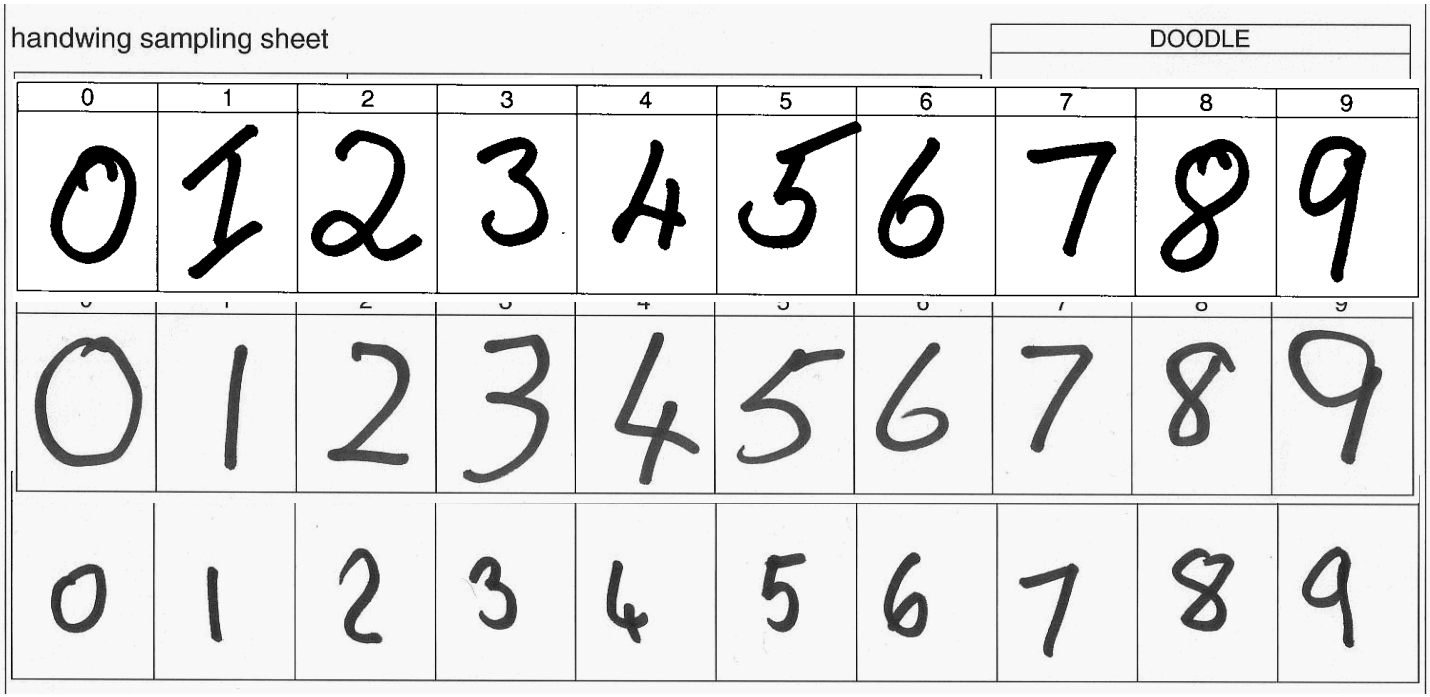

Pic 2 name
Pic 3 is
Pic 4 Robin


RUBBER DUCK
the revolution has begun
YO MAMMA
turestle
NINJA
WCC pod
WappBlog.com
MEET FRANCIS
DORKBOT AUSTIN
wazzup
WHAT A WONDERFUL WORLD
zZZ
THE WARRIORS
it be raining out my eye girl
panda
SEPARATE
I LOVE TYPE
dogs
TRAFFIC

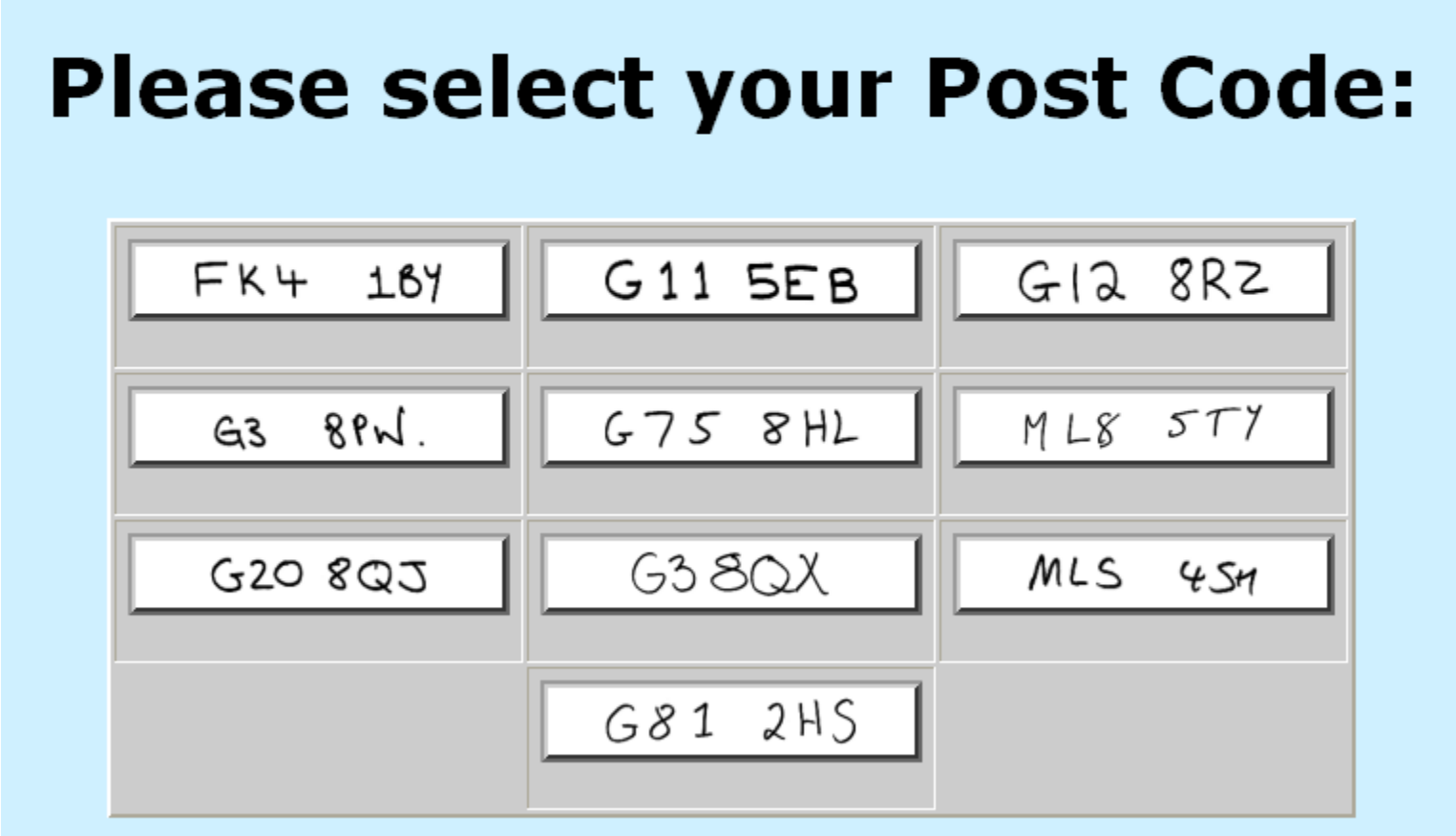


Handwing
Visuo-biometric

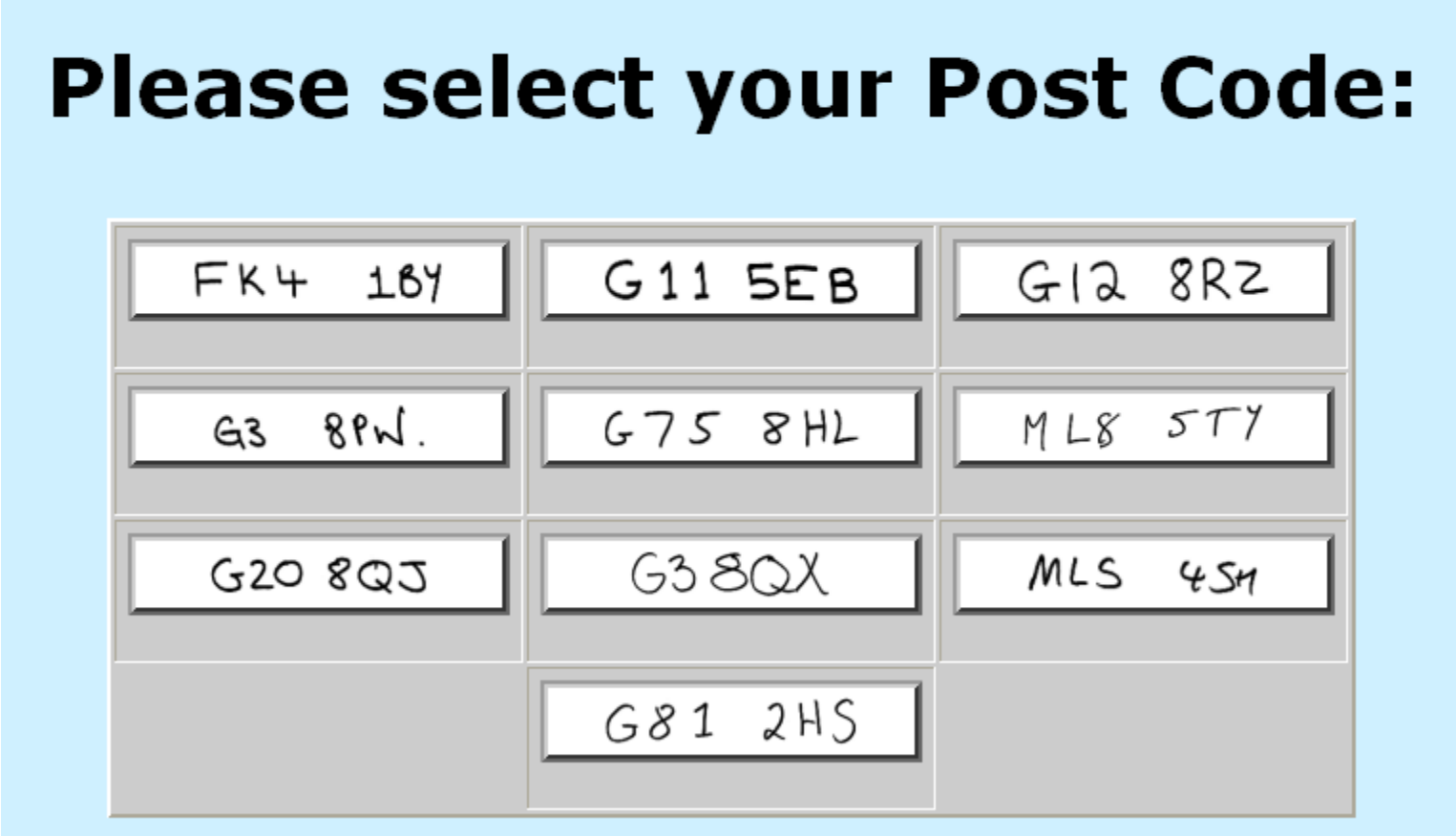
User recognises his or her own handwritten PIN, postal code and doodle



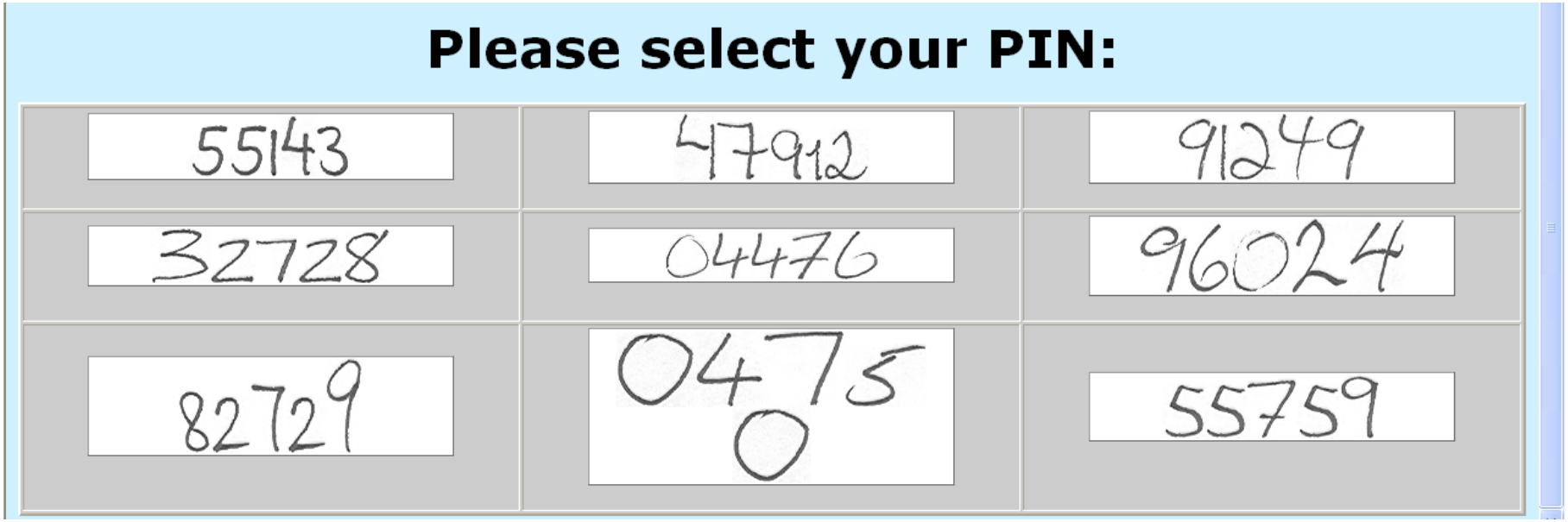
Handwing – stage 2

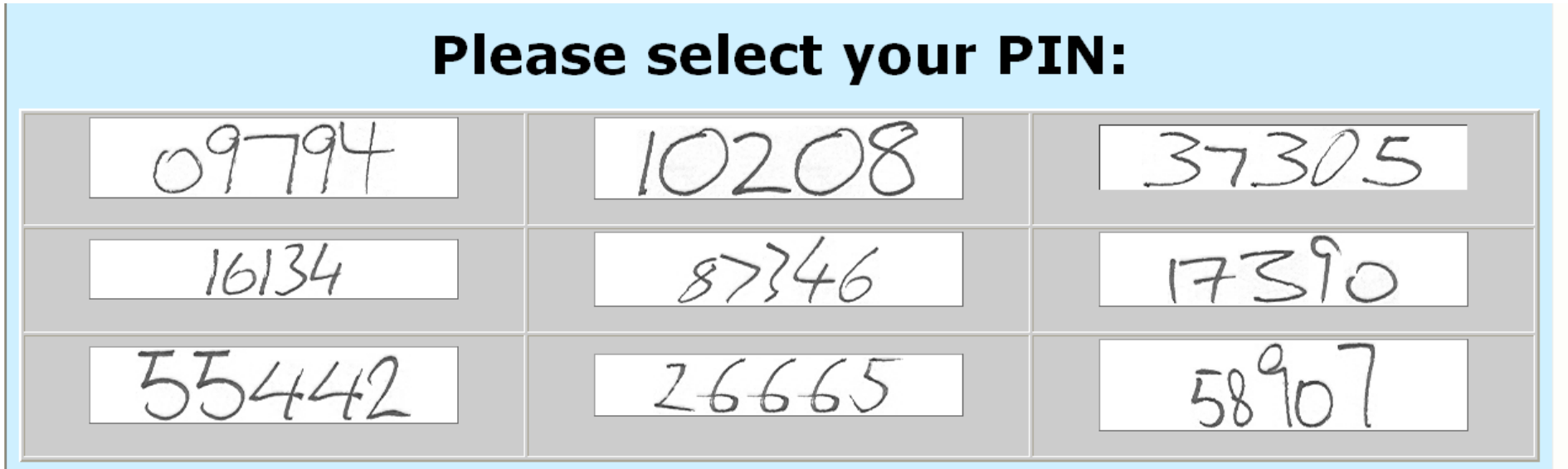


Handwing – stage 2



DynaHand (Olsen & Renaud)





What about Chipping Humans?

Necessary & Sufficient Authentication

- We don’t always need a password
- We don’t always need a “strong” password
- Match the risk level to the stringency requirement

Assurance	Description	Verification	Type	Protection Requirements
1	Little confidence	No verification	Identity only	None
2	Self service apps	Little verification	Single factor	3 times lockout
3	High confidence – access restricted data	Stringent verification	Multifactor	Cryptographic techniques
4	Very high confidence – highly restricted data	In-person registration	Multifactor & hardware	Cryptographic techniques

Judging an Authentication Mechanism (User Experience)

- Ease of Use
- Convenience
  - To Enrol
  - To Authenticate
  - To Replace

Concerns?

- Privacy
- Moving the vulnerability to the human
- How cancelled?
- How well is the data protected?
- Who will gain access?
- What it will be linked to?

Multimodal Biometrics

- Independent evidence
- Deals with missing biometrics
- Harder to spoof
- Challenge-Response possible
- Good performance

Problem Solving

- An ATM manufacturer has approached you to ask you to determine whether they could incorporate an alternative authentication mechanism into their ATM machine to be used in an old age home
- Acceptability & Usability NB!
- I'll randomly choose group(s) to:
  - sell your solution to me

Discussion Topics

- Come up with a personalised password scheme for your grandmother which ensures that
  - Passwords are memorable
  - Yet strong (unpredictable)
  - Is easy enough for your grandmother to use